FFI-rapport 2013/01139

MilTech report 2012

Harald Erik Andås, Tom Arild Blix,
Svein Otto Solheim and Gunn Alice Birkemo

FFI Forsvarets forskningsinstitutt

MilTech report 2012

Harald Erik Andås, Tom Arild Blix,
Svein Otto Solheim and Gunn Alice Birkemo

Norwegian Defence Research Establishment (FFI)

5 June 2013

FFI-rapport 2013/01139

Prosjekt: 1185

P: ISBN 978-82-464-2260-2
E: ISBN 978-82-464-2261-9

Keywords

Technological development

Military technology

Defence planning

Approved by

Sigurd Glærum	Project Manager
Espen Skjelland	Director

Summary

Developments within different technology areas and within specific defence related technologies are important for any small country. It is therefore essential to follow the technological developments in order to decide on which areas to prioritise and follow closely – technologies that could have significant impact on the future of the armed forces. The purpose of this report on military technology is to describe trends within relevant technology areas and to indicate the direction of technology developments. It is based on the report "Trends in military technology – an overview 2004", a result of the former FFI project "Technology and defence after 2014" [1]. The report was welcomed by the military community, but the technological advances since then have made it necessary with an update.

The present report is the result of this effort and should be regarded as an input to the long-term development of the Norwegian armed forces. It is not intended to give a complete overview of the technology field but attempts to describe the technological advances and challenges as fully as possible without going into too much detail.

Technological and operational advance since the last report was published has essentially been in the direction of *combining new technologies*. As an example, progress within the area of unmanned platform systems can illustrate this development. In recent years, attention has centred mostly on applying them for new and more sophisticated operations in the battlefield, not so much on the development of the basic platform itself (with some important exceptions). Hence, various sensor systems, weapon systems and communication systems have been combined and implemented on many of these platforms, something which is still a current development. With this in mind, the findings of this report are summarised in the following main technology areas and trends:

a) *Dismounted soldier systems.*
b) *New fields of application for unmanned systems in the maritime, aerial and ground-based domains.*
c) *Space-based systems for intelligence, surveillance and target acquisition.*
d) *Wide area surveillance underwater, on the surface and on land.*
e) *Open architecture in combat systems.*
f) *Force protection against irregular threats.*
g) *Rapid detection and new types of protection against biological and chemical agents.*
h) *Operations in the cyber domain*.
i) *Modeling, simulation and game technology*.
j) *Terahertz technology*.

It is expected that these technology trends, as well as several others, will be central in the development of future forces. It remains, however, to be seen how far they will be developed and how soon systems and equipment will be employed by the military in real operations.
.

Norsk sammendrag

Teknologiutvikling generelt, og utviklingen innen spesifikt forsvarsrelevante teknologiområder spesielt, er av stor betydning for småstater og kan få avgjørende innflytelse på deres fremtidige forsvar. Det blir dermed viktig for en småstat å følge med på denne utviklingen for å kunne avgjøre hvilke områder som bør prioriteres og følges opp. Hensikten med denne rapporten er derfor å beskrive løpende trender innen relevante teknologiområder og å skissere retningen videre for disse. Den bygger på "Militærteknologiske trender – oversiktsrapport 2004" [1] utgitt under det tidligere FFI-prosjektet "Teknologi og forsvar etter 2014", og bør betraktes som et supplement til og oppdatering av det som tidligere har blitt publisert.

Rapporten bør sees i lys av den langsiktige utviklingen av Forsvaret, men må ikke oppfattes som en fyllestgjørende oversikt over hva som rører seg på det militærteknologiske feltet i dag. Til det er feltet altfor stort. Vårt hovedmål har vært å beskrive de teknologiske fremskrittene og utfordringene så godt som mulig uten å befatte oss med alle detaljene.

Det mest fremtredende trekket ved den teknologiske og operasjonelle utviklingen i dag ligger i *kombinasjonen* av ny teknologi. Som et eksempel kan nevnes evolusjonen av ubemannede plattformer. I dag fokuseres det hovedsakelig på hva disse plattformene kan benyttes til, ikke så mye på utviklingen av selve plattformene (dog med viktige unntak). Diverse sensorer, våpen og kommunikasjonssystemer har blitt innført og kombinert på disse plattformene etter hvert som de er blitt utviklet, noe som fremdeles er hovedtrenden. Med dette som bakteppe kan noen sentrale teknologitrender identifiseres som følger:

a) *Utviklingen av nye systemer for fotsoldaten.*
b) *Nye bruksområder for ubemannede systemer i de maritime-, luft- og landbaserte domenene.*
c) *Rombaserte systemer for etterretning, overvåkning, målfølging og målangivelse.*
d) *Områdeovervåkning både under vann, på overflaten, på land og i luften.*
e) *Åpen arkitektur i stridssystemer.*
f) *Styrkebeskyttelse mot irregulære trusler.*
g) *Rask deteksjon av og beskyttelse mot nye typer biologiske og kjemiske stridsmidler.*
h) *Operasjoner i "cyberrommet".*
i) *Modellering, simulering og spillteknologi.*
j) *Terahertzteknologi.*

Det forventes at punktene som er nevnt ovenfor, så vel som mange andre, vil stå sentralt i fremtidens styrkeplanlegging og i utviklingen av de militære styrker. Det gjenstår imidlertid å se hvor langt utviklingen vil gå og hvor raskt nye systemer og utstyr vil bli utviklet for og benyttet av militære styrker i reelle operasjoner.

Contents

Preface

This work is the result of a team effort at the FFI. As well as the core editing group, several FFI scientists have supported this endeavour. We acknowledge contributions from the following authors:

Halvor Ajer
Håkon Storli Andersen
Lorns Harald Bakstad
Arne Petter Bartholdsen
Jan Kenneth Bekkeng
Ole Ingar Bentstuen
Stian Betten
Øystein Borlaug
Per Andreas Brodtkorp
Lars Erling Bråten
Stein Grinaker
Svein Haavik
Marius Halsør
Svein Erik Hamran
Jon Øistein Hasvold
Mariann Hauge
Bjarne Haugstad
Ole Erik Hedenstad
Harald Hovland
Tor-Odd Høydal
Arne Cato Jenssen
Greger Johansson
Bjørn Arne Johnsen
Ørnulf Kandola
Frank Åge Kippernes
Stein Kristoffersen
Kirsten Kvernsveen
Jørn Kårstad
Rune Lausund
Torleiv Maseng
Arvid Melkevik
Bjørn Mikkelsen
Erik Nordø
Asgeir Nysæter
Atle Ommundsen
Richard Olsen
Guro Rognsvåg
Ole Jakob Sendstad
Marte Elisabeth Skogvoll
Knut Stenersen
Nils Størkersen
Torkjel Søndrol
Ivar Tansem
Bård Tokerud
Tore Ulversøy
Jan Erik Voldhaug
Ronny Windvik
Alf Lars Ødegård
Hans Øhra
Einar Østevold
Torunn Øvreås

1 Introduction

Developments within different technology areas and within specific defence related technologies are important for any small country. It is therefore essential to follow the technological developments in order to decide on which areas to prioritise and follow closely – technologies that could have significant impact on the future of the armed forces. The purpose of this military technology report is to describe trends within military technology areas and to indicate the direction of technology developments. The report was edited by a core team, but is based on contributions from more than 50 scientists at FFI.

One of Norwegian Defence Research Establishment's (FFI) main tasks is to follow the scientific and military technology developments worldwide, and give advice to the military and political leadership regarding the future force structure and material procurement. This is achieved through analyses supporting long term defence planning, reports from FFI's many technologically oriented projects and through continuous consultation. FFI does occasionally present an overview, in the form of a report, of the evolution and importance of military technology, one of which was the TEK14-report on trends in military technology trends published in 2004 [1].

The current report is a follow-up and extension of the TEK14-report and gives an overview of projected trends in military technology from 2012 onwards for roughly a decade. The material has been organized into chapters mainly based on the platform-centric approach inherited from the previous report. Chapter 2 focuses on land platforms and associated systems, while Chapters 3 and 4, respectively, have a similar approach towards the sea and air domains. Missile systems are treated separately in Chapter 5, whereas Chapter 6 considers developments in space. CBRN-related topics are discussed in Chapter 7 and issues regarding information operations in Chapter 8. Chapter 9 considers CCIS and networks, while Chapter 10 finally discusses various military-related technological themes of interest.

We emphasize that this report does not give any definite advice on Norwegian defence procurement. The report does, on the other hand, aim at presenting a firm foundation for understanding technological trends which can affect Norwegian long term defence planning. The report does not cover every defence related technology development, but it describes the most important trends and examples as they appear today. Additional work is needed to elaborate on the consequences of these trends for defence planning. An analysis of these issues is currently being addressed by the FFI [2].

The collaborative nature of this work unavoidably entrains a certain inhomogeneity in choice of topics to be discussed as well as in effort. Consequently, the level of detail and complexity will vary between topics treated by different authors. Likewise, this may also apply to the format of references et cetera.

The report is kept unclassified in order to increase knowledge about military technology amongst a wider circle of readers and to be used in forums where future Norwegian force structure is on the agenda. Hence, a number of relevant, but classified, technical details are not included in the report. The report is written in English since it is also intended to be used in different technology forecasting collaboration groups (e.g. NATO, ANNC and NORDEFCO). Editing of contributions was completed in June, 2012.

2 Land Platforms and Subsystems

2.1 Dismounted Soldier Systems

2.1.1 Introduction

The development of Dismounted Soldier Systems and components and equipment for soldiers in different operational roles and environments has been an important area of research over the last 10–15 years. Therefore, Norwegian soldiers have access to better ballistic protection, squad-level internal communication and more accurate navigation systems today than 10 years ago. A few specialists also have access to digital map based situational awareness equipment, e.g. Forward Air Controllers. In addition, the development of the NORMANS (Norwegian Modular Arctic Network Soldier) C4I system [3] has given a prototype system that will be introduced into service within the next few years. A NORMANS-equipped unit will have an individual soldier system that gives each soldier in a section better navigation, blue force tracking and an improved command and control system. The more advanced NORMANS commander system will be a digital map based system for each commander and each specialist within the dismounted unit. Tests and evaluations of NORMANS C4I system in the definition phase of the procurement programme prove a significant increase in the combat unit's effectiveness. According to the acquisition plan, the first operational NORMANS C4I system will be implemented in the period 2012–2016.

A soldier system is by definition all the equipment the dismounted soldier carries and consumes to fulfil his or her tasks, see e.g. [4]. NATO has defined five capability areas for soldier systems. These are Lethality, Survivability, Sustainability, Mobility and C4I. No soldier systems will operate as standalone systems. In a mechanized manoeuvre unit the soldiers will operate in close co-operation with the units fighting vehicles. In other operations soldiers and soldier systems will operate organically with other units like fighter aircraft (FAC) and artillery (OP). The integration of soldier systems with other platforms and systems will therefore be highly prioritized.

One of the most focused areas for future research is to improve the soldier's situational awareness and reduce the soldier's physical as well as cognitive burden. More intuitive Human-Machine Interface systems using Augmented Reality will be developed. New equipment in all capability areas will focus on light weight materials, adaptive solutions and Tactics, Techniques and Procedures (TTP) highly focused on accurate and timely target hand-off.

2.1.2 Lethality

Dismounted soldiers have three main contributions to the delivery of adequate weapon effects. These are personal weapons, portable high effect weapons and sensor systems for target handoff.
Personal Weapons: These weapons include self defence weapons, assault rifles and weapons for delivery of Less than Lethal effects. The focus on weight reduction will within the next 10 years result in new ammunition using lightweight casing materials. Several parts of the weapons, including barrels, may be built using composite materials. It is also likely that case-less

ammunition will be introduced in some weapon systems before 2020. Throughout the last decade there has been a high focus on Less than Lethal effect weapons for dismounted soldiers. The development of Less Lethal Weapons has matured in recent years, and a large variety of options for individual soldiers and land warfare platforms are available. Currently, almost all NATO countries have fielded LLWs, and analyses and statistics from operational use are starting to appear. Most nations use LLWs for one or more of the following tasks:

- Riot control
- Warning
- Neutralization or arrest of individuals
- Neutralization of buildings
- Area denial for individuals
- Area denial for vehicles
- Stopping vehicles
- Stopping vessels

Major arms and ammunition manufacturers have caught on to the LLW trend, and are now producing military grade equipment. Previously, the market was dominated by smaller companies producing LLWs for law enforcement. Differences between products for police and military users are mainly in ruggedness and range. The police are usually satisfied with 5–10 meter ranges, while military users would like 40–50 meter range against individuals and 100+ meters against crowds, this in order to engage suspected suicide bombers etc. outside their lethal range.

2.1.3 Survivability

Protection against ballistic threats is crucial for the soldier's survivability. The focus on light weight materials has been and still is an important driver for developing improved materials and protection solutions. Low-weight solutions give the opportunity to increase the protected area, upgrade the protection level or simply gain better mobility.

Protection against shrapnel is achieved through fibre fabrics. The widely used fibres are Aramid fibres, such as Kevlar and Twaron, and high density polyethylene (HDPE), such as Dyneema or Spectra. Numerous grades exist, and more grades will probably appear in the years to come. However, these will most likely be small improvements and optimizations. Currently, there is no known upcoming fibre at this moment that would radically change the level of protection during the next few years. The most promising new development was the so-called M5 fibre, but after a decade of research it is still not commercially available. However, new production techniques for the M5 fibre have been proposed, and several research establishments have started to investigate new fibres with even better properties than the M5 fibre. Thus, the push towards lighter protection for future soldier systems has boosted this development and it is likely that new fibres will be developed within the next 10 years.

Protection against small arms threats is achieved through combinations of ballistic fibres and ceramic plate inserts. The most common ballistic ceramics for personal protection are alumina, silicon carbide and boron carbide. Although transparent ceramics are very promising, these types

of materials will most likely not be used for personal protection. They are, however, currently being introduced for use with military vehicles.

Most of the latest improvements seen in the field of personal protection are in optimizing the combination of materials and how they are assembled. One example is adding impact-absorbing materials in order to improve the in-service durability. Another example is using different grades of ballistic fibres in order to optimize the energy absorbing ability as the threat is penetrating the various layers.

Signature management for the dismounted soldier is an integral part of survivability enhancement. In general, modern sensors are good at detecting single soldiers, particularly night vision systems in near infrared and thermal infrared. This threat is clearly increasing not only with regard to single soldiers, but also their unit and its ability to perform its task and to survive.

Current approaches to reducing the signature of the Battle Dress Uniform (BDU) in a multispectral sense will continue. Often, the solution will be to develop materials and systems that are passively adaptive to the background such as sniper guile suits in the thermal spectrum. More focus will be on developing such capabilities to BDUs that can be used in more general operations without compromising performance in terms of weight and flexibility, and avoiding interference with personal equipment.

There will also be developments in personal signature management equipment. Currently, two-sided, lightweight 2-D net, with multispectral properties is a promising approach. In the next decades results from nanotechnology with respect to better optical properties will emerge. It is still unclear if actively adaptive colours and reflectance will be of practical use, but at least for special applications this can be expected.

2.1.4 Sustainability

Future soldier systems will use more sensors and more CPU power regarding energy. Within the next 10–15 years fuel cells will play an important role in combination with rechargeable batteries. Batteries with higher energy density will be introduced, such as Li – Air. Electronic devices will become more power effective, and more intelligent power management systems will be implemented. The most innovative developments will probably be in energy harvesting systems to charge the soldiers batteries, such as thermoelectric systems used in cold weather operations.

New textiles using nano-technology coatings, and new clothing systems specifically tailored for better protection will, in addition to increased CBRNE protection, give better fire protection and increased sustainability in a various climate conditions.

2.1.5 C4I

The need for enhanced situational awareness, more accurate navigation and better target information will require further development of the soldier's C4I system. The technological development will continue, and within the timeframe give significantly better performance in CPU power, displays, sensors and software systems. The main challenge in this area is, however, not the technology, but how the different C4I systems are implemented, integrated and used operationally. A combat capability requires that the acquisition programmes for radio systems, sensor systems, battle field management systems on all platforms, soldiers included, are coordinated, tested, evaluated and fully integrated within the combat unit. It also requires that tactics, techniques and procedures are developed to effectively use new technology when introduced. NORMANS C4I trials clearly show the increased combat effectiveness when new C4I technology is implemented in an Army combat unit [5].

Figure 2.1 Left: The NORMANS C4I System provides C2, navigation aid, blue force tracking as well as a user friendly planning tool. An advanced situational awareness system for the commander combined with a lighter system for the individual soldier raises a dismounted maneuver unit's effectiveness by 30–40 % over baseline (photo: Thales). Right: NORMANS C4I System used in operational evaluation (photo: FFI).

Technology wise, the US Army focuses a lot on using smart phone technology for soldier systems. These new devices will in the short term be linked to the tactical radio systems similar to how e.g. NORMANS advanced will be linked into current radio systems. In the longer term we will, however, see the devices hooked up as "network devices" to tactical networks. Due to legacy issues this will take years to implement, but research is ongoing and technology is rapidly under development in the civilian industry. Furthermore, lightweight augmented reality systems will be developed and probably introduced into service within the next decade.

2.2 Combat Vehicles

2.2.1 General Discussion

For combat vehicles, it is natural to review performance, technological status and evolution in four main areas: i) protection, ii) mobility, iii) firepower and iv) command, control and information systems, or what we in more general terms could call decision support. Although there are ongoing developments within all four areas, it is probably the development of decision support, adapted to Network Enabled Capabilities, including Battlefield Management Systems (BMS), which will bring about the most fundamental changes in military thinking and operations. We will therefore review the subjects in the above mentioned sequence. Sensors, power supply and autonomous vehicles will also be discussed.

2.2.2 Ballistic Protection

Within the field of passive protection, new materials giving substantially better passive protection per weight unit than steel are emerging. Ceramic armour, composites and not the least laminated structures are being introduced, initially as additional protection, but will gradually become a part of the main structure of the vehicles. In the longer term we can foresee a further development of carbon fibre, including nanostructures. Currently, the majority of these materials are very expensive, but prices will probably drop.

Another important protection effort is within vehicle design in order to mitigate the damage the impetus from IED and mine detonations will have on vehicle personnel. The development of Active Protection Systems (APS) is ongoing, and the first systems have been fielded, like the Israeli Trophy system on Merkava Main Battle Tank. APS offers adequate protection of even lightweight vehicles for a relatively small weight penalty. Most APS are designed to stop shaped charge weapons, but we will probably experience a development towards systems having substantial effect against kinetic energy weapons as well.

Figure 2.2 Left: APS – Hemispheric shield (source: IBD). Right: FFI demonstrator/test-bed (photo: FFI).

2.2.3 Tactical Mobility

Weight is an important factor for mobility, and any effort that contributes to keeping the weight down improves mobility. The following developments should be mentioned:

a) Rubber tracks: Reduces weight and operational reliability and increases comfort. Can probably not be used on the heaviest vehicles. A large part of our M113s, including all recently modified versions, have rubber tracks, the CV 90 has been tested with them, and they are now an option for the CV 90 upgrade.

b) Semi-active or active suspension [6]: Improves mobility on rough surfaces substantially; increases comfort, enables higher speed, more payload etc. It is being developed now and will probably appear on wheeled vehicles first, where the gains are highest. We will probably see semi-active systems long before fully active systems are available.

c) Hybrid electrical propulsion [7, 8]: Offers several potential gains. The basic technology exists, but practical and economical solutions for military vehicles have still not reached the market. It will probably appear within the next 5–10 years, most likely through the introductions of new variants of existing vehicle types or the development of new generations of vehicles.

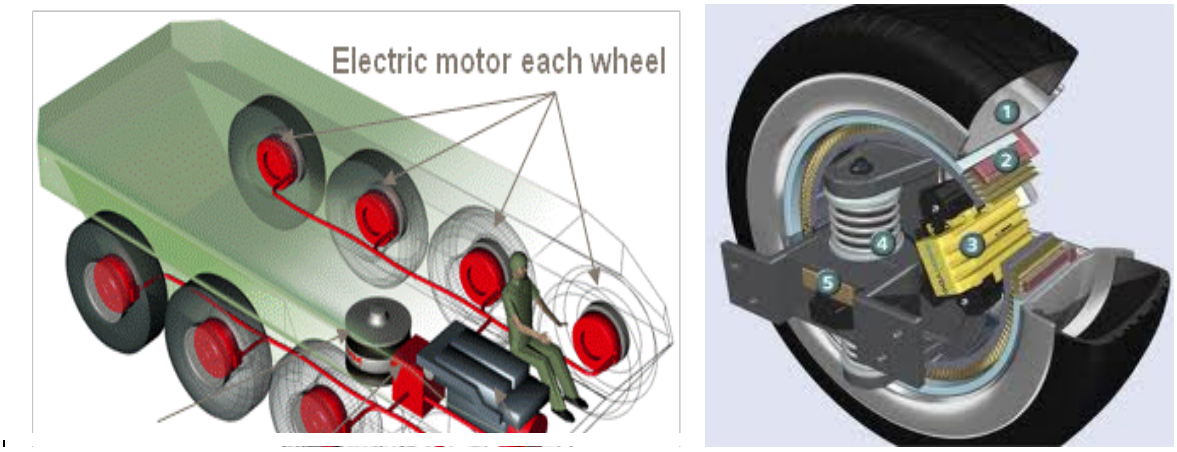

Figure 2.3 Left: Hybrid electric vehicle (source: FMV). Right: In-hub electric motor (source: Drives & Controls Magazine).

2.2.4 Firepower

With respect to the near-term developments regarding fire power for combat vehicles the following should be noted:

a) Remote weapon station (RWS): Enables firing of weapons under protection, faster and more accurately than before. This is based on current technology, but will be improved and redesigned for a wider range of weapons and even better performance. The RWS sensors will also contribute significantly to situational awareness (SA).

b) Automatic tracking in fire control systems: This may be fire control for own weapons (e.g. RWS) or fire control for others (e.g. mortars or artillery). BMS will be integrated with the fire control system.

c) Unmanned turrets: This will offer better protection for the crew and reduced weight, contributing to faster slewing of the gun. The new Russian main battle tank, T-95, will probably have an unmanned turret. Kongsberg Protech Systems is developing an unmanned turret for medium calibre (30–50 mm) guns [9].

d) Integration of various missile systems on RWS and unmanned turrets, e.g. the anti-tank missile Javelin [10] and possible developments of low-cost precision weapons such as 70 mm rockets with guidance kit.

e) Programmable ammunition (air burst) for e.g. Infantry Fighting Vehicles (typically 30 mm gun) and Main Battle Tanks (typically 120 mm gun) is being developed and will be available in a few years time. This type of ammunition may significantly increase the effect of vehicle gunfire against soft and semi-soft targets, and will also have effect on targets that otherwise cannot be engaged by direct fire.

f) Less lethal weapons: This is an area where a lot of resources are invested; some are relevant for vehicles. Many different technologies, including micro waves, directed energy weapons (DEW) and sound, as well as non-lethal ammunition for 40 mm AGL.

Figure 2.4 Left: Kongsberg's Remote Weapon System, Protector. Right: Protector mounted on an Iveco vehicle (photos: Kongsberg).

With regard to long-term developments, the following technologies are being investigated:

a) Electro-Thermal-Chemical (ETC) gun [11]: Exploits electromagnetic energy in addition to chemical in order to increase and control the initial velocity of the projectile. ETC gun requires far less electric energy and is also technologically a more feasible solution than potential alternatives like coil gun or rail gun (see below). The system has been under development for years, but is still not mature.

b) Coil Gun and Rail Gun [8]: There exist different solutions for electromagnetic guns. Has been under development for years, but there are huge challenges. It's doubtful that these

technologies will be applicable for vehicles, though coil gun could be developed into a vehicle gun firing lower velocity ammunition.

c) Hypervelocity missile (HVM) [12]: It's challenging to design systems that are compact enough for practical application by vehicles. Could be realized within 5–10 years, but the lowered priority of the traditional anti-armour warfare has reduced the efforts spent on this technology.

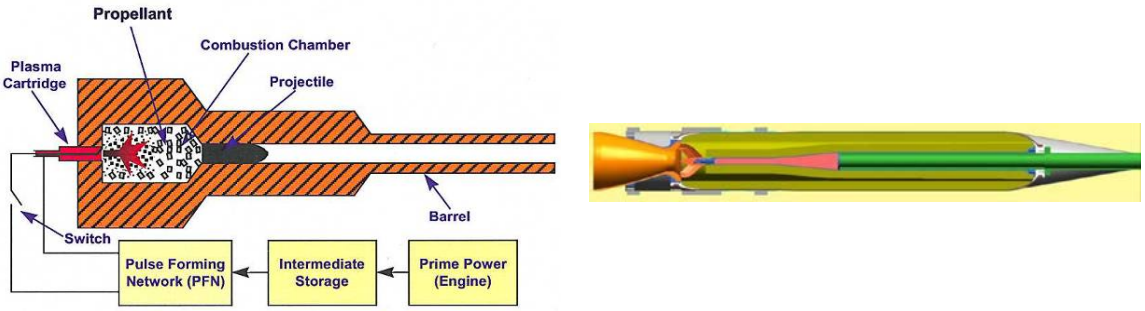

Figure 2.5 Future weapons for vehicles – Left: ETC Gun. Right: Hypervelocity missile (CKEM) (source: Nammo Raufoss).

2.2.5 Situational Awareness (SA) – Decision Support

Battlefield Management Systems have been available for some time. A temporary Norwegian system (NORTaC BMS) has even been used in international operations, and the Norwegian army has recently selected Teleplan's NorBMS (formerly FACNAV) as its BMS. Thus, the technology for a "basic" BMS exists and is mature. However, a BMS requires more than technology to give full effect. As part of the crew's situational awareness, as well as of their command and control structure, it requires training, understanding of the system and possibly changes in doctrines and procedures to yield full effect. This can, and probably will, be realized within a few years after a common BMS is available to all units and used in training and operations.

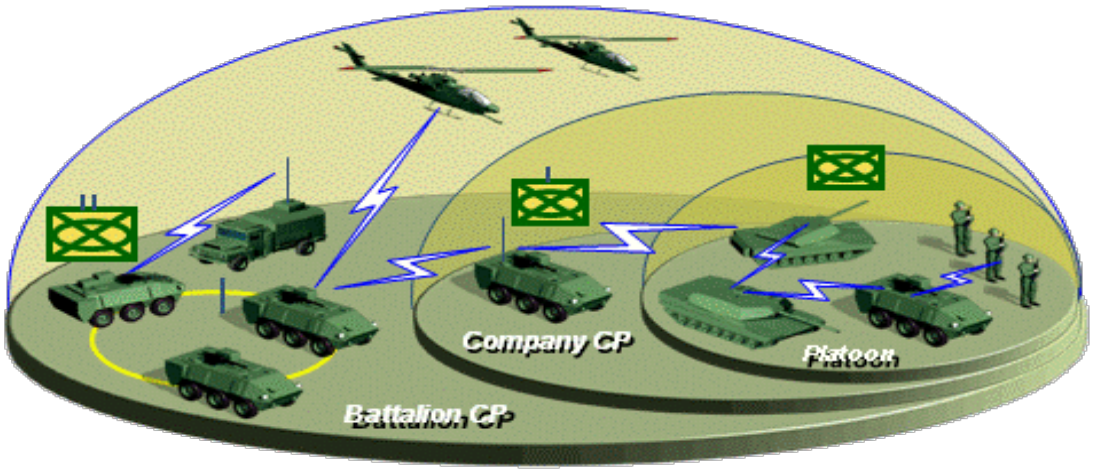

Figure 2.6 BMS and network, from the individual unit (vehicle and soldier) to Battalion level (source: Thales).

Apart from the basic BMS functionality, which comprises primarily map functions, blue force tracking (BFT) and data collection, more advanced functions will probably emerge in the near future. Perhaps the most interesting technology is Augmented Reality, (AR), which will give the users easier access to the BMS information by displaying this information directly, and in correct position, in the vehicle sights, i.e. in the image of the scene. This will take the BMS from being (primarily) a planning, manoeuvring and after action review tool to a support tool also in time critical operations, like the actual combat. An AR system may also be used as an IFF (Identification Friend or Foe) system, to avoid blue-on-blue incidents. For this purpose one needs, however, timely information about the position of own units. Currently a BMS transmits its own position at best once every 10 seconds, in many cases closer to once per minute. Even this can be useful, but to get full effect from AR used as IFF, this time should preferably be reduced to around 1–2 seconds, at most. This can probably be achieved by using two radios, one with high bandwidth for short distances, and one with longer range, but lower bandwidth. Or the job can be done by so-called Software Defined Radios (SDR) [13], currently being developed. These radios will be tuneable on range and bandwidth, and will probably be on the market in about five years.

Figure 2.7 Augmented Reality (AR) – Information in BMS is displayed in the image from the day sight of CV90 Infantry Fighting Vehicle (source: FFI).

Given radios with higher bandwidth, more functionality becomes available in a BMS. One could for instance request images from a UAV or other vehicle, or perhaps even live video.

A BMS should also be able to communicate seamlessly with higher level systems, such as the tactical C2IS. This requires the ability to automatically transmit information between systems having different security levels. This is not only a matter of technology, but also a matter of regulations and formalities related to security. Hopefully these problems will be solved within 5–10 years. Another important issue is standardization, or rather lack of standardization. Though there is a lot of effort put into standardization, different companies and nations still tend to develop their own solutions, hampering integration and communication between systems and nations. Moreover, each nation seems to develop their own BMS, so that the sharing of information between BMS from different nations participating in the same operation becomes difficult or even impossible. The exchange of information must then be on a higher level, increasing the security challenges and reducing the timeliness.

2.2.6 Sensors for Situational Awareness

Combat vehicles will in the years to come steadily be equipped with new sensor types, primarily to increase the crew's situational awareness while still being protected by armour. Some types of vehicles, like reconnaissance vehicles and fire control vehicles, will be equipped with long range sensors (typically radar and electro-optical sensors with day and night camera, and possibly low-light camera), whereas (typically) combat vehicles will be equipped with sensors covering the immediate vicinity of the vehicle, primarily for self protection purposes. Examples of such sensors are panoramic camera (360°, day and night camera) and acoustic sensors (for sniper detection, warning of helicopters, UAVs, enemy vehicles etc). In the longer term, hyperspectral cameras, laser scanners (e.g. for detection of snipers prior to shot) will see a market for vehicle applications. An important trend is implementation of image analysis in imaging sensors, so that these sensors will go from being pure observation aids to being autonomous systems for alert and fire control (hunter-killer capability). Firing will, however, due to Rules of Engagement (RoE), probably still require man-in-the-loop.

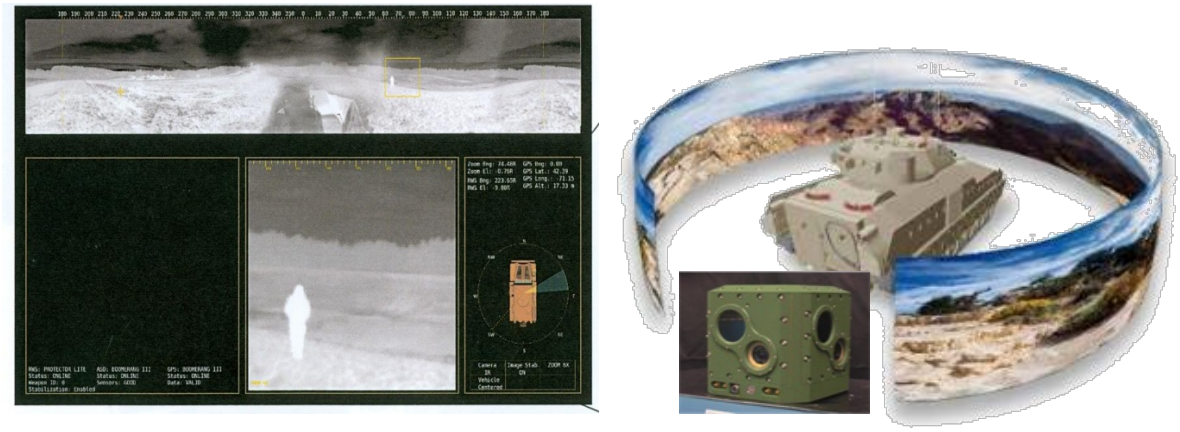

Figure 2.8 Panoramic camera – Operator's screen (left), 360° view (right), Camera assembly with 4 IR and 4 visual cameras (inserted) (source: Kollmorgen).

High level sensor fusion and integration of sensor systems with the map based user interface of BMS is already underway. A lot of challenges still remain, however, concerning low level fusion between different sensor types, for instance combined acoustic-optical shot detection in order to provide more reliable detection of snipers in cluttered and/or noisy environments.

2.2.7 Power Supply

More and more systems that require electrical power are steadily being introduced in vehicles. In addition, there exist operational requirements for silent watch and silent operations, in particular for reconnaissance missions. Various types of additional (auxiliary) power units (APUs) are being developed, including optimized (small) diesel generators, fuel cells and small gas turbines [14]. Diesel generators are based on today's technology and will probably be the first to appear in vehicles. However, to achieve even more quiet-running engines, one must probably resort to fuel cells. Within this area there are many challenges, and we will have to wait some years until we see a viable fuel cell based APU for military vehicles realized. Gas turbines represent a more mature technology, but have the obvious drawback of being quite noisy.

APUs have to operate in conjunction with a battery system serving as an energy buffer. Li-Ion batteries stand out as the best technology concerning energy and power density. There are, however, safety problems that need to be solved, but there is a lot of ongoing research in this area.

2.3 Land Based, Indirect Fire

This section briefly discusses some technological trends within the area ”land-based indirect fire” (denoted artillery in the remainder of the section, but including both traditional effectors like mortars, tube- and rocket artillery as well as mini missiles). The trends being discussed have a range of time frames; from currently available systems to systems that only have reached demonstrator level. The first group is discussed here because it is not yet implemented in the Norwegian Armed Forces and because it brings along considerable change in capabilities and roles for the artillery.

It is useful to divide technological trends with corresponding consequences into a few principal themes:

- Delivery systems
- Warheads
- New concepts / systems

Delivery systems are constituted by ammunition and firing platforms. The traditional types are bombs and shells fired from mortars and guns (often howitzer), respectively, and rockets from launchers. Through a number of years, an effort to develop guided munitions based on various guidance principles has been ongoing.

Some delivery systems have been put into operational use during the last several years. This includes upgrades in the form of guided rockets for MLRS (GMLRS) with unitary warheads in particular. This system delivers GPS/INS-guided warheads in the 200 lb range, slightly smaller than the Small Diameter Bomb (SDB). This means that one MLRS-launcher (M270-based) can deliver 12 GPS-guided warheads in one salvo up to a range of 70–90 km. The system has already seen service in Iraq and Afghanistan. The system characteristics make it suitable to maintain fire readiness over time and with availability unaffected by weather or light conditions. This makes it a good alternative to Close Air Support (CAS) (with supporting tankers, other support units and also limitations on availability) in some scenarios. GPS/INS-guided munitions from tube artillery have in a corresponding manner been put into operational use through the use of Excalibur. Warhead and effects are comparable with ordinary 155 mm ammunition, but the precision is equivalent to other GPS-guided weapons. In general, there are ongoing developments to improve precision, with some programmes being terminated and some continuing. In addition to precision guidance, there are also ongoing developments of systems that are meant to compensate for delivery errors (Course-Correction Fuses – CCF). A modified 120 mm mortar bomb with course-correction was planned to be delivered to US forces during the first part of 2011. Precision delivery also for smaller-calibre ammunition types is being developed.

The second principal component that deserves comment is the warhead. The most important development is the Sensor Fused Warhead (SFW). Albeit available since the 1990s, the utilization of SFWs has not reached the same extent as precision delivery, which can be explained by a combination of availability and the nature of recent conflicts. Known employment of SFWs has been in the latest war in Iraq and includes the use of SADARM (155 mm) and the air delivered variant BLU-108. In both cases the results in terms of effect and cost efficiency were very good. SFWs have been integrated with the GMLRS, providing a precision delivery of 4 SFWs per rocket at ranges of 80 km+. As of late March 2011, no contracts appear to have been concluded for this product. The Russian system SMERCH (300 mm) with 5 SFWs in each missile (unguided) is another example.

The developments in warheads and delivery systems bring about a significant change in the roles and capability for traditional artillery. In addition to non-lethal effects like screening (smoke) and illumination (light), the capability traditionally consisted primarily of effects on area targets, depending on the target hardness and target density. For both hard and semi-hard area targets, a large effort with cluster munitions (now forbidden) was required, and for hard targets there was in reality a requirement for rocket artillery. With current warheads (SFW) and precision capabilities, land based artillery can achieve destructive effects, often with moderate effort, on nearly the whole range of targets, from point targets to area targets and from soft (personnel) to hard (MBT) targets. A force with such a capability combined with satisfactory target locating systems and situational awareness, could neutralize substantial parts of opposing force without close contact between the manoeuvre units. The ability to protect friendly units against such weapons will hence be important.

Another interesting concept that has surfaced recently in the warhead category is the development of warheads with scalable effects. That is, the explosive power in each warhead can be adjusted to suit each target and situation (equivalent to ”Dial a Yield” – warheads for nuclear weapons). The status of this programme is unknown, but demonstrations have been performed, and development is said to be ongoing for a customer [15].

Another trend is the development of alternative concepts/systems [14]. One concept that differs considerably from existing ones is the use of loitering missiles. Currently, such concepts are mainly in the development stage with programmes going on in the US, UK and Germany. These systems can be characterized as disposable UAVs with an attack capability. This will potentially give a very short sensor-to-effect time. Additionally, such systems can contribute to information gathering.

2.4 Ground Based Air Defence Systems

The trend in Ground Based Air Defence over the last decades or so has been a change in focus from opposing the traditional fighters and helicopters, i.e. the platforms, towards countering opposing missiles, i.e. weaponry. This is partly due to the fact that tactical ballistic missiles have evolved from a threat to deployed forces, towards a threat to the homeland of countries in Europe, America and Japan from countries like Iran and North Korea. There is a great US emphasis on

putting a flexible missile defence system in place based on a distributed sensor network and Standard Missile-3 (SM-3) interceptors. The plans for developing both the sensors and the SM-3 missile extend to 2020.

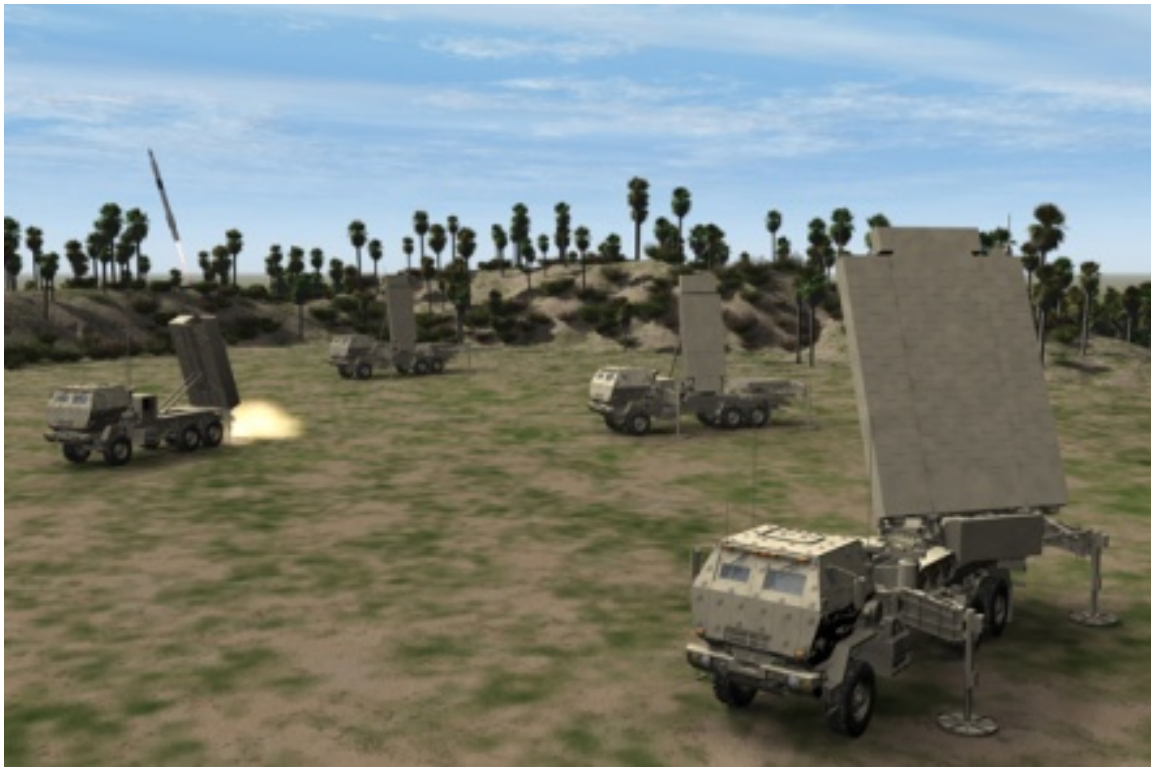

Figure 2.9 Artistic impression of MEADS (source: meads-amd.com).

