BRIEF
NO. 2 2025

NATIONELLT KUNSKAPSCENTRUM OM KINA

Kinesisk underrättelseverksamhet: en översikt

Perry Johansson Vig

Sammanfattning

- Kinesiskt underrättelsearbete har under de senaste decennierna expanderat i omfattning och komplexitet och utgör i dag ett växande säkerhetshot mot västliga demokratier. Denna rapport ger en översikt av den kinesiska underrättelseverksamhetens organisation, metoder och mål, med särskilt fokus på dess globala räckvidd, sofistikerade tekniska utveckling och politiska drivkrafter.
- Kinas underrättelseverksamhet är nära sammanflätad med kommunistpartiets maktbevarande och präglas av en leninistisk säkerhetskultur där statens säkerhet likställs med partiets stabilitet. I stället för att begränsas till traditionellt spionage riktat mot andra staters försvarsmakter omfattar den kinesiska verksamheten även systematiskt industrispionage, cyberattacker, påtryckningar mot utländska medborgare och övervakning av kinesiska dissidenter i exil.
- Rapporten belyser huvudaktörerna i Kinas underrättelseapparat – bland annat Folkets befrielsearmé, ministeriet för statssäkerhet (MSS), ministeriet för offentlig säkerhet (MOS) samt det inflytelserika partiorganet Enhetsfronten – och visar hur dessa aktörer agerar genom både statliga och privata kanaler. Särskild vikt läggs vid den nya underrättelselagstiftningen från 2017 och dess långtgående krav på samarbete som ställs på alla kinesiska medborgare och organisationer, även i utlandet.
- En särskild del av rapporten behandlar det kinesiska cyberspionaget, som i dag är den mest expansiva och aggressiva delen av Kinas underrättelseverksamhet. Genom avancerade cyberoperationer har kinesiska aktörer systematiskt stulit känslig information från västvärldens myndigheter, företag och forskningsinstitut.
- Sammantaget visar rapporten att Kinas underrättelseverksamhet inte bara är ett säkerhetshot i klassisk mening utan även ett uttryck för ett geopolitiskt projekt med ambitionen att forma det internationella systemet i en riktning mer gynnsam för auktoritärt styre. Detta kräver uppmärksamhet, motståndskraft och ett strategiskt säkerhetstänkande även från mindre länder som Sverige.

Varför oroa sig för kinesiskt spioneri?

År 2020 meddelade FBI-chefen Christopher Wray den amerikanska senatens underrättelsekommitté att byrån inledde ett nytt Kinarelaterat kontraspionageärende var tionde timme.[1] Två år senare beskrev Wray den kinesiska staten som drivande kraft bakom världens mest omfattande hackningskampanjer.[2] Chefen för Storbritanniens underrättelsetjänst MI5, Ken McCallum, förklarade året därpå det kinesiska industrispionaget mot väst såsom varande av ”episka proportioner”.[3]

Dessa och liknande uttalanden kan verka alarmerande. Den omfattning som kinesiskt spioneri har uppnått de senaste åren behöver dock inte i sig själv ge upphov till panik. Att samla information om andra stater är en grundläggande del av varje lands underrättelseverksamhet.[4] I själva verket kan underrättelseverksamhet bidra till ökad säkerhet genom att minska okunskapen om andra staters intentioner, vilket i sin tur kan förhindra farliga missförstånd och förhastade beslut. Att Kina, givet sin storlek och globala betydelse, ägnar stora resurser åt underrättelseverksamhet är därför inte i sig förvånande.

Men det finns skillnader mellan olika former av spioneri. Vissa stater använder sina säkerhetstjänster inte uteslutande för att skydda nationen utan även för att förfölja politiska dissidenter och regimkritiker utomlands.[5] Sedan har vi den lilla exklusiva grupp stormakter som inte bara ser som sin uppgift att trygga sitt land och sin regi utan dessutom har geopolitiska ambitioner att ändra andra länders politiska system, ja ibland hela världsordningen. Dagens Kina är en sådan stormakt.

Att beskriva den kinesiska underrättelseverksamheten

Syftet med de följande sidorna är att presentera en genomtänkt översikt på svenska om kinesisk underrättelseverksamhet. Fokus ligger på organisationer, metoder och mål.[6] Jag vill samtidigt säga något om hur spioneriet och säkerhetshoten i världen har förändrats, vad det innebär för vår nära framtid och för möjligheterna att skydda oss mot potentiellt kinesiskt spioneri. Det material som ligger till grund för denna översikt är såväl forskningsmonografier och artiklar som rapporter från tankesmedjor och statliga säkerhetstjänster samt ett stort antal fall av spioneri och cyberattacker som det rapporterats om under de senaste fem åren.

