Technology Forecast 2016: The Military Utility of Future Technologies

- A Report from seminars at the Swedish Defence University's Military-Technology Division.

Summary

Three technology forecast reports from the Fraunhofer Institute and four reports on literature studies (sometimes called scanning reports) from the Swedish Defence Research Institute (FOI) have been reviewed by staff at the Military-Technology Division at the Swedish Defence University (SEDU). The task given by the Defence Material Administration FMV was to assess the military utility of the given technologies in a time frame to 2040, from a Swedish Armed Forces (SwAF) point of view.

In the review we assess the **military utility of a certain technology** as a possible contribution to the operational capabilities of the SwAF, based on identified relevant scenarios. Since a new capability catalogue is under development at the SwAF Headquarters, this report will only present general assessments of the capability impact from the technologies under study.

The technologies were grouped into four classes: potentially significant, moderate, negligible, or uncertain military utility.

The following technology was assessed to have a potential for **significant** military utility;

- Multi robot systems

The following technologies were assessed to have a potential for **moderate** military utility;

- Over-the-Horizon Radar
- Space-based imaging radar

The following technology was found to have **negligible** military utility.

- Moving Target Defence

The following technologies were assessed to have **uncertain** military utility;

- Software-Defined Networking
- Transient Materials- Programmed to Perish, but this technology should be monitored since it might reach high technical readiness level (TRL) by 2050-60

The method used in this technology forecast report was to assign each report to one reviewer in the working group. First, a summary of each forecast report was made. The Fraunhofer assessment of TRL in the time period to 2035 was held to be correct. The technology was then put into one or more scenarios that were deemed to be suitable in order to assess the military utility as well as indicate possibilities and drawbacks of each technology. Based on a SWOT-analysis, the assessed contribution to the fundamental capabilities and to the factors DOTMPLFI (Doctrine, Organization, Training, Materiel, Personnel, Leadership, Facilities and Interoperability) were listed. Furthermore, the expected requirements on the SwAF R&D in order to facilitate the introduction of the technology are given.

As a consequence of our continuing development of the evaluation process, we have for the first time used a model developed at the division of Military-Technology to assess the

Military utility[1] of the technologies. Finally, conclusions and an overall rating regarding the potential military utility of each technology were presented.

The chosen definition of military utility clearly affects the result of the study. The definition (the military utility of a certain technology is its contribution to the operational capabilities of the SwAF, within identified relevant scenarios) is the same as used in our Technology Forecasts since 2013.

Our evaluation of the method used shows that there is a risk that the assessment is biased by the participating experts' presumptions and experiences from their own field of research. Also, it should be stressed that the six technologies' potential military utility was assessed within the specific presented scenarios, and their possible contribution to operational capabilities within those scenarios, not in general. When additional results have been found in the analysis this is mentioned. The last chapter of this report analyzes thinking and debate on war and warfare in three military great powers: USA, Russia and China. Therefore, this chapter has a different structure. Aspects of military technology are discussed at the end of the chapter, but no assessment of the military utility is made.

The greatest value of the method used is its simplicity, cost effectiveness and that it promotes learning within the working group. The composition of the working group and the methodology used is believed to provide a broad and balanced coverage of the technologies under study. This report is to been seen as an executive summary of the Fraunhofer reports and the reports on literature studies from FOI. The intention is to help the SwAF Headquarters to evaluate the military utility of emerging technologies within identified relevant scenarios.

Overall, the quality of the Fraunhofer reports is considered to be balanced and of a high level of critical analysis regarding technology development. These reports are in line with our task to evaluate the military utility of the emerging technologies. The FOI reports are considered to be high quality. However, the selection of topics can be discussed since the selection criteria are not transparent. Some reports also lack an explicit military perspective.

Table of contents

[1] K. Andersson et al, Military utility: A proposed concept to support decision-making, Technology in Society, 43, 2015.

Introduction

Scope

This report is the result of a review of three technology forecast reports from the Fraunhofer Institute and four scanning reports from the Swedish Defence Research Institute (FOI). The review has been carried out at the Swedish Defence University by staff at the Military-Technology Division, commissioned by the Swedish Defence Materiel Administration, FMV. The task was to assess the military utility of the different technologies in a time frame to 2040.

The review and evaluation of each technology form one chapter in this report.

References

The following reports, composed for FMV at the Fraunhofer Institute and FOI, were reviewed:

[1] Software-Defined Networking, Fraunhofer INT, January 2016

[2] Transient Materials – Programmed to Perish, Fraunhofer INT, February 2016

[3] Multi robot systems, Fraunhofer INT, April 2016

[4] Over-the-Horizon Radar, FOI, December 2014

[5] Moving Target Defence, FOI, September 2014

[6] Space-based imaging radar, FOI, December 2015

[7] Örnen, Björnen och Draken, militärt tänkande i tre stormakter, FOI, September 2015

Some of the reports were reviewed in Swedish.

Definitions

In this report **military utility of a certain technology** is defined as the technology’s contribution to the operational capabilities of the SwAF, within identified scenarios.

Method

The method consists of four steps chosen in order to be efficient and takes advantage of the professional expertise of the reviewer.

Step 1: The reports are assigned to the participants of the working group, on the basis of their special expertise and interest. Each reviewer is responsible for reviewing one report.

The reviewer writes a summary of the report and defines one (or more) tentative military technical system and puts it in a possible scenario for the Swedish Armed Forces in the timeframe of 2040. The purpose of the scenario is to illustrate the utility of the technology and to put the described reported technology forecast in to a relevant context.

Step 2: Each review is discussed at a seminar. At the seminar the technology is briefly introduced, the technical system concept and the scenario are presented. The reviewer’s role is to be an advocate of the military utility of the specific technology in the scenario developed. The other participants’ role is to support or criticize the concept.

In the seminar the technology is analyzed by conducting:

- a SWOT-analysis,
- an assessment of the technology’s contribution to the fundamental capabilities,
- an analysis of the technology’s military utility, see below,
- an assessment of its contribution to DOTMPLFI (Doctrine, Organization, Training, Materiel, Personnel, Leadership, Facilities and Interoperability), and
- an analysis of the requirements that can be expected of SwAF R&D in order to facilitate the introduction of the technology.

The military utility is assessed using the model developed by Andersson et al., se figure 1.

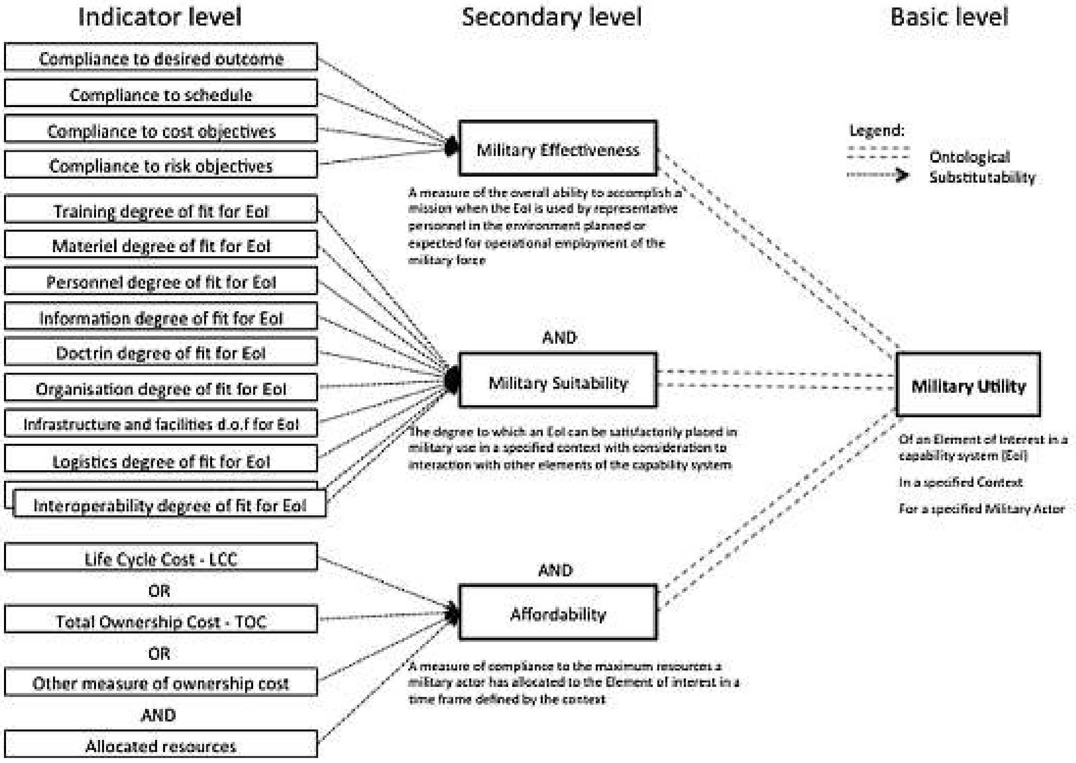

Indicator level
Secondary level
Basic level
Compliance to desired outcome
Compliance to schedule
Compliance to cost objectives
Compliance to risk objectives
Training degree of fit for EoI
Materiel degree of fit for EoI
Personnel degree of fit for EoI
Information degree of fit for EoI
Doctrin degree of fit for EoI
Organisation degree of fit for EoI
Infrastructure and facilities d.o.f for EoI
Logistics degree of fit for EoI
Interoperability degree of fit for EoI
Life Cycle Cost - LCC
OR
Total Ownership Cost - TOC
OR
Other measure of ownership cost
AND
Allocated resources
Military Effectiveness
A measure of the overall ability to accomplish a mission when the EoI is used by representative personnel in the environment planned or expected for operational employment of the military force
AND
Military Suitability
The degree to which an EoI can be satisfactorily placed in military use in a specified context with consideration to interaction with other elements of the capability system
AND
Affordability
A measure of compliance to the maximum resources a military actor has allocated to the Element of interest in a time frame defined by the context
Legend:
Ontological
Substitutability
Military Utility
Of an Element of Interest in a capability system (EoI)
In a specified Context
For a specified Military Actor

Figure 1. Military Utility consists of Military Effectiveness, Military Suitability and Affordability. Source: K. Andersson et al, *Military utility: A proposed concept to support decision-making*, Technology in Society 43, 2015. In the concept the object for the assessment is an element in the capability system, labelled the Element of Interest (EoI). LCC is the Life Cycle Cost. TOC is the Total Ownership Cost.

Step 3: The result of the seminar is documented and conclusions on the potential for military utility of the technology are drawn, using the Delphi method.

The last chapter of this report has a different character; therefore no assessment of the military utility is made.

The composition of the working group

The working group consisted of experts from the military-technology faculty at SEDU:

Stefan Silfverskiöld, Cdr (N), Assistant Professor of Military-Technology, project manager

Hans Liwång, Assistant Professor of Military-Technology, deputy project manager

Gunnar Hult, Chaired Professor of Military-Technology

Peter Bull, Associate Professor of Military-Technology

Björn Persson, PhD

Ola Thunqvist, Cdr (N)

Johan Sigholm, Maj (AF), MSc

Peter Sturesson, Capt (AF), MSc

Software-Defined Networking

Ref: [1] Referee: Johan Sigholm

Introduction

Software-Defined Networking (SDN) is a virtualization-based network architecture concept that aims to simplify network configuration and management by decoupling control functions from the operating system in a network device, leaving it to merely handle forwarding of data packets. The network intelligence is instead gathered in the SDN controller, which can be distributed over several physical systems.

