Omstrukturering av Folkets befrielsearmé

Cyberrymden som militär domän påverkar Kinas försvarsmaktsreform

av Dirk Roland Haupt

Résumé

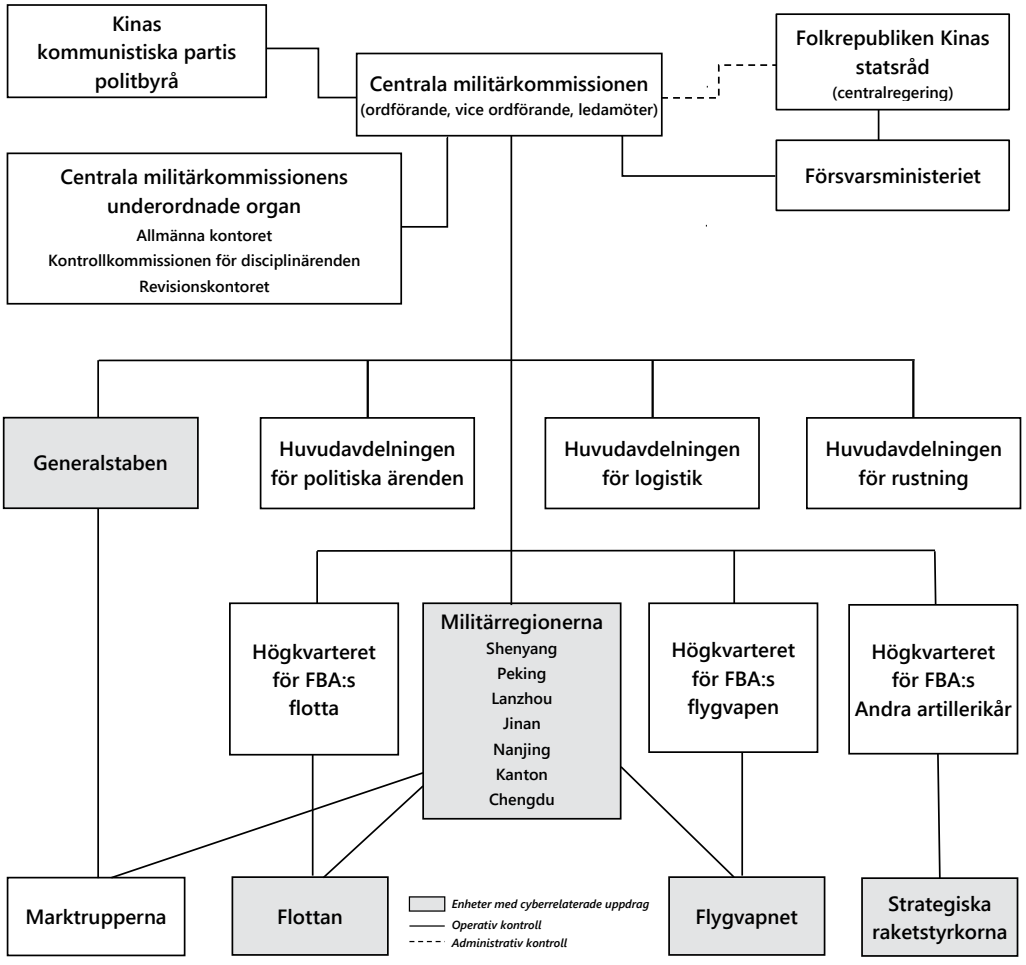
Restructuring of the People's Liberation Army (PLA) is a long-term project; launched in 2015, it is to be completed in 2020. This contribution focuses on the reform of the armed forces of the People's Republic of China inasmuch as it affects the cyber units that are re-organized in, and under, the newly established "Strategic Support Force". Applying key concepts of Chinese military doctrine such as "active defense", "informatization" and "comprehensive information dominance", the clustering of cyber units will conduce to balance various attack scenarios and to recalibrate target arrangements with respect to network and information operations. Another objective of the restructuring is the adaptation and improvement of existing procedures of attack as well as the development of new procedures and methods. These measures further complicate attribution endeavors merely relying on technical parameters to a particular grouping within the State actor's organization. The restructuring measures and the holistic development of its cyber capabilities will enhance the potential of the PLA to carry out information operations. The level of threat, by Chinese State actors, against Western information and communication systems remains high.

DEN DJUPGÅENDE OMSTRUKTURERINGEN av Folkets befrielsearmé (FBA) och dess försvarsgrenar – ett långsiktigt projekt som lanserades år 2015 och som ska vara slutfört år 2020 – påverkar de militära cyberenheter som nu dels underställs, dels koncentreras i den nyinrättade "strategiska understödsstyrkan".[1] På nätverks- och informationsoperationernas område sker en omorganisation och styrkekoncentration av cyberenheterna, som troligen kommer att användas för att balansera olika angreppsscenarion och att uppnå en ny avstämning av mål. I detta sammanhang vore det nära till hands att tro att man med omstruktureringen eftersträvar att anpassa och förbättra befintliga förfaranden samt att utveckla nya anfallsförfaranden och -metoder. Åtgärder av detta slag bidrar till att avsevärt försvåra att anfall kan tillräknas en viss gruppering inom aktörens organisation enbart på grundval av tekniska parametrar.

