Informationssäkerhet i radionät

ÅSA WAERN, TOMMY GUSTAFSSON

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se

FOI-R--3432--SE
ISSN 1650-1942 April 2012

Åsa Waern, Tommy Gustafsson

Informationssäkerhet i radionät

Titel	Informationssäkerhet i radionät
Title	Information security in radio network
Rapportnr/Report no	FOI-R--3432--SE
Månad/Month	April
Utgivningsår/Year	2012
Antal sidor/Pages	31 p
ISSN	1650-1942
Kund/Customer	FMV
FoT område	Ledning
Projektnr/Project no	E533665
Godkänd av/Approved by	Lars Höstbeck
Ansvarig avdelning	Informations- och aerosystem

Sammanfattning

Informationssäkerhet i radionät är en stor utmaning. Skyddsvärdet baseras många gånger på ett värsta scenario, vilket leder till att säkerhetslösningen blir både onödigt resurskrävande och administrativt betungande att hantera. Kan vi motivera en lägre sekretessnivå borde det innebära ett enklare administrativt arbete. Om bedömningen av informationssäkerhetsklassen kan göras i ett tidigt skede i designfasen skulle den kunna påverka tekniska lösningar. Det finns dock inte så mycket arbete gjort rörande radiosystemets teknik med hänsyn tagen till sekretessnivån.

Denna rapport redovisar en första ansats att bedöma olika tjänsters behov av sekretess. Bedömningen gjordes genom resonemang, men visar att det borde vara möjligt att bedöma behovet av sekretess från fall till fall eller från system till system. Rapporten redovisar även en litteraturstudie om dynamisk sekretessvärdering, overhead i radionät och multi level security (MLS).

Arbetet har uteslutande fokuserat på grupp, pluton och kompaninivå i markscenarion. Informationsinnehållet på högre nivåer omfattas inte. Därmed studeras inte strategisk planering på stabsnivå.

Nyckelord: sekretess, radionät, multi-level security, värdering

Summary

Information security in radio networks is a major challenge. The level of protection is based often on a worst case scenario which leads to a security solution that will be both unnecessarily costly and administratively burdensome to manage. Can we justify a lower level of security it would imply an easier administrative work. If the assessment of the information security class can be done at an early stage in the design phase, it could affect the technical solutions. However, there is not so much work done for radio system technology with regard to security classification.

This report presents a first attempt of assessing different services security requirements. The assessment was done by reasoning, but shows that it should be possible to assess the security requirements on a case or for a system. The report also presents a literature review on dynamic security assessment, overhead and multi-level security (MLS). The work has focused exclusively on the group, platoon and company level in ground scenarios. The information content at higher levels, e.g. strategic planning, are not included.

Keywords: security, radio network, multi-level security, assessment

Innehållsförteckning

1 Inledning

Informationssäkerhet i radionät är en stor utmaning. Ofta hanteras säkerheten på radionätet i slutdesignfasen, vilket kan leda till att säkerhetslösningen brister i prestanda och skyddsförmåga. Skyddsvärdet baseras också många gånger på ett värsta scenario vilket leder till att säkerhetslösningen blir både onödigt resurskrävande och administrativt betungande att hantera. Skulle vi i en driftsatt plattform kunna anpassa säkerhetslösningen för att hantera kraven för respektive uppgift skulle det kunna ge flera fördelar. Ett sådant område är administrationen där informationssäkerhetsklassningen medför en administrativ process, ju högre sekretessnivå desto mer omfattande process. Kan vi motivera en lägre sekretessnivå borde det innebära ett enklare administrativt arbete. Om bedömningen av informationssäkerhetsklassen kan göras i ett tidigt skede i designfasen skulle den kunna påverka den tekniska lösningen av systemet. Det finns dock inte så mycket arbete gjort om vi studerar radiosystemets teknik med hänsyn tagen till sekretessnivån.

Denna rapport redovisar en första ansats till att bedöma olika tjänsters behov av sekretess och vad det skulle kunna få för konsekvenser för designen av radionätet. Rapporten redovisar även en litteraturstudie om dynamisk sekretessvärdering, overhead i radionät och multi-level security (MLS) samt ett exempel på kommunikationsscenario med sekretessaspekter.

Arbetet har uteslutande fokuserat på grupp, pluton och kompaninivå i markscenarion. Informationsinnehållet på högre nivåer omfattas inte. Därmed studeras inte strategisk planering på stabsnivå.

2 Tjänster i radionät

För en lyckad design av ett radiosystem är kunskapen om slutanvändarens behov av kommunikationstjänster avgörande. Vanligtvis tas behoven fram via enkäter, interjuver eller speciella studier. Exempel på projekt där behovet av kommunikationstjänster studerats är Wolf [1] och COALWNW [2]. För att få de olika behoven hanterbara är det bekvämt att gruppera dem i olika klasser av information, vilket gjorts i projekten Wolf och COALWNW. I Wolf-projektet klassades tjänsterna enligt tabell 1.

WOLF		
Tjänst	Kompanichef till	Informationsklass
alternative plans before approval	TFCP, Platoon comm	planning
intelligence	TFCP, Platoon comm	planning
Tactical overlays	TFCP, Platoon comm	planning
Entities and symbols	TFCP, Platoon comm	planning
GIS thematic maps	TFCP, Platoon comm	planning
warning orders	Platoon comm, Squad comm	Directions and combat orders
operations orders	Platoon comm, Squad comm	Directions and combat orders
Patrol orders	Platoon comm, Squad comm	Directions and combat orders
Fragmentary order	Platoon comm, Squad comm	Directions and combat orders
text	TFCP	Reports and warnings generation
images	TFCP	Reports and warnings generation
video	TFCP	Reports and warnings generation
logistic request	TFCP	Combat service support
logistic report	TFCP	Combat service support
medical evacuation	TFCP	Combat service support
call for fire	TFCP	Combat support
close air support	TFCP	Combat support

XML-like messages	TFCP	Synchronization of SA info and LOP generation
alternative plans before approval	TFCP	COP reception
intelligence	TFCP	COP reception
Tactical overlays	TFCP	COP reception
Entities and symbols	TFCP	COP reception
GIS thematic maps	TFCP	COP reception
alternative plans before approval	Platoon Comm	CROP dissemination
intelligence	Platoon Comm	CROP dissemination
Tactical overlays	Platoon Comm	CROP dissemination
Entities and symbols	Platoon Comm	CROP dissemination
GIS thematic maps	Platoon Comm	CROP dissemination

Tabell 1: Olika tjänster i ett radionät kan med fördel grupperas i olika informationsklasser. Tabellen visar tjänsternas gruppering enligt Wolf-studien. TFCP står för Task Force Command Post, COP är Common Operational Picture, CROP är Common Relevant Operational Picture

Tjänsterna och informationsklasserna i tabell 1 är inte kompletta utan visar exempel på tjänster som kan grupperas till samma informationsklass och kan antas ha samma sekretessnivå.