SDN network architecture allows for an efficient, responsive and scalable network, where central monitoring, policy decisions, and optimization can be done based on a bird's-eye view of the network. An SDN-based network can be programmed via standardized application programming interfaces (APIs), making it easy to reconfigure the network without changing the underlying network hardware.

Military applications of SDN technology mentioned in the report include systems for Network Centric Warfare, secure computing and efficient transferring of sensor data. By simplifying the design and management of military networks, they may become more flexible in adjusting to operational requirements. Moreover, SDN technology could increase datacenter efficiency with respect to energy consumption, interoperability and network security.

Identified possibilities and constraints

Advantages

- Simplified network control and management
- Increased network security through common configuration
- Reduced energy consumption

Disadvantages

- Requires new network equipment
- Security concerns, possible SDN controller or Denial of Service attacks

Assumptions

The concept scenarios are based on the following assumptions.

- Subsystems based SDN-technology are available on the market

Suggested military use

The following applications are mentioned in the report:

1. Systems for Network Centric Warfare, adjustable to operational requirements
2. Reinforcing network security
3. Efficient sensor data distribution with reduced energy consumption

Concept scenarios in 2025

As the SDN technology has already reached a high level of maturity (TRL levels up to 9 as of today), the two scenarios presented below are set in a 2025 timeframe.

Scenario 1: SDN-based network in a military platform

Most military platforms, such as aircraft, armored fighting vehicles and navy vessels, contain computer networks used to collect, process and disseminate data. In this scenario, the computer network of a fighter aircraft is considered, where the traditional configuration is replaced by an SDN-based architecture. The aircraft needs to be able to collect large amounts of data from its various sensors, in a time-critical manner, and distribute that data to the recipient systems. Hostile weapons fire or jamming may cause disruption in the network, requiring high levels of over-provisioning and redundancy. At the same time, only a fraction of the available resources are commonly used. The possibility to make use of unused computing power in a given component could thus increase the performance of another component.

Scenario 2: SDN technology used in data centers or in the Swedish Armed Forces' IP Network

Besides such networks as those described in the scenario above, the Swedish Armed Forces also has a substantial digital supporting infrastructure, carrying data in the sensor chain, maintaining intra-forces communications, and supporting ordinary office computer use and logistics services. This infrastructure contains data centers, server farms, and Internet Protocol (IP) networks using commercially-procured technology and components. Data centers with servers and network elements could make use of SDN technology to allow for network virtualization, increased network security through common configuration, a higher degree of component interoperability, and reduced energy consumption.

SWOT-analysis

The following strengths, weaknesses, opportunities and threats with the SDN technology within the scenarios were identified at the seminar:

Strengths:

- The network will be cheaper to design and procure as the components become more generic, requirements are similar for components, interference between components could be reduced and over-provisioning of components could be reduced
- Resources may be reallocated on demand, such as in increase of calculation resources or extra bandwidth
- Possibility to reduce weight and volume of system components
- Reduces energy consumption
- Increased robustness; network reconfiguration in case of damage
- Reduced development costs as the commercial market moves towards SDN and thus R&D costs may be shared
- Modular hardware results in reduced costs for maintenance and education of technicians
- Identification and mitigation of malware, cyberattacks, and malfunctioning components is easier in a homogeneous network environment
- Decision support systems may be enhanced by using resources from several components

Weaknesses:

- SDN controller may be attacked, or disabled through unintentional interference, resulting in an impaired or non-functional network
- Network robustness may be reduced in comparison to over-provisioned network
- Configuration management required as updates may cause problems in the network
- Restarting the SDN controller could take a longer time if it is more complex
- Design of SDN controller becomes challenging as it needs to be done for the specific platform (implies higher TRL)

Opportunities:

- Possibility to reuse SDN-network equipment as operational requirements evolve
- Support of sensor fusion and Network Centric Warfare

Threats:

- Compromise of SDN controller by adversary through cyber attack
- Consequences of successful cyberattack on the SDN network could be more serious, affecting the entire network and possibly spreading to platforms in other arenas
- SDN network could be susceptible to specially-crafted Denial of Service attacks
- Current research and development within SDN technology is focused on civilian applications, mainly for use in large computer centers, which could reduce the military utility
- Assuming that all resources are not needed all the time is a risk

Assessed capability impact

SDN-based networks will primarily have an impact on maintenance, command and control, and intelligence.

Assessment of Military Utility

In regards to the first scenario, the military effects of implementing SDN technology could be significant. However, as networks in military platforms already tend to be very specifically designed, it is unlikely that this technology could be implemented “off the shelf,” but would rather need to be refined and modified to suit the needs of the specific military implementation and thus be applicable in the given scenario. Even though the technology is considered to have a high Technology Readiness Level (up to TRL 9 in a 2025 perspective), the fact that current research and development within SDN technology is primarily focused on civilian use in large computer centers, makes the military utility offered by SDN in the first scenario uncertain.

Nevertheless, as presented in the second scenario, the Swedish Armed Forces has a large amount of supporting infrastructure using commercial computer systems, where the suitability of SDN technology is high. As network design for such commercial networks is expected to be based on SDN in a 2025 perspective, and the military specific costs associated with the technology are low, the resulting affordability of implementing SDN will be high. However, the possible security risks associated with SDN, and the possibility that vendors relying on sales of proprietary networking hardware may be reluctant to support SDN, results in an uncertain level of military utility in the second scenario.

Footprint/cost 2025

The following list is a compilation of anticipated footprints created by the use of SDN technology to the factors DOTMPLFI (Doctrine, Organization, Training, Materiel, Personnel, Leadership, Facilities and Interoperability) as well as the expected requirements on the SwAF R&D in order to facilitate the introduction of the technology.

Item	**Comment**
Doctrine	-
Organization	-
Training	Training requirements may be greater as the network control becomes more complex.
Materiel	SDN network components could become more standardized, reducing materiel costs.
Personnel	Possibility to reduce personnel as network configuration and management is centralized.
Leadership	-
Facilities	-
Interoperability	Interoperability could be improved in combined or joint operations as the network components become more homogeneous.
R&D	Civilian and military SDN-technology will differ, limiting the value of civilian R&D.

Discussion and conclusions

Based on the current and assessed Technology Readiness Level of Software-Defined Networking, the SwAF is presumed to be able to employ this technology in a 5-10 year timeframe, at least in applications that are close civilian counterparts.

Further research into this area is not considered necessary at the moment, but the area should be followed as it is likely that best-practice network design for commercial networks, as those used by the SwAF in its supporting and logistics infrastructure is expected to be based on SDN in a 2025 perspective. Remaining challenges include resolving uncertainties in network security.

The military utility is assessed to be uncertain due to questionable applicability and lingering security issues.

Transient Materials – Programmed to Perish

Ref: [2] Referee: Peter Bull

Introduction

Transient materials belong to a category of materials that under certain conditions will dissolve into their surroundings and leave only trace elements. A current example is biodegradable surgical suture, which dissolves after a certain time and therefore makes it unnecessary to remove the stitches after the surgical procedure. In the current study more complex components are described, e.g. sensors and electronic circuitry. Possible applications mentioned in the study are medical sensors and vessels for medicines, self-destructible electronics for data storage, and self-destructible sensors for surveillance.

The constituent materials are usually relatively easily degradable when subjected to physical, chemical, or biological influences. Water-soluble materials are the most commonly used for transient materials. It is, however, possible to use more resistant materials such as silicone or tungsten in extremely thin layers.

The decay process relies on a controlled initiation; the report describes three ways this can happen, see figure 2: either the transient material is subjected to water, acid or another fluid, which dissolves the material; or a fluid is kept in a UV sensitive container, when this container is subjected to UV light the fluid is released and dissolves the transient material; or the transient material is heat sensitive, a heater is triggered by a signal which starts the decomposition process.

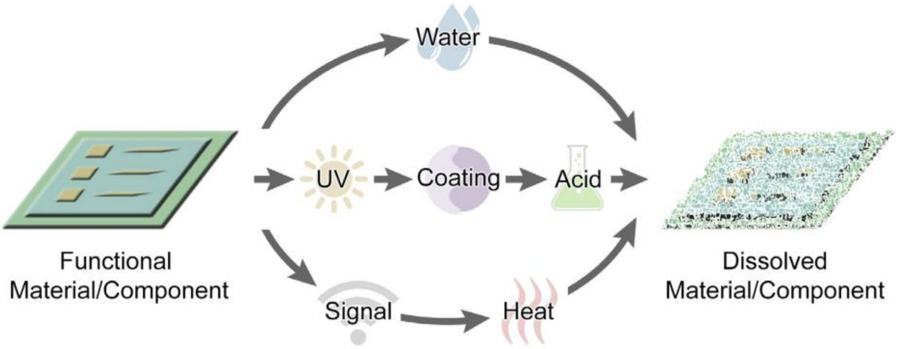


Figure 2: Schematic illustration of trigger mechanisms as shown in ref [2].

Identified possibilities and constraints

Advantages

- In surgery it can reduce the necessity to remove the components after use
- It might be a way to tamper-proof components
- It might be a way to remove evidence of covert activities, which is beneficial for someone conducting covert activities

Disadvantages

- Trace elements of the components can leave a negative environmental footprint
- Components can dissolve prematurely
- It might be a way to remove evidence of covert activities, which is detrimental for someone subjected to covert activities

Assumptions

The concept scenarios are based on the following assumptions:

- The assumed developmental hurdles have been passed
- It is possible to trigger the self-destruction in a predictable and controlled way

Suggested military use

The following applications are mentioned in the report:

1. Self-destructible systems for data storage
2. Self-destructible systems for surveillance and information-gathering

Concept scenarios in 2040

One/two scenarios are presented and subjected to a SWOT-analysis.

1. Self-destruct circuitry in a missile
2. Anti-tamper device on an unmanned vehicle

Scenario 1 – Self-destruct circuitry in a missile

Cruise missiles and other long-range weapons are not intended to return to wherever they are launched from. They will pass over, or through, areas which rules of engagement dictate should not be affected by the weapons.

In some cases it might become necessary to abort the mission. Today the most common way to abort such a mission is to destroy the weapon by detonating its explosive charge. Explosives materials can either detonate or deflagrate depending on how they are ignited. Some explosives will burn, or deflagrate, if lit by a spark or a fire as long as they are not contained in a closed encasement. The same explosive might detonate if contained in a closed encasement if lit the same way. If part of the encasement is made of a transient material it should be possible to make the explosive burn out, and the weapon hit the ground in one piece. This can potentially reduce the possibility for collateral damage.

If the weapon hits the ground and is broken up in large pieces it might be possible to salvage important parts. In order to reduce that possibility, those important parts should also be made from transient materials. That way critical information contained in the guidance system, as well as the guidance system itself, can dissolve upon self-destruction. This will make it nearly impossible to recover and re-engineer the guidance system and the information contained in it.