With respect to lower layer air defence the emphasis has been on countering cruise missiles. The reason being the proliferation of cruise missiles and that air delivered missiles can be launched from distances where the delivering platform itself is out of reach for medium range ground based air defence systems. There are a number of ground based air defence systems in service or under development in the West today. Even if Western air superiority in recent conflicts tends to be taken for granted, one does not deploy forces without ground based air defence. This is partly, as mentioned above, because of the threat from tactical ballistic missiles (TBMs). To oppose the threat from TBMs the PATRIOT system is commonly used. This system has been operational since 1984, and has since been through a number of upgrades.

The US, Italy and Germany is collaborating on the development of a new medium altitude ballistic missile-defence/air-defence system – MEADS (Medium Extended Air Defence System). The original intention was to replace the HAWK and NIKE HERCULES systems and supplement the PATRIOT systems in the three countries. Germany and the US stated early in 2011 that they will only fund the system up to development. Further funding, up to procurement, is uncertain. The US is reported to field the THAAD (Terminal High Altitude Air Defense) system for a dedicated theatre ballistic missile defence role.

Figure 2.10 THAAD radar installation to the left and a missile launcher to the right (source: fas.org).

Although there has been focused on ballistic missile defence, the traditional threat; fighters, helicopters and cruise missiles, is still relevant. An example of the medium range ground based air defence systems in operation today, is the Norwegian NASAMS that has been procured by a number of countries. NASAMS is a product of the Norwegian company Kongsberg Defence System and Raytheon. Raytheon is also developing the SLAMRAAM system for the US Army, a system with great similarities to the NASAMS. However, this program was cancelled by the government early 2011 due to budgetary constraints.

As mentioned above, fighters and attack helicopters still pose a threat to ground forces, which means that short range air defence systems (SHORAD-systems) are still an essential capability for the manoeuvring army units.

There are trends towards a more open architecture in air defence systems, caused by the need to integrate sensors and weapon that are more or less tailored for the operational requirements. Another trend is to use the existing air defence systems in a CRAM (Counter Rocket, Artillery and Mortar) role as a static base defence. Traditional air defence systems can detect incoming targets and give early warning, but new interceptors will probably be needed to counter incoming fire.

2.5 Unmanned Ground Vehicles

Unmanned Ground Vehicles (UGVs) is now being introduced into most countries' military forces. Disposal of suspicious objects (EOD) is still the main task, but over the last few years it has become more common to employ UGVs in support of military operations. The main development trends for UGVs are currently automation and collaboration, making it possible for one person to control multiple UGVs. There is also development of systems able to carry equipment and supplies in order to reduce the load the soldiers need to carry themselves. The aim is mainly to improve the mobility and endurance of dismounted military units.

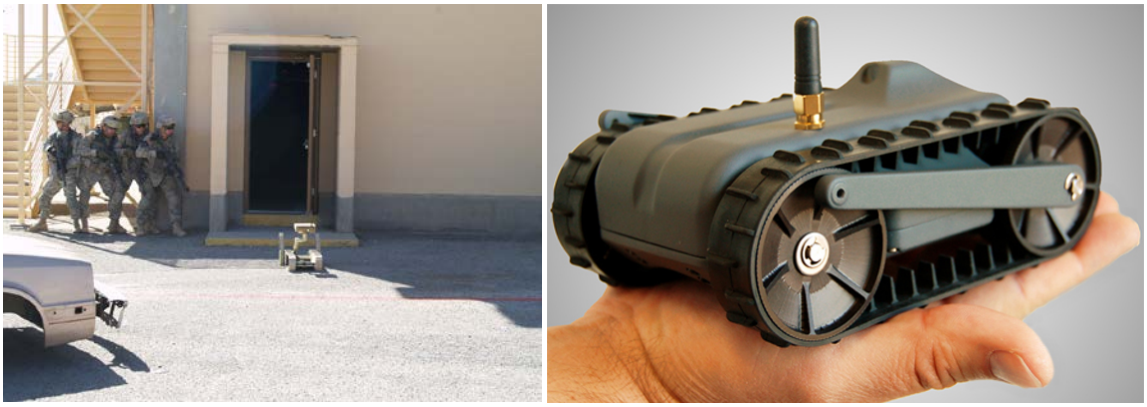

Figure 2.11 Left: SUGV (Packbot) assisting soldiers in operations. Right: LANdroids (photos: iRobot Corporation).

An increased level of automation and better sensors are expected to result in increased efficiency of unmanned platforms. There is also a trend that unmanned systems are regarded as part of the solution to secure communications in military operations. E.g. this is the case for DARPA's LANdroids programme, which is studying the possibility of small inexpensive UGVs to self-configure a robust communications network.

Figure 2.12 BigDog is an example of a UGV under development that can carry equipment and supplies for dismounted soldiers in rough terrain. It is at the foundation of DARPA's recent prototype Legged Squad Support System, LS3 [17] (photo: Boston Dynamics).

Figure 2.13 The Armed Robotic Vehicle-Assault-Light (ARV-A-L) infantry support UGV of the now terminated FCS programme with sensors and effectors to take out personnel and armoured vehicles (source: Wikimedia Commons).

Many of the current UGVs are small vehicles equipped with sensors for observation or equipped with a manipulator arm for EOD purposes. Within the area of manipulator arms there are several projects ongoing to make them easier and better to use. There has also been a trend towards larger UGVs that can work as effectors in a fire support role. The FCS (Future Combat Systems) programme of the US Army consisted of several unmanned and relatively large vehicles. The level of ambition in the US has since been reduced and all the large UGV programmes have now been cancelled. This was mainly due to high costs and the unexpected technological complexity of the autonomous UGVs.

The very complex operational environment makes the UGV less widespread with respect to military use compared to for example UAVs. The Pentagon earlier stated that 1/3 of all US vehicles in the battle field should be unmanned by 2015 [18]. It is likely that such ambitious plans will be postponed or terminated. Even if the development of UGVs has not progressed as expected, one should also keep an eye on non-military developments that can contribute to reduced risk and lower costs. Innovation from the civilian sector can be in many cases directly transferred to military use, especially within logistics and engineering.

Figure 2.14 Left: Three trucks with one lead driver conducting a test in 80 km/h (photo: NEDO). Right: Remotely controlled shovel and dumper at Hjerkinn firing range (photo: Geir Olav Slåen).

3 Developments in Maritime Military Technology

3.1 Maritime Surveillance

3.1.1 Wide Area Surface Surveillance

Cold War type information gathering will remain a necessary requirement for the future building of strategic and tactical pictures of military threats. In addition, events in recent years have caused nations to consider a long list of new threats. These can take very different forms, such as acts of terrorism, drugs trafficking or piracy, and can differ with respect to origin, size, stealth, navigation, command, control, and in their degree of autonomy. How serious these threats are will also vary.

Villains and insurgents may operate in densely populated areas and initiate illegal operations at close proximity to authorities. New threats are often inherently camouflaged by civilian infrastructure and traffic. Additional intentional concealment is easy. Even so, unfriendly operations will frequently reveal discoverable signatures of ‘unfriendly’ behaviour, such as navigation patterns, operational employment or transmitted messages that may be noted as ‘hostile’.

Long range surveillance sensors with increased capability, aimed at threats of predominantly military character, are still being developed and improved. However, new long range sensors are not only radars or other active sensors. Quite the opposite is true, passive sensing of the opponent’s radar is developed for ranges out-competing radar sensor coverage. Similarly, passive sensing of the optical spectra of equipment and people is possible at much longer ranges than active optical systems (lasers) can achieve. Limiting the application to longer range sensing, passive radar systems, passive ESM against radar and optical sensing have had a tremendous technological development over the past few years. Even so, long range passive sensors, at radio or optical frequencies, tend to be rather expensive. The reason is that they need to uphold a very high degree of receiver sensitivity in order to work well at long range.

Other architectures and updated sensor technologies are emerging which will deal with the new types of surveillance targets. The main features of these new systems are that they can provide a high level of detail, and are cheap to produce. They tend, however, to only have short range capability.

The diversity of both traditional and new targets calls for passive sensors suitable for different ranges and different spatial dimensions as well as for different domains, such as information, navigation and the general electromagnetic and acoustic domains. In turn, this variable mix of old and new surveillance targets and sensors call for an entirely new infrastructure for the system side of sensor data handling. The architectural trend is to offer computer services that serve standardized formatted tracks and positions over fast communications networks. Some of these services

may be available only on classified networks, while others will be available on unclassified networks.

3.2 Ship-launched UAS

Surface ships maintain their surface picture based on radars, ESM and EO sensors. These are restricted by the radar/visual horizon and screening by landmasses. These challenges are particularly felt in littoral operations. Traditional solutions include operating with Maritime Patrol Aircraft (MPA), long-range, land-based, Unmanned Aircraft Systems (UAS) or organic helicopters. The availability of these assets may vary and can often be quite limited. For example, helicopters have relatively low endurance and require frequent maintenance.

Many navies have started trials and operations with smaller, ship-based UASes for improved surface domain situational awareness. Long endurance, no risk for own personnel, and cost-effectiveness are the main merits of such solutions. Small size may even allow the operations of several UASes from the same ship.

Two US navy operated UASes are the Northrop Grumman MQ-8 Fire Scout and the Boeing Scan Eagle. Fire scout (Figure 3.1) will be operated from the Littoral Combat Ship. Scan Eagle (Figure 3.2) has recently been used extensively in operations off Somalia combating pirate operations.

Figure 3.1 US Navy's Fire Scout (photo: Wikimedia Commons).

Figure 3.2 US Navy's Scan Eagle (photos: Wikimedia Commons).

3.3 Underwater Surveillance using Off-Board and Networked Sensors

Effective underwater operations depend on detailed and up-to-date information about threats, bottom conditions and oceanography. Rapid insertion of sensor assets for Rapid Environment Assessment (REA) and Intelligence, Surveillance and Reconnaissance (ISR) over longer periods of time in areas of interest is therefore a critical capability to obtain and maintain underwater situation awareness. Many nations are pursuing underwater surveillance solutions using off-board sensors. These may be sensor-equipped, unmanned underwater or surface vehicles or stationary autonomous sensor-nodes deployed on the sea floor, in the water column or on the surface. Their main advantages are to make expensive assets, such as frigates or helicopters, available for other tasks, the possibility of operating covertly, and the ability to share the gathered information between several force elements [19, 20, 21].

AUVs in this role may gather information about the mine threat in an area of interest, oceanographic information (currents and sound speed) and map the seabed in detail (topology and bottom parameters). This type of information will aid the planning and execution of an operation, enable increased speed of operations, and offer the opportunity to exploit the topography to own advantage.

Figure 3.3 illustrates this concept. The AUV may be deployed from any ship. The collected information is distributed to the rest of the force from the mother ship. Fitted with sonars for detection of submarines and surface traffic, an AUV may provide persistent and covert surveillance of prioritized areas. With long range capacity, this may be achieved with high value units at safe stand-off range.

Long endurance and significant payload capacity is necessary to implement such a concept. New fuel cell technology is expected to enable continuous, covert operation in the area of interest for time periods of days to weeks.

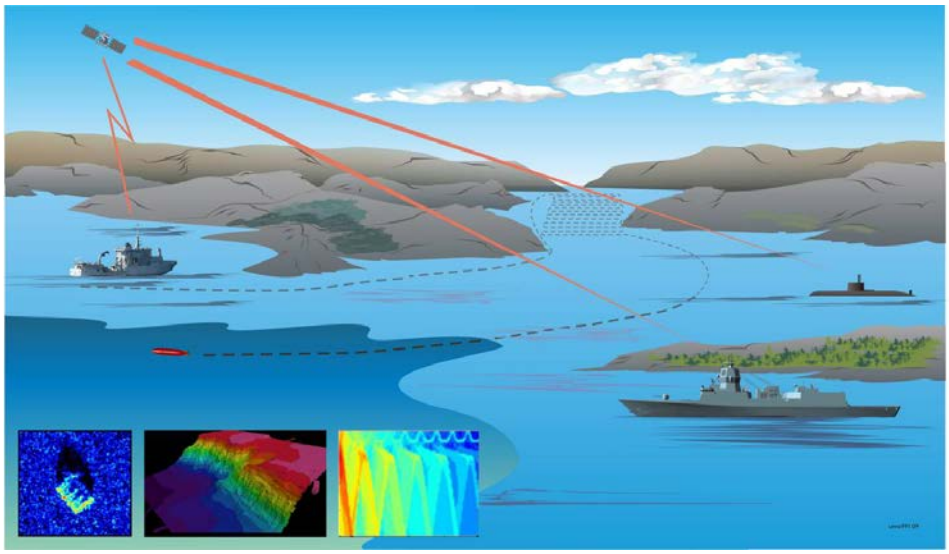

Figure 3.3 Covert information gathering exploiting long-endurance capacity of future AUVs (source: FFI).

Such solutions depend critically on communications, as the mother ship must receive information from the sensors quickly in order to exploit both information and sensors effectively. For subsurface sensors, this will involve acoustic communication. When more than one sensor is deployed, a network designed for non-interference and relaying of messages enhances the effectiveness of the sensors. Fixed sensor nodes may also be used as relay stations between AUVs, submarines and surface vessels.

Underwater communication has proved challenging due to spatial and temporal variability of the environment. Communication protocols must therefore be robust against frequent disruptions [22]. Several underwater communication systems are available commercially today, but we are not aware of operational underwater networks. The underwater network systems developed closest to operational use that we are aware of are the US systems Seaweb [23] and PLUSNet [24]. Seaweb is a general-purpose system able to automatically configure the network and send information from e.g. bottom-mounted sensors, while PLUSNet is a system tailored for sending short command and control messages to and from AUVs. There are also European efforts which in the long term may lead to new operational underwater network systems, e.g., the EDA project RACUN (Robust Acoustic Communications in Underwater Networks) [25].

When deploying several heterogonous systems in the same area, interoperability will also be an issue. As opposed to radio communication systems, standards are very sparse in the underwater communications area. To remedy this situation, NURC has initiated a standardization effort called JANUS [26].

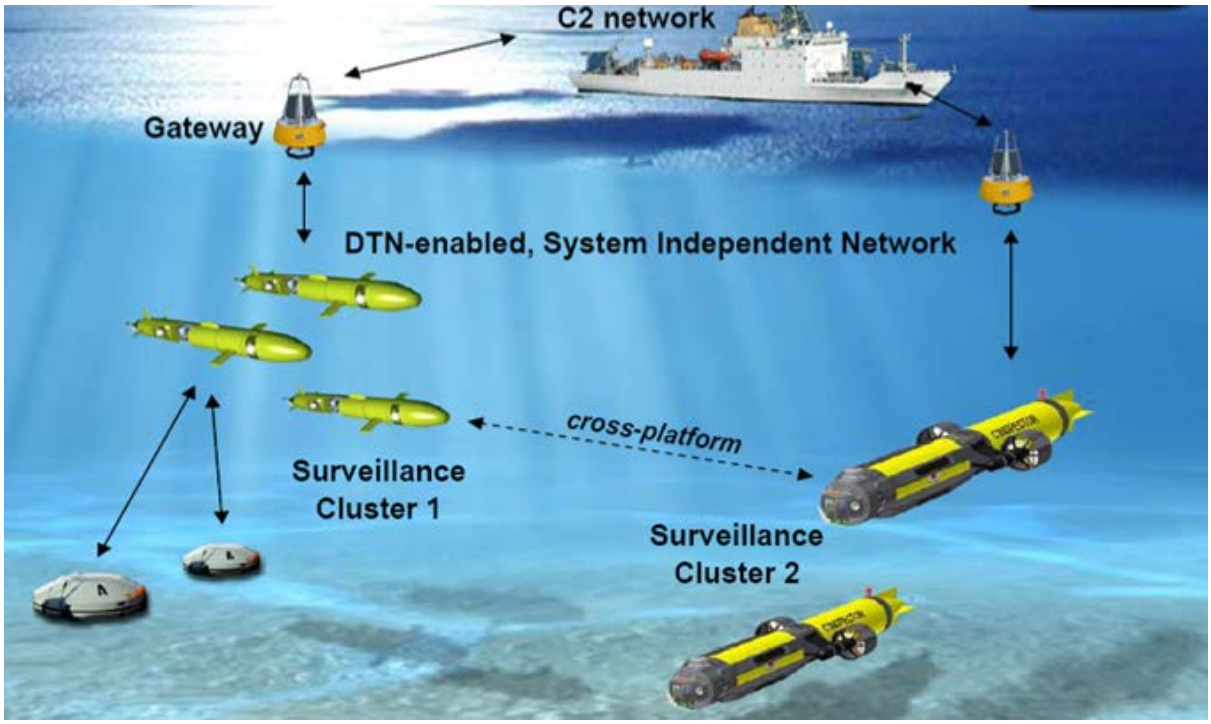

Figure 3.4 NURC concept illustrating a system with both fixed and mobile nodes using disruption tolerant networks (source: see [22]).

3.4 Multistatic Sonar Operations

Anti-Submarine Warfare (ASW) operations are challenging, and increasingly so, due to the quiet nature of current threat submarines operating in the complex acoustic environments in shallow waters [27]. Multistatic sonar systems have been proposed as a way to improve detection capabilities in such areas.

A multistatic system places the source(s) and multiple receivers in different locations. This offers more detection opportunities than a monostatic sonar by providing multiple angle observations, and combining the localization effectiveness of active sonar with the covert properties of passive sonar. The position of the receivers and the main platform may be covert, thus denying the submarine operational latitude to exploit an aspect advantage and reduces the risk for own platforms.

Multistatic sonar is a wireless sensor network. In such networks detection could be centralized or distributed. In the centralized approach, low level data are communicated to a fusion centre, which performs the detection. In the distributed or decentralized approach, each node carries out the detection and communicates contact level data (detections) to the fusion centre. While centralized detection usually gives the best performance (since detection thresholds are globally optimized), the advantage of the decentralized approach is that considerably smaller communication bandwidth is required. Distributed detection also work better when one or more sensors perform poorly.

The main challenges of bi- and multistatic sonar systems are the need for an improved communication network and a suitable acquisition, processing and display system. The operator will also need a planning tool to optimize the sensor configuration before and during the operation.

One possible configuration for a bistatic operation is shown in Figure 3.5 [19]. An AUV may autonomously position itself optimally with respect to the target and the emitter. If it is equipped with towed-antenna sonar, it may detect reflections of the submarine from the emissions of the frigate towed array sonar, the dipping sonar of a helicopter or sonobuoys (dropped from helicopters or maritime patrol aircraft (MPA)). In other scenarios these sonars may act as receivers.

New low frequency (1–2 kHz) sonobuoys are now being developed that are particularly suited for multistatic operation. At these frequencies the propagation loss is reduced and the target strength of submarines is larger than for the traditional 5–10 kHz frequency range of DICASS (Directional Command Activated Sonobuoy System) buoys.

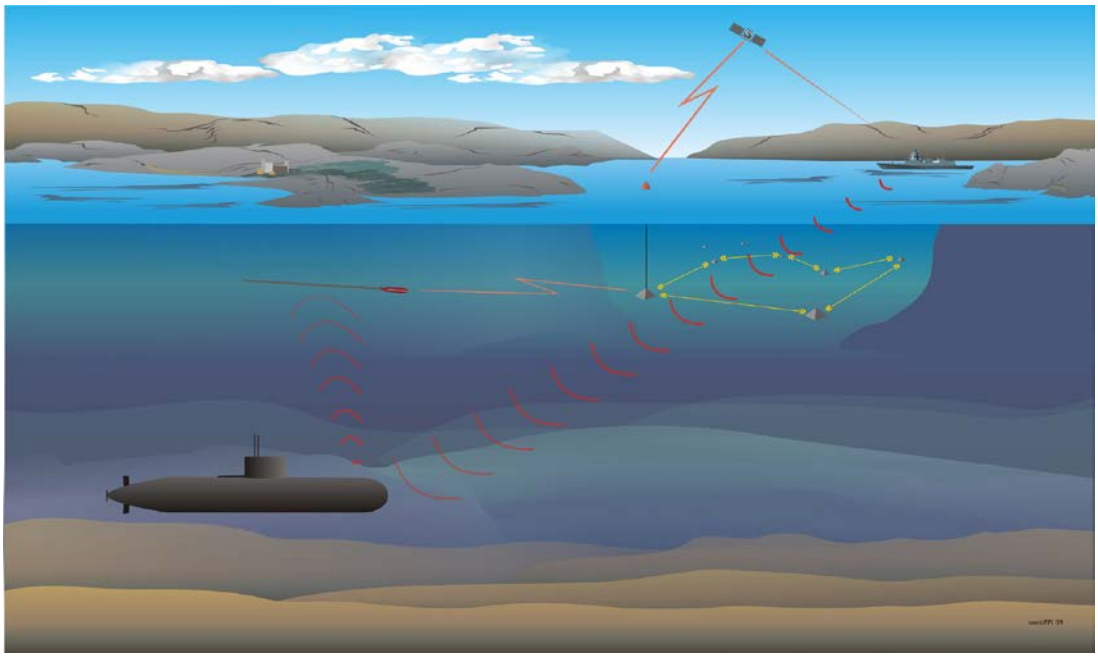

Figure 3.5 Bistatic detection of a submarine (source: see [19]).

The technology needed for realizing the multistatic concept is still immature. It has been under evaluation in NATO in the past several years [20, 28, 29]. Research findings conclude that multistatic active sonar systems have proven to be technically feasible and showed improved performance when compared with monostatic systems [30]. It was also found that improved performance can be exploited automatically.

3.5 Maritime Radars – Active Array Antennas

New maritime multi-function radars are now often using active array antennas. Generally, this is due to the development in analogue and digital semiconductor technology, and decreased hardware cost. This development will continue, the capacity of the components will increase and the cost will decrease. The possibility of including more functionality and enhanced capacity in new radar systems will therefore increase. This type of technology may well be a contender when considering a mid-life update of the SPY-1F frigate radar.

Active array antennas have a number of advantages compared to passive arrays:

- In a passive system the antenna is driven by a single large transmitter amplifier, while in an active system there is a transmit/receive module behind each radiating element. The signal path between the amplifier and the antenna element is therefore significantly shorter, which reduces the signal loss.
- The power amplifier in a passive system is usually made by tube technology distributing power to the antenna elements through waveguides, it could be a travelling wave tube (TWT) or a cross-field amplifier (CFA). In an active system solid state amplifiers are used with reduced amplification requirements, since the antenna power is the sum of the power from each element antenna.

- The tubes need warm up time, meaning that the duty cycle or time the pulse is on in the pulse repetition interval will be shorter than for an active system.
- The tubes are expensive components with generally shorter time between failures than for solid state components.
- For an active array the degradation will be more graceful since the radar will work even if a few of the transmit/receive modules are malfunctioning.
- The signal to noise ratio will, in general, be better in an active than in a passive system since transmit and receive amplifiers are near the antenna element, and therefore give better detection sensitivity.
- The noise reduction and clutter attenuation will also generally be better in an active system since the errors de-correlate with distributed transmit/receive amplifiers.

It will be increasingly common to digitize receive signals near the antenna element and to do the rest of the signal processing digitally, including beam forming. This will increase the dynamic range of the receiver. With digital beam forming it is possible to form multiple simultaneous beams, i.e. a broad beam can be transmitted and the return signal can be processed with simultaneous beams. This means that the same volume can be covered with fewer dwell intervals. This translates to a shorter time needed to cover the surveillance volume, and hence targets will be detected earlier and longer waveform integration times may be used. In this way higher detection sensitivity and better clutter mitigation is attainable.

The trend is further towards massive integration of Radio Frequence (RF) components [31]. The RF transmit and receive parts before the transmit power amplifier / receive low noise amplifier can be integrated into one silicon-germanium (SiGe) chip including digital-to-analogue (DA) and analogue-to-digital (AD) converters. SiGe allows the complementary metal-oxide-semiconductor (CMOS) logic[1] to be integrated with heterojunction bipolar transistors, making it suitable for mixed signal circuits.

With regard to the transmit power amplifier/ receive low noise amplifier part, amplifiers based on Gallium Nitride (GaN) technology are showing very promising results. GaN is a hard, wide band-gap material with high heath capacity and thermal conductivity. It has a high breakdown voltage, high electron mobility and high saturation velocity which make it ideal for high power and high frequency operations. With its properties GaN based power amplifiers can be made extremely effective permitting large bias voltages for high RF power output without breaking down, and also relaxing the requirements for cooling. On the receiver side, GaN based amplifiers are made with a low noise figure. GaN based transmit and receive amplifiers can be put into one monolithic microwave integrated circuit (MMIC).

[1] CMOS is a technology for constructing integrated circuits.

Figure 3.6 Two antenna elements with transceiver module packed in plastic (photos: see [32]).

Digital-to-analogue and analogue-to-digital converters are now available with Gigahertz capacity, making it possible to perform only one stage of analogue up and down-mixing before RF power amplification. These hardware improvements make it possible to implement sophisticated digital signal processing algorithms. Two such possibilities are Space Time Adaptive Processing (STAP) and Generalized Likelihood Ratio Testing (GLRT) [33]. Using STAP the lobe pattern of the array antenna can be adjusted dynamically by weighting in order to minimize the interference from jammers, clutter and own noise. GLRT is an optimal detector making constant false alarm processing with optimum detection probability possible.

An important development is Multiple-Input Multiple-Output (MIMO) processing where independent waveforms can be transmitted on the antenna elements [34]. With a MIMO system the signal vector transmitted can be designed both to approximate a desired beam pattern and also to minimize the cross-correlation between returned target signals. By transmitting orthogonal waveforms on the N antenna elements, a virtual antenna is created with N×N elements compared to 2×N for a conventional antenna. This gives the MIMO antenna superior parameter identification properties. Furthermore the MIMO array offers angular resolution of targets comparable with much larger phase array radar to a fraction of weight and cost. It offers the advantage of allowing long dwell times required for target detection and clutter suppression, while maintaining continuous coverage of the entire volume. Some European companies making MIMO radar are Thales and Selex. MIMO array technology is used both in 4.th generation mobile telephone systems (LTE) and WiMax systems to exceed the Shannon capacity limit for a communication channel.

3.6 Thin Towed Antenna Sonar

Submarines emit low frequency acoustic noise mainly caused by engine and propeller, but also emanating from coolers, fans and other types of machinery. To detect these low frequencies, long antennas with low self-noise are required. Even the most modern flank array sonars do not have sufficiently low self-noise performance and may also be too short due to the hull length restriction. The only realistic option seems to be towed antennas.

So far passive antennas have been relatively thick with diameters larger than 30 mm. This has been based on an assumption that the hydrophones must be well separated from the surrounding water for flow noise to be negligible. It causes the antennas to be heavy and difficult and costly to integrate on existing submarines.

Progress in hydrodynamic modelling has lately indicated that antennas with substantially smaller diameter (under 5 mm) may be essentially noise free. A new EDA project is designed to test this hypothesis. If substantiated, such antennas may provide significantly better detection performance and can easily be retrofitted in legacy submarines.

3.7 Mines and Mine Counter Measures

3.7.1 The Naval Mine Threat

Mines give every navy, no matter what its level of technical expertise, the ability to prevent even modern naval forces from approaching its ports and coastal waters. As a naval weapon, mines offers many advantages over other types of defensive assets, they work in all sea states, are easy to manufacture, are resistant to obsolescence, and when in place represent a long term threat to the enemy [35].

Sea mines can be used at all levels of conflict, particularly defensively in the early stages to exert political pressure. They can be laid by aircraft, submarines and surface vessels, covertly and without advance warning. The low cost and highly effective nature of mines means that economically constrained countries or non-governmental groups may be able to employ a destructive capability out of proportion to its cost. This is illustrated by the repair costs incurred by three mine incidents in Figure 3.7 [36].

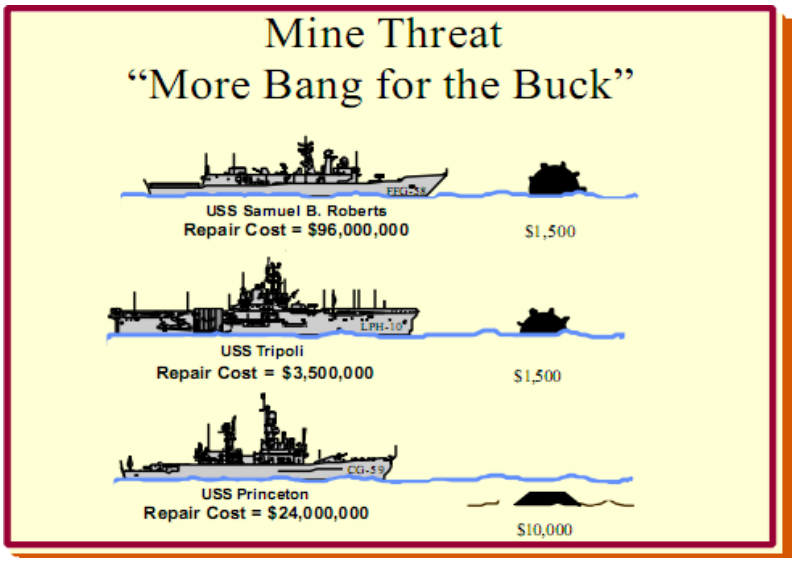

Figure 3.7 Sea mines – a potent asymmetric weapon (source: see [36]).

The comparative simplicity of sea mines combined with their high level of effectiveness has resulted in many countries establishing a development and/or production capability. According to US estimates, the number of countries deploying such weapons has risen from 35 to 50 in the period from 1990 to 2000 (a 40% increase). Of these, 32 produce sea mines and 24 export them (representing a 60% increase in each case) [37]. Advanced sea mines are being exported worldwide for a reasonable price. Historically, since 1950 the losses from sea mines for US warships have been three times larger than the combined losses from missiles, torpedo, aerial attack and small boat attack as shown in Figure 3.8.

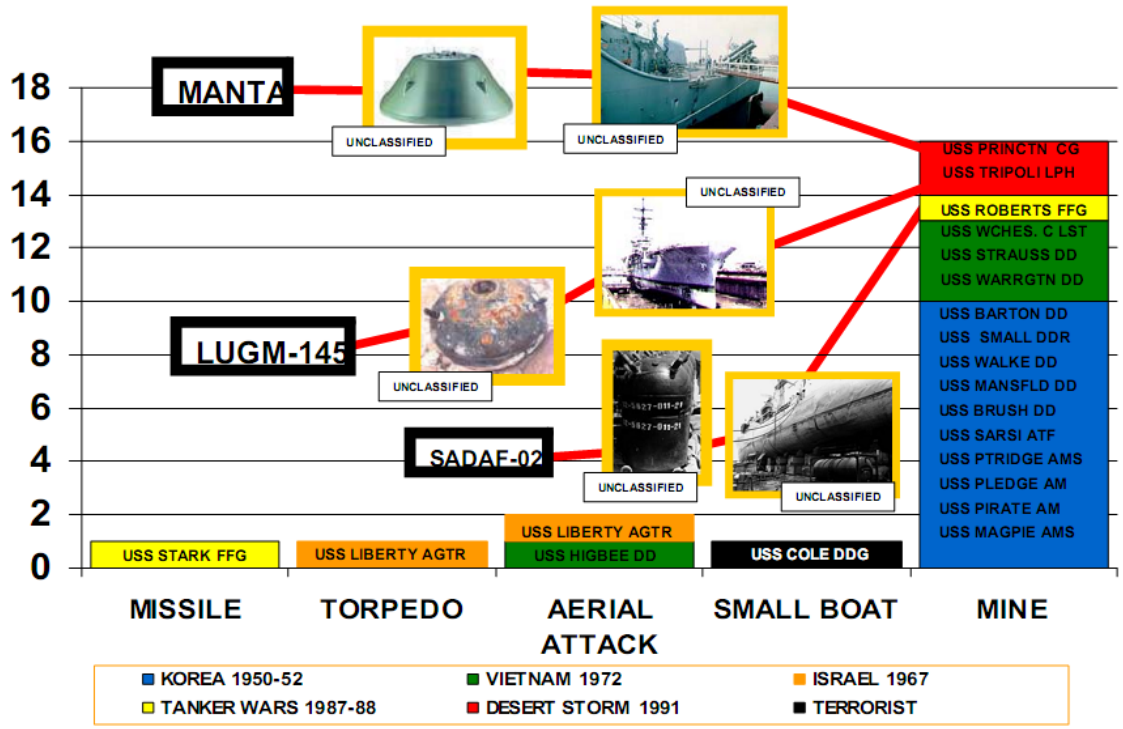

Figure 3.8 US warship casualties by weapon type from 1950 to present (source: see [38]).

Technological developments over the last 20–30 years have resulted in a significant increase in the effectiveness of sea mines. The firing geometry and depth coverage are the most important ones. At the beginning of the 20th century, the contact mine was developed with a firing geometry restricted by the target-vessel size measured in width and draft. During World War II, the stationary-influence mine emerged with a firing geometry given by the explosive charge's damage radius. During the post-war era sea mines with self propelled effectors increased the firing geometry to the sensor-/effector-combination range. All of these mine types exist today. The first two have been used extensively. The last, which represents a huge leap, has so far not been used in any wars, but are available on the market today. Several nations are believed to possess them. When it comes to depth coverage, this has increased to more than 200 metres mooring depth and 500–600 metres effectors depth. This results in greater difficulties for mine clearance operations. The most important consequence of this development is that mine laying efforts will no longer be limited to coastal waters or the continental shelf. Mine laying is now fully conceivable on the open sea.

The technological development will make sea mines more resistant to mine clearing operations. The main developments in the future will be the self-propelled mine and mines which can be buried [39]. Both of these developments will pose great problems for MCM forces.
Stealthy mines will seek to reduce their acoustic and magnetic signatures to an absolute minimum by the use of non-magnetic components and casings, and the use of acoustic absorbent materials. These in turn, will enable the mine's own acoustic and magnetic sensors to become more effective. Mines covered with coatings that promote marine growth will also make them difficult to find and classify in mine hunting operations.

Other likely developments include increasing the mine's effectiveness against specific targets, in particular mine hunters, submarines and helicopters, and seeking to capitalize on influences so far not developed. For example, the availability of mines which respond to the mine hunter and its equipment such as the sonar can be foreseen. However, the most effective protection of mine-fields will still be in tactical cooperation with other types of weapons. In this context also simple tactical mechanisms, such as ship counters and arming delay, still have a major effect. The purpose of the ship counter is twofold. One is to achieve a more even distribution of the minefield threat over a larger number of transit attempts. The second is to impede influence minesweeping by forcing the opposing forces to increased clearing effort [40].

Mine employment will be more difficult to detect in the future because covert mine laying will be easier. Smaller sensors combined with increased firing geometry (range) will require fewer mines, which in turn will make them easier to hide, for instance in the surf zone. Smaller mines ease delivery and enhance stealth. This also gives units with restricted load capacity an increased sea mining potential. Mine laying can be carried out covertly in connection with other legitimate operations.

Surface combat units follow an unbroken trend: They are becoming more costly and sophisti-cated, and as a result, fewer. With declining redundancy there is also a reduced acceptance of risk. Each loss of a surface unit will have greater impact, making mining effort, with its potential to hurt an enemy with low risk for exposure, more attractive than ever before. For sea mines the redundancy is still considered high because the technological developments for many kinds of mines mean that they have more advanced electronics in the sensor instrument section. The rest of the system remains unchanged.

For more advanced mines with moving effectors the cost increase will be more than compensated for by improved performance [40]. In an area-minefield[2], a mine with moving effectors and extended firing geometry could replace anywhere from 10 to 100 stationary mines, or even higher. In a closure-minefield[3] the requirement on resilience yield a much lower replacement ratio, estimated in the range from 3 to 10. This means that the mine, as opposed to other weapon

[2] Area minefield is a minefield with *low mine density* which aims at preventing shipping from moving *in* an area.
[3] Barrier minefield is a minefield with *high mine density* which aims at preventing shipping from moving *through* an area.

systems, can maintain or even increase their redundancy. The sea mine is today the only sea-war measure that allows the combination of high technology and mass action. In the relationship between mining efforts and mine countermeasures, lots of low-tech mining efforts can defeat high-tech low-redundancy combat units.

3.7.2 Mine Counter Measures

Maritime Mine Counter Measures (MCM) operations are experiencing conceptual changes due to new developments in autonomous systems and their commercialization. Next generation MCM-systems will use Autonomous Underwater Vehicles (AUV) and Unmanned Surface Vehicles (USV) and this will entail the same kind of development as seen in ISTAR (Intelligence, Surveillance, Target Acquisition, Reconnaissance) based on unmanned air vehicles.

In maritime MCM, special-purpose vessels have traditionally been used for mine hunting and mine sweeping, respectively. Mine hunters locate mines on the sea floor or in the water column in order to destroy them, while mine sweepers try to fool the mines into detonating by imitating the electromagnetic and acoustic signature of a vessel the mine has been primed for (influence sweep). The MCM-vessels thus have to operate in the mine field which poses a great risk to the vessel and its crew. Much of the cost of such vessels goes into reducing this risk to acceptable levels. This is achieved by reducing the signature of the ship and making them resistant to underwater explosions. They also need sophisticated sonars and signature generators to solve their tasks. These factors contribute to cost escalation and expensive vessels.

Developments in AUVs and USVs have given impetus to new MCM concepts which reduce the risk and increase effectiveness and operational capability. The core of the new concepts is to make use of these unmanned assets to conduct mine clearance operations from a manned mother ship at a secure distance from the mine threat. The systems are based on mobile containers configured for specific operations. This way one can make use of conventional vessels and avoid costly risk reducing measures.

Mine hunting modules will consist of a number of AUVs that are dispatched into an operational area and carry out a methodical search of the area. They detect and classify mine-like objects by means of synthetic aperture sonar (SAS) and identify the contacts using an optical camera before returning to the support vessel. This provides a detailed map of the mine threat in addition to environmental information of the area. Based on this information a USV guides a number of expendable disposal weapons (EDWs) towards the mines by remote control. Communication between support ship and USV is by radio link and by fibre between USV and EDW. The mine is then set off by a directed charge after positive identification and the USV then continues to its next target until the area is rendered safe for transit.

Mine sweeping modules will consist of USVs towing influence sweep equipment remotely controlled from the support ship by radio. The sweep comprises signal generators that emulate electromagnetic signatures and low frequency sound generators imitating propeller and motor

noise of ships to be protected. Normally, sweeping is used when mine hunting is ineffective due to difficult bottom conditions or when mines are buried.

3.8 Missile Defence

3.8.1 Hard-kill Missile Defence

As the technology of anti-ship missiles continues to develop, and the number of nations with anti-ship missile capability increases, more capable surface-launched air defence missiles are needed. One trend is that defence missiles in the future will have active seekers, or dual mode seekers with both an active and a semi-active seeker component. An active seeker component will allow the missile to engage targets beyond the firing ship's illumination radar horizon, as is the case for semi-active missiles. Examples of defence missiles with an active and a semi-active seeker component are SM-6 and the planned development of ESSM Block II.

Future defence missiles will also have extended range and better manoeuvrability. The SM-6 missile is an example of a newly developed missile with extended range, and thus the ability to expand the boundaries of the battle space. Future defence missiles may also increase their capability due to better signal processing, which will reduce the influence of multi-path effects and clutter. Development in fuse technology is expected to provide more reliable solutions, increasing the possibility of successful hit.

As mentioned in the above section on anti-ship missiles, China has developed an anti-ship ballistic missile which can be used against moving targets [41]. This missile has the capability to manoeuvre both during midcourse phase and during terminal phase. Current missile defence solutions are not capable of encountering ballistic missiles, but it is expected that future development will include this capacity.

3.8.2 Soft-kill Missile Defence

The missile threat faced by naval ships today and in the near future is complex and strongly dependent on the mission. Thus a wide range of threats from old legacy to new seekers with advanced electronic counter-countermeasures (ECCM) are possible. Land-based irregular threats with laser-guided weapons can also be relevant in some situations.

The emphasis on hard-kill (HK) in Anti Shipping Missile Defense (ASMD) for larger naval vessels seems to continue. On US destroyers for instance, HK might comprise long range (SM), medium range (ESSM) and short range (RAM) missiles and close in gun systems (Phalanx). Nevertheless, such vessels also have comprehensive soft-kill (SK) assets (chaff/IR decoys, jammers and/or active RF decoys). SK is to some extent considered as backup if HK systems fail or in situations with multiple threats and probability of one or more 'leakers'. One possible future scenario is the employment of modern effective Digital Radio Frequency Memory (DRFM) jammers operated from an UAV or from shore. The jammers could mask real targets or introduce multiple false targets sufficiently credible to trigger HK engagements. Also, HK reactions can be restricted due to strict ROEs.

Smaller vessels, like the Skjold class, have only very limited ASMD HK defence capability (Mistral and 76 mm guns). Thus the ability to escape a hit depends to a much larger degree on the SK performance. The vessels low signature and ability to operate close to shore also contributes in the ASMD.