3 Scenarier för sekretessbedömning av kommunikationstjänster

Informationssäkerhetsnivån i ett radionät är kritiskt. Har vi för låg säkerhet så kan kanske vem som helst höra vad som sänds men har vi för hög säkerhet blir den onödigt komplicerad att hantera. För att kunna välja rätt sekretessnivå är det önskvärt att på ett systematiskt sätt kunna värdera informations-innehållet från fall till fall. Om vi har metoder för att värdera informations-innehållet skulle vi kunna applicera lämplig sekretessnivå för varje enskild operation eller system.
Som en första ansats att bedöma värdet på informationen, d.v.s. hur känslig informationen är ur sekretessperspektiv, genomfördes en workshop på FOI den 13 februari 2012. Informationen hade grupperats i olika klasser enligt tabell 1. Informationens känslighet för spridning samt under hur lång tid informationen var känslig studerades sedan i tre olika scenarier.

Scenario 1:

Scenariot är hämtat från Wolf-projektet och beskriver en operation där ett kompani ska genomsöka och säkra en byggnad, bild 3.1.

Kompani B har fått i uppgift att säkra tre byggnader inne i staden efter uppgift om att upprorsmän befinner sig där. Byggnaderna ligger i ett område med större tegelbyggnader, ca 8 våningar höga och 50 m långa. På gatan utanför finns två nedgångar till tunnelbanan. Uppgiften är att säkra byggnaderna och tillfångata upprorsmännen. Kompaniet är uppdelat i tre plutoner som får följande uppgifter:

Grön pluton, yttre stödfunktion:

- Säkra utomhus runt byggnaden
- Hindra att någon tar sig ner i tunnelbanan
- Övervaka omgivningen för att förhindra fientlig eld till stöd för upprorsmännen

Blå pluton, attackstyrka:

- Gå in och säkra byggnaderna inifrån. Inbrytningen sker från norr

Röd pluton, inre stödfunktion:

- Stödja Blå pluton under aktionen
- Förmedla lägesbild till Blå pluton
- Ta hand om tillfångatagna upprorsmän
- Ta hand om skadade

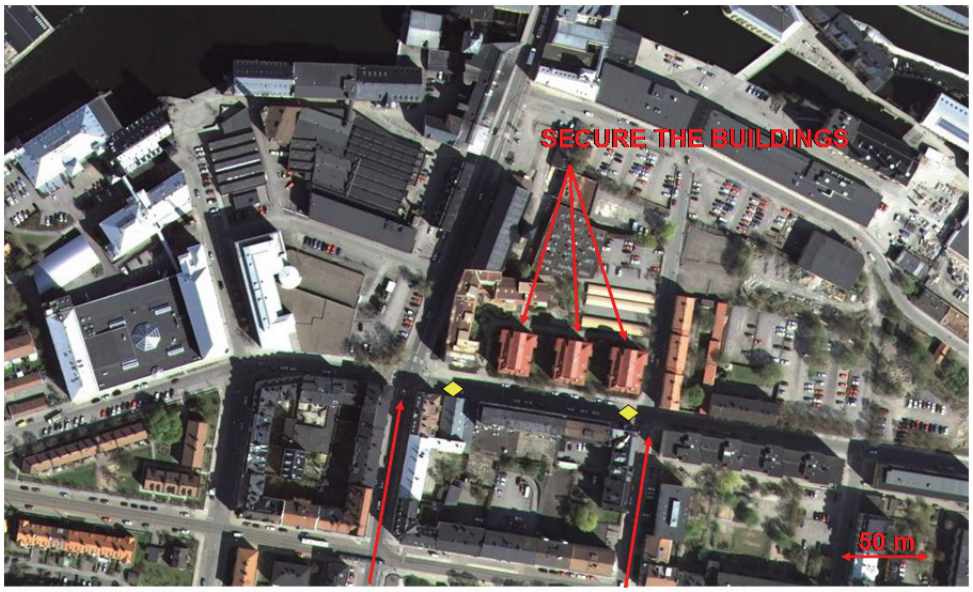


Bild 3.1: Karta som visar området där byggnaderna finns.

Scenario 2:

Även detta är hämtat från Wolf men är omarbetat och beskriver ett anfall i en hamn, bild 3.2. Anfallet genomförs av tre kompanier. Orange och grönt kompani genomför anfallet och blå kompani stödjer genom att skydda norra, nordvästra flanken mot krypskyttar och indirekt eld. I scenariot studerar vi en microsituation, bild 3.3, där två plutoner från grönt och orange kompani gemensamt närmar sig ett mål. Plutoncheferna från de olika kompanierna har då behov av att samverka och till hjälp finns funktioner i form av såväl markunderstöd som flygunderstöd. Några mål av intresse har angivits på förhand vid planeringen av anfallet men ytterligare information om målen kan vara önskvärd under genomförandet, främst för att underlätta ett eventuellt flygunderstöd.

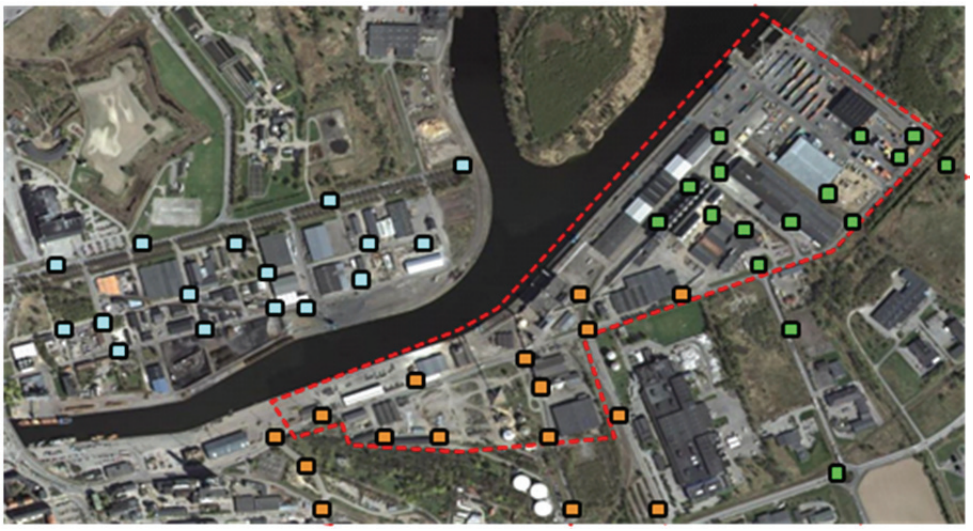


Bild 3.2: Karta som visar hela området där anfallet sker.