Underrättelseverksamheten är endast en del av en stats hela säkerhetsapparat och brukar sägas bestå av tre delar: analys, inhämtning och hemliga operationer.[7] I den här genomgången har begränsningen gjorts till inhämtningsdelen. Analysdelen är svår att veta något om vad gäller Kina.[8] I det kinesiska specialfallet är underrättelseinhämtning dessutom tätt sammanvävt med andra för regimen säkerhetsskapande aktiviteter, som propaganda och annan informationspåverkan, samt också direkta påtryckningsmedel. I den här rapporten har valet varit att försöka särа på dessa två områden inom kinesiskt säkerhetsarbete: spioneri och påverkan. Detta betyder inte att jag anser att spioneriet är mer betydelsefullt för Kinas geopolitiskt revisionistiska ambitioner. Tvärtom! Det handlar, precis som avgränsningen kring inhämtning, om de arbetsmässiga ramarna kring detta projekt. Flera rapporter på svenska om kinesiskt påverkansarbete har dessutom redan skrivits av Nationellt kunskapscentrum om Kina.[9]

Säkerhetstänkandet i en leninistisk enpartistat

I ett i grunden laglöst internationellt system där man inte kan känna andra länders verkliga intentioner behövs en underrättelsetjänst för att försöka ta reda på just detta och annan information som kan stärka den egna säkerheten.[10] Samtidigt behövs i de länder som utsätts för spioneri ett kontraspionage för att förhindra att motståndaren skaffar sig ett sådant informationsövertag. Detta är generella självklarheter som gäller alla länder. Det speciella med kommunistiskt ledda stater är att de kom till i en förmodad revolutionär situation, där inte bara andra enskilda länder sågs som potentiella hot utan där hela den ”kapitalistiska” världen utgjorde en existentiell fiende från vilken man måste vänta sig en attack och som ett kommunistiskt parti i en pågående världsrevolution i slutändan skulle förgöra, eller i alla fall bistå till att kasta över ända.[11]

Eftersom Kina är en så kallad leninistisk stat lyder den kinesiska säkerhetsapparaten inte, som i demokratiska rättsstater, under statliga institutioner och lagar mer än på ett formellt eller tekniskt plan. Den tjänar i stället främst Kinas kommunistiska parti (KKP).[12] Säkerhetsapparaten tjänar inte främst till att upprätthålla den nationella säkerheten utan den politiska, det vill säga att säkra kommunistpartiet vid makten. Därför har de styrande låtit den utrikes riktade underrättelsetjänsten tillsammans med den inrikes säkerhetspolisiära apparaten anta enorma dimensioner. En underrättelsetjänsteman från ett icke uppgivet västland uppskattar att Kina har omkring 600 000 människor som arbetar med underrättelseverksamhet och säkerhetsfrågor, betydligt fler än någon annan stat i världen.[13]

Trots sin styrka är Kinas kommunistiska parti ändå oroligt för sin egen överlevnad.[14] Det fruktar kanske inte en direkt invasion från USA, men tror att USA vill störta partiet från makten. Därför misstänker Peking utländsk inblandning i allt från demokratisträvanden till protester kring socialt missnöje. Partiets ömtålighet påverkar även utanför Kinas gränser, med skarpa reaktioner på kritik och med omfattande övervakning av olika exilgrupper. Man spionerar på såväl tibetanska och uiguriska exilgrupper som de individer som flytt från Hongkong. Man infiltrerar även de kinesiska studentföreningarna i utlandet samt alla försök till politisk organisering mot partiet av kineser.[15]

Ömtåligheten hos världens mäktigaste politiska parti har tilltagit under Xi Jinpings (习近平) ledning (2012–) och partiet har fokuserat starkt på säkerhetsfrågor de sista åren. Chen Yixin (陈一新), chef för ministeriet för statssäkerhet (MSS), har betonat att det är politisk säkerhet som har högsta prioritet. Att skydda KKP:s ledarskap är centralt för MSS. Partiets politiska stabilitet går före allt annat i det kinesiska säkerhetstänkandet.[16] Därmed inte sagt att den kinesiska underrättelseverksamheten enbart är av defensiv karaktär. Somdet förklarades i inledningen är Kina en stormakt med globala anspråk, och mycket av dess underrättelseinhämtning, även dess illegala rekrytering av spioner, rör sig numera kring geopolitiska ambitioner riktade mot utlandet.