Certain scenarios, as close littoral operations, lead to very short reaction times which challenge both the HK and the SK defence. Automatic reaction rules are necessary with only a very small timeframe available for veto (a few seconds). Relevant sensor systems are also essential, e.g. laser warning receivers. Sufficient trust and adoption of such automatic modes in the combat system by responsible warfare officers are difficult.

Large military powers, e.g. US and UK, develop own missile seekers and SK countermeasures and thus possess both theoretical and experimental knowledge which make it possible to assess SK effectiveness and develop adequate reaction algorithms. It is important to realize that SK systems usually are delivered without reaction rules or only generic reaction rules. A certain level of national programming is therefore typically required.

Cooperation between nations in the SK field is limited due to high levels of national secrecy. Still, smaller nations are dependent on such cooperation and utilization of experimental assets. Thus groups like NATO MCG-8 are considered extremely important today and will be so even more in the future. For smaller nations it is a challenge to be sufficiently up-to-date concerning threats and seeker details necessary to program the SK systems effectively.

Although advanced integration of HK and SK has been investigated for the last two decades, very few operational systems with such functionality exist. Instead coordination is accomplished by the combat system operators. This seems to be the state of art in most navies today. Manual coordination may be robust but is obviously suboptimal. For vessels and navies with less HK assets a well designed automatic coordination function in the combat system might increase the ability to survive a missile attack significantly. The Canadian Navy has introduced an advanced decision aid for SK (chaff and jamming) that also calculates and presents the recommended ESSM firing solution according to the weapon control algorithm in the combat system [42]. Thus this tool facilitates manual coordination of SK and HK. In the future, this tool might be a part of the combat management system, and would make more automatic reactions possible.

Chaff is the oldest and most widespread countermeasure against RF missiles (which heavily dominate in actual threats) and is found on all naval ships. The efficacy of chaff in ASMD is controversial because modern seekers with advanced ECCM are able to discriminate between the ship’s RF signature and the chaff cloud. Existing and future development of imaging seekers and dual mode (RF and imaging) will further reduce the usefulness of chaff. Still, many contend that appropriately launched chaff decoys might seduce certain types of existing seekers. Likewise, IR flares might seduce simple IR seekers. Such tests are done regularly by MCG-8.

Modern chaff/IR flare systems, like the Mass system on the Skjold class, have trainable launchers and use a sequence of multiple decoys coordinated in position and time in order to maximize the effect of the countermeasure. The stealth and manoeuvrability of such vessels also contribute to the effectiveness of these countermeasures. Still, in order to utilize this potential, detailed knowledge of threat seekers and experimentation is imperative.

A relatively new addition to such systems is decoys containing expandable corner reflectors, which contributes somewhat to a more ship-like RF signature. A more capable SK defence would include both an onboard jammer and off-board active decoys. Such decoys are expensive, and the content of the payload will probably be subject to export restrictions and require national threat programming. An active decoy like the NULKA hovering rocket system, has short reaction time, full control with direction of seduction, independence of wind and cannot be discriminated based on speed and altitude. The radar repeater in the decoy also simulates a ship-like signature which cannot easily be discriminated.

3.9 Torpedoes and Torpedo Defence

3.9.1 The Torpedo Threat

The global threat to naval forces from torpedoes could be expected to increase over the next two decades. Despite the financial situation in several countries, the need to replace obsolescent weapons will contribute to further developments in torpedo design. Due to the increasing competition in the international arms market and the need to share costs, it is not unlikely that high-quality, advanced torpedoes will be exported to many countries which currently employs torpedoes that are technically inferior to those in the inventories of Western countries.

Today, there are more than 100 variants of torpedoes and approximately 60 countries that have torpedo inventories. Russia, France, Germany, China, Italy, Sweden, United Kingdom, and the United States are the primary producers and exporters of torpedoes [43].

The overall shift in emphasis toward coastal and littoral warfare has caused a significant change in the requirements for torpedo design. This is especially noticeable in the latest generation of light weight torpedoes. During the cold war, fast deep-diving submarines were the primary targets. Today quiet diesel-electric submarines are perceived as the main adversary for Western ASW-forces. For the next 10 to15 years, torpedoes will incorporate more advanced homing systems and quieter propulsion systems to make them better suited for operations in the acoustically challenging shallow water environment. It is likely that each country’s torpedo inventory will become smaller in the future.

Due to more advanced shore-based training facilities it is also likely that there will be an increased focus on quality rather than quantity with regards to sea trials. This means that the propulsion system will need to be adapted to the requirements of cost-effective logistics for small stocks and fewer in-water runs. Thermal propulsion systems used to be more cost effective if a country had large stocks of torpedoes and performed many in-water runs per year. Today,

however, operating the facilities needed to handle fuels used in thermal propulsion systems as well as the organization to carry out maintenance on the propulsion system itself. This might cause too much overhead cost compared to the level of activity and the number of torpedoes. To reduce overall cost a higher cost per in-water run will be acceptable since the activity will be relatively low. These factors might also lead to many of the old torpedo designs being phased out in favour of new more advanced torpedoes better suited for today's logistical and operational requirement. This indicates that the typical threat torpedo in the future will be a silent electric torpedo that is more difficult to detect.

It is expected that wake-homing torpedoes will remain the primary torpedo against surface ships throughout the next 20 years. They are simple to employ, which allows countries to maintain a substantial surface-ship attack capability with relatively limited in-water trials programme. Stand-alone, wake-homing systems are expected to evolve into even more capable systems by integration with acoustic homing systems. This is especially true when it comes to updated versions of old designs from the Soviet Union.

The most common wake-homing torpedo is the American 53-65 torpedo. The 53-65 is a heavy gas-turbine propulsion, wake-homing anti-ship torpedo originally developed in 1965. The late 1960s witnessed the introduction of an oxygen version 53-65K which was extensively employed by the Soviet Navy. The 53-65KE is the improved export variant which has been exported to many countries. The PLA Navy ordered some unknown number of the 53-65KE and TEST-71 torpedoes in the late 1990s to arm its four Kilo class diesel-electric submarines [43]. The 53-65KE is reliable and easy to operate, requiring no maintenance even when stored in torpedo tubes, on carrier racks, or in arsenals for a long time. Although this is a simple design compared to Western torpedoes there are no commercially available soft-kill torpedo countermeasures that are capable of interrupting the torpedo's homing on the target.

3.9.2 Soft-kill Torpedo Countermeasures

Soft-kill torpedo countermeasures have been available since the introduction of the homing torpedo. The most common way to implement this has been to tow an acoustic projector behind the vessel. The most widely used towed torpedo countermeasure is the American AN/ SLQ-25A Nixie countermeasure. This type of countermeasure can be active as long as needed, and it is fitted to vessels which do not have torpedo detection capabilities as well as ASW platforms. It could be argued that having a towed decoy continuously turned on could help the torpedo getting in the vicinity of the target since the towed decoy presents a strong target to the torpedo. On the other hand it is difficult for a homing torpedo to hit a target it does not detect because the noise is masked by a countermeasure.

An increasing number of ASW platforms that possess torpedo detection capabilities are employing expendable torpedo countermeasures. These can be either mobile or stationary. Mobile countermeasures are primarily used as decoys which mimic the target signature both actively and passively. Towed antennas are used to simulate a true spatial extent. Stationary countermeasures can be used as decoys, but because of the limitations with regards to simulating spatial extent and

movement they are often used as jammers. The purpose of a jammer is to mask the target signature and preventing detection rather than mimicking it.

In the future, we might see dedicated torpedo detection systems. Systems of a modular design could be integrated with combat systems and ship borne sensors or operated as standalone systems onboard non-ASW platforms. It is also likely that soft-kill and hard-kill systems will be designed to augment each other in order to form a layered anti-torpedo defence system.

3.9.3 Hard-kill Torpedo Countermeasures

Since it appears that countering wake-homing torpedoes using acoustics cannot be done effectively, several nations have put effort into so-called hard-kill systems. Germany is one of these countries, and they have been developing the TAUW system that uses the Seaspider (Mini Torpedo Welcome – MTW) as the effector. This is a small torpedo which is highly manoeuvrable and very fast developed specifically as an Anti-Torpedo Torpedo (ATT) [44]. The American WSQ-11 performed successful trials in 2006. This system also aims to utilize an ATT, the so-called Common Very Lightweight Torpedo (CVLWT), as the effector in the system. Both systems are designed to be integrated with ship sonars. WSQ-11 also uses an upgraded version of the AN/ SLQ-25A Nixie soft-kill system that is capable of augmenting the ships own underwater sensors [45].

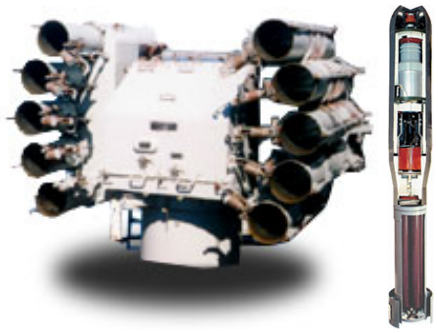

Figure 3.9 KT-153M Rocket Launcher and 111SO2 Diverting Rocket Projectile (photos: splav.org).

The Russian UDAV-1M “Ships Anti-Torpedo Defence Multiple Rocket Launcher System” is a hard-kill system that has been operational since the beginning of the 1990’s. The UDAV-1M system is primarily designed to use different types of rockets for multi-layer defence of surface ships against torpedoes. The system is also capable of engaging submarines and divers. Three different types of rockets are launched from a remotely controlled ten-barrel launcher known as the KT-153M (see Figure 3.9). The first defence-layer consists of multiple 111 SO decoy rockets to divert homing torpedoes from the surface ship by creating false acoustic targets and mask the launching vessel’s own signature. The middle layer consists of several 111 SG depth-charge rockets with HE warhead and impact-time fuse to engage underwater targets. The inner defence layer consists of multiple 111 SZ mine-laying rockets with hydro acoustic proximity fuse for remote mining of a water area to make a barrier for incoming torpedoes. All the layers are tethered from buoys and the inner defence layer has resemblance to the Spanish mine barrier

system. UDAV-1M can be used at ranges from 100 meters and up to 3000m and the submarine engagement depth is reported to be 600m. Reaction time is 15 seconds, and the estimated probability of neutralizing an incoming homing torpedo is 76 % [46].
UDAV-1M is employed on a number of Russian vessels. Several other countries have launchers of Russian manufacture capable of firing similar rockets. These are mainly anti-submarine systems, and it is uncertain whether the complete UDAV-1M system has been procured by any navy other than the Russian navy.

3.10 Force Protection against Irregular Threats

3.10.1 Irregular Threats

In naval security operations possible adversaries may include insurgents, militias, criminals, terrorists and pirates [47]. Such non-state actors may use fast, small boats in combination with hand weapons, hand grenades, RPGs, small calibre guns and explosives. These threats are characterized by being:

- Suitable for asymmetrical warfare.
- Applicable without extensive training.
- Available in the grey market.

3.10.2 Less-than-lethal Countermeasures

When faced with irregular threats, it is not always necessary or desirable to kill the opponent. Naval forces have therefore been seeking less-than-lethal weapons with the purpose of incapacitating an opponent for a certain period of time. These are defined as : “Weapons which are explicitly designed and developed to incapacitate or repel personnel with a low probability of fatality or permanent injury, or to disable equipment, with minimal undesired damage or impact on the environment” [48]. They may, for instance, be useful in order to:

- Warn vessels approaching own ship.
- Render personnel on deck harmless.
- Repel unwanted boarding.
- Enable boarding of threat vessels.

It is not obvious that such countermeasures will be practicable and effective in all situations. Their effect will typically depend on mode of operation, the intended target and even chance events. Some examples are:

- Long Range Acoustic Device (LRAD): Powerful loudspeaker producing disagreeable high sound levels at ranges up to 300 meters.
- Running gear entanglement: A rope that interferes with the propeller of vessel.
- Taser gun: Uses a high-voltage discharge to disrupt voluntary control of muscles.

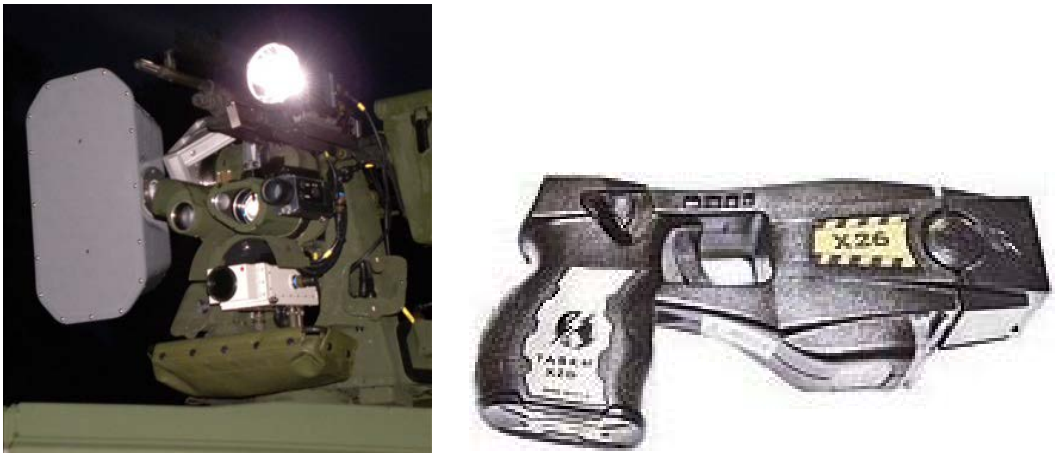

Figure 3.10 Left: LRAD on CROWS (photo: LRAD Corporation). Right: Taser gun (photo: Wikimedia Commons).

3.10.3 Passive/Active Protection

Passive protection is an alternative term for traditional armour. Add-on armour may be a cost-effective and flexible way of enhancing survivability against irregular threats. They may be categorized according to construction material: metal, fibre-composites and ceramics.

Active protection is a general term covering both hard-kill and soft-kill systems, but is mostly applied to short-range, short-reaction-time systems for protection of armoured vehicles against anti-tank missiles. Detection can be based on flat-panel radars, as in the Israeli-developed Trophy system, and intercept is typically achieved by a burst of fragments aimed in the direction of the incoming threat.

In a maritime setting active protection may give a significant reduction in the effect of a missile/rocket hit. Two ways of curbing the complexity of such a system would be to only cover critical parts of the vessel or increasing the range of defeating the threat. Two restricting factors are given by the need to avoid interference with other sensors and weapons as well as avoiding collateral damage. These restrictions are probably more severe for ground vehicles than for surface ships.

3.11 Open Architectures in Combat Systems

A dominating trend within combat systems is towards application of standardized technology and open architecture. This fact will lead to simpler and more affordable integration, more affordable components and subsystems, as well as increased flexibility facilitating increased competition among the contractors. Additionally, flexibility also leads to possible improvements related to reducing life cycle costs by simplifying modifications, updates and upgrades (adding and/or removing functionalities) both in the short and long term. Due to the increased flexibility, costs related to modifications and expansions are likely to be reduced.

Systems architecture for Combat Systems was introduced around 1960. Before this, sensors and weapons where independent components delivered by different contractors, and there were little interaction between the systems. Understanding of the need for design with a view to cooperation between systems formed the systems architecture.

Most existing Combat Systems consist of a large and increasing share of civilian information technologies. This includes sensors, processing systems, operator interaction, and communication with other platforms. The Combat System's main task is to process information in such a way that situation assessment and weapon engagement is handled as well as possible. Many civilian IT trends are very relevant also for next generation Combat Systems. The characteristics of civilian IT systems can be adapted to use in defence products if the latter follow the ground rules of the civilian market.

A Combat System should be flexible in order to replace, add or change components in such a way that the Combat System can be easily adapted to changes in operational requirements. Open architecture is regarded as the best way to achieve the desired flexibility during the life time of the Combat System. A premise for achieving this is the establishment of an infrastructure where components are easily connectable (plug and play). The infrastructure will typically consist of the open lower layers in the architecture that all potential contractors support as a standard.

An example of the development of open standard solutions is the sonar update on US submarines that started in 1997. These sonar systems were obsolete, had poor performance, and were very expensive to improve or upgrade. Lockheed Martin developed a new concept for sonar systems called A-RCI (Acoustic Rapid COTS Insertion) for the US Navy submarines. A-RCI is based on civilian technologies for hardware and software. Lockheed Martin is now developing similar solutions for the total combat system on the submarines.

In the UK, Dstl and QinetiQ have developed a similar system called Delivering Rapid Sonar COTS Insertion (DeRSCI). DeRSCI is based on a Generic Open Architecture (GOA) that connects application components. GOA is especially adapted to integrate third party software components.

Kongsberg Defence & Aerospace has integrated the DeRSCI architecture in their newly developed Passive Sonar System (PSS) for the Ula-class submarine. After finishing the on-going update programme, the Ula-class will have a COTS-based Combat System Information Infrastructure (CSI2) that includes common services and applications for the total combat system. The passive and active sonars, navigation system, communications system, periscope, ESM, radar, and Combat Management System (CMS) will be integrated with the CSI2.

The AEGIS air-defence system deployed on US Navy cruisers and destroyers (and on Norwegian frigates) was initially designed as an integrated and tightly coupled hardware and software CS. The US Navy has now started transitioning this system to an open architecture design. The goal is to achieve improved performance and affordability through use of modular designs, public access

to design specifications, reusing software code, mandating common interface standards, and achieving interoperability between system hardware and software applications [49].

The main characteristics of the approach are:

- Based on open, publicly available specifications – preferably maintained as standards by a consensus process (e.g. by an internationally recognized governing group)
- Well-defined, widely used, non-proprietary (standard) interfaces, services and formats
- Durable (stable or slowly evolving) component interfaces that facilitate component replacement and addition of new capabilities
- Upgradeable through incorporation of additional or more capable components with minimal impact on the system

3.12 Maritime Fuel Cells and Batteries

3.12.1 Submarines – Air Independent Propulsion (AIP)

Two systems are in use today: The German hydrogen oxygen fuel cell (FC) used in U212 and 214 and the Swedish Stirling (diesel fuel / oxygen) used in the Gotland class. Closed cycle diesel has been evaluated, but the associated noise makes it less useful. Both systems use cryogen (liquid oxygen) and this is expected to be used in all future AIP systems. The German FC system is developed by Siemens and based on acid polymer electrolyte membrane (PEM) using super pure hydrogen stored as metal hydride. The advantage is very high efficiency, low noise and no product gas that must be ejected as only water is produced. The disadvantage is cost of the fuel and the expense in building an organization for supply of pure hydrogen and liquid oxygen.

In contrast, Stirling uses low cost diesel but needs to compress, dissolve in seawater and eject the carbon dioxide produced. Oxygen consumption rate per kW is also significantly higher than for the Siemens fuel cells. On the other hand, a lower purity oxygen grade may be used.

Other navies are considering the reformation of methanol to hydrogen (India) and diesel to hydrogen. This lightens the logistic burden, but implies a complex on-board reformer. As with Stirling, carbon dioxide must be dissolved in seawater and expelled.

3.12.2 Submarines – Batteries

Lead acid has been in use for more than 100 years in submarines. New lithium ion batteries increase the energy density by a factor of at least two, but have safety and cost implications. Safety can be improved by location in new submarines, but for refit, an increased trust in the technology is needed. Work is in progress and e.g. BWB and HDW supports this development in Germany. The recent complete loss of a US Navy Advanced SEAL Delivery Vehicle (a small 60 ton submarine) in October 2008 caused by a lithium ion battery fire, has not been helpful.

There are a large number of different chemistries in use in lithium ion batteries. They differ in specific power, specific energy, calendar- and cycle life and abuse tolerance (safety). They all use

organic electrolytes, however, and the main concern regarding the introduction of LiIon batteries is their use of a flammable electrolyte. This, combined with their ability to store large amounts of energy in a small volume, makes them potentially hazardous.

Given the size of batteries for maritime use, the level of safety for lithium ion must be way above what is considered acceptable for water based chemistries such as lead acid.

At present, the automobile industry is pushing the lithium ion technology in order to achieve acceptable range capability for electric vehicles at an acceptable cost and without compromising safety. This development may have great potential for naval use and will be worthwhile watching.

3.12.3 Torpedoes

Today, reserve batteries based on silver oxide zinc or silver oxide aluminium are used in torpedoes. Lithium ion batteries can match silver zinc batteries on all aspects of performance, and for exercise torpedoes their much greater shelf-life and similar or even reduced cost compared to rechargeable silver/zinc will probably result in their rapid introduction. Again, safety is crucial, but can be brought to acceptable levels, at least for exercise torpedoes.

3.12.4 The “All-electric Ship”

The “all-electric ship” is an increasingly popular concept as the use of pods for propulsion gives:

- Excellent manoeuvrability
- Freedom of location of heavy machines, no shafts between propeller and primary propulsion source (e.g. diesel generator)
- Reduced noise
- Improved survivability (multiple pods and generators)

Recently developed high power batteries (e.g. lithium titanate/iron phosphate) make rail guns an interesting option as armament for ships.

3.13 Littoral/Modular Ship Design

Currently there are several ongoing projects at different stages which all strive for cost-effective, littoral combat ship capacity. Navies typically plan to retain larger vessels (frigates, destroyers), but the low number of such vessels leaves a significant capacity gap in the littorals. Some similarities between the projects are evident: They typically have low signature and high speed. They have strong communication capabilities, and several have modular mission systems as a cornerstone of the design. That is, a basis hull can be equipped with mission specific add-on modules, which helps keeping the ships relatively small.

3.13.1 USA

The US Navy has been working on their Littoral Combat Ship (LCS) since 2001 [50, 51]. The idea is to get a relatively small and inexpensive surface combatant ship covering the near coast operations. While larger vessels typically have a multi-mission capability – the LCS will be a focused-mission vessel, i.e. they will be equipped for one type of operation at a time. Without any

mission package, the basic LCS version is referred to as the LCS sea frame. The plan is to achieve 55 LCS sea frames and 64 mission packages (16 ASW, 24 MCM, and 24 ASuW). Some important characteristics of the vessels are high speed and low draft. This means that the vessels can visit ports and waters not accessible to the larger ships.

The ship specifications include a helicopter deck and hangar, and will have the ability to launch and recover unmanned platforms. This includes both unmanned aerial vehicles (UAV) and unmanned surface vehicles (USV). Some characteristics:

- Displacement: approx. 3000 tons
- Max speed: 40+ knots
- Crew size: Core crew 40 + mission specific up to 35

The basic missions for the LCS are ASW, ASuW against small boats and MCM. But they also include peacetime engagement and partnership-building operations, intelligence, surveillance, and reconnaissance (ISR) operations, maritime intercept operations, operations to support special operations forces, and homeland defence operations. It must be able to solve these missions at any time, regardless of its installed mission module.

Figure 3.11 Left: Lockheed Martin-designed LCS. Right: General Dynamics-designed LCS (photos: NAVY.mil).

Two US companies, Lockheed Martin and General Dynamics, are in parallel prototyping their own LCS. Both are capturing the specifications, but despite that, quite different implementations. Currently, the two companies are asked to build a total of twenty vessels (10 from Lockheed Martin and 10 from General Dynamics), and the procurement period for the vessels last until 2015.

3.13.2 Sweden

In 1996, the construction of a new Visby class corvette started, and in 2000 the first vessel of the class was launched [52]. This is a stealth-design ship, with respect to radar cross section, IR-, optical- and under-water signature (hydro-acoustic and magnetic). The weapon systems are all

integrated below the surfaces, which is the key to keeping the radar cross section (RCS) low. The hull material comprises a sandwich construction were both PVC and carbon fibre are applied. This is crucial in meeting the design criteria of high speed and low signature. The class has of a total number of five vessels.

Some characteristics:

- Displacement: approx. 640 tons
- Max speed: 35 knots
- Crew size: 43

The platform is a multi-mission unit, having capabilities within MCM (including a ROV), ASW, ASuW and AAW. The ship is a quite capable platform in many of the surface combatant ship domains. The ship is equipped with a helicopter deck.

3.13.3 Norway

The Skjold-class represents an alternative approach to littoral combat vessels. High speed, low signature and low weight are key features of the platform. The vessel does have capabilities within both ASuW and AAW.

To enable the low weight of the vessel, a composite construction material based on glass fibre and carbon laminate is applied. From this the hull is manufactured, based on an air cushion in the centre of a catamaran hull. This concept gives a small wetted area on the hull, which again enables high speed performance and good stability.

Some characteristics:

- Displacement: approx 270 tons
- Max speed: 60 knots
- Crew size: 20

3.13.4 Australia

The Offshore Combatant Vessel (OCV) is currently a conceptual work in the Royal Australian Navy [53]. The missions to be captured are MCM, patrol boat, and hydrographical and oceanographical surveying. Despite that the class is named combatant vessel, the combatant capacity will be minor and basically defensive.

Like the US LCS, the idea is to have a basis hull and special mission add-on modules. Key issues for the OCV are flexibility and mobility, where the mission modules constitute the flexibility and the mobility includes an expeditionary force ambition.

The planned number of vessels is around twenty, and will replace 26 vessels distributed over a total of four classes. Due to the early stage of the OCV project, technical characteristics are not available. The displacement is nonetheless specified to be above 2000 tons.

4 Air platforms and air delivered weapons

4.1 Combat Aircraft

Fighter aircraft have traditionally had roles within defensive counter air missions. Today's modern multi role combat aircraft are expected to fulfil several other requirements like offensive counter air missions, close air support and other anti-surface missions. This trend is expected to continue, and fighter aircraft will increasingly be required to contribute to roles such as the intelligence, surveillance and reconnaissance, stand-off jamming support, and destruction of air defences (see e.g. [54]).

Many of today’s Western combat aircraft such as the F/A-18E/F, the Rafale and the Eurofighter are expected to continue their operational status after 2020. Upgrade programmes and enhancements are expected to add improved sensors such as Active Electronically Scanned Array (AESA) radar and network centricity.

The F-22 is believed to be the world’s most advanced air-to-air fighter. Elements such as low signature, speed and manoeuvrability were important in the F-22 design. When the F-22 programme was conceived the US Air Force was expected to acquire more than 500 aircraft. During the 1990s this number was cut back, and in 2009, funding for additional aircraft was halted at a total of 187 aircraft. The F-22 is also being continuously upgraded, with more emphasis on networking capabilities and the air-to-ground mission.

Figure 4.1 Lockheed Martin’s F-22 Raptor is an air superiority fighter but will also have a limited air-to-ground capability by 2020 (photo: Lockheed Martin).

The F-35 is a multi role combat aircraft. Three variants are being produced: conventional take-off and landing, short take off and vertical landing and a carrier based variant. Together they will replace the F-16, the F/A-18, the A-10, and the Harrier. The aircraft is being developed for the US and eight international partner nations, including Norway. The US plans to acquire well above 2000 F-35 aircraft in addition to international orders. The F-35 is characterized by a low signature design, an advanced sensor suite, and a high level of network centricity in addition to advanced concepts for production and maintenance.

Figure 4.2 F-35A Lightning II test planes during ferry flight (photo: Lockheed Martin).

In Russia, the Su-27 family of combat aircraft is expected to be the pre-eminent fighter family, and it will be upgraded and enhanced the same way as Western aircraft. The Su-27 family has been widely exported, and this is expected to continue. In 2010, Russia showcased for the first time the new PAK-FA T-50 prototype. Little is known about this aircraft, but according to published pictures it looks as though low signature and the air-to-air role have been emphasized. The path to operational capability is unclear.

China has traditionally been dependent on Russian aircraft technology. However, the J-10 combat aircraft has now reached operational capability and this aircraft is claimed to be China's first indigenously developed multi role combat aircraft. This makes China the fourth country together with United States, Russia and France which possesses such a capability[4]. Little is published

[4] The UK, Spain, Italy and Germany have this capability jointly through the Eurofighter Typhoon.

about the J-10, but the aircraft has some design elements which supposedly sets it in the same class as today's European combat aircraft.

On the 11th of January 2011, the Chengdu J-20 made its maiden flight. Although the designation suggests it's a fighter, it has been speculated that the stealthy, canard-design may be a strike-aircraft, or even a naval strike aircraft designed to take out high value assets like tankers, AWACS or even aircraft carriers. Little is known about the fairly advanced design, which by some sources is touted as the Chinese equivalent of F-22 and F-35. There are plans for fielding this aircraft by the 2018–2019 timeframe, but time will show whether the Chengdu will actually manage to overcome numerous technological hurdles in a timely manner.

Figure 4.3 China's indigenously developed multi role combat aircraft J-10 (photo: Wikimedia Commons).

Figure 4.4 The Russian 5th generation fighter Sukhoi PAK-FA T-50 prototype (photo: Sukhoi).

4.2 Other Fixed Wing Aircraft

4.2.1 Bombers

As the stealthy F-117 has been phased out, the US relies on the even stealthier B-2 to supply global reach for their air-delivered conventional and nuclear capability. As this platform is nearing its end of service life, the US is exploring ways to replace its prime long range strike capability. Even though the Next Generation Bomber programme was cancelled, the US is looking at a system-of-systems approach to its penetrating bomber capability requirement, meaning that the platform developed will focus primarily on range, payload and stealth, while supporting assets would supply surveillance, electronic attack and stand-off cruise missile capabilities. Long, dangerous and tedious missions call for an unmanned vehicle. However, the nuclear mission dictates a crewed bomber, therefore advances in optionally manned aircraft is expected. As this platform will be available after 2025 at the earliest, the current bomber fleet will have to extend their service life to provide the long range strike capability.

Currently, the B-1 and B-52, with their long endurance and large payload, are much needed in low intensity conflicts in Iraq and Afghanistan to supply close air support with a large number of stowed kills, and long time on station. As the service life is extended, the B-52 seems slated to become the first aircraft to reach 100 years of service [55]. Due to increased cost, the US might find itself having to replace the old workhorse with smaller platforms – and even though the F-22 may have received a limited air-to-ground capability by 2020, this role will primarily be covered by the F-35, some units which will have received Full Operational Capability by that time.

Figure 4.5 The B-52 may be the first aircraft to reach a hundred years of service life (photo: Wikimedia Commons).

Russia, having extended the service life of the Tu-160 Blackjack supersonic bomber until 2030 [56], must make some hard decisions regarding the future of the Tu-95 Bear and Tu-22 Backfire fleet, as these are nearing their end of service life, being stalwarts of the strategic bomber force, and important for projecting Russian air power.

Figure 4.6 *Russia has taken measures to extend the service life of the Tu-160 Blackjack supersonic bomber (photo: Wikimedia Commons).*

4.2.2 Surveillance Aircraft

With a number of surveillance platforms based on the venerable Boeing 707 platform (E-3 Sentry, E-8C), operators will be faced with the challenge of escalating operating costs and requirements for modern avionics, spurring the need to either re-engine and install glass cockpits, or migrate the surveillance capability to either large platforms like the Boeing E-767, smaller aircraft, like the ubiquitous Boeing 737 or light platforms, like the Gulfstream G550, Saab 2000 or Beechcraft King Air.

Airborne early warning, battle management and command and control systems are essential to the conduct of an air war, as well as ensuring the safe conduct of missions in support of ground forces. This capability will be upheld by the various nations involved, and nations who do not possess it, will look for ways to acquire it.

As the P-3 Orion maritime surveillance aircraft is progressively phased out and substituted by the Boeing 737 based P-8 Poseidon Multi Mission Aircraft, it will be tempting to use the P-8 as a platform for providing surface and ground surveillance services. Even though the last E-8C

J-STARS was phased in during 2005, the US is currently considering ways to upgrade or replace the E-8C fleet.
Other surveillance platforms include the USAF RC-135 Rivet Joint SIGINT platform, and the USN EP-3 Aries Electronic Reconnaissance aircraft. As the former has been refitted with new engines, the programme for replacing the latter with a modern platform has been slated for cancellation, meaning that original large aircraft must receive a service life extension unless the role is to be filled by other, smaller aircraft.

Manned surveillance craft are envisaged to operate in tandem with large surveillance UAVs, the prime example being the P-8 Poseidon working in concert with the Broad Area Maritime Surveillance (BAMS) UAV. A big challenge for the military forces of the West will be to ensure that all the various relevant surveillance assets are able to be networked with the user such that critical intelligence can be received in a timely manner.

Figure 4.7 P-8 Poseidon is based on the Boeing 737 airframe and will replace the P-3 Orion (photo: Boeing).

4.2.3 Transports/Tankers

Operations in Iraq and Afghanistan (a land-locked country), has emphasized the need for airborne transport assets, both inter-theatre as well as intra-theatre. An increasing fleet of strategic transport aircraft has met the immediate pressing need for the ability to transport large items, but there is still a need for transporting outsize cargo between theatres, needs that must be met by chartering very large transports. In 2020, the A-400M will finally have entered service, allowing early versions of the venerable C-130 Hercules to be retired [57]. Simultaneously, smaller transports like the C-27J Spartan and the KC-390, would operate in concert with small C-295,

allowing bespoke transport assets to be allocated to various transport missions. Notably, Russia and India is collaborating on developing a replacement multi role transport aircraft which tentatively should start to enter service after 2016, replacing a number of transport aircraft, including the Antonov An-32. As this seems a bit optimistic, in-service date may well slip beyond 2020, but the main topic of interest here is the developing and deepening ties between Russia and India. A cause for concern is the vulnerability of the transport aircraft against MANPADS and small arms fire during the first and final stages of a mission, driving the need for ballistic protection as well as electronic countermeasures.

A main enabler of any air operation is airborne refuelling, without which a number of operations would simply not be possible. The US currently operates around 500 KC-135, which is slated for replacement under a troubled and controversial acquisition programme dubbed KC-X. By 2020, it must be expected that the differences will have been settled, and that a number of modern platforms will have entered service, alongside the older KC-135. A number of nations acknowledging their importance have acquired aerial refuelling assets, some nations operating dedicated tankers, others opting for a multi-role tanker/transport variant, whereas still others modify existing cargo aircraft to be able to perform the aerial refuelling role. Several nations have concepts using a “buddy-buddy” tanking capability, where combat aircraft through the use of a refuelling pod can refuel similar aircraft, either for increasing bomb load on take-off, or being available as a fuel reserve as aircraft return from missions. If Norway was to go for this option, it would mean ensuring that the F-35 acquired can use the hose-and-drogue refuelling system, as well as ensuring that refuelling tanks with hose drums are integrated on the F-35. Albeit expensive, it may prove to be a cheap way of obtaining extra time on station for the F-35 without having to acquire large tanker aircraft.

Figure 4.8 Touchdown of the much-delayed A-400M Grizzly (photo: EADS).

4.3 Helicopters

4.3.1 Combat Helicopters

Proving their worth during Gulf War I, and their versatility during Gulf War II and in Afghanistan, combat helicopters' main role has shifted somewhat, from the main tank-busting role as envisaged during the cold war, to acting as escort helicopters, armed reconnaissance assets, and support fire platforms for ground troops. Being used not only in rural and channelling terrain, extensive use in urban areas has shown the helicopters to be very vulnerable to MANPADS, rocket-propelled grenades and small arms fire.

European countries have adopted the combat helicopter, using it to support not only air mobile units, but also to support air assault operations through air manoeuvrability, making it possible to perform vertical envelopment manoeuvres. Despite their popularity, operational needs and economy has dictated that countries update and upgrade their existing assets, rather than develop brand new platforms. A number of countries have cancelled development programmes in favour of making use of existing platforms.

Intensive operations in dusty, hot and high conditions have highlighted shortcomings in helicopter's performance, reliability and survivability, making it apparent that keeping a progressively outdated fleet operational is going to prove very challenging in the years to come. Thus, a number of technology development programmes have been initiated. The resulting platforms are not slated to become operational before the latter half of the 2020s. A number of technological paths being followed look promising, and there may be possibilities for retrofitting new technologies into existing platforms around 2020. Promising technologies are tilt-rotor, advanced counter-rotating main rotors which may be slowed down during fast forward flight, and compound helicopters with added thrust supplied by fans or propellers, something which may lead to helicopters finally managing speeds faster than 400 km/h.

Figure 4.9 Sikorsky X2 is an experimental helicopter with coaxial rotors and auxiliary propulsion (photo: Sikorsky).

In the timeframe leading up to 2021, there are no known new Western combat helicopter programmes which may provide a new combat aircraft capability. Russia is investing heavily in the manufacturing site of the Ka-50/52 combat helicopter, which may portend either helicopter export, or preparation for upgrades/updates and new-build helicopters. Having selected the Kamov Ka-50 as their main attack helicopter due to replace the Mi-24/35 “Hind”, Russia later reversed this decision and started acquiring Mil Mi-28 “Havoc”, stating it would operate in conjunction with the twin seat Ka-52 in the reconnaissance/battle management role [58].

China is meanwhile developing their own combat helicopter, the WZ-10, which not surprisingly bears a striking resemblance to the Agusta A129 Mangusta, as Eurocopter and Agusta Westland has assisted China in the development of the Z-10 multirole helicopter, upon which the WZ-10 is based. It was due to enter service in 2009, but was delayed as there have been problems with developing indigenous engines based on Pratt&Whitney Canada’s PT6Cs.

Figure 4.10 Agusta A129 Mangusta (photo: Wikimedia Commons).

4.3.2 Utility Helicopters / Other Roles

Not only fixed wing transport aircraft, but also rotary wing transports are in high demand in all the major operation theatres. A number of new platforms have been phased in, lately the Eurocopter UH-72 Lakota. Production of tried and tested helicopters are still going on – albeit the designs hark back to the 60s and 70s. The helicopter industry’s warning about a production gap beyond 2020 has led to the initiation of advanced helicopter technology programmes which may lead to new helicopters placed in production around 2025. There are hopes that technology

demonstrators based on the Sikorsky X2 prototype will lead to a family of helicopters that may ultimately replace all of the US Army's medium helicopters, and which may be scaled up and down according to the size of helicopter being replaced.

Shortcomings in performance, reliability and survivability are main targets for research efforts, the US focusing to reclaim lost territory to European development efforts. In Europe, the effort has, amongst other, been on reducing vibrations and increasing performance through the use of full length piezo-electric flaps along main rotor blades.

Other notable developments are the long awaited introduction to service of the NH-90 family of helicopters, as well as the continued use of the MV-22 Osprey tilt-rotor. As Augusta Bell's BA609 civilian tilt-rotor is set to receive certification in 2011–2012, a military utility variant may be developed. USMC has also examined the possibilities of using an armed BA609 as escort for the MV-22.

As the world helicopter fleet has been forecasted to grow by 30% by the year 15, a big challenge may be to train and retain qualified helicopter pilots in the armed forces [59].

4.4 Unmanned Aircraft Systems (UAS)

Over the last few years the term Unmanned Aircraft System (UAS) has started to replace Unmanned Aerial Vehicle (UAV). The reason for this is the wish to reflect the whole system (data links, ground station, personnel, aircraft etc.) and not only a vehicle. The term UAV is here used to refer to the aircraft itself. The number of hours flown with UASes has also increased much over the last few years, mainly because of the US and ISAF use of UASes in Iraq and Afghanistan to raise situational awareness in the theatre.

One of the main trends that can be observed is the generational change among the UASes in the West. This is caused by increased focus on operating costs and the desire for better performance, especially longer endurance. New systems are constructed with more composite materials and have been equipped with propulsion systems designed for and adapted to unmanned aircraft. The reduced operating costs and the improved performance of the "new" UASes, mean that the potential candidates for a Norwegian acquisition 4–5 years ago are now completely outdated.

The increased focus on cost/benefit also contributes to a change in the traditional classes of UAS. The largest types, like High Altitude Long Endurance (HALE) and Medium Altitude Long Endurance (MALE), are still the same, but the class that used to be called tactical UAV (TUAV) is disappearing. The tactical systems are getting larger in order to gain better endurance, but also to carry payloads like image building radar (SAR) and ESM sensors. Also, as the system no longer requires catapult and parachute as takeoff and landing method, the operating costs are dramatically reduced. At the same time, the former TUAV class is under "attack" by smaller systems that have obtained considerably better performance due to developments within battery technology and miniaturization of sensors. These are approaching a performance that corresponds

to, or to some degree exceeds the performance of the ”old” TUAV with considerably lower operating costs and manning requirements.