Här behandlas ej de s k cybermiliserna, d v s den framför allt i företag och universitet rotade organisation som stöder FBA:s aktiva enheter med säkerhetsåtgärder.[2]

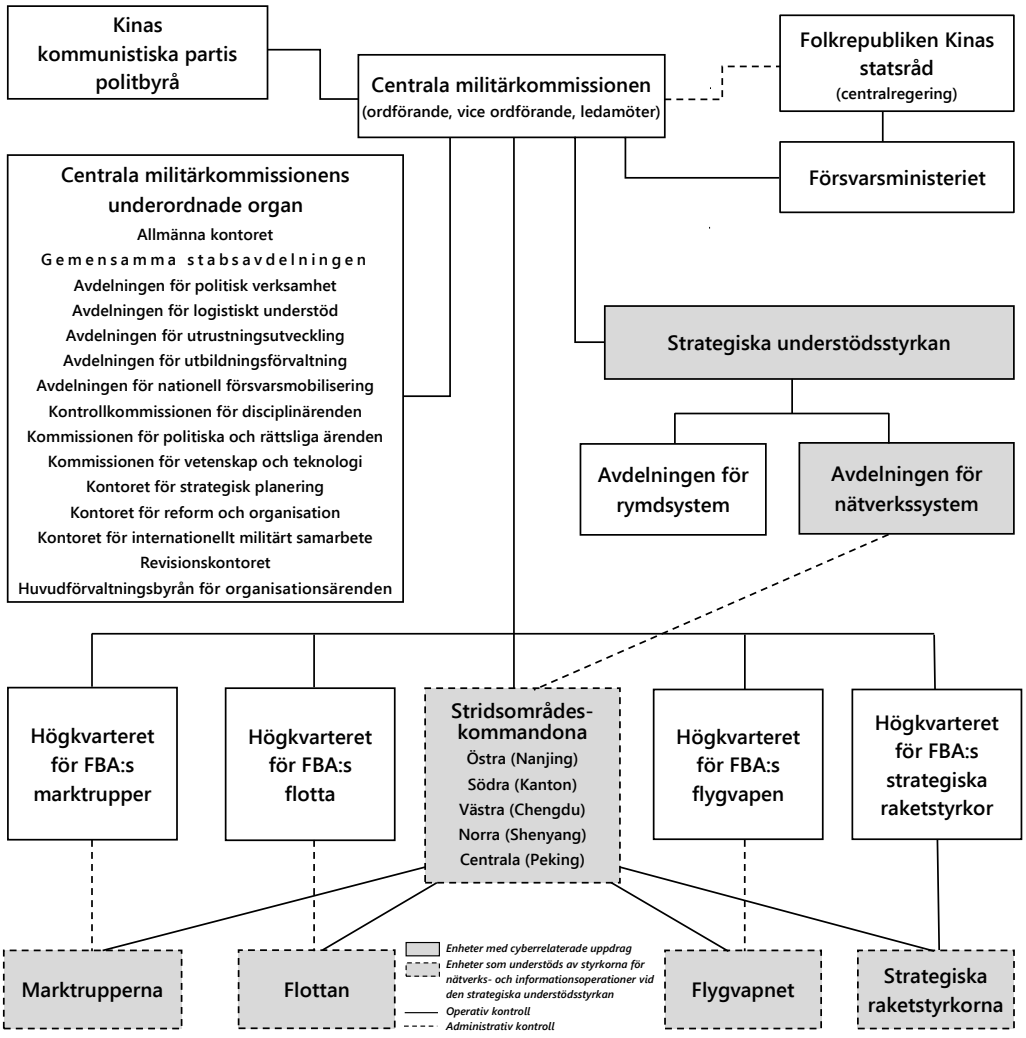
Försvarsmaktsreformen och den nya strategiska understödsstyrkan

Sedan år 2006 har Folkrepubliken Kina haft militära strukturer och specialiserade förband för cyberanfall och cybersabotage. Som framgår av figur 1[3] var dessa emellertid fördelade över samtliga försvarsgrenar och utgjorde, såvitt känt, inte föremål för en gemensam operativ ledning.[4]



Figur 1. Enheter med cyberrelaterade uppdrag i FBA:s organisation före försvarsmaktsreformen

Ledda av det ”Nationella utvecklingsprogrammet för vetenskap och teknologi på mellanlång och lång sikt (2006–2020)” är en av det kinesiska kommunistpartiets och Kinas regerings prioriteter den s k informationaliseringen[5] av Kinas civila och militära infrastruktur som ett medel för att säkerställa en fortsatt ekonomisk tillväxt, att konkurrera globalt på informations- och telekommunikationsteknikens område samt att trygga nationell säkerhet. I detta sammanhang är det inte alldeles lätt att på ett adekvat sätt översätta termen ”xìnxī huà” till svenska – eller för den delen till engelska, andra nordiska språk eller tyska. Begreppet har en mycket utbredd användning i Kina och förekommer praktiskt taget i alla officiella dokument och yttranden om cyberpolitik. Den bygger på ordet för information – ”xìnxī” – och betecknar processen att sätta aktiviteter i stånd att utföras i cyberrymden och med elektroniska medel. Den här valda översättningen ”informationalisering” respektive ”att informationalisera” må uppfattas som



Figur 2. Enheter med cyberrelaterade uppdrag i FBA:s nya organisation.

mindre elegant eller vedertagen. Emellertid förmedlar den något av den bakomliggande, bredare förståelsen i kinesiskt språkbruk, som inte på ett rättvisande sätt skulle återges med ord som ”datorisering” eller ”att datorisera”.

På en grundläggande nivå nyorienterar sig FBA för att bättre kunna föra informationaliserade krig. FBA har aldrig varit organiserad helt i överensstämmelse med västerländska arméers organisationsprinciper. Det har alltid lagts mindre tonvikt på försvarsgrenarna och större fokus på olika funktioner, inte minst den politiska. Denna skillnad kommer att växa i framtiden i takt med att FBA förbereder sig för att utkämpa informationaliserade krig. FBA berörs redan i sin helhet av den därav resulterande

översynen, inklusive vad gäller utrustningen, doktrinen, övningskulturen och organisationsskepnaden, med avseende på både den fredstida administrationen och den krigstida kommandostrukturen. Informationaliserade krig gör skiljelinjerna suddiga mellan fredstid och krigstid, mellan vad som anses militärt och vad som anses vara civilt. Enligt kinesisk uppfattning är en del av denna översyn nödvändig, för i informationsåldern är fred och krig, militärt och civilt alltmer oskiljaktiga. En konsekvens att detta synsätt är att Kina inte kan vänta tills kriget börjar med att inhämta underrättelser, påverka psykologiska stämningslägen, utveckla antisatellitsystem eller utforma cybervapen. Tvärförbindelserna mellan informationsinfrastrukturen innebär att alla dessa element är sammankopplade. Förberedelse för och genomförande av informationaliserade krig kommer därför att omfatta verksamhet i fredstid, riktade mot civila och kommersiella enheter, samt krigsoperationer mot motståndares militära system.