Scenario 2 – Anti-tamper device on an unmanned vehicle

The rise in the use of unmanned vehicles will make it increasingly interesting to capture those vehicles in order to ransom, copy, or use them against their original users. Transient materials could potentially be used as anti-theft, or anti-tamper, systems on unmanned vehicles. If the vehicle is captured, either its own sensors or a remotely-located controller could trigger the anti-theft system. That way the vehicle itself, and information contained within it, can be rendered useless.

SWOT-analysis

The following strengths, weaknesses, opportunities and threats with the proposed technology within both scenarios were identified at the seminar:

Strengths:

- Makes it possible to remove important parts or important information from critical systems that risk being captured

Weaknesses:

- Since the materials are transient, thus made to decay rapidly, they might not last long. Military systems are often used for a very long time.
- Might not decay rapidly enough
- Uncertain performance compared to traditional electronics

Opportunities:

- Advanced tamper-proofing, enabling new ways of distributing software libraries with a reduced risk of interception
- Can enable possibilities to dispose of weapons without the use of explosives. E.g. control systems and igniters in mines can self-destruct in a controlled way, and explosives that decompose.

Threats:

- Unintended triggering of decay process
- Triggering of decay process by antagonist

Assessed capability impact

In the examples above transient materials are parts of an evolution rather than a revolution. They may facilitate removal of evidence in surveillance systems, they may also make forensic investigations difficult, and they can contribute to systems that make long-range weapons systems die gracefully rather than going up in a ball of flames and shrapnel. Thus transient materials can provide new ways to protect critical systems, contributing to the core capability protection.

Assessment of Military Utility

Within the scenario(s) analyzed the military effectiveness is mainly coupled to risk, and risk mitigation. The risk of losing important information or important systems can be reduced, as well as the risk of collateral damage from aborting missions with cruise missiles and other long-range systems. On the other hand, the risk of having to abort a mission because of limited endurance of systems containing transient materials might increase.

The military suitability is potentially high. As this is, in principle, just another way to make existing electronic circuitry, current electronics could quite possibly be swapped out with transient electronics. As long as the users are aware of the transient systems’ possibilities and limitations it should be possible to use as before, with the added possibility of making important parts vanish if needed. Also see table under Footprint 2040

The affordability is uncertain. Currently the technology readiness level is low for the systems described. Therefore it is nigh on impossible to predict the cost of these systems, as is predicting how fast these materials will evolve.

In total therefore the military utility of the technology is uncertain, mainly depending on the very uncertain cost of systems containing transient materials. Since such systems are meant to dissolve relatively rapidly on command they might lack the necessary endurance. That might increase life cycle cost, as the components containing transient materials have to be changed often, or set endurance limits to the systems in which they are embedded.

Footprint/cost 2040

The following list is a compilation of anticipated footprints created by the use of transient materials to the DOTMPLFI factors (Doctrine, Organization, Training, Materiel, Personnel, Leadership, Facilities and Interoperability) as well as the expected requirements on the SwAF R&D in order to facilitate the introduction of the technology.

Item	Comment
Doctrine	Might need to take the possibilities and limitations into account
Organization	Limited
Training	Need to take the possibilities and limitations into account
Materiel	New components for current materiel needed
Personnel	Need to understand the possibilities and limitations
Leadership	Limited
Facilities	Maintenance facilities for new componentry
Interoperability	Limited
R&D	Has to be monitored

Discussion and conclusions

With the exception of surgical sutures, the development of transient materials is in its infancy. Obstacles may occur that prove to be difficult and time-consuming to overcome; therefore the biggest uncertainty in the above scenarios is whether the transient materials will have reached maturity within the given time frame.

The scenarios described can be generalized to cover other types of situations or other types of weapons. One example is mines designed to decompose after a certain time or after being triggered by a certain self-destruct command.

The possibility to make systems, or part of systems, that can dissolve on command can open interesting possibilities both in medicine and in military operations. The possible success of the latter, however, will be dependent on the cost and endurance of such systems. If they turn out to be very expensive or have a limited endurance they will not readily be used in high-risk operations.

The military utility is assessed to be uncertain, mainly depending on the very uncertain cost of systems containing transient materials.

Multi-robot systems

Ref: [3] Referee: Björn Persson

Introduction

The development in miniaturization and computational power has led to the possibility to field unmanned military platforms which can provide operators with situational awareness and even deliver effect in the operational area, using armed unmanned vehicles. A natural next step in this development is to allow such systems to cooperate in order to achieve mutual mission objectives. The goal is very similar to that of humans cooperating which is known to increase mission effectiveness and even to complete missions that are impossible to do without cooperation. The same types of effects are expected to be seen when unmanned vehicles are designed to work together.

Research on such topics is often called Multi-Robot Systems (MRS) which is defined as *"the use of multiple robots to achieve a mission objective"* and the requirement to be defined as a robot or an agent of an MRS is given in [3] as "*can be any electronic device that is able to process data and communicate or perceive its environment*". This makes it possible to classify a wide range of technical systems as MRS. In this report an alternative definition is used in order to narrow down the technology field: "*an MRS is a constellation of unmanned platforms working together to reach common mission objectives. Some parts of the system possess a high level of autonomy".*

The report identifies three technological areas of particular importance for MRS. First, different types of control strategies are discussed, which is a research field that should be expected to be driven and developed as part of research on MRS. Second, MRS agents will need various ways of communicating within the system and MRS may put slightly different requirements on the communication technology compared to more traditional military platforms. This is since the agents are expected to be within closer range to each other than is the case with other military platforms; therefore, development in communication technology is an important aspect. Also, communication is a key enabler for MRS systems to work at all. Third, to increase mission effectiveness MRS rely on a resource manager which aims at calculating and executing optimal mission plans. The resource manager is the brain of the MRS and thus research on resource management is likely something that military organizations which intend to deploy MRS need to participate in.

Identified possibilities and constraints

Advantages

- Higher redundancy and flexibility which leads to improved availability
- More efficient use of resources
- Harder to jam, due to close-range communication
- Can be harder to detect as a result of their small size
- Releases the operators, who can focus on the decision-making process instead of control
- Faster response to changes in the environment

Disadvantages

- It may be hard for the operator to know what the robots are doing and will be doing; on the other hand this relieves the operator for other tasks.

Assumptions

The concept scenarios are based on the following assumptions:

- Efficient communication technology for communication within the group is available.
- Sensors and technologies for sense-and-avoid are operational.
- Sufficient advances in resource management have been made.

Suggested military use

The following applications are mentioned in the report:

1. Saturation of enemy defenses using disposable swarms of robots.
2. Coordinated surveillance missions.
3. Establishing and maintaining a communication network.
4. Mapping of buildings using miniature robots.

Concept scenarios in 2040

One scenario is presented and subjected to a SWOT-analysis.

Scenario: Suppression of Enemy Air Defenses (SEAD)

The scenario is a high-level conflict where enemy forces have taken control of an island in the vicinity of the mainland. Intelligence indicates that the enemy has deployed several sophisticated air defense systems which severely restrict conventional combat aircraft from entering the airspace in the vicinity of the island. In order to facilitate a counter-attack with air support it is first required that the enemy air defenses are suppressed or destroyed. The operation in this scenario is what is commonly referred to as Suppression of Enemy Air Defense (SEAD), and an example of a relevant operational area is given in figure 3.

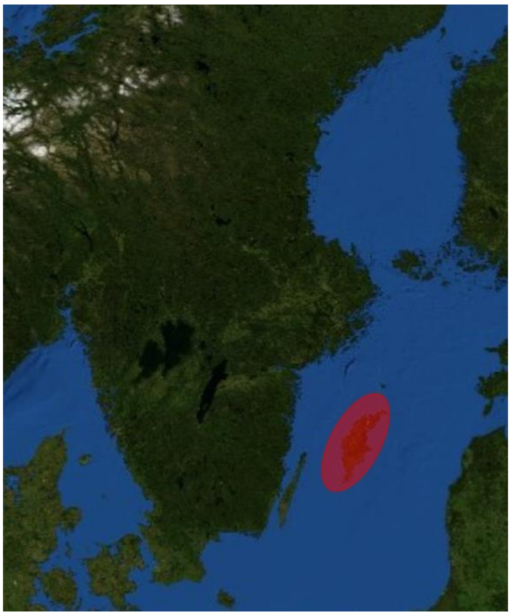


Figure 3. An example of geography relevant for the described scenario.

The key technology to achieve SEAD capability in this scenario is disposable unmanned combat aerial vehicles (UCAV) equipped with signal-seeking sensors and a warhead. An example of what such a platform could look like is given in figure 4.

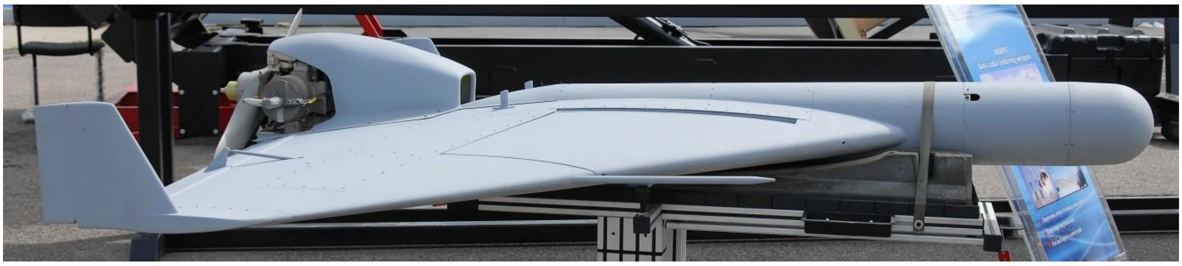


Figure 4. An example of what the disposable UCAV might look like.

The UCAV can be launched from the ground or from a transport aircraft and has high endurance which allows it to loiter over the target area for hours while searching for hostile emitters. If such a signal is found the UCAV chooses a tactical trajectory to engage the target and the warhead detonates when the UCAV is sufficiently close to the target, aiming at destroying the radar antenna and other vital equipment.

The UCAVs are significantly cheaper and numerous compared to the ground-to-air missiles that the air defenses use. In addition, the disposable UCAVs are supported by other UAVs which carry radar, electronic support measures and jammers. By using MRS it is possible to get the different types of UAVs to cooperate, and to react to the environment and hostile actions in a highly autonomous manner. This relieves the human operator who then only has to define mission objectives and other high-level decisions. The following SWOT-analysis considers the difference between the MRS alternative and conventional centralized control (where each UAV is controlled by an operator). Thus, it is not the SEAD capability with disposable UCAVs that it the objective for the SWOT analysis, but rather the difference between the two control philosophies.

SWOT-analysis

The following strengths, weaknesses, opportunities and threats with the proposed technology within the scenario were identified at the seminar:

Strengths:

- The MRS can make better use of the same resources since an effective resource manager can make sure that different resources are used and correctly positioned in a timely manner. This increases operational efficiency. For example, a disposable UAV can alert the rest of the group to the presence of a hostile emitter, wait until another UAV with jamming capabilities starts jamming the sensor, and then choose the most suitable UAV to attack the target.
- UAVs in an MRS will be closer to each other than to the control station, which can make the communications between the UAVs much harder to jam than communication between the control station and the UAVs. This can also reduce power requirements for communications and make it harder to intercept communication from the MRS by the enemy.
- The above argument also suggests that an MRS may require less sophisticated communication equipment.
- The operation of the UAV group is highly autonomous; this relieves the command and control operators.

