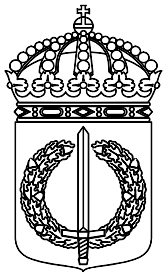


FÖRSVARSHÖGSKOLAN

C-UPPSATS

Författare	*Förband*	*Kurs*
Stefan Berner	HKV	CHP 04-06 T
FHS handledare		*Tel*
Bertil Wennerholm, Hans Liwång		
Uppdragsgivare	*Beteckning*	*Kontaktman*
FHS MVI	19 100:1348	

”Kill with a borrowed sword”

Kinesisk förmåga till informationsoperationer och CNO

Efter Kuwaitkriget 1991 har Kina påbörjat att modernisera sin försvarsmakt där informationsteknologin fått en ökad betydelse. Informationsteknologin har medfört ett ökat kinesiskt intresse för informationsoperationer som ett sätt att angripa en motståndares system.

Syftet med denna uppsats är att lägga en grund för fördjupad kunskap kring Kinas syn på och förmåga till informationsoperationer och informationskrigföring, samt att inom dessa områden speciellt belysa CNO. Detta för att få en insikt i Kinas militära upprustning.

Metoden som används för att analysera detta är att genom textanalys jämföra kinesisk och amerikansk krigföringsförmåga inom informationsoperationer i allmänhet och CNO i synnerhet. Teoriansatsen för jämförelsen bygger på den svenska ”Pelarmodellen” som analysverktyg för krigföringsförmågan.

Resultatet visar på att det finns likheter mellan USA och Kina, men att det också finns avgörande skillnader. Dessa består främst i Kinas integrering av civila och militära resurser där milisförband utgör ett viktigt bidrag till armén, samt användandet av strategier som ett sätt att kompensera tekniska tillkortakommanden och jag har där funnit en avsaknad av diskussion kring legala frågor kring nyttjandet av CNO på den kinesiska sidan.

Nyckelord:

Kina, USA, informationsoperationer, informationskrigföring, CNO, milis, strategier, krigslist.

ABSTRACT

The English version of the former printed text

After the Kuwait war in 1991 has China begun to modernize is defence force and where the information technology have got a more important role. The information technology has brought to consequence an increased Chinese interest for information operations as a method to attack adversary systems.

The purpose with this essay is to lay a foundation for a increased knowledge in Chinese views and capacity to information operations and information warfare, and within these areas especially highlight CNO. The reason for that is to get an insight in the Chinese rearmament.

The method used to analyse this is by text analyses compare Chinese and American fighting capability in information operations in general and in CNO in particular. The theory base for the comparison is build upon the Swedish ”Pelarmodellen” as the tool for the analyse of the fighting capacity.

The result shows that there is similarities between USA and China, but there is also crucial differences. They consists mainly of Chinese integration between civil and military resources where militia units constitute a important contribution to the army, and the use of strategies as a way to compensate technological inferiority in witch I discovered a lack of discussion on legal aspects revolving the use of CNO on the Chinese part.

Keywords:

China, USA, information operations, information warfare, CNO, militia, strategies, stratagems.

INNEHÅLLSFÖRTECKNING

1. INLEDNING

”You fight your way and I fight my way”

Mao Tse-tung

1.1 Bakgrund

Kina är världens folkrikaste land med sina 1,3 miljarder innevånare och till ytan det tredje största landet i världen.

Kina har sedan 2:a världskriget förlitat sig på att de stora ytorna och den stora folkmängden ska avskräcka en angripare. Kuwaitkriget 1991 utgjorde en vändpunkt för dem. Kina fick då se hur en folkrik irakisk armé med till stor del rysk utrustning besegrades av styrkor utrustade med högteknologiska vapen som stöddes av informationssystem. Vidare hade den USA-ledda alliansen tidigt skaffat sig luftöverlägsenhet och informationsöverlägsenhet genom att bekämpa irakiska kommunikationssystem.

Analyserna efter kriget gjorde att Kina påbörjade modernisera sin försvarsmakt. Förändringen sker inom två områden. Försvaret går från en personaltung armé med omodern teknologi till en kvantitativt mindre styrka men med högre tekniskt kvalitet. Den andra förändringen är att Kina går från att ha varit beredda kämpa ett stort defensivt krig på kinesiskt territorium till att tala om att strida i begränsade krig i Kinas närhet.

För att möta detta nya synsätt genomför Kina nu en kraftig upprustning av hela sin krigsmakt. Amerikanska källor hävdar att Kina köper moderna stridsflygplan, luftvärnsrobotar och fartyg från Ryssland. Kina utvecklar själva nya plattformar och förbättrar sina ballistiska robotar. Kina har dock insett att de under överskådlig tid kommer att vara tekniskt underlägsna många högteknologiska krigsmakter, främst USA. De har då sökt andra vägar för att kompensera för dessa tekniska svagheter.

Ett område som Kina anser sig ha identifierat som en svaghet hos USA är deras beroende av informationssystem för krigföringen. Kina har därför studerat amerikanska teorier för informationsoperationer, IO, och ser det som ett möjligt verktyg att kompensera för USA:s överlägsenhet. Informationsoperationer syftar till att påverka information och informationssystem hos motståndaren, samtidigt som egna system skyddas. Inom IO finns det en rad förmågor och där USA bland annat följer den kinesiska utvecklingen av Computer Network Operations, CNO, med stort intresse. Detta beroende på att kineserna själva framhäver detta område.

Trots att Kina genomför denna omvandling och upprustning av sitt försvar talas det inte speciellt mycket om den vid utbildningen på Försvarshögskolan. Då jag ser Kina som ett fascinerande land med lång tradition inom det militära området kan denna uppsats ses som ett sätt att fördjupa min egen kunskap om detta land.

1.2 Syfte

Syftet med denna uppsats är att lägga en grund för fördjupad kunskap kring Kinas syn på och förmåga till informationsoperationer och informationskrigföring, samt att inom dessa områden speciellt belysa CNO. Detta för att få en insikt i Kinas militära upprustning.

Ett underliggande syfte är att genom att studera Kinas förmåga till IO och CNO, även ge underlag för att i framtiden belysa svenska koncept inom dessa områden.

1.3 Problemformulering

Beskriv större skillnader mellan Kinas och USA:s krigföringsförmåga inom informationsoperationer med tyngdpunkt på CNO, idag och i nära framtid. Om det finns sådana, diskutera och dra slutsatser vad de innebär.

För att kunna svara på det måste jag på vägen diskutera följande:

- Hur definieras Informationsoperationer och Informationskrigföring i Kina respektive USA?
- Hur definierar Kina och USA CNO?
- Vilka resurser finns inom CNO?
- Betonar de olika strategier inom IO och CNO?
- Vilken vilja finns att nyttja CNO?

1.4 Avgränsningar

Kina och USA:s försvarsmakter och förmågor är omfattande. Denna uppsats kommer bara studera deras respektive förmåga till informationsoperationer och inom informationsoperationer kommer tyngdpunkten att ligga på CNO. Orsaken till detta är att Kinas möjligheter att genomföra CNO är en förmåga som uppmärksammats, inte minst i USA samt omfånget på uppsatsen.

Uppsatsen kommer inte att ge svar på om det är Kina eller USA som har den bästa krigföringsförmågan vad avser IO och CNO. Detta beroende på att det i de öppna källorna inte finns tillräckligt med underlag för att på ett vetenskapligt sätt kunna svara på den frågan.

Nytt material publiceras hela tiden kring dessa förmågor och definitioner förändras. För denna uppsats har strävan varit att studera nuläget, vilket medför att inga härledningar görs kring hur begreppen har vuxit fram och förändrats över tiden.

Uppsatsen kommer inte att beröra tekniska detaljfrågor av typen ”Vad är ett datavirus?” eller ”Vilken skada kan en motståndare göra i ett informationssystem med hjälp av datavirus?”. Detta beroende på att det finns tidigare studier inom dessa områden.

1.5 Antaganden

Uppsatsen vänder sig till studerande och anställda vid Försvarshögskolan samt övriga intresserade av Kinas förmåga till informationsoperationer. Läsaren förutsätts därför vara insatt i de normalt förekommande begreppen och förkortningarna samt ha en grundläggande kunskap inom området.

1.6 Tidigare forskning

På Försvarshögskolan, FHS, finns det på c-uppsatsnivå, ingen tidigare forskning kring Kina och deras syn på informationsoperationer och CNO. Vad gäller forskning utanför FHS finns det en stor mängd litteratur, främst på Internet och främst från amerikanska analytiker.

Då begreppet *Krigföringsförmåga* är centralt i uppsatsen utgör det grunden för teorikapitlet. Kring detta begrepp finns tidigare forskning och där jag har valt att, förutom svenska doktriner, studera Gustaf Dufbergs c-uppsats *Krigföringsförmåga* från 2005.

1.7 Centrala begrepp, Definitioner & Förkortningar

Då USA används som jämförelse till Kina nyttjas den amerikanska doktrinen *Joint Publications 3-13* förkortningar och definitioner kring begreppet informationsoperationer. Uppsatsen kommer inte att analysera deras uppkomst.

I uppsatsen används följande förkortningar regelbundet. För definitioner kring dessa begrepp, se bilaga 1.

IO: Information operations

IW: Information warfare

CNO: Computer network operations

CNA: Computer network attack

CND: Computer network defense

CNE: Computer network exploitation.

2. TILLVÄGAGÅNGSSÄTT

2.1 Disposition

I det första kapitlet beskrivs bakgrund, syfte och problemformuleringar. Detta för att skapa en ram kring vad uppsatsen ska handla om.

Kapitlet som följer beskriver tillvägagångssättet för att få en spårbarhet i arbetet och för att ge en syn på det material som används i uppsatsen.

I teorikapitlet beskrivs hur jag ser på krigföringsförmågan utifrån krigföringsförmågans tre faktorer.

I det fjärde och femte kapitlet återfinns empirin. Den är uppdelad i två huvudområden – Kina och USA. För respektive land ges en beskrivning av de fysiska, konceptuella och moraliska faktorer som framkommit i textanalysen.

I kapitel sex görs en analys där Kina och USA:s förmågor för respektive faktor, jämförs genom att studera skillnader och likheter i deras koncept. Kapitlet avslutas med att frågorna som ställts besvaras.

Uppsatsen avslutas med en diskussion och förslag på fortsatt forskning samt käll- och litteraturförteckning.

2.2 Metod

Målet med denna uppsats är att belysa Kinas förmåga till IO/IW samt CNO. För att kunna göra det jämförs Kina med USA där likheter och olikheter vad gäller förmågor inom IO och CNO analyseras. Det är deras krigföringsförmåga idag och en nära framtid som ska analyseras. I begreppet ”större skillnader” menar jag att det är avvikelser av avgörande karaktär som jag ska diskutera och dra slutsatser kring.

Orsaken till att Kina jämförs med USA är att USA är den enda supermakten idag, är välkänd och kan därför användas som resonansbotten mot det mer okända Kina. Tyngdpunkten i uppsatsen kommer däremot att ligga på Kina.

För att besvara frågeställningarna görs en komparativ, kvalitativ textanalys av relevanta dokument. Med detta menar jag att jag ska göra en systematisk jämförelse av olika dokument som jag tolkar för att få en förståelse hur de kan ge svar på mina frågeställningar.

För att systematiskt beskriva och analysera krigföringsförmåga används den svenska doktrinen. I doktrinen anges att den så kallade *Pelarmodellen* kan nyttjas som analysmodell av krigföringsförmågan. Förmågan delas där in i Fysiska, Konceptuella och Moraliska faktorer. I teorikapitel beskrivs detta och analysfaktorer tas fram för respektive faktor.

I de **Fysiska faktorerna** kommer jag att analysera förband med personal och utrustning, vilka stödresurser som finns samt utbildning och övningar för förbanden.

För att kunna svara på detta kommer jag att beskriva vilka förband som finns för IO och CNO, vilken IT-industri som finns då det kan ge en bild av den utrustning som landet disponerar, infrastruktur för IT i form av datanätverk med utrustning, samt utbildnings- och övningsverksamhet inom IO och CNO för respektive land.

I de **Konceptuella faktorerna** kommer jag att analysera hur Kina och USA ser på IO och CNO samt nyttjande av detta.

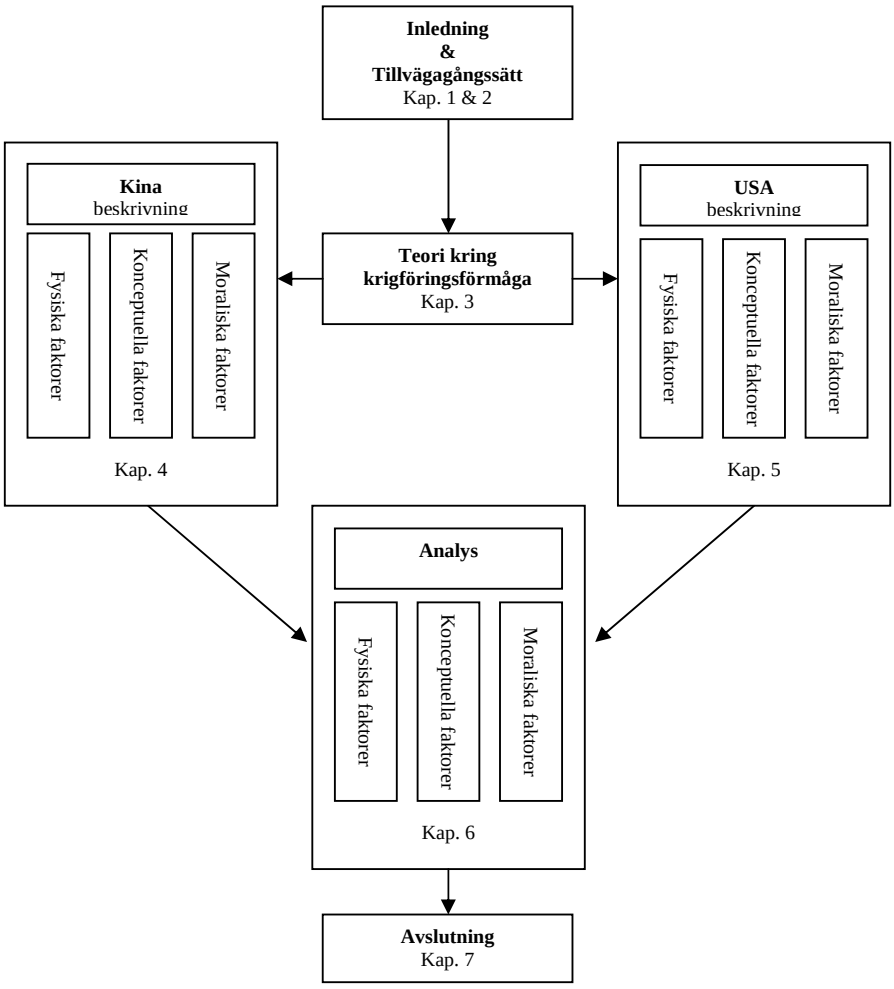
För att kunna svar på det inleder jag med att studera doktriner för att se ländernas definitioner kring begreppen IO/IW och CNO. Om doktriner saknas kommer jag att studera andra styrdokument eller analyser av begreppen. Därefter ska jag studera hur de ser på användande av IO och CNO.

I de **Moraliska faktorerna** ska jag översiktligt analysera i vilken eller vilka situationer Kina och USA skulle kunna tänka sig nyttja förmågan till IO och CNO samt vilka erfarenheter de har av detta.

För att kunna svara på detta ska jag översiktligt studera hur länderna resonerar kring legala frågor kring att nyttja IO och CNO samt studera om de använt IO och CNO i konflikter.

Jämförelsen mellan Kina och USA, vad gäller IO, IW och CNO görs genom att för respektive ”pelare” diskutera skillnader och likheter och utifrån detta dra egna slutsatser.

Arbetsgången kan åskådliggöras på följande sätt:



2.3 Material & Källkritik

Det finns en stor mängd material kring Kina, USA, informationsoperationer och CNO. Denna uppsats bygger i huvudsak på material från officiella dokument från respektive lands myndigheter samt analyser från olika organisationer. För att på ett vetenskapligt sätt hantera materialet har följande aspekter beaktats.

2.3.1 Materialet – Allmänt

För teorikapitlet, *Teorier kring krigföringsförmåga*, har svenska doktriner samt c-uppsatsen *Krigföringsförmåga*, publicerad vid FHS 2005, studerats.

Vad gäller val av material till empirin, har jag sökt material främst med hjälp av Internet men också via samtal med Nils Mauris Rekkedal, professor i krigsvetenskap vid FHS, samt Lars Nicander och Fredrik Konnander, lärare inom IO vid FHS, samt genom Anna Lindh-biblioteket.