Informationaliserade krig är mer än bara cyberkrig; cyberkrig är bara en del av det större hela. I kinesisk syn sträcker sig informationaliserade krig bortom cyberaktiviteter och handlar istället om att i tidigast möjliga skede etablera ”omfattande informationsdominans”.[6] Detta innebär att kunna inhämta, överföra, analysera, bedöma och utnyttja information snabbare och mer exakt än motståndaren och förutsätter att både det elektromagnetiska spektrumet och den globala cybersfären behärskas, oavsett om den är politisk, ekonomisk eller militär.[7] Att uppnå omfattande informationsdominans innefattar att föra politiskt krig, som påverkar vänligt sinnade staters, motståndares och tredje parters åsikter och bedömningar. Enligt rådande kinesisk militärdoktrin om aktivt försvar[8] och om utkämpande av lokala krig under informationaliseringens förhållanden[9] beror segrar i framtida krig på att etablera egen informationsdominans, samtidigt som denna nekas motståndaren.

Informationskrigföring bestämmer på ett grundläggande sätt hur FBA ser ut, inte minst när det gäller dess organisation. Försvarsmaktsreformen, vilken beräknas ta sex år i anspråk, och de planerade förändringarna inom huvudadministrationens organisation genomgående innesluter också enheterna med cyberrelaterade uppdrag.[10] Men medan den avsedda slutliga målstrukturen ska vara intagen senast år 2020, satte presidenten XI Jinping redan den 31 december 2015 i tjänst dels de strategiska raketstyrkorna, dels den strategiska understödsstyrkan och gav därmed en särskild innehållslig accent på reformen av de väpnade styrkorna.[11] Den strategiska understödsstyrkan samlar under ett enda byråkratiskt paraply alla viktiga stridselement som FBA anser vara centrala för att föra informationskrig: rymdstyrkor, nätverksstyrkor och styrkor för elektronisk krigföring. Mot bakgrund av den organisatoriska upplösningen av den tidigare generalstaben[12] i januari 2016 hade det under tiden varit oklart, hur cyberenheterna skulle inpassas i den nya strukturen. FBA:s nya struktur och den strategiska understödsstyrkans placering inom denna framgår av figur 2.[13]

Omstruktureringens inriktning och återverkningar på FBA:s enheter med cyberrelaterade uppdrag

Den nya ”Gemensamma stabsavdelningen”,[14] ett av de femton nya kontor som är underordnade Centrala militärkommissionen, ansvarar för planering, organisation, förberedelse och

genomförande av cyberanfall, cybersabotage och cyberförsvar samt för sammanställning av mål och resultatutvärdering. Den nyetablerade strategiska understödsstyrkan är indelad i två huvudansvarsområden:[15] avdelningen för rymdsystem[16] och avdelningen för nätverkssystem.[17]

I den kinesiska militärdoktrinen är termen ”informationskonfrontation”[18] ett övergripande koncept som betecknar den integrerade användningen av element i elektronisk krigföring, datanätverksoperationer, psykologiska operationer, militär vilseledning och operativ säkerhet. Den kinesiska strategin uppfattar inte cyberrymden som en singulär domän i analogi med hur begreppets används av västerländska militärteoretiker. Uttrycket ”cyberrymd” translittereras på kinesiska med ”sài bó”[19] för att återge och analysera västerländska krigsvetenskapliga bidrag om nätverkskrig, men är annars i stort sett frånvarande i kinesiska skrifter. Det grundläggande koncept som används av kinesiska analytiker i dess ställe är förekomsten av en informationsdomän[20] vid sidan om de traditionella domänerna luft, hav, land och yttre rymd. Även om informationsdomänen definieras i breda termer i klassiska kinesiska verk såsom den av Militärvetenskapsakademin numera i tredje upplagan utgivna handboken ”Militärstrategins vetenskap”,[21] vars betydelse och inflytande inte kan skattas högt nog, betraktas domänen som sammansatt av ett antal bestämda, tydligt definierade underdomäner, såsom datanätverksdomänen, den elektromagnetiska domänen, den psykologiska domänen och det militära underrättelseväsendets domän.

Krigföring i informationsdomänen (eller informationaliserad krigföring) är, som framhållits ovan, således inte bara en synonym för krigföring i datanätverk eller för cyberkrigföring, utan snarare en holistisk beteckning som inbegriper krigföring i var och en av dessa distinkta underdomäner. I allmänhet avses sålunda en helhetssyn på anfalls- och försvarsåtgärder, baserad på premissen att ”man inte vet hur man bör försvara sig utan att förstå hur man anfaller”[22] och med målsättningen att försämra, försvåra, inskränka eller lamslå motståndarens informationsutrymme och att samtidigt skyddar den egna informationssfären.

I uppdraget för styrkorna för nätverks- och informationsoperationer ingår teknisk signalspaning, psykologisk krigföring, cyberrelaterad militär underrättelseinhämtning och -verksamhet samt nätverksoperationer. Med utgångspunkt i detta uppgiftsspektrum kan vissa härledningar göras om hur enskilda delar av den tidigare generalstaben och de tidigare underordnade huvudförvaltningarna har omgrupperats. Stora delar av den tidigare generalstabens tredje huvudförvaltning har tillförts de nya styrkorna för nätverks- och informationsoperationer.[23] På samma sätt tyder allt på att också delar av den tidigare fjärde huvudförvaltningen med ansvar för elektronisk krigföring blev en del av de nya styrkorna.[24] Inte minst de enheter som fått i uppdrag att genomföra nätverksoperationer – d v s operationer som manipulerar, avbryter, förhindrar eller förstör motståndarens åtkomst åt information på datorer, i datornätverk eller i molnet genom att använda hård- eller mjukvara – är nyuppställda.[25]

Omorganisationen är inriktad i synnerhet på de enheter och forskningsinstitut av den tidigare generalstabens tredje huvudförvaltning, som beskrivs närmare nedan. I vilken utsträckning understödsenheterna i den tidigare generalstabens tredje huvudförvaltning integrerades i den strategiska understödsstyrkan kan f n inte besvaras med säkerhet. I vart fall skulle ett sådant underordnande inte te sig ogrundat.

