



Självständigt arbete i krigsvetenskap, 15 hp

<i>Författare</i> Flkd Johan Resare		<i>Program</i> OP 07-10
<i>Handledare</i> Fil.mag. Fredrik Petersson		
	<i>Beteckning</i>	
<h3>Vad gör jag om piraten stör min GPS?</h3> <p><i>En studie av hur marinen påverkas taktiskt vid störning av GNSS-system.</i></p> <p>Den svenska marinen likväl som världens handelssjöfart nyttjar alltmer satellitnavigering för sin positionering. Enligt totalförsvarets forskningsinstitut kan sådana system störas med förhållandevis enkla medel. Nu när den svenska marinen alltmer engagerar sig i insatser utomlands mot irreguljära motståndare väcks frågan om hur en irreguljär motståndare kan påverka den svenska marinen och den svenska marinens taktik. I denna uppsats kommer frågor kring en irreguljär motståndares förmåga att påverka GNSS att ställas. Samt frågan om vilken påverkan detta har för såväl den svenska marinens fartyg som handelssjöfarten. Uppsatsen kommer även att behandla möjligheterna till skydd mot störning samt hur den svenska marinens taktik kommer påverkas om en irreguljär motståndare försöker störa ut GNSS-system.</p> <p><u>Nyckelord:</u> GNSS, GPS, taktik, taktikanpassning, RMP, AIS, irreguljär motståndare</p>		

What to do if the pirate jams my GPS?

A study of how the Swedish marine is affected by interference in GNSS-systems.

The Swedish Navy as well as the worlds shipping industries use more and more satellite navigation for positioning purposes. According to the Swedish Defence Research Agency, those types of systems can relatively easily and at a low cost be jammed. With the Swedish Navy becoming more and more involved in missions overseas against insurgents, the question is whether an insurgent can affect the Swedish Navy and its tactics. This paper investigates the questions about what opportunities an insurgent have to affect the GNSS-system and how that can affect the Swedish Navy as well as the shipping industries. This paper is also about how the tactics of the Swedish Navy will be affected if an insurgent attempts to jam the GNSS-systems and the possibility of protection against jamming.

Key words: GNSS, GPS, tactics, tactics adaptation, RMP, AIS, insurgents

Innehållsförteckning

1 Inledning	5
1.1 Bakgrund	5
1.1.1 En hypotes	6
1.2 Problemformulering	6
1.2.1 Frågeställning	7
1.3 Syfte	7
1.4 Avgränsningar	7
1.5 Tidigare forskning	8
1.6 Centrala begrep	9
1.7 Metod	10
1.8 Material och källkritik	11
1.9 Disposition	13
2 Empiri	14
2.1 GNSS beskrivning och uppbyggnad	14
2.2 Olika GNSS-system	14
2.2.1 GPS	15
2.2.2 GLONASS	15
2.2.3 Ej operativa system	16
2.2.4 GPS som allmängiltigt GNSS-system	17
2.3 Störning av GNSS	17
2.4 Åtgärder för störskydd	18
2.4.1 Störskydd genom adaptiv gruppantenn	19
2.5 Den irreguljära motståndares förmåga till störning av GNSS-system	20
3 Analys	22
3.1 Påverkan på fartygssystem	22
3.2 Påverkan på marinens fartyg	22
3.3 Påverkan på handelssjöfarten	23
3.3.1 Påverkan på AIS-systemet	24
3.4 Taktisk påverkan av telekrig mot GNSS	25
3.5 Mötet med den irreguljära motståndaren	25
3.5.1 Att utöva kontroll	26
3.6 Den direkta påverkan	27

3.7 Den indirekta påverkan	27
3.7.1 Närhet till land	28
3.7.2 Upprätthållande av RMP	28
3.7.3 Identifieringsmetoder vid påverkat AIS-system	29
3.7.4 Ökade krav på rörlighet	30
3.8 Hypotesprövning.....	30
3.8.1 Jämförelser mellan direkt och indirekt påverkan.....	31
3.9 Slutsatser	31
3.9.1 Möjlighet för en irreguljär motståndare att påverka GNSS.....	32
3.9.2 Alternativa positioneringsmetoder och direkt verkan	32
3.9.3 AIS-systemet och förmågan till RMP	33
3.9.4 Taktisk anpassning	33
4 Diskussion.....	34
4.1 AIS-systemet ur ett vidare perspektiv.....	34
4.1.1 Motståndarens behov av GNSS	34
4.2 Uppsatsens allmängiltighet	35
5 Avslutning	36
5.1 Sammanfattning.....	36
5.2 Behov av vidare forskning	38
6 Litteraturförtäckning.....	39

1 Inledning

På senare år har den svenska marinen varit delaktiga i operationer inom den lägre delen av konfliktskalan. Bland annat utanför Somalias kust för att skydda FNs mattransporter och handelsfartyg mot kapningsförsök. I denna nya roll som väsentligt skiljer sig från marinens roll under senare delen av det kalla kriget så har den förväntade motståndaren skiftat från en stormakt på andra sidan Östersjön till en mer diffus irreguljär motståndare.

Under de senaste åren har även den svenska marinen såväl som världens handelssjöfart blivit mer och mer tekniskt avancerad, inte minst inom navigationsområdet.

Enligt Totalförsvarets forskningsinstitut (FOI) är möjligheterna stora även för en dåligt finansierad irreguljär motståndare att kunna förfoga över teknik för att störa dagens elektroniska navigationssystem.

En utförlig beskrivning av en enkel, billig och portabel GPS-störare finns tillgänglig på Internet [...] Komponenterna som skall användas är specificerade och kan köpas från en godtycklig elektronikfirma.¹

Även om det i nuläget inte uppfattas som ett problem med störningsförsök mot navigationssystem så finns uppenbarligen möjligheten att detta kan utvecklas till ett reellt problem inom en överskådlig framtid. Det är således möjligt att en risk föreligger för att navigationssystem kan utsättas för störningsförsök. Därför finns det ett behov av studier inom området. Detta resonemang ligger till grund för valet av ämne för denna uppsatts.

1.1 Bakgrund

I ett framtida scenario där en irreguljär motståndare nyttjar störning av navigationssystem som en del av sin taktik uppstår många frågor. Kan en irreguljär motståndares förmåga till telekrig riktade mot navigationssystem utgöra ett hot mot den svenska marinen?

Hur kan detta påverka den svenska marinens taktiska uppträdande?

Den svenska marinen har ännu inte någon omfattande erfarenhet av en taktisk situation där telekrig mot navigationssystem ingått. Våra doktriner ger heller inte någon fullständig beskrivning av en taktisk anpassning till en miljö där störning av navigationssystem

¹ Eklöf 2004 sid 7

förekommer. Detta leder till att det inom det taktiska området finns ett behov av studier kring ämnet fientlig störning av navigationssystem.

Detta arbete syftar till att undersöka och sprida kunskap om de problem och den taktikanpassning som kan komma att bli nödvändig i en situation då en irreguljär motståndare nyttjar störning av navigationssystem inom sjöarenan.

1.1.1 En hypotes

Redan på detta stadium uppstår en fråga, nämligen om den svenska marinens skyddsåtgärder ger ett fullgott skydd mot störning av GNSS? Om så är fallet kan då en störning av GNSS ändå påverka den svenska marinen genom att påverka andra mer oskyddade system? Detta kan formuleras till en hypotes enligt följande:

Den direkta taktiska påverkan på marinens fartyg är försumbar i jämförelse med den indirekta påverkan.

Där direkta påverkan är den påverkan som sker förutsättningslöst mot ett eller flera fartyg.

Den indirekta påverkan är den påverkan som sker på en högre nivå och som inte är förutsättningslös. Se kapitel 5 Taktisk påverkan av telekrig mot GNSS

Denna hypotes skall vara genomgående i uppsatsen och frågeställningen skall utgå från denna hypotes. Genom uppsatsen skall hypotesen prövas på så sätt att den antingen skall kunna verifieras eller falsifieras. Om hypotesen inte kan verifieras eller falsifieras fullständigt så kan hypotesen brytas ner till delar och dessa verifieras eller falsifieras var för sig.

1.2 Problemformulering

Mot bakgrund av vad som tidigare nämnts under rubriken bakgrund och den formulerade hypotesen så kan en frågeställning formuleras. Detta med utgångspunkten att arbetet skall belysa förhållandet mellan taktik och möjligheten för en irreguljär motståndare att verka inom telekrigsområdet mot GNSS-system. Då kan en frågeställning formuleras kring värdeorden taktik, fientlig störning av GNSS-system samt irreguljär motståndare. I kapitlet avgränsningar avgränsas uppsatsen till sjöarenan. Med hänsyn till detta och den marina aspekten i bakgrunden så kan även värdeorden inom sjöarenan adderas till summeringen av värdeord för

frågeställningen. Detta sammantaget ger frågeställningen hur påverkas marinen taktiskt av fientlig störning av GNSS-system vid möte av en irreguljär motståndare inom sjöarenan?

1.2.1 Frågeställning

Hur påverkas marinen taktiskt av fientlig störning av GNSS-system vid möte av en irreguljär motståndare inom sjöarenan?

1.3 Syfte

De senaste årens teknikutveckling i kombination med den svenska marinens nya fokus på internationella insatser har till viss del ändrat de taktiska förutsättningarna. Med detta som bakgrund vill författaren i denna uppsats undersöka en del av den taktiska utvecklingen inom sjöarenan. Detta genom att undersöka vilken taktisk påverkan en störning av GNSS kan innebära med utgångspunkten att störningen orsakas av en irreguljär motståndare.