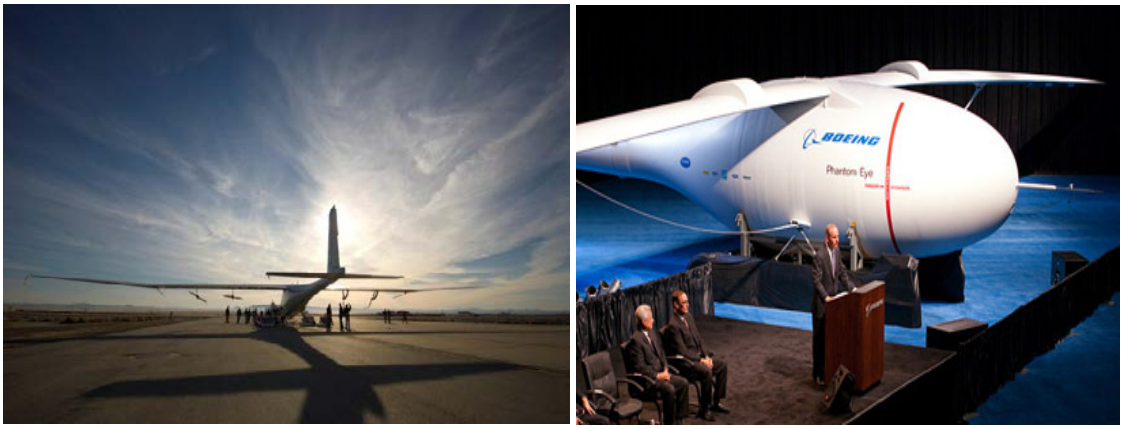

Figure 4.11 Left: Global Observer (photo: AeronVironment Inc.). Right: Phantom Eye (photo: Boeing) are examples of new UASes that can carry considerable payload at high altitudes but are nevertheless able to give an endurance up to a week.

These ”new” smaller systems have made it possible to extend the range of applications of UASes. It is now possible to operate organic air resources with long endurance from smaller surface vessels without helo- or flight-deck. In the lowest end of the size range, small personal UASes (Nano-UASes) are now appearing. These will be available in the near future and will constitute something completely new in military operations.

Figure 4.12 Left: Scan eagle from Insitu during landing on a boat (photo: Insitu). In 2010, the US Navy signed contracts within their STUAS programme for deliveries of UASes to some of their smaller vessels. Right: PD-100 from Prox Dynamics is an example of a Nano-UAS (photo: Prox Dynamics).

The progress of development within electrical propulsion systems will contribute to an increase in the number of electrical UAVs in the years to come. This will include larger systems than the current Mini-UAS (MUAS). The advantages with an electrical propulsion system are higher reliability, less maintenance, smaller acoustical signature and far less vibration that allow for simpler and less expensive sensor installations.

Rapid development is also going on within the area of sensors adapted for use in UASes. Miniaturization of the sensors allows smaller systems to carry multiple sensors simultaneously. SAR radars with a weight of approximately 1 kg have been carried by UAVs in operational use. The same is the case for the more traditional sensor packages containing daylight cameras and IR-cameras. They can be built smaller and have characteristics like HD resolution and IR designation. In addition to making the sensor equipment smaller, an emerging trend is to replace expensive and maintenance-heavy hardware with software. Software-integration of several sensors can, for instance, give the same performance as “stabilized” and “guided” sensors without requiring demanding and expensive installation. This will also open the possibility to “observe” in several directions simultaneously.

Figure 4.13 Left: MX-10 from L-3 that weighs 16.5 kg. Right: NANO- SAR that weighs 1 kg (photos: Gizmag).

Another ongoing trend within the UAS area is digitalization of data links. The main reason for this is a demand for encryption of the ”weak” link in a UAS system. Digitalization will in addition reduce the loss in sensor quality that is experienced in analogue links. Digital links make it easier to transfer data from other sensors on board. They also offer simpler administration and adaptation of usage to the available electromagnetic spectrum.

There are some programmes under way on Unmanned Combat Air Systems (UCASes). These are aircraft that are specially designed to carry weapons. Funding of these programmes has gone up and down over the last 10 years. Presently, the US Navy is in the lead with their UCAS-D programme. The goal is to demonstrate carrier operations with a low signature platform with the

ability to penetrate, keep under surveillance, and attack targets in a high threat area. The weapon size may be reduced because it is able to hit the target more precisely, and there is also a need to reduce collateral damage. The development of non-kinetic weapons adapted to UAVs can also be expected in the time to come.

Figure 4.14 Artistic impression of a UCAS-D on the flight deck of a carrier (source: US Navy).

As a supplement to the development of UCAS, there are also ongoing demonstration programmes concerning conversion of former manned aircraft to UAVs. In the US, DARPA is now carrying out programmes where, among others, unmanned A-10s will be used for Close Air Support (CAS). A demonstration is planned for 2012–2013. Such activities will probably stimulate interest in converting 3rd and 4th generation combat aircraft, that are now being phased out in the West, as ”inexpensive” UCASes.

While the work to reduce the technical operating costs of UASes is going on, there is also effort put into reducing manning requirements. This is done by automating some processes. The field with the highest potential for manning reductions is probably within processing of sensor data. But there are also put effort into reducing UAS operating errors. One example is the introduction of automated landing which reduced the number of crashes compared to manual landings.

Another important trend is co-operation between manned and unmanned platforms. So far this has been a US Army activity but it is likely that others will follow. US Army has achieved such promising results that they will set up a unit with helicopters and UASes. The US Army has upgraded their AH-64Ds, and plans to upgrade their OH-58s, with equipment that receives sensor data directly from a UAV. In addition, interoperability level 4 is included in the AH-64D upgrade, which means that the crew in the helicopter has full control over the UAV except for takeoff and landing. The upgraded AH64D will be delivered from 2011. This concept was tested by Boeing with their Optional Piloted Vehicle (OPV) AH-6U in 2009.

Figure 4.15 Left: AH-6U together with AH-64 (photo: Boeing). Right: K-max, during replenishment demonstration (photo: Lockheed Martin).

A new application for UASes is being explored within logistics. The USMC is currently in the lead. They want UASes that can carry out replenishment of forward bases (minimum 1500 kg within 6 hours at a range of 150 nm). The plan is to get this in place in Afghanistan within a few years. Medevac from forward positions is also a task where the UAS will take over the role of today's manned helicopters. Initially, it is to be expected that these "logistic" UASes will consist of manned aircraft that later on will be converted to unmanned aircraft. The UAVs pictured in the Figure 4.15 are both examples of such OPVs.

4.5 Air Delivered Weapons

4.5.1 Bombs

Use of unguided munitions such as ballistic bombs is declining. With the combination of reduced risk for the delivery platform by increased stand-off range, reduced risk for causing collateral damage through improved precision and that guidance kits are getting quite affordable means, it is simply not cost effective to drop unguided bombs on military targets. The contractors are either developing kits for existing ballistic bombs or developing entirely new concepts. Examples of the latter are Small Diameter Bomb Increment I (SDB I), Small Diameter Bomb Increment II (SDB II) and Joint Stand-off Weapon (JSOW). GBU-39/B SDB I is a Boeing developed weapon [60]. Its small size allows multi role fighters to carry up to 24 of these. The Diamond Back wing kit can carry the GPS-guided bomb more than 110 km. SDB I can penetrate in excess of three feet of steel reinforced concrete, which is more than one can expect from other 250 lbs sized weapons. The SDB I warhead weighs 93 kg. Raytheon's GBU-53/B SDB II [61] is based on the SDB I, but apart from the size there are many differences. SDB II can receive target updates in-flight due to a two-way weapons data link. The weapon uses the tri-mode seeker to refine the aim point and to find and engage moving targets. Millimetre wave radar, a semi-active laser seeker and an un-cooled imaging infrared seeker allows the weapon to be used in different scenarios, adverse weather conditions and against various targets.

Figure 4.16 Left: GBU-39/B SDB I (source: Boeing). Right: Two JSOW glide bombs being inspected (photo: Raytheon/US Navy).

Another weapon developed by Raytheon is JSOW [62]. This family of glide weapons has a maximum range of 130 km and carries 500 lbs payloads. The newest JSOW version has a two stage penetrating warhead, a two-way weapons data link and an imaging infrared seeker. Raytheon is also developing a powered version called JSOW-ER. The addition of a motor is expected to increase the maximum range to over 290 km, but at the expense of a smaller 300 lbs warhead.

There are also a few special bombs that are designed for extremely hard targets or large area destruction. An example of the latter is the US Air Force project Massive Ordnance Air Blast (MOAB).

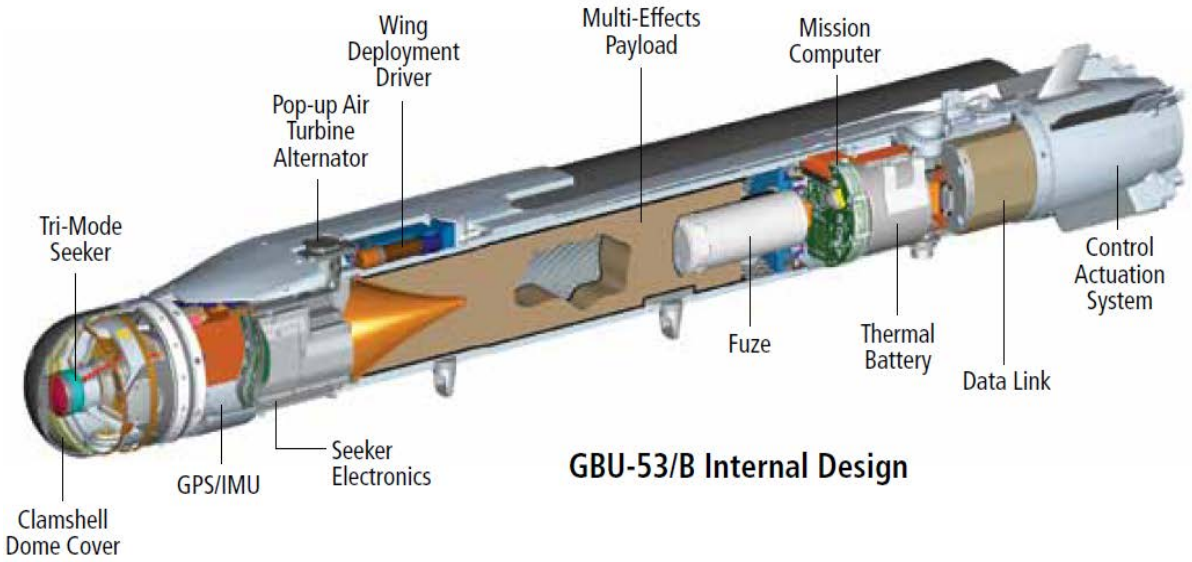

Figure 4.17 Internal design of the GBU-53/B SDB II (source: Raytheon).

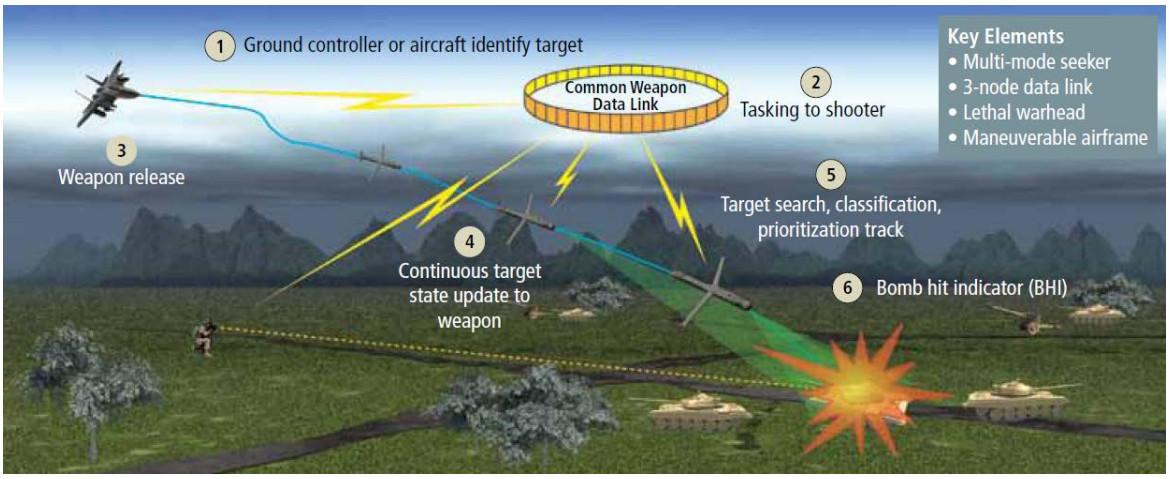

Figure 4.18 SDB II mission concept (source: Raytheon).

Figure 4.19 GBU-43/B Massive Ordnance Air Blast Bomb on display (photo: Wikimedia Commons).

4.5.2 Rockets

As for bombs, the use of ballistic rockets is also declining, but not as quickly. Work is, however, underway by manufacturers such as KDA to equip simple rockets with guidance kits. The most likely guidance mode is semi active laser guidance, but also EO/IR is being explored. Either of these modes can conceivably be combined with GPS, though only for longer range indirect fire flights. The primary platforms for guided rockets are helicopters and UAVs. The target set is point targets that are not excessively armoured.

The advantage of guided rockets is that they can multiply the kills per sortie from an attack helicopter and at a much reduced cost. For example: an AH-64 Apache helicopter can carry 76 2.75” (70mm) rockets, alternatively 16 AGM-114 Hellfire missiles, or a 38:8 mix [63].

An expected probability of kill of 0.5 for 76 guided rockets against light vehicles or other point targets would result in a potential of 38 kills, compared to using Hellfires and a max of 16 assuming a kill-probability of 1.0. The cost for the 76 rockets is also expected to be much less than for 16 Hellfires.

Figure 4.20 *Hydra 70 rockets in an M261 launch pod on a Dutch AH-64 Apache on display at the RIAT2007 (photo: Wikimedia Commons).*

5 Missiles

5.1 General Trends

As for other military programmes, the number of missile programmes in development is shrinking globally. Going against this trend is China, India, Israel and some newer missile producing nations such as Iran, South Korea, South Africa and Taiwan where the number of missile programmes is steady or increasing. Missile development is a long and costly exercise and requires lots of testing and infrastructure. Development time is anything from 5–10 years for simple systems that build on previous developed technology, to up to 20 years or more for completely new systems. Hence, it is foreseen that during the next decade only a few handfuls of totally new missile systems can be expected to see operational service, mainly associated with UAVs, anti-tank missiles and other small munitions.

Furthermore, the cost of new sensor capabilities is constantly rising, due to an ever increasing need for more information by military and civilian leaders. One side-effect of this development is that the munitions depend more and more on external systems, e.g. satellite navigation, data links and the superior sensors of non-expendable systems like manned and unmanned aerial platforms.

This can still result in very effective weapon systems, though they may be more vulnerable to countermeasures.

In general, missile development can be divided into two main schools of thought. One is the traditional role of a highly advanced weapon that is designed to strike a target that is heavily defended at stand-off range. In such scenarios air/land/sea superiority is either not expected or expected for a short time. This results in systems that are highly autonomous, and hence costly, if the platform or operator is to survive the engagement. Nations that cannot trust external systems and cannot expect to have either air superiority or air supremacy are much more likely to have to rely on such advanced and autonomous air-to-surface weaponry in order to get through enemy defences. Large Western nations, who can afford a full tool-kit of weaponry, are also likely to have a limited amount of such advanced autonomous missiles. Hence, during the next decade up to 2021, countries such Russia, China and India are expected to be catching up with at least Western Europe when it comes to the development of advanced aerial delivered weaponry. A very good indication of this can be seen in air-to-air missiles, where Russia, China and India are developing increasingly advanced missiles at a rate that is staggering to Western military forces.

The other school is capitalizing on US and NATO air/land/sea/space superiority, where one can make use of simpler missiles and other air-to-ground munitions without unduly risking the platform or operator. Here, the focus is on making sure the munitions strike the right target and that the operator has control over the weapon until the last possible moment. The ability to set fuses and the size of the warhead effect are also expected to be more common during the next decade.

Much focus here is also on reducing size in order to carry as many munitions as possible and again to reduce unit costs. A way to reduce costs is to make such munitions as flexible as possible. Though this may add to development and production costs, a trend is to replace two or more older systems with just one new and better. This can save quite a bit of money in logistics and investment.

Another trend is to replace as many different weapon families as possible with only one or two new flexible multi-role weapons. Examples are the Raytheon Small Diameter Bomb II, GBU-53/B and the Joint Air-to-Ground Missile (JAGM) programme [64]. Apart from these systems, the development of air-to-ground weaponry is expected with few exceptions to be quite slow in the Western world in the coming years due to lack of funding (and threats). Hence, updates of existing weapons seem far more likely than completely new weapons in the decade to come.

GPS or other satellite systems have been standard for all weaponry developed during the last decade. The introduction of network enabled weapon data links seems to be the trend in the near future. The most important development expected in missile technology in the next decade, is that munitions will be able to accept control by other actors than the actual delivery platform.

There is an ongoing debate whether hypersonic long range missiles will make it into operational service during the next decade. The only nation that really is working on this subject is US, but

even here money is tight. It seems unlikely that such capability will be produced for export by USA in the foreseeable future. Other, though more unlikely, countries that could also come up with such long range hypersonic missiles are China, Russia and India, but not before 2025.

Figure 5.1 NASA's X-43A scramjet-powered research aircraft (source: NASA).

Ballistic missile defence is a technology driver within the surface-to-air sector. Meanwhile, the wars in Iraq and Afghanistan demonstrated the effectiveness of very simple anti-aircraft missiles against helicopters.

Anti-ship missiles have been more or less neglected in the Western world and Russia during the last 20 years. Some updates have occurred to Harpoon and Exocet adding longer range, improved littoral capability and land attack capability. The only new anti-ship missiles in the Western world during the next decade are expected to be the Norwegian Naval Strike Missile (NSM) launched from ships, land and helicopters and the Joint Strike Missile (JSM) from combat aircraft. These passive stealth missiles combine a whole spectre of innovative new technologies to create the most advanced subsonic anti-ship missiles in the world.

In India and China, work on anti-ship missiles is continuing. In India the focus is on developing the supersonic Brahmos missile with Russian assistance. This missile is being made into a multi-platform sea and land attack missile. In China, a wide range of sub and supersonic anti-ship missiles are being developed. Some of this work has been based on Russian technology, but during the last years China seems to develop missiles based on own technology. The most innovative type of anti-ship missiles being developed seems to be long range ballistic missiles with radar guidance in the terminal phase. The main reason for developing such a large and costly weapon is the need to be able to attack US Navy Carrier Battle Groups. No other country, apart from possibly Russia, is likely to have the means to develop and acquire such weapons.

5.2 Ballistic Missiles

Intercontinental ballistic missiles armed with nuclear weapons have been used as a deterrent against nuclear attacks since the late fifties. Today the United States, France, UK, Russia, China and Israel have operational systems. In January 2010, France successfully carried out a test firing

from a submarine of its new intercontinental ballistic missile M–51. M–51 is intended to replace the M–41 ballistic missile onboard the Le Triomphant submarines.

A new use of ballistic missiles has been explored by the US Air Force in their development of the Conventional Strike Missile (CSM). CSM was one of the solutions competing for the realization of the Conventional Prompt Global Strike (CPGS) capability. This is a capability to launch a conventional attack anywhere in the world within an hour.

The CSM consists of a ballistic missile that launches a glider into hypersonic flight (mach 18). The glider is then remotely controlled and updated to achieve a high precision impact. The Hypersonic Test Vehicle 2 (HTV-2) from DARPA is the selected glider and it is launched by a Minotaur IV Lite from Orbital. The first test took place on 22 April 2010. In this first flight, the rocket successfully separated from and delivered the Falcon HTV-2 into space, but due to a malfunction it didn't succeed in its intended 30 minute flight over the Pacific Ocean [65].

The CSM has proven to be a controversial issue with the U.S. Congress on the one hand and Russia on the other. The CSM could be mistaken for an intercontinental ballistic nuclear missile and trigger a counter-attack from for instance Russia. Another issue is that the CSM would be counted as part of the missile’s quotas agreed upon in the New Strategic Arms Reduction Treaty (New START).

Figure 5.2 Depiction of Hypersonic Test Vehicle 2 in re-entry phase (source: DARPA [65]).

Figure 5.3 Historic first launch of HTV-2 from Vandenberg Air Force Base on 22 April 2010 (photo: see [66]).

5.3 Cruise Missiles

During the period 1990–2010 a whole generation of subsonic Western cruise missiles (Tactical Tomahawk, JASSM, Scalp/Storm Shadow, KEPD350) have been developed and put into service in most Western nations that can afford to purchase and support such weapons. Apart from a follow on development of Scalp called Scalp Navale for use from submarines and ships, new developments are unlikely. Updates to these cruise missiles in the form of data links, new terminal seekers and new warheads are possible in the next 15 years. The main focus in the West has recently been on destruction of hard targets. Examples of this are JASSM, SCALP and KEPD350. This work seems to be continuing since the European missile developer MBDA recently published a test of the HARDBUT warhead. It is currently uncertain which of the weapon systems will incorporate this bunker busting warhead.

Figure 5.4 Left: JASSM – a stealthy subsonic air launched cruise missile (photo: Lockheed Martin). Right: Boeing X-51 – a prototype hypersonic cruise missile (photo: Boeing).

The US is also pursuing hard target cruise missile capability, but is instead working on hypersonic missiles using kinetic penetrators. The most developed programme seems to be the Boeing X-51 [67]. This test prototype has flown up to 143 seconds at hypersonic speed utilizing a scramjet engine. Only USA is foreseen to be able to develop and put into operational use the latter during the decade to come.

It's also possible to make extremely low-cost cruise missiles. An example of this is the Affordable Weapon [68], which was tested by the US Navy. It is based on off-the-shelf components, with limited range (1100 km) and a small warhead (90 kg). The expected price of such a weapon is 30–40 times cheaper than today's Tomahawk.

Cruise missile development is spreading and quite a few nations have the capability to develop such weapons. Russia, China, India, Taiwan, Iran and others are likely to either develop new or refine their current designs both for own demands and for exports. These weapons can either be sub- or supersonic and delivered from different types of platforms.

Figure 5.5 Sleigh test of MBDA's new HARDBUT warhead (photo: MBDA).

5.4 Anti-ship Missiles

Anti-ship missiles have seen a decline in interest in the Western world and Russia during the last 20 years. Some updates have occurred with Exocet and Harpoon adding longer range, improved littoral capacity and land attack capability. An exception is the Norwegian Naval Strike Missile (NSM), the completely new development mentioned in section 5.1, and shown in the figure below.

Figure 5.6 NSM – a newly developed anti-ship missile on display (photo: Wikimedia Commons).

The latest generation of Western anti-ship missiles (NSM, Harpoon Block II and Exocet Block 3) has remarkably similar characteristics; long range (120–180 km), use of a gas turbine engine, and precision navigation through the use of GPS and inertial measurement units (IMUs). Helicopter-based anti-ship missiles have seen little development during the last decade. However, in late 2009 France and UK announced a common assessment study for a new development (Future Anti-Surface Guided Weapon) to be launched from French NH-90 and UK Lynx helicopters [69].

The drivers for anti-ship missile development are littoral engagements. Apart from the NSM, which uses a passive infrared seeker designed for littoral scenarios, most other missiles utilize active radar seekers. Radar seekers have traditionally had reduced performance close to land, so much effort has been put into mitigating this problem in recent years.

The lack of weapon data links in NSM, Exocet, RBS15 and Harpoon is restrictive from an operational point of view. Given that an engagement takes up to 10 minutes from fire to hit, it is problematic not to be able to update the target position or abort the mission. Retrofitting data links are therefore considered in the above-mentioned programmes.

Several companies are looking into installing their missiles in vertical launch tubes to free up deck space, but so far this has not led to any new contracts. The potentially biggest Western programme coming is the US Navy considering replacements for the Harpoon missile. An analysis of alternatives for offensive anti-surface weapons was started in December 2010 and is expected to conclude by late 2011. This include submarine, surface and air delivered weapons including the two Long Range Anti-Ship Missile concepts developed by Lockheed Martin for DARPA/ONR [70].

Anti-ship missiles are meeting competition from other weapons in crises and terrorist scenarios. Shorter-range anti-air missiles such as the Standard Missile, Sea Sparrow, Rolling Airframe Missile (RAM) and Mistral can also be used against surface targets. Such missiles typically have a shorter response time for use in self-defence operations. Guns are also getting more precise, making them useful for short-range engagements of surface ships. The high cost of dedicated anti-ship missiles (1–2 million USD) make them less useful for engagement against smaller targets including fast terrorist vessels.

China and India are pursuing other ideas to penetrate Western-type ship defences, incorporating supersonic sea skimming missiles (like India's Brahmos) and ballistic anti-ship missiles like China's DF-21D [71], see Figure 5.7. Some of this work is based on Russian technology or is being performed in cooperation with Russia. Lately, China seems to be developing missiles based on domestic technology.

Figure 5.7 Dongfeng 21D (photo: Wikimedia Commons).

5.5 Ground Based Air Defence Missiles

Modern air defence systems are good at countering the threat from aircraft. The technological challenge today is to improve the air defence system's capability towards ballistic missiles and cruise missiles and at the same time retain the capability towards the traditional threats. This trend poses a challenge to both sensors and interceptors. Countering the threat from ballistic missiles and cruise missiles are two different challenges. A ballistic missile moves fast, far beyond the speed of a fighter. The most significant development on the missiles design to intercept ballistic missiles is the use of the hit-to-kill/direct impact missiles. Proximity fuses and fragmenting warheads are not used. To improve the capability to intercept cruise missiles, the development of warheads with even more, but smaller shrapnel is ongoing.

Based on experience from the first Gulf war, the US fielded the PATRIOT Advanced Capability 3, PAC-3, which introduced a new missile – the MIM-104F.

The THAAD system (as mentioned in Section 2.4) has an interceptor that will be able to intercept incoming missiles at an altitude of 150 km. This is a hit-to-kill missile that has no warhead but relies on kinetic energy on impact.

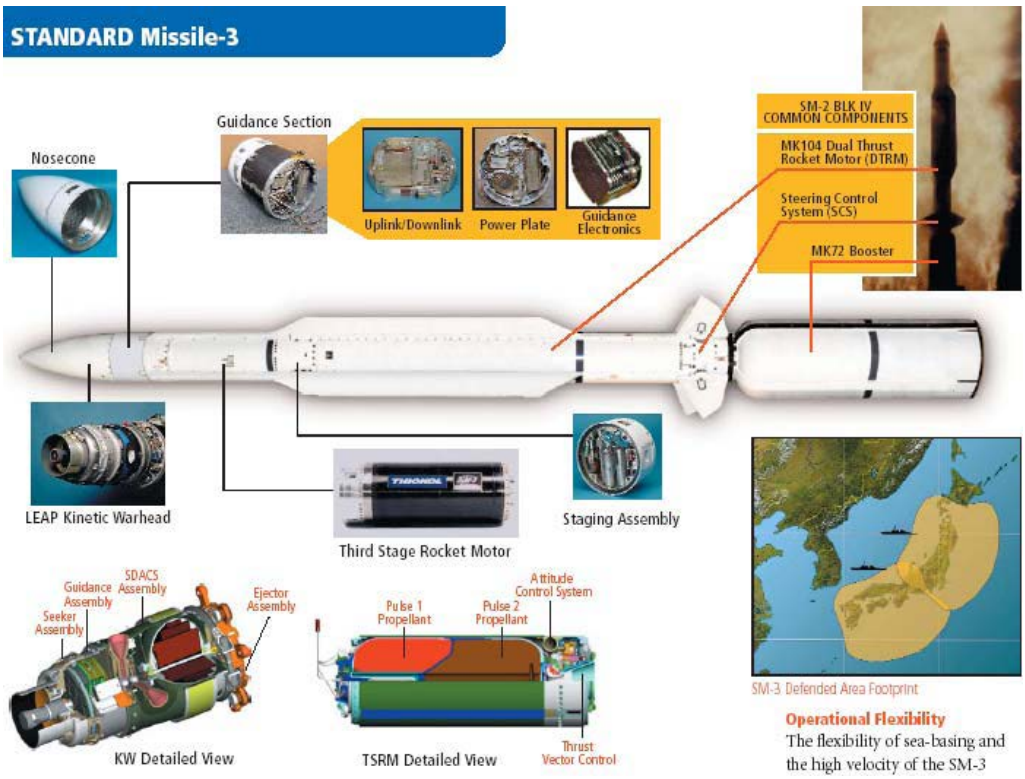

Figure 5.8 Standard Missile 3 (SM-3) could play a central role in the US and Japan's defence against ballistic missiles. The Norwegian Fridtjof Nansen class frigate can be modified to carry these missiles (source: Raytheon).

The Standard Missile 3 (SM-3) is a naval system with an exo-atmospheric hit-to-kill capability. This missile is the main interceptor in the missile defence strategy that is currently evolving in NATO. There exist plans for upgrading this missile until 2020. The first phase includes the ability to launch the missile from land-based systems. The Standard Missile 6 (SM-6) takes full advantage of the legacy from the Standard Missile's airframe and propulsion technology and the AIM-120 guidance control.

There are some examples on ground based air defence systems that incorporate an air-to-air missile used in a surface-to-air role. The Norwegian NASAMS and Raytheon's SLAMRAAM system use the AIM-120 AMRAAM missile as a surface launched air defence missile. The German air to air missile IRIS-T will be integrated in a surface launched version (IRIS-T SL) in the MEADS system as a secondary missile.

Another European-based missile is the ASTER missile, a French/Italian ship and ground based surface-to-air missile. There are two version of this missile. The main difference is their operational range: ASTER-15 and ASTER 30. These missiles rely on an active radar seeker, a proximity fuse and a fragmenting warhead.

5.6 Air-to-Ground Missile Programmes

The most important development programme in the air-to-ground missile sector today is the Joint Air to Ground Missile (JAGM) programme [72]. The goal of this programme is to develop a cost effective and flexible air-to-ground missile. JAGM is designed to replace Maverick, Hellfire and TOW. The missile will probably be used by the US Navy, US Marines and US Army, and will be integrated on a variety of helicopters and fixed wing aircraft. The tri-mode seeker will allow operations in different kinds of weather, both night and day. The three modes consist of active millimetre wave radar, semi-active laser and imaging infrared. The maximum range will be 16 km when launched from a helicopter and 28 km when launched from a fixed wing aircraft. Lockheed Martin is competing against the Boeing/Raytheon-team for the JAGM contract. In 2011, US Navy and US Air Force proposed to stop the JAGM program due to budget cuts; however, in 2012 it was decided that the program should continue with reduced funding [73]. Initial operational capability is planned for 2016 [74].

Figure 5.9 Left: Raytheon JAGM test firing (photo: Raytheon). Right: Lockheed Martin JAGM fit check (photo: Lockheed Martin).

5.7 Air-to-air Missiles

General trends within air-to-air missile technology should be evaluated in terms of Western missile trends, and non-Western missile trends, as these two groups have had a slightly different focus over the last few years. This difference in focus is expected to last into the 2020's.

One difference is the West's focus on handover and mid course correction capability for medium and long range missiles. This has been made possible due to added functionality given by two-way data-links. Non-Western missiles of similar range tend to be more fire-and-forget oriented with active radars or IR seekers.

Another difference between the approaches is how these system families have developed. In the West most military forces have decided on a convergent strategy for most military assets. This means fewer missile designs with more functionality with the intent of creating a set of relatively few missiles that can perform any task. The penalty is the need to add components to missiles, such as two-way data link, GPS and INS.

The non-Western trend appears to be more divergent, in that specific iterations of a missile are designed for one specific task only. The result is that they use fewer components on any given iteration than a similar Western missile. This frees up space for payload and/or fuel, and could also result in more resistance to counter-measures. However, as a result there are more missiles types, albeit only slightly different from one another. All these must be maintained, and missions must be planned taking the different missile iterations into account.

One common trend is the economic incentives inherent in improving existing missile designs as opposed to developing new or novel missile concepts from scratch. Several missile systems have gone through numerous upgrades, adding functionality or improving effectiveness. The AIM-120 (AMRAAM) family and R-77 (AA-12 Adder) family are the most prominent examples. One should expect that these families will continue to spawn new iterations.

Figure 5.10 F-16 with an AIM-120 AMRAAM on its wing tip station (photo: Raytheon).

Figure 5.11 R-77 Vympel (AA-12 Adder) on display (photo: Wikimedia Commons).

Another common trend is the emergence of ram-/scramjet missiles or BVRAAM (Beyond Visual Range Air to Air Missile). The British METEOR missile (scheduled to enter UK service in 2015, pushed back from 2012 [75]) is probably the best known, but there are also similar R-77 scramjet derivatives, although these may not be completed without further funding. BVRAAM missiles aim at extending the range of air-to-air missiles while maintaining high lethality. More ramjet missiles will probably emerge, and the technology might well expand from the BVRAAM / AMRAAM (Advanced Medium Range Air to Air Missile) group to the high end of the ASRAAM group, due to the potential benefit of variable throttle. China is likely to develop its own ramjet missiles in the near future, being one of the few countries that are developing genuinely new missiles.

The main driver behind the differences in missile technology and trends between the two groups is aircraft design. The West leads the way in terms of stealth and sensor technology, and tends to favour more fuel efficient engine designs rather than opting for more power. The next decade should see a continued difference in missile designs until non-Western stealth aircraft emerge from production lines and the gap in sensor technology disappears. After that, one should expect to see more convergence in missile technology across the board.

Missile technology is sensitive to aircraft stealth and sensor technology. As sensor technology improves, we should see more long range BVR missiles emerge to take advantage of added sensor range. New designs will likely build on the work done with the METEOR, and there will be improvements upon the AIM-120 series. An opposing trend, however, is that as stealth improves, the detection distance decreases, crating the need for improved short/medium range missile. This development means that further improvements upon the AIM-9 series become more likely.

Stealth and sensor technology are applying different pressures to the engagement envelope of air-to-air missiles. The needs of the two groups are different. Western nations require long range missiles to take advantage of the difference in the ranges where their aircraft are capable of detecting an enemy aircraft and where that enemy can detect them. Non-Western designs may focus on either long range missiles with improved, or multiple, sensors to “sniff” out stealth aircraft or on the improvement of medium range missiles to the extent that when they do detect Western aircraft they may immediately launch and expect high lethality. Both are likely since there is a need to be able to engage both 5th generation Western aircraft and legacy aircraft.

5.7.1 Air-to-air Missile Programmes

METEOR is expected to enter UK service in 2015 [75] (pushed back from 2012) but could be put in service on the Swedish Gripen as early as 2014, as the missile are scheduled for delivery before the end of 2013 [76]. A variant of METEOR with clipped wings has also been tested. Four of these missiles will fit in the weapons bay of the F-35. It will be ready for the Block 5 F-35s. The METEOR is more capable than the AMRAAM family due to the use of ramjet and variable throttle technologies.

One should expect to see work starting on an AIM-9X replacement. MBDA’s ASRAAM (AIM-132) is already a more capable missile at longer range than the AIM-9X in the same way that the METEOR is more capable than the AIM-120D. However, one should expect improvements on the AIM-9 and the ASRAAM, as well as the competing R-73 and IRIS-T families. It is unlikely that these systems will be replaced by entirely new and novel missiles systems, although competitors may certainly emerge.

Figure 5.12 IRIS-T short range air-to-air missile with an IR-seeker (photo: Wikimedia Commons).

The Vympel R-77 has already been tested with ramjet technology, but it is not yet a mature and capable system. If funding is given it will likely be upgraded, and time will tell if it is capable of competing with METEOR and JDRADM.

NCADE (Network Centric Airborne Defense Element) is a modified AIM-120 with the specific task of engaging short and medium range ballistic missiles, in the boost and ascent phases. It combines the IR seeker from the AIM-9X and a two stage rocket engine. Having been tested in

2007 [77], it will be integrated onto most USAF platforms if the programme survives. It is also expected that the missile will be able to target other air platforms.

JDRADM (Joint Dual Role Air Dominance Missile) is a very interesting programme for two reasons. On one hand it promises to be an upgrade of the AIM-120D while at the same time integrating the anti-radar capability of the AGM-88 (HARM). It would replace two missile systems, and is a proof of the intent in the West to reduce the number of missile systems by combining capabilities in new missiles. The other innovation is the addition of SWIFT (sub-millimetre wave imaging fuse technology). It adds an adapted directional warhead to JDRADM capable of classifying the intended target and using directional fragmentation to take it down. The technology has been available for surface-to-air missiles but this is the first time it has migrated to air-to-air missiles. SWIFT should allow smaller fragmentation yields to take down similar targets or equal fragmentation yields to take on tougher targets.

China is rapidly developing missiles to compete with Western designs, but it is always difficult to verify the actual status of the various programmes. The following three missiles may enter service or receive upgrades within the next decade. The new PL-10 may outrange the AIM-9X and perhaps even the ASRAAM in the short range category. Development started in 2005 and flight testing has been going on since 2008. The PL-12 entered service in 2007 and is derived from the R-77 and comparable to the AIM-120 family. We should expect upgrades to the sensors that should increase lethality to, and perhaps beyond, the levels seen in the AIM-120 family. The rumoured ramjet PL-13 (may also be named PL-21), is likely a Chinese METEOR derivative with two-way data link and an active radar seeker. This missile, if completed, would extend the range of Chinese AAMs to, or more likely beyond, similar Western missiles. Development is believed to have begun in 2009/2010.

6 Developments in Space

6.1 The Global Picture in Space

The US has maintained a leading position in space technology development and the use of space, both for civil and military purposes since the early 1960s. Other major space faring nations are Russia, Japan and China, with China and Japan growing very rapidly. Europe's largest space programme is managed by the European Space Agency (ESA), an international agency with 18 member states. In recent years, the European Union has also established a space budget, funding large developments both in satellite-based navigation and Earth observation. A number of European states also have national space programmes. France is the largest European investor in space programmes (both nationally and through ESA), followed by Germany and Italy.

Table 6.1 provides an overview of estimated space budgets for the largest nations and international bodies. Estimates of spending on military space programmes is much less accessible, and can only be reasonably reliable estimated for the US and France. In addition, it is reasonable to assume that significant parts of the Russian and Chinese space budgets are dedicated to military programmes.

Country/Organisation	Budget (billion US $)
USA	64.5 (Incl. $ 43.5 billion US $ on military space programs)
ESA	5.2
Japan	3.7
Russia	2.9
China	1.8
EU	1.6
France	1.1 (National funds, incl. 0.7 billion US $ on military space programs) 1.0 (Additional funds – French contribution to ESA)
India	1.1
Norway	0.08 (470 MNOK, including 0.06 billion US $ contribution to ESA)

Table 6.1 National space budgets for major space nations, 2009. ESA, the EU and Norway are also included (source: see [78, 79]).

6.1.1 Some High-level Trends

The commercial space business totals revenues are approximately 3 times the combined national space budgets of the world, dominated by the global SATCOM industry. The commercial space business is experiencing strong growth, both for SATCOM services and for launch services. Russia is the largest commercial launch provider.

Russia is also the largest provider of cargo and crew transportation services for the International Space Station (ISS). The US has also developed a new policy to promote commercial space

transportation both for servicing the ISS and also to support development of space tourism. The American need for commercial space transportation has become especially relevant, as the Space Shuttle is being retired, and NASA's development of a new crew transportation vehicle and associated launch vehicle has been delayed.

Figure 6.1 The Dragon spacecraft, built by the American company SpaceX, completed the first orbital test in December 2010, orbiting the Earth twice. This spacecraft can take up to 7 astronauts to the ISS, or serve as a cargo transporter (source: see [7]).

Furthermore, we see a large growth in the so-called geo-location services market. GPS receivers are now available on a microchip, and are being incorporated in a wide range of consumer electronics products (as well as in military equipment). Innovation is driving the development of many new applications and services, often delivered through new gadgets, resulting in a multi-billion dollar industry. Hence, society has become very dependent on GPS and similar systems.

Miniaturisation of electronics has a strong influence on the design of equipment being launched into space. So-called "micro-space" technology is now making it possible to build very small, but capable, satellites, resulting in low cost vehicles and reduced launch costs.

Cost reductions associated with commercialisation of space are making access to space affordable to an increasing number of countries. Some are developing indigenous space capabilities, while others are simply buying satellites delivered in orbit. Approximately 40 countries operate satellites in orbit around the Earth. In addition, a number of companies in the private sector now operate constellations of communications and Earth observation satellites. This means that virtually anyone can purchase a satellite image at 50 cm resolution, from almost anywhere in the world, in a matter of hours or at most a few days. Commercial providers have also become important suppliers of satellite imagery and SATCOM capacity for military customers in countries such as the US, UK, Spain, as well as to NATO.

6.2 Navigation Satellites

The American GPS system continues to be the dominating global navigation satellite system (GNSS). The Soviet Union developed a similar system, GLONASS, but in the post-Soviet era GLONASS was left to deteriorate for many years. In recent years, however, Russia has launched a recovery programme and GLONASS is almost operational again, despite the loss of 3 satellites in a recent launch. Russia has also embarked on an upgrade programme for GLONASS, to deploy a second generation system in the coming years.

The European Union (EU) is also developing an alternative system to GPS, Galileo. Galileo is a civilian system, and will provide signals for several services or channels. The Public Regulated Service (PRS) will provide encrypted signals to approved users, primarily civilian authorities in the EU and its partners. Norway has negotiated an agreement with the EU to participate in Galileo. The date for initial operational capability has been around 2014, although this is now expected to slip.

India, Japan and China are also developing their own navigation satellite systems. While Japan and India are focussing regional systems, China has declared an ambition to build a global system, COMPASS.

The US is developing upgrades to GPS. GPS II is being deployed already, while GPS III is still under development. GPS is a military system, and both GPS II and GPS III are designed to be incrementally more robust against jamming, and will provide signals for an encrypted service (M-Code) available only to approved military users. Such users are expected to be US military users and allied forces.