Enskilda enheter av särskild betydelse

En rad enheter med specifika förmågor eller uppdrag förtjänar förstärkt intresse. Uppmärksammas bör i synnerhet

- andra kontoret (enheten 61398):[26] Denna enhet, som till stor del är baserad i Shanghai, blev känd i samband med Mandiant-rapporten,[27] i vilken den fick beteckningen ”avancerat ihållande hot 1” (Advanced Persistent Threat 1; APT-1). Andra kontoret är förmodligen ansvarigt för USA och Kanada.[28] Ett avancerat ihållande hot är en långsiktig, systematisk, komplex och ofta finurligt sammansatt informationsinhämtningsoperation, som utförs i delar med hjälp av högutvecklade metoder och tekniker och som vanligtvis stöds av en statlig aktör.[29]
- fjärde kontoret (enheten 61419):[30] Kontoret i Qingdao är förmodligen ansvarigt för inhämtning av information från Japan och Korea.[31]
- femte kontoret (enheten 61565):[32] Såvitt känt har detta Peking-baserade kontor i uppdrag att inhämta underrättelser från Ryssland.[33]
- åttonde kontoret (enheten 61046):[34] Enheten, med huvudkontor i utkanten av Peking, är inriktad på den sydostasiatiska regionen, med fokus på Malaysia, Filippinerna, sammanslutningen av sydostasiatiska stater i ASEAN samt Australien.[35] Detta område är av stort intresse för FBA på grund av de territoriella tvisterna i Sydkinesiska havet.[36] Dessutom planerar kontoret antagligen även spionageattacker mot mål i Europa, Afrika, Latinamerika och Mellanöstern.[37] Åttonde kontoret är indelat i tio avdelningar, som bl a förfogar över avsevärd översättningskapacitet.[38]
- tolfte kontoret (enheten 61486):[39] Denna enhet, vars huvudlokal finns i Shanghai, är ansvarig för dels avlyssning av satellitburen kommunikation, i synnerhet från europeiska och japanska företag, dels nätverksoperationer och annan handräckning i samband med rymdövervakning samt dels översättningsuppdrag och signalspaning.[40] I denna enhet ingår ett förhållandevis stort antal filialkontor i sydöstra och södra Kina, bland vilka ett driver en anläggning för ett stort fasstyrt radarsystem.[41]

Forskningsinstitut

Följande forskningsinstitut är en del av de nya strategiska understödsstyrkorna:

- 56:e forskningsinstitutet (Forskningsinstitutet för datorteknologi i Jiangnan):[42] Detta forskningsinstitut ligger i Wuxi i Jiangsu-provinsen och sysslar med vetenskapen om högpresterande datorer. Det samverkar med Nationella universitetet för försvarsteknologi och -vetenskap[43] i Changsha, Kinas ledande försvarshögskola, som också bedriver avancerad forskning om högpresterande datorer, bl a i samband med utvecklingen av världens näst högst presterande superdator, ”Tianhe-2” (”Vintergatan 2”).[44] Dessa datorer används antagligen också i kryptografins tjänst.[45]
- 57:e forskningsinstitutet (Sydvästra institutet för elektronik och telekommunikation):[46] Detta forskningsinstitut har sitt huvudkontor i Chengdu med två filialer i Guangdong och Shuangliu.[47] Dess arbetsspektrum omfattar signal-

spaning på kortvågsbandet i spektrumet 3 till 30 MHz. Det upprätthåller forskningsförbindelser med Kinesiska akademin för rymdfärdsteknologi[48] och dess avdelning för forskning och utveckling av satellitteknik.[49]

- 58:e forskningsinstitutet (Sydvästra institutet för automation):[50] Detta institut ligger i Mianyang i Sichuan-provinsen. I sin verksamhet ägnar det sig bl a åt kryptologi;[51] med Nanjings universitet för vetenskap och teknologi[52] har institutet kommit överens om projektsamarbete.

FBA:s målstruktur

Före reformen var cyberenheterna utspridda i de tidigare militärregionernas liksom i försvarsgrenarnas organisationsstrukturer, vilket åskådliggörs i figur 1. Integrationen i den strategiska understödsstyrkans sammanhållande organisation innebär en påtaglig förändring.

Stridsområdeskommandona

Folkrepubliken Kina har hittills varit indelad i sju militärregioner.[53] Den pågående försvarsmaktsreformen medförde att militärregionerna omformades till fem stridsområdeskommandon – Norra, Södra, Östra, Västra resp Centrala stridsområdeskommandot.[54] Som framgår av figur 3 ligger de respektive högkvarteren i städerna Shenyang, Kanton, Nanjing, Chengdu och Peking.