1.4 Avgränsningar

Uppsatsen avgränsar sig i tid till tiden efter kalla krigets slut. Detta för att Sveriges Försvarsmakt från och med kalla krigets slut övergått från ett fokus på invasionsförsvar till ett insatsförsvar. Ett insatsförsvar vars tonvikt snarare legat på insatser mot irreguljära motståndare än försvar mot stormakter.²

Uppsatsen avgränsar sig i rummet till att behandla Sveriges Försvarsmakt då uppsatsen skrivs i Sverige och delvis syftar till att främja Sveriges Försvarsmakt.

Uppsatsen avgränsar sig i till sjöarenan, dels för att författaren huvudsakligen är verksam inom denna arena. Dels för att elektroniska navigationssystem har en särställning inom sjöarenan. En särställning i det avseendet att sjöarenans aktörer i stor grad förlitar sig på elektroniska navigationssystem i den dagliga verksamheten.

I frågeställningen avgränsas motståndaren till en irreguljär aktör, detta dels för att en irreguljär aktör i nuläget upplevs som mer aktuell med tanke på de missionerna som den

² Försvarsmakten 2005 Doktrin för marina operationer sid.120-122

svenska marinen för närvarande bedriver. Dels för att en reguljär aktör kan förväntas ha tillgång till långt mycket mer kvalificerade system för störning av elektroniska navigationssystem, kvalificerade störsystem som kan antas vara omgärdade av omfattande sekretess.

Utöver dessa avgränsningar så avgränsas uppsatsen juridiskt till att endast behandla öppen information. Av den anledningen kommer ingen presentation ske om vilka fartyg som är utrustade med vilken typ av system, exempelvis för störskydd.

1.5 Tidigare forskning

Den forskning som tidigare bedrivits inom området störning av GNSS-system har haft en mer tekniskt karaktär. Två olika projekt har bedrivits av FOI, det ena projektet genomfördes av Bengt Boberg, Fredrik Eklöf och Lars Pääjärvi och avslutades under 2003. Detta projekt kretsade kring frågan:

[H]ur skyddar man ett eget navigationssystem eller omvänt hur stör man (degraderar navigationsprestande) en fiendes navigationssystem³

Det andra FOI projektet genomfördes av Fredrik Eklöf och Lars Pääjärvi och avslutades 2005. Detta projekt kretsade kring följande frågeställningar:

1. Hur skall en GNSS-motagare som skyddas av en adaptiv gruppantenn störas på ett effektivt sätt, dvs. hur skall störscenariot utformas?
2. Vilka risker tas genom att utnyttja GNSS för tidgivning och positionering i NBF och hur skall en adaptiv gruppantenn utformas för att minimera dessa risker i en telekrigsmiljö?⁴

Båda dessa FOI rapporter fokuserar på den tekniska aspekten av störning av GNSS-system och tar inte upp den taktiska tillämpningen.

³ Boberg mfl. 2003 sid.4

⁴ Eklöf mfl 2004 sid.6

Utöver dessa rapporter finns även två uppsatser, en skriven av Matias Fernandez med titeln ”Telekrig riktat mot GNSS, GPS i fokus”. Denna uppsats är skriven vid yrkesoficersprogrammet år 2009 och kretsar kring telekrigshot riktade mot GNSS inom Försvarmakten. Inte heller denna uppsats behandlar de taktiska aspekterna av störning mot GNSS.

Den andra uppsatsen är skriven av Torbjörn Lundströmmer och har titeln ”Hjälp! Vem tog min GPS? Studie av redundanta metoder i integrerade positioneringssystem.” Denna uppsats är skriven under chefsprogrammet 07-09 vid försvarshögskolan. Uppsatsen behandlar huvudsakligen stöttning av GPS inom Försvarmakten. Men även hur GPS kan integreras med system för tröghetsnavigering för att uppnå en större säkerhet vid signalbortfall eller störning. Som summering av tidigare forskning inom området så finns inga svenska öppna studier på samspelet mellan störning av GNSS och taktik, dock finns tidigare studier kring den tekniska aspekten av störning av GNSS-system.

1.6 Centrala begrep

För att öka förståelsen för uppsatsen i stort krävs en genomgång av några av de centrala begrepp som frekvent förekommer i uppsatsen.

- GNSS – *Global Navigation Satellite System*. Detta är samlingsbetäckningen på alla satellitbaserade navigationssystem med global täckning. Det finns i nuläget tre sådana system i världen, det amerikanska GPS systemet, det ryska GLONASS systemet samt det ej färdig utvecklade europeiska Galileo systemet.⁵
- RMP – *Recognised Maritime Picture*. Den för de marina stridskrafterna gemensamma lägesbilden där såväl civila som egna militära och fientliga mål läggs in.⁶ RMP presenteras normalt i ett datoriserat stridsledningssystem ombord på fartygen samt på staber.
- Irreguljär motståndare. En part i en konflikt som kan beskrivas som en militariserad upprorsmakare. Någon exakt definition finns ej, men begreppet brukar ofta appliceras på miliser, paramilitärer, gerillor, legosoldater, krigsherrar, banditer, medlem av olovligt medborgargarde samt militanta gängbildningar. Under förutsättning att någon

⁵ Andrews, m.fl. 2007 sid.2-5

⁶ Försvarmakten 2005 Doktrin för marina operationer sid.105

av dessa ej tillhör en stats organiserade väpnade styrkor vars syfte är att försvara staten från externa angripare.⁷

- AIS – *Automatic Identification System*. AIS-systemet är ett tekniskt system bestående av transpondrar på alla fartyg. Systemet sänder med jämna mellanrum ut identifierings-, positions-, kurs- samt fartinformation till övriga fartyg.⁸

1.7 Metod

Uppsatsens frågeställning syftar till att skildra en taktisk påverkan av företeelsen fientlig störning av GNSS-system. Då denna företeelse enligt tillgänglig öppen litteratur ännu inte har ägt rum så blir ett besvarande av frågeställningen att betrakta som en förutsägelse. En sådan förutsägelse är det som inom vetenskaplig metod benämns som en prediktion.⁹

Som stöd i denna process finns den tidigare formulerade hypotesen som genom prövning kan ge stöd åt prediktionen. För att kunna angripa frågeställningen krävs en uppdelning av den metod som skall nyttjas för att kunna göra prediktionen.

Det första steget är att genom kvalitativ textanalys beskriva GNSS system och deras uppbyggnad samt möjligheten till störning av GNSS-system.

Det andra steget är att genom kvalitativ textanalys skildra vilken typ och vilken omfattning som en irreguljär motståndare inom sjöarmeen kan nyttja sig av störning mot GNSS-system. Informationsläget beträffande irreguljära förbands förmåga till telekrig mot GNSS är dock bristfälligt. Detta leder till att utgångspunkten i denna textanalys snarare kretsar kring vilka tekniska system det är troligt att ett irreguljärt förband kan förfoga över än vilka förmågor till telekrig mot GNSS som ett sådant förband besitter.

Det tredje steget utgår från slutsatserna från den kvalitativa textanalysen i steg ett och två. Med dessa slutsatser som bas skall det tredje steget genom teoribildning beskriva vilken påverkan fientlig användning av störning av GNSS-system skulle ha på Marinens fartyg. Denna typ av teoribildning ställer krav på att det är möjligt att utifrån givna faktum genom logiskt resonemang dra nya slutsatser och därigenom formulera prövbara hypoteser. Sådana

⁷ Rekkedal 2006 sid.30

⁸ Borg, m.fl. 1999 sid.189

⁹ Ejvegård 2003 sid.42

hypoteser måste sedan kunna härledas tillbaka till givna faktum och därigenom kunna ge en beskrivning av påverkan på fartygens system.

Därefter upprepas detta steg men på handelsfartygens system för att undersöka om handelsfartygen påverkas på ett annat sätt. Detta steg bedöms som nödvändigt då samspelet mellan handelssjöfart och marinens enheter kan vara av betydelse för den taktiska påverkan.

Det fjärde steget är att med ingångsvärdena från det tredje steget och vedertagna taktiska teorier och uppfattningar nyttja en teoribildning. Denna teoribildning skall nyttja ett logiskt resonemang och en tydlig härledning. Därigenom skall en möjlighet att pröva hypotesen mot teorierna och slutsatserna från tidigare steg skapas. Om den direkta taktiska påverkan på marinens fartyg är försumbar i jämförelse med den indirekta påverkan.

Utfallet från denna hypotesprövning kan sedan ligga till grund för besvarande av uppsatsens frågeställning. Hur påverkas marinen taktiskt av fiendlig störning av GNSS-system vid möte av en irreguljär motståndare inom sjöarenan? Slutligen måste en diskussion föras om slutsatsernas allmängiltighet och rimlighet.

1.8 Material och källkritik

För att säkerställa uppsatsens trovärdighet krävs en genomgång om hur källmaterial har hanterats av författaren. Denna uppsats bygger till stor del på teoribildning utifrån en kvalitativ textanalys. Detta förfarande ställer stora krav på att de källor som ligger till grund för textanalysen är trovärdiga. Om så ej är fallet kommer det vetenskapliga värdet på slutsatserna kraftigt att reduceras. Då GNSS är ett förhållandevis nytt system och som förändras fortlöpande är författarens bedömning att tidskriteriet är av avgörande betydelse för källornas tillförlitlighet. Därav har författaren beslutat att till denna uppsats endast nyttja källmaterial som ej är äldre än tolv år.

För insamlande av underlag till denna uppsats har Anna Lindbiblioteket och dess databaser nyttjats, material som inte är tillgängligt direkt via Anna Lindh biblioteket har beställts från andra högskolebibliotek.