- The high level of autonomy can greatly improve the availability since fewer operators are required to operate the complete MRS.
- The MRS could lead to reduced operational and infrastructure costs.
- The high level of autonomy could allow the MRS to have a faster OODA-loop.

Weaknesses:

- The MRS will inevitably rely on more complex subsystems for communication and coordination.
- There is a risk that the MRS system becomes predictable.
- The consequences would be much more severe if the enemy manages to affect the information flow in the MRS.
- The initial investment costs may be higher.

Opportunities:

- The MRS system may be able to use deception as part of its inherent tactics which could greatly decrease the opponents' ability to affect the system as a whole.
- The command and control function can focus on using other resources better if they can be relieved from most of the control duties related to the MRS mission.

Threats:

- As with most technologies that rely on IT there is a cyber-threat.
- An effective counter-technology is likely to be an opponent using another MRS designed to counter our MRS.
- Most decisions made by the MRS are made by the resource manager, it may be possible to construct intelligent decoys designed to target the resource manager.

Assessed capability impact

The use of MRS firstly requires that the user is in possession of a large number of unmanned platforms. If that is the case, MRS can be used to increase mission effectiveness by making better use of the available resources, regardless of which capabilities the unmanned systems contribute to.

Assessment of Military Utility

Within the scenario(s) analyzed the military effectiveness is the main contribution to the military utility of MRS. Agents in an MRS are expected to become more effective when collaborating compared to the same number of agents working with an agenda of their own. However, in what way MRS will become more effective depends greatly on the mission objectives and how good the future resource managers becomes. Similarly, humans can become more effective when performing certain task if they cooperate and are under good leadership. There is no reason why we should not expect the same phenomenon to apply to robots or unmanned vehicles.

The military suitability is deemed high since all the required infrastructure (except the resource managers) are already required in order to operate robots or unnamed vehicles. MRS is also well suited for mission type tactics, which is an essential part of SWAF doctrine.

The affordability is expected to be high since MRS requires fewer operators and the only extra cost ought to be expenses related to the resource manager.

In total, therefore the military utility of the technology is significant, since we believe that the mission effectiveness in particular can be greatly improved if unmanned vehicles or robots are given the possibility to cooperate to a large extent, when undertaking various tasks.

Footprint/cost 2040

The following list is a compilation of anticipated footprints created by the use of MRS to the factors DOTMPLFI (Doctrine, Organization, Training, Materiel, Personnel, Leadership, Facilities and Interoperability) as well as the expected requirements on the SwAF R&D in order to facilitate the introduction of the technology.

Item	**Comment**
Doctrine	Needs to take the new possibilities and limitations into account.
Organization	Fewer personnel required to operate the robots.
Training	Different types of training are required for operators and decision makers.
Materiel	Communication systems for group communication.
Personnel	Different competences required.
Leadership	Limited
Facilities	Limited
Interoperability	Limited
R&D	Research for resource management and efficient algorithms for combat scenarios.

Discussion and conclusions

The deployment of various types of unmanned systems is common in modern military operations and they can assist in a multitude of mission types. The idea behind MRS is that such systems can be more effective in reaching their mission objectives if they work together. If this can be achieved there is much to gain for military organizations, however much research is still required to realize effective and safe MRS.

In this work only one scenario was considered, however MRS is expected to be useful in any scenario where cooperation between the agents can lead to higher mission effectiveness.

The military utility of MRS is significant, since we believe that the mission effectiveness can be greatly improved.

Radar bortom horisonten - Over-the-Horizon Radar

Ref: [4] Referent: Stefan Silfverskiöld

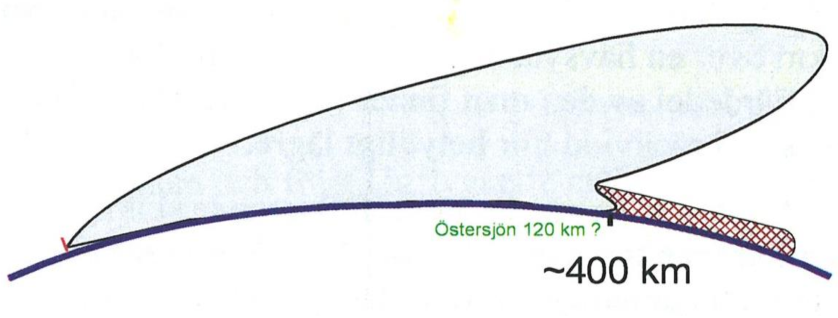
Introduktion

Tekniken för radar med räckvidd bortom horisonten har studerats tidigare. Spaningssystem av denna typ brukar benämnas OTH-radar (”Over-The-Horizon” radar). FOI har under 2014 genomfört en litteraturstudie som visar att det hänt en del de senaste decennierna. Fokus har legat på publikationer rörande ytvågs-OTH, som för svenska förhållanden bedöms mest intressant av både operativa, ekonomiska och praktiska skäl jämfört med rymdvågs-OTH.

Den teoretiska förståelsen har ökat, liksom möjligheterna att med hjälp av nya vågformer och avancerad signalbehandling komma runt några av de traditionella begränsningarna. Nya konceptidéer har börjat komma fram med potentiellt bättre prestanda än tidigare.

Ytvågs-OTH utnyttjar principen att radiovågor som utbreder sig utmed jordytan har en tendens att, speciell över vatten, följa ytan lite längre bort utmed horisonten, se figur 5. Effekten varierar beroende på val av frekvens och beskaffenheten hos ytan. Typiska frekvenser för OTH-effekt över havsyta med normal salthalt är 3-50 MHz. Effekten beror på en kombination av flera olika fysikaliska fenomen. Den vanliga radarhorisonten för en kustradar på mikrovågsbandet är i storleksordningen 40 km medan räckvidden för ett OTH-system kan bli uppåt 400 km.

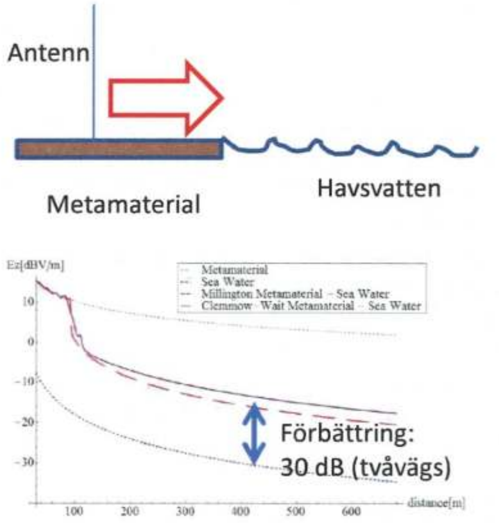
Eftersom dessa system måste vara relativt smalbandiga p.g.a. låg bärvågsfrekvens och frekvensallokering mm, så blir avståndsupplösningen låg. Upplösning i vinkelled (sidled eller azimut) blir också dålig då man ofta inte använder så stora antenner i förhållande till våglängden. Upplösningen kan här förbättras genom användning av ett nätverk bestående av flera stationer.



Figur 5. Principskiss för ytvågs-OTH. Angivna typsiffor för maximal räckvidd gäller för en markvåg medan det streckade området indikerar en fortsatt utbredning för en ideal ytvåg. Källa: Ref [4].

Bourey et al (2013) visar intressanta teoretiska beräkningar där metamaterial[2], i en övergångszon mellan mark och hav, kan öka fältstyrkan med 30 dB för att förstärka ytvågen, se figur 6.

[2] **Metamaterial** är artificiella material som framställts för att uppvisa egenskaper som inte återfinns i naturen.



Figur 6. Användning av metamaterial vid sändarantenn för att minska vågutbredningsförlusterna. Teoretisk beräkning enligt Bourey et al (2013). Källa: Ref [4].

Identifierade möjligheter och begränsningar

Möjligheter

- I den militära kravbild som FOI ser framför sig ingår ytvågs-OTH som ett av flera spaningssystem som samverkar i en framtida sensorkedja för luft- och sjömål.
- Detektera och följa lågflygande mål på stort avstånd.

Begränsningar

- Till skillnad från konventionell radar på frekvensband över 1 GHz finns det ännu inga internationellt överenskomna frekvensintervall som upplåtits för OTH-radar som den primära tjänsten för att utnyttja aktuellt frekvensutrymme, vare sig i rymdvågs- eller ytvågsfallet.

Antaganden

Scenariot baseras på följande antaganden:

- Utveckling av ny teori, nya systemkomponenter och signalbehandling gör det möjligt att bearbeta data på helt annat sätt än tidigare vilket innebär goda ytvågsräckvidder 2040.

Föreslaget militärt nyttjande

Följande tillämpningar nämns i den skannande rapporten:

- Detektera och följa fartyg långt bort från kustområdet.
- Fungera som robust ”snubbeltråd” för att larma operatörerna. Operatörerna kan därefter fokusera övriga sensorer för att närmare ta reda på vad som utlöst larmet.
- Ge en grov positions- och hastighetsuppskattning samt om möjligt grovklassning i de områden där vi kan detektera objektet ifråga.
- Vara verksam mot smyganpassade mål och vara svårupptäckt av motsidans signalspanare och/eller deras signalsökande robotar.
- På ett robust sätt kunna hantera naturliga och mänskligt skapade störningar, liksom att frekvensallokeringen ska fungerar visavi andra aktörer civilt och internationellt.

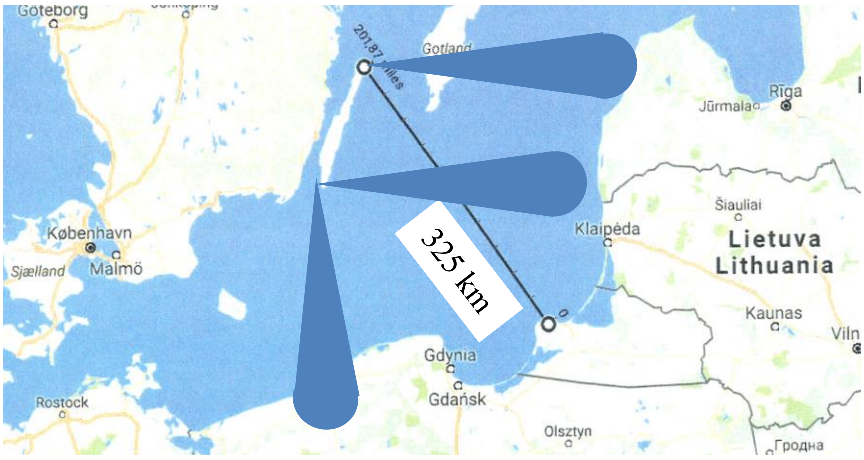
Koncept scenario 2040

Ett scenario presenteras och får genomgå en SWOT-analys.