Denna omstrukturering har hittills inte inneburit några lokala förändringar för cyberenheterna.[55] Det är snarare frågan om en ren omstrukturering inom kommandostrukturen, vilket leder till en sammanslagning av enheter som hittills tillhört olika försvarsgrenar.[56] Utplaceringen av de s k tekniska spaningskontoren, vilkas uppgiftsspektrum, förutom signalspaning, också omfattar cyberspionage, är sig därför tillsvidare lik. Värda att nämnas är enheten 75770 i Kanton, vars uppdrag gäller övervakning av anslutningar för internettelefoni, analys av skadlig programvara och högpresterande datorer, samt därutöver enheterna 78006 och 78020 i Chengdu, 66407 i Beijing, 72959 i Jinan, 68002 och 69010 i Lanzhou, 73610 och 73630 i Nanjing och 65016 i Shenyang, vilka samtliga förfogar över relevanta cyberkapaciteter.[57]

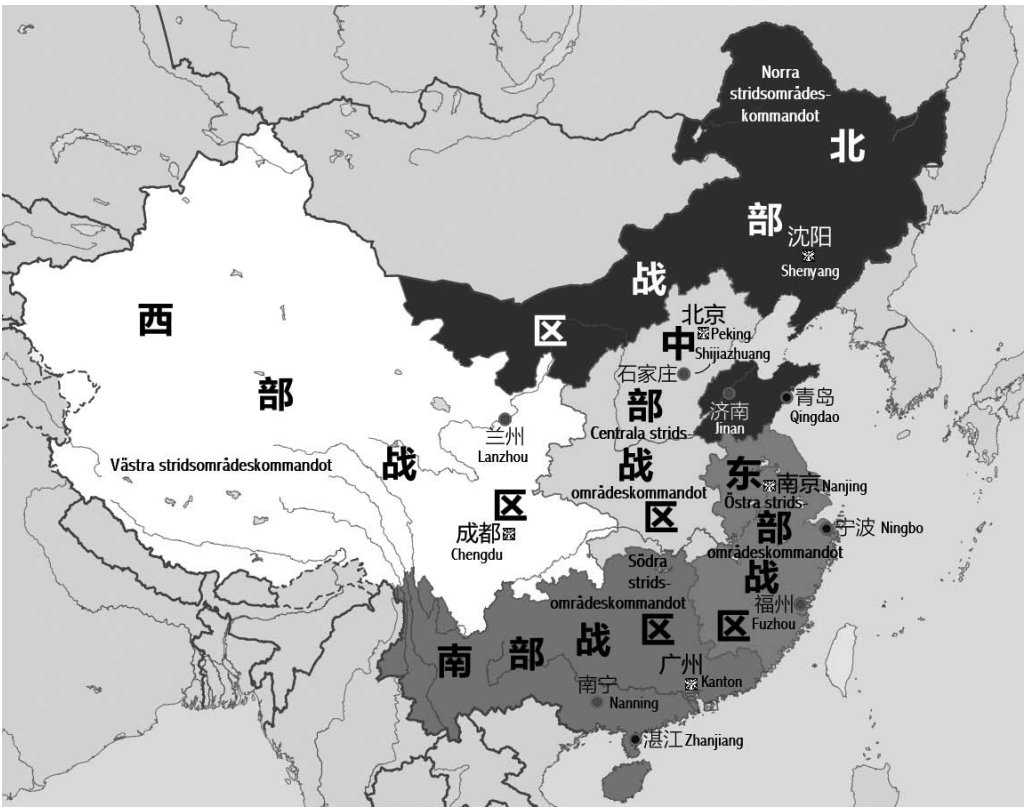
Kommunikations- och teknisk spaning på nätverksinfrastruktur som huvuduppgift fördelades enligt följande prioriteringar:[58]

- Östra stridsområdeskommandot ansvarar för Taiwan, Japan och Okinawa.
- Södra stridsområdeskommandot täcker Vietnam, Indonesien och Filippinerna.
- Västra stridsområdeskommandot ansvarar för Indien och Centralasien.
- Norra stridsområdeskommandot handlägger den japanska huvudön och den koreanska halvön.
- Centrala stridsområdeskommandot slutligen fokuserar på USA, Japan samt Nord- och Sydkorea.

Att vissa områden har uppdragsmässig dubbeltäckning är uttryckligen önskat. Däremot är det oklart, huruvida olika prioriteringar har fastställts för regioner med samma spaningsmål.

Flygvapnet, flottan och de strategiska rakettrupperna

De hos försvarsgrenarna flygvapnet, flottan och de strategiska rakettrupperna inrättade kontoren för teknisk och kommunikationsspaning har – liksom de motsvarande strukturerna hos marktrupperna – också i uppgift



Figur 3. Folkrepubliken Kinas nya stridsområdeskommandon

att bedriva cyberspionage och cybersabotage. I FBA:s flygvapens organisation ingår tre tekniska spaningskontor – det första tekniska kontoret (enheten 95830), det andra tekniska kontoret (enheten 95851) och det tredje tekniska kontoret (enheten 95879) –, medan flottan har två spaningskontor, det första tekniska kontoret (enheten 91746) och det andra tekniska kontoret (enheten 92762).[59] Dessas uppgifter består främst av militär signalspaning och informationsinhämtning i samband med kommando- och uppdragsstyrning, tidig varning och eldledning i insatsområdena i Öst- och Sydkinesiska haven och i luftrummen över dem.[60]

Vidare upprätthåller de strategiska rakettrupperna (tidigare Andra artillerikåren) ett kontor för teknisk spaning (enheten 96669).[61] Denna enhet fungerar också som en ”blå armé”, som vid övningar agerar i rollen som fiende i cyberrymden.[62] Dessutom ansvarar den för militär nätverksspaning inom områdena tidig missilvarning och flyg- och missilförsvar i förhållande till Taiwan, Japan, Indien och Sydkorea.[63]

Cyberenheternas insatser

Det går visserligen inte att leda i bevis att den minskning av detekterbara cyberanfall på europeiska mål av påstått kinesiska aktörer och den motsvarande intensifiering av cyberanfall

i Asien som kännetecknar den aktuella trenden[64] har ett visst orsakssamband med de pågående omstruktureringsprocesserna och dessas återverkning på FBA:s cyberkapacitet. Såvitt kinesiska statliga aktörer förmodas vara delaktiga, låter sig däremot både en förändring av skadlig programvara och en anpassning av cyberspionageverksamhetens taktik och procedurer påvisas.