För att skapa en struktur och överblick över det material som nyttjas till uppsatsen har författaren delat upp materialet i två kategorier. Den första kategorin har författaren valt att

benämna teknisk litteratur. I denna kategori ingår de verk som är skrivna i tekniska syften och som kan nyttjas för att besvara metodens första och andra steg.

Den andra kategorin har författaren valt att benämna taktisk litteratur. I denna kategori ingår de verk som är skrivna i syfte att belysa taktik, företrädesvis marin taktik. Litteraturen ur denna kategori är av relevans för uppsatsen beträffande besvarande av metodens tredje och fjärde steg.

Inom kategorin teknisk litteratur dominerar rapporter från FOI. FOIs rapporter är att anse både som primär och sekundär källa då de dels presenterar resultat från egen forskning och sammanställer resultat från utländsk forskning. Med hänsyn till att FOI är ett statligt finansierat och väl etablerat forskningsinstitut så bedöms trovärdigheten i detta källmaterial som högt. Utöver dessa rapporter från FOI finns i denna kategori även rapporter från andra statliga myndigheter exempelvis Sjöfartsverket, Banverket, Vägverket och Lantmäteriet.

Inom kategorin taktisk litteratur finns två tydliga undergrupper av material. Där den ena gruppen utgörs av svenska doktriner och den andra av övrig taktisk litteratur. Vad doktrinerna beträffar så är ju dessa skrivna som riktlinjer för hur Försvarmakten skall genomföra verksamhet och förhålla sig till olika förtretelser. Således får dessa en särställning då de beskriver Försvarmaktens egen syn och doktrinerna kan därmed inte ifrågasättas som källa i frågor som berör Försvarmaktens syn och inställning i sakfrågor.

Beträffande övrig taktisk litteratur så har författaren valt att begränsa sig till litteratur utgiven av Försvarethögskolan och till väletablerade utländska teoretiker som Milian N. Vego och Wayne P. Huges Jr.

Vad hanteringen av Internetkällor beträffar finns endast två Internetkällor upptagna i uppsatsen. Den första källan berör antalet satelliter i det ryska GLONASS-systemet. Då denna uppgift är i ständig förändring är författarens bedömning att en Internetkälla i detta fall är mer pålitlig än vad en tryckt källa är. Den andra Internetkällan berör International Maritime Organizations (IMO) SOLAS konvention. Då denna konvention är i ständig förändring är författarens bedömning även här att en Internetkälla i detta fall är mer pålitlig än vad en tryckt källa är.

1.9 Disposition

I uppsatsens första kapitel behandlas bakgrunden till valet av ämne likväl som den hypotes som ligger till grund för formuleringen av frågeställningen. I detta kapitel behandlas även uppsatsens frågeställning, centrala begrepp och den metod som författaren ämnar nyttja i uppsatsen. Slutligen i första kapitlet behandlas valet av material samt författarens förhållande till källkritik.

I uppsatsens andra kapitel behandlas uppsatsens empiri. I detta kapitel ges en beskrivning av GNSS-systems uppbyggnad och möjligheten att störa ett GNSS-system. Slutligen behandlar detta kapitel vilken förmåga en irreguljär motståndare inom sjöarenan bedöms ha att störa ett GNSS-system. Detta kapitel behandlar metodens steg ett och två.

I uppsatsens tredje kapitel behandlas uppsatsens analys. I detta kapitel analyseras vilken påverkan telekrig mot GNSS har på fartygssystem samt vilken taktik påverkan som en störning av GNSS-system får för den svenska marinen. Avslutningsvis i detta kapitel prövas den hypotes som framlades redan i uppsatsens bakgrund och uppsatsens slutsatser presenteras. Detta kapitel behandlar metodens steg tre och fyra.

I uppsatsens fjärde kapitel diskuteras uppsatsens slutsatser och hur allmängiltiga dessa är.

I uppsatsens femte kapitel presenteras en sammanfattning av uppsatsen samt förslag på vidare studier inom området presenteras.

Uppsatsens sjätte och sista kapitel är en litteraturförtäckning över den litteratur som använts i uppsatsen.

2 Empiri

I detta kapitel kommer de frågor som beskrivs i metod steg ett och två att behandlas. Kapitlet syftar till att genom beskrivning skapa förståelsen för hur GNSS-system är uppbyggda och hur en teleteknisk störning av dessa system kan ske. Kapitlet syftar även till att beskriva vilken typ och i vilken omfattning som en irreguljär motståndare inom sjöarrendan kan nyttja sig av störning mot GNSS-system. Dessa beskrivningar kommer senare att ligga till grund för kapitlet analys där slutsatserna från detta kapitel skall nyttjas för att kunna besvara frågeställningen.

2.1 GNSS beskrivning och uppbyggnad

Ett GNSS-system är ett system för att fastställa sin position på jordytan genom att ta emot radiosignaler från satelliter i omloppsbana runt jorden. Genom att jämföra tidssignalerna från de satelliter som mottagaren har kontakt med kan mottagarens position fastställas. För att kunna ge en tillförlitlig position förutsätts att tidsangivelserna från satelliterna är mycket exakta. Detta säkerställs genom att alla satelliter är utrustade med mycket exakta atomur samt att en kontinuerlig uppföljning och korrektion sker från kontrollstationer på jorden.

Ett GNSS-system kan anses bestå av tre huvuddelar, ett rymdsegment bestående av ett antal satelliter som rör sig i väl bestämda banor. Ett marksegment bestående av kontrollstationer vilka svarar för kontroll, övervakning och upprätthållande av systemet. Samt en användardel vilket är den del som oftast benämns mottagare, alltså den del som mottar signalerna och beräknar aktuell position.

2.2 Olika GNSS-system

Det första GNSS-systemet blev operativt år 1964 men kunde inte leva upp till den tekniska utvecklingens krav på exakthet.¹⁰ Detta system har efterföljts av flera andra system varav det idag finns två system som är mer utbyggda och ytterligare några system som är påbörjade alternativt planerade. De olika systemen har i grunden samma uppbyggnad och är i stort mycket lika.

¹⁰ Borg, mfl. 1999 sid.78

2.2.1 GPS

Det amerikanska GPS-systemet är idag det helt dominerande GNSS-systemet i världen.¹¹ GPS systemets rymdsegment bestod i mars 2006 av 28 satelliter varav 24 är nödvändiga för att hålla systemet operativt.¹² Systemet introducerades operativt år 1995 och har sedan dess utvecklats successivt bland annat genom att nya generationers satelliter har ersatt de äldre.¹³

I GPS-systemet sänds signaler på två olika bärvågsfrekvenser benämnda L1 och L2. Där L1 ligger på 1575,42 MHz och L2 på 1227,60 MHz.¹⁴ GPS-systemet sänder data med två olika kodsystem med olika funktion och egenskaper.

Det första kodsystemet benämns C/A-koden och detta är en öppen kod, det innebär att den är tillgänglig för alla användare världen över och att den är helt avgiftsfri. Denna kod sänds endast med L1 bärvågsfrekvensen och finns således inte dubblerad i systemet.

Det andra kodsystemet benämns P(Y)-koden, denna kod är inte öppen utan är av USA reserverad för eget militärt bruk samt för allierade. Sverige har dock sedan 2003 ett bilateralt avtal med USA som ger Sverige tillgång till P(Y)-koden.¹⁵ P(Y)-koden sänds i båda bärvågsfrekvenserna och blir således mer bredbandig.

För att summera GPS kan konstateras att GPS är det idag helt dominerande systemet. Att GPS signalerna sänds med två olika kodsystem den civila C/A-koden och den militära P(Y)-koden där den militära P(Y)-koden är fördelad på två olika bärvågsfrekvenser samt har en större bandbredd, vilket innebär att den är betydligt mer svårstörd än C/A-koden.

2.2.2 GLONASS

Det ryska GLONASS-systemet är i sin generella uppbyggnad mycket likt GPS systemet. GLONASS-systemet har efter Sovjetunionens fall dragits med en ansträngd ekonomisk situation och systemet hade under slutet av 1990-talet endast 14 operativa satelliter. På senare år har dock flera uppskjutningar genomförts och nu uppger den ryska rymdstyrelsen på sin

¹¹ Borg, mfl. 1999 sid.81

¹² Mohinder 2007 sid.2

¹³ Borg, Björn mfl. 1999 sid.82

¹⁴ Mohinder 2007 sid.2

¹⁵ Lundströmer 2009 sid.34

hemsida att systemet är utbyggt med 23 satelliter och operativt.¹⁶ Det faktum att GLONASS-systemet fram tills nyligen inte varit fullt utbyggt har lett till att systemet inte är lika etablerat som GPS-systemet. Något som medfört att det därmed inte finns lika många användare. Faktum är att mottagare för GLONASS är mycket ovanliga och de som finns på marknaden är betydligt mycket dyrare än mottagare för GPS.

Vad kodsystemen beträffar så har GLONASS i likhet med GPS en öppen civil kod benämnd C/A-koden och en militär kod benämnd P-koden. Till skillnad från i GPS-systemet så krypterar GLONASS-systemet inte sin P-kod vilket innebär att även civila mottagare kan nyttja den signal som är avsedd för militärt bruk.¹⁷

För att summera GLONASS systemet kan konstateras att det inte är lika använt som GPS-systemet på grund av priset på mottagarna och att systemet först nyligen blivit helt funktionellt. GLONASS-systemet har dock fördelen att även den kod som är avsedd för militärt bruk kan användas av vem som helst som har en mottagare avpassad för detta.