Scenario Ytvågs OTH-radarsystem för sjömålsdetektion

Kunskapsuppbyggnad genom försök med ytvågs OTH-radar pågår redan på västkusten. Därför har ett scenario för ytvågs OTH-radar i Östersjön utarbetats: En högnivå konflikt pågår där underrättelser indikerar att en motståndare har för avsikt att placera ett flertal sofistikerade luftvärnssystem på Gotland. Detta skulle kraftfullt begränsa rörelsefriheten för konventionellt stridsflyg och sjöstridskrafter i södra Östersjön.

I syfte att bortom horisonten kunna upptäcka fartygsrörelser har ett flertal ytvågs OTH radarsystem monterats på vidkraftsparken utanför Öland, se figur 7. Upplösningen i sida förbättras tack vare ett nätverk av flera stationer. Effekten av modulation från vindkraftverkens rotorer bedöms kunna kompenseras bort.



Figur 7. I scenariot har ett flertal ytvågs OTH-radarstationer utplacerats i ett nätverk i syfte att kunna upptäcka fartygsrörelser i södra Östersjön. Avståndet från Ölands norra udde till Kaliningrad indikeras.

SWOT-analys

Följande styrkor, svagheter, möjligheter och hot för den föreslagna ytvågsteknologin inom det givna scenariot identifierades vid seminariet:

Styrkor:

- Kan med egna resurser upptäcka mål på stora avstånd (upp till 400 km) med god förmåga till uthållighet
- Bättre skydd än andra spaningsresurser med möjlighet att nå lika långt
- Lågteknologisk hårdvara blir billig att reparera
- Ytterligare en sensor som bidrar till yt- (och på kortare avstånd) även till luftlägesbild
- Möjlighet styra motståndaren genom skapande av ytterligare kanalisering
- Störfast p.g.a. lägre frekvens än vanlig radar
- De låga frekvenserna gör signaturanpassning av ubåtstorn, kortvågsantenn, kryssningsrobot och flygplan overksam, vilket innebär att dagens smyganpassade fartyg kan upptäckas

Svagheter:

- Låga salthalten (varierande med tid) i Östersjön begränsar räckvidden, särskilt gäller detta i Bottenviken
- Dålig upplösning i sida och avstånd, som dock i sida kan begränsas med utnyttjande av flera stationer
- Ytvågsstationerna är förutsägbar till läge och lober, således möjliga att bekämpa och störa med elektronisk krigföring

Möjligheter:

- Montera ytvågs OTH-radar på vindkraftverk utanför Öland ger fler möjliga placeringar än bara på fastlandet
- En rymdvågsbaserad OTH-radar placerad på lämplig plats i övre Norrland bedöms kunna upptäcka en ballistisk missil som avfyras t.ex. från hela Europa (öst och väst) vilket skulle ge en strategisk underrättelseförmåga.

Hot:

- Salthalten i Östersjön kan variera över tiden
- Den låga upplösningen kan utnyttas av motståndaren för att dölja sig bakom annat mål
- Att internationellt överenskomna frekvensintervall som upplåts för OTH-radar inte kommer till stånd

Bedömt förmågebidrag

Ytvågs OTH-radar bidrar till den grundläggande förmågan und/info och till förmågorna upptäckt av luft- och sjömål.

Värdering av militär nytta

Inom det studerade scenariot bedöms ytvågs OTH-radar, givet prognosticerad teknikutveckling, kunna på väsentligt större avstånd än dagens kustradarstationer upptäcka och följa lågflygande luftmål samt sjömål.

Ett multistatiskt system med hög komplexitet är med naturlighet dyrare än ett enkelt monostatiskt system med låg uteffekt. En stor del av totalkostnaden representeras av kostnaden för antennsystemet och installationen av detta samt systemintegrationen. Eftersom det erfordras en hel del forskning och teknikutveckling innan systemet kan bli operativt föreligger en risk att kostnadsmålen överskrids.

Eftersom framgångsrik forskning kring flera delteknologier, t.ex. antennteknik, vågutbredning, vågformer, signalbehandling och systemutformning erfordras, finns en påtaglig risk för att önskad TRL-nivå inte uppnås i tid. Om en motståndare tillägnar sig teknologin finns en risk att våra smyganpassade ytstridsfartyg upptäck på stora avstånd.

Således bedöms den militära effektiviteten, främst p.g.a. kostnadsaspekten och osäkerheten kring prestanda i Östersjön vara svårförutsägbar.

Systemets militära lämplighet bedöms vara hög. Givet att det kan utvecklas till TRL-9 till 2040, bör det utan svårighet kunna integreras i befintlig sensorkedja. Se vidare under Footprint 2040, nedan.

Kostnadsdimensionen är osäker. För närvarande är TRL-nivån för ytvågs OTH-radar låg även om ett antal exempel på utländska system av olika status presenteras i FOI-rapporten. Det är därför näst intill omöjligt att förutsäga totala livscykelkostnaden för systemet och hur snabb teknikutvecklingen kommer att vara.

Sammantaget bedöms den militära nyttan vara måttlig, främst p.g.a. den svårförutsägbara kostnadsdimensionen. Givet att nödvändig forskning och teknikutveckling nationellt och internationellt kommer till stånd bedöms den militära nyttan att på långa avstånd med ytmåls OTH-radar kunna upptäcka sjömål och lågflygande luftmål vara ett värdefullt tillskott till den grundläggande förmågan und/info samt till förmågorna upptäckt av sjömål och lågtflygande luftmål.

Footprint/cost 2040

I nedanstående tabell förtecknas ytvågs OTH-radarsystemets påverkan på faktorerna DOTMPLFI (Doktrin, Organisation, Träning, Materiel, Personal, Ledarskap, Anläggningar och Interoperabilitet). Dessutom anges ev. behov av FoT-satsningar för att underlätta introduktion av teknologin i Försvarsmakten.

Item	Comment
Doktrin	Försumbar påverkan på doktrin, endast ytterligare några stationer i sensornätverket
Organisation	Ingen påverkan då det inte kräver särskilt förband
Träning	Ingen särskild träning erfordras, inryms i sjöövervakningsoperatörens ordinarie uppgifter
Materiel	Förutsätter att nya systemkomponenter och signalbehandling utvecklas och att ytvågs-OTH radar blir operativa till 2040
Personal	Begränsat behov av underhållspersonal
Ledarskap	Ingen påverkan
Anläggningar	Ingen påverkan
Interoperabilitet	Frekvensallokering för OTH-radar behöver lösas internationellt
FoT	Forskning kring antennteknik, vågutbredning, vågformer, signalbehandling och systemutformning föreslås.

Diskussion och slutsatser

Ytvågs-OTH radar har tidigare ansetts få dåliga prestanda i Östersjön p.g.a. låg salthalt och låg bandbredd vilket ger dålig avståndsupplösning. Snabba mål har förväntats vara svåra att upptäcka. Den nu genomförda FOI-studien har nyanserat bilden till viss del.

Rymdvågs-OTH innebär fortfarande stora, dyra och resurskrävande anläggningar, även om länder som Ryssland och Iran nyligen gjort nyinstallationer. En rymdvågsbaserad OTH-radar placerad på lämplig plats i övre Norrland bedöms kunna upptäcka en ballistisk missil som avfyras t.ex. från hela Europa (öst och väst) vilket skulle ge en strategisk underrättelseförmåga.

Avseende ytvågs-OTH har det hänt en hel del på de flesta områden som gör tekniken intressant igen. För att ytvågs OTH-radar ska kunna bli operativ till 2040 förutsätts dock att viktiga pusselbitar i den teoretiska förståelsen kommer på plats. Dessa avser bland annat antennteknik, vågutbredning, vågformer, signalbehandling och systemutformning. Av intresse är också att studera hur OTH-enheter i nätverk passar in i och samarbetar med det övriga spanings och underrättelsesystemet.

Baserat på den här studien föreslås att FOI med stöd av FoT-projekt från Försvarsmakten undersöker de möjligheter och hot som tekniken i dagsläget ger givet specifikt de osäkerheter som finns för nyttjande i Östersjön, inte minst hur radarns bärvågsfrekvens i MHz-området påverkar smygåtgärder gjorda i GHz-området.

Sammantaget bedöms den militära nyttan vara måttlig, främst p.g.a. den svårförutsägbara kostnadsdimensionen.

Moving Target Defence

Ref: [5] Referee: Hans Liwång

Introduction

All or most systems have cyber-security vulnerabilities that expose them to attackers. Moving Target Defense (MTD) is a type of technique that attempts to protect the systems by changing the exposed surface, i.e., the target. In this way the system changes between different, usually vulnerable, configurations rather than attempting to completely mitigate existing vulnerabilities. The system's security is therefore created by moving the target, i.e. replacing the configuration by a new one, before the attacker has been able to identify where vulnerabilities are located.

The FOI report [5] is a literature survey that used a systematic literature search to identify 56 articles that discuss variants of technical (code) implementation of MTD. The report analyzes how useful these are, what processes are involved, and what kind of security they bring. This discussion does not take specific military aspects into account and does not discuss the military implications of the concepts analyzed. The report has not studied articles concerned with MTD as a general defense concept based on, for example, game theory methodology.

According to the report MTD is a relatively new concept, but the report also acknowledges that its core ideas have been available in the IT-community for more than a decade. For example, a variant of MTD has been available for Linux since 2001 and another variant was tested by DARPA the same year. The report describes that a major proportion of the research that is being carried out regarding MTD was initiated a few years ago when large investments were made by the Department of Homeland Security in USA.

The report [5] identified six different types of computer system MTDs:

1) moving code transformation,

2) moving memory allocation,

3) moving applications,

4) moving machines,

5) moving network addresses and

6) combinations of these five kinds.

These six types are described in detail in the FOI report.

In the articles studied by FOI the focus is on introduction of protection mechanisms rather than examining the quality of these mechanisms. The FOI authors propose that future work within the area should focus more on evaluating the quality of protection mechanisms, in particular in regard to how the MTD affects the systems' performance and how the end-user is affected given a realistic threat model.

The report does not discuss or assess the Technology Readiness Level (TRL) of the six different versions of MTD. However, from descriptions it can be estimated that moving code transformation is TRL 9 and that the other five are on TRL 4-6.

Identified possibilities and constraints

Advantages

- Introduces a way of defense that protects computer systems by change rather than by mitigating specific vulnerabilities.

Disadvantages

- Reduces performance of the computer.
- Complicated to introduce a complete change of the target, i.e., the change is always limited.

Assumptions

The concept scenarios below are based on the following assumptions.

- Today's civilian development of MTD will continue if MTD is estimated to improve cyber security.
- The development of methods for cyber attack and cyber protection will continue at least at today's rate.

Suggested military use

The report does not explicitly mention military applications of MTD. However, cyber defense is as important for military applications as for civilian. Furthermore civilian and military system differ in how are they are open to the internet and to other networks. The military use must in the general case be assumed to be relatively similar to the civilian one, and therefore the suggested military use is MTD as one defense mechanism among others for protecting military cyber systems.

Concept scenarios in 2025

Given today's development in cyber security and an assumption that MTD will increase security it is likely that the role and importance of MTD will change relatively rapidly. A scenario set in 2040 will necessarily introduce significant uncertainties in an analysis of the military utility of MTD. Therefore, the scenarios in this analysis are set in 2025. Two scenarios are considered for the SWOT-analysis:

Scenario Alfa: A military server used for communication with the public during crisis.