Huvudparten av materialet i uppsatsen är nedladdat från Internet. Orsaken till detta är främst det resonemang som förs under *Tidskriterium* nedan, men även att det på Anna Lindh-biblioteket saknats de tryckta källor jag sökt.

Huvuddelen av materialet i denna uppsats är skrivet på engelska och de kinesiska texter som nyttjats är översatta till engelska av olika organisationer.

2.3.2 Materialet - Kina

Ett syfte med denna uppsats är att studera doktriner. Det närmaste som kan kallas en kinesisk doktrin och som är översatt till engelska, anser jag vara *China's National Defense in 2004,* och är ett så kallat *White Paper* från de kinesiska myndigheterna. Enligt *Federation of American Scientist,* FAS, utgavs detta i december 2004 av Kinas *The State Council Information Office*.

Kinas regering har publicerat dessa dokument om sin försvarsmakt regelbundet sedan år 2000. Vitboken från 2004 är den tredje i serien och innehåller tio kapitel där Kina beskriver sin policy i försvarsfrågor och försvarsmaktens moderniseringsprocess.

Ett White Paper är en officiell redovisning av en regerings policy .[1] Ett svenskt begrepp är *vitbok* som är en ”*officiell dokumentsamling i utrikespolitiskt eller diplomatiskt ärende*” och i engelsk – svenska lexikon översätts white paper med vitbok.[2,3] I uppsatsen används därför i huvudsak det svenska ordet vitbok vid referenser till *China's National Defense in 2004*. Någon annan kinesisk doktrin av öppen karaktär och översatt till engelska har jag inte funnit och jag accepterar detta dokument som ett uttryck för kinesisk säkerhetspolitik.

Vidare har jag studerat artiklar på kinesiska försvarsmaktens hemsida, *PLA Daily Online*. Jag accepterar även dessa som uttryck för kinesisk uppfattning eller vad Kina vill att omvärlden ska tro. Artiklarna bör dock vara officiellt sanktionerade och författarna till dem bör ha källor som är insatta i de frågeställningar som berörs. Jag har i min analys av dessa artiklar försökt väga dem mot andra källor.

Under arbetet med uppsatsen har en stor mängd analyser av främst amerikanska organisationer och författare studerats. I detta arbete konstaterades att de ofta refererade till samma kinesiska författare och artiklar. Jag har därför sökt dessa artiklar för att själv tolka dem, men tyvärr utan framgång. Detta medför att jag, med resonemang som redovisas nedan i åtanke, förlitat mig på de referat av dem som gjorts av andra författare.

Då det gäller material från amerikanska organisationer, har tre källor nyttjats:

Hudson Institute, en amerikansk, finansiellt oberoende, så kallad ”think-tank” och som anses vara politiskt oberoende, men konservativ. Från dem har en artikel i *China's New Great Leap Forward – High Technology and Military Power in the Next Half-Century* använts för att belysa Kinas industriella utveckling. Författaren till den artikeln är Ernest Preeg, forskare inom internationell ekonomi.

International Assessment and Strategy Center beskrivs som en finansiellt- och politiskt oberoende ”think-tank”. Där har artikeln *Top Ten Military Modernization Development* använts för fördjupning av en aspekt i Kinas modernisering.

---

[1] Källa: Wikipedias engelska upplaga. Se: http://en.wikipedia.org/wiki/White_paper (2006-10-06).
[2] Källa: Nationalencyklopedin http://www.ne.se/jsp/search/article.jsp?i_art_id=O392820 (2006-10-20).
[3] WordFinder 04, Lexikon: En-Sv Norstedt, sökord: *white paper*.

Center for Naval Analyses är en amerikansk ekonomiskt oberoende organisation som ger stöd kring operationsanalyser till civila myndigheter och organisationer. Från dem har jag studerat artikeln *Joint Operations: Developing a New Paradigm* i konferensrapporten *China's Revolution in Doctrinal Affairs: Emerging Trends in the Operational Art of the Chinese People's Liberation Army.*

2.3.3 Materialet - USA

Vad gäller material från USA så är öppenheten större. En amerikansk motsvarighet till Kinas vitbok, är dels *The National Security Strategy* (NSS), dels *Quadrennial Defense Review Report* (QDR).

Vidare har *Joint Publications 3-13 Information Operations,* studerats då det är en doktrin specifikt för informationsoperationer. Precis som för deras kinesiska motsvarighet accepterar jag dessa handlingar som uttryck för amerikansk säkerhets- och försvarspolitik.

Vidare har jag studerat ett antal rapporter från amerikanska kongressen och försvarsdepartementet som beskrivit amerikanska förmågor inom IO och CNO. Vissa av dessa beskriver dessutom amerikansk syn på den kinesiska försvarsmakten. Ett exempel på ett sådant dokument är *Military Power of the People's Republic of China 2006,* som är en årlig rapport till kongressen om kinesisk strategi och militär utveckling. Dokumenten från olika amerikanska departement och myndigheter anser jag redovisar amerikansk syn på egen och kinesisk förmåga.

2.3.4 Äkthet

En äkthetsaspekt är att denna uppsats har förlitat sig på att de översättningar som olika organisationer och myndigheter gjort från kinesiska till engelska är korrekta eftersom uppsatsskrivarens kunskap i det kinesiska språket är obefintliga. Men det är likväl en osäkerhetsfaktor, speciellt som jag uppfattat att det kinesiska språket är mångfacetterat och att det därför kan vara svårt att korrekt översätta nyanser i det.

Tolkningen av de engelska texterna är i sin tur en potentiell felkälla. För att minimera detta har jag i denna uppsats nyttjat programmet *WordFinder 04* som tillhandahållits av FHS. I det har Nordstedts lexikon använts för att översätta från engelska till svenska. På några ställen i uppsatsen är det för tydlighetens skull infogat citat från källorna på originalspråket.

Jag har haft dessa aspekter i åtanke under uppsatsen och betraktar översättningarna som äkta och mina översättningar som tillräckligt bra.

De hemsidor jag hämtat material från, har jag betraktat som äkta och antagit att de inte varit utsatta för någon manipulation i form av en informationsoperation.

2.3.5 Tidskriterium

I arbetet med uppsatsen konstaterades tidigt att analytiker anser att Kina snabbt utvecklar sin förmåga och sina teorier kring informationsoperationer och CNO.

För att hantera den snabba utvecklingen på detta område har strävan varit att nyttja de senast publicerade officiella dokumenten. Ett exempel på det är amerikanska försvarsdepartementets rapport om Kina som utkommit regelbundet de senaste åren, men där jag för denna uppsats valt att studera den

som publicerades 2006. Ett annat exempel är tidigare nämnt policydokument från Kina.

Tidsfaktorn har även präglat urvalet av övriga källor där strävan har varit att i största möjliga mån söka och analysera så moderna källor som möjligt. Jag har därför undvikit att nyttja litteratur som publicerats innan år 2000. Detta har medfört att materialet till huvuddelen är hämtat från Internet.

2.3.6 Beroende

Jag har försökt att ta detta i beaktande genom att studera flera olika källor. Jag har även sökt en del primära källor som västerländska analytiker ofta refererar till. Ett sådant exempel är *China Military Science* från april 2000 där det finns ett antal artiklar kring kinesisk uppfattning om informationsoperationer som det ofta refereras till. Som nämnts under *Material* har jag inte hittat dessa i ursprunglig (engelsk) form, vilket medför att det kan bli en spridningseffekt om dessa artiklar tolkats på ett felaktigt sätt.

Jag har därför sökt och studerat flera olika amerikanska källor för att se om de är samstämmiga. Jag har däremot inte studerat andra länders analyser, beroende på att det är USA som Kina jämförs med.

2.3.7 Tendens

Då det gäller myndigheter, teoretiker och skribenter, både i USA och i Kina, kan det bland dem finnas egenintressen att vinkla synpunkter så att det passar deras agenda, som för mig är okänd.

Det är dessutom ett problem att bedöma trovärdigheten hos de icke-officiella aktörerna. För att hantera detta har jag försökt studera deras bakgrund.

Jag har försökt att ta detta i beaktande i min textanalys, bland annat genom att söka efter flera källor samt att använda skribenter som personer, väl förtrogna med IO och CNO, rekommenderat. Ett exempel på en sådan skribent är amerikanen Timothy L. Thomas som Fredrik Konnander, lärare vid FHS, rekommenderat och som han uppfattar som trovärdig.

Timothy Thomas är pensionerad överstelöjtnant i USA:s armé. Han arbetar nu vid *Foreign Military Studies Office*, Fort Leavenworth, Kansas och har skrivit ett flertal artiklar om informationsoperationer.

Foreign Military Studies Office (FMSO) är ett forsknings och analys-center under *U.S. Army's Training and Doctrine Command* (TRADOC). FMSO studerar framtida och asymmetriska hot samt den säkerhetspolitiska utvecklingen i en rad regioner.

2.3.8 Kontext

Då metoden i denna uppsats bygger på textanalys har jag haft de ovanstående kriterierna i åtanke i granskningen av materialet.

Jag har dock inte funnit material som kraftigt avviker från den allmänna bilden.

2.3.9 Sammanfattning

Materialet för denna uppsats har inneburit en rad utmaningar vad gäller att ta ställning kring källkritik. Detta har framförallt gällt vilket material som ska nyttjas för att få en så rättvis bild som möjligt av främst kinesisk krigföringsförmåga till informationsoperationer och CNO.

Trots detta anser jag, med ovanstående resonemang i beaktande, att jag har haft tillräckligt med material för att kunna svara på mina frågeställningar på ett för denna uppsats trovärdigt sätt. Men problemen som redovisats måste tas i beaktande när resultatet av uppsatsen nyttjas.

3. TEORIER KRING KRIGFÖRINGSFÖRMÅGA

I denna uppsats skall jag studera Kinas och USA:s krigföringsförmåga. Vad är då krigföringsförmåga?

Militärstrategisk doktrin menar att krigföringsförmågan kan beskrivas som ett tempel där taket – krigföringsförmågan, bärs upp av tre pelare – faktorer. Dessa pelare är de fysiska, konceptuella och moraliska faktorerna. Jag kommer hädanefter att benämna detta som *Pelarmodellen*. I doktrinen menas dessutom att krigföringsförmågan är avgörande för att Försvarsmakten skall kunna lösa sina uppgifter.[4]

Major Gustaf Dufberg har i sin c- uppsats *Krigföringsförmåga* definierat det som:

> *"… en parts förmåga att utöva organiserat våld samt förmåga att motstå annan parts organiserade våld för att uppnå mål."*[5]

Ur detta kan man läsa att krigföringsförmåga inte är ett mål i sig, utan ett medel för att nå ett mål.

Ur *Militärstrategisk doktrin*[6]

Dufberg menar i sin uppsats att ett åskådliggörande av pelarmodellen på detta sätt kan ses som en bildlig metafor. Krigföringsförmågan byggs och hålls uppe av pelarna men man kan genom att påverka en eller flera pelare få hela taket – förmågan –att kollapsa.[7] I *Doktrin för gemensamma operationer* hävdas att pelarmodellen med fördel kan användas som analysmodell för att studera sin

[4] Försvarsmakten, (2002), *Militärstrategisk doktrin*, Stockholm, Försvarsmakten, M7740-774002, s.75.
[5] Dufberg, Gustaf, (2005), *Krigföringsförmåga*, Stockholm, Försvarshögskolan, C- uppsats, s.8.
[6] Försvarsmakten, (2002), *Militärstrategisk doktrin*, s.75.
[7] Dufberg, Gustav, (2005), *Krigföringsförmåga*, s.9.

egen och motståndarens tyngdpunkt, avgörande punkter och kritiska sårbarheter.[8]

3.1 Fysiska faktorer

Doktrin för gemensamma operationer menar att de fysiska faktorerna omfattas av stridskrafterna, personalen samt övriga reella resurser för att kunna genomföra en militär operation.[9]

Gustaf Dufberg utvecklar detta vidare och jämställer stridskrafter med krigsförband bestående av personal, förnödenheter och anläggningar. Han pekar på att många komponenter kan, beroende på hur man ser på det, placeras i flera pelare. Ett exempel är personal, där han menar att:

> *”Om man bara ser personalen som ”tomma” människor hör de otvetydigt och uteslutande hemma i den fysiska pelaren men om man genomfört utbildning och träning av personalen utifrån valda doktriner var hör de hemma då? Om personalen är bärare av såväl konceptuella idéer som viljan, kan man i så fall placera dem i bara en pelare?”*[10]

Han placerar dock personalen i den fysiska pelaren då det kan ses som en ändlig resurs. Dufberg menar att alla ting som krävs för att uppsätta och vidmakthålla stridskrafter och personal hör hemma i den fysiska pelaren då det kan ses som en investering i krigföringsförmågan. Ett exempel på det är utbildning och träning av personalen.

Slutligen skriver han att:

> *”Förutom att viljan att använda delar av statens samlade resurser för krigsförberedelser kan variera, så sätter statens samlade resurser i någon mån en gräns för vilken krigföringsförmåga en stat kan utveckla.”*[11]

Utifrån detta resonemang kring de fysiska faktorerna, kommer jag för att belysa dem, studera följande:

- Förband med personal och utrustning
- Kinas och USA:s stödresurser till sina väpnade styrkor
- Utbildning i IO och övningar

3.2 Konceptuella faktorer

Policy och styrdokument på olika ledningsnivåer, exempelvis doktrindokument, är exempel på vad konceptuella faktorer består av enligt Försvarsmaktens doktriner. De konceptuella faktorerna beskriver föreställningar och kunskaper kring hur en stat planerar att nyttja sina militära maktmedel.[12]

Dufberg skriver i sin uppsats att:

> *”Doktrinen i sig ger inte fler flygplan, ubåtar eller soldater men doktrinen ger vägledning för hur stridskrafterna skall användas så att maximal effekt*

[8] Försvarsmakten, (2005), *Doktrin för gemensamma operationer*, s.59.
[9] Försvarsmakten, (2005), *Doktrin för gemensamma operationer*, s.59.
[10] Dufberg, Gustav, (2005), *Krigföringsförmåga*, s.9.
[11] Dufberg, Gustav, (2005), *Krigföringsförmåga*, s.10.
[12] Försvarsmakten, (2005), *Doktrin för gemensamma operationer*, Stockholm, Försvarsmakten, M7740- 774003, s.59.

kan uppbringas ur befintliga förband och dess materiel, alltså den fysiska pelaren."[13]

Doktriner och andra styrdokument kan alltså ge en vägledning om hur stater ser på att nyttja och utveckla sina resurser. Jag kommer därför för att belysa de konceptuella faktorerna genom att studera följande:

- Kinas och USA:s doktriner kring IO och CNO
- Definitioner av begrepp inom IO och CNO
- Andra styrdokument och analyser av strategier som kan belysa föreställningar och kunskaper inom IO och CNO

3.3 Moraliska faktorer

"…de moraliska faktorerna består av det ledarskap, de värdegrunder och den moral som präglar en försvarsmakt och dess ledning."[14]

Detta är vad som karakteriserar de moraliska faktorerna enligt den svenska doktrinen. I pelaren i sig står dessutom *Vilja* som en faktor och doktrinen talar om att krigföringsförmågan beror på resurser i form av stridskrafter samt viljan att använda dem när så behövs.

Gustaf Dufberg menar att benämningen *Moraliska faktorer* är ett språkligt misstag och att den rätta benämningen borde vara *Moralfaktorer*.[15] Jag kommer i denna uppsats dock att fortsätta benämna dem enligt vad som står i doktrinerna.

Han utvecklar vad de moraliska faktorerna består av och menar att det krävs ett övervägande att besluta om att använda sina stridskrafter, där vinster vägs mot risker. De beslut man fattar beror på vilken situationsuppfattning man har, som i sin tur beror på flera faktorer. Exempel som Dufberg ger på sådana faktorer är egna erfarenheter, kultur, självbild samt förtroende för eget koncept och egen materiel. Han menar att *"En övertygelse (eller indoktrinering) att man slåss för den goda saken … ökar troligtvis riskvilligheten…"*.[16]

I denna uppsats kommer jag för att belysa de moraliska faktorerna av IO och CNO att studera:

- Om Kina och USA har använt CNO
- Om de ser några hinder och moraliska problem med förmågorna

4. KINA OCH FÖRMÅGAN TILL IO & CNO

"To achive victory we must as far as possible make the enemy blind and deaf by sealing his eyes and ears, and drive his commanders to distraction by creating confusion in their minds"

Mao Tse-tung

---

[13] Dufberg, Gustav, (2005), *Krigföringsförmåga*, s.10.
[14] Försvarsmakten, (2005), *Doktrin för gemensamma operationer*, s.59.
[15] Dufberg, Gustav, (2005), *Krigföringsförmåga*, s.3-4.
[16] Dufberg, Gustav, (2005), *Krigföringsförmåga*, s.11.