2.2.3 Ej operativa system

Utöver de operativa GNSS-systemen GPS och GLONASS så finns även ett flertal system som befinner sig under uppbyggnads eller planerings fas. Det kanske mest intressanta av dessa är det europeiska systemet Galileo som planeras vara fullt utbyggt år 2012.¹⁸ Detta system som ägs och kontrolleras av EU är i sin uppbyggnad mycket likt GPS-systemet. Galileo har liksom GPS både en öppen del som är öppen för allmänheten och en del avsedd för myndigheter som polis, kustbevakning och militär. Den enskilt största skillnaden mot GPS-systemet är att i Galileo-systemet finns fler bärvågsfrekvenser.¹⁹

Ett ytterligare GNSS-system som är under utveckling är det kinesiska Compass-systemet. I likhet med övriga system sker sändningar i Compass-systemet på två olika koder, en för militärt bruk och en öppen för alla användare.²⁰

¹⁶ <http://www.glonass-ianc.rsa.ru/> (2010-04-19)

¹⁷ Borg, mfl. 1999 sid.104

¹⁸ Engfeldt, Jivall, Lilje 2007 sid.21

¹⁹ Mohinder 2007 sid.5-7

²⁰ Engfeldt, Jivall, Lilje 2007 sid.26

2.2.4 GPS som allmängiltigt GNSS-system

Som tidigare beskrivits så finns det idag flera olika GNSS-system varav i nuläget endast det amerikanska GPS-systemet och det ryska GLONASS-systemet är fullt operativa. Skillnaden mellan de operativa GPS och GLONASS-systemen i fråga om signalens utformning är av underordnad betydelse jämfört med tillgången på mottagare.

För Sveriges del har vi ett bilateralt avtal med USA som möjliggör användande av den militära P(Y) koden för Sveriges Forsvarsmakt. Enligt FOI är möjligheten att störa ut ett GNSS-system likvärdigt för samtliga GNSS-system.²¹ Med hänsyn till detta och till denna uppsats ringa omfattning avser författaren härmed att utgå från GPS-systemet i fortsatt text och endast ta upp andra system om någon relevant skillnad föreligger.

2.3 Störning av GNSS

Då alla GNSS-system är beroende av mottagning av signaler från satelliter så finns en given möjlighet att genom telekrigsåtgärder störa ut möjligheten till mottagning. Därmed kan möjligheten att nyttja systemen förhindras. Vad möjligheten till utstörning beträffar så finns flera parametrar att beakta. Först och främst är den från satelliterna mottagna signaleffekten intressant. Eftersom moderna GMDSS satelliter (GLONASS) sänder med en total effekt av runt 100W²² och med ett avstånd till jordytan på omkring 20000km²³ så blir signaleffekten på jordytan mycket liten. Enligt FOI är signaleffekten så låg vid jordytan som 10⁻¹⁶W och ligger därmed under gränsen för det termiska bruset.

Detta innebär att även en störsändare med en förhållandevis låg uteffekt kan störa ut ett GNSS-system även på förhållandevis långa avstånd. Andra parametrar som påverkar störningens effektivitet är hur störvågformen utformas, terrängen och på vilken höjd över omgivningen störsändaren befinner sig.²⁴

²¹ Boberg, Eklöf, Pääjärvi 2003 sid.11

²² Borg, mfl. 1999 sid.112

²³ Engfeldt, Jivall, Lilje 2007 sid. 10

²⁴ Boberg, Eklöf, Pääjärvi 2003 sid.11

2.4 Åtgärder för störskydd

Som tidigare omnämnts så finns en skillnad i störtåligheten mellan de olika kodsystemen. Den öppna C/A-koden återfinns bara i L1 signalen och har en mindre bandbredd än P(Y)-koden. P(Y)-koden finns dessutom dubblerad . Detta innebär att en simpel störskyddsåtgärd är att nyttja mottagare för C/A-koden och därmed uppnå ökat skydd genom ökad spridningsvinst. Detta stöds av FOIs egna beräkningar.

För en civil och militär GPS-standard-mottagare, utan yttre stöttning, kan störavståndet beräknas till 98,93 km respektive 46,3 km för en 4 watts bredbandig brusstörare och fri sikt mellan sändare och mottagare.²⁵

Möjligheten att övergå till mottagning av P(Y)-koden är dock som tidigare nämnts förbehållen enheter som av USA har tillgång till P(Y)-koden, detta innebär att civila fartyg är undantagna från denna möjlighet.

Ett alternativ för dessa enheter kan vara att istället nyttja sig av ett annat GNSS-system förslagsvis GLONASS där P-koden är fri. Detta ställer dock krav på att enheten förfogar över en mottagare anpassad för mottagning av GLONASS systemets P-kod något som i nuläget är mycket ovanligt.

I sammanhanget måste även poängteras att nyttjande av P(Y)-koden på inget sätt ger ett fullgott skydd mot störning utan endast minskar det avstånd på vilket mottagaren kan störas. Sammanfattningsvis kan sägas att enheter som har möjlighet att nyttja P(Y)-koden får ett förbättrat skydd mot störning. Dock är skyddet ej heltäckande och många plattformar lämnas helt utan denna möjlighet till skydd.

²⁵ Boberg, Eklöf, Pääjärvi 2003 sid.11

2.4.1 Störskydd genom adaptiv gruppantenn

En teknik för att ge förstärkt skydd mot störning utöver övergång till P(Y) koden är genom användande av en adaptiv gruppantenn. Tekniken bygger på att genom att nyttja ett antensystem med förmåga att anpassa sitt strålningsdiagram undertrycka mottagna signaler baserat på signalernas infallsvinklar.²⁶ På detta sätt kan signaler som inte kommer från den riktningen där satelliterna befinner sig diskrimineras bort.

För att effektivt kunna verka med telestörningsåtgärder mot ett system som skyddas av en adaptiv gruppantenn bör alltså störsändare placeras runt mottagaren på samma sätt som satelliterna vid tillfället är orienterade. System för adaptiva gruppantenner finns i nuläget på marknaden, det norska fartyget KNM Vidar var enligt FOI redan utrustat med ett sådant system år 2004.²⁷

System av denna typ är i nuläget så kostsamma att introduktion av dem på civila plattformar i nuläget förefaller otroligt. För att summera kan sägas att teknik involverandes adaptiva gruppantenner ger ett mycket kraftfullt skydd²⁸ mot störning men att tekniken än så länge av ekonomiska skäl till största delen är reserverad för militära användare.

²⁶ Eklöf, Pääjärvi 2004 sid.30

²⁷ Eklöf, Pääjärvi 2004 sid.8

²⁸ Boberg, Eklöf, Pääjärvi 2003 sid.14

2.5 Den irreguljära motståndares förmåga till störning av GNSS-system

För att kunna besvara uppsatsens frågeställning krävs en beskrivning av vilken typ och vilken omfattning som en irreguljär motståndare inom sjöarrendan kan nyttja sig av störning mot GNSS-system.

Informationsläget om vilka förmågor till teleteknisk störning av GNSS-system en irreguljär motståndare förfogar över är mycket bristfälligt. Detta leder till att fokus för denna beskrivning kommer att ligga i vilka tekniska system det kan bedömas som troligt att en irreguljär motståndare förfogar över.

En irreguljär motståndare kan bedömas ha tillgång till all teknik som finns tillgänglig på den öppna marknaden. Hänsyn måste dock tas till motståndarens ekonomiska situation. En bedömning över vilken typ av teknik som en irreguljär motståndare kan köpa på den öppna marknaden blir därmed till större delen en ekonomisk bedömning.

På marknaden finns flertalet färdiga störare för GPS och GLONASS, enligt FOI tillverkar exempelvis det ryska företaget Aviaconversiya:

en störsändare med 20 W och störavstånd upp till 221 km mot civila GPS-mottagare. Kostnaden för störsändaren har tidigare uppgivits till 40000 USD²⁹

Med hänsyn till den uppgivna kostnaden för en sådan störsändare bedömas det som inte orimligt att en irreguljär motståndare förfogar över eller kan komma att förfoga över den typen av utrustning.

Utöver inköpta färdiga störsändare kan en irreguljär motståndare även ha tillgång till egenkonstruerade störsändare.

En utförlig beskrivning av en enkel, billig och portabel GPS-störare finns tillgänglig på Internet [...] Komponenterna som skall användas är specificerade och kan köpas från en godtycklig elektronikfirma. [...] [GPS-störaren har] uteffekten 500mW och ett störavstånd på upp till 10 kilometer.³⁰

²⁹ Eklöf, Pääjärvi 2004 sid.7

³⁰ Eklöf, Pääjärvi 2004 sid.7

En enkel egenkonstruerad störsändare har inte samma prestanda som en professionellt tillverkad modell. En egentillverkad störsändare kan dock med tanke på priset och tillgängligheten bedömas vara en trolig del av en irreguljär motståndares telekrigsarsenal.

För att bedöma en irreguljär motståndares tekniska utrustning för att kunna störa ut en enhet utrustad med en adaptiv gruppantenn får en annan rimlighetsbedömning göras. För att kunna störa ut ett sådant system krävs som tidigare redovisats att ett flertal störsändare kan placeras runt enheten i en likartad konfiguration som satelliterna för tillfället befinner sig. En sådan störning ställer alltså stora krav på tillgång till flygande enheter samt förmågan att positionera dessa runt enheten. Dessa flygande enheter kan exempelvis vara fjärstyrda flygplan eller ballonger utrustade med störsändare. En rimlighetsbedömning klargör att ett sådant scenario med stor sannolikhet ej kan uppnås av en irreguljär motståndare på grund av tekniska och ekonomiska begränsningar.