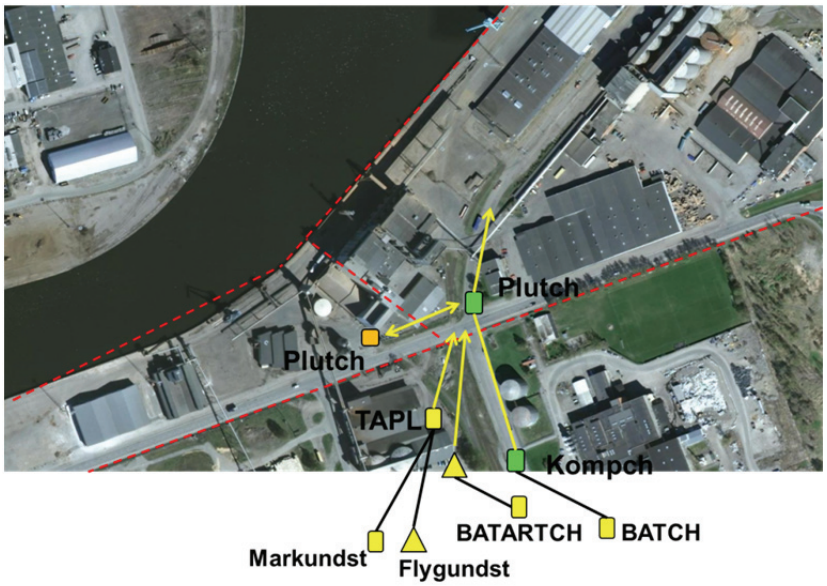


Bild 3.3: Karta som visar området för microsituationen i anfallet.

Scenario 3:

Detta scenario beskriver en fordonskolonn där ett antal lastbilar transporterar förnödenheter, bild 3.4. En lastbilskonvoj kan innehålla upp till 32 långtradare och 4 terrängbilar. Konvojen blir då 3-4 km lång. Konvojen organiseras så att en terrängbil åker före konvojen och rekognoserar så att färdvägen är framkomlig. Därefter följer lastbilskonvojen med resterande terrängbilar placerade först, sist och i mitten. Huvuduppgiften för dessa är att hålla ihop konvojen, arrangera säkra raster och assistera vid eventuella problem. Plutonchefen åker i första bilen. Kompanichefen och bataljonschefen befinner sig på campen. I detta fall är det en transport av förnödenheter som beräknas ta 10 timmar att genomföra inkluderande 2 raster. Rasterna tas på förbestämda platser där samtliga fordon kan parkera.


Pansarterrängbil 203 A.
Foto: Lukas Linné/Försvarsmakten

Bild 3.4: Fordonskollonen eskorteras av terrängbilar

Minnesanteckningar från workshopen redovisas i bilaga 1.

4 Värdering av sekretessbehov – resultat från workshopen

Informationsinnehållet diskuterades utifrån de olika informationsklasserna. För varje informationsklass gavs exempel på tjänster som kan grupperas till klassen från tabell 1 ovan. Tjänsterna diskuterades först allmänt och sedan för de olika scenariona. Resultatet redovisas i nedanstående tabell 2.

Informa-tionsklass	Tjänst	Allmänt	Scenario 1	Scenario 2	Scenario 3
Planning	- Alternative plans - Intelligence - Tactical overlays - Entities and symbols - GIS thematics maps	Inför en insats kan en stridsplan överföras. Stridsplanen kan innehålla planerad rutt med stoppunkter (fordonsavlämningsplats, inbrytningspunkt, mm) inlagda.	Plutonen på gatan är mer utsatt än de i byggnaden. Positionsdata kan vara skyddsvärd men kortlivad	Positionsdata har kort livslängd. Rör vi oss är den mer eller mindre ointressant för fiende	Positionsdata kan vara känslig eftersom den visar vilken väg vi valt och att vi sannolikt kommer använda den igen. Positionsdata kan ge information om hur lång tid det tar att färdas sträckan.
Orders (directions and combat orders)	- Warning orders - Operations orders - Patrol orders - Fragmentary orders - Tactical maneuver	Orderinformation kan vara känslig men ofta kortlivad. Livslängden på en order ökar dock för varje organisatoriskt steg.	Bataljonchefen (task force command post) har delegerat uppgiften till Kompanichefen och ger därför normalt inga order. Kompanichefen är troligtvis med inne i huset.	Ordrar är skyddsvärd men kort livslängd. Kan anslöja vad vi vet om fiende. Samordning mellan kompanierna. Kompanicheferna måste kunna samordna manöver.	Ordrar här består främst av trafikledning.
Report and warning generation	- Text - Images - Video	Rapportering sker oftast i text men bilder är mer intressant.	Bilder kan vara intressant att förmedla. Det kan vara bilder på hur det ser ut inne i huset eller objekt man upptäcker på vägen.	Bilder på anfallsmål är högintressanta för den egna organisationen, men även fiende.	Skickar bild om något är fel/tveksamt mm, tex en sönderkörd bro. Informationen har lång livstid eftersom det är bra ingångsdata till nästa gång man kör transporten.
Combat service support	- Logistic request - Logistic report - Medical evacuation	Bataljonschefen bestämmer sjukhanteringen genom kvartermästaren. Sjuktransporten får positionsdata vart de ska vilket kan ha betydelse för fienden.	Logistiken består troligtvis av mattransporter och ev ammunition framåt och evakuera skadade bakåt.	Under förutsättning att det går som planerat så består logistiken bara av att evakuera skadade.	Konvojen har med sig nödvändig utrustning själva. De är mest utsatta när de tar rast.
Combat support	- Call for fire - Close air support - Call for QRF	Indirekt eld har en kort livslängd. Lägger man in mål i förtid, i planeringsstadiet kan det underlätta	Helikoptrar kan tänkas sätta ner folk på taken.	Helikoptarar kan lyfta ut enheter i kanterna i insatsområdet. De flyger inte in i insatsområdet. Om de gör det så flyger de i förbestämda	Det finns larmstyrkor, QRFer (quick reaction force), som är beredda att rycka ut. Det är intressant för

		målangivelse under operationen, då får informationen betydligt längre livslängd men man skulle kunna uttrycka tex ordrar på ett annat sätt. För flygunderstöd skickas målkoordinater, typ av ammunition och klockslag.		korridorer där man inte får skjuta.	fienden att veta hur lång tid det tar för dem att nå platsen.
Synchronization of SA info and LOP generation	Tolkar tjänsten som att det handlar om att komma överens om lägesbilden.	Mycket tal. Försök har visat att ett bättre datorstöd (mer information) ger högre kvalitet på samtalen mellan cheferna. Det är svårt att bedöma känsligheten i tal. Kanske kan mottagaren av talmedelandet indikera en känslighetsnivå.			

Tabell 2: Informationsinnehållets känslighet diskuterades utifrån de tre specificerade scenarierna.

4.1 Slutsats från workshopen

Workshopen genomfördes i syfte att se om det är möjligt att bedöma behovet av säkerhet med tanke på informationsinnehållet, d.v.s. hur känslig är informationen i sig och under hur lång tid är den känslig för spridning? I detta fall gjordes bedömningen genom ett resonemang. Resultatet visar att det borde vara möjligt att värdera behovet av sekretessnivå men bedömningen bör ske med en mer strukturerad metod. FOI har tidigare genomfört tekniska värderingar av kommunikationssystem och sensorsystem med hjälp av COAT-metoden [3, 4]. Genomförs en värdering av informationsinnehållet med hjälp av COAT skulle resultatet bli spårbart och det blir lättare att förstå vilka val och prioriteringar som gjorts.