4.1 De fysiska faktorerna

Som nämns i teorikapitlet kan en analys av de fysiska faktorerna göras inte bara utifrån stridskrafterna, utan även utifrån en rad kringfaktorer såsom utrustning och utbildningsnivå. Jag kommer inledningsvis att belysa stridskrafterna för att därefter beskriva Kinas IT- industri, deras infrastruktur och slutligen deras utbildnings- och övningsnivå.

4.1.1 Stridskrafterna

Kinas försvarsmakt består av tre huvudbeståndsdelar.

- Kinesiska Folkets Befrielsearmé, hädanefter benämnt People's Liberation Army (PLA). PLA är i sin tur uppdelat i armén, marinen, flygvapnet och de strategiska robotstyrkorna[17].
- Kinesiska Folkets Beväpnade Polis, hädanefter People's Armed Police (PAP).
- Folkets Milis

PLA består av aktiva styrkor och reservstyrkor och har ansvaret för att försvara Kina mot externa hot. Milisen och PAP karaktäriseras som paramilitära förband där milisen, precis som PLA, har nationellt försvar som sin förstahandsuppgift allt medan PAP har inrikessäkerhet som sitt ansvarsområde.

PLA: s numerär varierar lite beroende på källa. Kina hävdar att de har 2.3 miljoner man och specificerar inte hur de är fördelade mellan försvarsgrenarna.[18] Denna siffra bekräftas i stort av The International Institute for Strategic Studies, IISS, som hävdar att PLA består av ungefär 2 255 000 man, uppdelat på 1.6 miljoner i armén, 255 000 i marinen, minst 100 000 man i robotstyrkorna och 400 000 i flygvapnet. Till detta kommer reserven på totalt cirka 800 000 man och de paramilitära styrkorna på ungefär 3 969 000. [19]

De styrkor som har IO och CNO som huvuduppgift är svåra att lokalisera då den kinesiska informationen kring dessa är restriktiv. Men i *The Chinese Army Today* nämns att det i var och en av de sju militärregionerna, finns "indipendent units" med förband för elektronisk och psykologisk krigföring.[20] Numerären på dessa förband går inte att fastställa, men IISS nämner att det i armén beräknas finnas 50 regementen med ledning och kommunikation som uppgift.[21]

Till detta kommer dessutom milisen. Milisen har sedan Mao Tse-tungs tid utgjort en hörnsten i folkförsvaret av Kina och defineras som en "*armed*

---

[17] Den kinesiska översättningen till engelska på denna del av PLA är *Second Artillery Force.* De har till uppgift att verka avskräckande mot kärnvapenanfall, att genomföra motanfall med kärnvapen samt att genomföra precisionsanfall med konventionella robotar.

[18] Federation of American Scientist (FAS): http://www.fas.org/nuke/guide/china/doctrine/natdef2004.html *White Paper on China's National Defense in 2004*. (2006-09-26), s.7. (Hädanefter White Paper on China's National Defense in 2004).

[19] The International Institute for Strategic Studies, (2005), *The Military Balance 2005-2006*, London, The International Institute for Strategic Studies, s.270. (Hädanefter IISS *Military Balance 2005-2006)*.

[20] Blasko, Dennis J., (2005), *The Chinese Army Today- Tradition and transformation for the 21st century*, s.32-44. (Hädanefter Blasko, Dennis J., *The Chinese Army Today*)

[21] IISS, *Military Balance 2005-2006*, s.271.

organization composed of the masses not released from their regular work".[22] Milisen består av två kategorier - *primary* och *ordinary,* där Kina uppger att storleken på den primära milisen är 10 miljoner man. Storleken på den ordinära milisen anges inte. Uppgiften för milisen är att assistera och förstärka PLA med exempelvis transportkapacitet och reparation av infrastruktur.

Milisen är också intressant ur ett IO och CNO perspektiv då de har fått en stor betydelse inom informationskrigföringen. De kan ses som en högteknologisk koppling till Maos gamla strategier kring "Folkets krig". I *White Paper on China* nämns att kvaliteten på milisen har ökat på bekostnad av kvantiteten de senaste åren och att specialiserade enheter inom bland annat informationssystem har prioriterats.[23] Milisen har för att möta de nya kraven, skapat förband med anställda och utrustning från universiteten, forskningsinstitut och telekomföretag, för att ge stöd till PLA i informationskrigföring.[24]

Ytterligare bevis på milisens roll i informationsoperationer, är kinesiska teoretiker som menar att vem som helst som äger en dator, från tonåringar till soldater, kan delta i försvaret av landet. De rekommenderar att sammansatta förband bör skapas av forskare, poliser, soldater och andra som är bevandrade i informationskrigföring.[25]

Målsättningen för dessa förband är dessutom att de, vad gäller informationsoperationer, skall integreras med PLA och genomföra gemensamma operationer med dem. USA:s försvarsdepartement skriver i en rapport:

> *"The PLA is … integrating militia and reserve units into regular military operations. This units reportedly participate with regular forces in traning and exercises."*[26]

Numerären på milisstyrkor som har informationskrigföring som uppgift har inte gått att få fram, men IISS anger att i de paramilitära styrkorna finns över 69 000 som har *Comms* som uppgift.[27] Detta är inte en orimlig siffra. Svenska Dagbladet skriver i artikeln *Internet både hotar och stöder Kinas regim,* att utländska bedömare menar att mellan 30 000 – 100 000 personer arbetar med att kontrollera Internet i Kina. Myndigheter i Kina hävdar att enbart ett dussintal personer arbetar med att övervaka Internet. Syftet är att förhindra och försvåra att regimkritisk materiel publiceras.[28] Detta kan i sig ses som en inrikespolitisk resurs men också som en potentiell resurs för CNO.

I artikeln *Over 500 information professionals enrolled into militia organization,* maj 2005, skriver *PLA Daily Online* att åtta stycken med doktorsexamen samt 16 stycken på magisterexamen från ett forskningsinstitut i

---

[22] White Paper on China's National Defense in 2004, s.25.
[23] White Paper on China's National Defense in 2004, s.25.
[24] Office of the Secretary of Defence, (2005), *Annual report to congress- Military Power of the People's Republic of China*, s. 35. (Hädanefter DoD, *Military Power of China*.)
[25] Thomas, Timothy L., (2000), *Like Adding Wings to the Tiger: Chinese Information War Theory and Practice*, Nedladdad från: http://www.iwar.org.uk/iwar/resources/china/iw/chinaiw.htm (2006-09-27), s.3. (Hädanefter Thomas, Timothy L., (2000), *Like Adding Wings to the Tiger)*
[26] DoD, *Military Power of China,* s.35.
[27] IISS, *Military Balance 2005-2006*, s.275.
[28] Lundblad, Nicklas, *Internet både hotar och stöder Kinas regim*, Svenska Dagbladet, 2006-10-02.

Sichuan-provinsen har blivit medlemmar i ett informationsförband. Artikeln nämner också att det i milisförbandet nu finns över 500 stycken *"information professionals"*.[29] Det ska poängteras att den organisationsnivå som artikeln beskriver är på en låg nivå. Det vill säga att det är på en lokal nivå dessa har rekryterats och organiserats.[30]

4.1.2 Kinas IT- industri

För att ge en bild av PLA:s potentiella utrustningsnivå kan studier av Kinas IT-industri vara lämplig.

Kina håller snabbt på att utvecklas till en högteknologisk supermakt. Det menar Ernest H. Preeg i artikeln *The Rapid Development of China's Advanced Technology Industry and Its Impact on Military Modernization*.[31] Han menar att Kinas ekonomiska strategi sedan 1995 har varit fokuserad på att utveckla den avancerade teknologiska industrin och att det har gått hand i hand med en fördjupad integrering mellan de civila och militära delarna av industrin. Hur Kinas ledning resonerat kan illustreras med ett uttalande från Kinas tidigare ledare, Deng Xiaoping:

> *"Combine the Military and Civil*
>
> *Combine Peace and War*
>
> *Give Priority to Military Products*
>
> *Let the Civil Support the Military"*

Kina satsar dessutom stora summor på forskning och utveckling, FoU, med en strävan att vara oberoende av utländska företag då det gäller innovationer. FoU ökar i Kina med 20% per år, jämfört med 6% för USA och 5% ökning för EU och Japan. Trots denna satsning, uppgick utgifterna till FoU i Kina år 2005 endast till en tredjedel jämfört med USA och till hälften jämfört med EU. Kina hade dock passerat Japan i detta avseende.

Det som är intressant ur ett IO perspektiv är att de kinesiska FoU-anslagen främst är koncentrerade till två områden. Dels till exportorienterad tillverkning, då främst IT-produkter och telekommunikation, samt till försvarsindustrin. Exempel på nyligen presenterade kinesiska produkter inom IT området är en superdator, Dawning 4000-A, som anses tillhöra topp 15 i världen vad gäller snabbhet, samt dataprocessorn Godson II som kan användas i vanliga datorer. Västliga bedömare anser den dock vara två generationer efter de modernaste chipen från till exempel Intel.[32,33] Ett annat exempel är John Chambers, VD för Cisco, som under ett möte i Peking i september 2004, ska ha sagt att "Kina

---

[29] PLA Daily Online, *Over 500 information professionals enrolled into militia organization*, http://english.pladaily.com.cn/site2/columns/2004-09/07/content_2960.htm (2006-10-10).

[30] För en närmare beskrivning av PLA:s organisation, se Blasko, Dennis J., *The Chinese Army Today*, s. 32-44.

[31] Preeg, Ernest H., (2005), *The Rapid Development of China's Advanced Technology Industry and Its Impact on Military Modernization*, i Hudson Institute, (2005), *China's New Great Leap Forward – High Technology and Military Power in the Next Half-Century*, s.2. (Hädanefter Preeg, Ernest H., (2005), *China's New Great Leap Forward)*

[32] Preeg, Ernest H., (2005), *China's New Great Leap Forward*, s.2-9.

[33] För att se artikel om Dawning 4000-A, se exempelvis: http://news.com.com/Chinese+supercomputer+headed+to+top+ranks/2100-1001_3-5226240.html (2006-10-27). För att se artikel om Godson II, se exempelvis: http://cio.co.nz/cio.nsf/0/F30DED537E6C42B2CC2570500077CD9C?OpenDocument (2006-10-27).

kommer att bli världens IT centrum".[34] När han tror att detta kommer att ske specificerades dock inte.

Intressant är att Preeg anser att utvecklingen inom Kinas högteknologiska civila industri kommer till gagn i den kinesiska försvarsmaktens modernisering och då främst inom missilteknologi, satellitteknologi samt inom "cyberkrigföring". Han anser att utvecklingen inom industrin framför allt har nyttjats för att utveckla militära C4I system (Command, Control, Communications, Computers, Intelligence).[35]

Man ska hålla i minnet att Kinas satsningar på FoU och expansion av försvarsmakten troligtvis är, som för alla stater, beroende på landets totala ekonomiska utveckling och att Kina det senaste decenniet haft en stark sådan. Vidare att även USA satsar stora resurser inom dessa områden för att bibehålla det försprång man har. Men, som Preeg lite cyniskt konstaterar, satsar företag i USA i dag mer på skadeståndsrättegångar än på forskning och utveckling.[36]

4.1.3 Kinas infrastruktur

För att distribuera information har PLA byggt ett fiberoptiskt nätverk som omfattar hundratals mil med fiberkabel och som med moderna routrar och switchar kopplar ihop förband och staber.[37]

Kina beskriver det själva på följande sätt:

> *"In the past two decades, … [PLA] has completed a series of key projects to build military information systems and made great progress in building information infrastructure. As a result, command means have been substantially improved at all levels of headquarters and combat troops. Computers and other IT equipment have been gradually introduced into routine operations."*[38]

Ett problem i detta som PLA har identifierat, är att deras hårdvara ofta härstammar från utländska tillverkare, något som de är misstänksamma emot. Det finns därför rekommendationer att komponenter till PLA: s nätverk ska genomgå omfattande tester. Bedömare drar därför slutsatsen att till känsliga delar av nätverken används främst inhemska produkter. [39] Med beskrivningen ovan av den expanderande kinesiska IT- industrin, bör detta kunna tillmötesgås.

4.1.4 Kinesisk utbildning och övningar

Även i form av antalet utexaminerade studenter från universitet och högskolor har det skett en snabb utveckling i Kina. Under de tio senaste åren har antalet utexaminerade studenter ökat från en miljon till tre miljoner per år, vilket är jämförbart med USA. Kinesiska studenter är dock i högre grad inriktade mot matematik-, forsknings- och ingenjörsutbildningar. Ser man till dessa områden examineras det sex till åtta gånger fler studenter i Kina än USA. Vad gäller högre ingenjörsutbildningar har Kina dubbelt så många doktorander per år

---

[34] Preeg, Ernest H., (2005), *China's New Great Leap Forward*, s.29.
[35] Preeg, Ernest H., (2005), *China's New Great Leap Forward*, s.16 samt 29-30.
[36] Preeg, Ernest H., (2005), *China's New Great Leap Forward*, s.33.
[37] Preeg, Ernest H., (2005), *China's New Great Leap Forward*, s.16.
[38] White Paper on China's National Defense in 2004, s.8-9.
[39] Bi, Jianxiang, *Joint Operations: Developing a New Paradigm*, i Mulvenon, James och Finkelstein, David M. (edit.), (2005), *China's Revolution in Doctrinal Affairs: Emerging Trends in the Operational Art of the Chinese People's Liberation Army*, s.56-57.

jämfört med USA och då är inte de tiotusentals kinesiska studenter som studerar på skolor utanför Kina medräknade, av vilka många återvänder till Kina efter examen.[40]

Hur många av dessa studenter som arbetar inom försvarsindustrin eller i civila företag med koppling till det militära går inte att säga. Man kan ändå anta att en hel del av dem på ett eller annat sätt kommer att arbeta inom områden som har militära intressen. Detta med tanke på integreringen mellan civil och militär industri samt nyttjandet av civila företag som en del av milisen vilket tidigare beskrivits.

Då det gäller militära skolor med IO/IW inriktning inom PLA, menar Timothy Thomas att det finns ett antal. Han identifierar fem stycken i artikeln *Adding wings to a tiger: Chinese information war theory and practice*, där högskolan i Wuhan i Hubei provinsen, anses vara den främsta.

I artikeln beskriver han dessutom hur kinesiska officerare utbildas i IW och att de beroende på ålder får olika typer av utbildning. Orsaken till denna differentiering ska enligt honom vara att PLA anser att de äldre inte har den grundkunskap inom IT som krävs. Thomas hävdar att de över 40 år är beslutsfattare som får utbildning vilket syftar till att minska deras ”*information illiteracy*” och att de ges en grundläggande förståelse för IW.

De mellan 30-40 anses vara de framtida ledarna och ges en mer omfattande utbildning där deras eventuella brister i IT- kunskap åtgärdas. Vidare ges de en mer ingående utbildning i vad IW innebär och hur de ska utnyttja teorierna kring det. De under 30 år ges en lång och avancerad IW utbildning. De anses vara väl införstådda i vad informationssamhället innebär så deras utbildning är fokuserad på både ledning och teknologi.[41] Det framgår inte av Thomas artikel om alla inom PLA ges denna utbildning eller hur många som utbildas per år.

Då det gäller övningar med IO och CNO profil beskrivs i *PLA Daily Online* i april 2004, en övning i Pekings militärdistrikt där flyg och markförband övade i syftet att testa förbandens ”*…the IT fighting capacity of its signal communication troops*.”[42] I artikeln beskrivs hur tidigare övningar med dessa styrkor enbart var teoretiska men att de vid detta tillfälle kunde öva fullt ut tack vare ny simuleringsutrustning som tagits fram i samverkan med kinesiska forskningsinstitut. Reportern beskriver hur:

> *“The "Red Army" launched several waves of attack by adopting different offensive tactics. "Electromagnetic killers" directed precision strikes at its adversary's (the "Blue Army") "soft" and "hard" targets, as a result, its adversary's communication systems were soon paralyzed. During the exercise, the commanders of both sides used their new equipment skillfully on the complex and volatile electromagnetic battlefield, and they were able to acquire, analyze and transmit in a real time manner.”*

Thomas hävdar att PLA:s första övning i IW, var i oktober 1997 där en armégrupp utsattes för CNA och där armégruppen kunde besvara attacken med egen CNA.[43]

---

[40] Preeg, Ernest H., (2005), *China’s New Great Leap Forward*, s.3-4.
[41] Thomas, Timothy L., (2000), *Like Adding Wings to the Tigers*, s.12-16.
[42] PLA Daily Online, *Group army improves its IT fighting power*: http://english.pladaily.com.cn/site2/columns/2004-09/12/content_11968.htm (2006-10-28)
[43] Thomas, Timothy L., (2000), *Like Adding Wings to the Tiger*, s.19-21.