Vid en summering av bedömningen av en irreguljär motståndares förmåga till störning av GNSS-system framkommer vissa rimliga bedömningar. För det första så är det sannolikt att en irreguljär motståndare kan förfoga över egen tillverkade störsändare med en mer begränsad effektivitet. För det andra är det inte orimligt att i alla fall en någorlunda välfinansierad irreguljär motståndare kan förfoga över professionellt tillverkade störsändare av en högre effektivitet. För det tredje bedöms det som osannolikt att en irreguljär motståndare kan förfoga över utrustning för att störa ut mottagare som skyddas av adaptiva gruppantenner.

3 Analys

I detta kapitel kommer de frågor som beskrivs i metod steg tre och fyra att behandlas. Kapitlet syftar till att genom teoribildning och hypotesprövning besvara frågeställningen. I detta kapitel kommer slutsatserna från empirikapitlet att nyttjas för att dra slutsatser vilka kan ge underlag för att verifiera eller falsifiera hypotesen. I kapitlet kommer frågan om vilken taktisk påverkan telekrig mot GNSS-system har på den svenska marinen att behandlas.

3.1 Påverkan på fartygssystem

Som tidigare har påvisats så kan en irreguljär motståndare inom sjöarenan ha förmåga till störning av GNSS-system i tidigare nämnd omfattning. Detta faktum leder in på frågan om vilken påverkan ett användande av denna förmåga kan ha på fartygssystem. Fartygssystem som begrepp är för brett för att ett allmängiltigt svar skall kunna ges. Därför fokuserar denna uppsatts på de fartygssystem som är relevanta med hänsyn till aktuella avgränsningar.

Då uppsatsen avgränsar sig i rum till den svenska marinen är det just marinens stridsfartyg generellt som kommer att behandlas istället för enskilda fartygstyper. Uppsatsen avgränsas även juridiskt till att endast hantera öppen information något som omöjliggör att i detalj presentera vilken typ av utrustning som finns på vilket fartyg.

Utöver detta kommer handelsfartyg som generellt fartygssystem att tas upp, detta för att ge underlag till att verifiera eller förkasta den hypotes som formulerades i inledningskapitlet.

3.2 Påverkan på marinens fartyg

Marinens fartyg har genom Sveriges bilaterala avtal med USA möjligheten att nyttja mottagare för P(Y)-koden. Genom detta kan marinens fartyg uppnå ett förbättrat skydd mot störsändning. Enligt FOIs studier minskas störsavståndet vid störning med fri horisont med en 4 watts bredbandig brusstörare från 99 km vid användning av C/A-kod till 46 km vid användning av P(Y) kod.³¹ För att en störning skall vara möjlig även på P(Y) koden krävs givetvis även att motståndaren har tillgång till den något mer avancerade utrustningen för mer bredbandig störning på två separata bärvågsfrekvenser.

³¹ Boberg, Eklöf, Pääjärvi 2003 sid.11

Marinens fartyg har utöver möjligheten till nyttjande av P(Y) kod vanligen även olika typer av integrerade navigationssystem där GNSS-positioneringen kan stöttas av exempelvis system för tröghetsnavigation. Detta innebär att en kortare tids förlust av GNSS-signal kan kompenseras med andra tekniska system. Om fartyget i fråga dessutom är utrustat med en adaptiv gruppantenn utgår helt effekten av en störning mot GNSS. I händelse av att telekrig mot GNSS börjar förekomma i ett operationsområde är det även fullt möjligt att marinens fartyg tillfälligt utrustas med en adaptiv gruppantenn.

Vad påverkan av ett bortfall av GNSS-system beträffar så får detta som huvudsaklig konsekvens att en annan navigationsmetod behöver nyttjas. Enligt Försvarens egna föreskrifter skall navigation genom GNSS-system endast vara ett komplement och skall ej ensamt utgöra huvudsystem.³² Detta innebär att påverkan även vid ett helt utstört system ej bör vara avgörande för navigationen. Sammanfattningsvis kan sägas att marinens fartygssystem förblir opåverkade om adaptiv gruppantenn nyttjas. Om adaptiv gruppantenn inte nyttjas så kan påverkan ske genom att möjligheten till positionering genom GNSS-system reduceras och andra metoder för positionering får nyttjas.

3.3 Påverkan på handelssjöfarten

Handelssjöfarten saknar möjligheten att nyttja P(Y) koden och är därmed mer sårbar för störning, dels för att störsändare inte behöver vara lika tekniskt avancerade vilket ökar sannolikheten att en irreguljär motståndare besitter denna typ av utrustning. Dels för att C/A koden har ett sämre störskydd. Även om det inom handelssjöfarten inte finns samma föreskrifter om att GNSS-system inte får nyttjas som huvudsystem så finns krav på att alternativa navigationsmetoder skall kunna nyttjas.

³² Försvarensmakten, Riktlinjer för nyttjande och anskaffning av satellitnavigeringshjälpmedel inom Försvarensmakten sid.6

3.3.1 Påverkan på AIS-systemet

Sedan 2002 skall alla civila fartyg över 300 gross ton³³ vara utrustade med en AIS-transponder. En AIS-transponder är en apparat som överför sjösäkerhetsrelaterad information mellan fartyg och mellan fartyg och land. Apparaten får sin ingående positions och tidsinformation direkt från en GNSS-mottagare ombord, vanligen från en GPS-mottagare. Transpondern sänder kontinuerligt ut information om bland annat sin aktuella position kurs och fart. Systemet arbetar helt utan inverkan från landstationer något som möjliggörs genom att alla transpondrars sändningar synkroniseras med hjälp av tidsinformationen från GNSS-mottagaren.³⁴

Som systemet är uppbyggt skulle alltså en pålagd störning av GNSS-signalen kunna få AIS-systemet att sända ut inaktuella eller felaktiga positionsangivelser till övriga fartyg och till landstationer. Risk föreligger även för att AIS-systemet slutar att överföra information om transpondrarnas synkronisering på grund av störning upphör. AIS-systemet har dock en viss förmåga till att motstå detta då fartyg som helt tappat GNSS-mottagningen kan få tidsangivelser från andra fartyg.

Eftersom handelsfartyg endast nyttjar C/A koden och saknar adaptiva gruppantenner så kan handelssjöfartens GNSS-mottagare störas med förhållandevis enkla medel. Med hänsyn till AIS-systemets uppbyggnad kan en störning av GNSS även överföras till AIS-systemet. Därmed kan störningen gå från att endast påverka det egna fartygets möjligheter till positionering till att även slå ut alternativt överföra inkorrekt eller föråldrad information genom AIS-systemet.

För handelsfartygens del bör denna påverkan inte vara alltför avgörande då AIS mestadels är ett medel för att uppnå förbättrad sjösäkerhet och minska risken för kollision. Detta faktum att AIS-systemet kan bli opålitligt kan dock få konsekvenser även för marinens fartyg.

³³ Exakta krav framgår i IMO SOLAS kapV regel 19.2.3.

³⁴ Malmquist 2001 sid.31-33

3.4 Taktisk påverkan av telekrig mot GNSS

För att på ett effektivt sätt kunna beskriva den taktiska påverkan av telekrig mot GNSS krävs en begreppsapparat för att särskilja mellan olika typer av påverkan. För denna uppsatts har författaren valt att beskriva den taktiska påverkan med begreppen direkt och indirekt påverkan.

Där direkt påverkan är den påverkan som sker förutsättningslöst mot ett eller flera fartyg. Ett exempel på en direkt påverkan kan vara möjligheten att i en specifik situation nyttja ett specifikt vapensystem. Eller att utföra en viss typ av uppdrag eller att uppträda i en viss typ av område. Medan indirekt påverkan är den påverkan som sker på en högre nivå och som inte är förutsättningslös. Ett exempel på en indirekt påverkan kan vara minskad möjlighet för en viss typ av samordning eller en längre beslutsprocess.

3.5 Mötet med den irreguljära motståndaren

Som tidigare definierats är den irreguljära motståndaren en motståndare som inte är del av ett lands reguljära styrkor. I vissa fall kan den irreguljära motståndaren ha en koppling till en specifik stat exempelvis om det är frågan om en medlem av en paramilitär organisation. I andra fall kan motståndaren representera en organisation utan koppling till en specifik stat, exempelvis om det är frågan om en medlem av en grupp som drivs av vissa politiska eller ekonomiska intressen.

Gemensamt för alla irreguljära motståndare är att de representerar en asymmetrisk motståndare, en motståndare som i organisation, resurser eller målsättning vida skiljer sig från de konventionella styrkor som de möter. Vid möten med asymmetriska motståndare blir kontrollen till sjöss och bestridande av densamma allt viktigare.

När den ena partens resurser för sjökrigsföring vida understiger den andra partens blir den direkta konfrontationen mellan parterna oönskad för den svagare. Detta leder till att bestridande av kontroll snarare än utövande av kontroll blir den tillgängliga sjöstridsmetoden för den underlägsna parten.³⁵ Som summering kan sägas att i mötet med en irreguljär motståndare inom sjöarenan kommer utövandet av kontroll till sjöss att utgöra en av huvudkomponenterna.

³⁵ Elg, Smedberg 2005 sid. 25

3.5.1 Att utöva kontroll

I den svenska doktrinfloran definieras begreppet att utöva kontroll i skriften doktrin för marina operationer som:

Syftet att utöva kontroll föregås av endera av moment för att etablera eller för att bestrida kontroll. Att utöva kontroll av ett maritimt område innefattar förmåga att hantera området i alla dimensioner inklusive informationsarenan. Utövandet av kontroll kräver ett gott informationsläge³⁴.