6.2.1 Perspectives

GPS, GLONASS and COMPASS have some level of interoperability for civilian users. It is therefore likely that future user equipment will be able to use signals from many satellites, which will improve reliability in densely wooded areas and in urban areas (urban canyons).

GPS is expected to be the main GNSS system for the Norwegian military, for the foreseeable future. In connection with crisis response and other situations requiring civil-military cooperation, the Norwegian Defence should be prepared to have to cooperate with entities equipped with Galileo units equipped to make use of PRS signals, also in situations where it may be necessary to disrupt open GNSS signals in order to deny an opponent the use of them.

An increasing number of military platforms and weapons systems are equipped with GPS, which also has led to development of more advanced techniques for so-called navigation warfare (NAVWAR). It is therefore important to ensure that Norwegian forces are capable of using both offensive and defence NAVWAR measures.

Improved targeting capabilities are also leading to more precise delivery of fire power, thus reducing the amount of ammunition and/or missiles required to complete a given operation.

6.3 Surveillance Satellites

Surveillance satellites comprise in the broadest sense:

- Photo and radar satellites with an ability to acquire imagery with a spatial resolution better than 1 m. These satellites are equipped with either radar or electro-optical sensors operating at wavelengths from visible light to infra red. The military applications for such satellites are often denominated IMINT (Imagery Intelligence), GEOINT (Geospatial Intelligence) and METOC (Meteorology/Oceanography), discussed further below.

- SIGINT satellites for detecting and locating signal sources (radio and radar transmitters), and analysis and decoding of signals from those sources. SIGINT satellites can be categorised into two main groups: COMINT and ELINT satellites.

Surveillance satellites are mainly used to monitor the Earth's surface. The US is a world leader in developing satellites to monitor other satellites in Earth-bound orbits.

Until about the year 2000, there was a reasonably well defined distinction between military surveillance and civilian earth observation satellites. Today, we have civilian satellites capable of monitoring objects, infrastructure, and mapping the Earth's surface with sufficient detail to be of military value. The cost of the required technology has come down, thus enabling several countries (e.g. Germany, France and Italy) to develop national satellites that are purely military, purely civilian or so-called dual-use.

6.3.1 IMINT / GEOINT

The US's military reconnaissance satellites were originally developed for collection of high resolution images for strategic surveillance during the Cold War. Since then, a number of programmes have been initiated to develop new generations of both optical and radar satellites. The most well known are Future Imagery Architecture (FIA) and Space Based Radar, followed by Broad Area Space-based Imagery Collector (BASIC) and Space Radar, all of which were cancelled due to large cost and schedule over-runs.

These development programmes were driven not only by strategic surveillance requirements, but also by requirements for reconnaissance and surveillance at the operational level. In parallel, the enormous development in modern communications infrastructure have led to substantially more demanding requirements with respect to response time from initiating satellite acquisitions to delivery of imagery and analyses. This has no doubt raised the level of complexity for both mission architectures and technology solutions.

Since the termination of the above mentioned programmes, less information has been publicized on programmes for replacement of the aging reconnaissance satellites, although the US National Reconnaissance Office has recently completed a very intensive launch programme to place new

classified satellites in orbit. Information about the exact missions of these satellites have, however, not been released.

As a supplement to the above mentioned programmes, not least because demands for imagery have increased substantially, the US military makes use of increasing volumes of commercial satellite imagery though programmes such as NextView and EnhancedView. For optical imagery, the main suppliers are DigitalGlobe and GeoEye, while Canadian MacDonald Dettwiler has been the main suppliers of radar imagery. More recently, European InfoTerra and eGeos have also become radar imagery suppliers.

American commercial imagery is now available at resolutions as small as 40 cm (grey tones or pan-chromatic) and approximately 2 m in colour, to US government users. For the moment, the highest resolution available to commercial customers and for export is 50 cm. The quality significantly exceeds that of imagery available from other satellites such as Kompsat (South Korea), EROS (Israel) and the IRS/Cartosat satellites from India. Most likely, some other nations possess satellites with about the same image quality, e.g. Russia, China, France and Japan. Most other imaging satellites, e.g. from Indonesia, Nigeria and Thailand, produce imagery at resolutions of 3 m or lower.

Looking beyond the US and Russia, Canada has long been a leader in developing near real time operational radar satellite capabilities. Norway has exploited this, and radar images can be downlinked in Tromsø, for delivery to Norwegian government users within 30 minutes of acquisition by Radarsat-2. Standard high resolution imagery is available at 3 m resolution, although a spotlight mode has been defined to provide imagery at twice that resolution.

Germany has also invested in both a military radar satellite programme (SAR Lupe, 5 satellites) and a civil programme (TerraSAR-X, 2 satellites) with resolutions approaching 50 cm. Italy has deployed a constellation of 4 COSMO-Skymed (CSK) satellites, categorized as dual-use. The CSK satellites can operate in a military mode, likely producing 50 cm resolution imagery.

Tests carried out at FFI show that the radar images from the above mentioned satellites are of good quality, but require more specialized training to fully exploit compared to analyses of optical imagery. One of the definitive advantages, however, is the ability to do highly sensitive change detection, providing information on changes in both natural conditions (snow, ice, moisture, vegetation) as well as infrastructure (roads, buildings, harbour facilities etc.).

6.3.2 SIGINT

At present, only few nations have deployed SIGINT satellites in space: The US, Russia and France. China has probably deployed SIGINT payloads on satellites with other primary payloads.

There is, however, a development under way that could change this. Several countries and organizations, including Norway, are developing satellites for reception of maritime VHF radio signals form ships (The Automatic Identification System – AIS). This could result in the

development of similar satellites capable of intercepting signals from aircraft, general radio communications, and radar signals from marine navigation radars. The European Space Agency is currently undertaking studies of such possibilities with Norwegian, British and German participation.

6.3.3 METOC

The major contributors to the world's weather satellites are the US, Russia, Japan, and more recently, the international organisation EUMETSAT.

The US has long had an ambition to merge its military and civilian programmes for polar orbiting meteorological satellites. The Defense Meteorological Support Program (DMSP) and the NOAA Polar Operational Environmental Satellites (POES) were intended to merge into a common system, the National Polar-orbiting Operational Environmental Satellite System (NPOESS). NPOESS experienced very substantial budget and schedule problems. The programme was therefore terminated in February 2010. The replacements are known as the Defense Weather Satellite System and the Point Polar Satellite System. The latter is a joint programme between NOAA and NASA.

NASA also operates several other environment monitoring satellites, e.g. Aqua and Terra, that are used by the US military for detailed analyses and prediction of various conditions affecting military operations, such as sand storms in desert areas, under water visibility related to diver, mine and submarine detectability.

6.3.4 Perspectives

Satellite systems have become more responsive, provide more coverage, and hence are more useful in operational and even tactical contexts than just 3–5 years ago. This is a trend that is expected to continue as more satellites are launched.

Together with various units in the Norwegian Defence, FFI has experimented with commercial satellite images in order to evaluate new application areas and responsiveness.

Experience gained to date shows that response time of less than 24 hours from image request to delivery of imagery to a military analyst can be achieved. This is appropriate for operational planning, but not short enough for tactical use. The same can be said about imagery content and level of detail.

6.4 Satellite Communications

Most of today's available satellite communications capacity is provided by geostationary satellites orbiting approximately 36 000 km above the Earth, which is excellent for mid to low latitudes. For high latitudes, however, they provide little or no coverage. Russia became an early leader in using satellites in highly elliptical orbits inclined to provide long "dwell times" and good coverage over the Arctic. The orbital altitude of such satellites typically varies between 1000 km

and 39 000 km. The US has a somewhat similar system known as the Interim Polar System. Canada has initiated design studies for the same kind of SATCOM system.

In the US, military satellite based communications infrastructure was developed independently by the different military services, due to different operational requirements, resulting in a large number of different systems (see Figure 6.2). The Defense Satellite Communication System (DSCS) and Milstar have, however, provided a common backbone since the 1980s /90s. Following the Gulf War in the early 1990s the US military embarked on very large programmes to modernize its SATCOM infrastructure, e.g. the Wide Band Gap Filler System (WGS), Advanced Extremely High Frequency (AEHF) satellites, and ultimately the Transformational Satellite (TSAT) programme. Other narrower band systems with lower capacity have also been developed, e.g. in the UHF frequency band.

WGS is currently known as the Wide-band Global Satcom System [80], consisting of three satellites in orbit, with another three to be deployed from the end of 2011 and onwards. One of the latter will be Australian. WGS is considered to be the replacement for DSCS. A single satellite exceeds the total capacity of the older DSCS constellation.

Global Broadcast Service (GBS) [81] is, as implied by the name, a one-way, large bandwidth, broadcast system. It is used to broadcast information to US armed forces worldwide, including video, satellite imagery, and other large data files. The service is implemented through hosted payloads on other satellites including the WGS and UHF Follow-On (UFO) satellites.

AEHF [82] has started the deployment phase. The first launch was on 14th August 2010, and experienced some problems in achieving the intended orbit. Two launches are planned for 2011 and 2012.

The AEHF system will be the most advanced of the US military SATCOM systems. It will provide secure and robust communications at high bandwidths, while being resilient against jamming and effects of nuclear detonations. On a channel per channel basis, however, the communications capacity is somewhat lower than that of WG and GBS.

The Enhanced Polar System (EPS) is designed to be an extension to the AEHF programme, designed to deliver robust and secure communications at high latitudes. It will replace the Interim Polar System, currently providing military SATCOM at latitudes north of 65ºN, with hosted payloads deployed on satellites forming part of the US missile defence system SBIRS. The system will consist of two satellites in very elliptical orbits, providing continuous coverage of the Arctic.
TSAT was intended to be the military ”internet in the sky” (also known as the Global Information Grid), compared to current systems that can be compared to old style telephone networks with manually operated telephone exchanges. Like several other ambitious military satellite

programmes, TSAT has been terminated. The AEHF system will be enhanced instead, initially by deploying more satellites as described above.

The Mobile User Objective System (MUOS) [83] will operate at lower frequencies (UHF) than WGS and AEHF, and is slated to take over for the UFO programme. It will be enhanced to provide more reliable signal propagation in difficult conditions, such as those encountered in thick woods. The first satellite is schedule to be launched in December 2011.

In addition to developing its own systems, the US military makes use of commercial SATCOM services from entities such as Hughes, Intelsat, Hisdesat and Iridium. The latter system provides global coverage, albeit with low data transfer rates (4.8 kbps).

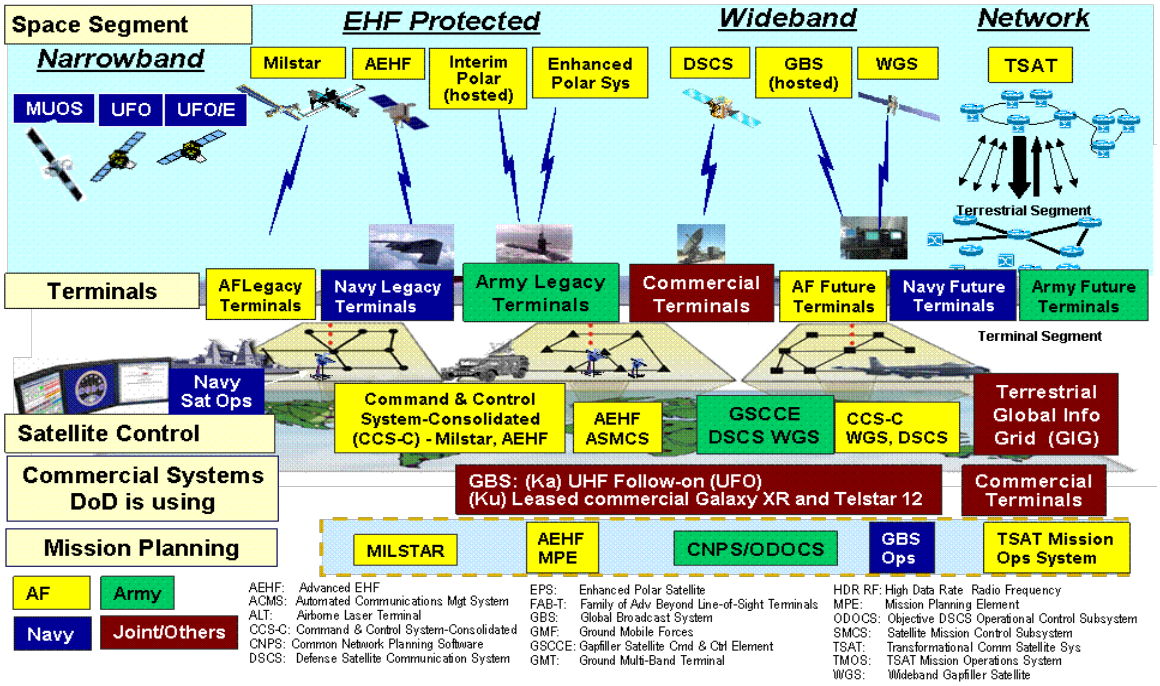

Figure 6.2 Overview of US military SATCOM systems (source: see [84]).

NATO and several European countries also use commercial providers of SATCOM services meeting military specifications, e.g. the UK and Germany. Astrium Services is one of the providers, with a service called Paradigm Secure. France and Italy have national military SATCOM programmes, Syracuse and Sicral respectively. France and Italy have also formed a joint, dual-use programme, Athena-Fidus.

Russia has developed a new generation of military communications satellites, known as Meridian. Meridian is slated to replace the aging Molniya satellites, deployed in highly elliptical orbits. The third Meridian satellite was launched in November 2010. The two first, however, have failed.

6.4.1 Perspectives

The capacity of military communications satellites has grown rapidly over the last 20 years, particularly in the US. The capacity to use the ever increasing bandwidth has increased at least as quickly, however, partly due to the evolution towards network-centric operations. This trend is expected to continue for the foreseeable future.

Communications at high latitudes, i.e. above 65° N, however, continue to lag, and only limited coverage is expected to be available at least for the next decade.

6.5 The US Military Space Programme

As mentioned in the previous sections, the US has a very large military space programme. In this section we review some of the elements beyond the aforementioned GPS, surveillance and communications satellite programmes.

Access to space is extremely important for the US military operational capability. The US recently published a National Security Space Strategy [85], confirming this and outlining some of the challenges that face the US and other space faring nations. In recent years, the US has had a focus on securing access to space and unhindered use of space (Space Superiority), protection of space assets (Counterspace) and Space Situational Awareness (Space Surveillance and Space Reconnaissance). The recent Space Security Strategy emphasizes that the number of objects orbiting the Earth is increasing at an accelerating rate, and that there is a need for international cooperation to ensure safe and secure operations in space. The amount of space debris is of concern, as well as the spreading capability for attacking objects in space from the ground, as illustrated by a Chinese test firing that destroyed an old weather satellite, spreading thousands of pieces of debris in a commonly used low Earth orbit.

The above mentioned concerns underlie US investments in programmes to increase Space Situational Awareness (SSA), primarily managed by the Space Superiority Systems Wing (SysW) at Los Angeles Air Force Base. Monitoring of outer space is done using both ground-based and space based sensors to detect and track objects, as well as to monitor the radiation and solar wind environment around the Earth (Space Weather). The North American Aerospace Defense Command (NORAD) tracks around 19.000–20.000 objects orbiting the Earth, and frequently provides warnings of possible close encounters between different satellites and other objects. This is vital to operations of both manned space craft and unmanned satellites. Space weather services are mainly provided in the civilian domain.

The US Air Force continues to develop an unmanned re-usable spacecraft, Boeing X-37B [16]. Due to Wikipedia the first mission (OTV-1) was launched on 22 April 2010, returning to Earth on 3 December 2010. The second mission was launched a year after, lasting for approximately two moths, and the third mission was launched on 11 December 2012. However, details are classified beyond statements about testing of new technologies in areas such as manoeuvring in space.

Figure 6.3 USAF's X-37B completed its first mission in space 3 December 2010. (source: see [14]).

Finally, we mention the US programme for Operationally Responsive Space (ORS). The programme is primarily intended to establish new military space capabilities on short notice. Russia demonstrated this kind of responsiveness by launching two satellites in a matter of days during the conflict with Georgia in 2008.

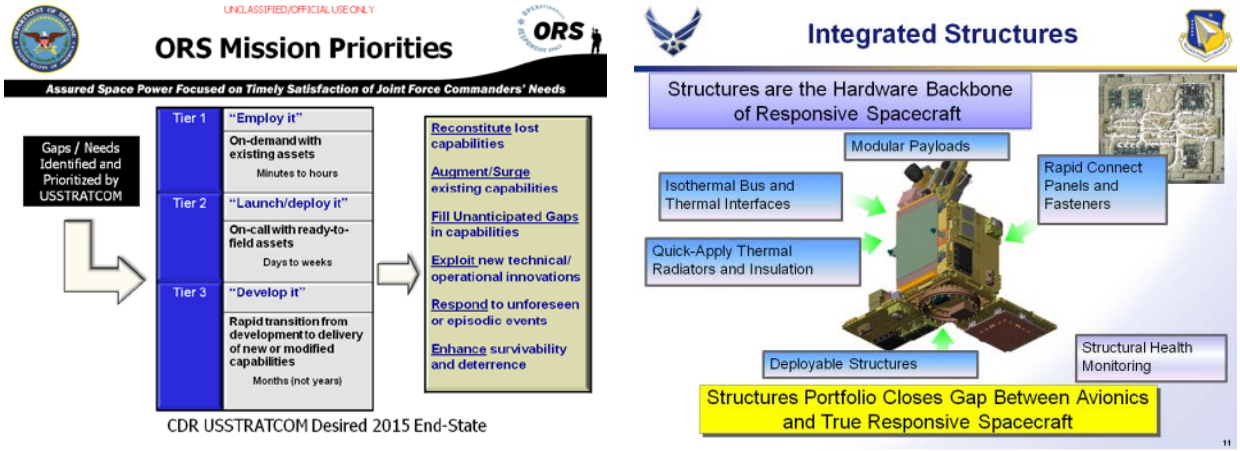

Figure 6.4 Operationally Responsive Space. Left: Overarching principles for implementation (source: see [10]). Right: Illustration of "off the shelf" hardware for rapid response (source: see [11]).

ORS has a three-tiered approach for responsiveness. Following the statement of a need from US Strategic Command (Stratcom), a response team is established to determine if, for example, a surveillance requirement can be met using commercial imagery from existing satellites. If not, a

new satellite is needed on orbit, so a mission has to be designed on short notice, including building a satellite from “Plug and play” components. ORS is developing mission design kits, as well as plug-and-play satellite components built around a new set of standards. Such components can be sub-systems or smaller components, e.g. for avionics, telemetry, power generation, as well as sensors. The ORS concept also involves rapid set-up of a ground segment, as well as provision of a launch vehicle and launch range. The initial target is a response time of around two weeks from requirement statement to launch.

The third tier of ORS addresses cases where more advanced systems needs to be developed. A goal of ORS is to develop alternative approaches to new missions to avoid mistakes that were made in the large and cancelled programmes mentioned in previous sections. This can in part be done by using a micro space approach with numerous small satellites will a limited range of capabilities.

6.6 Developments in Asia

China’s growing space programme has also led to an increased focus on space in neighbouring Asian countries. This response has been enhanced further by developments in North Korea, particularly in India, South Korea and Japan. North Korea is known to be developing long distance missiles capable of carrying nuclear warheads. They have also established programmes for building military reconnaissance and communications satellites.

Iran has also declared its intentions to become a space power, working with countries such as North Korea and Pakistan. Iran carried out its first launch of a satellite into orbit in 2009. This indicates that Iran also has a ballistic and inter-continental missile launch capability, which is of considerable international concern.

China has demonstrated the use of anti-satellite weapons through a test of demolishing an old satellite on orbit. Officially, China supports the United Nations initiative to prevent weaponisation of space. However, high ranking officials have said publicly that militarization of space is unavoidable.

India has recently developed a military space doctrine, Defense Space Vision 2020. The doctrine addresses programmes to acquire surveillance and reconnaissance satellites, military communications satellites and a national constellation of navigation satellites. India has also established an Integrated Space Cell for coordination of Indian military space requirements with its civil counterpart, the Indian Space Research organisation (ISRO).

7 CBRN Threats and CBRN Protection

This chapter will discuss the development of the threat posed by chemical (C), biological (B), radiological (R) and nuclear (N) weapons and the protection against such weapons.

7.1 General Trends

The proliferation and military use of nuclear, biological and chemical weapons is subject to a number of international agreements. With a few exceptions, the agreement of non-use of chemical weapons in war has been respected after WWI. Nuclear weapons have not been used after Hiroshima and Nagasaki in 1945.

New asymmetric threat scenarios have, however, over the last decade led to increased attention to the danger posed by CBRN weapons against NATO personnel and civilians. This has renewed the focus on non-proliferation work and on technology for protection of people, vehicles and buildings. It is also the fear of long range delivery of Weapons of Mass Destruction that is the background for the US Missile Defense Program. We will in this chapter primarily discuss detection of, and protection against biological and chemical weapons, but also the development trends for nuclear and radiological weapons will be addressed.

There exists, in general, much sensor technology for in-situ detection and to a certain degree identification of such threat materials. An important technological trend seems to be to connect such sensor systems in networks (aiming at complete integration in command and control systems). Another priority area internationally seems to be stand-off detection (by using e.g. laser) in order to monitor a larger area without needing to deploy in-situ sensors everywhere.

Over the last 10 years, the field of biology has gone through what is often referred to as “bio-revolution” and is characterized by:

- Human genes have been mapped.
- Human brain structures and functions are better understood.
- Cellular mechanisms are being studied in detail.
- DNA-sequencing of the human genome (the Human Genome Project).
- DNA-sequencing of bacterial and viral genomes.

A consequence of this is expected to be synergies between biology, information technology and micro-/ nanotechnology. This area is developing slower than was expected around the turn of the millennium and the military implications from this increased insight are difficult to foresee today.

Detection of biological threat agents can be time consuming because of the need to grow bacteria for a confirmed identification. New techniques based on gene technology are being developed. Combined with micro-technology, this will probably deliver small chips that quickly and with high sensitivity will be able to detect microorganisms that are used as biological threat agents.

Research efforts within nanotechnology may in the long term lead to substantial consequences for the production of protective clothing. Future protective clothing might contain a chip with reactive nano-particles that will both detect and destruct biological threat agents.

A consequence of the human gene mapping is that someone in the future could build biological threat agents that attack only certain parts of a population, develop microbes that are resistant to medical countermeasures, including antibiotics, or develop much more aggressive microbes with new properties.

7.2 Nuclear Weapons

Nuclear weapons – sometimes referred to as the only real weapons of mass destruction – are the most destructive of all weapons. The enormous energy released comes from a very large number of atomic nuclei undergoing transformations, either fission (splitting of uranium or plutonium nuclei) or fusion (merging of special hydrogen nuclei into helium).

The use of nuclear weapons is not forbidden by international law. It is widely acknowledged, however, that a world with a large number of nuclear weapons located in a large number of states is not wanted. Therefore, almost all nations in the world have signed and ratified the Treaty on the Non-Proliferation of Nuclear Weapons (commonly known as the Non-Proliferation Treaty or just the NPT). The main points of the treaty, which entered into force in 1970, are:

- Temporarily acknowledges the five states which had tested nuclear weapons before 1967 (the United States, the Soviet Union (now Russia), the United Kingdom, France and China) as nuclear weapons states;
- Commits all other Member States to remain non-nuclear weapons states;
- Prohibits the transfer of nuclear weapons from a nuclear weapons state to a non-nuclear weapons state, as well as any assistance in order to help a non-nuclear weapons state acquire nuclear weapons;
- Prohibits the acquisition or the development of nuclear weapons by any non-nuclear weapons state and also prohibits them from seeking knowledge about the manufacture of nuclear weapons from other states;
- Grants all Member States an inalienable right to the peaceful use of nuclear technology (such as nuclear power, nuclear medicine etc.);
- Commits all states to negotiate in good faith on measures eventually leading to complete nuclear disarmament.

India, Israel and Pakistan never signed the NPT, and North Korea has withdrawn from it.

As of 2010, the nuclear weapons states possess more than 20 000 nuclear warheads, about 95 % of them in the United States or Russia. A few other states have become de facto nuclear weapons states in the years since the NPT entered into force, however. India (1974 and 1998), Pakistan (1998) and North Korea (2006 and 2009) have actually carried out nuclear weapons tests. South Africa has admitted to having developed and built a few nuclear bombs in the 1980s, but they

were later decommissioned, and in 1991 South Africa became a member of the NPT as a non-nuclear weapons state [86]. Also Israel is widely considered a de factor nuclear weapons state, but has never admitted to the possession of nuclear weapons. Instead, it has adopted a policy of opacity under which its possible possession of nuclear weapons is intentionally kept unclear [87]. Israel and the de facto nuclear weapons states have at most a few hundred nuclear warheads altogether. Finally, it should be mentioned that after the break-up of the Soviet Union in the early 1990s, the newly independent states of Belarus, Kazakhstan and Ukraine for a while held a large number of formerly Soviet nuclear weapons. By the end of 1996, all these weapons had all been transferred to Russia which had inherited the international treaty status of the former Soviet Union.

The existence of the NPT has most likely prevented a substantial number of states from "going nuclear." Not because they were incapable of developing their own nuclear weapons, but because they saw no need for them. To maintain this situation in the future, it is therefore important not to increase the attractiveness of nuclear weapons or the perceived "need" for any such. There are two important paths toward increased attractiveness: one would be an increased emphasis on the usefulness of nuclear weapons among the nuclear weapons states, and the other an increase in the number of more or less "accepted" de facto nuclear weapons states.

China is the only acknowledged nuclear weapons state with a no-first-use-policy (that is, nuclear weapons will only be used in retaliation of a nuclear attack), but the general importance of nuclear weapons among the nuclear weapons states appears to be somewhat lower in recent years compared to the early 2000s. Even though none of these states are deemphasizing the strategic usefulness of the weapons, the United States in particular now promotes the vision of a world free of nuclear weapons, and the 2010 Nuclear Posture Review declares a reduced role of US nuclear weapons. The report also contains a "negative security assurance" stating that the United States will not use or threaten to use nuclear weapons against non-nuclear weapons states that are party to the NPT and in compliance with their nuclear non-proliferation obligations. These are all good moves in reducing the interest in nuclear weapons among the non-nuclear weapons states.

The picture is not so bright when it comes to new de facto nuclear weapons states and the interest in nuclear weapons in various corners of the world. India, Pakistan and North Korea have never experienced any serious consequences of their nuclear testing except for loud criticism and half-hearted trade bans. On the contrary, these countries appear to be taken maybe more seriously now than before, and this is of course a dangerous message to any other aspiring nuclear weapons states.

So far, nuclear weapons have never been used, even as a threat, by any non-state actors. This could change as basic knowledge about these weapons is fairly widespread. The likelihood of a nuclear terrorist attack is small, but one should keep in mind that even a "small" nuclear explosion will be much more powerful than any other terrorist attack that the world has seen. It is generally acknowledged that the biggest obstacle to making a nuclear weapon is to get hold of a sufficient quantity of suitable uranium or plutonium. To produce such materials from scratch is

most likely beyond reach for any organization without governmental support. This underlines the importance also in the future of carefully guarding all fissile materials and of an international safeguards regime. The latter is the task of the International Atomic Energy Agency (IAEA).

7.3 Radiological Weapons

The dispersion of radioactive materials serves no military purpose, but is often mentioned as a possible means for terrorists. Such methods will hardly lead to situations where people become acutely ill from radiation, but they can cause high levels of anxiety and damage over time. The dispersion of radioactive materials is therefore referred to as a “weapon of mass disruption” and not weapon of mass destruction. Another term for such dispersion of radioactive materials is “radiological weapon”.

Several fundamentally different methods to disperse radioactive materials can be envisaged. The most serious would be an attack on a nuclear facility such as a nuclear power plant, a reprocessing plant for spent nuclear fuel or a storage facility for such fuel. The purpose may be to destroy the plant in order to disperse radioactivity, e.g. by bringing down an aircraft at the facility or by blowing it up. The purpose may also be to take over control of the plant as a means for political blackmail. A third motive for attacking a nuclear facility may be to get hold of radioactive material in order to disperse it or threaten to disperse it.

Another method to disperse radioactive materials is to create a so-called “dirty bomb” (Radiological Dispersion Device – RDD). A dirty bomb is a weapon that disperses radioactive material over an area by using conventional explosives (a conventional bomb). This is not a nuclear weapon because nuclear reactions (fission and fusion) do not occur. The consequences are not as dramatic as with a nuclear explosion. Dirty bombs will still have a major terror effect, however, with deaths (from the conventional explosives), great fear, chaos, difficult cleanup operation and substantial financial costs. No terrorists have until now used this method, but many fear that it may be used in the future. Radioactive material can also be dispersed in ways other than by conventional explosions.

Until now, society has primarily focused on protecting individuals against radioactivity. In the future, we assume that the focus on also to "protect the radioactivity against people" becomes greater. In the future, it will be important that institutions that are in possession of radioactive material or fissile material (nuclear materials), watch it well to prevent theft. It is expected that detectors that can warn of an abnormally high radiation, will be deployed in places that might be targets of terrorist acts.

7.4 Chemical Weapons and Threat Agents

7.4.1 Detection – Sensors

The production of and protective measures against chemical weapons has a long history. Stockpiles of such chemical threat agents do still exist in many countries. The known stockpiles

are, however, declared and subject to inspections and the requirement to be destroyed in accordance with the Chemical Weapons Convention (CWC). The problem is that destruction in safe and secure circumstances is demanding in terms of time and resources. This means that the stockpiles in several countries will continue to exist for at least 10 years and will thus constitute a continuing risk.

There are several chemical agents than can be characterized as threat agents and, based on developments within the organic and biotechnological industry, their number is increasing as well as their accessibility and the possibility to produce them. The developments of medicines that are designed to cause effects in the nervous system are particularly important. Combined with a better understanding of the structure and functions of the brain, mapping of cellular processes and the human genes, these medicines contribute to an increase in the number of possible threat agents. Another cause for concern is the allegation that research and development of new threat agents has been going on in Russia/USSR since the seventies. It has been claimed that these agents have qualities that make them harder to detect, harder to protect against with traditional protective measures and that today's medical treatment regime is not sufficient. These chemicals have a higher degree of toxicity than the known nerve agents and have structures that are not covered by CWC's lists of chemicals to be declared. The disclosure of some structures of such chemical compounds might make them easier to obtain for groups or states that want to possess such weapons. This means a changed threat that increases the need for development of new technology for protection, both physical and medical.

Figure 7.1 CATSS (Chemical, Atomic and Toxic compounds Surveillance System) [88] is an example of how an automatic, network based surveillance system for nuclear radiation, chemical threat agents and toxic industrial chemicals can be built based on existing and available sensors that are put together as required for the operation or situation (photo: FFI).

Presently, a number of stationary C-detectors are on the market. They are based on different principles such as: ion mobility spectrometry, surface acoustic wave, etc. The development is definitely moving in the direction of automatic and network-based systems for stand-off/in situ detection that combines several different sensors. These systems are suited for force protection both in peace support operations and in a conventional war. A long term trend is that the C-detectors are miniaturized and equipped with radio transmitters in order to deploy them over larger areas.

Stand-off detection of chemical threat agents is another promising area [89], particularly for detection of threat agents in the air. Chemical threat agents in the form of steam have an absorption band in the IR range, and both active and passive IR techniques have a potential for detection. A couple of passive IR detection systems are already on the market. An interesting idea for the longer term is to build a capability for stand-off detection of chemical threat agents in to the soldier's ordinary night vision goggles or aiming devices.

Figure 7.2 Passive Stand-off IR detector Bruker RAPID, range 5 km (photo: FFI).

Chemical threat agents in the form of liquids or steam can inflict significant damage to unprotected people and may cause death even in small concentrations. Fluids contaminating equipment, buildings or terrain could transfer to people or could emit dangerous fumes. Liquids that contaminate the skin must be removed immediately. Ever since chemical weapons were used for the first time, the development and use of different types of detergents to remove and, if possible, break down the chemical substance has been ongoing. Many chemical weapons are, however, difficult to remove, mainly because of the addition of special substances that make cleaning difficult. The detergents in use today are often very powerful and could harm people, sensitive equipment and the environment. In many countries, therefore, intensive work is ongoing to develop better quick-acting systems that are less harmful. Future R&D efforts should include development of cleaning equipment adapted to smaller, mobile devices. This will make the units more self-sufficient in case of contamination and thereby more quickly enable restoration of operating status.

Toxic industrial chemicals are another threat which has been actualized through international operations (e.g. Kosovo). Many of these chemicals are stored in significant amounts in areas of unrest and the labelling of containers and maintenance of the warehouses is often poor. This implies both a risk of exposure by accident, and that irregular combatants or terrorists can acquire and make use of such threat substances. Detection capacity for industrial chemicals is currently included in newly developed and improved C-detectors. The challenge now is to find the most relevant substances and to prevent the expansion in the number of threat substances causing a large number of false alarms. Manufacturers of detectors are to some extent in the process of doing this, but there is still work to be done.

7.4.2 Respirators

The most important protection against chemical threat agents is the respirator. It protects both the respiratory system and the eyes. Further development will go in the direction of more flexible systems that are more comfortable in use and provide better protection against any type of threat agents. In this context, an important element is research and development with respect to filter technology to increase capacity and reduce breathing resistance. Several developers are working on positive-pressure systems. A newer solution is systems where the helmet and the respiratory protection are integrated. These systems will also be able to provide an enhanced protection against biological weapons/threat agents, as well as providing protection against chemical threat agents with higher toxicity.

New threat agents will increase the need for improved filter technology, but also the need for better fit and reduced leakage, i.e. better seal between skin and mask.

Figure 7.3 Field testing of respirators (photo: FFI).

7.4.3 Protective Clothing

There are three important trends concerning the future's protective clothing. One trend is to integrate the protective concept into the soldier's standard clothing, where for example a regular uniform utilising membrane textiles constitutes the first protective layer. Two things are achieved by this solution: Firstly, the soldier wears a uniform that he already knows well concerning pockets and zippers. Secondly, the protective clothing becomes less heavy. As described in Section 2.1, FFI has developed the future Norwegian soldier system, NORMANS, in this way, where a normal outer layer made in membrane textiles with repellent characteristics is adapted to an inner lining with activated carbon with absorbing characteristics. The outer uniform also has a hood that fits the respirator. An extreme version of this concept, based on a regular uniform, comes from the Institute for Soldier Nanotechnologies (ISN) that was founded in 2002 at the Massachusetts Institute of Technology (MIT). They suggest that the soldier could take a" protective shower" in full uniform before entering an area with B/C risk. It is hard to asses when such revolutionary technology will be of practical use.

The second trend, partly associated with the first, is to construct protective clothing that produces lower heat stress. This can be done by the use of lighter and smarter textiles. In order to reduce the heat stress, it is important that perspiration is allowed to escape through the textiles so that the soldier does not overheat. Unfortunately, textiles that allow water vapour to pass through will often also allow chemical agents to do the same. This problem is usually solved by adding a second layer that absorbs the agents. There is, however, ongoing research on so called selective membranes that will allow water vapour to pass through, but not chemical agents. These selective membranes can be laminated into a textile and the need for an absorbing layer thereby eliminated. This will reduce both weight and heat stress. Such textiles already exist, but are not yet sufficiently tested. The potential for improvements of such membranes, using nano-technology to enable effective protection against chemical agents while at the same time allow the venting of water, has been identified.

The third trend is based on a more differentiated use of protective clothing and is associated with developments on the sensor side with regard to safe detection of threat agents combined with effective warning of such threats. This offers the opportunity to give the protective clothing vents that could be open when the threat is low. If the soldier is alerted via his sensor or communication system that there is battle gas in the area, he would quickly be able to don his respirator and close the vents. Looking further into the future, the combination of information technology and smart textiles could offer new possibilities for protection that are aimed at specific agents. It could, for example, be envisioned a warning system directly coupled to advanced textiles that could change their protective characteristics in order to respond optimally to the actual threat.

Depending on the characteristics and functional mechanisms of future threat agents, e.g. as "dust particles", tighter textiles, possibly in the form of membranes, could make up essential parts of future protective clothing.

Figure 7.4 NORMANS' integrated protection in two layers. Normal outer wear with membrane textiles and a lining with absorbing activated carbon (photo: FFI).

7.4.4 Medical Protection against Chemical Threat Agents

The main challenges in improving medical protection against chemical threat agents are to develop more effective protection and treatment of exposed persons. The current use of medical prophylaxis increases protection against certain nerve agents, but it would be beneficial if one could reduce the use of prophylaxis and rather implement better medical treatment. Then we would avoid unnecessary use of medicine. The need for improvements in medical treatment includes both treatment of military persons and civilians, having been exposed to nerve agents, vesicant agents or toxic weapons.

There are still few effective medical remedies against most of the chemical threat agents except for some of the nerve agents [90]. However, these remedies are far from effective enough and the measures must be employed immediately after exposure. The challenge is to find measures that, in order to limit development of permanent injuries in the nervous system could be employed some time after the acute phase following exposure to nerve agents. This is relevant both for military use and to treat civilians in a terror scenario. Even if, through the last 50–100 years much research has been carried out to understand the injuries caused by exposure to vesicant agents like mustard gas, no effective remedies against them has been developed. The understanding of cellular processes and mechanisms will be vital pillars for developing such countermeasures into practical and useful remedies.

Toxins are a large and broad-spectrum group of threat agents. Weapons based on toxins in most cases target the nervous system, but also many of the body's other cells might be damaged. It is therefore not sufficient to develop only one countermeasure strategy. It is vital to have a broad knowledge about the different threat agents' mechanisms in order to develop measures that are effective against current and potential new toxins. These toxins can be synthesized and possibly targeted against certain areas both in the nervous system and against other cells in the body.

7.5 Biological Weapons and Threat Agents

Biological threat agents include living microorganisms (bacteria, rickettsias, viruses and fungi) and toxins that can cause injury, disease or death to human beings, animals or plants. A biological weapon is defined as a biological threat agent and its delivery system (bomb, missile, spray tanks). In this section we focus on detection of the microorganisms (not the delivery system).

Bio-terrorism has received increasing attention from public health officials and experts in infection medicine. The anthrax episodes in the US in the fall of 2001 and the increased focus in the US on Homeland Defense lead to the establishment of The Office of Homeland Security and a vigorous escalation of R&D programmes within defence against biological threat agents. Norway has also increased focus on emergency planning against biological threat agent attacks [91]. Such emergency planning has to include detection and physical and medical protection against these microorganisms. The new threat and risk situation caused a renewed significance of civil emergency and a necessary shift in the emphasis towards a closer civil-military co-operation. Technology advances includes deployable equipment for preliminary identification of threat agents both for civil and military use.

There exists no single instrument today that both detects and identifies biological threat agents in-situ. Comprehensive R&D efforts are necessary and are ongoing globally to realize such a system. Concerning stand-off detection for early warning of incoming aerosol clouds, LIDAR (laser-radar) has been considered a promising technique [92]. LIDAR detects only fluorescent bio-molecules and will therefore be unable to identify which microorganism is present in the cloud. For the time being LIDAR seems to work effectively at night and on cloudy days. Some optimizations seem to be necessary to make LIDAR work in sunlight and on distances larger than 5 km. The development of point detection equipment for biological threat agents is ongoing. The main challenge is to reduce the false alarm rate and distinguish between naturally occurring and deliberately released pathogens. Further improvement is needed and will most likely imply a combination of different methods/technologies.

It is essential to be able to quickly identify the employed biological threat agent. Several complementary methods have to be used to obtain positive identification: One that is presently in use, is the cultivation of bacteria in a selective growth medium. This method is often time-consuming and requires the presence of viable cells, but is an essential method to obtain bacterial isolates for further investigation, for example to identify antibiotics resistance. Immunoassays that are based on specific antigen reactions are also used for identification, but the sensitivity may vary and could result in false results. Several companies have developed test strips that are based

on immunological reactions for a rapid detection of biological threat agents. Molecular-based techniques using genetic markers for detection are today the fastest method, but these techniques do not distinguish between dead and living micro organisms. The techniques are based on the fact that the DNA sequence of the microorganism to be identified is known. The Institute for Genomic Research in the US has initiated a programme for sequencing bacterial genomes of biological threat agents causing among others anthrax, plague and botulism. Future identification equipment will probably include genetic techniques where certain regions of the microorganism's genes are used as identification markers. This can be used in combination with a trigger (detection/warning) system before the identification analysis is initiated. Mass Spectroscopy (MALDI-TOF) has demonstrated the ability to quickly classify bacteria. This method is being developed further to be able to achieve a quick detection followed by a more exact genetic identification analysis. A part of this process involves building a database of fingerprints of the various biological agents.