Efter detta har PLA genomfört regelbundna övningar där ovan citerad övning kan ses som ett exempel. Även milisen har medverkat i övningar som beskrivs i kapitel 4.1.1. Exempelvis genomfördes i juni år 2000, en övning i Hubei provinsen där enheter från milisen och reserven övades.[44] Noterbart är att detta skedde i samma provins som där den ledande skolan för informationsoperationer inom PLA ligger.

4.2 De konceptuella faktorerna

Vilka föreställningar kring IO och CNO har då Kina? Hur ska Kina använda sina styrkor? Här kommer jag först att belysa hur Kina ser på den militära faktorn för att därefter studera vilka definitioner de har inom detta område. Slutligen ska jag i de konceptuella faktorerna studera Kinas strategier kring IO och CNO.

4.2.1 Doktrinen och definitioner

Som nämns under avsnittet *Material & Källkritik,* är *China's National Defense in 2004* det närmaste som kan kallas en kinesisk doktrin och som är översatt till engelska. Jag kommer i huvudsak använda det svenska ordet *vitbok* då jag refererar till *China's National Defense in 2004*.

Dokumentet inleds med *The Security Situation* som ger en översiktlig beskrivning på hur Kina ser på omvärlden. Hur de ser på den militära faktorn citeras i följande stycke:

> *"The military factor plays a greater role in international configuration and national security. Worldwide Revolution in Military Affairs (RMA) is gaining momentum. The forms of war are undergoing changes from mechanization to informationalization. Informationalization has become the key factor in enhancing the warfighting capability of the armed forces. Confrontation between systems has become the principal feature of confrontation on the battlefield. Asymmetrical, non-contiguous and non-linear operations have become important patterns of operations. The world's major countries are making readjustments in their security and military strategies and stepping up transformation of their armed forces by way of developing high-tech weaponry and military equipment and putting forth new military doctrines. As a result, the generation gap in military technology between informationalization on the one hand and mechanization and semi-mechanization on the other is still widening, and military imbalance worldwide has further increased. The role played by military power in safeguarding national security is assuming greater prominence."*[45]

Värt att notera i denna text är ordet *informationalization* och vilken vikt Kina lägger på det. I texten ovan framgår att kineserna anser att formerna för krig går från *"mechanization to informationalization"* och att detta har blivit en nyckelfaktor för att förstärka krigföringsförmågan. Men i den kinesiska doktrinen specificeras inte vad de menar med det ordet.

En sökning på *informationalization* i lexikon för att översätta det till svenska, eller i engelska referenslexikon ger inga träffar.[46] Om man däremot söker på

---

[44] Thomas, Timothy L., (2000), *Like Adding Wings to the Tiger*, s.4-5.
[45] White Paper on China's National Defense in 2004, s.2.
[46] Jag har använt det på FHS datorer installerade översättarprogrammet *WordFinder 4*, på Oxford Reference Online http://www.oxfordreference.com/views/GLOBAL.html samt uppslagsverken Wikipedia http://en.wikipedia.org/wiki/Main_Page och via Anna Lindh bibliotekets nätverk på Encyclopaedia Britannica http://search.eb.com/ med sökordet *"Informationalization"* (2006-10-16).

Google med sökorden *"Informationalization + Dictionary"* så menar referenslexikonet *Doubletongued Wordwrester Dictionary* att det betyder datorisering av affärsvärlden, industrin och militären och att det är ett uttryck som mest används i Sydostasien.[47]

William Moss, PR konsult inom teknik och bosatt i Peking, menar att begreppet är ett exempel på smidigheten och elegansen i det kinesiska språket och problemen som ibland finns med att översätta kinesiska till engelska. Han menar att det är en direkt översättning av det kinesiska ordet *xinxihua*, där xinxi betyder *information* och hua betyder *förändring* eller *transformation*. Hua i kinesiskan är också en ofta använd ändelse för att böja ord och översätts då till de engelska suffixen –ize eller – ization.[48]

Jag kommer hädanefter i uppsatsen att översätta *informationalization* med *informationalisering.*

I en artikel från *International Assessment and Strategy Center* i mars 2005 beskrivs begreppet lite närmare. De menar att informationalisering är PLA: s förmåga att:

> *"…to use the latest technologies in command, intelligence, training and weapon systems. New automatic command systems linked by fiber-optic Internet, satellite and new high-frequency digital radio systems, allow for more efficient joint-service planning and command, while also enabling a reduction in layers of command. The PLA can also better contest the information battlespace with its new space-based, airborne, naval and ground based surveillance and intelligence gathering systems, and its new anti-satellite, anti-radar, electronic warfare and information warfare systems."*[49]

Detta fokus på informationalisering återkommer på flera ställen i den kinesiska doktrinen. Inledningen på det tredje kapitlet *Revolution in Military Affairs with Chinese Characteristics* lyder:

> *"The PLA, aiming at building an informationalized force and winning an informationalized war, deepens its reform, dedicates itself to innovation, improves its quality and actively pushes forward the RMA with Chinese characteristics with informationalization at the core."*[50]

Men vad består då detta av enligt kineserna? I en notis i *PLA Daily Online* i mars 2004, menas att arméns informationalisering består av sex nyckelfaktorer:

- IT applikationer ska utgöra drivkraften för arméns modernisering och utgöra grunden för utvecklingen.
- Informationsresurser *("information resource")* för militära ändamål är kärnan för arméns datorisering och för att man ska få praktisk nytta av denna utveckling.
- Informationsnätverk för militära ändamål är grunden för att kunna hantera informationsresurserna och de olika IT applikationerna. De är

[47] Doubletongued Wordwrester Dictionary http://www.doubletongued.org/index.php/dictionary/informationalization/ (2006-10-16).
[48] Moss, William, (2006), *The curse of informatization*, CNet Asia Blogs, http://asia.cnet.com/reviews/blog/littleredblog/0,39056119,61953570,00.htm (2006-10-20).
[49] International Assessment and Strategy Center, *Top Ten Military Modernization Development*, http://www.strategycenter.net/printVersion/print_pub.asp?pubID=65 (2006-10-18).
[50] White Paper on China's National Defense in 2004, s.6.

en nödvändighet för att kunna hantera information och utan dem blir de andra faktorerna meningslösa.

- Begreppet *informationized weaponry* refererar till vapen och vapensystem som är baserade på modern informationsteknologi. Dessa har en förmåga att förstöra och paralysera fiendens information och informationssystem.
- De mänskliga resurserna avgör kvaliteten och hastigheten på utvecklingen av datoriseringen.
- Policys, bestämmelser och standarder är viktiga komponenter i utvecklingen för att koordinera olika delar och en förutsättning för en snabb och hälsosam utveckling av arméns datorisering.[51]

Ett tecken på målsättningen Kina har med den modernisering och datorisering som de påbörjat, är att de behöver stärka förmågan att vinna *"local wars under informationalized conditions"*. Vidare skall PLA, för att öka denna förmåga, intensifiera forskningen inom en rad högteknologiska områden såsom precisionsvapen, elektronisk krigföring och informationsoperationer.[52]

Men i vitboken står inget direkt om informationsoperationer och än mindre om CNO. Att Kina anser att informationsarenan är betydelsefull framgår dock av andra dokument. I *PLA Daily Online* i december 2003 finns en kort artikel med namnet *Attention should be given to the information territory.* I den artikeln definieras följande:

> *"The information territory of a state refers to the virtual space and its physical carrier existing in the electronic equipment used by the infrastructure system, government and non-governmental institutions and even individuals. It is of vital importance to the national security. The information territory not only refers to the Internet in common sense, but also to key information network systems such as finance, electric power, telecommunications, transportation, energy, military and statistics."*[53]

Artikeln fortsätter med att säga att informationsteknologin ger helt nya utvecklingsmöjligheter men också hittills okända (*unprecedented*) hot mot säkerheten. Författarna menar att problem i informationssystemen kan leda till kaos i ekonomin, samhället och i det militära. De fortsätter med att de potentiella hoten mot *"the information territory*" är hackers, kriminella element samt *"the digitalized troops for information warfare in some countries"* och de rekommenderar att staten inrättar ett departement för att skydda informationsarenan. Det skulle i så fall bestå av *"information security troops"* där personal från militären, olika regeringsorgan samt civila experter skulle ingå och med uppgift att förhindra kriminalitet och informationskrigföring.

Men vad är då informationskrigföring enligt Kina? Som jag tidigare har beskrivit har jag inte hittat några officiella kinesiska definitioner på IO och IW.[54] Bland kinesiska tänkare refereras dock till olika definitioner. I Timothy

---

[51] PLA Daily Online, *Keep a firm grip on key factors of informationization*: http://english.pladaily.com.cn/site2/columns/2004-09/11/content_11936.htm (2006-10-17).
[52] White Paper on China's National Defense in 2004, s.9.
[53] PLA Daily Online, *Attention should be given to the information territory*: *http://english.pladaily.com.cn/site2/columns/2004-09/11/content_11935.htm* (2006-10-17).
[54] Vid sökning på Google 2006-10-19 med sökord "informationwarfare + china + definitions + official + pdf" fås ungefär 964.000 träffar. Jag har tittat på de tio första träffarna utan att

L. Thomas artikel *China's Electronic Strategies* återges två definitioner. Dels överste Wang Baocun, tidigare chef för Kinas högskola för militärvetenskap, som i april år 2000 definierar IW som:

> *"a form of combat actions which attacks the information and information systems of the enemy while protecting the information and information systems of one's own side. The contents of IW are military security, military deception, physical attack, electronic warfare, psychological warfare and net warfare, and its basic purpose is to seize and maintain information dominance."*[55]

Hur överste Baocun, eller officiella Kina, definierar begreppet *information dominance*, har jag inte hittat.

I samma artikel ges generalmajor Dai Qingmins syn på informationsoperationer där han definierar dem som:

> *"a series of operations with an information environment as the basic battlefield condition, with military information and an information system as the direct operational target, and with electronic warfare and a computer network war as the principal form."*[56]

Generalmajor Dai är intressant då han för tiden för artikeln var chef för PLA: s avdelning för IW och IO och därför kan anses ha ett stort inflytande på den kinesiska synen.[57] Noterbart är att Dai säger att elektronisk krigföring och *"computer network war"*, CNO, är den huvudsakliga formen för informationsoperationer.

Ytterligare en aspekt kring IO och IW hos Kina, ges av Barret Barrington Jr., chef för "Information - in – Warfare" vid USA:s Stilla Havs-kommando. I artikeln *Information Warfare: China's Response to U.S Technological Advantages*, menar han att då kineser skriver IW menar de inte *Information Warfare* utan *Information War*. Han refererar till den kinesiska generalen Wang Pufeng som sammanfattat skillnaderna på detta vis:

> *"…information war refers to a kind of war and a kind of war pattern, while information warfare refers to a kind of operation and operational pattern."*[58]

Han menar att kineserna ser på IW som en ständigt pågående kamp, såväl i fred, kris och krig och att denna kamp förs på flera plan och i varierande grad.

Detta är en synvinkel som ytterligare komplicerar bilden av kinesisk syn på IO och IW då västerlänningar ska analysera Kina och som man kan ha med sig. För denna uppsats kommer dock IW och IO även i fortsättningen stå för informationskrigföring och informationsoperationer. En fördjupning av vad Kina menar då de använder de olika begreppen överlämnas till fortsatt forskning.

---

kunna urskilja en officiell kinesisk definition. Jag har vidare studerat www.fas.org, *White Paper on China* samt DoD, *Military Power of China* med samma resultat.

[55] Thomas, Timothy L., (2001), *China's Electronic Strategies*, Fort Leavenworth, Foreign Military Studies Office, s.3 nedladdad via http://leav-www.army.mil/fmso/documents/china_electric/china_electric.htm (2006-10-19), s.3. (Hädanefter Thomas, Timothy L., (2001), *China's Electronic Strategies).*

[56] Thomas, Timothy L., (2001), *China's Electronic Strategies*, s.4.

[57] Thomas, Timothy L., (2001), *China's Electronic Strategies*, s.1.

[58] Barrington, Barrett M. jr., (2005), *Information Warfare: China's Response to U.S. Technological Advantages*, i International Journal of Intelligence and Counterintelligence, Volume 18, Number 4, Routledge, Taylor & Francis Group. Nedladdad från FHS nätverk på http://www.ingentaconnect.com/content/routledg/ujic/2005/00000018/00000004/art00006 (2006-10-23).

Finns det då några definitioner på Computer Network Operations, CNO? Precis som för IO och IW har jag inte hittat några officiella kinesiska definitioner översatta till engelska.[59] Enligt USA:s försvarsdepartement saknas bevis för att det finns en formell kinesisk doktrin inom CNO. Enligt dem består Kinas CNO av CNA, CND samt CNE.[60]

Det närmaste jag kommit en definition på CNO från en kinesisk teoretiker är från tidigare nämnd generalmajor Dai, som menar att kärnan i *computer network warfare* är att ”störa och förstöra de olika lager som information bearbetas i med syftet att ta och behålla kontrollen i nätverken”.[61] De lager som Dai syftar på antar jag är lagren i OSI och TCP/IP modellerna som används för att beskriva arkitekturen för datakommunikation i nätverk.

4.2.2 Kinas syn på att använda förmågorna

Men om det saknas kinesiska definitioner kring informationsoperationer och CNO finns det då några officiella doktriner kring hur de ser på *användandet* av dessa förmågor?

Tyvärr har jag även i detta avseende inte hittat några dokument och frånvaron av sådana bekräftas av USA:s försvarsdepartement.[62] Men det finns desto fler kinesiska och amerikanska tänkare som skriver kring hur de ser på strategier inom dessa förmågor.

Generalmajor Dai Qingmin skrev i april 2000 en artikel kallad ”*Innovating and Developing Views on Information Operations*” i *China Military Science* vilken Timothy Thomas refererar till i en analys av Kinas elektroniska strategier. Generalmajor Dais syn på informationsoperationer anser jag, bygger på fem delar.[63] De är:

- Betydelsen av **strategier**
- Betydelsen av **informationsöverlägsenhet**
- Vikten av att vara **offensiv** i IO
- Användningen av **krigslister**
- **Integrering** av civila och militära resurser

Då det gäller betydelsen av **strategier** är Thomas slutsats att kineserna anser att överlägsna strategier kan hjälpa till att övervinna tekniska tillkortakommanden och han återger vad Dai har skrivit, nämligen att en bra strategi kan:

> *“serve as a type of invisible fighting capacity; may make up inadequate material conditions to a certain extent; may narrow a technological or equipment gap between an army and its enemy; and may make up for a*

[59] Vid sökning på Google 2006-10-19 med sökord ”CNO + china + definitions + official + pdf” fås ungefär 964.000 träffar. Jag har tittat på de tio första träffarna utan att kunna urskilja en officiell kinesisk definition. Jag har vidare studerat www.fas.org, *White Paper on China* samt DoD, *Military Power of China* med samma resultat.
[60] DoD, *Military Power of China*, s.36.
[61] Thomas, Timothy L., (2005), *Chinese and American Network Warfare*, Joint Forces Quarterly, s. 77, nedladdad från: http://www.dtic.mil/doctrine/jel/jfq_pubs/1538.pdf (2006-10-23).
[62] White Paper on China’s National Defense in 2004, s.36.
[63] Thomas, Timothy L., (2001), *China’s Electronic Strategies*, s.4-7.

shortage of information, fighting forces or poor information operational means.”[64]

Dai menar att en del av dessa strategier innebär att:

- Störa och sabotera fiendens information och informationssystem.
- Sabotera fiendens övergripande operativa informationsstruktur.
- Försvaga fiendens förmåga till informationskrigföring.
- Sprida fiendens styrkor, vapen och eldkraft medan egna resurser koncentreras.
- Förvirra eller avleda fienden och själv skapa överlägsna förutsättningar för strid.
- Avleda fiendens försök till underrättelseinhämtning medan du gör tillräckliga egna förberedelser.
- Ge fienden ett falskt intryck och genomför samtidigt en överraskande informationsattack.
- Förblinda eller döva en fiende med falska intryck.
- Förvirra fienden eller störa hans tänkande.
- Få fienden att tro att det som är sant är falskt och det som är falskt är sant.
- Förmå fienden till att göra felaktiga bedömanden eller felaktiga ageranden.[65]

För att dessa strategier ska kunna nyttjas krävs **informationsöverlägsenhet** enligt Dai. För att uppnå detta fordras flera faktorer.