[34. ”Inklusive en etablerad metod för att bygga upp den marina lägesbilden (Recognised Maritime Picture (RMP))”]

Förmåga till insatser måste finnas. Den som utövar kontroll styr och avgör dueller och insatser.³⁶

Härmed framkommer med all tydlighet att förmågan till att skapa och upprätthålla RMP är en förutsättning för utövande av kontroll till sjöss.

I samma doktrin förekommer även begreppet havskontrolloperationer vilket i doktrinen beskrivs på följande sätt:

Närhelst handlingsfriheten för en maritim styrka hotas, i synnerhet när den närmar sig operationsområdet, finns ett behov att skapa en tillräcklig grad av kontroll över havet för att säkerställa dess skydd och möjliggöra de fortsatta operationerna. Utan erforderlig kontroll över havet påverkas den marina styrkans förmåga att manövrera, kraftsamla till offensiva insatser, utöva påtryckningar, projicera makt i land att ta ifrån motståndaren samma möjligheter. Alla maritima operationer kräver någon form av kontroll över havet och alla typer av operationer [...] är antingen en del av denna kontroll, i så stor utsträckning att de inte kan skiljas från den, eller också är de beroende av havskontroll som en förberedelse för att de skall kunna genomföras. [...] Havskontroll, genom närvaro till sjöss med kvalificerade marina enheter, skapar grunden för fri och säker maritim kontroll och säkerhet. Det säkerställer därmed maritim rörlighet.³⁷

³⁶ Försvarsmakten 2005 Doktrin för marina operationer sid. 90

³⁷ Försvarsmakten 2005 Doktrin för marina operationer sid. 84

I och med detta framkommer att kontroll utgör grunden för genomförande av havskontrolloperationer likväl som en av grundbultarna i alla marina operationer. I dagens svenska marin är havskontrolloperationer av stor betydelse. Båda de marina missionerna i Libanon och utanför Somalia kan anses som havskontrolloperationer. Det är också i denna typ av missioner som mötet med den irreguljära motståndaren hittills har skett, i Libanon i form av Hissbolla och i vattnen utanför Somalia i form av pirater. Betydelsen och behovet av att utöva kontroll kan sammanfattas som att utövande av kontroll är av avgörande betydelse för genomförande av alla marina operationer. Vid mötet av den irreguljära motståndaren inom sjöarenan är utövandet av kontroll av extra stor betydelse. Förmågan till RMP är en förutsättning för utövandet av kontroll.

3.6 Den direkta påverkan

Den direkta taktiska påverkan på marinens fartyg är som tidigare konstaterats avhängd av om fartyget är utrustat med en adaptiv gruppantenn eller ej, om så är fallet blir påverkan obefintlig då en irreguljär motståndare inte bedöms kunna påverka ett sådant system. Om fartyget ej är utrustat med en adaptiv gruppantenn kommer som tidigare konstaterats förmågan till exakt positionering försämrats något och andra navigationsmetoder än systemnavigering baserad på GNSS-system få nyttjas. Eftersom andra navigationsmöjligheter finns att tillgå så blir påverkan endast att de taktiska moment som ställer extremt stora krav på exakt positionering utsätts för en direkt påverkan.

3.7 Den indirekta påverkan

Den indirekta påverkan av telekrig mot GNSS vid möte av en irreguljär motståndare inom sjöarenan är mer svårdefinierat. Detta då kedjan av påverkan kan vara mycket lång och svår att bedöma. Därför och med hänsyn till denna uppsats omfattning väljer författaren att huvudsakligen fokusera på de påverkansområden som hittills framkommit under uppsatsen.

3.7.1 Närhet till land

En faktor som kan vara av intresse för den taktiska påverkan är hur möjligheterna att uppträda nära land påverkas vid störning av GNSS-system av en irreguljär motståndare. Som tidigare omnämnts är en avgörande faktor för hur effektiv en störning kan vara hur stort avståndet är mellan störsändaren och den enhet som skall störas. För att kunna på ett effektivt sätt störa mot fartyg från störsändare placerade på land krävs alltså att fartyget uppträder nära land. Dessa områden nära land som ofta benämns *littorals* är av extra stort intresse för mariner världen över då dessa tenderar att vara mer trafikintensiva. Risker för asymmetriska hot anses även vara högre i dessa områden.³⁸

Den direkta taktiska påverkan av störning av GNSS behöver dock inte vara högre i ett område nära land. Som tidigare konstaterats är den direkta påverkan begränsad till taktiska moment som ställer stora krav på en exakt positionering. Det kan anses som mindre komplicerat att placera en störsändnings utrustning på land än att placera den på ett fartyg till sjöss där tillgången till elström och andra förutsättningar är mer begränsade. Således kan sannolikheten för att utsättas för en störsändning av en irreguljär motståndare inom sjöarenan anses som större i områden nära land än fritt till havs.

3.7.2 Upprätthållande av RMP

Som tidigare omnämnts är RMP att betrakta som en direkt förutsättning för upprätthållande av kontroll till sjöss. Tidigare i uppsatsen har även konstaterats att en irreguljär motståndare inom sjöarenan har möjlighet att påverka AIS-systemet. Vid upprätthållande av RMP nyttjas flera olika sensorer där radar i de flesta avseenden är att betrakta som den mest betydelsefulla sensorn. Radarn har dock den nackdelen att det enbart genom nyttjande av radar som sensor ej är möjligt att identifiera fartyg, därför krävs sensorer som har möjligheten att binda ett fartygs identitet till ett specifikt radarmål.

För denna identifiering kan utöver traditionella metoder som optisk identifiering och utfrågning via radio numer även identifiering ske genom nyttjande av AIS-systemet. Detta innebär alltså att om en irreguljär motståndare nyttjar telekrig mot GNSS-system och därmed påverkar AIS-systemet så blir möjligheten att nyttja AIS-systemet för att koppla samman ett fartygs identitet med ett radarmål reducerad.

³⁸ Elg, Smedberg 2005 sid.15

3.7.3 Identifieringsmetoder vid påverkat AIS-system

Vid en reducerad förmåga att nyttja AIS-systemet för identifiering av fartyg kommer därmed traditionella metoder som optisk identifiering och utfrågning via radio att få ökad betydelse. För nyttjande av optisk identifiering krävs att sikt finns mellan identifierande fartyg och det fartyg som skall identifieras. Detta medför att det finns krav på att identifierande fartyg och det fartyg som skall identifieras ligger i närheten av varandra för att metoden skall kunna nyttjas. Således kan väderförhållanden som medför försämrade sikt samt mörker kraftigt minska det avstånd på vilket en optisk identifiering är möjlig.

För identifiering genom utfrågning via radio krävs att det fartyg som skall identifieras har en fungerande sambandsutrustning. Utöver detta krävs att det identifierande fartyg och det fartyg som skall identifieras befinner sig inom radoräckvidd från varandra. Marin VHF-radio är den idag vanligast förekommande radioutrustningen på fartyg, även AIS-systemet nyttjar VHF-radio³⁹ för överföring av AIS-information. Detta innebär att ett bortfall av AIS-systemet inte påverkar räckvidden för identifiering av fartyg om metoden utfrågning via radio nyttjas.

Utfrågning via radio har dock en betydande nackdel nämligen att ingen garanti finns för att det utfrågande fartyget verkligen är det som det utger sig för att vara. Detta leder alltså till att endast optisk identifiering kan ge en fullständigt säker identitet på ett radarmål om AIS-systemet inte kan nyttjas för identifiering.

Utöver optisk identifiering, utfrågning via radio och identifiering via AIS-systemet så finns även möjligheten att nyttja signalspaningsanläggning eller sonarsystem för att i viss mån identifiera fartyg som sedan tidigare är registrerade i signalbibliotek.

För att sammanfatta identifieringsmöjligheter om AIS-systemet ej är till förlitligt kan sägas att optisk identifiering blir av större betydelse. Vilket ställer krav på kortare avstånd mellan enheter.

³⁹ Malmquist 2001 sid.32

3.7.4 Ökade krav på rörlighet

I händelse av att AIS-systemet blir opålitligt och optisk identifiering behöver nyttjas i högre grad så kommer avståndet mellan identifierade enhet och det fartyg som skall identifieras att minska. I en sådan situation finns det två olika tillvägagångssätt för att vidmakthålla RMP i samma omfattning som med stöttning av AIS-systemet.

Antingen så måste fler enheter som har förmågan att optiskt identifiera fartyg tillföras för att på så vis minska avstånden mellan enheterna. Eller så måste de enheter som redan finns i operationsområdet nyttjas på ett mer effektivt sätt. Ett effektivt sätt kan i detta fall innebära att enheterna uppträder mer rörligt för att på så vis täcka in ett större område.

För att fullt ut kunna tillgodo se denna ökade rörlighet är det rimligt att anta att kraven på rörlighet därigenom ökar. En kombination av de två tidigare nämnda tillvägagångssätten kan givetvis också nyttjas. Detta kan ske exempelvis genom att i större omfattning tillföra en marin styrka förmågan till rörlighet genom att tillföra spaningsflygplan eller sjöbaserade helikoptersystem.

3.8 Hypotesprövning

För att underlätta besvarandet av frågeställningen har författaren valt att genom arbetet besvara hypotesen:

Den direkta taktiska påverkan på marinens fartyg är försumbar i jämförelse med den indirekta påverkan.

Med hänsyn till det som tidigare behandlats i detta kapitel så finns det nu möjlighet att med stöd av det som tidigare behandlats i uppsatsen försöka besvara frågeställningen. Som tidigare nämnts så är den direkta påverkan på marinens fartyg begränsad till att inskränka möjligheten till systemnavigering genom nyttjande av GNSS-system. Detta innebär att uppgifter som kräver mycket hög exakthet i fråga om navigation och positionering försvåras något då andra metoder än systemnavigation får nyttjas. Om fartyget är utrustat med en adaptiv gruppantenn sker ingen påverkan över huvud taget.