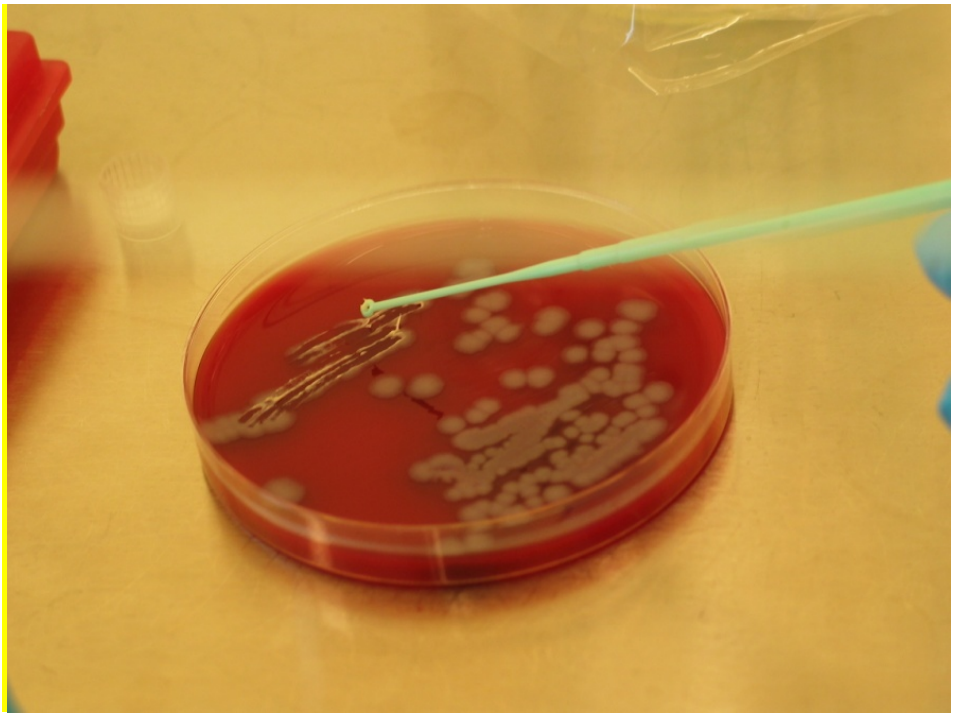

Figure 7.5 Colonies of anthrax bacteria on blood agar media (photo: FFI).

Polymerase Chain Reaction (PCR, Figure 7.6) is an essential molecular biological tool for identification of biological threat agents and is needed for genotypes of bacteria. A small PCR-instrument (weight ca. 4 kg) for detection of some biological threat agents was developed by Idaho Technologies for field use. This instrument was recently further developed to detect infectious airborne microorganisms (for example influenza viruses and legionellae). Intensive work is ongoing on the development of microarray chips where the DNA of the biological threat agent is printed on a glass surface in the chip. DNA from the unknown sample is isolated and hybridized against DNA on the glass surface. Positive signals are achieved using fluorescent reactions. The microarray technique is a sensitive method, but requires a comprehensive sample processing step prior to the analysis.

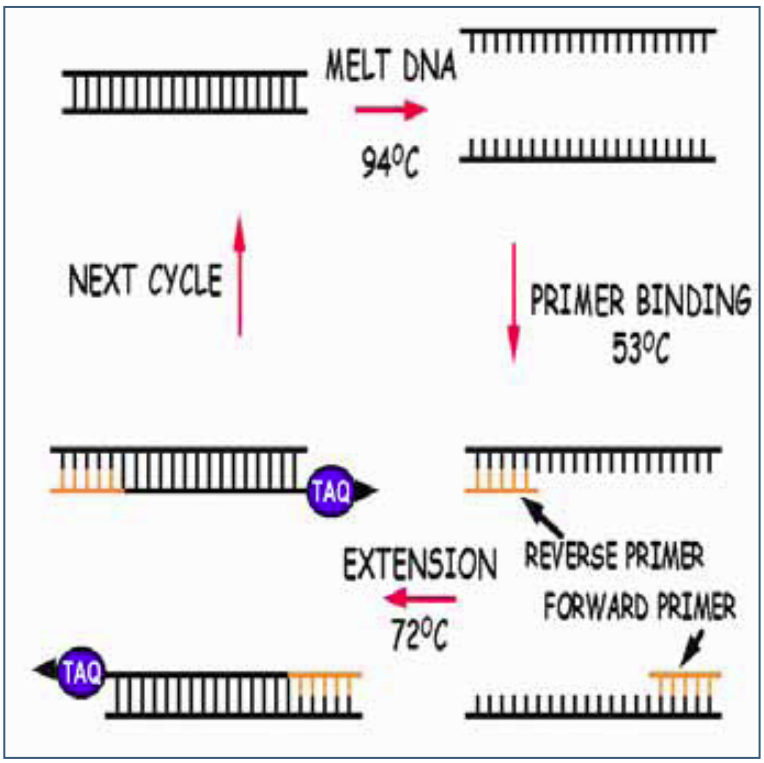

Figure 7.6 Polymerase Chain Reaction (PCR) is an essential molecular biological tool for identification of biological threat agents (source: Roche Diagnostics).

The microorganisms that can aerosolise represent a threat to the soldier, because this way of infection is considered the most effective. The entire category A threat substances listed at CDC can aerosolise, and they cause the highest mortality and infection rate. It is therefore essential to obtain good air samples if contamination by infectious micro-organisms is suspected. Equipment for sampling of microorganisms (bacteria, fungi, viruses) from the air has been developed and is commercially available [93]. FFI and others have tested several air sample collectors. FFI has also ongoing studies of microorganisms in the air in different environments where the established techniques can be used to identify the different microorganisms [94].

Figure 7.7 RAZOR is a handheld PCR instrument developed by Idaho Technologies (photo: FFI).

For all the molecular biological techniques, comprehensive sample processing is important. Time, resources and often optimisation is required for such techniques for different test matrixes (environment and clinical tests). An integrated system with stand-off detection, point detection, sample collection and genetic identification does not exist today, but intense effort is directed towards development of each of these modules, both nationally and internationally. Completely automated equipment, however, will probably not be on the market for a number of years. The most promising solution seems to be a combination of different techniques and modules, e.g. by use of micro- and nanotechnology together with genetic identification techniques where a trigger system is in place to initiate the identification analysis. Operational systems for detection and identification of biological threat agents within half an hour is regarded as ambitious, but may be feasible in the longer term (Figure 7.8).

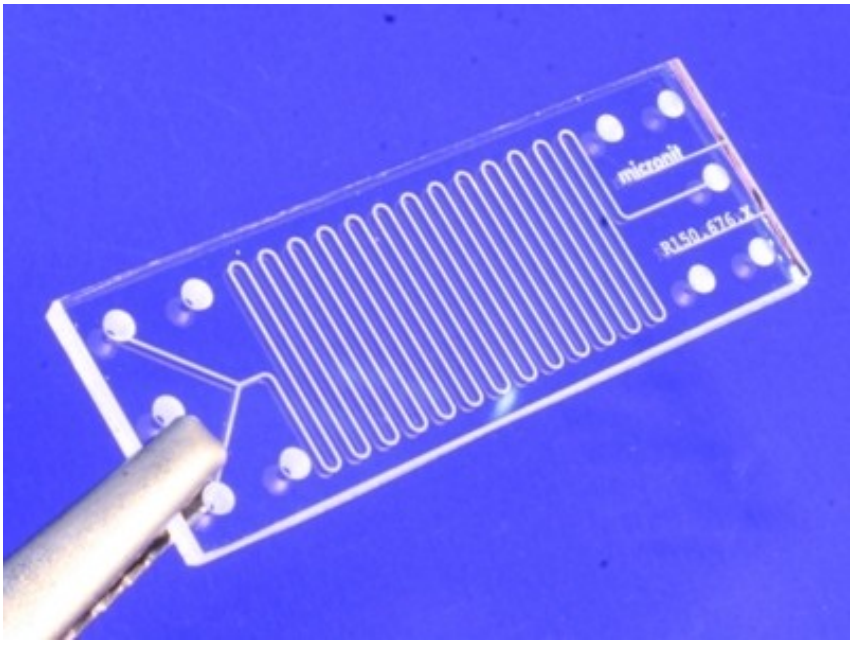

Figure 7.8 The combination of gene technology and micro- / nanotechnology could by 2020 give very compact systems that can quickly confirm the presence of different types of biological threat agents (photo: Wikimedia Commons).

8 Information Operations and Electronic Warfare

8.1 Electronic Warfare

The purpose of Electronic Warfare (EW) is domination and exploitation of the electromagnetic domain. EW as a warfare discipline has a long history and is an information-related core capability in achieving information superiority. EW should not be confused with Information Operations (IO) which is an integrating and coordinating staff function. The US definition of IO has recently been revised by the Defense Secretary Robert Gates in a memorandum from the US DoD [95]. The new US definition of IO reads:

> "The integrated employments during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own".

In this integrated employment of capabilities, EW plays a major role in most military operations. The most recent NATO definition of EW is given in the organisation's EW policy document [96]:

> "Electronic Warfare is military action that exploits Electromagnetic (EM) energy to provide situational awareness and achieve offensive and defensive effects. EW, the conduct of Electromagnetic Operations (EMO), is warfare in the Electromagnetic Environment (EME). It comprises:
>
> - Electronic Attack (EA) – use of EM energy for offensive purposes[5].
> - Electronic Defence (ED) – use of EM energy to provide protection and to ensure effective friendly use of the EM spectrum.
> - Electronic Surveillance (ES) – use of EM energy to provide situational awareness and intelligence[6]."

8.2 Electronic Attack

Electronic Attack (EA) is in the new definition of the application of EM energy for offensive purposes and includes directed energy weapons, high power microwave and EM pulse as well as RF devices. This section will not cover the entire range of EA effects described in the definition but focus on EA applied to radar, communications and navigation warfare.

8.2.1 Radar EA

Radar EA is in its nature a response to the radar capability of a potential adversary. Previously, the hardware and technology needed to effectively jam radars were so specific to the given task that in several areas it was actually driving the technology development. This was true for e.g. wide band high power amplifiers or wide band antennas capable of handling high transmit power.

[5] EA includes Directed Energy Weapons, High Power Microwave and EM Pulse as well as RF devices.
[6] ED includes protection of forces, areas and platforms.

Also, the jamming systems were tailored to a specific task and radar threat. They were not easily reprogrammed or even reconfigured. Today this is changing. Modern jammers can be based on a digital core which is more or less totally reprogrammable. When a number of such cores are connected to a wide band antenna system, preferably a phased array, radar jamming becomes less of a high power radar blinding system and more of a sophisticated deception device. The transition from analogue noise to digital deception is the main overall trend in radar jamming. The programmability and flexibility even open up the possibility of using the same hardware for multiple tasks, such as radar, ESM, radar jammer and communications jammer.

Radar EA intended to protect other platforms than the one carrying the jammer, is called support jamming (SJ). Today (2011), only US has this capability operationally in the EA-6B Prowler fleet, consisting of about 120 manned aircraft. The EA-6B can detect, locate and jam enemy surveillance radar and communication systems. It has been a very important contributor to establishing air control and supporting ground attack missions in the conflicts in Kosovo and Iraq. EA-6B is a stand-off jammer (SOJ) or escort jammer (ESJ) which can employ noise jamming to make detection of air targets and guidance of missiles difficult for air defence systems. EA-6B is currently being replaced by EA-18G Growler shown in Figure 8.1 [97]. So far, this replacement is primarily a platform upgrade as the EA-18G will operate the same jamming system as the EA-6B, the ALQ-99. A development programme is, however, underway in the US, named Next Generation Jammer (NGJ), to develop a replacement system for the ALQ-99 [98]. This new system will probably be a scalable system which can also be operated from other platforms than the EF-18G. NGJ is currently in the Technology Maturation Phase.

Figure 8.1 EA-18G Growler (photo: Boeing).

The NGJ will most probably be designed around a Digital RF Memory (DRFM) core. This makes the system capable of producing highly programmable jamming signals which may be based on stored replicas of the radar signal from the radar which is currently being engaged. This makes the jamming much more efficient in terms of transmit power required for a certain effect on the

radar (when compared to conventional noise). The reduced power requirement makes modern wide band phased arrays a technically feasible antenna option. The use of phased arrays allows fast beam switching and multi-threat handling.

Manned support jammers are usually operated at stand-off ranges, i.e. outside the engagement zone of the weapon system being attacked. Modern radars are becoming increasingly robust against stand-off jamming. Additionally, the protection provided by a certain jamming signal is often much more robust for platforms at longer range from the radar than the jammer. This calls for SJs operating inside the engagement zone of the weapon system, usually called stand-in jammers (SIJ) [99]. A stand-in jammer operates in a high threat area, and it is therefore usually a UAV. Operating a highly power efficient DRFM jammer close to a radar to protect aircraft of increasingly lower detectability through reduced radar cross section (RCS) requires even less transmit power. This, combined with the development towards miniaturized digital electronics (driven by the civilian market), makes it possible to develop affordable, small and capable radar jamming systems for UAVs. One example of such a UAV is the jammer equipped version of the Miniature Air Launched Decoy (MALD-J) which is in the engineering, manufacturing and development (EMD) phase and expected to reach operational status in 2012 [100]. MALD-J can be operated from fighter aircraft. It is shown in Figure 8.2.

Figure 8.2 Miniature Air Launched Decoy – MALD (source: Raytheon).

8.2.2 Communications EA

Communications EA refers to active electronic means of denying an adversary access to his communicated information, or also the degrading or invalidating of this information. While the traditional EA method has been brute-force broadband barrage jammers, performing physical-layer denial-of-access over a broad frequency area while using high amounts of energy, the current trend is towards more energy-efficient and agile EA techniques, as will be reviewed below.

The performance objectives of EA are to have high levels of disruption of communications while having high energy efficiency and a low probability that the EA is detected or tracked by the adversary [101]. The ongoing evolution of communication equipment into very flexible software-defined and self-adapting devices, leading to larger flexibility and rapid variability in waveforms, will challenge EA systems, and require equally flexible and rapid-reacting EA systems to be developed in the coming years.

Wide-band Jammers

The current wideband or barrage jammers spread the jamming energy typically over broad spectrum intervals. While wasteful in terms of jamming energy, these are expected to be relevant also in the near-term future, e.g. when the properties of the communication system of the targeted adversary are unknown. They are still relevant in the case of self-protection jammers, in cases where there is limited information about the type of communication signals to target. Another application is the denial of communication in confined, small areas.

Smarter EA

The aim of smarter EA is to achieve better levels of disruption of communications at lower energy levels, by exploiting information about the communication system of the adversary. Modern communication waveform standards typically have intrinsic vulnerabilities, both on the physical layer of the waveform and on higher layers, which can be exploited by smarter forms of EA. Smart EA may directly attack the physical layer waveform, with a jamming signal targeted at the specific waveform, e.g. using knowledge as to what level of error-correction the relevant waveform has. In this way, energy savings of several orders of magnitude may be obtained. Deceptive attacks exploit other types of vulnerabilities, e.g. the insertion of large amounts of regular traffic into the network of the adversary, or offering false retransmission routes for his network traffic.

While sometimes the system to be targeted in the theatre is known beforehand, smart EA attacks normally will be combined with monitoring, in order to determine in real-time the EA targets. As a current example, a prototype reactive vehicle-protection jammer has been described [102], which do very rapid spectrum scans and proceed to rapidly jam observed targeted signals. It is expected that the development and refinements of reactive jammer systems with monitoring, system recognition and a database of jamming techniques to be applied to specific systems, will be an area of priority. A library of optimized jamming signals may be built up by running computer simulations beforehand. The development of smarter EW systems is likely to be a continued major effort in the coming 10 years.

Cognitive Jammers

There is a strong trend in communications systems to include elements of artificial intelligence, providing communication nodes that are referred to as cognitive radios. For the communication systems, the goal is that they should better adapt to the electromagnetic environment in the actual theatre and be self-configuring in terms of the use of the spectrum. Another goal is that they should take distributed and autonomous anti-jamming type action towards an adversary.
With the inclusion of artificial intelligence elements in communication systems, it is evident that the EA counteraction needs to include equivalent functionality in the jammers, resulting in the cognitive jammer. The cognitive jammer will take distributed and learning-aided decisions which EA actions to employ. It is also clear from available research literature [103] and a US Air Force Request For Information (RFI) [104] that cognitive jammers are already a topic for research and development.

The evolution of software defined transceiver platforms, implying that both communication and EW functionality can be run as applications on the same platform, provides possibilities for integration of combined EW and communications. Combined with cognitive functionality, jamming and anti-jamming measures may then simultaneously be optimized. A motivation for this trend is the present lack of an integrated and combined overview of EW and communication systems, sometimes causing own communication systems to be affected by EW measures targeted at adversaries.

It is expected that there will be major research and development efforts on both cognitive radios and cognitive jammers in the coming 10 years, but it will probably take much more than 10 years for these systems to mature.

8.2.3 Electronic Navigation Warfare (NAVWAR)

Military weapon platforms and information systems depend on knowledge of accurate position, navigation and time (PNT). The primary source of PNT information is Global Navigation Satellite Systems (GNSS), cf. Section 6.2. The dominating GNSS is the US Global Positioning System (GPS), which is the system used by NATO. The Russian GLONASS is again close to having a fully populated satellite constellation. The European Galileo and the Chinese Compass are under development and expected to become operational in the 2015–2020 timeframe.

The terrestrial, regional navigation system, LORAN C, is phased out in the US. LORAN-C is still in operation in northern Europe and covers Norwegian territory and may enter into cooperation with a similar Russian system.

The vulnerability of GNSS signals is a defined threat in NATO operations [105]. There are concerns that possible physical attacks may be directed towards the GNSS satellites themselves. In recent conflicts where NATO-countries have been involved, threats against GPS information have not been a big concern, although Iraq attempted to jam the GPS in the Second Gulf War [106]. Advanced adversaries must be expected to exploit GNSS vulnerabilities to a larger extent. An overreliance on satellite navigation systems should therefore be avoided.

The known ways of electronic attacks on GNSS systems are jamming, spoofing and replay [107]. Concerning jamming, and with the current civilian GPS signals, a single one-Watt jammer will deny GPS information in an area of about 35 km radius [107]. With the military signals the denied area will be less, but may still be in the order of 20 km with a one-Watt jammer and a basic receiver.

An adversary may be expected to have high power jammers that cover large areas/distances. Several, distributed, low power jammers may deny GNSS information throughout large areas. GPS jammers are commercially available.

The civilian, unencrypted, GPS signal may be vulnerable to spoofing, with false GPS messages giving incorrect position information that is unnoticed by the operator. Since the military signals

are encrypted, it is less likely that military receivers may be spoofed. However, attacks where a military GPS receiver is exposed to retransmitted GPS signals may possibly also constitute a threat. The degree of vulnerability may depend on the actual type of receiver.

The latest generation of receivers ensures maximum signal protection and compatibility with the newest military GPS signals (M-code). Another countermeasure against electronic attacks is to use advanced receiver antennas, for example antennas that can direct zero sensitivity towards a jammer. Such a system may also be integrated with inertial navigation systems, for further increased robustness. Lastly, it is important that operators have been trained in terms of identifying electronic attacks and how to minimize the implications of such an attack.

The most significant change in satellite navigation over the next ten years is probably that there will be four operational systems with global coverage. In addition to GPS and GLONASS, the plan is that GALILEO and Compass will be fully deployed. GPS will be fully operational with the new military signals (M-code) that provide improved resistance against electronic attacks and fratricide. The handling/distribution of crypto keys will be simpler than today. In a crisis situation, satellite signal power may be increased to improve jamming resistance. Towards 2020 it is expected that GPS satellites will have the possibility to direct a high power spot-beam towards specific conflict regions to further increase the jamming resistance. Planned development of the ground control segment may provide new information services to the military. It is necessary to have user equipment with the ability to take advantage of the new functionality.

In order to deny a future adversary access to GNSS navigation information, it may be necessary to jam several of the systems mentioned above. It is expected that the required jamming power will be higher, as the above systems may be able to increase signal power. Distributed jammers are regarded as an effective means to deny access to PNT, in that they both may cover a large area and require more extensive use of resources to counteract. This includes resources to locate and destroy the jammers. Software Defined Radio technology in the satellites, ground stations and receivers, which makes it possible to change the waveforms and employed frequencies while the satellites are in orbit, may be additional challenges for GPS jammers.

Vital weapon platforms and systems should be properly protected against electronic attacks to maximize availability of PNT. Advanced antennas provide improved resistance, e.g. beam-forming antennas that constantly track the satellite signals and blocks jammer signals. It is expected that such technology will mature over the next 10-year period. The use of Software Defined Radio technology, which makes it possible to do waveform and frequency changes, will possibly be another technology that can contribute to the defence of GNSS signals.

In summary, the GNSS information will continue to be susceptible to electronic attacks, and an advanced adversary is likely to exploit these vulnerabilities to deny or possibly falsify GNSS PNT information to weapon systems and information systems. Against an advanced adversary, it is important to have the best possible means to deny his navigation information, and the best

possible means to protect own access to PNT. It remains important to train operators to minimize the operational implications of loss of PNT.

8.3 Electronic Defence

Electronic Defence (ED) is in the new definition the application of EM energy to provide protection and to ensure effective friendly use of the EM spectrum. ED also includes protection of forces, areas and platforms. This section will not cover the entire range of ED effects described in the definition but focus on ED applied to platform protection (against both radar and electro-optic/infrared threats), force protection (counter RC-IED), radar vulnerability to EA (and possible protective measures) and finally navigation warfare ED.

8.3.1 Platform Protection – Radar

Systems for electronic self-protection for radars benefit from the rapid development in general computing power, especially when products from the commercial market can be utilized. The main challenge in military applications is to exploit the available computing power from the commercial market in modular, upgradeable and scalable system solutions.

Warning sensors for platform self-protection against radar guided threats currently have available enabling technologies such as digital receivers and advanced distributed antenna systems that make it possible to detect, identify, and accurately measure the direction to radar based emitters in a very dense and complex signal environment.

The capabilities for advanced active electronic countermeasures against radar systems and seekers have increased dramatically over the last decade with the introduction of advanced jamming systems with the DRFM (Digital RF Memory) as a core component. DRFM technology is now mature and enables effective deception and confusion techniques against modern radar systems. Furthermore, the development of solid-state power amplifiers and active phased array antennas enables directional jamming to be applied to a large number of threats by very rapid electronic steering.

Radar countermeasures for self-protection can be subdivided into an on-board and an off-board component. On-board radar countermeasures will rely heavily on DRFM-technology as the core component. Typical features are:

- DRFM as the core component (multi-bit and multi channel)
- Techniques generator for off-board decoys
- Directional jamming with phased array antennas
- Programmable and scalable to cope with very dense threat environments

The off-board component of radar countermeasures can be chaff, a towed decoy or a free falling active decoy. Typical features are:

- Advanced chaff dispensers handling both chaff and active radar decoys
- Fibre optic towed decoys
- Jamming signals via fibre optic cable from on-board jammer
- Integration with on-board jammer with possibility for cooperative jamming (on-/off-board)

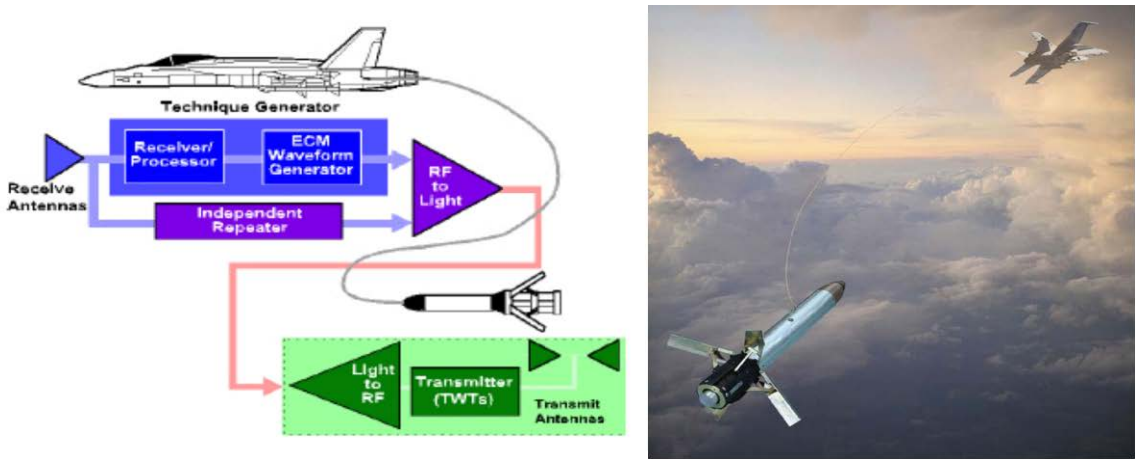

Figure 8.3 Example of radar countermeasures system, IDECM system on F/A-18E/F (source: BAe Systems/ITT).

The IDECM RFCM (Integrated Defensive Electronic Countermeasures RF Countermeasures System) jointly developed by BAe Systems and ITT consists of an on-board DRFM based jamming system (ITT) and an off-board fibre optic towed decoy known as ALE-55 (BAe Systems), Figure 8.3. This RF countermeasures system represents the state-of-art on-board and off-board technology and is the primary radar self-protection system for US Navy F/A-18E/F Super Hornets [108].

8.3.2 Platform Protection – EO/IR

The most common way to protect military aircraft against infrared (IR) guided missiles is to use expendable flare decoys. Advanced electronics and sensors enables modern missiles to use several target characteristics (e.g. intensity, position, speed, colour) to discriminate against false targets. This has driven the development of spectrally matched and trajectory controlled (propelled and aerodynamic) flares, a development still ongoing. With the advent of imaging IR seekers, the pace of development is expected to increase even further. IR signature suppression and/or modification systems will be required to meet this emerging threat, and have the general benefit of increasing the countermeasure performance and reduce the engagement envelope of the platform.

In order to detect the incoming missile, a missile approach warning system (MAWS) must be installed on the aircraft. Up till now the majority of the MAWS have been based on ultraviolet sensors. However, at the moment several new imaging dual-colour IR MAWS systems are under development, and other multispectral systems are under consideration. These new MAWS will offer, among other factors, increased detection range and lower false alarm rates, but strong

cooling requirements may limit their application to larger platforms. Advanced image- and signal processing are used in the new MAWS, and many manufacturers are working to integrate hostile-fire-indication to detect small-arms fire as well. There is also ongoing work to include detection of rocket propelled grenades in addition to small arms fire, since both are common threats to military aircraft today.

An aircraft carries a limited number of flares, and the future threat expected from advanced (including imaging) IR seekers has been a driver for development of laser-based directed infrared countermeasure (DIRCM) systems. Based on the angle of arrival information from the MAWS, the DIRCM system tracks the incoming missile and points a laser beam towards the missile in order to misguide or dazzle the IR seeker. Laser-based DIRCM systems have been in service on transport aircraft since 2005, and also on large helicopters since early 2009 [109]. Initially used in the US, UK and Israel, an increasing number of transport and helicopter platforms in several countries are equipped with laser-based DIRCM systems.

There are several new ongoing DIRCM development programmes both in the US and in Europe. Today a lot of effort is put into making the DIRCM systems smaller, with lower weight and power consumption. This is necessary in order to integrate the DIRCM systems also on small helicopters. To achieve a smaller system several companies are working on making smaller jammer heads (turrets). Another important component to improve in today's DIRCM systems is the laser itself. Up to now DIRCM systems have used combinations of lasers and nonlinear optical devices in order to reach the desired wavelength regions. It is expected that future miniaturized systems will use compact semiconductor-based lasers, such as quantum cascade lasers. Two-Watt versions of such lasers with output in the 4–5 µm waveband have already been announced by US companies.

Figure 8.4 Illustration of a DIRCM system in use (source: Raytheon).

Most DIRCM programmes today aim for development of open-loop systems, which means that no attempt is made to classify or identify the incoming threat system. Closed-loop systems can classify the threat by detecting reflected radiation and thereby optimize the jammer code for that specific threat. Open-loop systems are simpler with respect to system design, but require a more complex jam code (or sequence of codes) to defeat all possible threat systems in a given scenario. Such a code will typically need more time to defeat the seeker than an optimally adapted code in a closed-loop system.

Lasers used in DIRCM systems available today are not powerful enough to induce damage or destruction of the missile's IR detector. To induce such damage, the laser radiation must be concentrated in a high-energy pulse, and a significant fraction of the beam must hit within the aperture of the missile seeker. In order to achieve this, an advanced beam steering system will be required, probably using an adaptive optical system to correct beam distortion induced by atmospheric turbulence. It is not expected that damaging DIRCM systems will become operational on air platforms during the next decade.

DIRCM systems available today, and in the near future, are not a substitute but rather a complement to flares on military aircraft. This is partly related to the fact that flares are simple and reliable, even in a variety of severe environments.

The threat from infrared guided MANPADS (Man-portable air-defence systems) has significantly changed during the last decade, and today also civilian airliners are potential targets. Therefore, development of flares and dispenser systems for use on civilian aircraft has gained interest, and DIRCM systems have been adapted and tested for use on civilian aircraft. So far the conclusion from the airlines is that DIRCM systems must be improved with respect to maintenance requirements (increase the Mean Time Between Failure – MTBF), and the unit price must be lowered in order to make them affordable for the civilian airliners. Today, a DIRCM system typically has a unit price of 1–2 million US dollars, with an MTBF in the order of 300 hours. The use of DIRCM systems on commercial platforms will require an order of magnitude increase in reliability.

8.3.3 Force Protection – Counter RC-IED

During Norwegian participation in what is commonly described as "asymmetric conflicts" the threat from so-called IED (Improvised Explosive Devices) constitutes a majority of the losses to our forces. Many of these devices are armed or triggered via various types of remote control mechanisms. Radio controlled (RC) remote triggering is one of the types used. Jamming of these trigger devices is today an important part of our force protection, especially during troop transports and convoys. This situation is expected to persist for as long as our forces are participating in these types of conflicts.

Electromagnetic countermeasures, or jamming, have proven to have a dual effect: first of all a preventive effect in the sense that our opponents avoid targets that are equipped with

Counter-IED protection. Secondly, active jamming does provide a real, but not a full 100% protection against those RC-IED attacks that are carried out.

An imaginary jamming-bubble is often used as an illustration of the protection range provided by jamming. It is a major challenge to obtain maximum IED-protection, yet maintain full communication capability both within a column and also back to the HQ. Modern military operations are heavily dependent on reliable communications; hence it is a problem that the jammers tend to interfere with our own communications over ranges much greater than the protective jamming-bubble.

First generation IED-jammers operated in a static or open-loop mode, with a pre-programmed jamming behaviour tailored to defeat known threats. One disadvantage of this concept is that most of the jamming power is wasted on threats that are not present. Another source of conflict is the interference to own communications. An improved coordination for the use of the electromagnetic spectrum during military operations will therefore be imperative. Such coordination must include the three disciplines Communication Security (COMS), Communication-Electronic Warfare (COM-EW) and Counter-Radio controlled-Improvised Explosive Devices (C-RC-IED).

Figure 8.5 Picture of a RC-IED jamming system (photo: L-3 TRL Technology).

Responsive, or closed-loop, jamming has been proposed as an attractive concept in order to reduce fratricide between jamming and own communications. Basically, such jammers consist of one receiving branch that is monitoring the radio spectrum in search of target signals. Upon detection of a threat the transmit branch will initiate jamming using a waveform that is matched to the threat. Normally, responsive jammers are operating in a look-through mode where the jamming is interrupted for a short time interval, enabling the jammer to check if the threat is still present or whether any new threats have turned up.

The main advantage of responsive jamming against RCIEDs is that the jamming effort is focused directly on the threats. This leads to a reduction of the interference. One of the challenges of such a concept is to obtain both fast and reliable threat detection, yet maintaining a good discrimination against false alarms. False alarms may waste part of the jamming output power on non-existing threats. A more serious consequence is that it may in fact prevent detection of real threats. Another issue is the fact that IEDs are not designed according to any standards; they are manufactured based on what is available of hardware and knowledge. This means that threat detection is a quite difficult task. It is questionable whether responsive jamming can be a suitable countermeasure for this kind of changeable threats.

It is a paradox that even though IEDs are quite simple and inexpensive to manufacture, they constitute a real, substantial threat that is costly to counter and lead to substantial operational restrictions. This fully underlines the meaning of the term asymmetric operations. It is difficult to predict in which direction the threats will evolve, but the past have shown that our opponents are capable of adapting to our countermeasures by constantly developing new types of remote-control devices.

8.3.4 Radar Electronic Protection

In recent years, radar jamming has moved from high power noise to low power coherent deception through the introduction of the digital RF memory (DRFM). The DRFM makes it possible to detect and store a radar signal, and to use this stored signal as the basis for a jamming signal.

Up until recently, Electronic Protection (EP) was focused on minimizing the effect of noise jamming on the radar through e.g. generating jamming strobes in the direction of a jammer or through having adaptive antenna patterns that could steer a null in the direction of a jammer. EP will now have to move towards minimizing the effect of DRFM based jammers. This will significantly increase the requirement on processing power in the radar, but processing power should be readily available if the radar takes advantage of the same technology development as jammers do. The protective measures may have to be designed into the radar processing during radar development, since they probably need to be an integral part of the radar processing to be effective with minimum detrimental effect on the radar operation during normal operation.

The increase of processing power opens for another development in radar technology: The use of wide bandwidth, low power and highly variable waveforms, while maintaining or even improving performance. Examples can be found in [110, 111]. These waveforms make the radar signal difficult to detect, difficult to identify as belonging to particular radars and hence difficult to jam. Also they introduce increased processing gain over noise (jamming). Somewhat further into the future more or less all of the radars will be digital, and hence in principle software defined. Anything software defined can be highly variable, multi function or even adaptable to the current situation. This will make the radar signal even more difficult to handle for the jammer receiver (or the ES system operated in conjunction with the jammer).

The increasing capabilities of radar networks have the potential to increase the total system performance against EA. Bistatic radar operation can also make jamming more difficult since the position of the radar receiver in that case might be unknown to the jammer. If the radar utilizes transmissions of opportunity, e.g. broadcast transmissions, it is difficult for the EA system to determine whether or not a radar is operating in an area at all.

8.4 Electronic Surveillance

Electronic Warfare Surveillance (ES) are actions taken to gain information superiority by effectively understanding the situation, protecting own forces and provide undisturbed operation of own systems. Electronic systems radiating electromagnetic energy are heavily used military and commercially, the systems coexist and in many situations the adversary may use commercial systems. ES must therefore cover all systems, and the actual situation will define the ones that need monitoring.

8.4.1 Radar ES

The technology trends can be divided into three important areas: New hardware, new methods and integration of ES into network centric warfare.

Hardware Trends

ES sensors (Radar Warning receivers (RWR), Electronic Support Measures (ESM) and Electronic Intelligence (ELINT)) have always challenged the available technology; development of equipment and components has been done by a small number of specialized companies. Availability of components has been limited by export restrictions and very high cost.

The limiting technology has mainly been in high frequency analogue components and in high speed digital signal processing. During the last five years the commercial market has seen a big increase in these areas. Miniaturized analogue components have been developed for communications and tools for efficient design and production of small quantities are available. Signal processing cards with analogue-to-digital converters and Field Programmable Gate Arrays (FPGA) for high speed digital signal processors are available on the commercial market (COTS) at reasonable prices. The hardware for ES-sensors is now available and makes it possible to produce hardware for advanced ES-sensors by any high tech electronic company. The use of this technology is also seen as a trend in new ES products that are available on the market.

Method/Information Trends

The hardware described above needs methods and algorithms implemented in software to become an ES-sensor. Development of methods has been ongoing for the last ten years and operations that previously were performed in analogue hardware are now being implemented in digital signal processing. This gives an advantage in reproducibility and stability of the system, but it also open for new capabilities for ES-sensors.

The new operational capabilities under development are precise geo-location and identification of the radar (fingerprinting and specific emitter identification). This can only be achieved by

extraction of very detailed information about the signals. Modern hardware has also improved the radar systems; sophisticated multifunction radars, low probability of intercept radars and radars having completely different war-modes are being developed. This will cause problems for ES-sensors and new methods will have to be developed. Methods and software implementation is not COTS. The traditional protection of ES hardware, both from governments and companies, will shift to protect the implementation of methods in the sensor.

Integration Trends

ES has mainly been used for protection of military platforms by detection of threat radars. ES also produce a lot of information that can be used on a higher military level for situational awareness and for planning new operations. During the last five years, national and NATO demonstrations have showed the value of ES information as a complement to the traditional information in command and control systems. Integration of ES will benefit from the communication infra-structure introduced by the network centric approach. The current limiting factor for use of ES in such a way is the vast manpower needed – a lot of manual work has to be carried out in order to validate and integrate ES information. Methods integrating ES information into the air, sea and ground picture will need major efforts. In the future, this will also be performed automatically. The next decade will be dominated by the effort to understand ES as an information source and to develop, test and implement this into command and control systems.

8.4.2 Communication ES

Communication Electronic Surveillance is the ability to maintain situational awareness and to provide intelligence by monitoring and extracting the opponent's use of EM energy for communication. It is a very important information source regarding the opponent's position, movement, identity, possible intentions and use of the electromagnetic spectrum. One of the applications of ES information is as an input to the process of creating and updating the real-time situation picture. Other applications are to maintain the electronic order of battle, and as input to EA.

The trend in wireless communication is the continued transformation from open analogue communication systems to digital transmission systems. Most of the digital transmission units will be linked together in networks. Mobile phone systems and military cognitive radios are good examples of this trend. Future communication systems will be adaptive in both frequency and in selection of waveforms. Software Defined Radio principles will in the future be the preferred implementation technology since it enhances the ability to update the communication systems by applying new waveforms in software. This will be challenging to ES, since communication systems can be frequently updated.

Digital transmissions will in the future be encrypted to ensure information transfer integrity and confidentiality. ES will have to adapt to this challenge by focusing more on analysis of technical waveform parameters, transmission rates and other behavioural patterns. The trends for improving future communication ES systems will be on increased performance from hardware

such as Analogue to Digital (AD) and Digital to Analogue (DA) converter technology, and especially the affordable and readily available computer processing power.

To exploit the benefits of the future ES sensors, they must be integrated in an organization optimized for rapid analysis and information dissemination. This organization needs optimized C2IS tools to exploit the large quantity of information collected by ES. Reach-back support will be increasingly necessary to analyze unknown signals, and to update databases of identified signals. Reach-back support will provide linguistic support if necessary.

The future ES systems will be wideband systems that can detect and process a vast number of signals in parallel. To process these signals, automation is necessary.

Some of the future ES trends are:

- Extensive use of automated signal processing.
- Sensor to sensor cooperation.
- Close integration with communication authorities (Electronic Order of Battle, EOB).
- Close integration with EA to perform real-time support.
- Intelligent signal filtering to aim the sensor to specific targets.
- Predefined alarms on specific characteristic events or patterns.
- Automatic information extraction and report production using:
    - Artificial intelligence (Intelligent behaviour, training and adaptation).
    - Automatic identification of communication signal waveforms.
    - Use of communication signal waveform signature database.
    - Automatic recognition of communication networks and production of traffic diagrams.
    - Automatic target tracking (possible movement of communication nodes).
    - Database with knowledge from previous events.
    - Automatic position localization:

The future ES systems will not be a single universal type, but a variety of systems optimized for the different classes of tasks. Classes of ES systems that will be found in the future battlefield are:

- Small autonomous systems with automatic signal processing.
- Remotely controlled systems (with real-time data-links to the control centre).
- Portable systems light enough to be carried by soldiers in the field (Figure 8.6).
- Larger mobile systems, mounted on mobile armoured platforms.
- Large stationery systems.

One possible future trend is the deployment of common Communication, ES and EA units on the battlefield. This unit would be the soldier's standard communication radio, but it could perform ES when not used as a communication node or as an EA. The cognitive radio concept can be modified to include such roles. This will give the EW units a lot more ES sensors in the battlefield, and in that way gain a possibly better and more accurate situational picture.

Figure 8.6 Illustration of a modern portable ES sensor (photos: FFI). Left: MEWS sensor, Right: MEWS controller/analysis unit.

Figure 8.6 is an example of a modern portable ES sensor, the "Man portable EW System" (MEWS), from L-3 TRL Technology. The picture at the left shows the sensor in the field mounted on a tripod. The unit is battery powered with the battery on the ground. The DF antennas are mounted inside the radome on top of the sensor. The picture at the right shows the MEWS controller/analysis application run on a ruggedized PC.

8.5 Operations in the Cyber Domain

The cyber domain is a virtual world that is created and accessed through computers and networks. This virtual world can be thought of as consisting of multiple enclaves[7], which may or may not be interconnected. The difference between a computer network and an enclave is that the former is technologically and physically oriented, while the latter is the virtual environment that is carried by the infrastructure and systems. Multiple cyber enclaves can be intentionally interconnected, for instance when joining two separate networks, or as part of a security breach against the will of their owners.