Det finns flera fördelar med att situationsanpassa sekretessnivån. Dels kan administrationen som följer med sekretessnivån påverkas positivt, dels kan sekretessnivån påverka möjligheten att optimera överföringen av data.

Workshopen visade också att en strukturerad värdering av sekretessnivån kan resultera i att systemet får en lägre sekretessnivå än vad som annars skulle vara fallet.

5 Litteraturstudie

Workshopen visade att det bör gå att värdera behovet av sekretessnivå från fall till fall eller från system till system. För att undersöka vilken påverkan sekretessnivån kan ha på tekniska lösningar genomfördes en begränsad litteraturstudie.

Bandbredd, energitillgång, sändartid och processorkraft är exempel på begränsade resurser i Försvarsmaktens operativa miljö. Därför är det viktigt att kommunikationen i ett radionät sker så effektivt som möjligt. På ett tekniskt plan är det önskvärt att kommunikationen sker med rätt sekretessnivå samt att trafiken innehåller så lite overhead, dvs information som inte är nyttodata, som möjligt. En begränsad litteraturstudie med fokus på dynamisk sekretessvärdering samt optimering av kommunikationen med avseende på overhead har därför genomförts.

5.1 Dynamisk sekretessvärdering

Dynamisk sekretessvärdering är en term som använts i denna förstudie för att beskriva en process för att i realtid automatiskt värdera data ur ett sekretessperspektiv. En dynamisk sekretessvärdering säkerställer att varje uppgift hanteras och skyddas korrekt. För ett radiosystem kan detta till exempel vara intressant eftersom det då går att välja den krypteringsmetod som kombinerar tillräckligt skydd med så låg resursförbrukning som möjligt. Vidare är det intressant eftersom det kan minska exponeringen av kryptogram vilket i sin tur försvårar knäckning.

Söktermer
För att finna tidigare forskning inom området för dynamisk sekretessvärdering har följande söktermer används:
assess information, security, content based security classification, differentiated security, multi-level security, dynamisk informationsvärdering, assessing confidentiality, sekretessvärdering, dynamisk sekretessvärdering

Sammanställning
Dynamisk sekretessvärdering visade sig vara ett relativt outforskat område, vilket kan bero på svårigheten att automatiskt tolka textbaserad information [5]. Det finns dock forskning som ger exempel på hur dynamisk analys och hantering av sekretess kan ske, men i dessa fall har alltid någon form av värdering redan gjorts [6, 7]. Det finns också exempel på mer användar-orienterade system men även dessa använder någon form av fördefinierad värdering [8]. Den dynamiska analysen och hanteringen består i de fall som presenteras här i princip av en sammanställning av redan givna värden men angriper inte själva grundproblematiken, d.v.s. att göra den första värderingen.

5.2 Effektivisering av kommunikation

Overhead är en branschterm för den del av trafiken som inte utgörs av nyttodata. Det kan till exempel röra sig om adresseringsdata eller krypteringsinformation som skickas i samma paket som nyttodata, eller ren trafikinformation som utbyts separat. För nätverk som kan hantera 10, 100 eller 1000 Mbps är overhead sällan ett problem men för radionät med kapaciteter som kan vara så låga som 1 kbps kan belastningen från overhead inte ignoreras. Detta är inte minst viktigt eftersom många protokoll och lösningar idag utvecklas för högre bandbredder varför en tillräcklig optimering inte alltid sker under utvecklingen.

En annan aspekt av effektivisering av overhead är att själva databehandlingen sker så effektivt som möjligt, till exempel vid kryptering och dekryptering. En ineffektiv behandling kan leda till längre svarstider och ökad energiförbrukning. Återigen är en del av problematiken att många protokoll och lösningar idag utvecklas från perspektivet att användaren sitter på en kraftfull utrustning med ansluten strömkälla och med tillgång till ett snabbt nätverk, något som inte motsvarar Försvarsmaktens operativa miljö.

Söktermer
För att finna tidigare forskning inom området för optimering av kommunikationen har följande söktermer används:
Overhead, security performance, encryption overhead, optimized header, bandwidth optimization, multi-level security.

Dessa ord har på varierande sätt kombinerats med orden:
network, radio och wireless.

Trafikdata

Det finns flera möjliga metoder för att effektivisera trafikdata. En metod som är vanligt förekommande är att statiskt eller dynamiskt anpassa paketstorleken baserat på nätverk och trafiktyp [9, 10]. En annan metod är att anpassa så kallade headers[1] till det nätverk som de trafikerar så att de inte bär med sig onödig information [11]. Ytterligare metoder är att sätta samman nyttodata från olika paket till ett paket med en header [11] eller att se till att samma data endast skickas en gång [12].

Kryptering

Med avseende på kryptering, var en första uppgift för litteraturstudien att kartlägga hur olika krypteringsalgoritmer och säkerhetslösningar påverkade kommunikationen. Inom detta område finns det mycket forskning som bland annat visar påverkan från kommersiella algoritmer i IPSEC [13] samt i trådlösa nätverk [14]. Vidare framgår av dessa studier att valet av algoritm har påverkan på svarstider, processoraktivitet och overhead som definitivt är relevanta att väga in när man hanterar kommunikation med låg bandbredd. Utöver rena prestandasiffror innehåller dessa artiklar metoder som kan användas för att utvärdera militära krypton på motsvarande sätt.

Vid kryptering finns det två huvudsakliga chiffreringsmetoder som kan användas, blockchiffer och strömchiffer. Förenklat innebär ett blockchiffer att ett block av förutbestämd storlek används för att kryptera ett meddelande medan strömchiffer sker löpande. Blockchiffer kan liknas vid att man packar något i en låda av en viss storlek och när nyttolasten är mindre än lådan behöver denna fyllas ut. Strömchiffer kan med motsvarande allegori liknas med att slå in något i bubbelplast och förpackningen anpassar sig då till storleken på det man skickar. Inom Försvarsmakten finns idag system som har paket med 51 bitar och om denna trafik skulle krypteras med ett blockchiffer på 128 bitar skulle det bli mycket krypteringsrelaterad overhead. Här borde valet således falla på strömchiffer men denna teknik bedöms inte tillräckligt utforskad ur ett säkerhetspespektiv utan istället föreslår

[1] Header är den del av ett paket som placeras längst fram och innehåller bland annat adresseringsdata och information om hur ett enskilt paket skall hanteras.

Younis mfl att man väljer mindre blockstorlek och en längre nyckel [15]. Påverkan från blockstorlek i förhållande till lösenordslängd bör dock utredas vidare eftersom det är oklart hur små block som är lämpliga.

Multi-level security

Multi-level security eller MLS är en samlingsterm som används för tekniker som kan hantera flera säkerhetsnivåer i samma system. Dessa tekniker skulle göra det möjligt begränsa antalet utrustningar som Försvarsmakten behöver. Younis mfl definierar fyra olika paketeringsmodeller baserat på sekretessnivåer och jämför hur man genom att sampaketera dessa kan påverka bandbreddsutnyttjandet i ett trådlöst MLS-nätverk [15]. Kidston presenterar en något enklare paketeringsmodell i [11].