3.8.1 Jämförelser mellan direkt och indirekt påverkan

Den indirekta påverkan genom att AIS-systemet kan bli opålitligt vilket leder till att svårighet uppstår genom att identifiering av fartyg för upprätthållande av RMP försvåras. Detta försvårande av upprätthållandet av RMP tvingar den marina styrkan att vidta åtgärder för att upprätthålla RMP. Styrkan kommer att tvingas att öka sin förmåga till rörlighet genom att exempelvis tillföra helikoptersystem till styrkans organisation. Vid en jämförelse mellan den direkta påverkan och den indirekta påverkan så framgår tydligt att den indirekta påverkan ställer krav på förändring av en grundläggande förmåga något som den direkta påverkan inte gör anspråk på.

Således kan konstateras att den indirekta påverkan är väsentligt större än den direkta påverkan. Att avgöra om den direkta påverkan är försumbar i förhållande till den indirekta blir dock en subjektiv bedömningsfråga. Detta då det tidigare har konstaterats att det föreligger en viss direkt påverkan. Om de fartygsenheter som ingår i styrkan däremot är utrustade med en adaptiv gruppantenn kan hypotesen anses som verifierad. Detta då konstaterande tidigare gjorts att den direkta påverkan försvinner om fartyget är utrustat med en adaptiv gruppantenn.

3.9 Slutsatser

GNSS-system utgör idag en betydande komponent för positionering, såväl inom militären som i civila tillämpningar. Av de olika GNSS-systemen som finns i dag så är det amerikanska GPS-systemet det som fullständigt dominerar. Även om det ryska GLONASS-systemet är fullt användbart är så gott som uteslutande alla mottagare helt beroende av GPS-systemet. Detta gör att redundans bland GNSS-systemen i dag saknas. Så länge endast GPS nyttjas finns en tydlig svaghet i GNSS. Nämligen att endast ett system behöver påverkas genom telekrig för att slå ut möjligheten till positionering genom GNSS. I framtiden kan möjligheten att påverka GNSS-system minskas under förutsättning att fler mottagare kan ta in signaler från flera olika GNSS-system.

3.9.1 Möjlighet för en irreguljär motståndare att påverka GNSS

En irreguljär motståndare inom sjöarenan bedöms ha förmåga att störa ut GPS-systemets civila kod C/A-koden genom nyttjande av antingen inköpta eller hembyggda störsändare. Hur effektiva sådana störsändare är, kan inte fullständigt besvaras då avståndet till stor del förutom störsändarens uteffekt påverkas av antennhöjd och hur terrängen ser ut. Enligt FOI kan dock en enkel och billig störsändare ha en räckvidd på ca 10 km.

Vad en irreguljär motståndares förmåga att påverka mottagare som nyttjar sig av den militära P(Y)-koden beträffar så bedöms denna som mindre säker. Teknik för att störa den militära P(Y)-koden är mer avancerad eftersom den kräver störning på två olika frekvenser och på en större bandbredd. Detta innebär att om en irreguljär motståndare har tillgång till störsändare som kan verka mot P(Y)-koden så har dessa ett mindre verkansområde än sändare med samma uteffekt avsedda för C/A-koden.

Eftersom Sverige har ett bilateralt avtal med USA beträffande nyttjande av P(Y)-koden så kan Svenska stridskrafter uppnå ett visst skydd mot störsändning genom att använda P(Y)-koden. Enheter som har en adaptiv gruppantenn bedöms som helt skyddade mot störsändning från en irreguljär motståndare. Detta eftersom störning mot system som skyddas av adaptiva gruppantennar anses som för tekniskt avancerat och för resurskrävande för en irreguljär motståndare.

3.9.2 Alternativa positioneringsmetoder och direkt verkan

Så väl inom den svenska marinen som inom handelssjöfarten så är positionering genom GNSS endast en metod bland flera. Om GNSS-system till följd av telekrigsåtgärder skulle bli så pass påverkat att det ej längre kan nyttjas så skulle detta endast få till följd att andra positioneringsmetoder skulle få en större betydelse. Endast vissa verksamheter som ställer mycket höga krav på exakt positionering skulle kunna försvåras eller omöjliggöras. Avståndet till land måste här även nämnas som en betydande parameter, en irreguljär motståndare bedöms ha större möjligheter att påverka fartygssystem i områden nära land. Således begränsas den svenska marinens möjligheter till att genomföra verksamhet som ställer mycket höga krav på exakt positionering mer i områden nära land än fritt till havs. Enheter som är

utrustade med adaptiva gruppantenner skulle dock oförändrat kunna bedriva verksamhet som ställer mycket höga krav på exakt positionering.

3.9.3 AIS-systemet och förmågan till RMP

AIS-systemet är beroende av GPS-signaler som indata både för positionsangivelse i systemet och för tidssynkronisering av sändningarna. Om GPS-systemet störs ut så kommer AIS-systemet efter en tid att bli opålitligt. Detta medför att AIS-systemet i ett sådant scenario ej längre kan användas för identifiering av fartyg. Således försvåras möjligheterna att knyta en identitet till ett radarmål. Detta innebär i förlängningen att förmågan att upprätthålla RMP försämras.

3.9.4 Taktisk anpassning

För att kunna upprätthålla RMP på samma nivå som med full tillgång till identifieringsmöjlighet i AIS-systemet så krävs en högre förmåga till rörlighet. För att tillgodose detta ökade behov av rörlighet så kan det vara nödvändigt att tillföra den marina styrkan ytterligare komponenter som kan tillgodose detta behov. Sådana komponenter bör ha hög rörlighet och förmåga till optisk identifiering oberoende av ljusförhållande och väderlek. Förslagsvis kan spaningsflyg med allväderskapacitet eller helikoptrar med allväderskapacitet tillföras.

4 Diskussion

För att skapa en mer nyanserad bild av uppsatsens slutsatser och uppsatsens allmängiltighet krävs en diskussionsdel. Denna diskussionsdel har till syfte att från flera håll belysa såväl slutsatserna som avgränsningarna och uppsatsen i stort. I denna diskussion skall områden som uppsatsen ej täcker in presenteras för att ge underlag till vidare studier av ämnet. Genom detta tillvägagångssätt kan även intressanta områden för ytterligare studier utanför denna uppsats ramar framhållas.

4.1 AIS-systemet ur ett vidare perspektiv

I uppsatsen framhålls hur nyttjande av telekrigsåtgärder mot GNSS-system kan skada tillförlitligheten på AIS-systemet och därigenom försvåra upprätthållande av RMP. Om man studerar detta resonemang ur ett vidare perspektiv än störning av GNSS så framkommer kritik mot denna slutsats. Om en irreguljär motståndare har för avsikt att störa AIS-systemet så kan detta ske direkt mot AIS-systemet istället för att störa GNSS.

Exempelvis kan en motståndare vars avsikt är att slå mot AIS-systemet nyttja telekrigsåtgärder mot de tre VHF-frekvenser där AIS-information överförs mellan transpondrarna. Ett sådant tillvägagångssätt skulle ställa andra krav på teknisk utrustning och uteffekt. En motståndare som har för avsikt att slå mot AIS-systemet skulle även kunna nyttja sig av ett flertal AIS-transpondrar och ansluta dessa till inkorrekt indata. Därigenom skulle en motståndare kunna införa falska mål i AIS-systemet och därigenom minska AIS-systemets tillförlitlighet. Ingen av dessa metoder finns upptagna i uppsatsen då dessa går utanför uppsatsens frågeställning kring GNSS-system.

4.1.1 Motståndarens behov av GNSS

En faktor som uppsatsen ej behandlar är en irreguljär motståndares egna behov av GNSS-system för att genomföra verksamhet. En av slutsatserna i uppsatsen beträffande påverkan av telekrig mot GNSS är att den direkta påverkan ej är allt för stor. Om så är fallet kan frågan ställas om den irreguljära motståndaren påverkas kraftigare och därmed har mer att förlora på att störa GNSS än att vinna. Exempelvis kan en irreguljär motståndare med stora brister

beträffande redundanta metoder för navigation antas vara av så stort behov av fungerande GNSS att det ej ligger i motståndarens intresse att nyttja telekrig mot GNSS.

En irreguljär motståndare kan även nyttja information från AIS-systemet som underrättelseunderlag och därigenom vara i behov av ett fungerande GNSS. Något som stärker denna tes är att vissa rederier uppmanar sina fartyg att stänga av sina AIS-transpondrar i vatten där piratverksamhet förekommer för att försvåra för piraterna att lokalisera handelsfartyg.⁴⁰

4.2 Uppsatsens allmängiltighet

För att skapa en bild av uppsatsens allmängiltighet måste en återkoppling till uppsatsens avgränsningar och eventuella brister i slutledningen göras. I uppsatsen sker avgränsningar till Sveriges Försvarsmakt. Detta sänker allmängiltigheten då slutsatserna således endast är tillämpliga om de appliceras inom Sveriges Försvarsmakt. I uppsatsen avgränsas tiden till efter det kalla krigets slut, detta får som konsekvens att slutsatserna i uppsatsen ej kan appliceras i ett historiskt perspektiv. Då GNSS-system som koncept är en förhållandevis modern företeelse bör denna avgränsning i tid inte sänka uppsatsens allmängiltighet i någon större omfattning.