A clear trend is the interconnection and convergence of military and civilian cyber enclaves. The biggest enclave in the cyber domain today is the Internet, with over 2 billion users connecting through computers as desktops, laptops, cell phones, tablets and other network computer devices. Instant access to information and services on the Internet is valuable for military operations, resulting in a push for merging civilian and military technology and the cyber enclaves themselves. The US Army is now planning to issue every soldier an iPhone or Android cell phone, because "at war, smart phones would let soldiers view real-time intelligence and video from unmanned systems overhead, and track friends and enemies on a dynamic map" [112].

The convergence of traditionally separate cyber enclaves requires advanced multi level security (MLS) systems, for managing information and access originating from different (un-)classified cyber enclaves. From the practical standpoint of efficiency, why not use the Internet connection

[7] The term cyber enclave is inspired by the political / geographical enclave, which is a piece of land totally surrounded by a foreign territory.

on the iPhone as the communication link for the classified battle management system? Such convergence, of military and civilian cyber enclaves, requires new methods and technologies for efficient and secure communication.

Due to the inherent structure of the Internet and the constituent technologies, identifying the instigators of a cyber attack is very difficult. The cyber attacks on Estonia in 2007 [113] is a case in point. This makes retaliation a problematic defence strategy, because the attacker could be working through a compromised system or with a false identity. Deterrence by overt retaliation in the cyber domain could result in a high degree of collateral damage and be highly counter-productive, and quite possibly be a response explicitly sought and desired by the instigators. The interwoven nature of merged civilian and military cyber enclaves might be better addressed by improving cooperation and coordination between civilian and military authorities responsible for cyber security, investigation and forensics, and the private industry owning and operating cyber infrastructure (e.g. Internet Service Providers, service providers and others).
Cyber power may be defined as the ability to maintain control over own cyber enclaves, and to manoeuvre in the cyber enclaves of others. Computer Network Operations (CNO) are military operations against target cyber enclaves initiated from the CNO unit's cyber enclave. CNO is (by nature) a cost effective military capability, useful both strategically and tactically in operations. A CNO unit basically changes the state of disks, memory (RAM), processing (CPU) and bandwidth, potentially anywhere in the target cyber enclave. Communication systems can be taken offline by attacking routers (bandwidth), applications can be exploited to run attacker provided code (CPU/memory), logistics databases can be altered (disks), GPS coordinates on cell phones can be faked (memory), alarm and video surveillance systems can be disturbed (bandwidth), and messages created by Psychological Operations (PSYOPS) units can be displayed to target users (memory/disks/CPU). In principle, all of these attacks can be launched from physically distant locations, but CNO attacks require some form of connection between the attacker and target cyber enclaves. Note that the connection between the cyber enclaves may also be indirect, by exploiting USB sticks or other means.

The cyber domain is strongly related to the electromagnetic spectrum where Electronic Warfare (EW) takes place. Civilian and military cyber enclaves often make use of various types of wireless communication links as carriers for network traffic, and systems targeted or used by EW usually have a cyber component. This makes the ability to manoeuvre in the electromagnetic spectrum in concert with activities in the cyber domain an integral part of information operations. Information operations (INFO OPS) are coordinated efforts to influence enemy decision making, by affecting the enemies' will, capability and understanding, while protecting our own. INFO OPS can coordinate a wide range of capabilities, including but not limited to CNO, PSYOPS, EW, deception and physical destruction. The coordinating effort requires new ways of integrating military capabilities, and new ways of planning military operations that includes both kinetic and non-kinetic means.

Technologies supporting INFO OPS include methods and tools for planning and coordinating EW, CNO, PSYOPS, and other means while maintaining consistency with activities like public affairs (PA). While EW and CNO are effective weapons, they may also be dangerous weapons due to collateral damage and unintended effects. This is especially the case when joining civilian and military cyber enclaves. For instance, the physical or logical destruction and disruption of communication satellites may stop enemy communication channels, but may also disable GSM communication used by own soldiers or others in the zones of conflict. In other words, CNO and EW must be de-conflicted before use. This is, of course, also the case for all other military means, but de-conflicting INFO OPS means is probably more difficult due to a higher degree of unpredictability and uncertainty.

The usefulness of INFO OPS requires military leadership that understands the advantages and disadvantages of INFO OPS, but it is also necessary that the various military units and components communicate the effects they are able to achieve in this domain, in order to inform their military commanders. For example, which services, and with what level of precision, can CNO offer to help accomplish the objectives of the military leadership – without using technical terms? Knowing that computers in the target enemy military unit runs vulnerable Internet Explorer web browsers doesn't help much in high level military operation planning. Defining and understanding these service interfaces between highly technologically oriented units and the planners of military operations is important for the efficient use of technological INFO OPS. In conclusion, the use of INFO OPS requires highly technologically oriented units as well as technology for integrating INFO OPS with other traditional military operations.

Incidents in the cyber domain will have effects on military operations in the physical domains of war; land, sea, air and space. Cyber power is therefore equally important as land, sea, air and space power, and we need to prepare for the use of cyber power by monitoring technological trends, acquiring and utilizing advanced technology, developing useful concepts and adapting our training. One thing is certain: The man-made, intangible and invisible cyber domain will never disappear from the theatre of war.

9 CCIS Systems

9.1 General Trends

The quest for Network Enabled Capabilities (NEC) continues, but now a bit more distinct and realistic since the previous MilTech report in 2004. Since the NATO treaty [86] was signed, the member states have carried out quite independent defence acquisition programmes resulting in efforts to standardize to support interoperability. Over the years these efforts have been quite successful, but struggling to keep pace with new technology. In the field of communications and data systems, the military is in a migration phase where it is necessary to utilize both traditional (often proprietary) Combat Net Radios (CNR) and IP based equipment using civilian standards. In tactical networks the military are still awaiting solutions to provide the extra mechanisms that are needed to make the civilian standards suit the additional requirements necessary for efficient tactical use. Recent large-scale operations with many nations involved have made the need for interoperability even more important. The nations need to be able to bring their national command and control systems normally developed by national industry over a long time period and share a joint operational picture of ongoing operations.

9.2 Service Oriented Architectures

In the migration towards NEC, NATO has adopted the concept of service-oriented architecture (SOA) in order to promote interoperability and efficient information exchange in the NATO organization and between the nations. SOA is an architecture making it easier to publish, discover and exchange information between heterogeneous systems. Military resources can be made available as services, which may be discovered and utilized by parties that don’t need to know where they are in advance.

SOA can be described by three main functional components: A service consumer, a service provider and a service registry. The service producer makes services available to others by publishing service descriptions to a service registry. The service descriptions provide information about what the service does, where it is located and how it may be invoked. Services may for instance give access to sensor information, a common operational picture or an intelligence report. The service consumer may browse a service registry for services such as, for instance, sensors providing information within a given geographical area. The service consumer may then, if authorized, connect to the service providers in order to download the information, initiate actions or subscribe for automatic updates of information when it becomes available.

A NATO SOA supporting international operations will have to allow for communication across system and national boundaries while at the same time taking legacy systems into account. A key concern is that open standards and available products should be used when possible, both to ensure interoperability and to reduce costs. Web services technology is becoming increasingly popular for implementing loosely coupled service-oriented civilian systems. Interoperability is the main concern, and thus Web services are based on standards. NATO has identified Web services standards for the realization of SOA and as the enabler for interoperability between the different

military systems of the various NATO nations. The NATO Core Enterprise Services Working Group (CESWG) has defined a set of core services, which may be regarded as the foundation for more advanced services in NATO NEC.

In military operations, information often needs to traverse several different types of networks with different characteristics with respect to data rate, error rate and frequency of disconnections (disadvantaged grids). It would be desirable to have a common information infrastructure based on the same set of standards. Thus, the solutions chosen need to work in the different types of networks in order to exchange information across operational levels. The Web services standards have been developed for use in fixed high bandwidth networks with stable connections, but research is ongoing with the focus of finding solutions for enabling the use some of these standards in disadvantaged grids as well. Results from this research are promising and show that realization of a generic information infrastructure across different operational levels is possible.

9.3 Multilateral Interoperability Programme (MIP)

One of the key enablers to network centric warfare is interoperability. The Multilateral Interoperability Programme (MIP) [114] is an initiative to define a common data model, upon which heterogeneous command and control (C2) systems from different nations can base their data exchange. By using the same reference model, information can be transferred from one system to another without changing the content, giving the foundation for the operators to interpret the situation the same way. Modelling is also a prerequisite for applying semantic technologies, for instance to automate translation between models or derive new information. The main product from MIP is the Joint Consultation Command and Control Information Exchange Data Model (JC3IEDM). MIP is recognized as the most significant interoperability approach for the land domain within NATO, with JC3IEDM as a mandatory STANAG. Maritime, Air and Joint aspects are also included in addition to the initial Army requirements, to enable information exchange between different domains, but these domains are not as well covered yet. JC3IEDM is developed for information exchange between C2 systems with human operators.

MIP has now initiated a major restructuring of the data model, while maintaining the capabilities, before further development continues. This is to get more in line with software tools and technologies used among the member nations, but also to be more attractive to potential users, and includes changing to UML notation and a modelling approach more suited for object-oriented programming. One of the main criticisms of JC3IEDM has been that it has gotten too big and all-including, covering more domains than any individual C2 system. The model is now being made more modular, to facilitate a split-up into several smaller models as the next step. NATO and MIP (and other Communities of Interest) will then take custodianship of different domains, still with a common core to ensure interoperability. The modular approach will also make it easier to use only parts of the model (relevant for each C2 system) and to implement more dynamic information flow through service-oriented architecture. The RTO group ‘IST-084 Domain-based Approach for Coalition-wide Information Exchange’ used JC3IEDM as a case to demonstrate that interoperability can still be maintained when a large model is split up into several smaller models with a common core [115].

9.4 Information Security

The need to share information on the battlefield is increasing and the capabilities of the information infrastructure evolve to meet the needs. At the same time new threats to the information infrastructure are identified, and it is necessary to introduce new security functions to meet these threats.

In the past, confidentiality protection has been the major concern for secure information sharing in military operations. It is still important to prevent unauthorized access to the information content. Moreover, it is important to preserve the authenticity and integrity of information. Authentication refers to the verification of identities, and authentication of an information object assures the receiver that the object at some point in time originated from the claimed source. Integrity will ensure that an information object has not been manipulated by unauthorized parties during the lifetime of the object. The consequence of a security breach with respect to authenticity and integrity can be severe damage to ongoing military operations. Information can be modified, e.g. orders, target data and reports providing positions for own units.

The role of the network may be changed. The network makes up a fundamental part of the information infrastructure and provides the transport of user data between user systems. Traditionally, the network has provided the confidentiality protection of user data. This function may be moved to the user domain, i.e. end-to-end confidentiality protection. The advantage of this is that domains at different confidentiality (classification) levels, as well as different nations, can use the same transport infrastructure. The network will still provide security functions. New functions may be authentication of links, management information and signalling within the network. Confidentiality protection of the signalling and management information may also be provided.

One of the major challenges is information exchange between domains at different confidentiality (classification) levels. The interconnection of various information domains with different ownership and policies, potentially even civilian, will require platforms at high assurance levels[8] for critical components. The availability of certified platforms at sufficient levels will be a critical premise for the implementation of MLS security mechanisms. Some security functions and components will presumably require an assurance level as high as EAL 6–7 according to the Common Criteria (CC), depending on the threat scenario and the security span. For others EAL 4–5 may be sufficient.

The MILS architecture is a candidate for more general purpose high assurance systems as needed for implementing security critical functions in distributed military information systems for command and control, which for this purpose require security evaluation according to CC. The basic idea of MILS is to make the security critical part of the system small and with minimum functionality in order to have it certified for the highest assurance levels (i.e., EAL 6–7).

[8] EAL 1–EAL 7 is a measure that grades systems according to a set of standard security criteria (Common Criteria)

The limited size makes development, certification, and accreditation more practical, achievable, and affordable.

Cross-domain guards may be introduced in the medium to near future. Such a guard will assure that labelled information objects are exchanged correctly according to the policy. These guards will be at a medium assurance level and thus can only be employed when the classification span (the range of classification levels) is small. For cross-domain information exchange between domains having a larger classification span, high assurance multilevel secure (MLS) systems are needed. A main challenge for these systems is covert channels. Integrity protection of processes and labelled information objects are key functions in future MLS systems. High assurance MLS systems may be introduced in the longer term.

9.5 Network Communications

Most of the changes in network communication are happening in the tactical domain, both in the deployed infrastructure and in the mobile tactical networks. Up until recently, data communication in mobile tactical networks has been conducted locally on many small isolated radio networks often designed specifically for a certain application (or for voice only). Communication between these networks has been implemented with post-it notes and manpower. The goal in NATO is to remove the tight coupling between application and network and provide a communication platform available for all application types. A second goal is to create an efficient network of networks to improve interoperability in the mobile network and between mobile networks and the deployed infrastructure. IP-family network protocols have been chosen as the standardized interface (glue) in this network. By and large, IP-protocols are well suited for this environment, but there are some challenges that must be solved to utilize the network in the most efficient manner, especially for mobile tactical networks.

9.6 Mobile Tactical Networks

In mobile tactical networks, the network nodes are moving and they continuously relay messages through other nodes. Today, most of the communication in mobile terrestrial networks is over narrowband VHF and HF radios. These are long-range radios where most receivers can be reached with one radio-hop. However, these radios provide very low data-rates. A general trend in military operations is the need for more data, also at the lowest echelons in the military structure, thus many countries have (or are planning to) introduce UHF radios in the mobile tactical networks. These radios can provide higher data-rates at the cost of much lower transmission ranges. A consequence of the low transmission range is that much of the network communication must be relayed by intermediate nodes to reach the receivers. Thus, the main focus in develop-ment for new radios (mainly UHF) has been to provide a routing protocol for the radio to handle rapid topology changes and still provide fairly stable routes in the local radio network. These protocols are often based on civilian developments for mobile ad hoc networks (MANET) with some small modifications for military networks.

As the networks change their nature from a one-hop broadcast network to a multi-hop network, there is also a need to exchange the traditional broadcast mechanisms for group communication with a multicast mechanism. The trend among the different radio manufacturers is to provide a simple flooding mechanism to support multicast. Ways to connect this flooding mechanism in the mobile network with a multicast protocol in the deployed network are not available, thus both the multicast solution in the mobile network and its interconnection with other networks will receive attention in the time to come.

As routing in the mobile networks mature, more focus will be on interconnection of different radio networks. As of today, different radio suppliers typically provide their own routing protocols that are not interoperable with others. Thus the networks must be connected with a standard IP-protocol that provide connectivity but hide the local topologies. This has consequences for other mechanisms that must be present for a mobile ad hoc IP-network to work well: Admission control, Quality of Service (QoS) support and traffic priority. Mobile military networks will have limited capacity. As more and more networks are interconnected, there is a demand for additional services, thus, there may be more traffic available than the network can handle. In order to preserve a functioning network, it is necessary to control the amount of traffic in the network with admission control, support different treatment of different services to provide QoS to the user, and prioritize and pre-empt traffic to free resources for the most important users. These issues are still research topics. The isolation of network topology knowledge, as is the result of different radio networks running different routing protocols, complicates the admission control and QoS handling for flows that traverses several networks. Better ways of creating the network of networks, admission control and QoS as well as efficient group communication (multicast) are the major challenges for these networks in the near future.

9.7 SATCOM

NATO and member nations are leasing capacity on both commercial and military satellites. In addition to the US, the larger European nations such as UK, Germany, France, Italy and Spain operate their own military satellites providing services including UHF, X and Ka frequency bands (also cf. Section 6.4). The DoDs in the US and Australia have launched three of their geostationary (GEO) Wideband Global SATCOM system (WGS), GEO satellites providing high capacity X- and Ka-band services with near global coverage. Another US initiative, the Mobile User Objective System (MUOS) GEO constellation, will provide UHF narrowband mobile communications mainly to US. The system is currently delayed, and the first launch is expected in 2011. In addition to GEO constellations, low Earth orbiting (LEO) satellites in polar orbits provide communications covering Norway’s northern territories. One such planned commercial system (Iridium Next) is expected to provide global broadband services from about 2015.

Satellite communication links are increasingly used by the military, with a resulting growing transmission capacity requirement. In the VHF / UHF frequency bands (235–322 MHz and 335–400 MHz) there is only limited capacity at relatively high cost available for lease. An increasing effort is carried out to develop SATCOM technology for vehicular installation operating in governmental X- and Ka-band. The objective is to enable tactical broadband communications on

the move in areas with sufficient non-obstructed line of sight to the satellite. Deployable tactical SATCOM nodes will be integrated with the terrestrial tactical narrowband (VHF) and broadband UHF networks requiring interoperable network technologies. Capacity demanding services will be available during operations in areas without fixed infrastructure or microwave links, complementing narrowband HF reach-back.

The US has for some years utilised a non-protected joint IP modem based on DVB-S and RCS technology to provide demand assignment multiple access (DAMA) and broadcast services to stationary users. This technology is standardised by NATO in STANAG 4622 (and ETSI), and is utilised by both commercial and defence SATCOM operators. In addition there are available non-protected NATO STANAGS on DAMA for smaller tactical terminals (4485) and fixed rate SCPC for VSAT type of terminals (4486).

Currently, several new SATCOM modem technologies systems are being standardised by NATO. STANAG 4606 in its Edition 3 is being extended with a protected frequency hopping DAMA IP technology and adaptive coding and modulation. Two additional waveforms are being standardized in NATO with DAMA functionality for tactical applications. One is a MF-TDMA hybrid star/mesh waveform (STANAG 4707) based on the Network Centric Waveform (NCW) developed and implemented by L-3 communications for the US DoD. The other is a CDMA star network (STANAG 4708) based on a waveform developed and implemented by Indra for the Spanish MoD. Both have SATCOM on the move solutions, Indra also has a manpack version. In addition, a part of the iDirect star network is also being standardized (STANAG 4494) for utilisation in the NATO management and control (M&C) system of their transportable ground terminals. The message set for this M&C is being standardized in STANAG 4706.
It is worth mentioning that some of these STANAGs seem to be competing and therefore might contradict interoperability.

NDLO is currently acquiring a satellite together with the company Hisdesat in Spain. It is planned that the new Norwegian/Spanish satellite will be launched into a geostationary orbit positioned at 29^{o} East in 2014/2015. The communication payload will provide both X- (7/8 GHz) and Ka-band (20/30 GHz) communication capacity. The coverage area is limited by about $\pm 75^{o}$ North/South, 46^{o} West and 104^{o} East. European coverage will be provided by regional antenna beams for both frequency bands. Steerable spot beam antennas will provide additional capacity anywhere within the coverage area, enabling SATCOM support to international operations. There are several ongoing projects with the objective of defining and acquiring relevant SATCOM equipment for land, sea and air forces. Interoperability is an issue in these projects and it is a goal to comply with the NATO Satellite Ground Reference Architecture (SGRA). In this regard, implementing some of the STANAGs is of interest. So far, STANAG 4606 Editions 1 and 3, and 4486 Edition 3 (Enhanced Bandwidth Efficient Modem – EBEM), are being implemented in the Norwegian frigate project.

9.8 Tactical Radios

The future tactical Software Defined Radios (SDR) will be able to switch rapidly from one waveform to another, thereby adapting to varying requirements and conditions. Compatibility with existing radios, in a transition phase, is possible reusing and porting legacy waveforms. A large effort is applied to standardize the operating environment for SDR in order to reduce the cost of porting a waveform from one platform to another.

There is a strong desire for new standardized networking waveforms for interoperability with enhanced capabilities. NATO has initiated the development of a new Narrowband Waveform (NBWF), while the Wideband Waveform standardization is waiting for the results from ESSOR and COALWNW. New generations of tactical radios might operate in VHF and UHF, combining narrow- and wideband waveforms.

The largest programme for SDR is the US Joint Tactical Radio System programme. These new generation radios will be equipped with legacy waveforms for backwards compatibility as well as a small number of new waveforms. It was expected that SDR radios should be cheaper since the hardware could be produced in larger quantities, reusing legacy radio waveforms. However, so far the reprogrammable radios have turned out to be even more expensive then legacy radios.

Another problem is the lack of coordinated radio frequencies causing the allies in an international operation to disturb each other, UAVs to crash due to lack of a working control link etc. To solve this, a new spectrum management language has been developed (SMADEF). In 10 years it is expected that all radio terminals will be able to coordinate their need for spectrum resources among each other, with a minimum of human intervention (Dynamic Spectrum Allocation and cognitive radios).

9.9 Battle Management Language (BML)

Digitization of Command and Control (C2) information is vital in order to improve C2 interoperability, to enable computer based C2 support tools, improve simulation based training and for the automation of C2 processes. BML is an emerging technology bridging the C2 domain and the simulation domain. One way to define BML is “the unambiguous language used to command and control forces and equipment conducting military operations and to provide for situational awareness and a shared, common operational picture” [116].

BML allows C2 systems to specify plans and orders that are executable by a simulation system or an automated system such as an unmanned force, and to provide situational awareness by feeding reports to the C2 system. BML has the potential to:

- reduce manpower required to conduct training by minimizing manual transfer between C2 systems and simulation systems
- improve decision support by performing courses of action analyses using simulation during planning or execution of operations

- improve interoperability between C2 systems
- enable tasking of automated systems or robotic forces
- reduce the ambiguity of plans and orders, and thus improve understanding between humans

Technical activities under the umbrella of NATO RTO Modelling and Simulation Group are important players in directing the future of BML and in investigating the potential for the use of BML in NATO [117].

A Coalition BML, C-BML is currently being standardized by Simulation Interoperability Standards Organization (SISO). C-BML is based on the JC3IEDM as basis for XML namespace semantics, grammars (nouns, verbs, adjectives) and ontology work [118].

9.10 New Challenges

One of the challenges in tactical networks is the large jitter and delay sometimes encountered. These networks consist of a variety of link types (HF-, UHF- and VHF- terrestrial radios as well as different types of Satellite terminals). Accommodating all these types of links in one network are leading to large delays and jitter variations. Some of the commonly used IP network protocols are not designed to handle this. Solutions to this are to design military application that uses existing protocols that can handle this or use proxy/gateway solutions that adapt to the challenges. For example the Delay and disruption tolerant SOAP Proxy, called DSProxy solution can bridge different networks and offers store-and-forward capabilities.

Improvised Explosive Devices represent a challenge to all radio systems, as indicated in Section 8.3. Broadband jammers are mounted on vehicles to counter this threat, which in turn disturb radio communication reception on these vehicles. To reduce the problem, co-site (programmable narrow band-pass) filters should be used for the radios and dedicated band-stop filters for the jammers.

10 Some Other Military Technology Themes

10.1 Laser Weapons

Laser weapons have some unique properties compared to conventional weapons [119]:

- They can attack targets at the speed of light, which allows for very short engagement times. This is particularly advantageous in long range engagements. The time required for the beam to reach the target is negligible, but the beam must typically be kept on target for a few seconds to achieve a destructive effect by heating.
- Due to the short engagement time, such weapons are able to engage several targets in quick succession.
- By adjusting the power of the laser beam, one can achieve flexibility with regard to effect in the target. This can be important in situations where one wants to stop a threat without destroying it.
- The laser beam can be pointed at the target with extreme precision, which is important for reducing "collateral damage". This characteristic is reinforced by the fact that the primary effect inflicted by the laser beam is heating of the target (no explosion). This "quiet" impact may cause confusion and fear to the opponent who does not understand what is going on.
- Laser weapons are characterized by having a big "magazine", which means that the weapon can be used as long as the weapon platform carrying it is able to provide enough energy to power the laser. This enables a far higher number of engagements compared to using e.g. missiles.
- Laser weapons have a completely different cost profile than other weapons (e.g. missiles) because the main cost is constituted by the acquisition of the weapon, while the cost per shot is very low. Thus, once acquired, the cost of using the weapon is low, which gives a great flexibility in that one can afford to use the weapon against many more target types.

Laser weapons have some significant limitations/challenges:

- The target needs to be within line of sight.
- The laser beam is influenced by processes in the atmosphere (absorption, scattering, turbulence), which tend to weaken the beam and increase the beam spot size on the target.
- The laser beam must be focused on a relatively small spot on the target to give the desired damaging effect, and this requires extremely precise tracking and pointing stability.
- Laser technology at the required power levels is very complicated. Traditionally, only so-called chemical lasers have been able to produce sufficient radiation power to provide weapon effects. Such lasers have a large footprint and require complex systems for handling of the chemicals used in the laser process. In recent years, there has been a rapid development of solid-state lasers that use electricity as their primary source of energy. These allow for a handier and compact weapon system, but the radiated power from such lasers is currently at least a factor ten lower than for chemical lasers.

- It is also a significant challenge to obtain good data for the amount of radiation power and beam diameter required to achieve the intended effect against different target types.

The development of such weapons has primarily taken place in the United States, with a number of impressive demonstrations during the last decades [120]. The best-known programme was the Airborne Laser programme (ABL), where a very advanced chemical laser gun was built into a jumbo jet. The weapon was intended for engagement of ballistic missiles in the boost phase, at distances of up to several hundred kilometres. After 14 years of development, an ABL system was tested in February 2010, demonstrating successful shoot-down of a boosting ballistic missile at a distance of about 80 km [121]. Other well known laser weapon programmes include the Advanced Tactical Laser (ATL); a short range laser weapon built into a C-130 for use against ground targets, and the ground-based Tactical High Energy Laser (THEL) used to demonstrate shoot down of rockets and artillery shells. All these systems were based on chemically driven lasers, which can provide output powers in the MW-range, but which pose serious problems related to size and logistics, as mentioned above. These programmes have therefore all been abandoned.

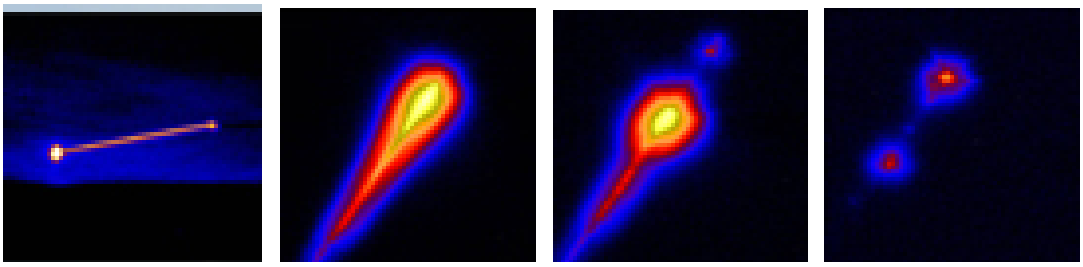

Figure 10.1 Photographs from the ABL shoot-down of a boosting ballistic missile on 11 February 2010. The image to the left shows scattered laser light from the beam path, and the other images are close-ups of the laser-illuminated target and its break-up after destruction (photos: Missile Defense Agency).

In recent years, emphasis has shifted towards development of electrically-powered solid-state lasers for laser weapons applications. Such lasers can be much more compact and practical in use than chemical lasers, and power levels of more than 100 kW have recently been achieved. This is still more than an order of magnitude below the power level of chemical lasers, but it is possible that this could be sufficient against many air targets and "soft" surface targets, at least at short range. An important task in this respect will be to establish detailed knowledge of the effects of laser weapons against the wide variety of possible targets and establish requirements for laser power and beam control. A successful further scaling of efficient and compact solid-state lasers would certainly open up for a wide use of this technology. A number of development programmes are underway, aiming at integrating such weapons on a variety of platforms, including aircraft, ships, and land vehicles. Best known among these are the High energy Laser Technology Demonstrator (HEL-TD) for land vehicles [122] and the Maritime Laser Demonstrator (MLD) for ships [123].

Figure 10.2 Illustration of the High Energy Laser Technology Demonstrator (source: Boeing).

10.2 New Types of Explosives and Warheads

Today, there is an ongoing search for new energetic materials. This development is expected to continue for several years. In this field the research and development may be divided into three categories:

- Explosives with better performance (i.e. higher energy density) than current explosives.
- Insensitive munitions (IM), i.e. munitions with good stability with respect to handling, transportation and storage.
- Green munitions, i.e. munitions with more environmentally friendly properties than current munitions with respect to production, handling, transportation, storage and disposal. In addition, health hazards originating from green munitions should be substantially lower than other munitions throughout its life cycle.

TNT was the first modern explosive. Later, nitramines like RDX and HMX were developed, and these are the explosives that are most widely used today. Several methods for synthesis of new energetic molecules have been attempted, but it seems like the cost of materials like CL-20 will be too high to be a major constituent in explosives, even though the production costs will decrease if larger quantities of such materials should be demanded. However, such high energetic materials may be used as an additive in future explosives for special purposes. There has been an interest in whether molecules like N8 (octa-nitrocubane) could be used as ingredients in explosives. N8 should be more energetic as well as more stable than HMX, but any large scale synthesis method of such materials is unlikely to occur within the next decade. Therefore, explosives with substantially better performance than today's materials should not be expected within the next few years.

Recently, several energetic materials have been synthesized for IM purposes. Two examples are FOX-7 and the even less sensitive FOX-12. The synthesis methods for these materials have been highly improved, and they are now produced in pilot plants.

The desired properties of explosives from the three categories above are partly contradictory. However, it is of great interest to develop IM and green munitions with as high energy as

possible. An IM example is nitramines (like RDX and HMX) with reduced sensitivity (RS-RDX, RS-HMX). It is most likely that such materials will be major ingredients in future explosives.

Less sophisticated explosives are also expected to be used during the next years. Widespread knowledge of how some easy available chemicals can be used in explosives may inspire individuals or groups to prepare and use so-called “home-made explosives” (HME). A common HME example is the TATP. This compound has slightly lower performance than e.g. TNT and is less stable. However, the simplicity of the making of this explosive may attract potential terrorists.

10.3 Biometrics

Authentication – claiming a proven identity – is divided into something you know, something you have and something you are, where biometrics is associated with the latter. Biometric characteristics can be divided into two types: Physiological and psychological. Physiological characteristics are measurable physical traits such as the shape of ones fingerprint, iris and face. Psychological characteristics are related to a person’s behaviour and include the voice, signature, gait and keyboard frequency. Another research area is cognitive biometrics, where brain signals are measured when a person see different colours, hear certain words etc. [124]. A large and unsolved problem is, however, what to do if ones biometric traits are lost or stolen. One possible solution is revocable biometrics [125].

Although there has been research on biometric systems for several years, it received increased attention after 11 September 2001, as well as after the International Civil Aviation Organization (ICAO) decided that all EU members should offer electronic passports capable of storing fingerprints, face and iris to its citizens [126]. They have also requested automatic border controls, where electronic gates capable of reading passports replace present border control agents. Such gates will be able to handle an increasing number of passengers without employing more agents. The gates will probably contain fingerprint and face recognition, and next generation iris scanners capable of reading from a distance [127].

Figure 10.3 Automated border control tested at Frankfurt Airport in 2009 (photo: Zimbio Inc.).

ABIS (Automated Biometric Identification System) is the name of the biometric infrastructure used by the US DoD, handling both personnel and operational biometrics. As of present, it is a standalone system with no interface to similar systems used by DHS (Department of Homeland Security) or FBI, but this will probably change in the future. There is also a demand for sharing data with UN and ISAF members. Before this is possible, a robust infrastructure is needed, probably where data are stored using cloud computing. As a scenario, 15 years in the future the soldier will probably be able to access ABIS whenever necessary regardless of operation, position and network interface, and he will employ a mobile phone capable of collecting and processing all biometric data necessary. NATO members will have their own ABIS system similar to the one used by the US, and the two infrastructures will share information seamlessly. They will also include future biometrics such as DNA and 3D face recognition. A next generation of ABIS was tested during the 2009 NATO CWIX exercise.

10.4 Inforensics Trends

BBC News, 5 October 2010: "A teenager has been jailed for 16 weeks after he refused to give police the password to his computer" [128]. Inforensics is methods and tools for accessing and analyzing data from digital systems, including computers, mobile phones and memory sticks. Inforensics is often used for collecting evidence for a trial. Therefore, data and the confiscated equipment should not be altered in any form during the data collecting process.

Today we see a clear trend that digital systems include security mechanisms, which makes inforensics harder. Encryption and access mechanisms in hardware or software are examples of security mechanisms. Sometimes these mechanisms can be circumvented by altering the equipment hosting the data. There is also a clear trend in relation to increasingly storing more data, e.g. location information and backup data. This makes the investigators job easier, but only after circumventing the security mechanisms. Storing more data in a secure manner may result in laws and regulations requiring data access for the governments. The lawful data access could e.g. be done via an USB port on a laptop [129].

Figure 10.4 A solution for extracting data from mobile phones (photo: Micro Systemation).

Inforensics in a military context is more about security than collecting evidence for a trial. After a cyber attack against military systems, inforensics may help answering the following questions: Which systems were attacked? Who was responsible for the attack? What was the intention of the attack? Which methods were used and which vulnerabilities were exploited? Is the attacker still present in the system? How can the system be useful and trusted again? Can this attack cause NATO to invoke Article 5 of the NATO Charter [130, 131]? The ability to answer these questions is important for implementing further military actions, and may require cooperation at a technical level with our allies.

Methods, systems, tools and knowledge in the field of military inforensics are today immature. This requires inforensics research and system development, as a consequence of the central role data systems have in the network centric military future. These systems will probably be available in a 5–10 year perspective, but the ability to integrate information from these systems into other military strategic, operational and tactical systems will take longer, probably 10–15 years.

10.5 Modelling, Simulation and Games Technologies

Over the last decade, a tremendous technology development in the area of modelling, simulation and games (M&SG) has taken place – a development that will continue in the coming years, partly because of the rapid development outside of the defence sector. M&SG technologies already play an ever more important role in support of military training and exercises and their use is also becoming more and more important in support of almost every conceivable defence process: defence analysis, concept development and experimentation, acquisition, test and evaluation of operational systems (of systems), mission rehearsal/mission specific training, and planning, execution and evaluation of operations. M&SG is at the brink of becoming ubiquitous.

The rapid development of defence M&SG is enabled by taking advantage of the technology advancements in civilian information and communication technologies. Developments in graphics processing units, high performance computing, network technology and software engineering have e.g. already dramatically changed the cost-performance ratio for training simulators by the exploitation of COTS hardware and software, moving away from proprietary, purpose-built components.

The increased availability of high resolution data of the physical natural and man-made environment makes it possible to generate synthetic environments which in great detail mirror the physical world. This trend, together with the development of tools to support the generation of high-resolution environment databases used for visual simulation, computer generated forces and sensor simulation, makes it possible to seamlessly blend the real and the synthetic worlds, blurring the distinction between the two. A networked blended environment of live forces (live simulation), simulators (virtual simulation) and computer generated forces (constructive simulation), so called LVC-simulation, has the potential to drastically change the way training and exercises are delivered and performed [132]. Training will be more realistic and widely available to a reduced cost. Other enabling technologies for such LVC-simulations are augmented reality and accurate positioning and attitude systems.

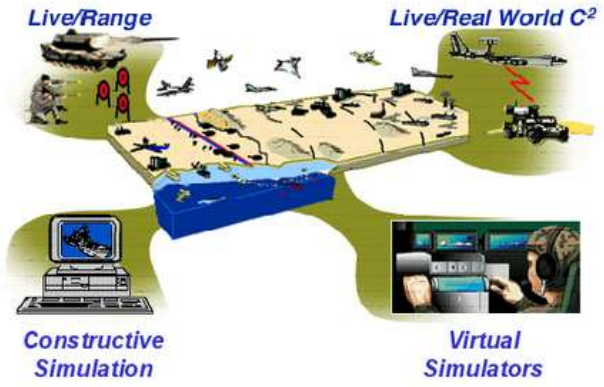

Figure 10.5 LVC Simulation (source: Calytrix technologies).

The most difficult problem to overcome to reach a fully mixed reality/synthetic battlespace is to incorporate computer generated human activities with plausible behaviour. Despite advancements in artificial intelligence technology and computational psychology and social science, the state-of-the-art within behavioural modelling and simulation has not changed significantly during the last decade and the field is still in its infancy. It is hard to predict how developments in this field will be in the next 10–15 years, but an educated guess is that we will only see small steps of advancements within specific, constrained domains. No general technology breakthrough will occur before an understanding of how the brain works is achieved, which quite possibly is the most difficult task humans have yet to undertake.

Both in NATO and nations, mixed reality battlespaces are in development and embryonic capabilities are in place. E.g. in NATO, the NATO LVC project is underway and NATO's long-term capability requirements and priority shortfall areas call for advanced distributed training with enhanced modelling and simulation.

10.6 Military and Security Applications of Terahertz (THz) Technology

Now that sources have become available that operate in the THz frequency domain (0.1–10 THz, 1 THz = 10^{12} Hz), a number of applications have surfaced that could be used in military and security-related operations. The most prominent applications are:

- Stand-off detection of explosives
- Detection of hidden objects through imaging
- Non-destructive testing/evaluation of materials

In stand-off detection of explosives, broadband (0.1–3 THz) radiation is used to measure either a transmission or, most likely, a reflection spectrum. Since most explosives have characteristic spectral absorption features, such spectra can be used to identify the specific explosive [133]. There are, however, challenges that need to be overcome before the technology can be deployed in the field. A severe problem is the damping of THz-radiation by water vapour in the atmosphere. In addition to decreasing the signal strength, absorption by water molecules adds features to the measured spectra, making analysis (detection and identification) more difficult. Another issue is the scattering of the THz radiation by surface roughness, curved surfaces, and materials

covering the explosive. Although THz-radiation is transmitted through common materials, such as paper, cardboard, plastic, and cloth, the weaving pattern of cloth could distort the spectral features. Development of more powerful sources and or more sensitive detectors will advance the technology readiness level. Whether a stand-off distance of e.g. 30 metres will be realized is presently hard to predict.

THz imaging applications are generally single frequency (narrow band) systems, whose frequencies are chosen to avoid the water absorption lines in the spectrum. Typically, the frequencies are limited to 600 GHz = 0.6 THz. The techniques used for source development are mainly based on radar technology. The difference is that, on the detector side, two-dimensional arrays are preferred to avoid scanning a single detector over the object, a process that is time consuming. Producing sensitive, un-cooled detectors is a challenge. One application of THz imaging is the scanning of packages and / or people at relatively short distances, less than one metre, to see if they contain or carry illegal or dangerous objects, such as concealed weapons. System development is ongoing and seems practical already now; cf. Figure 10.6, although it may compete with for instance back-scatter X-ray systems. TeraView and ThruVision are companies that specialize in THz-imaging systems.

De-lamination of composite materials that have been exposed to mechanical stress may be detected by using THz radiation. Aircraft that have undergone high g-force turns during a mission could be evaluated in this non-destructive way and without the precautions necessary for an X-ray scan. De-lamination causes empty spaces between layers, resulting locally in a changed dielectric constant. This change may be detected using THz radiation. Also, control of thickness of, for instance, a layer of paint could be performed with this technique.

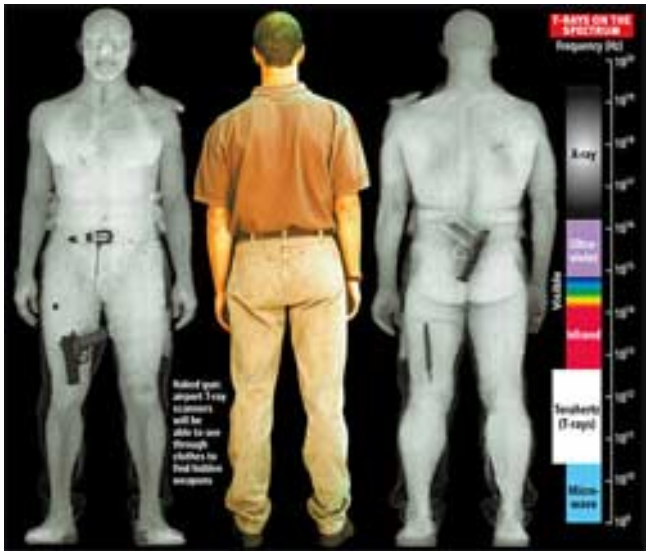

Figure 10.6 Man carrying weapons concealed by his clothes revealed by THz-scanning. (source: Homeland Security News Wire).

The challenge here is to account for all the contributions from a multi-layered structure. In addition, electrically conducting layers are excluded from this technique. Figure 10.7 illustrates

how THz radiation may be used in a non-destructive evaluation scheme to detect damage layered materials. This damage could be hidden under the surface.

Rather than looking at THz-systems as stand-alone systems, a suite of sensor capabilities that operate together is envisioned, each with its own strength, to detect and identify threats. This idea is relatively new and requires a careful evaluation of which sensor concepts would complement each other best. In addition, the issue of data fusion needs to be addressed.