De strukturella anpassningarna bör åtminstone temporärt påverka FBA:s cyberförmågor. Dessutom bör kunna förväntas att tillfället av cyberenheternas sammanslagning tas i akt för att justera olika anfallsscenarion och för att avstämma nya mål. Omstruktureringen kommer därutöver också att användas för att anpassa och optimera befintliga förfaranden och för att utveckla nya anfallsförfaranden och -metoder. Det ökade antalet cyberanfall som kan konstateras i den asiatiska regionen[65] verkar också användas för att testa förbättrade och samordnade förfaranden. Sannolikheten av ett samtidigt cyberanfall av två enheter mot samma mål bör därför minska i framtiden. Ytterligare en konsekvens är ett utbyte av skadlig programvara mellan olika anfallsgrupperingar och nya måluppdrag för dessa. Till exempel har företags- och forskningsmål anfallits med cybermedel som hittills företrädesvis använts mot statliga mål.[66] Genom denna utveckling försvåras tilldelningen av anfallsuppgift till en viss gruppering inom aktörens organisation på grundval av tekniska parametrar. Senast efter slutförandet av FBA:s omstrukturering måste en förbättring av både kvaliteten och mängden cyberanfall från detta håll tas med i beräkningen.

Sammanfattning

Genom att utöka sin förmåga till cyberanfall är Kina i stånd att inrikta sin signalspaning på en ökad användning av internetbaserade överföringsmetoder. För detta ändamål har cyberenheterna inom FBA:s organisation specialiserats både regionalt och tematiskt och inriktats mot att följa en strategisk orientering. Förekomsten av militära forskningsanläggningar som bedriver cyberinriktad utvecklingsverksamhet, liksom förbindelserna med vissa civila universitet, skapar förutsättningarna för en fortsatt holistisk teknisk utveckling och för en adekvat utbildning av den militära personalen. Att behålla och utveckla FBA:s förmåga till cyberspionage kommer även i framtiden att vara en hög prioritet.[67] Genom sina kapaciteter är Kina i stånd till att punktuellt påverka informations- och kommunikationssystem på geografiskt avlägsna platser och att därifrån inhämta tillgängliga data. Omstruktureringsåtgärderna och den fortsatta expansionen av dessa förmågor med målsättningen att nå militär och civil informationsdominans kommer att ytterligare stärka Kinas potential.[68]

I det övergripande perspektivet kommer hotet mot västerländska informations- och kommunikationssystem genom cyberanfall som härrör från kinesiska statliga aktörer att ligga kvar på en hög nivå och kan även komma att öka när försvarsmaktsreformen så småningom konsolideras.[69]

Författaren är jur lic.

Noter

1. På kinesiska: Zhōngguó rénmín jiěfàngjūn zhànlüè zhīyuán bùduì, 中国人民解放军战略支援部队.
2. Sheldon, Robert och McReynolds, Joe: ”Civil-Military Integration and Cybersecurity. A Study of Chinese Information Warfare Militias” i Lindsay, Jon R; Cheung, Tai Ming och Reveron, Derek S: *China and Cybersecurity. Espionage, Strategy, and Politics in the Digital Domain*, Oxford University Press, New York 2015, s 188-222. – Nigel Inkster, som undrar huruvida cybermiliserna skulle kunna uppfattas som en modern fortsättning av den maoistiska doktrinen om ”folkets krig”, framhåller visserligen att cybermilisernas nytta är omtvistad även i Kina och att fortfarande mycket lite är känt om dessas slagkraft; Inkster, Nigel: *China's Cyber Power*, International Institute for Strategic Studies, London 2016, s 93 och 104. Ur öppna källor har Sheldon och McReynolds, ibid, s 212-218, gjort en sammanställning av ett åttiotal cybermilisenheter, vilkas förankring i Kinas näringsliv och forskningsvärld ger en antydan om deras potentiella betydelse som reservstyrka.
3. Denna figur är en bearbetning av figur 1 i Saunders, Phillip C och Wuthnow, Joel: “China's Goldwater-Nichols? Assessing PLA Organizational Reforms”, *Strategic Forum*, nr 294 2016, s 2, *http://ndupress.ndu.edu/Portals/68/Documents/stratforum/SF-294.pdf*. (2017-07-02)
4. Op cit, Sheldon, Robert och McReynolds, Joe, se not 2, s 199.
5. På kinesiska: xìnxī huà, 信息化.
6. På kinesiska: quánmiàn de zhì xìnxī quán, 全面的制信息权.
7. Op cit, Inkster, Nigel, se not 2, s 99-105. – Den 27 december 2004 publicerade den kinesiska regeringen en s k vitbok om Kinas nationella försvar år 2004 [“2004 Nián Zhōngguó de guófáng” báipíshū, 《2004年中国的国防》白皮书]. I dess kapitel II om nationell försvarspolitik anfördes bl a att ”Kina följer den militära strategin av aktivt försvar och arbetar för att påskynda revolutionen i militära angelägenheter med kinesiska särdrag: Att ta den sammansatta utvecklingens väg som gör det möjligt att hoppa över flera utvecklingsfaser. Genom att gå i takt med världens militära utveckling och att röra sig i riktning mot informationaliseringen i moderniseringsprocessen ska Folkets befrielsearmé gradvis uppnå övergången från mekanisering och halvmekanisering till informationalisering”, i ”China's National Defense in 2004”, State Council Information Office, Peking 2004, *http://www.china.org.cn/e-white/20041227/II.htm*. (2017-07-02)
8. På kinesiska: zhǔdòng quán, 主动权 eller jījí fángyù, 积极防御.
9. På kinesiska: xìnxī huà tiáojiàn xià júbù zhànzhēng, 信息化条件下局部战争.
10. Cheng, Dean: *Cyber Dragon. Inside China's Information Warfare and Cyber Operations*, Praeger, Santa Barbara/Denver 2017, s 193-199.
11. Buchas, Peter: ”Bedrohungswahrnehmungen und sicherheitspolitische Konzepte Chinas”, *Sicherheit und Frieden*, nr 3 2016, s 182-184.
12. Se utförligt härom op cit, Cheng, Dean, se not 10, s 178-190.
13. Denna figur är baserad på figur 2 i op cit, Saunders, Phillip C och Wuthnow, se not 3, s 3, vilken dock uppdaterats med avseende på den strategiska understödsstyrkans organisation och institutionella ställning.
14. På kinesiska: jūnwěi liánhé cānmóu bù, 军委联合参谋部.
15. Kania, Elisa: ”PLA Strategic Support Force: The 'Information Umbrella' for China's Military”, *The Diplomat*, 2017-04-01, *http://thediplomat.com/2017/04/pla-strategic-support-force-the-information-umbrella-for-chinas-military/*. (2017-07-02)
16. På kinesiska: hángtiān xìtǒng bù, 航天系统部.
17. På kinesiska: wǎngluò xìtǒng bù, 网络系统部.
18. På kinesiska: xìnxī duìkàng, 信息对抗. Se närmare härom op cit, Inkster, Nigel, se not 2, s. 99.
19. Med kinesiska skrifttecken: 赛博. Ibid, s 23 fotnot *.
20. På kinesiska: xìnxī lǐngyù, 信息领域. Se utförligt härom op cit, Sheldon, Robert och McReynolds, Joe, se not 2, s 197 f.
21. SHOU Xiaosong [寿晓松] (red): *Zhànlüè xué* [战略学, *Militärstrategins vetenskap*], Jūnshì kēxué chūbǎn shè [军事科学出版社, Militärvetenskapliga förlaget], Peking 2013 (tredje uppl).
22. På kinesiska: bù dǒng jìngōng jiù bù huì fángshǒu, 不懂进攻就不会防守. Se härom (1) Stokes, Mark A: ”The Chinese People's