Scenario Beta: A military computer or server situated on a military-only network without an internet connection. The network is used for communicating and exchanging information about an ongoing operation within a headquarters.

SWOT-analysis

The following strengths, weaknesses, opportunities and threats of the MTD in the scenario were identified at the seminar:

Strengths:

- Contributes to security by presenting an alternative approach to security.

Weaknesses:

- Can/will reduce the systems' performance.

- The constant change of the system configuration can risk critical functions of the system failing to complete their task.
- Current development is for commercial (civilian) systems; if specific military requirements are needed such functionality may be dependent on substantial military-specific efforts.

Opportunities:

- The concept of moving target defense has a strong tie to military thinking in general. If today's conceptual development of MTD (which is not discussed in the FOI report) changes how cyber security is understood, this could be a step forward in protection of military systems in a wider sense.
- If MTD is implemented and used so that it also affects the behavior of the users of the system, this may assist in the understanding the idea that you are never 100% secure.
- As the protection with MTD is based on different concept than other security measures it may create a more robust system which can be a first step towards a resilient system.

Threats:

- As the proposed target motion is limited, it is possible that the protective effect is limited or short lived.

Assessed capability impact

The MTD technology enables continuous updating and strengthening of cyber security, which is important for the protection of all computer systems, civil or military.

Assessment of Military Utility

Within the scenario(s) analyzed the specific military effect is low or limited because the protection mechanism is general and not military-specific. However, the military specific cost is also low and the effectiveness can therefore be substantial.

The military suitability is high as the solutions proposed are fit for commercial computer systems which are also the typical computer settings in military systems.

The affordability is high as there are none or low military-specific costs associated with the technology.

In total the military usefulness of the technology is marginal but also requires marginal military efforts; therefore military utility is uncertain as a small change in usefulness or required effort will have a large effect on the utility.

Footprint/cost 2025

The following list is a compilation of anticipated footprints created by the use of MTD to the factors DOTMPLFI (Doctrine, Organization, Training, Materiel, Personnel, Leadership, Facilities and Interoperability) as well as the expected requirements on the SwAF R&D in order to facilitate the introduction of the technology.

Item	Comment
Doctrine	Limited
Organization	Limited
Training	Limited
Materiel	Software changes, but no changes in functionality
Personnel	Limited
Leadership	Limited
Facilities	Limited
Interoperability	Limited
R&D	Limited

Discussion and conclusions

This analysis has limitations and uncertainties especially in relation to the military aspects of MTD. Neither the source literature nor the FOI report discussed military use and the concept of MTD is not put in a larger military context.

It is assumed here that the development of methods for cyber-attack and cyber protection will continue to develop at a high rate which would entail significant uncertainties for a forecast into 2040; the analysis is therefore conducted for 2025. The FOI report includes no TRL estimation and also indicates that several types of MTD which looked promising ten years ago have not developed as estimated. It is therefore possible that in 2025 a couple of MTD types will be TRL 9 and others will still be on TRL 4-6. It is also possible that one or several MTD types are out of date by 2025.

It is likely that the assessment of MTD can be generalized to other types of computer system protection under civilian development.

The military utility is assessed to be negligible.

Satellite-based radar imaging

Ref: [6] Referee: Peter Sturesson

Introduction

This report presents a survey of the current state-of-the-art for civilian and military satellites using radar, preferably with synthetic apertures (SAR), for remote sensing and imaging. The concept of SAR and its early systems–in-use hark back to the Cold War era but it is during the last 10-15 years that the critical conditions for relevant effectiveness, suitability and affordability has reached sufficient levels to attract an increasing number of users.

From 2005, European satellite constellations equipped with SAR payloads have been launched and exhibited spatial resolution that challenges their electro-optical contemporaries. Also, an increasing consumer market and structures for cost-sharing have implied collaborative initiatives on the bilateral level. Multi-lateral levels are still challenged by national interests, information integrity and operation coordination.

In general, earth observation satellites add an essential component for the warfighter in terms of non-intrusive global coverage for surveillance and reconnaissance. Activities of interest, treaty verification, position and reallocation of troops and battle damage assessment are typical tasks for both foreign and military components of security policy. Constellations of typically 2-5 satellites reduce the observation period compared to stand-alone satellites. SAR-systems also add operational sustainability to daylight and cloud coverage variations, as well as valuable data for geographical analysis.

The number of active satellites with SAR-payloads varies over time but for the last ten years European systems together with systems from USA, Russia and China have been consistent with a low but steady addition of new systems and users.

Since requirements for performance in terms of resolution, communication reliability and life-time provide a threshold for new innovations to be implemented, development is following a moderate pace. The general interest in cost reductions and the consequent large-scale trend of miniaturization of satellite systems have, however, been studied and tested for the last ten years.

This report presents the state-of-the-art for SAR-satellites and some future alternatives.

Predicted technology development regarding:

- Advances within material science
    - New Tx/Rx-elements
    - Lightweight and foldable antennas
- New frequency domains and increased bandwidths.
- Multistatic systems and swarms.

Studies of orbit parameters can utilize knowledge and indications regarding satellite payload, coverage and time-frames for operation and charging respectively.

Identified possibilities and constraints

Advantages

- High spatial resolution.
- Large area coverage.
- Includes data for detecting moving objects and for extracting geographically-related information.
- Global coverage over time.
- Flexible orbit design.
- Legally non-intrusive.

Disadvantages

- The first two advantages cannot be achieved simultaneously.
- Predetermined times for every given position reduces the operational flexibility.
- Requires launch facilities and long preparation times.
- Can be regarded as intrusive.
- Strong transmitter over a large area.

Assumptions

The concept scenarios are based on the following assumptions.

- Anti-satellite capabilities are not taken into account.
- Main focus is to identify and characterize SAR-satellites rather than use them.
- Emphasis on civilian use for geographical analysis, with secondary military utility.
- Space Situational Awareness (SSA) capabilities are available.

Suggested military use

The following applications are mentioned in the report:

- Image Intelligence
- Geographical intelligence

Two scenarios are presented and subjected to a SWOT-analysis.

Scenario 1

A major conflict resulting from regional decadence and political struggles between different religious groups causes significant destruction in an increasing number of sovereign national-states. In order to prevent the conflict expanding, a UN-resolution provides a mandate to the EU to lead a combined force to conduct a time-limited military intervention. Logistics lines are planned and the operational planning is in its initial stage

Scenario 2

A country with regional dominance has taken strategic measures during the last decade in order to strengthen its political prestige and reputation. As a part of this, a new military doctrine states that the armed forces of the country will be upgraded with new state-of-the-art-systems in all domains and its international behavior will become more aggressive. Neighboring countries are targets for political influence and cyber-attacks, and covert operations are reported. Conventional military forces have been and are operating in certain neighboring regions and the country is using presumptuous threats about the use of military force to secure its political interests.

SWOT-analysis 1

The following strengths, weaknesses, opportunities and threats with the proposed technology within scenario 1 were identified at the seminar:

Strengths:

- Surveillance of several actors over long time-periods enables situational awareness (SA) in theatre.
- Sustainable against daylight and weather conditions during operations enables freedom of action for operational planning.

Weaknesses:

- Surveillance and reconnaissance are distinct from each other at any given time; only high spatial resolution or large area coverage may be chosen.
- Limited field-of-view at high spatial resolution decreases the general SA in favor of a specific area.
- Short observation time per passage implies that many activities may go undetected.

Opportunities:

- Gain information about other actors' activities and positions without encroaching on foreign territory.
- Gain information about geographical conditions in theatre to understand prerequisites for, and make prediction of, future hostile activities.
- Concentrating own troops to achieve local dominance at critical vulnerabilities if necessary.

Threats:

- Deception. Space Situational Awareness (SSA)-based analysis can be used by hostile actors to create a fictitious normal state thus biasing intelligence analysis and predictions about hostile activities.

SWOT-analysis 2

The following strengths, weaknesses, opportunities and threats with the proposed technology within scenario 2 were identified at the seminar:

Strengths:

- Surveillance of stations and movement of conventional forces over long time-periods allows for analysis of pattern-of-life.
- Sustainable against daylight and weather conditions during operations enables freedom of action for operational planning.
- Can penetrate some camouflage and discover hidden objects.
- Small satellites in constellations can be replaced if damaged and constellations can be reconfigured if the operational requirements demand it.

Weaknesses:

- Antagonists' SSA makes own satellites somewhat predictable in time and position.
- Recharging is still dependent on sunlight exposure and may degrade the freedom of action for collection at any given moment.
- Short observation time per passage implies that many activities may go undetected, and real-time updates are not feasible with the number of satellites in a normal constellation.
- Small satellites may not carry large reflectors and will have inferior performance compared to larger conventional satellites that are the current state-of-the-art.

Opportunities:

- Satellites have a larger surprise element than aircraft since a passage over a territory does not automatically reveal whether the satellite is collecting data, until it begins to transmit.
- Material discrimination challenges deception tactics. Extracted geographical data supports operational planning to identify possible false targets and allows correct targets to be selected.
- Support to air-land-sea operations. Satellites fly over all other physical domains and their data collected can support all services when acting independently or in joint operations.
- Sweden has favorable geography for using satellites in polar orbits, which are typical for SAR-satellites. The advantage lies in communication, where tasks can be given to a satellite and data can be downloaded from it.
- Constellations allow several receivers to cooperate on one transmitted signal and can synthesize high-resolution images.

Threats:

- Deception. SSA-based analysis can be used by hostile actors to create a fictitious normal state thus biasing intelligence analysis and predictions about hostile activities.
- Jamming. If hostile actors acquire the transmission signal from a SAR-satellite, they may jam or deceive the receivers of the satellite with false signals.

Assessed capability impact

Satellite-based radar imaging provides increased intelligence capability and operation planning support on strategic, operational and tactical levels. SAR-satellites are enablers for all military operations that require this kind of information.

Assessment of Military Utility

- Effectiveness:
  - Better than 0.5 m spatial resolution, which is a general requirement in strategic IMINT.
  - Global coverage.
  - Daily passages.
  - Weather independant.
- Suitability:
  - IMINT resources already exist.
  - Low-spread knowledge within SwAF.

- Affordability:
  - 10-15 years life cycle.
  - Different cost levels have been reported in previous reports.
  - Partnership alternatives

In sum the military utility is assessed to be moderate while it's potential to maintain imaging performance independent of weather and daylight is not redundant from any other technology.

Footprint/cost 2040

The following list is a compilation of anticipated footprints created by the use of satellite-based SAR to the factors DOTMPLFI (Doctrine, Organization, Training, Materiel, Personnel, Leadership, Facilities and Interoperability) as well as the expected requirements on the SwAF R&D in order to facilitate the introduction of the technology.