Som tidigare nämnts under rubriken AIS-systemet ur ett vidare perspektiv så finns det för slutsatserna relevanta faktorer som ej behandlats i uppsatsen. Detta med hänsyn till uppsatsens fokus på störning av GNSS-system. Detta medför att uppsatsens allmängiltighet blir begränsad då de slutsatser som presenteras är en effekt av frågeställningen och avgränsningarna. Slutsatserna är således endast verifierade ur perspektivet störning riktat mot GNSS och med rådande avgränsningar.

⁴⁰ Sörenson 2008 sid.36

5 Avslutning

5.1 Sammanfattning

Den tekniska utvecklingen inom navigationsområdet går snabbt och såväl militära som civila fartyg nyttjar i allt högre grad satellitbaserade navigations system (GNSS). Samtidigt blir den svenska marinen allt mer involverad i insatser utomlands där fienden är en irreguljär motståndare vars medel är begränsade. Enligt totalförsvarets forsknings institut (FOI) är det möjligt att med enkla medel och till ringa kostnad tillverka en störsändare som stör ut möjligheten till nyttjande av GNSS. Detta ligger till grund för denna uppsats frågeställning: *Hur påverkas marinen taktiskt av fientlig störning av GNSS-system vid möte av en irreguljär motståndare inom sjöarenan?*

I dag finns flera olika GNSS-system varav endast två är helt operativa. Av dessa två är det endast det amerikanska GPS-systemet som används i större utsträckning. GPS-systemet sänder signaler för positionering på två olika bärvågor och med två olika kodsystem. Av dessa två kodsystem benämns den ena C/A-koden, denna kod är öppen för alla användare och sänds bara på den ena bärvågsfrekvensen. Medan den andra är koden benämnd P(Y)-koden är reserverad för militära ändamål. P(Y)-koden är fördelad på båda bärvågsfrekvenserna vilket gör den betydligt mycket tekniskt avancerad att störa ut. Sverige har ett bilateralt avtal med USA som möjliggör nyttjande av den mer svårstörda P(Y)-koden för Sveriges Försvarsmakt.

En irreguljär motståndare bedöms ha förmåga att störa ut både den öppna C/A-koden och den militära P(Y)-koden, dock blir störavståndet väsentligt mindre vid störning mot P(Y)-koden. En irreguljär motståndare bedöms inte ha förmåga att störa GNSS för ett fartyg utrustat med adaptiv gruppantenn. Adaptiva gruppantenner är dock så pass dyra att endast vissa militära fartyg är utrustade med sådana.

Enligt Försvarsmaktens föreskrifter skall positionering genom nyttjande av GNSS endast ses som ett komplement till andra metoder. Även inom handelssjöfarten finns liknande bestämmelser om att andra metoder för positionering skall kunna nyttjas.

Den påverkan som en irreguljär motståndares telekrigsåtgärder mot GNSS kan åstadkomma mot den Svenska marinen uppdelas i denna uppsats i direkt påverkan och indirekt påverkan.

Där direkt påverkan är den påverkan som sker förutsättningslöst mot ett eller flera fartyg. Medan indirekt påverkan är den påverkan som sker på en högre nivå och som inte är förutsättningslös. Ett exempel på en indirekt påverkan kan vara minskad möjlighet för en viss typ av samordning eller en längre beslutsprocess.

Den direkta påverkan för den Svenska marinens fartyg är högst begränsad då positionering genom GNSS endast är ett komplement till andra metoder. Den direkta påverkan är således mycket liten och kan anses begränsad till att endast påverka verksamhet som kräver extremt hög precision i positioneringen. Det samma gäller för handelstrafiken.

Vad den indirekta påverkan beträffar så kan en störning av GNSS få som följd att handelsfartygens AIS-system blir utslaget eller opålitligt till följd av inkorrekt indata från handelsfartygens GNSS-mottagare. Detta får till följd att AIS-systemet inte längre kan användas till att understödja upprätthållandet av RMP genom att knyta identiteter till radarmålen.

För att en marinstyrka skall kunna upprätthålla RMP i samma omfattning med störningar riktade mot GNSS som utan så måste åtgärder vidtas för att kompensera för bortfallet av möjligheten till identifiering via AIS-systemet. Dessa åtgärder kan antingen vara att tillföra mer enheter eller öka rörligheten på de enheter som finns. Förslagsvis kan en kombination nyttjas och enheter med hög rörlighet tillföras, exempelvis helikoptersystem eller spaningsflyg.

Avslutningsvis kan konstateras att den direkta påverkan på den svenska marinen vid möte av telekrig av en irreguljär motståndare riktat mot GNSS-system är låg i förhållande till den indirekta påverkan. Den indirekta påverkan består av att rörlighet får en högre betydelse för att kompensera för förlusten av möjligheten till identifiering av fartyg genom nyttjande av AIS-systemet.

Det kan även konstateras att slutsatserna i uppsatsen är en produkt av frågeställningen i förhållande till avgränsningarna. För att få fram mer allmängiltiga slutsatser krävs att avgränsningarna breddas. Detta för att behandla frågor som den irreguljära motståndarens egna behov av GNSS. Samt för att behandla möjligheten för en irreguljär motståndare att nyttja telekrig direkt mot AIS-systemet istället för mot GNSS-systemet.

5.2 Behov av vidare forskning

Under rubriken diskussion har ett antal problemområden nämnts som begränsar denna uppsats slutsatsers allmängiltighet. Ur det resonemang som där presenteras kan det utläsas att för att göra slutsatserna mer allmängiltiga krävs en fördjupad studie. En sådan fördjupad studie bör ha betydligt breddade avgränsningar för att därigenom öka slutsatsernas allmängiltighet.

Förslagsvis kan en studie genomföras som behandlar hela AIS-systemet och dess utsatthet för störning och inte bara hantera störning relaterad till GNSS-systemet. Studien bör även involvera en irreguljär motståndares behov av AIS-systemet för genomförande av egen verksamhet. I detta perspektiv kan den allmänna definitionen irreguljär motståndare bli ett förbrett begrepp och en inriktning på en specifik motståndare kan bli nödvändig.

För att få ett större praktiskt utbyte av en framtida studie krävs förutom de breddningar i avgränsningarna som tidigare omnämnts även att en kommande studie även behandlar sekretessbelagd information. Detta för att utöka den praktiska nyttan då det i en sådan studie skulle vara möjligt att avgöra mer specifikt vilken direkt taktisk påverkan störning av GNSS-system kan få för enskilda fartyg i den svenska marinen.

6 Litteraturförtäckning

Andrews, Angus; Weill, Lawrence; Grewal, Mohinder 2007 *Global Positioning Systems, Internal Navigation, and Integration*. New Jersey: John Wiley & Sons, Inc.

Boberg, Bengt; Eklöf, Fredrik; Pääjärvi Lars 2003 *Störning av navigationssystem, slutrapport. FOI-R—1018—SE*. Stockholm: FOI

Boberg, Bengt; m.fl. 2006 *Robust Navigering – Slutrapport. FOI-R—2081—SE*. Stockholm: FOI

Borg, Björn; mfl 1999 *Navigation 3 – Navigering med teletekniska hjälpmedel*. Stockholm: Försvarmakten

Ejvegård, Rolf 2003 *Vetenskaplig metod*. Lund: Studentlitteratur

Eklöf, Fredrik; Pääjärvi Lars 2004 *Telekrig mot GNSS – årsrapport 2004. FOI-R—1415—SE*. Lindköping: FOI

Elg, Johan; Smedberg, Marco 2005 *Sjömakt – Nutida maritima operationer i en gemensam och multinationell kontext*. Stockholm: Försvarshögskolan

Engfeldt, Andreas; Jivall Lotti; Lilje Christina 2007 *LMV-rapport 2007:11—Introduktion till GNSS*. Gävle: Lantmäteriet

Försvarmakten 2002 *Militärstrategisk doktrin*. Stockholm: Försvarmakten

Försvarmakten 2005 *Doktrin för gemensamma operationer*. Stockholm: Försvarmakten

Försvarmakten 2005 *Doktrin för marina operationer*. Stockholm: Försvarmakten

Huges, Wayne 2000 *Fleet tactics and costal combat* Annapolis: Naval Institute Press

Larsen, Jeffery; Wirtz, James 2009 *Naval Peacekeeping and Humanitarian Operations – Stability from the sea*. Abigdon: Routledge

Malmquist Lars 2001 *AIS transponder till sjöss från idé till världsstandard*. Norrköping: Sjöfartsverket

Rekkedal, Nils Marius 2006 *Insurgency and Counter-Insurgency: A Presentation of Concepts and Problems*. Stockholm: Försvarshögskolan

Sörenson, Karl 2008 *State Failure on the High Seas –Reviewing the Somali Piracy*. FOI-R--2610--SE Stockholm: FOI

Vego, Milan 2003 (1999) *Naval Strategy and Operations in Narrow Seas*. London: Frank Cass publishers

Werner, Christopher 2002 *Den blå boken – Marina stridskrafter ur ett militärteoretiskt perspektiv*. Stockholm: Försvarshögskolan

Otryckta källor:

Försvarsmakten 2005 *Försvarsmaktens riktlinjer för nyttjande och anskaffning av satellitnavigeringshjälpmedel – GNSS*. Stockholm: Försvarsmakten

Lundströmer, Thorbjörn 2009 *Hjälp! Vem tog min GPS? – Studie av redundanta metoder i integrerade positioneringssystem*. Självständigt arbete i militärteknik ChP(T) 07-09
Stockholm: Försvarshögskolan

Internet:

International Maritime Organization, www.imo.org/conventions/mainframe.asp?topic_id=250
Åtkommen 2010-06-08

Russian Federal Space Agency, <http://www.glonass-ianc.rsa.ru/> *Åtkommen 2010-04-19*