Liberation Army Computer Network Operations Infrastructure" i op cit, Lindsay, Jon R; Cheung, Tai Ming och Reveron, Derek S, se not 2, s 165 och s 178 not 9, och (2) op cit, Cheng, Dean, se not 10, s 139.
23. Op cit, Cheng, Dean, se not 10, s 194. För en mycket ingående analys av den tidigare generalstabens tredje och fjärde huvudförvaltningar se op cit, Stokes, Mark A, se not 22, s 163-187.
24. Op cit, Cheng, Dean, se not 10, s 194.
25. Op cit, Inkster, Nigel, se not 2, s 100-105, och op cit, Saunders, Phillip C och Wuthnow, Joel, se not 3, s 8.
26. Op cit, Stokes, Mark A, se not 22, s 170 f.
27. *APT1. Exposing One of China's Cyber Espionage Unit*s, Mandiant FireEye, Milpitas CA 2013, *https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf*. (2017-07-02)
28. Op cit, Stokes, Mark A, se not 22, s 170.
29. Ett dylikt hots livscykel beskrivs i op cit, *APT1*, se not 27, s 27-38. I denna rapport beskrivs avancerade ihållande hot som enheter som i smyg och långvarigt utnyttjar datanätverk med målinriktning på specifika organisationer. Dessa hot kräver förberedande underrättelseinhämtning för att kunna forcera målspecifikt försvar i syfte att identifiera och avleda användbart datamaterial. Denna målinriktade verksamhet skiljer avancerade ihållande hot från sådan cyberbrottslighet som inriktar sig på att tillfoga ett stort antal användare skada i en engångsgärning. De flesta avancerade ihållande hot uppnår ett initialt komprometterande av målnätverket genom sociala tekniker eller missbruk av förtroende. När väl cyberoperationen fått fotfäste, tillskansar sig anfallaren privilegier i systemet, rekognoscerar nätverket och exfiltrerar data till ledningssystem på internet, många gånger i flera led förlagda till olika jurisdiktioner.
30. Op cit, Stokes, Mark A, se not 22, s 171.
31. Op cit, Cheng, Dean, se not 10, s 182.
32. Op cit, Stokes, Mark A, se not 22, s 171.
33. Op cit, Cheng, Dean, se not 10 s 182.
34. Op cit, Stokes, Mark A, se not 22, s 172. Enheten hade tidigare täckkoden 57318.
35. Ibid.
36. Om dessa territoriella tvister se Kiesow, Ingolf: "Kina vill expandera till havs", *KKrVAHT*, 1. häftet 2014, s 40-47.
37. Op cit, Stokes, Mark A, se not 22, s 172. I översikten över kontoren i op cit, Cheng, Dean, se not 10, s 182, saknas uppgiften om att åttonde kontoret är inriktat på mål i Europa, Afrika, Latinamerika och Mellanöstern. Detta tycks emellertid vara ett förbiseende, eftersom huvudkällan för denna översikt uppges vara Stokes, Mark A; Lin, Jenny och Hsiao, L C Russell: *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure*, Project 2049 Institute, Arlington VA 2011, *https://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf* (2017-07-02), som dock i sin tur antecknar denna regionala behörighet (på s 10 med utförliga källhänvisningar).
38. Ibid, s 184 not 65.
39. Op cit, Stokes, Mark A, se not 22, s 172.
40. Op cit, Cheng, Dean, se not 10, s 182.
41. Op cit, Stokes, Mark A, se not 22, s 173 och s 185 not 77.
42. På kinesiska: Jiāngnán diànnǎo kējì yánjiū suǒ, 江南电脑科技研究所. Se utförligt härom op cit, Stokes, Mark A; Lin, Jenny och Hsiao, L C Russell, se not 37, s 5.
43. På kinesiska: guófáng kēxué jìshù dàxué, 国防科学技术大学.
44. Närmare om superdatorn "Vintergatan 2" se Liao, Xiangke; Pang, Zhengbin och Wang, Kefei m fl: "High Performance Interconnect Network for Tianhe System", *Journal of Computer Science and Technology*, nr 2 2015, s 259-272.
45. Bouillaguet, Charles; Cheng, Chenmou och Chou, Tung m fl: "Fast Exhaustive Search for Quadratic Systems in $\mathbb{F}_2$ on FPGAs" i Lange, Tanja; Lauter, Kristin och Lisoněk, Petr (red): *Selected Areas in Cryptography – SAC 2013*, Springer, Heidelberg/New York NY/Dordrecht/London 2014, s 221. FPGAs är en förkortning för "field-programmable gate arrays", d v s integrerade kretsar som används inom digitalteknik och vilkas fysiska funktion kan ändras genom att ny programmering översänds genom anslutning av en enkel kabel. $\mathbb{F}_2$ betecknar en ändlig Galloiskropp med två element. Ändliga (Gallois-) kroppar är algebraiska strukturer som tillämpas inom kryptologin.
46. På kinesiska: Xīnán diànzǐ diànxìn jìshù yánjiū suǒ, 西南电子电信技术研究所.
47. Op cit, Stokes, Mark A; Lin, Jenny och Hsiao, L C Russell, se not 34, s 5.
48. På kinesiska: Zhōngguó kōngjiān jìshù yánjiù yuàn, 中国空间技术研究院.
49. Op cit, Stokes, Mark A, se not 22, s 167 och s 179 not 17.