Gamer mfl presenterar i [16] en metod som kan styra paket av en viss sekretessklass en viss väg i ett nätverk. Denna teori kan användas för att förhindra att sekretessklassad information hamnar i orätta händer även om flera personer med olika behörighet ansluter till ett gemensamt nätverk.

Samtliga teorier som presenteras i ovanstående artiklar förutsätter dock att någon form av sekretessmärkning redan gjorts.

6 Diskussion

För att bättre förstå vilka operativa krav som kan ställas på ett framtida radiosystem har förstudiegruppen valt att lyfta fram ett par behov som får exemplifiera detta. Dessa påvisar behovet av trafikoptimering samt att behandla flera informationssäkerhetsklasser i samma system.

6.1 Dynamik

Det är tänkbart att i förväg planera för hur radiosambandet under en insats kan se ut med avseende på vem som kommer att ha ett behov av att tala med vem. Det är även möjligt att fastställa vilka informationssäkerhetsklasser som gäller för respektive konversation men i enlighet med Moltkes konstaterande finns det inga planer som fullt ut överlever den första kontakten med fiendens huvudstyrka [19]. I en högintensiv stridssituation kan fiendens aktiviteter snabbt framtvinga nya behov av förändrade kommunikationsvägar och i en lågintensiv stridssituation kan en dynamisk kommunikationslösning ge ett betydande stridsövertag. För att hantera ett sådant behov behövs en säkerhetslösning som inte kräver i förväg fastställda kommunikationsvägar utan som dynamiskt kan anpassa sig efter rådande situation.

6.2 Dynamisk nyckelhantering

Dynamisk nyckelhantering är en teknik som innebär att krypteringsnycklar kan tillhandahållas vid behov. Detta gör det möjligt att kommunicera säkert men utan att samtliga nycklar i förväg måste installeras i enheten. Idag finns det lösningar för dynamisk nyckelhantering på den kommersiella marknaden och det är en teknik som eventuellt kan anpassas för Försvarsmaktens ändamål.

Andra fördelar med en dynamisk nyckelhantering är att det skulle bli enklare att byta ut en nyckel vid behov samt att en nyckel kan inaktiveras om den skulle hamna i fel händer.

6.3 Bandbredd

I takt med att tekniken som utnyttjar någon form av kommunikation utvecklas kommer det att behövas mer bandbredd. Det är till exempel tänkbart att ny utrustning innehåller funktioner som mäter och kommunicerar en enskild soldats hälsostatus och ammunitionsförbrukning och det finns redan system som åt andra hållet förmedlar stridsinformation. Allt detta kräver en uppkoppling med tillräcklig bandbredd. En lösning på ett sådant behov kan till exempel vara ett närområdesnät med en gemensam upplänk som alla använder. En annan lösning kan vara ett så kallat meshnät där trafiken väljer den lämpligaste vägen. Båda förslagen gäller främst för stationära nät. Oavsett vilken teknik som används är det viktigt att vi även optimerar paketen på ett effektivt sätt. Som Younis mfl skriver i [20] kan vanliga optimeringsscheman bli ineffektiva vid vissa trafikmönster.

6.4 Motståndskraft

Ett annat behov är motståndskraft mot fientlig verksamhet och förmågan att verka oupptäckt. En hel del sensordata är inte tidskritisk. Om vi väljer att sampacketera dessa data till fulla paketstorlekar kan det innebära att radion skickar information mer sällan.

6.5 Exempel på kommunikationsscenario

I detta avsnitt presenteras ett exempel på hur ett kommunikationsbehov kan se ut baserat på en variant av scenario 2. Scenariot inkluderar i flera fall ny teknik som är under utveckling redan idag eller som i annat fall bedöms möjligt inom 10-20 år. Ett exempel på sådan teknik är den igenkänningsteknik (IK) som Letalick mfl ger en bild av i [17].

Scenario

Scenariot utspelar sig enligt följande skeende. Ett kompani ges i uppgift att ta ett hamnområde för att beslagta en vapendepå samt att skaffa underrättelser om fientliga aktiviteter i området. Tre plutoner går in i respektive ansvarsområde. Stridsaktiviteten är till en början förhållandevis låg men en timme in i operationen meddelar underrättelsekällor att ett fientligt kompani framrycker från öster mot tredje pluton. Detta medför att insatsledningen omfördelar en grupp från första pluton i norr och en grupp från andra pluton i väster för att förstärka tredje plutons ställning. Dessutom skickas en förstärkningspluton från ett annat kompani till området samt understöd i form av två helikoptrar och fyra stridsfordon.

Informationsflöde

Vad är det för informationsutbyte som skulle vara tänkbar i detta scenario? Den första formen är rent tal som i stort sett skulle ske enligt dagens mönster, dock med undantaget att även direkt samband mellan marktrupp och understödseneheter kan ske via säkra kommunikationsmetoder. Utöver detta förmedlas en information från tekniska stödsystem, till exempel egen och fientlig positionsinformation till och från varje enskild soldat. Insatsledningen får löpande reda på ammunitionsåtgång, hälsoläge, värmekameror, ljud och video från enskilda soldater. Informationen ger en bild av skeendet som automatiskt eller manuellt sammanställs och vidarebefordras till berörda enheter i operationen. Denna förmåga innebär att egna enheter har information om var fienden befinner sig även om denne inte kan registreras med egna sensorer. Andra exempel på möjligheter är att en enskild soldat kan markera mål för både riktad eld och indirekt eld på bärbara enheter för att förenkla eldledning, eller att de framskjutna förbanden kan förses med administrativt stöd i form av tolkar och dylikt utan att sådana behöver befinna sig i främsta linjen.

Att klassificera sekretessnivån för tal är svårt. Möjligtvis skulle mottagaren av talet kunna avgöra behovet av sekretessnivå. Sker kommunikationen med högre chef eller understödsenheter skulle eventuellt sekretessnivån bedömas högre än om kommunikationen sker inom gruppen.

Sekretessnivån på transmitterad sensordata skulle kunna bestämmas genom att tagga informationstypen, enligt tabell 1, med en förbestämd sekretessnivå.

Sekretessnivån skulle också kunna bestämmas genom att vi delar upp kommunikationsnätet i flera delnät med olika sekretessnivåer för de olika delnäten. Varje soldat har en anslutning till sin grupp genom ett närområdesnät och utgör därmed en kommunikationsnod. Från varje grupp finns det sedan två eller flera noder som har anslutningar till det uppdragsgemensamma nätverket. Varje nod kan ansluta till andra gruppers nätverk beroende på situation och behov. Dessutom är det tänkbart att trafiken studsar via en nod till en annan för att på så sätt nå det uppdragsgemensamma nätverket. De omfördelade grupperna och den nyanlända plutonen kan på så sätt upprätta ett direkt samband med den närmaste stridsgruppen, det vill säga tredje pluton. De understödsenheter som ansluter till striden utgör direkt noder på det uppdragsgemensamma nätverket. Tack vare denna lösning är det möjligt att alla enheter kan utbyta information med varandra på ett dynamiskt och säkert sätt.