Item	**Comment, effect on item**
Doctrine	Limited
Organization	Limited, some changes in placement of interpreting skills. Analysts can be placed on strategic, operational and tactical levels. No new units are needed.
Training	Limited, however operational and tactical levels need to practice the use of SAR-data for planning and assessment.
Materiel	Limited, government ground element exists for control and data download, SSA means might be optional.
Personnel	Limited, current staffs need to be trained or some new staff must be recruited.
Leadership	Limited.
Facilities	Limited to medium requirements, depends on whether we operate own satellites or not. Satellite control and data management facilities already exist.
Interoperability	Limited, image formats are common standards.
R&D	Limited, R&D development should be continuously monitored.

Discussion and conclusions

The report does not extensively lay out the future roadmap for SAR systems and is mainly focused on the state-of-the-art current operational systems rather than for today's forecast on future systems. In many ways, the report has an emphasis on SSA presenting analysis tools and methods. It does however provide some alternatives and potential future development.

SAR satellites have been around for a long time and current systems are essential assets for those countries that are in possession of them.

Material science achievements and innovative engineering provide conditions for the armed forces to procure relatively small satellites with high-performance antennae at an affordable cost. This implies an increased number of actors and/or an increasing number of satellites in orbit. In either case, the outcome will to some degree justify the main interest in the report, hidden between the lines, of developing a SSA-capability.

The military utility is assessed to be moderate in respect to the total spectrum of capabilities and tasks that comprise of and is provided for the Swedish Armed Forces. However, it is a major part of the capability of space-based surveillance and reconnaissance, which in itself is a key enabler for modern warfare and is as such an essential element to be utilized within the armed forces. As this capability is already present in many countries, it cannot be regarded as entirely new. In fact, radar-based imaging satellite systems has already contributed to international missions in which Sweden has participated. Hence, this is a capability already in place in the domain of military and security political courses of action for Sweden, albeit not in our direct control.

Örnen, Björnen och Draken: Militärt tänkande i tre stormakter

Ref: [7] Referent: Ola Thunqvist

Detta kapitel skiljer sig väsentligt från de tidigare i det att rapporten fokuserar på militärstrategiska utvecklingstrender och inte på en specifik teknologis militära nytta. Därför kommer detta kapitel ha en egen struktur. Militärtekniska aspekter kommer behandlas i slutet av kapitlet.

Robert Dalsjö, Gudrun Persson och Kaan Korkmaz har i varsin artikel i nämnd ordning beskrivit USAs, Rysslands och Kinas militära tänkande. Artiklarna, som baserar sig på litteraturstudier ger sammanfattningar om respektive lands övergripande militärstrategiska utvecklingstrender. De ger även adekvata återkopplingar till de historiska orsakerna till ländernas olika vägval och situationer som lagt grunden till varför de står där de står och vilken utveckling de strävar mot. Ländernas relationer med varandra har påverkat utvecklingen, inget land utvecklas solitärt, och författarna tecknar tydliga och lättförståeliga bilder av utvecklingen och de svårigheter och möjligheter som respektive land har att möta i det militärstrategiska perspektivet. Sovjetunionens fall och Gulfkriget 1991 är en tydlig omslagspunkt för utvecklingen då man för första gången fick skymta det högteknologiska kriget och även komma till insikt om hur långt efter i utvecklingen de forna sovjetstaterna och Kina var jämfört med USA och västra Europa. Uppvaknandet var bryskt och Ryssland och Kina har sedan dess arbetat hårt för att komma ikapp den teknologiska utvecklingen med stora investeringar i ny teknologi och utveckling av militära doktriner eller dess motsvarigheter. Kina har som exempel ökat sina militära anslag 7 ggr under den senaste 20-års perioden. Satsningarna innebär även att nya arenor införlivas och omsätts i doktrinarbetet, idag är både rymdarenan och cyber- och informationsarenan naturliga delar i ländernas intressesfär med både möjligheter och hot. Ryssland har också visat prov på sin kapacitet inom bland annat informationsarenan i samband med annekteringen av Krim och den pågående konflikten med Ukraina. I ett militärtekniskt perspektiv framkommer inget revolutionerande i artiklarna utan författarna nämner mer vad teknologiutvecklingen erbjuder för möjligheter och hur den påverkar respektive lands utformande av doktriner och militärstrategiska utveckling.

USA, Örnen

Robert Dalsjö beskriver att USAs militärstrategiska utveckling har sedan Gulfkriget och med det uppvisande av sina högteknologiska landvinningar öppnat dörren till en ny typ av krigföring där teknologiutvecklingen återigen har fått en tydligare roll och betydelse. Det finns många andra exempel i historien när teknologiutvecklingen påverkar krigskonsten och omkullkastar tidigare doktriner och Gulfkriget kan förmodligen sällas till dessa omslagspunkter, likt svartkrutets eller stridsvagnens införande på slagfältet. Historien får utvisa om det är en korrekt iakttagelse. Gulfkriget, tillsammans med Sovjetunionens upplösning och Rysslands ekonomiska situation, skapade en unik frontposition för USA som en till synes oövervinnlig stormakt. Kina hade vid tillfället fortfarande en underutvecklad och föråldrad arme (PLA, People´s Liberation Army) som inte utgjorde något större strategiskt hot mot USA.

I samband med Sovjetunionens kollaps så kom USAs militärstrategiska fokus att flytta sig mot Asien och stödja de allierade länderna i området som till exempel Filipinerna, Japan, Sydkorea och Taiwan. De var oroade för Kinas växande försök att skapa dominans i området och tränga ut USA, som dominerat området sedan andra världskrigets slut. Ett större försök gjorde Kina i samband med valet i Taiwan 1996 när man försökte hindra en, i Kinas ögon, misshaglig presidentkandidat att komma till makten. USA svarade med en styrkedemonstration genom att sända två hangarfartygsgrupper till Taiwans undsättning. Efter den läxan, som vissa menar är en omslagspunkt för Kina, insåg Kina sin underlägsenhet och intensifierade arbetet med att bygga upp en förmåga för att begränsa USAs förmåga till maktprojektion i området. Kina har sedan dess byggt upp ett program, som i USA benämns Anti-Access/Area Denial (A2/AD). Programmet bygger på att dels hindra eller försvåra för en motståndare (USA) att ta sig till området (Anti-Access) och dels hindra eller försvåra för en motståndare att upprätthålla sig i och verka i området (Area Denial).

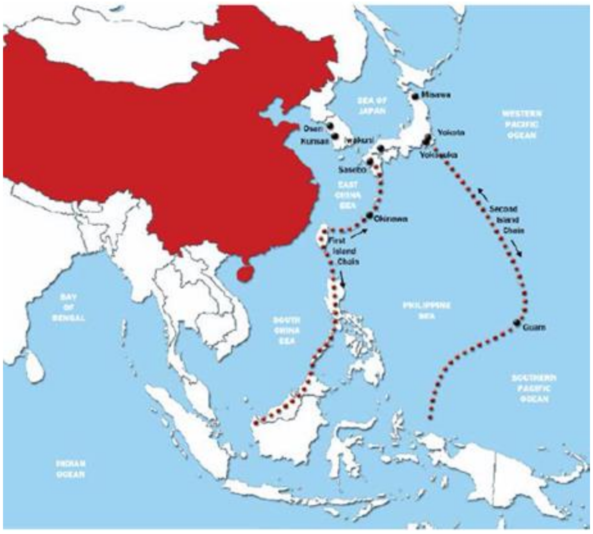


Figure 8. The Two Island Chains and Major Bases in the Western Pacific, hämtad från van Tol et al., sid 13. Återges i ref [7] med tillstånd från CSBA online.

Området omramas av en gräns på ca 1500 nm från Kinas kust och inringar USAs allierade i området.

USA har, för att möta hotet från Kina, tagit fram ett koncept som de kallar Air-Sea Battle (ASB). Konceptet är under ständig utveckling och omgiven av sekretess men författaren har valt att lyfta fram följande ledord som syntentiserar vad konceptet handlar om:

Networked; förmåga att kunna genomföra integrerade operationer på alla arenor utan hinder av försvarsgrensgränser.

Intergrated; Snarlik med föregående punkt men med fokus på försvarsgrensgemensam operationsträning innan insättning i operationsområdet.

Attack-in-depth; angrepp mot motståndarens kritiska svaga punkter för att begränsa dennes förmåga att utöva A2/AD.

Utöver ledorden nämns även *Disrupt* vilket avser att störa motståndarens C4ISR-system, *Destroy* vilket avser att bekämpa motståndarens A2/AD-vapensystem och slutligen *Defeat* vilket avser att slå tillbaka angrepp från motståndaren genom att till exempel skjuta ner missiler etc. För att konkretisera A2/AD-konceptet behöver Kina, enligt USA, utveckla ny teknik med anti-satellitvapen, cybervapen, förmåga till långräckviddig målinmätning, långräckviddiga kryssnings- och ballistiska missiler med hög precision, moderna tysta ubåtar med moderna torpeder och minor, avancerade sjöminor, moderna luftförsvarssystem, spanings-, lednings och attacknätverk för alla arenor och slutligen ett robust och integrerat ledningsnätverk.

ASB-konceptet är omtvistat i USA och företrädare för markarenan känner sig utanför och är oroliga för att satsningarna på konceptet kommer att negativt påverka satsningar på den egna arenan. Vissa menar även att ASB går mot det totala kriget där Kina kommer att trängas in och tvingas till motåtgärder som bara kommer att eskalera situationen - ett koncept utan strategi kommer att skapa farliga situationer. Man menar även att om kriget når Kinas fastland så har inte USA tillräckliga resurser för att kunna avsluta det.

Motståndarna till ABS framför istället att Kina, med dess känsliga geografiska läge och stora behov av sjötransporter kan mötas; med fjärrblockad av strategiska förträngningar i sjöhandelsvägarna, med asymmetrisk sjökrigföring i Kinesiska vatten och med stärkandet av allierades motståndsförmåga. Lösningen skulle även innebära ett bättre försvar mot Kinas asymmetriska salamitaktik som varit framgångsrik sedan några år i Kinesiska sjön.

USA har också att hantera ett mer aggressivt Ryssland som med den senaste tidens eskalation börjar innebära ett reellt hot mot både NATO och Europa.

Ryssland, Björnen

I sin text om Ryssland beskriver Gudrun Persson att Ryssland har en lång tradition av militärt tänkande, från Tsar-tiden såväl som från Sovjet-tiden och författaren menar att debattklimatet för strategiska diskussioner alltid haft högt i tak inom de ramar som ledningen tillåtit. Debatten har förts i många olika riktningar och med olika grupperingar och det sägs råda en djup konflikt mellan två huvudläger där det ena lägret vill framhäva behovet av modern teknologi och det andra lägret vill framhäva den ryske soldatens särskilda kvaliteter.

Det senaste 20 åren har det militärstrategiska tänkandet präglats av två olika fenomen; teknologisk utveckling och samhällsförändringarna i både Ryssland och omvärlden. Kopplat till det gäller även den identitetskris som Ryssland anses lida av efter Sovjetunionens fall, Rysslands krympta territorium och Rysslands roll i den pågående globaliseringen. Likt Kina och övriga världen så gav även Gulf-kriget 1991 en uppvaknade för Ryssland. USA uppvisade en teknologiutveckling/användning som tydligt visade hur långt efter Ryssland och ryska vapensystem var och förhållandet gav ett stort avtryck i det fortsatta ryska militära tänkandet och givetvis den militärteknologiska utvecklingen.