”Professionella styrkor” ska störa och sabotera fiendens information och informationssystem. Samtidigt ska ”icke – professionella” styrkor skydda egna viktiga resurser och skada motståndarens krigföringsförmåga.

Vidare är det viktigt att integrera förmågor till elektronisk- och nätverkskrigföring med varandra.

För det tredje ska hårda och mjuka (”*soft and hard*”) metoder nyttjas. Av materialet framgår att det Dai menar med mjuka och hårda metoder är elektronisk- och nätverkskrigföring å ena sidan, samt fysisk bekämpning å andra sidan.

Slutligen ska operationer genomföras med ett gemensamt, ”joint”, perspektiv med såväl mark-, sjö-, flyg- som rymdstyrkor. Någon närmare definition av vad Dai menar med informationsöverlägsenhet ges inte i artikeln.

Ett resonemang som Dai för, enligt ovan, är att för att lyckas med att nå denna informationsöverlägsenhet krävs det att se på IO som en ”*active offensive*” – en **aktiv offensiv**. Detta är något som inte framkommer i officiella kinesiska dokument, tvärtom. I vitboken nämns att Kina har säkerhetspolitik som är orubbligt defensiv i sin natur.[66] För att vara i harmoni med den officiella linjen

[64] Thomas, Timothy L., (2001), *China’s Electronic Strategies*, s.4.
[65] Thomas, Timothy L., (2001), *China’s Electronic Strategies*, s. 5. Egen översättning.
[66] White Paper on China’s National Defense in 2004, s. 4.

menar dock Dai att det är en defensiv attityd han avser, men för att den ska kunna vara ”positiv” krävs det att man har en ”aktiv offensiv defensiv”.[67]

Detta synsätt återfinns även i PLA Daily i en artikel benämnd *The key to sucess in informationzed war is to take offensive action.* Där hävdas att det är svårt att nå ett överläge i ett informationskrig om man är defensiv och inte genomför attacker. Bara genom att kombinera attacker med försvar, där offensiva operationer är det viktiga, kan informationsöverlägsenhet nås. Vidare menar de att ju mer omfattande en ”informationsattack” är, desto större blir manöverutrymmet.[68]

Ytterligare belägg för hur Kina ser på betydelsen av offensiva informationsoperationer ges i *China’s Revolution in Doctrinal Affairs.* Där hävdas att Kina anser att alla nätverk, även de mest avancerade, har sårbarheter som gör att de inte kan försvaras och att så länge nätverken används så kan PLA detektera och identifiera emitterade signaler. Detta gäller även omvänt. Det finns ett hot att de egna nätverken degraderas av en överlägsen motståndare. Detta gör att Kina fäster stor vikt i att slå först och att genomföra förebyggande anfall. Genom att attackera vid rätt tillfälle kan även en överlägsen motståndares, läs USA, överraskas och få sina operationer störda och detta till en relativt låg kostnad i jämförelse med att använda konventionella styrkor.[69]

Ett annat område som Timothy Thomas uppmärksammar och tar upp i sin artikel efter att ha studerat Dais teorier, är användandet av **krigslister**. I artikeln används ordet ”*stratagems”*. Det översätts med *krigslist, fint, knep* i WordFinder. I *Oxford Reference Online* ges det betydelsen ”*a plan or scheme intended to outwit* (överlista – översatt från WordFinder) *an opponent*”.[70] För denna uppsats kommer hädanefter *stratagems* att översättas med krigslister.

Thomas refererar dels till Dai, men också till artikeln *On Information Warfare Strategies* i *China Military Science* i april 2000 (samma nummer som Dai publicerade sina teorier i) skrivet av generalmajor Li, överste Jiangzhou och major Dehui.[71] De definierar i sin artikel krigslister inom IW som:

> *“schemes and methods devised and used by commanders and commanding bodies to seize and maintain information supremacy on the basis of using clever methods to prevail at a relatively small cost in information warfare”*[72]

Författarna till artikeln menar att asiater och västerlänningar ser olika på att kombinera teknisk utveckling och krigslist, där asiater traditionellt framhäver krigslist och västerlänningar teknik. De hävdar att soldater från västvärlden söker tekniska lösningar på de problem som dyker upp medan asiatiska soldater accepterar den teknik de har och istället försöker använda krigslister för att kompensera bristfällig teknik. Exempel på krigslister för IW enligt

---

[67] Thomas, Timothy L., (2001), *China’s Electronic Strategies*, s. 7.
[68] PLA Daily online, *The key to sucess in informationzed war is to take offensive action: http://english.pladaily.com.cn/site2/columns/2004-09/11/content_11934.htm* (2006-10-23).
[69] Bi, Jianxiang, *Joint Operations: Developing a New Paradigm*, i Mulvenon, James och Finkelstein, David M. (edit.), (2005), *China’s Revolution in Doctrinal Affairs: Emerging Trends in the Operational Art of the Chinese People’s Liberation Army*, s. 57-58.
[70] Oxford Reference Online: http://www.oxfordreference.com/views/SEARCH_RESULTS.html?q=stratgems&category=s7&ssid=24396667&scope=subject&time=0.451818378447694 (2006-10-25).
[71] Thomas, Timothy L., (2001), *China’s Electronic Strategies*, s.3-4.
[72] Thomas, Timothy L., (2001), *China’s Electronic Strategies*, s.3.

författarna är att styra beslutsfattares tankar genom att attackera kognition och tilltro till system, att använda virus för att påverka information samt att dölja verkligheten genom att skapa en falsk bild av verkligheten.[73]

Thomas menar i sin tolkning av dessa artiklar att även 300 år gamla kinesiska läror kring krigslister kan användas idag för IO. Ur *The Thirty-Six Stratagems: The Secret Art of War* ger han exempel på hur dessa gamla läror kan tillämpas än idag.[74,75] Ett exempel är den tredje strategin ”*Döda med ett lånat svärd*” där filosofin är att om du inte kan angripa fienden direkt, attackera med en annan styrka istället. Med moderna IO termer skulle metoden vara att med CNA angripa motståndaren.

Ett annat exempel Thomas ger är strategi fyra, ”*Invänta den utmattade fienden i lugn och ro*”. Enligt Thomas skulle det i en informationsoperation kunna innebära att fiendens försvar av sina datanätverk mättas av attacker utförda av den stora massan allt medan specialisterna avvaktar på rätt tillfälle att angripa det som man egentligen är ute efter. Detta tolkar jag som att milisen skulle kunna utgöra den stora massan och enheter ur PLA är de som utför de avgörande attackerna.

Slutligen betonar Dai **integrationen** av civila och militära förmågor som en faktor i informationskrigföringen och han ser på civila resurser som ett värdefullt stöd till PLA i framtida informationskrig. Jag anser att dessa idéer har fått genomslag i och med skapandet av IO/IW förband inom PLA: s reservstyrkor och milisförband.

Efter denna översikt kring kinesiska definitioner, och brist på officiella sådana, samt hur de ser på användandet av sina resurser ska jag nu övergå till att studera de moraliska faktorerna.

4.3 De moraliska faktorerna

I teorikapitlet beskrevs detta som faktorer påverkar moralen och besluten kring att nyttja sina stridskrafter. Besluten fattas utifrån faktorer som värdegrund, tidigare erfarenheter, samt förtroende för eget koncept och materiel.[76]

I vilka situationer är då Kina beredd att nyttja sin förmåga och finns det exempel på användande?

4.3.1 Värdegrund

Viljan att nyttja sina stridskrafter är svår att bedöma. Ett sätt är att studera vilken värdegrund som finns och studera vilka lagliga hinder opponenten ser.

Den kinesiska vitboken diskuterar inte några juridiska aspekter av informationsoperationer och CNO. Dt finns dock ett avsnitt i vitboken sm behandlar lagar, men det är mer kring att PLA strikt följa lagar. Om det innefattar några bestämmelser kring IO och CNO framkommer inte.[77]

---

[73] Egen översättning av ett urval av exempel. För att fler exempel se Thomas, Timothy L., (2001), *China’s Electronic Strategies*, s.4.
[74] Thomas, Timothy L., (2001), *China’s Electronic Strategies*, s.6-7.
[75] För samtliga exempel, se: http://www.chinastrategies.com/List.htm#Strategy%203 (2006-10-25) Där kallas dock boken för *Thirty-six startegies of Ancient China*. På andra hemsidor förkommer dock det Thomas refererar till. Innehållet är dock detsamma i texterna.
[76] Se kapitel 3.3.
[77] White Paper on China’s National Defense in 2004, s. 13 – 14.

Att kinesiska teoretiker resonerar kring legala problem med CNO, har jag inte funnit i materialet för denna uppsats.

4.3.2 Exempel på kinesiskt nyttjande

Ett annat sätt att betrakta de moraliska faktorerna är att se på vilka erfarenheter en stat har i användandet av förmågor, då erfarenheter kan ge underlag för beslutsfattande.

I Washington Posts nätupplaga den 6 oktober 2006, kan man läsa följande:

> *”Hackers operating through Chinese Internet servers have launched a debilitating attack on the computer system of a sensitive Commerce Department bureau, forcing it to replace hundreds of workstations and block employees from regular use of the Internet for more than a month, Commerce officials said yesterday.”*[78]

I artikeln beskrivs hur detta är andra gången under de senaste månaderna där USA har konstaterat att stora nätverksattacker kan spåras till Kina. Konsekvensen för den amerikanska myndigheten blev att de fick svårare att kommunicera med omvärlden beroende på de säkerhetsåtgärder som vidtogs. De var även tvungna att bygga upp ett helt nytt datasystem, köpa in nya datorer med ”ren” hård- och mjukvara vilket beräknades ta ett par månader. Vidare nämns att utrikesdepartementet bekräftat att kinesiska hackers har gjort intrång i deras datorer samt att deras försvarsdepartement och andra myndigheter är under ständiga attacker från oidentifierade kinesiska datorer.

I artikeln nämns inte om USA anser att attackerna kommer från kinesiska myndigheterna eller om det är så kallad ”*Nationalistic hacking*” utförda av hackare med nationalistiska och patriotiska motiv. Om USA ansåg att kinesiska myndigheter låg bakom intrången skulle USA troligtvis kraftigt protestera, men i artikeln framgår inte hur USA agerat. Men jag anser att det skulle i sig vara förvånande om dessa attacker är okända för de kinesiska myndigheterna.

5. USA OCH FÖRMÅGAN TILL IO & CNO

> *”We must fight the net.”*
>
> *USA:s försvarsdepartement*

5.1 De fysiska faktorerna

5.1.1 Stridskrafterna

Den amerikanska försvarsmakten har följande huvudbeståndsdelar:

- US Strategic Command – US STRATCOM
- US Army
- US Air Force
- US Navy
- US Marine Corps
- US Special Operations Command

78 Washington Post, (2006), *Computer System Under Attack*. Nedladdad från: http://www.washingtonpost.com/wp-dyn/content/article/2006/10/05/AR2006100501781.html (2006-10-18).

Numerären i dessa vapenslag är 1 473 960 aktiva, 10 126 civila och 1 290 988 i reserven.[79] Storlek på förband med IO och CNO som uppgift finns inte närmare specificerat av IISS.

Respektive försvarsgren har ett center för att stödja sina befälhavare vad gäller IO. Vidare finns ett gemensamt IO- center för planering av IO och för att ge stöd till regionala befälhavare och till Joint Task Forces, JTF.[80] Detta är organiserat under STRATCOM och benämns Joint Information Operations Warfare Command, JIOWC. Vidare finns under STRATCOM dels Joint Task Force - Global Network Operations, JTF-GNO, samt Joint Functional Component Command - Network Warfare, JFCC-NW.[81]

Uppgiften för JTF-GNO är att försvara infrastrukturen för information, *"the Global Information Grid"*, på strategisk, operativ och taktisk nivå. Personalramen för dem är 255 personer.

På STRATCOM:s hemsida är uppgiften för JFCC-NW mer diffus och det redovisas inte hur många de har i sin organisation. Men i en kongressrapport sägs att även de har försvar av nätverk som uppgift men de ska dessutom kunna bedriva offensiv nätverkskrigföring.[82]

I en nyhetsartikel sägs denna styrka vara "den bästa hackerstyrkan världen någonsin skådat". Storleken på styrkan anges inte i artikeln men att personalen troligtvis kommer från alla försvarsgrenarna, FBI, CIA, National Security Agency samt att det finns en "handfull" civila. Deras förmågor är "topphemliga" men de ska kunna ta sig in i nätverk för att stjäla data samt förstöra dem. Det Pentagon medger i artikeln, är att JFCC-NW kan genomföra offensiv CNA.[83]

5.1.2 Amerikansk IT- industri

I mina källor har jag inte hittat något som pekar på att USA:s försvarsdepartement eller analytiker ser ett problem i relationen mellan försvarsmakten och amerikansk IT-industri. I avsnitt 4.1.2, där Kinas IT-industri beskrivs, finns dessutom förhållandet mellan USA:s och Kinas satsningar på forskning och utveckling beskrivet. Av detta framkommer att USA år 2005 satsade tre gånger mer på FoU jämfört med Kina.

Jag tolkar det därför som att USA:s styrkor har tillgång till det absolut senaste i form av amerikansk teknik.

Det kan dock skönjas en begynnande oro över den roll Kina håller på att få vad gäller försörjning av komponenter till IT-industrin. USA:s försvarsmakt är beroende av civila leverantörer, speciellt inom IT, och dessa leverantörer flyttar allt mer av sin produktion utomlands, exempelvis till Kina. USA bedömer att det *för närvarande* inte finns något hot i detta, men att denna trend kan utgöra

---

[79] IISS, *Military Balance 2005-2006*, s.20-35.
[80] Armistead, Leigh (edt.), (2004), *Information operations: Warfare and the hard reality of soft power*, Dulles, Brassey's Inc., s.165-166.
[81] Se U.S STRATCOM http://www.stratcom.mil/organization-fnc_comp.html (2006-10-30).
[82] Wilson, Clay, (2006), Information Operations and Cyberwar: Capabilities and Related Policy Issues, CRS Report for Congress. Nedladdad från: http://www.fas.org/irp/crs/RL31787.pdf (2006-10-26), s.8.
[83] Lasker, John, (2005), *U.S. Military's Elite Hacker Crew*, Wired News. Nedladdad från: www.wired.com/news/privacy/0,67223-0.html?tw=wn_story_page_prev2 (2006-10-26).

ett framtida hot.[84] Ett exempel på denna trend var då det kinesiska dataföretaget Lenovo 2005 köpte IBM:s PC- avdelning för 1.75 miljarder dollar. Amerikanska myndigheter var då oroliga för industrispionage mot IBM:s övriga delar samt att detaljer i kontrakt mellan IBM och amerikanska myndigheter skulle hamna hos kineserna.[85]

Då det gäller stöd från den privata sektorn, har den i USA fått ett ökat ansvar vad gäller CND. Följande står i rapport till den amerikanska kongressen:

> *"The National Strategy to Secure Cyberspace, published February 2003, states that the private sector now has a crucial role in protecting national security because it largely runs the nation's critical infrastructure."*[86]

Rapporten refererar till *The National Strategy to Secure Cyberspace*, som menar att USA:s infrastruktur är extra känslig. De anser att en angripare kan attackera och nyttja datorer i hem och företag som har dåliga skydd mot intrång. Dessa smittade datorer kan därefter användas för olika typer av fortsatta angrepp. Det finns därför en önskan att dessa användare ska ta ett större ansvar men det identifieras också att det är ett svårlöst problem att få privata intressen att investera i datasäkerhet.[87]

5.1.3 Amerikansk infrastruktur

Då det gäller amerikanska försvarets infrastruktur vad avser utbyggnad av fibernätverk, modernitet på utrustning med mera, har jag inte funnit några källor som diskuterar detta. Detta tolkar jag som att analytiker inte bedömer ämnet som ett problem.

5.1.4 Amerikansk utbildning och övningar

Vad gäller amerikanska civila skolor och antalet studenter, beskrivs det i kapitlet *Kinas utbildning och övningar*.[88]

Inom den amerikanska försvarsmakten finns ett antal utbildningsplatser som utbildar inom IO. De är i huvudsak knutna mot respektive vapenslag.