Frågeställningar

Hur effektiva är Försvarsmaktens krypteringslösningar ur ett resursperspektiv?
Kan en dynamisk nyckelhantering lösa ut några hanteringsproblem för utrustningen?
Kan sekretessnivån påverka systemfunktionaliteten, t.ex. trafiklasten?
Kan nät enligt scenariot vara intressant? Vad skulle de i så fall krävas?
Kan taltolkning på anropssignalen användas för att styra informationssäkerhetsklasser och nyckelanvändning?

7 Slutsatser och förslag till fortsatt arbete

Arbetet som genomförts har varit begränsat i omfattning och vi har fokuserat på informationssäkerhetsklassningen för ett radiosystem. Informationen som skickas genom radiosystemet kan dock mycket väl komma från olika sensorsystem. Workshopen som genomfördes tyder på att det är möjligt att värdera behovet av sekretessnivå från fall till fall eller från system till system. Detta bör emellertid göras med en strukturerad metod, t.ex. COAT.

Literaturstudien visar också att valet av optimeringsscheman kan påverkas om sekretessnivån bedöms som en parameter i valet av schema.

Rapporten är en förstudie och vi kan se flera frågeställningar som kan vara intressanta att studera vidare. Följande förslag till fortsatt arbete bedömer vi som mest relevant.

7.1 Fördjupad behovsanalys

En fördjupad behovsanalys som värderar sekretessbehovet för en radiolösning enligt den systemdesign som föreslås i vårt exempelscenario, kap 6.5. Denna analys bör också besvara vilka system som finns idag och hur dessa skiljer sig från vårt exempel. Värderingen bör genomföras med COAT-metoden. Sannolikt behöver COAT-metoden först uppdateras för att kunna hantera värdering av sekretessnivåer.

7.2 MLS och integrerad säkerhet

En fördjupad studie av MLS-system och radionät där säkerheten integreras i nätet från början. Påverkas prestandan om sekretessen ingår som en designparameter? En viktig frågeställning är om och i så fall hur man skulle kunna konstruera ett radiosystem som kan hantera noder med olika sekretessnivå. Det är tänkbart att ett framtida radiosystem kan utnyttja principen för behörighet (pålitlighet, kunskaper om säkerhetsskydd och behov [18]) på ett nytt sätt. Ett ”hårdare” yttre skydd i form av uppdragsnyckeln hanterar att endast pålitliga och kunniga personer har möjlighet att ta del av informationen. Ett ”mjukare” skydd reglerar att endast den som har behov av uppgifter faktiskt kan ta del av den. En viktig frågeställning är då om man kan bygga ett nät med ett hårdare ”skalskydd” och ett mjukare internt skydd och vilka möjligheter det i så fall skulle ge.

7.3 Tidsaspekten för hemlig information

Tidsaspekten för hur länge en uppgift skall betraktas som hemlig skiljer i verkligheten och i teorin. Hur bör detta hanteras och hur påverkar detta möjligheterna i ett framtida radionät?

7.4 Effektivisering av krypto

Valet av algoritm har påverkan på svarstider, processoraktivitet och overhead som är relevanta att väga in när man hanterar kommunikation med låg bandbredd. Strömchiffer skulle kunna ha fördelar framför blockchiffer, men tekniken behöver studeras ytterligare.

8 Referenser

[1] Wolf, Wireless robust link for urban force operations, Defence R&T Joint Investment Programme on Force Protection (A-0692-RT-GC), 2008 – 2010.

[2] COALWNW, Coalition Wideband Networking Waveform

[3] Asp, B., Carling, C., Hunstad, A., Johansson, B., Johansson, P., Nilsson, J., Waern, Å.: COAT, Användarguide, FOI-R—2409—SE, 2007

[4] Grahn, P., Asp, B., Carling, C., Olsson, G., Follo, P., Näsström, F., Rasmusson, J., Nelander, A., Carlsson, L.: Taktisk värdering av sensorsystem - Slutrapport, FOI-R—3344—SE, 2011

[5] Bengtsson A, Fransson J, Kaijser T: Dynamisk Informationsvärdering, 2004

[6] Cha SC, Liu LT, Yu BC: Process-Oriented Approach for Validating Asset Value for Evaluating Information Security Risk, 2009

[7] Winkelvos T, Rudolph C, Repp J: A Property Based Security Risk Analysis Through Weighted Simulation, 2011

[8] Yau SS, Huang J: A User-Centric Approach to Assessing Confidentiality and Integrity of Service-Based Workflows, 2011

[9] Siew CK, Goodman DJ: Packet Data Transmission Over Mobile Radio Channels, 1989

[10] Lettieri P, Srivastava MB: Adaptive Frame Length Control for Improving Wireless Link Throughput, Range, d Energy Efficiency, 1998

[11] Kidston D. IP header compression and packet aggregation in mobile tactical networks, 2009

[12] Yao Y, Gehrke J: Query Processing for Sensor Networks, 2003

[13] Christos Xenakis, Nikolaos Laoutaris, Lazaros Merakos, Ioannis Stavrakakis: A generic characterization of the overheads imposed by IPsec and associated cryptographic algorithms, 2005

[14] Avesh K. Agarwal Wenye Wang: Measuring Performance Impact of Security Protocols in Wireless Local Area Networks. 2005

[15] Younis M, Farrag O, Lee S, D'Amico W: Optimized packet formation in multi-level security wireless data acquisition networks, 2010

[16] Gamer T, Völker L, Zitterbart M: Differentiated security in wireless mesh networks, 2009

[17] Letalick D, Björkert S, Gustavsson R, Rasmusson J, Waern Å: En teknikö̈versikt över IK-system, 2011

[18] Säkerhetsskyddsförordningen 1996:633

[19] Moltke HKB, Militarische Werke, Volume 2, 1923

[20] Younis M. Farrang O., D'Amico W.: Packet size optimization for increased throughput in multi-level security wireless networks, Milcom 2009

Bilaga A Minnesanteckningar från workshop 13 feb 2012

Deltagare: Lars Behm (MSS Kvarn), Tommy Gustafsson (FOI), Lars Westerdahl (FOI), Jonas Hallberg (FOI), Jimmi Grönqvist (FOI), Mattias Sköld (FOI), Åsa Waern (FOI)

Militära operationer som i scenario 1 och 2 går snabbt, 4-6 tim, såvida man inte kör fast. Man lämnar aldrig en operation utan roterar personalen (inom plutonen, kompaniet, bataljonen osv) för att förlänga uthålligheten.

Dimensionera för nationell insats och väpnad strid!