Under de senaste åren så har de ryska relationerna med omvärlden försämrats av olika orsaker, bl.a. kriget mot Georgien 2008 och annekteringen av Krim med den pågående konflikten med Ukraina samt även till viss del den ryska delaktigheten i den pågående konflikten i Syrien. Ryssland känner sig hotad av sin omvärld och NATOs utbredning i Östeuropa har inte förbättrat situationen. Situationen har återspeglat sig i det ryska doktrinarbetet med en mer återhållsam syn på omvärlden och en tydligare beredskap mot konflikter. Förändringen är tydlig och kan kanske exemplifieras med att 2010 års militärdoktrin omarbetades i förtid för att träda ikraft i december 2014, vilket var tidigare än planerat.

Även om väst menar att den 6:e generationens krigföring är en viktig del i Rysslands militärstrategi så omnämns den inte i någon större grad i den ryska debatten eller i doktrinarbetet. I 2014 års militärdoktrin lyfts istället andra delar fram även om doktrinen påtalar betydelsen av befolkningens protestpotential, irreguljära väpnade grupper, politiska krafter och samhälleliga rörelser som finansieras och styrs utifrån. Det är tydligt att man även visar på behov av att kunna klara av protester inom Ryssland, där särskilt unga ryssar ses som större hot än i tidigare doktrin. Intressant är även att Ryssland menar att den 6:e generationens krigföring är något som är skapat och används av väst och som Ryssland numera blir utsatt för. Man menar även att den Arabiska våren, som kanske kan vara ett exempel på 6:e generations krigföring, skapades och sjösattes av USA.

Kärnvapendoktrinen är i huvudsak intakt jämfört med tidigare doktriner med avskräckning och upprätthållande av global strategisk stabilitet som huvudsyften. Samtidigt så finns det en del som tyder på att taktiska kärnvapen lyfts fram som ett av de mer betydelsefulla vapnen för att förhindra militärt angrepp på Ryssland.

Enligt författaren så ser vissa militärstrategiska tänkare i Ryssland att det framtida kriget kan särskiljas i följande former:

- Upprorskrig; avseende icke-traditionella former av krig med t.ex. terrorism, olagliga militära grupperingar, informationsoperationer och psykologisk krigföring.
- Distanskrig eller kontaktlösa krig; ett krig utan direktkontakt mellan de stridande på slagfältet. Viktigt är tillgång på långräckviddiga precisionsvapen och underrättelser.
- Informationskrig; med cyberoperationer, elektronisk krigföring, inflytelseoperationer etc.
- Medvetandekrig eller samvetskrig; där gränsen mellan krig och politik har suddats ut. Kriget kommer att föras med informationsmedel och vara psykologiskt till formen. Här angrips landets kultur och historiska traditioner, d.v.s den nationella identiteten. Enligt den här idén så har det 3.e världskriget redan avslutats då det pågick mellan 1945-1975. Det 4:e värdskriget påbörjades i början av 1980-talet med info-operationer vilket ledde till Sovjetunionens kollaps och nu har det 5:e världskriget påbörjats med angrepp på Ryssland av väst.

Kina, Draken

In sin text om Kina skriver Kaan Korkmaz att Kinas militärstrategiska utveckling har vissa likheter med Rysslands. Likt Ryssland så har Kina legat långt efter väst och Gulfkriget 1991 samt Taiwankrisen 1996 visade tydligt hur mycket som behöver göras för att kunna mäta sig med USA som stormakt.

Kina har under en lång tid haft en stark ekonomisk tillväxt vilket också återspeglats i de militära satsningarna. Under de senaste 20 åren har försvarsanslagen ökat med över 10% årligen vilket innebär att anslagen ökat med ungefär 7 gånger under perioden. Den växande ekonomin har även ökat kraven på handels- och transportförbindelser med omvärlden och eftersom ca 50% av handeln sker sjövägen så har intresset av att säkerställa sjöfartsvägarna ökat i betydelse. Om sjöfartsvägarna skulle skäras av skulle landet sannolikt kastas i ekonomisk kollaps på kort tid. Vid sidan av intresset för sjöfartsvägarna så ser Kina även att den ekonomiska tillväxten ger möjligheter till att förverkliga både gamla och nya territoriella anspråk, t.ex. återföra utbrytarnationen Taiwan till moderlandet. Men eftersom USA med dess flotta fortfarande dominerar området så har Kina stora svårigheter att hävda sina intressen.

PLA (People´s Liberation Army) utveckling startade i samband med kulturrevolutionen 1949 och har varit Kommunistpartiets främsta verktyg för att säkerställa sin egen existens. De doktriner som styr PLA är dock inte öppna för utomstående så det råder en viss osäkerhet om vilka strategiska mål som PLA utvecklas mot. Viss dokumentation i form av halvofficiella dokument finns tillgänglig och viss debatt råder, men underlaget är osäkert och i många fall utgår bedömare från de materielsatsningar som Kina gör för att försöka bedöma vilka vägval Kina gjort och vilka strategiska mål och säkerhetspolitiska intressen som de drivs av. Kina har till exempel genomfört stora satsningar på hangarfartyg, anti-satellitmissiler, stridsflyg med stealth-förmåga och ubåtar, både atomdrivna och diesel-elektriska. Man är också relativt öppen med satsningarna och väl medveten om signaleffekten.

Kommunistpartiet har satt upp tre kärnintressen för Kinas säkerhetspolitiska intressen och PLAs moderniseringsprocess:

- Säkerställa Kommunistpartiets fortsatta maktställning
- Säkerställa Kinas nationella suveränitet
- Säkerställa Kinas fortsatta ekonomiska och social utveckling

Alla tre kärnintressena berör PLAs utveckling och strategiska målsättning. Även om namnet PLA antyder att det är folkets arme så är PLA i grunden Kommunistpartiets arme med sin främsta uppgift att säkerställa Kommunistpartiets maktställning. I samband med massakern på Himmelska fridens torg 1989 så har dock den rollen som upprätthållande av den inre säkerheten i Kina nedtonats något och man låter andra statliga organisationer ansvara för den delen.

Författaren pekar på att med utgångspunkt i tillgänglig dokumentation så inrymmer den militärstrategiska utvecklingen numera även rymden och cyberområdet. Vidare så deltar även PLA i olika fredsfrämjande operationer och andra internationella uppdrag, bland annat inom ramen för FN.

De framtida konflikterna eller krigen som Kina kommer att bli involverade i kommer sannolikt inte, enligt kinesiska bedömare, vara totala krig utan mer av vad det kallar lokala krig (Local Wars). Kriget genomförs med i grunden begränsade politiska och militära mål och syftet är inte att tillintetgöra fienden utan handlar mer om att säkerställa territorier, naturtillgångar eller handelsvägar. Den moderinseringsprocess som PLA genomför är också inriktad mot att möta förmågebehoven för lokala krig. Enligt vissa bedömare är dessa scenarior:

1. Relativt stort och högintensivt ”anti-separatist”-krig mot Taiwan. Bedöms som sannolikt och är ett högriskscenario.
2. Småskaligt och lågintensivt krig över omtvistade territorier och sjöområden. Bedöms med viss sannolikhet och viss risk.
3. Ett omfattande högintensivt defensivt krig på det kinesiska fastlandet. Bedöms vara ett osannolikt högriskscenario.
4. Småskaliga och lågintensiva kontraterrorism- eller stabilitetsoperationer. Tillskrivs ingen sannolikhets- eller riskbedömning

Ryssland, efter Sovjetunionens fall, är inte längre huvudfienden utan istället har USA med sina allierade i Kinas närområde blivit ett allt större hot då de kan hota handelsvägarna och därmed Kinas ekonomiska situation. Konceptet med A2/AD som USA försöker bryta ner med sitt ASB-koncept kan därvidlag vara av viss aktualitet. Teknikutvecklingen som krävs för ett A2/AD-lösning är fortfarande en bit bort för Kina och vissa nödvändiga tekniker saknas fortfarande innan det kan realiseras. Se USA, Örnen enligt ovan.

Den militärtekniska utvecklingen enligt FOI-författarna

Samtliga författare gör tydliga kopplingar mellan teknikutvecklingen och ländernas strategiutveckling tillsammans med doktrinära stadsfästelser och ambitioner. De slår också fast att det är tekniken som ger möjligheterna men också skapar en hotbild gentemot det egna landets utveckling och strävande. Ingen av författarna berör särskilt djupt vilka delar i den framtida tekniken som kommer att vara särskiljande på slagfältet men de pekar på att de nya arenorna med rymd och cyber, tillsammans med långräckviddiga precisionsvapen, kommer att ha stor betydelse i framtiden. Kopplingen till Rysslands annektering av Krim och 6:e generationens krigföring med asymmetri och infooperationer är tydlig även om Ryssland internt anser att det inte är något revolutionerande utan en beståndsdel som alltid funnits i all krigföring. Det nukleära kriget med stora kärnladdningar har tonats ner till förmån för konventionella vapensystem och i doktrinarbetet ges inte dessa vapen särskilt mycket utrymme förutom att författarna nämner att länderna är tydliga med att andraslagsförmågan måste vara intakt. Det finns dock en viss skillnad mellan ländernas syn på kärnvapen där Ryssland tydligare framhäver sin roll som kärnvapenmakt och det finns indikationer på att taktiska kärnvapen ges en större roll än tidigare i det ryska doktrinarbetet.

Ingen av författarna går i sina artiklar speciellt djupt in på vad teknologiutvecklingen kan skapa för framtida vapensystem och vad de skulle få för strategisk betydelse. Robert Dalsjö nämner vilken utvecklingsväg Kina behöver gå för att realisera A2/AD-konceptet men det gäller främst anskaffningar av dagens moderna vapensystem för att komma ikapp västvärldens och Rysslands försprång. Han nämner också strålvapen för försvar av baser och högvärda fartyg mot mättnadsanfall med främst ballistiska robotar. Ingen av författarna utvecklar heller förmågan till störningar i informationsmiljön, något som alla tre stormakterna, vid ett antal gånger visat exempel på att inneha god kapacitet för.

Reflections on the method used in the report

Our evaluation of the method used shows that there is a risk the assessment is biased by the participating experts' presumptions and experiences from their own field of research. The scenarios that were chosen do not cover all aspects of the technology and their possible contribution to operational capabilities. It should be stressed that we have assessed the five technologies' potential military utility in the presented scenarios, not the technology itself.

The chosen definition of 'military utility' clearly affects the result of the study. The definition is the same that has been used in the Technology Forecast since 2013. It is believed to be good enough for this report, but could be further elaborated in the future.

The greatest value of the method used is its simplicity, cost effectiveness and the tradeoff that it promotes learning within the working group. The composition of the working group and the methodology used is believed to provide for a broad and balanced coverage of the technologies under study.

This report provides executive summaries of the Fraunhofer reports which are believed to help the SwAF Headquarters to evaluate the military utility of emerging technologies within identified relevant scenarios.

The last chapter of the report is an executive summary of a report from FOI analyzing thinking and debate on war and warfare in three military great powers: USA, Russia and China. Obviously, that report cannot be fitted into our military utility assessment methodology.