Detta identifieras till viss del som ett problem i Pentagons rapport *Information Operations Roadmap,* från 2003. Där hävdas att de olika försvarsgrenarnas specialister tolkar och använder förmågor inom IO på olika sätt. Detta leder till att kunskapsspridning och karriärmöjligheter försvåras. För att komma till rätta med detta föreslår rapporten bland annat utökad utbildning inom IO för alla elever på högre stabsutbildningar samt bättre möjligheter till specialistutbildning inom informationsoperationer.

På en högre akademisk nivå har Naval Postgraduate School, NPS, i Monterey Kalifornien fått i uppdrag att bilda försvarsmaktens *"Center of Excellence"*

---

[84] U.S.-China Economic and Security Review Commission, (2005), *Report to Congress.* Nedladdad från: http://www.uscc.gov/annual_report/2005/annual_report_full_05.pdf (2006-10-28), s.97-98. (Hädanefter U.S.-China Economic and Security Review Commission, (2005).

[85] U.S.-China Economic and Security Review Commission, (2005), s.89.

[86] Wilson, Clay, (2006), *Information Operations and Cyberwar: Capabilities and Related Policy Issues*, CRS Report for Congress. Nedladdad från: http://www.fas.org/irp/crs/RL31787.pdf , s.13-14. (Hädanefter Wilson, Clay, (2006), *Information Operations and Cyberwar: Capabilities and Related Policy Issues).*

[87] Wilson, Clay, (2006), *Information Operations and Cyberwar: Capabilities and Related Policy Issues*, s.13-14.

[88] Se kapitel 4.1.4.

med uppgiften att inom IO forska och utbilda i ett brett spektrum på doktorsnivå samt ge stöd till doktrinutveckling.[89]

USA genomför även övningar inom IO och CNO. Ett exempel var ELIGIBLE RECEIVER som hölls 1997. Det var den första i en rad övningar där det genomfördes intrång i ett stort antal datasystem och påvisade såbarheter hos en rad myndigheter.[90] Övningar inom informationskrigföring och CNO är sedan dess regelbundet återkommande.

5.2 De konceptuella faktorerna

5.2.1 Doktrinen och definitioner

En amerikansk motsvarighet till Kinas vitbok, är dels *The National Security Strategy* (NSS) samt *Quadrennial Defense Review Report* (QDR), båda i nya utgåvor under 2006. Den förstnämnda beskriver USA:s säkerhetspolitik och vilka möjligheter och problem de ser. *Quadrennial Defense Review* publiceras av försvarsdepartementet. Där beskrivs läget för USA:s försvarsmakt samt den fortsatta inriktningen.

Fokus i USA:s säkerhetsstrategi ligger på att bekämpa terrorism och förhindra spridning av massförstörelsevapen. Då det gäller IO och CNO nämns kort att:

> *”We are pursuing a future force that will provide tailored deterrence of both state and non-state threats (including WMD employment, terrorist attacks in the physical and information domains, and opportunistic aggression) while assuring allies and dissuading potential competitors.”*[91]

Vidare utvecklas försvarsmaktens förmågor inom fyra kategorier:

- Traditionella utmaningar
- Irreguljära utmaningar
- Katastrofala utmaningar ”*Catastrophic*”
- Splittrande utmaningar *”Disruptive”*

IO och CNO sägs falla under den sistnämnda kategorin. USA menar att de ska utveckla förmågan att möta:

> *“**Disruptive** challenges from state and non-state actors who employ technologies and capabilities (such as biotechnology, cyber and space operations, or directed-energy weapons) in new ways to counter military advantages the United States currently enjoys”*[92]

QDR säger lite mer om de hot som USA ser kring CNO.

> *“The Department will maintain a deterrent posture to persuade potential aggressors that their objectives in attacking would be denied and that any attack on U.S. territory, people, critical infrastructure (including through cyberspace) or forces could result in an overwhelming response. U.S. forces*

---

[89] Department of Defence (2003), *Information Operations Roadmap*, Delvis offentlig januari 2006. Nedladdad från: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf (2006-10-20), s.12-13.

[90] För mer information, se: http://www.globalsecurity.org/military/ops/eligible-receiver.htm (2006-10-29).

[91] The National Security Strategy of the United States of America, (2006). Nedladdad från: http://www.whitehouse.gov/nsc/nss/2006/ (2006-10-30), s.43.

[92] The National Security Strategy of the United States of America, (2006), s.43-44.

> *must be capable of defeating threats at a distance and of swiftly mitigating the consequences of an attack."*[93]

QDR uttrycker en vilja att ominrikta försvarsmakten och vad gäller CNO så sägs att USA ska kunna slåss *med* och *mot* datanätverk precis som vilket vapen som helst. Vidare ska koordineringen av offensiva och defensiva CNO bli bättre. Slutligen sägs att de erfarenheter som finns av Computer Network Attack, CNA, och Computer Network Exploitation, CNE, användas för att förbättra Computer Network Defence, CND, och för att skapa ett "djupförsvar" inom informationsarenan och att den senaste civila tekniken ska utnyttjas för detta.[94]

Det kan noteras att QDR delar upp transformeringen av försvaret i olika områden och att IO och CNO nämns under avsnittet *Tailored Deterrence/New Triad* syftandes på avskräckning och kärnvapentriaden.[95] Detta kan återspeglas av att STRATCOM fått det övergripande ansvaret för ledning och utveckling av IO.[96] I ett annat avsnitt nämns den transformering som krävs inom *Achieving Net-Centricity,* men där talas mer om behovet av bandbredd och tekniska lösningar samt standarder för detta. Vidare sägs att fortsatt utveckling krävs inom CND för försvar av informationssystemen.[97]

Att USA identifierat att IO kan utgöra ett hot mot deras informationssystem kan åskådliggöras av följande citat från doktrinen *Joint Publication 3-13 Information Operations*, JP 3-13:

> *"Adversaries are increasingly exploring and testing IO actions as asymmetric warfare that can be used to thwart US military objectives that are heavily reliant on information systems. This requires the US military to employ defensive technologies and utilize leading-edge tactics and procedures to prevent our forces and systems from being successfully attacked."*[98]

Hur USA närmare ser på betydelsen av information kan studeras i JP 3-13. Där sägs att:

> *"Information is a strategic resource, vital to national security, and military operations depend on information and information systems for many simultaneous and integrated activities."*[99]

USA anser att deras styrkor verkar i en allt mer komplex informationsmiljö och att det därför är nödvändigt för dess försvarsmakt att skaffa och bibehålla informationsöverlägsenhet. Informationsöverlägsenheten kan vara svår att uppnå, men det är eftersträvansvärt eftersom det ger egna förband en manöverfrihet gentemot fienden. [100]

Då det gäller amerikanska definitioner kring informationsoperationer är de offentliga och lättillgängliga via Internet. JP 3-13, den amerikanska doktrinen

---

[93] Department of Defence, (2006), *Quadrennial Defense Review Report*. Nedladdad från: http://www.comw.org/qdr/qdr2006.pdf (2006-10-29), s.24.
[94] Department of Defence, (2006), *Quadrennial Defense Review Report*, s.49-51.
[95] Triaden bygger på att USA har kärnvapen på land, på ubåtar samt i flygplan.
[96] Se USA:s Stridskrafter, kapitel 5.1.1.
[97] Department of Defence, (2006), Quadrennial Defense Review Report, s.58-59.
[98] Joint Publication 3-13, (2006), *Information Operations*. Nedladdad från: http://www.fas.org/irp/doddir/dod/jp3_13.pdf (2006-10-30), Kapitel 1 s.13. (Hädanefter JP 3-13, (2006).
[99] JP 3-13, (2006), s. ix.
[100] JP 3-13, (2006), Kapitel 1 s. 1-6.

för IO, redovisar både förkortningar, akronymer och definitioner.[101] Eftersom de amerikanska definitionerna som nyttjas i denna uppsats antas vara kända samt att de är lättillgängliga, redovisas de endast i en bilaga.[102]

Att observera är att USA i denna upplaga av JP 3-13 inte definierar informationskrigföring – IW. Orsaken till att IW inte längre definieras i JP 3-13 är inte känd för uppsatsförfattaren. Däremot i en äldre utgåva finns definitionen och det är den som nyttjas i denna uppsats då informationskrigföring är ett återkommande begrepp i det kinesiska konceptet.

5.2.2 USA:s syn på att använda förmågorna

Vilken strategi har då USA för att använda IO och CNO?

Till att börja med anger *Information Operations Roadmap* att IO ska bli en *core competency* i försvarsmakten och därigenom jämställas med mark-, sjö-, flyg- och specialförbanden. Orsaken till att IO får en ökad betydelse är att USA anser att det är viktigt att dominera hela informationsarenan.[103]

Betydelsen av informationsoperationer kan också åskådliggöras med de första meningarna, i första kapitlet i JP 3-13:

> *"Information operations (IO) are integral to the successful execution of military operations. A key goal of IO is to achieve and maintain information superiority for the US and its allies."*[104]

USA betonar alltså nödvändigheten av IO i militära operationer och att informationsöverlägsenhet är målet för IO.

USA:s koncept för informationsoperationer bygger på fem förmågor:

- Psykologiska operationer – PSYOPS
- Militär vilseledning – MILDEC
- Operativ säkerhet – OPSEC
- Elektronisk krigföring – EW
- Nätverkskrigföring – CNO

Informationsoperationer sägs bygga på att samordnat utnyttja dessa förmågor.

USA anser att dessa förmågor kan nyttjas både i offensiva och defensiva operationer och att de kan förekomma parallellt i en operation. Om någon av dem prioriteras framgår dock inte i JP 3-13.

Syftet med informationsoperationer är, som framkommer av citatet ovan, informationsöverlägsenhet. Att påverka motståndarens beslut och beslutsprocessen allt medan den egna processen ska skyddas.

För att nå syftet kan IO påverka data, information och kunskap på tre sätt:

- *By taking specific psychological, electronic, or physical actions that add, modify, or remove information from the environment of various individuals or groups of decision makers.*

---

[101] Se JP 3-13, (2006).
[102] Se bilaga 2.
[103] Department of Defence (2003), *Information Operations Roadmap*,), s. 4.
[104] JP 3-13, (2006), Kapitel 1, s.1.

- *By taking actions to affect the infrastructure that collects, communicates, processes, and/or stores information in support of targeted decision makers.*
- *By influencing the way people receive, process, interpret, and use data, information, and knowledge.*[105]

Då det gäller CNO som förmåga inom IO, menar USA att det ökande användandet av datorer och datanätverk hos ”osofistikerade” försvarsmakter och terroristgrupper, ökar behovet av CNO inom informationsoperationer. Detta leder till nya möjligheter att påverka motståndare men också nya egna sårbarheter vad gäller att identifiera sårbarheter i egna system.[106]

JP 3- 13 ger inte någon närmare beskrivning än så om hur USA ser på att använda CNO, då det avsnittet är hemligstämplat.[107] Men *Information Operations Roadmap* menar att CNA kan genomföras på strategisk, operativ och taktisk nivå. USA menar att det är svårt att bestämma var gränsen går mellan dessa i informationssfären och att CNA på taktisk nivå kan innebära att man måste agera strategiskt.[108] En följd av detta resonemang kan anses vara att försvarsdepartementet beslutat att STRATCOM ska ha det övergripande funktionsansvaret för CNA.

En reflektion är att USA i sina doktriner talar relativt mycket om att försvara egna och allierades nätverk, CND. Det talas mindre om CNA och CNE i de doktriner som studerats. Men vad som sker i realiteten inom försvarsmakten kan följande citat illustrera:

> *"I've got to tell you we spend more time on the computer network attack business than we do on computer network defense because so many people at very high levels are interested," said former CNA commander, Air Force Maj. Gen. John Bradley, during a speech at a 2002.*[109]

5.3 De moraliska faktorerna

I vilka situationer är då USA beredd att nyttja sin förmåga och finns det exempel på användande?

5.3.1 Värdegrund

I USA:s doktriner diskuteras legala aspekter av informationsoperationer och detta gäller speciellt för CNO.

JP 3-13 betonar att informationsoperationer kan innebära komplexa juridiska och policyfrågor och att det kan krävas koordinering med andra stater för att genomföras. I doktrinen säga att Krigets lagar gäller även för IO.[110]

Information Operations Roadmap tar upp behovet av att klarlägga det juridiska läget för CNA. Både vad gäller att besvara nätverksattacker, som för att klarlägga hur USA själva kan nyttja förmågan.[111]

---

[105] JP 3-13, (2006), Kapitel 1, s. 9.
[106] JP 3-13, (2006), Kapitel 2, s. 4-5.
[107] JP 3-13, (2006), Annex A.
[108] Department of Defence (2003), *Information Operations Roadmap*, s.52-53.
[109] Lasker, John, (2005), *U.S. Military's Elite Hacker Crew*, Wired News.
[110] JP 3-13, (2006), Kapitel 5, s. 5.
[111] Department of Defence (2003), *Information Operations Roadmap*, s. 52.

5.3.2 Exempel på amerikanskt nyttjande

Ett exempel på de problem USA ser med CNA ges i en rapport till kongressen. Där beskrivs att under operation *Iraqi Freedom*, 2003, hade USA färdiga planer att genomföra CNA mot bland annat det irakiska banksystemet, men som aldrig verkställdes. Orsaken till detta var att Pentagon konstaterade att det fanns en risk för okontrollerbara spridningseffekter till bland annat europeiska banksystem. Vidare var de irakiska militära och civila nätverken till stora delar ihopkopplade, vilket gjorde att USA inte kunde garantera att en nätverksattack enbart fick militära konsekvenser.[112]

Samma rapport ger dock exempel på andra aspekter av IO, såsom PSYOPS och vilseledningsoperationer, som nyttjades i Irakkriget.

Ett exempel på en operation där CNA ska ha använts är mot Serbien under mitten av 90-talet. Historien är obekräftad men vida spridd och går ut på att amerikanska specialförband luftlandsatts i Serbien. Där ska de ha kopplat på utrustning på kablar till radarstationer som genererat falska ekon i det serbiska luftförsvaret.[113]

6. ANALYS OCH RESULTAT

6.1 Likheter och skillnader: Fysiska faktorer

6.1.1 Stridskrafterna

I beskrivningen av Kina och USA:s stridskrafter framkommer att bägge länderna disponerar stridskrafter för informationsoperationer och CNO. Antal förband har jag dock inte funnit.

En noggrannare efterforskning på den amerikanska sidan hade troligtvis kunnat ge ett svar vad gäller förband med IO som uppgift. Detta eftersom jag uppfattar att USA är relativt öppna med att redovisa antal förband i sin försvarsmakt. Att hitta öppna kinesiska uppgifter är svårare.

Då det gäller förband med CNO som uppgift och särskilt CNA, är uppgifterna även på den amerikanska sidan knapphändiga. På STRATCOM:s hemsida finns förbandet som arbetar med skydd av informationssystem, JTF-GNO, redovisat med antal och en egen hemsida. JFCC-NW, som enligt uppgift ansvarar för CNA, har ingen egen sida och antal personer anges inte.[114] På den kinesiska sidan är uppgifterna än mer knapphändiga.

En resurs som Kina har och som jag inte hittat någon direkt motsvarighet till hos USA, är milisen. Under Mao utgjorde de en hörnsten i ”Folkets Krig” och Kina ser i informationsteknologin att nya uppgifter finns för dem. Då det gäller militära operationer anger Kina själva att styrkor från milisen övar tillsammans med PLA och USA menar att milisen ger stöd till PLA vad gäller informationskrigföring.[115] Med tanke på den tradition som finns i Kina av att

---

[112] Wilson, Clay, (2006), *Information Operations and Cyberwar: Capabilities and Related Policy Issues*, s. 5-6.
[113] Lasker, John, (2005), *U.S. Military's Elite Hacker Crew*, Wired News.
[114] Se kapitel 5.1.1 samt http://www.stratcom.mil/organization-fnc_comp.html och http://www.stratcom.mil/fact_sheets/fact_jtf_gno.html (2006-11-01).
[115] Se kapitel 4.1.1.

nyttja milisen så bedömer jag det som högst sannolikt att Kina kommer att fortsätta att utveckla konceptet.

Antalet personer i milisen med IO och CNO som uppgift har jag inte funnit. Men min slutsats är att det är flera tusen som har detta som uppgift. Slutsatsen bygger på, att om uppgiften i PLA Daily Online stämmer, fanns det på en låg nivå i ett militärdistrikt (MD) år 2004 över 500 stycken inom milisen med dessa uppgifter. Sedan finns det ytterligare fyra MD i denna militärregion (MR). Vidare finns sju MR och jag antar att varje militärregion har liknande styrkor.[116] Ytterligare ett exempel är uppgifterna om att mellan 30 000 – 100 000 personer arbetar med att kontrollera Internet för inrikespolitiska ändamål. Det är dock oklart om de kan anses tillhöra milisen.