Viss information är skyddsvärd sett ur ett politiskt perspektiv. Går saker fel och det kommer ut kan man få opinionen mot sig. Detta utgör ett problemområde i sig själv, vad är det som är skyddsvärt? För vem vill man undanhålla information och varför? Skyddar man någon eller något genom att undanhålla information? Aktualiteten i informationen får en annan betydelse. Information som är gammal ur ett stridsperspektiv kan vara fortsatt användbar i ett propagandaperspektiv.

Känslighet hos utbytt information beror på händelseutvecklingen. Om något specifikt upptäcks vid en insats kan översänd data plötsligt bli mer känslig. Detta påverkar också den tidsfaktor som kan läggas på känsligheten, dvs. hur länge något behöver vara hemligt.

Även hotbilden är väsentlig för behovet av säkerhetsfunktioner, men det kommer egentligen efter att informationens känslighet har avgjorts.

Underrättelseförmågan kan vara mycket känslig. Signalspaningsförmågan är ofta hemlig/secret medan UAS-information är mindre känsligt

Intressanta frågor att studera:

- I vilken utsträckning är det möjligt att förutse känslighetsnivåer och tidsfaktorer? Dessa är dynamiska med avseende på händelseförloppet.
- Hur påverkar blandningen av olika system? Är det nödvändigt att beakta detta vid analys av känslighetsnivåer och tidsfaktorer?
- Avvägning mellan behov av sekretess och riktighet samt tillgänglighet
- Avvägning mellan strategiska och taktiska behov av säkerhetsfunktioner
- Tidsfaktorer varierar ofta mellan taktiska och strategiska behov. Det kan dock vara mer relaterat till situation än befattningsnivå.
- Vad är förhållandet i känslighet mellan lägesinformation och dess tolkning?

Planning

- Alternative plans
- Intelligence
- Tactical overlays
- Entities and symbols
- GIS thematic maps

- Kompanichef – ”task force command post”
- Kompanichef – Plutonchef
- Plutonchef – Gruppchef
- Gruppchef – Gruppmedlemmar

Inför en insats kan en stridsplan överföras. Stridsplanen kan innehålla planerad rutt med stoppunkter (fordonsavlämningsplats, inbrytningspunkt, mm) inlagda. Under genomförandet av insatsen anges de faktiska positionerna.

När vi tar oss fram i ett område (scenario 1 och 2) lämnar vi Trossen bakom oss. Därför kan gammal positionsdata vara intressant för att lokalisera var de befinner sig. Den kan också vara intressant eftersom den avslöjar vilken väg vi valt att använda. Har man säkrat en väg så använder man helst den igen. Sjuk- och logistiktransporter går samma väg tillbaka.

Överföring av information relaterad till signalspaning är känslig

Scenario 1: Plutonen på gatan är mer utsatt än plutonerna inne i byggnaden. Kompanichefen följer med in i byggnaden om så är lämpligt. Positionsdata på plutonen utomhus kan vara intressant för indirekt eld och krypskyttar. Positionsdata i realtid på plutonen inomhus kan vara intressant för krypskyttar eftersom de då kan följa rörelser och planera sin strid (tex vara beredd när soldaten inomhus närmar sig ett fönster). Informationen har kort livslängd på skådeplatsen, om det inte handlar om gruppering.

Scenario 2: Positionsdata har kort livslängd. Så länge vi rör på oss är den mer eller mindre ointressant. Om vi däremot fastnar så kan den få ett större värde.

Scenario 3: Här kan positionsdata vara mer intressant eftersom vi visar vilken väg vi valt. Sannolikheten att vi kommer att använda samma väg igen är stor. Positionsdata kan också ge information om hur lång tid det tar att färdas sträckan. Fiende kan använda den informationen för att beräkna tiden och positionen för tillslag.

Order (directions and combat orders)

- Warning orders
- Operations orders
- Patrol orders
- Fragmentary orders
- Tactical maneuver

- Kompanichef – ”task force command post”?
- Kompanichef – Plutonchef
- Kompanichef – Gruppchef
- Plutonchef – Gruppchef
- Gruppchef – Gruppmedlemmar

Orderinformation kan vara känslig men ofta kortlivad. Livslängden på en order ökar dock för varje organisatoriskt steg.

Kompani -> Pluton: timmar till dygn

Pluton -> Grupp: minuter till timmar

Grupp -> Soldat: minuter till timmar

Uppgiften och var i genomförandeprocessen man är avgör livslängden.

Scenario 1: Bataljonchefen (task force command post) har delegerat uppgiften till Kompanichefen och ger därför normalt inga order. Kompanichefen är troligtvis med inne i huset.

Scenario 2: Ordrar är skyddsvärd men kort livslängd. De är intressanta att komma åt i klartext i realtid. Vi vill inte avslöja att vi fått reda på hur fienden gör eller kommunicerar. Ordrar som kan avslöja detta är därför extra känsliga. Ordrarna kan vara av typen gör si för de andra ska göra så, frilägg där, flytta dit mm. Samordning mellan kompanierna. Kompanicheferna måste kunna samordna en manöver.

Scenario 3: Ordrar här består främst av trafikledning. Tex om vägen blivit blockerad eller något annat oförutsett inträffar.

Rapportering (report & warning generation)

- Text
- Images
- Video

- Kompanichef – ”task force command post”
- Kompanichef – Plutonchef
- Plutonchef – Gruppchef
- Gruppchef – Gruppmedlemmar

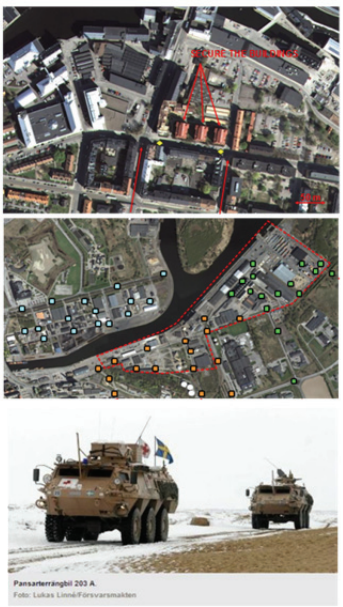
Rapportering sker oftast i text men bilder är mer intressant. Övningar har visat att video snarare kan leda till felaktiga beslut än att vara en hjälp. Kanske tenderar vi att tro mer på rörliga bilder än på det vi läser? Det krävs en förmåga att tolka video. När vi hamnar i strid (scenario 1 & 2) vill vi inte skriva något, då talar vi i radio.

Scenario 1: Bilder kan vara intressant att förmedla. Det kan vara bilder på hur det ser ut inne i huset eller objekt man upptäcker på vägen.

Scenario 2: Bilder på anfallsmål är högintressanta. Ett kompani kan skicka bilder till det andra kompaniet så att de tex ser anfallsmålet från en annan vinkel.

Scenario 3: Rapportering i form av ”jag är, jag gör…”. Skickar bild om något är fel/tveksamt mm, tex en sönderkörd bro. Informationen har lång livstid eftersom det är bra ingångsdata till nästa gång man kör transporten. Det är även bra att skicka bilder från tex den första bilen till längre bak i ledet. En lastbilskonvoj innehåller upp till 32 långtradare och 4 terrängbilar. Konvojen blir 3-4 km lång.