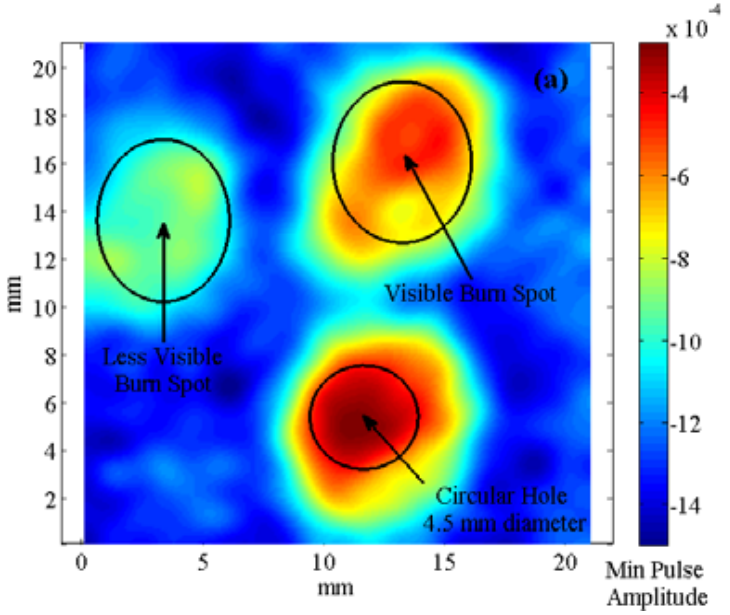

Figure 10.7 THz image of a glass fibre panel which has been damaged locally. These spots are clearly visible using non-destructive THz imaging (source: see [134])

10.7 Through-the-Wall Radar

Electromagnetic waves at optical frequencies cannot penetrate walls. Electromagnetic waves at lower frequencies can, however, penetrate materials. Frequencies lower than a few Megahertz can penetrate walls so that radars operating in this frequency range can look through them, so called Through-the-Wall (TTW) radar. The first use of penetrating radars was Ground Penetrating Radars (GPR). Some of the GPR systems have been converted and used as TTW radars. There are today several commercial TTW radars. Most of them operate at around two GHz. An example of a commercial handheld system from Cambridge Consultants is shown in Figure 10.8. This 5.7 kg product has been designed to operate with one or two hands and has a tripod mount for long term observation. The company claims that the waves are able to penetrate and find targets up to 20 meters away with a downrange resolution of 30 centimetres. Moreover, they claim that it has been proven to have an effective stand-off range of 10 metres. It has a field of view of 120º horizontal and 90º vertical.

Figure 10.8 Prim 200 TTW radar (photo: Cambridge Consultants).

Commercial radars today cannot give an image of the object behind a wall, but they can track movements inside a room like a person walking. The radars filter out everything that is not moving, effectively removing furniture and walls. This tracking can be done in 2D or 3D meaning that the height of the reflector is measured. Based on this, one can distinguish between whether a person is standing or kneeling. There are several potential improvements and a number of research groups are currently working on them. One expected enhancement is the possibility to detect respiration and heartbeats making it possible to detect persons in a room who are not necessarily moving around. By using synthetic aperture techniques, stand-off imaging of the interior of buildings is made possible. The radar is moving at a distance from the building and collects data over a certain distance. From these data a radar image is made and if the waves penetrate the walls an image of the interior is possible. Some reports claim that it is possible to classify corners and other objects based on polarimetric radar measurements. For an overview of the state of the art, see [135].

10.8 Speech Technology

Speech technology has found use – or is considered for use – in a broad range of application areas [136], also in the military domain [137]. Here we consider three broad application areas which have received particular attention from the international research community:

- Open-source intelligence (OSINT)
- Real-time speech-to-speech translation
- Human-machine interaction

The last decade has seen tremendous advances in the first two areas [138]. The driving force has been a huge increase in funding of large research programmes that develop speech technology tools for use in the “war on terror”. Such programmes typically have a twofold focus: The first is to improve core technologies such as:

- Speech recognition (what was said)

- Language and dialect recognition (what language and/or dialect was used)
- Speaker recognition (who spoke [when])
- Speech synthesis (text to speech)
- Spoken term detection (find occurrences of specified phrases)
- Text translation (text in one language to text in another language)

The second focus is to combine technologies into larger systems that can e.g. transcribe, annotate, index and translate speech content in various types of audio data. Based on new research programmes, we can expect further advances over the next few years (see e.g. [139]).

In terms of funding, the leading sponsor is DARPA. Their largest speech research programme to date is GALE (Global Autonomous Language Exploitation), which is [140]:

> "...developing computer software technologies to absorb, translate, analyze, and interpret huge volumes of speech and text in multiple languages. GALE automatic processing "engines" convert and distil the data, delivering pertinent, consolidated information in easy-to-understand forms to military personnel and monolingual English-speaking analysts in response to direct or implicit requests. GALE technology will automatically provide relevant, concise, actionable information to military command and personnel in a timely fashion."

GALE has a budget of several hundred million dollars, and centres on so-called "found" speech data, typically in the form of radio- and television broadcasts, telephone conversations, and multimedia from the internet. In the first phases of the programme the focus was on English, Mandarin and Arabic speech, while the focus in the current phase is on fast transfer of the technology to new languages. So far, the effort has resulted in several products for OSINT. One example is BBN Multimedia Monitoring System [141], which has been deployed in a number of US military units. Figure 10.9 shows a typical user's view from this system.

Figure 10.9 The BBN Broadcast Monitoring System shows transcriptions in both the original language and English with the synchronized video (source: Raytheon BBN Technologies).

A related DARPA programme is TRANSTAC (Spoken Language Communication and Translation System for Tactical Use) [140], which aims to develop technology for two-way speech-to-speech translation and communication in tactically relevant environments. One goal is that systems should handle free-form conversations on wide-ranging and quickly changing topics; another is that developing support for new languages should require less than 100 days. The purpose is to support military personnel in communication with foreign language speakers, thereby supporting increased situational awareness. An example of such a system is TransTalk from the BBN company [142].

In human-machine interaction, the potential of speech-based input and output for hands and eye free operation of systems (or subsystems) has been recognized for many decades, and there are numerous actual and potential military applications [136]. One of the most studied is speech input for control of non-critical functionality in combat aircraft. For example, speech control is now implemented in Eurofighter Typhoon, and announced for the rivals F-35 Lightning and Rafale. In aircraft, speech output is increasingly used to communicate various types of warnings to pilots. Other application areas of speech-based input and output of current interest include:

- Soldier systems
- Control stations for unmanned vehicles
- Medical information systems for field use
- Inspection, maintenance and repairs
- Battlefield management systems in combat vehicles

Successful use of speech-based input may be impeded by various contextual factors, such as acoustic noise from the environment, a need for thorough user training, or possible conflicts with cognitive processing of verbal information related to primary user tasks. Also, the design of speech-based input solutions requires a suitable and available speech recognition system for the language in question.

11 Conclusions

One of Norwegian Defence Research Establishment's (FFI) main tasks is to follow the scientific and military technology developments worldwide, and give advice to the military and political leadership regarding the future force structure and material procurement. This is achieved through analyses supporting long term defence planning, reports from FFI's many technologically oriented projects and through continuous consultation. FFI does occasionally present an over-view, in the form of a report, of the evolution and importance of military technology, one of which was the TEK14-report on trends in military technology trends published in 2004 [1]. The report was welcomed by the military community, but the technological advances since then have made it necessary with an update.

The present report is the result of this effort and should be regarded as an input to the long-term development of the Norwegian armed forces. It is not intended to give a complete overview of the

technology field, which is in practice impossible to do. Nevertheless, the report tries to describe the technological advances and challenges as fully as possible without going into too much detail.

In order to trace the development within key technology areas identified in this report, it is useful to start with the list of twelve central fields of research discussed in the previous report. Those were in random order:

1. Precision weapons against land targets, both from the air from the sea
2. The artillery revolution with guided munitions
3. Sensors against land targets such as synthetic aperture radar (SAR), GPS and combat ID systems
4. Remote control of weapons with man in the loop to control the delivery of fire
5. Lighter, but still well protected combat vehicles including additional armour or heavy armour but lighter ordnance
6. Small unmanned platforms supporting larger manned platforms both on land, in the air and in the maritime domain
7. The interaction between manned aircraft and big UAVs
8. Radiation weapons such as microwave weapons to destroy electronics and laser weapons for mine clearance and short-range air defence
9. Total asset visibility (TAV) combining logistics information with the status of platforms, systems etc.
10. Missile defence against ballistic missiles, including theatre ballistic missile defence
11. Stabilization operations and homeland defence with emphasis on protection, tracking and surveillance
12. Miniaturization leading to systems such as ball camera, small surveillance equipment, night-vision goggles, jamming equipment, BC sensors, targeting equipment etc that can be brought to the field by foot soldiers

All of these fields are more or less still of interest, but today they are in a more mature state. Technological and operational advance since the last report was published have basically been in the direction of *combining new technologies*. To illustrate this development, we take as an example progress within the area of unmanned platform systems. In recent years, attention has centred on applying them for new and more sophisticated operations in the battlefield, not so much on the development of the basic platform itself (with some important exceptions). Hence, various sensor systems, weapon systems and communication systems have been combined and implemented on many of these platforms, which is still the main current trend. With this in mind, the findings of this report are summarized in the following main technology areas and development trends:

a) *Dismounted soldier system.* The future soldier is a sensor in the field with a number of tasks and capabilities. These are lethality, survivability, sustainability, mobility and C4I. The soldier is equipped with more sensors and more CPU power in combination with rechargeable batteries with much higher capacity. New textiles applying nano-technology

will be available that can adapt to the environment (camouflage and climate). The soldier is integrated into a network with reach-back and surveillance capability.

b) *New fields of application for unmanned systems in the maritime, aerial and ground-based domains.* In the future, focus will be on the use of unmanned systems that can supplement as well as replace some of the older systems in service today. For Norway, there is a particular interest in maritime applications where unmanned underwater as well as surface vessels will be actively used for e.g. mine clearance, surveillance, decoys, communication etc.

c) *Space-based systems for intelligence, surveillance and target acquisition.* The use of space for military purposes is growing rapidly. In the future, space-based systems will be applied for a number of purposes. Amongst these is the traditional ISTAR capability as well as a number of new applications.

d) *Wide area surveillance underwater, on the surface and on land.* Many countries are today involved in the development of autonomous underwater surveillance systems that can be activated when needed. These can be deployed from surface vessels as well as AUVs. Sensor systems with a number of functionalities involving multispectral observations and magnetic, electric and acoustic detection capability is developed for use on land, e.g. for perimeter surveillance.

e) *Open architecture in combat systems.* A dominating trend within combat systems is to use standardized technology and an open architecture. Using off-the-shelf and affordable components leading to the reduced life-cycle costs by simplifying modifications, updates and upgrades.

f) *Force protection against irregular threats.* The increasing activity of pirates, criminals, guerrillas, terrorists etc has caused the international community to develop new and more sophisticated weapons in the less-than-lethal category. These weapons are developed to incapacitate personnel and to disable equipment.

g) *Rapid detection and new types of protection against biological and chemical agents.* New methods and sensors to identify BC threats at a distance as well as to categorize them in the laboratory are being developed. This will increase our ability to avoid or eliminate the potential threat of such weapons.

h) *Operations in the cyber domain.* The rapid development of computers and networks makes it possible for a potential enemy (country, group or individual) to affect or even destroy vital parts of our infrastructure, including military systems. Cyber warfare will be one of the biggest challenges in the future.

i) *Modelling, simulation and game technology*. During the last few years, a tremendous development has taken place within the gaming sector. This is driven mainly by the civilian sector, but the progress in this field will in the years to come play an increasing role also for military training and exercises. More realistic simulators will be developed, including virtual and augmented reality.

j) *Terahertz technology*. The development within this field will be utilized in applications such as stand-off detection of explosives, detection of hidden objects and testing/evaluation of new materials for various purposes.

We expect that these technology trends, as well as several others, will be central in the development of future forces. It remains, however, to be seen how far they will be developed and how soon systems and equipment will be employed by the military in real operations.

References

[1] B.Eggereide, T.Kråkenes, B.J.Meland, T-E.Schjelderup & T.Wahl, 2004, FFI-rapport 2004/03954, *TEK14: MILITÆRTEKNOLOGISKE TRENDER – Oversiktsrapport 2004 (in Norwegian)*

[2] G.A.Birkemo, H.E.Andås & S.O.Solheim, 2012, FFI-rapport 2012/02314, *Teknologitrender og konsekvenser for Forsvarets kapabilitetsutvikling (in Norwegian), Restricted.*

[3] *NORMANS (NORwegian Modular Network Soldier)*, Military Technology, 2009, Vol. 33, Issue 9, pp.83–85

[4] UK Defence Standardization (DStan), 2012, DEF STAN 23-12 Issue 05, DRAFT B, 7. February 2012, Unclassified, *Defence Standard 23-12 Generic Soldier Architecture*, www.mod.uk/DefenceInternet/AboutDefence/WhatWeDo/EquipmentandLogistics/dstan/

[5] C.Keith, G.Evenden, R.Lausund & L.E.Olsen, 2013, FFI-report 2013/0009, *NORMANS kompanisett week 44 – trial report*

[6] NATO NIAG, 2008, PFP(NIAG)D(2008)0006, PFP(NAAG-LCG/2)D(2008)0001, 6. October 2008, NATO/PFP Unclassified, *Final Report on NIAG SG-116 Study on Active Suspension Systems for Military Vehicles*

[7] P.Dalsjø, 2008, FFI-rapport 2008/01220, *Hybrid Electric Propulsion for Military Vehicles - Overview and status of technology*

[8] NATO RTO, 2012, RTO-TR-AVT-166, April 2012, NATO Unclassified, *Evaluation Criteria for Military Hybrid Electric Vehicles*, unpublished

[9] Kongsberg, 2011, *Protector Medium Calibre RWS*, www.kongsberg.com/en/kps/products/remoteweaponstation/protectormcrws/, accessed June 8, 2012

[10] Kongsberg, 2011, *PROTECTOR Javelin*, www.kongsberg.com/en/kps/products/remoteweaponstation/protectorjavelin/, accessed June 8, 2012

[11] ORBITAL VECTOR, 2007, *ETC WEAPONS*, www.orbitalvector.com/Tactical%20Weapons/ETC%20WEAPONS.htm

[12] GlobalSecurity, 2011, *Compact Kinetic Energy Missile (CKEM)*, www.globalsecurity.org/military/systems/munitions/ckem.htm, accessed June 8, 2012

[13] The Wireless Innovation Forum, 2012, *What is Software Defined Radio?*, www.wirelessinnovation.org/What_is_SDR, accessed June 8, 2012

[14] NATO NIAG, 2010, PFP(NIAG)D(2010)0007, PFP(NAAG-LCG/2)D(2010)0001, 12. July 2010, NATO/PFP Unclassified, *Final Report on NIAG SG-135 study on Auxiliary Power Units (APU's) for Military Vehicles*

[15] P.Myrick, 2010, *ATK Warhead Overview* , presentation at 8th Annual Future Artillery Conference, London, UK, March 26 2010.

[16] J.Kelly & M.Brennan, 2009, Land Warfare Studies Centre, Working Paper No. 134, *Distributed manoeuvre: 21st century offensive tactics*

[17] Army-technology.com, 2012, www.army-technology.com/news/newsdarpas-ls3-alphadog-begins-outdoor-testing/, accessed June, 2012

[18] *National Defense Authorization Act for Fiscal Year 2001*, Section 220, H.R. pp. 106–398, October 30, 2000. www.gpo.gov/fdsys/pkg/CRPT-106hrpt616/pdf, accessed January 18, 2013

[19] C.Jørgensen, N.Størkersen & J.Aas, 2009, FFI-rapport 2009/00607, *Framtidige AUV-kapasiteter i Forsvaret – veikart*

[20] R.Been, et al., 2007, NURC-PR-2007-011, *Multistatic Sonar: A Road to a maritime Network Enabled Capacity*

[21] R.Been, D.T.Hughes & A.Vermeij, UDT Glasgow, 2008, *Heterogonous Underwater Networks for ASW: Technologies and Techniques*

[22] R.Been, ASW Conference, London, 2009, *Cooperative ASW*

[23] J.Rice & D.Green, SENSORCOMM 2008 Cap Esterel, France: IEEE, pp. 715-722, 2008, *Underwater acoustic communications and networks for the US Navy Seaweb program*, in Proc. 2nd. Int. Conf. On Sensor Technologies and Applications

[24] M.Grund, L.Freitag, J.Preisig & K.Ball, Boston, MA, USA: IEEE, 2006, *The PLUSNet underwater communications system: Acoustic telemetry for undersea surveillance*, in Proc. MTS/IEEE Oceans 2006.

[25] R.Otnes, T.Jenserud, J.E.Voldhaug & C.Solberg, 2009, *A roadmap to ubiquitous underwater acoustic communications and networking*, in Proc. UAM 2009

[26] K.McCoy, B.Tomasi & G.Zappa, 2010, *JANUS: the genesis, propagation and use of an underwater standard*, in Proc. ECUA 2010

[27] L.Ødegaard & T.Jenserud, 2010, FFI-rapport 2010/00903, *Airborne multistatic sonar – a review*

[28] F.Ehlers, 2009, NURC-FR-2009-003, *NURC's Multistatic Sonar Project*, NATO UNCLASSIFIED, No Public Release

[29] F.Ehlers, 2009, NURC-FR-2009-001, *Final report on deployable multistatic sonar systems*, NATO UNCLASSIFIED, No Public Release

[30] NATO RTO, 2008, NURC-RTH-2008, *Research and Technology Highlights*

[31] P.Schuh et al., IEEE European Microwave Conference, 2010, *T/R-Module Technologies Today and Future Trends*

[32] C.Fulton et al., IEEE International Microwave Symposium, 2009, *A Digital Array Radar with Hierarchical System Architecture*

[33] F.Bandiera, D.Orlando & G.Ricci, Morgan and Claypool Publishers, 2009, *Advanced Radar Detection Schemes Under Mismatched Signal Models*

[34] J.Li & P.Stoica, Wiley-IEEE Press, 2008, *MIMO Radar Signal Processing*

[35] A.S.Zakartchenko, Y.N.Vinokurtsev & S.G.Troshkin, Naval Technology, 1994, *Russian naval mines development*

[36] G.J.Cornish, 2003, *US Naval Mine Warfare Strategy: Analysis of the Way Ahead*

[37] M.Hewish, Jane's International Defence Review, 2000, *Sea mines, simple but effective*

[38] W.Mason, MINWARA Spring Conference, 2009, *Mine warfare - home and away game challenges*, Breif on emerging Threats

[39] Jane's Underwater Warfare Systems, 2009, *Introduction to Mine Warfare*

[40] O.K.Svortdal, Norwegian Institute for Defence Studies, 2002, *Mineinnsats i sjøkrigen*

[41] National Defence Report Editing Committee, Ministry of National Defense (China), *2011 ROC National Defense Report*. www.andrewerickson.com/2011/08

[42] Guy Ferland: "The G2Chaff Algorithms", presentation at Naval Electronics Warfare Centre, Kiel, Germany, February 2010

[43] Janes, 2010, www.janes.com

[44] N.Friedman, 2005, *The Naval Institute Guide to world Naval weapon systems*, Fifth Edition

[45] United States Navy, 2010, http://www.navy.mil/navydata/cno/n87/usw/issue_32/antitorpedo.html, accessed desember 2010

[46] Splav, 2010, www.splav.org, accessed december 2010

[47] S.Skriudalen, O.Dullum, R.Rahimi, A.Skjold & J.Aas, 2010, FFI-notat 2010/01938, *Maritim styrkebeskyttelse - Våpenvirkninger og beskyttelsestiltak*, begrenset

[48] NATO Non-Lethal Weapons Policy Team, NATO, Brüssel, Belgia, 1999, C-M(99)44, Annex to AC/259-N/559, *Final Report*

[49] B.Buie, Presentation in Aegis Working Group meeting no 17, 3rd December 2010, *Aegis Open Architecture*

[50] Naval Technology, 2011, www.naval-technology.com/projects/littoral, accessed February 2011

[51] Federation of American Scientists, 2011, www.fas.org/sgp/crs/weapons/RL33741.pdf, accessed February 2011

[52] Naval Technology, 2011, www.naval-technology.com/projects/visby/, accessed February 2011

[53] The Royal Australian Navy, 2011, www.navy.gov.au/w/images/Semaphore_2010_4.pdf, accessed February 2011

[54] Jane's All the World's Aircraft, 2011, www.janes.com/products/janes/defence/air/all-the-worlds-aircraft.aspx

[55] Jane's International Defence Review, 2009, *Teaching old dogs new tricks: upgrades help B-52 bombers keep their relevance*

[56] MilitaryFactory ™, 2012, *Tupolev TU-160 (Blackjack) Stretegic Long-Range Bomber*, www.militaryfactory.com

[57] Airbus Military, 2012, *The versatile airlifter for the 21st Century*, www.airbusmilitary.com

[58] Jane's All the World's Aircraft, 2011, *Kamov Ka-50 Chernaya Akula*, www.janes.com/products/janes/defence/air/all-the-worlds-aircraft.aspx

[59] Heli-Expo 2011 Orlando Florida 06-03-2011 Press Release from Honeywell, USA, 2011, *Global Helicopter Purchases Expected to Increase*, www.honeywell.com/Pages/Home.aspx

[60] Boeing, 2012, *Small Diameter Bomb (SDB)*, www.boeing.com/defense-space/missiles/sdb/index.html, accessed May 31, 2012

[61] Raytheon Company, 2012, *Raytheon GBU-53/B Small Diameter Bomb II*, www.raytheon.com/capabilities/products/sdbii, accessed May 31, 2012

[62] Raytheon Company, 2012, *JSOW — Family of Precision Strike Weapons*, www.raytheon.com/capabilities/products/stellent/groups/public/documents/contents/cms01_055754.pdf, accessed May 31, 2012

[63] Jane's All the World's Aircraft, 2011, http://www4.janes.com/subscribe/jawa/doc_view.jsp?K2DocKey=/content1/janesdata/yb/jawa/jawa1193.htm@current&Prod_Name=JAWA&QueryText=%3CAND%3E%28%3COR%3E%28%28[86]ah-64+%3CIN%3E+body%29%2C+%28[106]+%28[106]ah-64+%3CIN%3E+title%29+%3CAND%3E+%28[106]ah-64+%3CIN%3E+body%29%29%29%29, accessed May 31, 2012

[64] Jane's Defence Weekly, 2012, *JAGM to see 'extended development' as budget is slashed*, www.janes.com/products/janes/defence-business/news/defence-weekly.aspx

[65] Defence Advanced Research Project Agency (DARPA), 2011, www.darpa.mil

[66] Albuquerque Kirtland Air Force Base, New Mexico, USA, 2011, www.kirtland.af.mil

[67] Boeing, 2011, *X51-A Waverider*, www.boeing.com/defence-space/military/waverider/docs/X-51A_overview.pdf, accessed July 2, 2012

[68] Defense Technical Information Center, 2006, *Affordable Weapon System*, www.dtic.mil/ndia/2006fuze/hubert.pdf, accessed May 31, 2012

[69] Jane's International Defence Review, 2009, *UK and France Join to develop helicopter-launched missile*

[70] Jane's International Defence Review, 2011, *Testing targets: Bridging the ASLM gap*

[71] Jane's International Defence Review, 2010, *US believes China is poised to field ballistic anti-ship missile*

[72] Lockheed Martin, 2011, *Joint Air-to-Ground Missile*, www.lockheedmartin.com/content/dam/lockheed/data/mfc/pc/jagm/mfc-jagm-pc.pdf, accessed May 31, 2012

[73] AolDefense, 2012, *JSF Survives, Global Hawk Dies, Global Strike Revives; Panetta's Budget*, http://defense.aol.com/2012/01/26/jsf-survives-global-hawk-dies-global-strike-revives-panetta-r/, accessed May 31, 2012

[74] Lockheed Martin, 2011, *Lockheed Martin Demonstrates JAGM Tri-Mode Seeker Against Moving Sea Targets in Captive Flight Test*, www.lockheedmartin.com/us/news/press-releases/2011/june/LockheedMartinDemonstrate.html, accessed May 31, 2012

[75] Jane's Air-Launched Weapons, 2011, *Meteor BVRAAM*, www.janes.com/products/janes/defence/air/air-launched-weapons.aspx

[76] Meteor missile on target for delivery this year, www.ainonlinecom/aviation-news/ain-defense-perspective/2013-03-22/, accessed January 29, 2013

[77] Jane's International Defence Review, 2007, *First successful NCADE flight trial proves key technology*, http://articles.janes.com/articles/International-Defence-Review-2008/First-successful-NCADE-flight-trial-proves-key-technology.html

[78] Space Foundation, Washington D.C., 2010, *The Space Report 2010*

[79] Nærings- og handelsdepartementet, 2009, *St.Prp. 1S 2009-2010*

[80] US Air Force, 2010, *Wideband Global Satcom (WGS)*, www.losangeles.af.mil/library/factsheets/factsheet_print.asp?fsID=5333&page=1, accessed December 20, 2010

[81] US Air Force, 2010, *Global Broadcast Service (GBS) joint program*, www.losangeles.af.mil/library/factsheets/factsheet_print.asp?fsID=7853&page=1, accessed December 20, 2010

[82] US Air Force, 2010, *Advanced Extremely High Frequency (AEHF) System*, www.losangeles.af.mil/library/factsheets/factsheet_print.asp?id=5319&page=1, accessed December 20, 2010

[83] GlobalSecurity, 2011, www.globalsecurity.org/space/systems/muos.htm

[84] S.Whitney, 2006, *Military Satellite Communications: Bridging to the Future*, Presentation DoD Commercial SATCOM Workshop

[85] US Department of Defense and the Office of National Intelligence, 2011, *National Security Space Strategy*, unclassified summary

[86] E.Enger, 2008, FFI-rapport 2008/00696, *South Africa's Nuclear Weapons Programme*

[87] A.Cohen, Columbia University Press, New York, 1998, *Israel and the Bomb*

[88] J.A.Tørnes, P.Prydz, J.R.Nilssen & B.Sagsveen, 2006, FFI-rapport 2006/02984, *Testing of Chemical, Atomic, and Toxic Compound Surveillance System – CATSS*

[89] G.Rustad, 2011, FFI-rapport 2011/01890, *Technologies for stand-off detection of liquid warfare agents*

[90] P.Aas, T.Myhrer & F.Heyerdahl, 2009, FFI-rapport 2009/01858, *Legemidler i supplerende medisinsk behandling ved nervegassforgiftning – aktuelle legemidler i beskyttelse av hjernen*

[91] J .M.Blatny & P.L.Lausund, 2012, FFI Focus no. 2, 2012, *The threat of Bioterrorism – Identifying the unknown*, www.ffi.no/no/Publikasjoner/Documents/FFI-Fokus_nr2_2012_Bio_web.pdf

[92] G.Rustad, 2008, FFI-rapport 2008/02025, *Stand-off detection of biological aerosols by UV-laser induced fluorescence*

[93] T.Tjarnhage, P.Jonnson, J .M.Blatny, G.Skogan & T.Humppi, 2011, NORDEFCO Report FOI-R-3267-SE (2011), *Detection of Airborne Biological Agents*

[94] M.Dybwad, P.E.Granum, P.Bruheim & J .M.Blatny, 2012, *Microbiological Characterization Of The Bioaerosol Environment At An Underground Subway Station*, Appl. Enviiron. Microbiol., 78(6):1917 (2012)

[95] R.Gates, 2011, *Memorandum from US DoD on Strategic Communication and Information Operations in the DoD*, 25.01.11

[96] MC64/10, 2008, *NATO Electronic Warfare (EW) Policy*

[97] Boeing, 2011, www.boeing.com/defense-space/military/ea18g/index.html, accessed February 3, 2011

[98] US Navy Naval Air Systems Command, 2011, *Next Generation Jammer Technology Maturation Studies Broad Agency Announcement*, www.navair.navy.mil/doing_business/open_solicitations/N00019-08-R0101/NGJ_BAA_Industry_Day_-_Final.pdf, accessed February 4, 2011

[99] G.Cowart & T.C.Moss, Aircraft Survivability Magazine Spring 2003 ed, pp 17-19, 2003, *Aiding Aircraft Survivability*, www.bahdayton.com/surviac/asnews/as_spring2003.pdf, accessed February 4, 2011

[100] Raytheon News release Feb 18, 2010, www.raytheon.mediaroom.com/index.php?s=43&item=250&pagetemplate=release, accessed February 4, 2011

[101] K.Pelechrinis, M.Iliofotou & S.V.Krishnamurthy, IEEE Communications Surveys and Tutorials, 2010, *Denial of Service Attacks in Wireless Networks: The Case of Jammers*

[102] J.Mietzner, P.Nickel & A.Meusling, The 2010 Military Communications Conference (MILCOM2010), 2010, *Jam-Duration Optimization for Responsive Vehicle-Protection Jammers*

[103] R.Janka, SDR'10 Technical Conference and Product Exposition, 2010, *Applying Cognetive Radio Concepts to Next Generation Electronic Warfare*

[104] Department of the Air Force, 2010, *Cognitive Jammer, RFI-PKS-001-2010*, www.fbo.gov, accessed January 20, 2010

[105] NATO STANAG 4621, 2011, *Navigation Warfare Definition*

[106] G.B.Lavezzi, 2010, *Possible Futures: Space Capability Risk and the Joint Force*, Master of Strategic Studies Thesis

[107] P.Papadimitratos & A.Jovanovic, IWSSC 2008, IEEE, 2008, *Protection and Vulnerabilities of GNSS*

[108] BAe Systems, 2011, AN/ALQ-214 IDECM RFCM, www.baesystems.com/BAEProd/groups/public/documents/bae_publications/bae_pdf_eis_idecm.pdf, accessed February 16, 2011

[109] G.Goodman, The Hournal of Electronic Defence, September 2009, Vol.32, No.9, 2009, *Defeating threats to large aircraft*

[110] SAAB, 2011, *Pilot LPI Radar description*, www.saabgroup.com, accessed January 30, 2011

[111] Simrad, 2011, *Simrad broadband Radar description*, www.simrad-yachting.com, accessed January 20, 2011

[112] Army Times, 2011, www.armytimes.com/news/2010/12/army-smart-phones-for-soldiers-121210w/, accessed December 12, 2010

[113] Wikipedia, 2011, http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia

[114] Information about MIP, 2011, https://mipsite.lsec.dnd.ca

[115] E.Lasschuyt etal., 2010, *Final Report of the NATO RTO IST-084 RTG-040 Working Group on the Domain-based Approach for Coalition-wide Information Exchange – Proof of Concept*

[116] S.Carey, M.Kleiner, M.Hieb & R.Brown, Fall Simulation Interoperability Workshop, Orlando, FL, 9.-14. September 2001, 2001, 01F-SIW-067, *Standardizing Battle Management Language - A Vital Move Towards the Army Transformation*

[117] NATO RTO, 2010, RTO-TR-MSG-048, *Modelling & Simulation Group 048 (C-BML) Technical Activity Final Report*, currently undertaking release process

[118] SISO, 2006, SISO-REF-016-2006-V1.0, *Coalition Battle Management (C-BML) Study Group Final Report*

[119] K.Stenersen, 2010, FFI-rapport 2010/00296, *Laser Weapons – Recent Developments*

[120] Technology and Logistics Office of the Undersecretary of Defense For Acquisition, 2007, 20301-3140, *Report issued by the Defense Science Board Task Force on Directed Energy Weapons*, www.acq.osd.mil/dsb/reports/ADA476320.pdf

[121] Missile Defense Agency, 2010, www.mda.mil/news/10news0002.html , accessed March 2, 2012

[122] Boeing, 2010, www.boeing.com/Features/2010/07/bds_feat_light_truck_07_26_10.html

[123] Northrop Grumman, 2011, www.as.northropgrumman.com/products/maritime_laser/assets/MLD_Datasheet.pdf

[124] Articlesbase, 2011, www.articlesbase.com/internet-law-articles/biometrics-542068.html

[125] The TURBINE Project, 2011, www.turbine-project.eu/

[126] Hasbrouck, 2011, http://hasbrouck.org/documents/ICA09303-pt1-vol2.pdf

[127] Technovelgy, 2011, www.technovelgy.com/ct/Science-Fiction-News.asp?NewsNum=930

[128] BBC, 2011, www.bbc.co.uk/news/uk-england-11479831

[129] Microsoft, 2011, www.microsoft.com/industry/government/solutions/cofee/default.aspx

[130] NATO, 2011, www.nato.int/cps/en/natolive/official_texts_17120.htm

[131] Online.no, 2010, www.online.no/sikkerhet/trygg_paa_nett/ruster_seg_til_cyberkrig.jsp

[132] A.Henninger et al., 2008, *Live Virtual Constructive Architecture Roadmap (LVCAR)*, Final Report, Institute for Defense Analyses, September 2008

[133] C.Konek, J.Wilkinson, O.Esenturk, E.Heilweil & M.Kemp, 2009, *Terahertz Spectroscopy of Explosives and Simulants - RDX, PETN, Sugar and L-Tartaric Acid*, in Proc. of SPIE, Vol. 7311 (2009)

[134] C.D.Stoik, 2008, *Nondestructive Evaluation of Aircraft Composites Using Terahertz Time Domain Spectroscopy*, Doctoral Thesis, Department of the Air Force Air University, *Air Force Institute of technology*, Wright-Patterson Air Force Base, Ohio, USA

[135] M.G.Amin (ed.), 2010, ISBN-10: 1439814767, *Through-the-Wall Radar Imaging*, CRC Press; 1.edition

[136] X.Huang, A.Acero & H.-W.Hon, Prentice-Hall, Upper Saddle River, NJ, USA, 2001, *Spoken language processing*

[137] S.Pigeon et al., NATO Research & Technology Organization, France, 2005, RTO-TR-IST-037, *Use of speech and language technology in military enviroments*, http://ftp.rta.nato.int/PubFullText/RTO/TR/RTO-TR-IST-037/TR-IST-037-$$ALL.pdf

[138] Defence Advanced Research Project Agency (DARPA), 2011, www.darpa.mil/WorkArea/DownloadAsset.aspx?id=2676

[139] IARPA, 2011, www.iarpa.gov/solicitations_babel.html

[140] Defence Advanced Research Project Agency (DARPA), 2011, www.darpa.mil/Our_Work/I2O/Programs/

[141] BBN Technologies, 2011, www.bbn.com/products_and_services/multimedia_monitoring_system/

[142] BBN Technologies, 2011, www.bbn.com/products_and_services/transtalk/

List of Acronyms

ABIS	Automated Biometric Identification System
ABL	Airborne Laser
AGL	Automatic Grenade Launcher
AIP	Air Independent Propulsion
AIS	Automatic Identification System
AMRAAM	Advanced Medium Range Air to Air Missile
ANNC	Anglo Netherlands Norwegian Collaboration
APS	Active Protection System
APU	Auxiliary Power Units
AR	Augmented Reality
ASW	Anti-Submarine Warfare
ATL	Advanced Tactical Laser
ATT	Anti Torpedo Torpedo
AUV	Autonomous Underwater Vehicle
BAMS	Broad Area Air Surveillance
BASIC	Broad Area Space-based Imagery Collector
BDU	Battle Dress Uniform
BML	Battle Management Language
BMS	Battlefield Management System
BVR	Beyond Visual Range
CBRN	Chemical, Biological, Radiological and Nuclear
CCF	Course-Correction Fuses
CDC	Centers for Disease Control and Prevention
CESWG	Core Enterprise Services Working Group
CFA	Cross-Field Amplifier
CKEM	Compact Kinetic Energy Missile
CMS	Combat Management System
CNO	Computer Network Operations
CNR	Combat Net Radios
COM-EW	Communication-Electronic Warfare
COMS	Communication Security
CPGS	Conventional Prompt Global Strike
CPU	Central Processing Unit
CRAM	Counter Rocket, Artillery and Mortar
C-RC-IED	Counter-Radio controlled-Improvised Explosive Devices
CROWS	Common Remotely Operated Weapon Station
CSM	Conventional Strike Missile
CWC	Chemical Weapons Convention
DARPA	Defense Advanced Research Project Agency
DEW	Directed Energy Weapon
DICASS	Directional Command Activated Sonobuoy System
DIRCM	Directed Infrared Counter Measures
DMSP	Defense Meteorological Support Program
DRFM	Digital Radio Frequency Memory
DRFM	Digital RF Memory
DSCS	Defense Satellite Communication System
EA	Electronic Attack
EAL	Evaluation Assurance Level
EBEM	Enhanced Bandwidth Efficient Modem
ECCM	Electronic Counter-Counter Measures
ED	Electronic Defence
EDW	Expendable Disposal Weapon
EO	Electro optic
EOB	Electronic Order of Battle

EOD	Explosive Ordnance Disposal
EP	Electronic Protection
EPS	Enhanced Polar System
ES	Electronic Surveillance
ESA	European Space Agency
ESM	Electronic Support Measures
ESSM	Evolved Sea Sparrow Missile
ETC	Electro Thermal Chemical
FAC	Forward Air Controller
FC	Fuel Cell
FCS	Future Combat Systems
FIA	Future Imagery Architecture
FPGA	Field Programmable Gate Arrays
GALE	Global Autonomous Language Exploitation
GaN	Gallium Nitride
GBS	Global Broadcast Service
GLRT	Generalized Likelihood Ratio Testing
GNSS	Global Navigation Satellite System
GOA	Generic Open Architecture
GPR	Ground Penetrating Radar
GPS	Global Positioning System
HALE	High Altitude Long Endurance
HK	Hard-Kill
HME	Home-made Explosives
HPDE	High Density Polyethylene
HVM	Hyper Velocity Missile
IAIA	International Atomic Energy Agency
ICAO	International Civil Aviation Organization
IED	Improvised Explosive Device
IFF	Identification Friend or Foe
IM	Insensitive Munitions
IMINT	Imagery Intelligence
IMU	Inertial Measurement Unit
ISN	Institute for Soldier Nanotechnologies
ISR	Intelligence, Surveillance and Reconnaissance
JAGM	Joint Air to Ground Missile
JC3IEDM	Joint Consultation, Command and Control Information Exchange Data Program
JDRADM	Joint Dual Role Air Dominance Missile
JSM	Joint Strike Missile
LCS	Littoral Combat Ship
LIDAR	Laser – Radar
LRAD	Long Range Acoustic Device
LLW	Less Lethal Weapons
LS3	Legged Squad Support System
MALD	Miniaturized Air Launched Decoy
MALE	Medium Altitude Long Endurance
MANET	Mobile Ad-hoc Network
MAWS	Missile Approach Warning System
MCM	Mine Counter Measures
MEADS	Medium Extended Air Defense System
METOC	Meteorology/Oceanography
MIMO	Multiple Input Multiple Output
MIP	Multilateral Interoperability Program
MLD	Maritime Laser Demonstrator

MLRS	Multiple Launch Rocket System
MLS	Multi Level Secure
MMIC	Monolithic Microwave Integrated Circuit
MOAB	Massive Ordnance Air Blast
MPA	Maritime Patrol Aircraft
MTBF	Mean Time Between Failures
MTW	Mini Torpedo Welcome
MUOS	Mobile User Objective System
NAVWAR	Navigation Warfare
NBWF	Narrowband Waveform
NCADE	Network Centric Airborne Defense
NEC	Network Enabled Capabilities
NGJ	Next Generation Jammer
NORDEFCO	Nordic Defence Cooperation
NORMANS	Norwegian Modular Arctic Network Soldier
NPT	Non Proliferation Treaty
NSM	Naval Strike Missile
OCV	Offshore Combatant Vessel
OP	Observation Post
ORS	Operationally Responsive Space
PCR	Polymerase Chain Reaction
PNT	Position Navigation and Time
POES	Polar Operational Environmental Satellites
PRS	Public Regulated Service
PSS	Passive Sonar System
QoS	Quality of Service
RACUN	Robust Acoustic Communications in Underwater Networks
RAM	Rolling Airframe Missile
RC-IED	Radio Control Improvised Explosive Device
RCS	Radar Cross Section
RDD	Radiological Dispersion Device
REA	Rapid Environment Assessment
RFI	Request For Information
RoE	Rules of Engagement
RPG	Rocket Propelled Grenade
RWS	Remote Weapons Station
SA	Situational Awareness
SAS	Synthetic Aperture Sonar
SDB	Small Diameter Bomb
SDR	Software Defined Radios
SFW	Sensor Fused Warhead
SIGINT	Signal Intelligence
SIJ	Stand In Jammer
SJ	Support Jamming
SK	Soft Kill
SOA	Service Oriented Architecture
SSA	Space Situational Awareness
STAP	Space Time Adaptive Processing
START	Strategic Arms Reduction Treaty
SWIFT	Sub-millimeter Wave Imaging Fuse Technology
TBM	Tactical Ballistic System
THAAD	Terminal High Altitude Air Defense
THEL	Tactical High Energy Laser
TSAT	Transformational Satellite
TTP	Tactics, Techniques and Procedures

TTW	Through-the-wall
TWT	Traveling Wave Tube
UAS	Unmanned Aircraft System
UAV	Unmanned Air Vehicle
UCAS	Unmanned Combat Air System
UFO	UHF Follow-on
UGV	Unmanned Ground Vehicle
USMC	US Marine Corps
USV	Unmanned Surface Vehicle
WGS	Wide Band Gap Filler System
WGS	Wideband Global SATCOM