6.1.2 It-industri

Då det gäller vilket stöd som kan ges från den civila delen av samhället och industrin till militären, anser jag att det i Kina är mer uttalat att den civila sidan ska kunna ge stöd åt den militära. I USA finns det en betydande IT- och försvarsindustri som, om bara det finns ekonomi, kan förse försvaret med det de beställer. Men vad som beskrivs i empirin om Kina är att den högteknologiska civila och militära industrin är djupt integrerade med varandra.

Vad gäller kvaliteten i form av modernitet på de produkter industrin tar fram, antas USA fortfarande vara världsledande och kommer antagligen att vara så under flera år eftersom amerikanska företag fortfarande satsar mest i världen på forskning och utveckling. Kinas kraftiga satsning på forskning och utveckling tyder på att de har ambitioner att minska USA:s försprång. I empirin beskrivs att större delen av Kinas anslag går till FoU inom IT, telekom samt försvarsindustrin.[117] Vad detta på sikt kommer att medföra samt Kinas allt viktigare roll i produktionen av IT-produkter, finns anledning att bevaka.

6.1.3 Infrastruktur

Infrastrukturen moderniseras i Kina och bedömare menar att de har byggt ut sin förmåga att via datanätverk kommunicera mellan förbanden. I USA diskuteras inte detta vilket jag tolkar som att USA inte ser det som ett problem.

Kina rapporteras använda, till en okänd del, inhemska produkter i känsliga delar av sina nätverk.[118] Jag anser att den militära oro som finns, att det i västerländska produkter ska finnas buggar som kan användas för att attackera deras nätverk, kommer att vara en fortsatt drivkraft för den kinesiska civila IT-industrin att utveckla egna produkter.

6.1.4 Utbildning och övningar

I både Kina och USA finns skolor som uppges utbilda och forska inom IO och CNO. Utbildningsinnehållet har inom ramen för denna uppsats inte studerats vilket gör att jag inte kan uttala mig om kvaliteten på utbildningen. Men i båda länderna finns det utpekade skolor, NPS i USA samt militärhögskolan i Wuhan i Kina, som ska utgöra center för högre utbildning inom IO.

---

[116] Se kapitel 4.1.1 sista stycket.
[117] Se kapitel 4.1.2 samt 5.1.2.
[118] Se kapitel 4.1.3.

Noterbart för Kinas del är den differentiering av utbildning inom IO som görs beroende på ålder. Slutsatsen av det är att kompetensen i framtiden kommer att bli ännu högre i Kina då de framtida ledarna får en längre utbildning inom IO.

Då det gäller milisen i Kina och deras utbildningsnivå anser jag att den troligtvis är hög. Detta med bakgrund av att personalen till styrkorna beskrivs komma från forskningscentra och industrier. Ytterligare grund för slutsatsen att milisen är en kvalificerad resurs, är den stora mängd studenter som examineras från högre tekniska utbildningar i Kina samt deras expanderande IT-industri.

Slutligen konstateras att båda staterna övar inom IO och CNO. Noterbart är att både USA och Kina verkar ha genomfört sina första övningar med CNO 1997.[119]

6.1.5 Slutsatser: Fysiska faktorer

Som anges i frågeställningen ska jag dra slutsatser kring större skillnader mellan Kina och USA.

I analysen visas att båda länderna har styrkor för IO och CNO, så i det avseendet finns inga större skillnader mellan länderna. Men det Kina har och USA verkar sakna helt, är milisförband med uppgifter inom IO och CNO. I milisen har PLA, efter mobilisering, en stor organisation som kan förstärka dem vid operationer. Med tanke på den kinesiska traditionen och erfarenheten av att leda och nyttja denna typ av förband, anser jag att dessa kommer att få en allt mer ökande betydelse. Då det gäller kvaliteten på milisstyrkorna för IO, är min slutsats att de troligtvis utgör en kvalificerad resurs med tanke på att de utrustas och rekryteras från Kinas snabbt expanderande teknikindustri.

En annan skillnad mellan länderna anser jag, är att det i Kina finns en betydligt djupare integrering mellan den civila och militära industrin. Min uppfattning är att detta leder till att PLA kan styra forskning och utveckling på ett sätt som inte USA:s försvarsmakt kan.

Slutligen vad gäller de fysiska faktorerna är min slutsats att USA fortfarande har ett kraftigt tekniskt försprång inom IT. Detta beroende på den kunskap och industri som USA byggt upp under decennier samt en stor satsning på FoU.

6.2 Likheter och skillnader: Konceptuella faktorer

6.2.1 Doktriner och definitioner

Inledningsvis konstaterar jag att det på den amerikanska sidan finns ett flertal doktriner. De finns på alla nivåer och i alla funktioner. *Joint Publications 3-13 Information Operations* har särskilt studerats för denna uppsats. De flesta amerikanska doktrinerna är dessutom offentliga och kan laddas ner via Internet.

För Kinas del har jag enbart funnit *White Paper on China's National Defense in 2004* som offentligt och på engelska uttrycker kinesisk syn på försvarsmakten. Jag antar att även Kina har ett flertal doktriner men att de inte är tillgängliga på Internet.

Om man jämför den kinesiska vitboken och dess amerikanska motsvarigheter på strategisk nivå i form av *The National Security Strategy* (NSS) och

[119] Se kapitel 4.1.4 samt 5.1.4.

Quadrennial Defense Review Report (QDR), konstateras stora olikheter. Jag anser att de amerikanska dokumenten speglar situationen som USA befinner sig i efter terrorattackerna 11:e september, då de talar mycket om hot från terrorister och spridning av massförstörelsevapen. QDR beskriver att USA ska kunna möta hot mot informationsdomänen från olika aktörer och att USA ska kunna besvara attacker samma medel.

Den kinesiska vitboken talar ofta om att Kina är mitt uppe i en modernisering av dess försvar och de betonar betydelsen av informationsteknologin i detta. Uttrycket kineserna använder är *informationalization*, ett begrepp som ofta återkommer i kinesiskt material och som jag i kapitel 4.2.1 försökt belysa innebörden av. I vitboken sägs Kina sträva efter att skapa en informationaliserad styrka för att vinna informationaliserade krig.

Min slutsats kring detta är att doktrinerna återger USA och Kinas situation just nu. USA har nyttjat informationstekniken i sin försvarsmakt länge. De anser att det är en naturlig del för dem och de behöver inte betona att informationssystem är viktiga. De talar mer om att informationssystemen ska användas för att stoppa terrorister. Kina å sin sida har påbörjat sin modernisering och genom att tydligt betona detta i *White Paper on China's National Defense in 2004*, ges signaler om att Kina identifierat betydelsen av informationsteknik för att vinna framtida krig. En vidare slutsats jag drar av detta, är om informationstekniken är viktig i de krig Kina ser framför sig, är det inte en omodern fiende de anser sig ska kunna möta.

Då det gäller definitioner av begrepp inom IO och CNO, är USA:s redovisade på samma sätt som deras doktriner. Officiella kinesiska doktriner har jag inte funnit utan därför bygger denna analys på det material som redovisas i kapitel 4.2.1.

Då det gäller informationsoperationer anser USA att det består av fem förmågor: PSYOPS, MILDEC, OPSEC, EW, CNO.

Intressant är att de förmågorna återfinns i överste Baocuns definition av information*skrigföring*. Han definierar att IW innehåller:

> *"The contents of IW are military security, military deception, physical attack, electronic warfare, psychological warfare and net warfare."*[120]

Fler likheter är att USA i IO talar om att påverka en motståndares förmåga till beslutsfattning samtidigt som egen förmåga skyddas. Baocun säger att i IW ska fiendens information och informationssystem attackeras allt medan egna system skyddas.

Amerikansk definition av IW i sin tur påminner mer om kinesisk IO. USA menar att IW är informationsoperationer som genomförs i kris och krig för att nå bestämda mål mot en bestämd motståndare. Generalmajor Dai i sin tur definierar IO som en serie av operationer med informationsarenan som stridsfält och där informationssystem och information är de direkta målen.

Slutsatsen av detta menar jag är att USA, Baocun och Dai talar om samma saker, men benämner de olika. En annan slutsats är att i brist på officiella kinesiska definitioner, måste analyser av kinesiska dokument ske med viss försiktighet om syftet är att noggrant studera deras koncept.

---

[120] Thomas, Timothy L., (2001), *China's Electronic Strategies*, s.3.

6.2.2 Syn på användande

För att analysera hur Kina ser på att nyttja IO används, i brist på officiella dokument, de fem faktorer som general Dai anser är viktigt i kinesisk IO: Strategi, Informationsöverlägsenhet, Offensiv, Krigslister samt Integrering.[121]

Dai menar att en bra strategi kan kompensera en rad svagheter som exempelvis teknologi, utrustning eller brist på underrättelser. Han menar att en strategi kan tjäna som en ”osynlig krigföringsförmåga”.

Detta resonemang kring att strategier kan kompensera svagheter, har jag inte funnit i amerikanska doktriner. JP 3-13 nämner *att* det finns strategier och att det handlar om planering för att genomföra operationerna på bästa möjliga sätt.[122] Jag tolkar det som att Dai talar om asymmetriska förhållanden och han menar att brister i fysiska faktorer kan kompenseras med bättre konceptuella faktorer.

Jag anser att ett område det råder samklang mellan JP 3-13 och Dais filosofier är betydelsen av informationsöverlägsenhet. Detta är vad som ska uppnås och även metoderna att nå och behålla överlägsenheten är jämförbara. Samordning av förmågor och nyttjande av mjuka och hårda metoder finns med hos bägge.

Ytterligare ett område som jag anser i stort är likvärdiga är teorierna kring betydelsen av offensiva aktioner. USA betonar att IO- förmågorna kan nyttjas parallellt i en operation både offensivt och defensivt. Dai menar att det krävs en ”aktiv offensiv defensiv” och min slutsats är att de talar om samma saker. Det som Kina betonar och som jag inte funnit i JP 3-13, är tankegångarna om att genomföra förebyggande förstaslag i informationsoperationer. Min slutsats kring detta är att Kina anser att deras informationssystem är dåligt skyddade och hotade vid en konflikt. Genom att då slå först, hoppas de kunna skada en oförberedd motståndares informationssystem och därigenom skapa bättre förutsättningar för fortsatt strid. Detta är ett hot som även USA har identifierat och säger i JP 3-13 att motståndare allt mer utforskar IO som en metod för asymmetrisk krigföring och för att på så vis påverka de amerikanska informationssystemen.[123]

Ett område som är intressant är krigslister. Är Kinas syn på krigslister och USA:s syn på Military Deception, MILDEC (vilseledning), samma sak? Timothy Thomas refererar till en kinesisk artikel då han diskuterar kring detta.[124] Jag har saknat den kinesiska artikeln och har därför haft svårt att noggrant analysera detta.

MILDEC strävar efter att få motståndaren att dra felaktiga slutsatser som leder till ett önskat agerande. Kina ser krigslister som ett sätt att kompensera bristfällig teknik. Min tolkning utifrån det Thomas skriver och JP 3-13, är att vilseledning och krigslist är i nära släktskap med varandra.

Men min slutsats är också att Kina har en lång tradition av krigslister och att de troligtvis ser på detta, inte som en separat förmåga som USA, utan ett tankesätt som ständigt ska finnas med i planeringen. De kinesiska traditionerna i detta område är värda en noggrannare studie.

---

[121] Se kapitel 4.2.2.
[122] Se JP 3-13.
[123] Se fotnot 98, katitel 5.2.1.
[124] Thomas, Timothy L., (2001), *China’s Electronic Strategies*, Fort Leavenworth, s.3-4.

Slutligen menar Dai att civila och militära styrkor skall integreras i informationsoperationer. Han menar att de civila kan ge ett värdefullt stöd till PLA. Jag har inte funnit något liknande resonemang hos amerikanerna. Med tanke på beskrivningen av milisstyrkorna och hur de övar med PLA, anser jag att dessa tankar har fått genomslag i Kina och att det stöder min analys att de har en ökande betydelse. Ett exempel på

6.2.3 Slutsatser: Konceptuella faktorer

De stora skillnaderna mellan USA och Kina i de konceptuella faktorerna är följande.

Det är svårt att analysera officiell kinesisk syn på IO och CNO då det, i motsats till USA, saknas doktriner som är öppet tillgängliga och översatta. Det får till exempel återverkningar då definitioner och strategier ska studeras och det kan leda till feltolkningar.

Definitionerna i Kina och USA skiljer sig åt vad gäller IO och IW. Förvirringen om vad kineser menar då skriver IW, för en västlig analytiker, är ett exempel på de problem som uppstår då de kinesiska doktrinerna saknas och en faktor man ska ha med sig.

Vidare präglas doktrinerna av ländernas situation. USA skriver om kriget mot terrorismen och för dem är informationsteknologin naturlig och de lägger inte stor vikt vid detta. Kina å andra sidan talar mycket om *informationalization* och betydelsen av detta för deras försvarsmakt. Slutsatsen jag drar av detta, är att de tydligt vill visa att de insett informationsteknologins betydelse för att vinna framtida krig mot moderna motståndare.

Den betydelse kineser ser i strategier och att de kan avhjälpa andra brister, tankarna på förebyggande anfall för att få motståndare ur balans samt integrering av civila styrkor i militära förband, är exempel på nyttjande av IO och CNO som jag sett att Kina och USA skiljer sig åt. Vidare anser jag att Kinas syn på krigslister förtjänar djupare studier för att ytterligare jämföra detta med västligt tänkande.

6.3 Likheter och skillnader: Moraliska faktorer

6.3.1 Värdegrund

Vad det gäller USA och Kinas vilja att nyttja CNO utifrån resonemang kring värdegrunder och legala aspekter, är det en stor skillnad mellan det officiella USA och det officiella Kina. USA resonerar öppet om vilka legala problem de ser med nuvarande lagstiftning att använda förmågan. Liknande resonemang har jag överhuvudtaget inte funnit hos Kina.

6.3.2 Exempel på användande

Hänsyn till legala frågor återspeglas i den amerikanska tveksamheten till CNA under Irakkriget 2003. USA ansåg att distinktions- och proportionalitetsprincipen i Krigets lagar inte kunde tillmötesgås då de upptäckte att de irakiska militära och civila systemen var för integrerade med varandra samt att finanssystem utanför Irak kunde påverkas av en attack.

De kinesiska hackerattackerna som beskrivs i empirin, anser jag speglar en annan syn. Nu är det oklart vilka som ligger bakom dessa attacker. Det kan

vara oorganiserade attacker av privatpersoner som av oklara anledningar utför dem.

Det är dock möjligt att denna typ av attacker har de kinesiska myndigheternas tysta godkännande och att Kina ser detta som ett sätt att inhämta underrättelser och dra erfarenheter utan att kunna ställas till svars.

6.3.3 Slutsatser: Moraliska faktorer

Det är en stor skillnad mellan USA och Kina vad gäller synen på CNO. Frånvaron av diskussioner på den kinesiska sidan och exemplen på attacker tolkar jag som att de är beredda att nyttja CNO i en större omfattning än USA.

Viljan att använda CNO finns även i USA, de planerade exempelvis för attacker mot Irak, men de tar större hänsyn till legala problem än Kina.

6.4 Resultat

Frågan i denna uppsats var:

”Beskriv större skillnader mellan Kinas och USA:s krigföringsförmåga inom informationsoperationer med tyngdpunkt på CNO, idag och i nära framtid. Om det finns sådana, diskutera och dra slutsatser vad de innebär.”

För att kunna svara på det skulle följande följdfrågor diskuteras:

- Hur definieras Informationsoperationer och Informationskrigföring i Kina respektive USA?
- Hur definierar Kina och USA CNO?
- Vilka resurser finns inom CNO?
- Betonar de olika strategier inom IO och CNO?
- Vilken vilja finns att nyttja CNO?

Jag har kommit fram till att det finns en skillnad mellan USA:s och Kinas sätt att *definiera informationsoperationer och informationskrigföring*. Då Kina talar om IW avser de ett begrepp som mer påminner om vad USA definierar som IO. Vidare att det omvända råder i form av att då kineser talar om IO är det mer likt det amerikanska IW.

En kinesisk *definition på CNO* har jag inte funnit i det material jag studerat. Det närmaste jag kommit är en definition på vad jag uppfattar vara CNA. Den påminner om motsvarande amerikansk definition, att störa och förstöra information i datorer och nätverk.