Combat service support



- Logistic request
- Logistic report
- Medical evacuation

- Kompanichef – ”task force command post”
- Kompanichef – Plutonchef
- Plutonchef – Gruppchef
- Gruppchef – Gruppmedlemmar

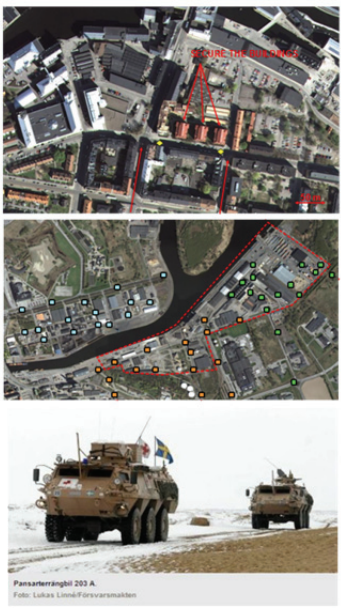
Bataljonschefen bestämmer sjukhanteringen genom kvartermästaren. Med- och logistiktransporterna är oftast skyddade. Hanteras transporten av kompaniet eller plutonen självt är de beväpnade. Vid sjuktransporter skickas information om personuppgifter och skadetyp vilket kan vara känsligt. Avtransportering av skadade tar i regel från några minuter till ½-timme. Sjuktransporten får positionsdata vart de ska, vilket kan ha betydelse för fienden. Åtminstone fram till de flyttat på sig (ca 4 dygn).

Scenario 1: Logistiken består troligtvis av mattransporter och ev ammunition framåt och evakuera skadade bakåt. Logistiken allra längst fram hanteras av kompaniet självt. Fångar evakueras när tid medges

Scenario 2: Under förutsättning att det går som planerat så består logistiken bara av att evakuera skadade.

Scenario 3: Konvojen har med sig nödvändig utrustning själva. De är mest utsatta när de tar rast.

Combat support



- Call for fire
- Close air support
- ~~Close air support evacuation~~ Call for QRF

- Kompanichef – ”task force command post”
- Kompanichef – Plutonchef
- Plutonchef – Gruppchef
- Gruppchef – Gruppmedlemmar

Indirekt eld har en kort livslängd. Lägger man in mål i förtid, i planneringsstadiet kan det underlätta målangivelse under operationen, då får informationen betydligt längre livslängd men man skulle kunna uttrycka tex ordrar på ett annat sätt (”B1” istället för ”röd lada”). Om kompanichefen behöver flygunderstöd så går han till Batchefen, Tactp-gruppen avgör om han får flygunderstöd eller ej. För flygunderstöd skickas målkoordinater, typ av ammunition och klockslag. Denna information skickas ”utanför kompaniet”. De får sedan svar när raket är på väg. Vilken flygkorridor som används är intressant att veta då eget luftvärn inte kan bekämpa i dessa.

Scenario 1: Helikoptrar kan tänkas sätta ner folk på taken

Scenario 2: Helikoptarar kan lyfta ut enheter i kanterna i insatsområdet. De flyger inte in i insatsområdet. Om de gör det så flyger de i förbestämda korridorer där man inte får skjuta.

Scenario 3: Close air support kan vara aktuell för att evakuera skadade. Konvojen ligger dåligt till om de blir beskjutna. Det finns larmstyrkor, QRFer (quick reaction force), som är beredda att rycka ut. Det är intressant för fienden att veta hur lång tid det tar för dem att nå platsen.

Synchronization of SA info and LOP generation

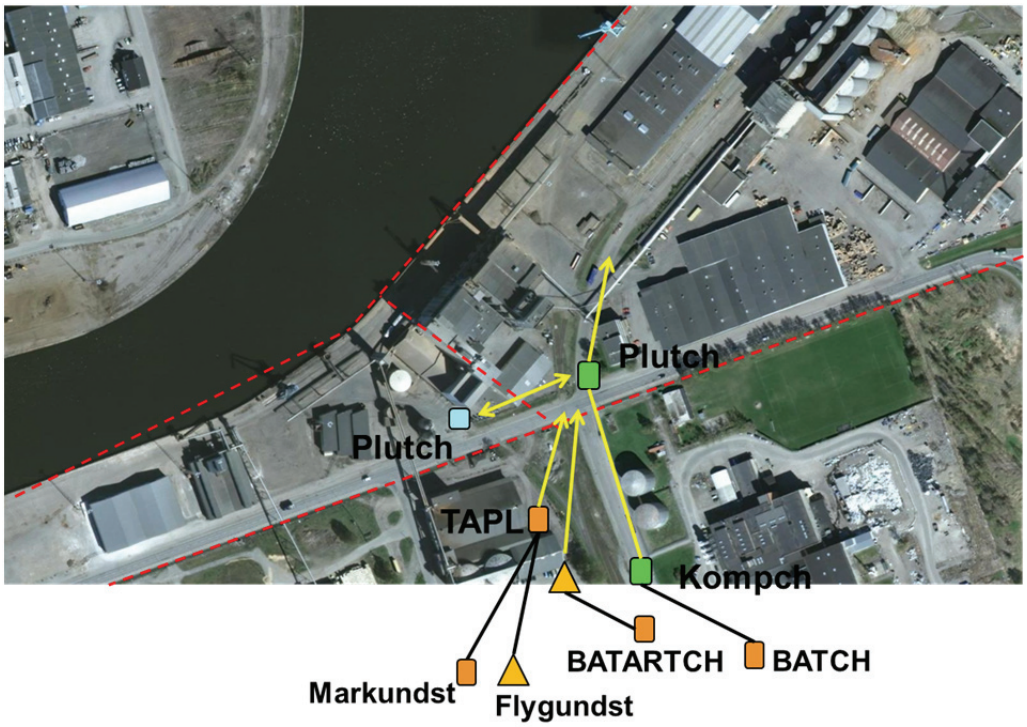
- …

- Kompanichef – ”task force command post”
- Kompanichef – Plutonchef
- Plutonchef – Gruppchef
- Gruppchef – Gruppmedlemmar

Mycket tal. Tolkar tjänsten som att det handlar om att komma överens om lägesbilden. Ser verkligheten ut på det sätt som kartan säger? Finns fienden, eller är de utslagna. Egna trupper finns de och vilken status har de?

Väldigt känslig info eftersom det avslöjar vår faktiska lägesuppfattning.

Försök har visat att med ett bättre datorstöd (mer information) höjdes kvalitén på samtalen mellan chefer. Fienden vill säkert gärna veta var vi finns och vad vi vet, men de kan sänka vår förmåga genom att störa dessa system – särskilt när systemvanan blir hög.



Ovanstående bild skulle kunna vara ett alternativt scenario 2. Scenariot beskriver ett anfall från Grönt kompani där blå pluton stödjer ena flanken och nödvändigt informationsutbyte sker. Grönt kompani tar hjälp av stridseldgrupp samt TAPL för flygunderstöd.