50. På kinesiska: Xīnán zìdònghuà yánjiū suǒ, 西南自动化研究所
51. Op cit, Stokes, Mark A; Lin, Jenny och Hsiao, L C Russell, se not 37, s 5.
52. På kinesiska: Nánjīng lǐgōng dàxué, 南京理工大学
53. På kinesiska: dà jūnqū, 大军区.
54. På kinesiska: zhànqū, 战区. Det kineskiska begreppet kan översättas på flera olika sätt, bl a med ”stridsområde”, ”krigszon” eller ”strategisk region”. Av försvarsmaktsreformens inriktning framgår emellertid att den nya terminologin avser det horisontella kommandot över ett stridsområde, varför detta bidrag använder termen ”stridsområdeskommando” i avgränsning mot den tidigare beteckningen ”militärregion”. För en analys av försvarsmaktsreformens målsättning och geografiska innebörd samt den därmed sammanhängande nya terminologin se också op cit, Saunders, Philip C och Wuthnow, Joel, se not 3, s 5-9 samt not 8 på s 9.
55. Författarens samtal i Peking 2016-10-20-22 och i Hangzhou 2016-11-14-16 med befattningshavare inom FBA, som bett att inte bli citerade med namn och rangbeteckning.
56. Om enheternas femsiffriga täckkoder kommer att ändras efter att omstruktureringen slutförts, är oklart i nuläget. När den logiska uppbyggnaden av täckkodssystemet frångicks år 2002, verkar enheternas täckkodning ha blivit mer slumpartad. Det får således avvaktas, huruvida FBA anser att de enskilda enheterna så småningom måste omkodas. Se också op cit, Cheng, Dean, se not 10, s 183.
57. Op cit, Stokes, Mark A; Lin, Jenny och Hsiao, L C Russell, se not 37, s 12 f.
58. GUO Yuandan [郭媛丹]: ”Zhuānjiā: Wǔdà zhànqū mùbiāo qīngxī dōngnán yánhǎi shì zuòzhàn zhòngdiǎn” [专家：五大战区目标清晰 东南沿海是作战重点. Experter: De fem stridsområdeskommandona har klara mål, den sydöstra kustens front är fokusen för framtida militära operationer], *Huánqiú shíbào* [环球时报, *Globala tider*] 2016-02-02, *http://mil.huanqiu.com/observation/2016-02/8489177.html*. (2017-07-02); Dean Cheng anser att avgränsningen mellan Norra, Östra och Södra stridsområdeskommandonas ansvarsområden i många avseende fortfarande är oklar, op cit, Cheng, Dean, se not 10, s 197 och s 215.
59. Op cit, Stokes, Mark A, se not 22, s 179 noter 81 och 82.
60. Op cit, Stokes, Mark A; Lin, Jenny och Hsiao, L C Russell, se not 37, s 14 och s 30 not 146; Friedberg, Aaron L: *A Contest for Supremacy. China, America and the Struggle for Mastery in Asia*, W W Norton & Company, New York 2011, s 7.
61. Ibid, s 14.
62. Krekel, Bryan: *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, Northrop Grumman, McLean VA 2009, s 17 f jämte not 28 på s 28, *http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-030.pdf*. (2017-07-02)
63. Cordesman, Anthony H och Kendall, Joseph: *The PLA Rocket Force. Evolving Beyond the Second Artillery Corps (SAC) and Nuclear Dimension*, Center for Strategic and International Studies, Washington DC 2016, s 12 f, *https://csis-prod.s3.amazonaws.com/s3fs-public/publication/161013_China_Missile_Forces_AHC.pdf*. (2017-07-02)
64. Op cit, Cheng, Dean, se not 10, s 183.
65. ”Dramatic Increase in Cyber-Attacks on Companies in Asia Pacific”, *Israel Defense* 2016-09-08, *http://www.israeldefense.co.il/en/content/dramatic-increase-cyber-attacks-companies-asia-pacific*. (2017-07-02)
66. Walters, Riley: ”Cyber Attacks on U.S. Companies in 2016”, *The Heritage Foundation Issue Brief*, nr 4636 2016-12-02, *http://www.heritage.org/defense/report/cyber-attacks-us-companies-2016*. (2017-07-02)
67. Op cit, Inkster, Nigel, se not 2, s 16.
68. Hansen, Simon: ”China's Emerging Cyberpower: Elite Discourse and Political Aspirations” i Lewis, James A och Hansen, Simon: *China's Cyberpower. International and Domestic Priorities*, Australian Strategic Policy Institute, Barton 2014, s 12 och 19 f, *https://www.aspi.org.au/publications/chinas-cyberpower-international-and-domestic-priorities/SR74_China_cyberpower.pdf*. (2017-07-02)
69. Jfr Mattis, Peter: ”Three Scenarios for Understanding Changing PLA Activity in Cyberspace”, *China Brief. A Journal of Analysis and Information*, band XV nr 23 2015, s 6-10, *https://jamestown.org/wp-content/uploads/2015/12/CB_15_23_1.pdf*. (2017-07-02)