Då det gäller *resurser inom CNO* har både USA och Kina styrkor för detta. Kina har i milisförbanden en personell resurs som med ett okänt antal personer kan utgöra en betydande tillgång efter mobilisering. Milisförbanden består av civila som sannolikt har en bra teknisk utbildning, utrustning från Kinas expanderande teknikindustri och som övas i CNO under militär ledning. Jag anser att de troligtvis kan utgöra både en offensiv och defensiv resurs inom CNO. Vad gäller tekniska resurser anser jag att både USA och Kina har tekniska förutsättningar för att bedriva CNO men att USA fortfarande har ett tekniskt försprång.

Skillnader i strategier som jag funnit mellan USA och Kina är att Kina fäster stor vikt vid att kompensera brister i fysiska faktorer med konceptuella

faktorer. Vidare att Kina förordar förebyggande anfall vilket jag tolkat som ett sätt att få motståndaren ur balans. Slutligen har Kina en strategi som betonar integration av civila och militära resurser.

Viljan att nyttja CNO har analyserats utifrån legala resonemang. Där har jag funnit att USA hade planerat CNA mot Irak 2003, men genomförde det inte då det fanns konsekvenser som inte var förenliga med Krigets lagar. Motsvarande resonemang har jag inte funnit hos Kina. Slutsatsen är att båda länderna är beredda att använda CNO men att USA har en högre tröskel innan de gör det.

Utifrån dessa svar konstateras att det inom krigföringsförmågans tre faktorer finns en *rad skillnader* mellan Kina och USA. Är det stora skillnader? Några av dem anser jag är det. Att definitioner av IO och IW skiljer sig åt anser jag inte vara en stor skillnad då de dels kan ändras över tiden och frånvaron av kinesisk doktrin gör att det inte går att ge ett säkert svar på detta. En definition på vad Kina innefattar i CNO begreppet har jag inte funnit, men även detta anser jag vara av mindre vikt med samma anledning som ovan.

Större skillnad är det då vad det gäller personella resurser. Kinas milis är en tillgång som saknas på den amerikanska sidan. Detta kan ses som bevis på ytterligare en stor skillnad, nämligen integreringen mellan civila och militära resurser i det kinesiska samhället. I det speglar sig de resurser som en stat av Kinas karaktär kan mobilisera om viljan finns.

Tankarna kring förebyggande anfall är en annan stor skillnad som jag konstaterat. Det i sig är ett exempel på två andra skillnader, synen på att kompensera tekniska svagheter med en överlägsen strategi samt frånvaron av diskussioner kring legala frågor.

Slutsatsen är att Kina utvecklar en förmåga till informationsoperationer och CNO som har många likheter med USA, men de nyttjar också traditionella kinesiska koncept för att kompensera teknisk underlägsenhet och på så vis skapar de ett koncept med en klar kinesisk karaktär.

7. AVSLUTNING

7.1 Diskussion

Är mina slutsatser korrekta? Uppsatsen bygger på öppet material och på kinesisk sida saknas det till stor del primära källor. Detta är en brist då det kinesiska konceptet analyseras utifrån material som är sekundära källor. Dessa faktorer ska man ha med sig då resultaten i uppsatsen nyttjas.

Jag har till skillnad från andra analyser använt pelarmodellen som analysverktyg. Likväl konstaterar jag att mina slutsatser inte avviker från annat material som jag studerat. Detta anser jag gör att uppsatsen ändå fyller grundläggande krav på tillförlitlighet.

Hur ska man då ställa sig till resultatet av min analys? Jag har analyserat Kina utifrån en jämförelse med USA och använt den svenska Pelarmodellen som analysverktyg. Orsaken till att USA valdes som referens till Kina var att jag ansåg det som välkänt för mig som svensk officer och att jag kan identifiera mig med deras synsätt.

Resultatet som jag kommit fram till är att kinesiska och amerikanska koncept inom informationsoperationer i stort påminner om varandra. Men de avviker

också inom en rad områden. Jag anser att orsaken till detta är att Kina, genom att utnyttja befintliga resurser och strategi, försöker kompensera teknologiska brister. Det asiatiska synsättet att använda strategier för att kompensera teknik som saknas är ett utmärkt exempel på ett tankesätt som jag som västerlänning kan dra erfarenheter av.

En resurs som Kina har i stort antal är befolkningen. Jag hävdar att i det stora antal kineser som examineras inom högre tekniska utbildningar, har PLA en bred rekryteringsbas för milisstyrkorna och en betydelsefull resurs för informationsoperationer. Jag antar att ha tillgång till ett stort antal kvalificerade personer är en fördel då de kan analysera data på en bred front, i alla aspekter inom CNO.

De tankegångar som Timothy Thomas har kring gamla kinesiska strategier gör milisen extra intressant. Han menar att det nya Kina ser på en 300 år gammal strategi som ”*Invänta den utmattade fienden i lugn och ro*” som att nyttja milisen till att mätta motståndarens nätverksförsvar för att sedan med experter attackera huvudmålen. Kombineras detta med Kinas syn på överraskande anfall inom informationskrigföringen fås ytterligare en dimension.

Är detta tekniskt möjligt? Det ligger utanför min kunskap men jag tycker att det ett bra exempel på att kinesiskt tänkande där gamla traditioner, modern teknik och tillgängliga resurser kombineras i strategier för att kompensera tekniska brister. Men vilken kapacitet PLA och milisen har att i en riktig konflikt genomföra informationsoperationer mot ett kvalificerat motstånd i form av militära system och förband återstår att se.

Samarbetet mellan civil och militär sektor i Kina är ytterligare ett område som har varit intressant att studera. Det påminner om den gamla totalförsvarstanken i Sverige och kan ses som ett exempel på vad en stat kan åstadkomma om alla resurser fokuseras på landets överlevnad. I Sverige och övriga västvärlden är detta ett koncept som hörde till det kalla kriget. Intressant är därför att Kina anser sig behöva ha denna filosofi.

Vad kan då svenska försvarsmakten och officierare lära av Kina? Jag anser att vi närmare bör studera kinesisk syn på krigslister och strategier som ett sätt att kompensera andra brister. Det framkommer i kinesiskt tänkande att *Stratagems* ska ses som att med små och tillgängliga medel använda det man har på nya och överraskande sätt. Ett tankesätt som kan leda till nya lösningar på de problem vi anser oss ha. Vidare kan det vara så att vi nu i västvärlden är utsatta för kinesisk krigslist. Kanhända är det kinesiska konceptet att satsa på IO ett sätt att dra bort fokus från andra områden. För vi ska komma ihåg att Kina inte bara utvecklar koncept för informationsoperationer. De genomför en kraftig upprustning och modernisering av *hela* sin försvarsmakt som förtjänar uppmärksamhet.

Slutligen vill jag säga att inför denna uppsats såg jag på Kina som ett land med en stor omodern armé och ett land som försåg västvärlden med billiga varor i våra butiker. Jag har efter arbetet med denna uppsats konstaterat att Kina är betydligt mer avancerat än så.

Jag hoppas därför att denna uppsats kan tjäna som inspiration till fortsatta studier av Kina och dess försvarsmakt.

7.2 Förslag på fortsatt forskning

Denna uppsats har haft brett perspektiv på Kinas krigföringsförmåga inom informationskrigföring och CNO. För att i framtiden ytterligare fördjupa kunskapen kring Kina och deras förmågor kan följande områden särskilt belysas:

- I den kinesiska vitboken nämns det att Kina utvecklar RMA med kinesisk karakteristik. Vad innebär det och hur har deras resonemang kring RMA förändrats och utvecklats de senaste åren?
- Denna uppsats har fokuserat på Kinas utveckling kring IO/IW och CNO. Men Kina utvecklar hela sin krigsmakt, vilka erfarenheter kan dras av deras modernisering av marinen, armén, flygvapnet och robotstyrkorna?
- Under kapitlet om kinesiska definitioner nämns att IW och IO i Kina kan ha en annan mening än det västerländska. Vart de härstammar de ifrån och finns det likheter i exempelvis Ryssland?
- Den civila och militära sektorn i Kina är djupt integrerade med varandra. På vilka sätt styr den kinesiska försvarsmakten en industri som har utländska intressen och blir allt mer affärsinriktad?
- I Kina finns begreppet krigslist. Hur ser de på nyttjandet av krigslister och vad är skillnaden mellan krigslist och vilseledning?

8. KÄLL- OCH LITTERATURFÖRTECKNING

8.1 Källor

8.1.1 Tryckta

- Försvarsmakten, (2002), *Militärstrategisk doktrin*, Stockholm, Försvarsmakten, M7740- 774002.

  -(2005), *Doktrin för gemensamma operationer*, Stockholm, Försvarsmakten, M7740- 774003.

- The International Institute for Strategic Studies, (2005), *The Military Balance 2005-2006*, London, The International Institute for Strategic Studies, ISBN 0-415-37393-x.

8.1.2 Elektroniska

- Department of Defence (2003), *Information Operations Roadmap*, Delvis offentlig januari 2006. Nedladdad från: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf (2006-10-20)

  -(2006), *Quadrennial Defense Review Report*. Nedladdad från: http://www.comw.org/qdr/qdr2006.pdf (2006-10-29)

- Federation of American Scientist (FAS): http://www.fas.org/nuke/guide/china/doctrine/natdef2004.html *White Paper on China's National Defense in 2004*. (2006-09-26)

- Joint Publication 3-13, (2006), *Information Operations*. Nedladdad från: http://www.fas.org/irp/doddir/dod/jp3_13.pdf (2006-1030)

- Office of the Secretary of Defence, (2005), *Annual report to congress- Military Power of the People's Republic of China*, Washington, Department of Defense. Nedladdad från: http://www.defenselink.mil/pubs/pdfs/China%20Report%202006.pdf (2006-09-27)

- PLA Daily Online: http://english.pladaily.com.cn/

  - Over 500 information professionals enrolled into militia organization *http://english.pladaily.com.cn/site2/columns/2004-09/07/content_2960.htm* (2006-10-10)

  -Keep a firm grip on key factors of informationization *http://english.pladaily.com.cn/site2/columns/2004-09/11/content_11936.htm* (2006-10-02)

  -Attention should be given to the information territory *http://english.pladaily.com.cn/site2/columns/2004-09/11/content_11935.htm* (2006-10-20)
  -The key to sucess in informationzed war is to take offensive action *http://english.pladaily.com.cn/site2/columns/2004-09/11/content_11934.htm* (2006-10-20)

-Group army improves its IT fighting power
http://english.pladaily.com.cn/site2/columns/2004-09/12/content_11968.htm (2006-10-05)

- The National Security Strategy of the United States of America, (2006). Nedladdad från: http://www.whitehouse.gov/nsc/nss/2006/ (2006-10-30)
- United States Strategic Command, http://www.stratcom.mil/
- U.S.-China Economic and Security Review Commission, (2005), *Report to Congress*. Nedladdad från: http://www.uscc.gov/annual_report/2005/annual_report_full_05.pdf (2006-10-28)
- Wilson, Clay, (2006), *Information Operations and Cyberwar: Capabilities and Related Policy Issues*, CRS Report for Congress. Nedladdad från: http://www.fas.org/irp/crs/RL31787.pdf (2006-10-26)

8.2 Litteratur

8.2.1 Tryckta

- Armistead, Leigh (edt.), (2004), *Information operations: Warfare and the hard reality of soft power*, Dulles, Brassey's Inc., ISBN 1-57488-698-3.
- Blasko, Dennis J., (2006), *The Chinese Army today – Tradition and transformation for the 21st century*, Oxon, Routledge, ISBN 0-415-77003-3.
- Dufberg, Gustaf, (2005), *Krigföringsförmåga*, Stockholm, Försvarshögskolan, C- uppsats
- Lundblad, Nicklas, *Internet både hotar och stöder Kinas regim*, Svenska Dagbladet, 2006- 10-02.

8.2.2 Elektroniska

- Barrington, Barrett M. jr., (2005), *Information Warfare: China's Response to U.S. Technological Advantages*, International Journal of Intelligence and Counterintelligence, Volume 18, Number 4, Routledge, Taylor & Francis Group. Nedladdad från FHS nätverk: http://www.ingentaconnect.com/content/routledg/ujic/2005/00000018/00000004/art00006 (2006-10-23)
- Hildreth, Steven A., (2001), *Cyberwarfare*, CRS Report for Congress. Nedladdad från: http://www.fas.org/irp/crs/RL30735.pdf (2006-10-30)
- Hudson Institute, (2005), *China's New Great Leap Forward – High Technology and Military Power in the Next Half-Century*, Cicero, Hudson Institute, ISBN 1-55813-148-5. Nedladdad från

http://www.hudson.org/files/publications/China_Great_Leap_Forward.pdf (2006-10-23)

- International Assessment and Strategy Center: *Top Ten Military Modernization Development* http://www.strategycenter.net/printVersion/print_pub.asp?pubID=65 (2006-10-18)

- Lasker, John, (2005), *U.S. Military's Elite Hacker Crew*, Wired News. Nedladdad från: www.wired.com/news/privacy/0,67223-0.html?tw=wn_story_page_prev2 (2006-10-26)

- Moss William, (2006), *The curse of informatization*, CNet Asia Blog. Nedladdad från: http://asia.cnet.com/reviews/blog/littleredblog/0,39056119,61953570,00.htm (2006-10-20)

- Mulvenon, James och Finkelstein, David M. (edit.), (2005), *China's Revolution in Doctrinal Affairs: Emerging Trends in the Operational Art of the Chinese People's Liberation Army*, Alexandria, Center for Naval Analysis. Nedladdad från: http://www.cna.org/documents/doctrinebook.pdf (2006-10-23).

- Thomas, Timothy L., (2000), *Like Adding Wings to the Tiger: Chinese Information War Theory and Practice.* Nedladdad från: IWS- The Information Warfare Site http://www.iwar.org.uk/iwar/resources/china/iw/chinaiw.htm (2006-09-27)

  - (2001), *China's Electronic Strategies*, Fort Leavenworth, Foreign Military Studies Office. Nedladdad från http://leav-www.army.mil/fmso/documents/china_electric/china_electric.htm (2006-10-19)

  - (2005), *Chinese and American Network Warfare*, Joint Forces Quarterly, nedladdad från: http://www.dtic.mil/doctrine/jel/jfq_pubs/1538.pdf (2006-10-23)

- Washington Post, *Computer System Under Attack*, http://www.washingtonpost.com/wp-dyn/content/article/2006/10/05/AR2006100501781.html (2006-10-18)

8.3 Referensmaterial

- Doubletongued Wordwrester Dictionary: http://www.doubletongued.org (2006-10-16)
- Encyclopaedia Britannica: http://search.eb.com/ (2006-10-16)
- Nationalencyklopedin: http://www.ne.se/jsp/notice_board.jsp?i_type=1 Tillgänglig från Anna Lindh bibliotekets nätverk.
- Oxford Reference Online: http://www.oxfordreference.com/views/GLOBAL.html (2006-10-16)
- Wikipedia: http://en.wikipedia.org/wiki/Main_Page (2006-10-16)

- WordFinder – Lexikon på PC, version 4.1. Installerat av FHS på datorer för chefsprogrammet 04-06T.

BILAGA 1: AMERIKANSKA DEFINITIONER KRING INFORMATIONSOPERATIONER

Definitionerna enligt nedan är urval av viktiga begrepp från Joint Publication 3-13. För en fullständig lista över definitioner inom informationsoperationer, se JP 3-13 tillgänglig från http://www.fas.org/irp/doddir/dod/jp3_13.pdf :

Information. 1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation.

Information system. The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

Information environment. The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

Information superiority. The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

Information operations. The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own. Also called IO.

Information warfare. Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.125

Computer network operations. Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations. Also called CNO.

Computer network attack. Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Also called CNA.

Computer network defense. Actions taken through the use of computer networks to protect, monitor, analyze, detect and respond to unauthorized

[125] Då det gäller begreppet informationskrigföring – information warfare, så har definitionen tagits bort i denna utgåva av JP 3-13. För denna uppsats kommer definitionen från 1998 ur JP 3-13 att nyttjas då det är ett begrepp som ofta förekommer i litteraturen, se http://www.iwar.org.uk/iwar/resources/us/jp3_13.pdf (2006-10-30)

activity within Department of Defense information systems and computer networks. Also called CND.

Computer network exploitation. Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. Also called CNE.

Electronic Warfare. Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called EW.

Military Deception. Actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly forces mission. Also called MILDEC. See also deception. (This term and its definition are provided for information and are proposed for inclusion in the next edition of JP 1-02 by JP 3-58.)

Operations Security. A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. identify those actions that can be observed by adversary intelligence systems; b. determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c. select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called OPSEC. (JP 1-02)

Psychological Operations. Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator’s objectives. Also called PSYOP. (JP 1-02)