Den kinesiska underrättelseapparatens olika enheter

Folkets befrielsearmé

Under Mao Zedongs (毛泽东) styre (1949–1976) var det främst Kinas ambassader och även nyhetsbyråer och tidningsredaktioner utomlands som härbärgerade kinesiska underrättelseofficerare. Deng Xiaoping (邓小平), som tog makten i slutet av 1970-talet, lierade sig med militären som sedan dess kommit att stå för mycket av underrättelsearbetet mot utlandet. Folkets befrielsearmé ägnade sig också, i en tid när korruptionen bredde ut sig, åt industrispionage för egen vinnings skull. Även om det finns en rad organisationer inom befrielsearmén – varje vapenslag har sin egen – som ägnar sig åt underrättelseverksamhet är det kanske Högkvarterets underrättelsebyrå (The Intelligence Bureau of the Joint Staff Department of the Central Military Commission) som bäst kan jämföras med svenska Must.[17]

Det militärt administrerade spioneriet hyser naturligtvis som alltid ett stort intresse för andra länders vapenutveckling och militärteknik. År 2014 åtalades till exempel en kinesisk affärsman bosatt i Kanada för att ha hjälpt hackare knutna till den kinesiska militären att komma över ritningar till olika amerikanska militärplan.[18] Förutom avancerad amerikansk militärteknik fokuserar Kina stor del av sin militära underrättelseverksamhet mot Taiwan. För inte alltför länge sedan, i augusti 2024, föll domarna mot medlemmarna i vad som beskrivs som en tio man stor spionring av taiwanesiska militära officerare som rekryterats till att, mot betalning, lämna över hemligstämplat material om Taiwans försvarsanläggningar och försvarsplanering inför en attack från Kina. I fråga om en av spionerna har man fastslagit att de som skötte rekryteringen hade kopplingar till den kinesiska militären. En identifierades som general medan den andra var befälhavare för militärregionen Guangzhou.[19]

Ministeriet för statssäkerhet

Forskningen om underrättelsetjänster brukar dela upp dessa i tre kategorier.[20] Först de riktade mot utlandet, sedan de vars verksamhet fokuserar på inrikes arbete. De amerikanska CIA och FBI skulle kunna stå modell för dessa två. Slutligen talar man om en tredje kategori av underrättelsetjänster som ”unitära”, det vill säga de kombinerar inrikes och utrikes underrättelseverksamhet. Det forna KGB skulle vara en sådan organisation. Även om Kinas kommunistiska parti historiskt lånat det mesta av sin organisation och verksamhet från Sovjetunionen har man aldrig försökt skapa en säkerhetsorganisation modellerad helt på KGB. I dag sköts säkerhetsarbete och den polisiära verksamheten av två myndigheter vars uppgifter till viss del i stället liknar FBI och CIA. Den kinesiska motsvarigheten till CIA skulle då vara ministeriet för statssäkerhet (MSS), som dock vad gäller just underrättelseverksamhet och kontraspionage har mer omfattande befogenheter än CIA.

MSS högkvarter i Peking representeras på provinsnivå och kommunal nivå, och det är de regionala utlöparna som sköter huvuddelen av underrättelseinsamlingen genom att övervaka stater som de har historiska, geografiska eller kommersiella förbindelser med.[21] Shanghais statliga säkerhetsbyrå ägnar sig främst åt spioneriverksamhet gentemot USA. Zhejiangbyrån fokuserar på västra Europa inklusive Storbritannien medan Tianjinbyrån samlar in information om Japan och Sydkorea. Guangdongbyrån fokuserar på Sydostasien.

Ministeriet för offentlig säkerhet

MSS systerorganisation, ministeriet för offentlig säkerhet (MOS), har de inre hoten som sin huvuduppgift. MSS sköter i och för sig också kontraspionaget inom Kinas gränser men MOS har till uppgift att övervaka utlänningar i Kina samt handhar också de religiösa rörelserna i landet inklusive falungong.[22] MOS är dessutom ibland involverat i utrikes underrättelseverksamhet och vissa mer offensiva verksamheter, speciellt mot kineser som av olika anledningar flytt från Kina.[23] MOS har till exempel skött operation ”Fox Hunt” samt den ansamling av över hundra kinesiska ”polisstationer” som upptäckts runt om i världen under senare tid vilka båda haft till uppgift att föra hem kineser med olika tvångs- och påtryckningsmetoder.[24] För den här verksamheten och för att infiltrera, spionera på och påverka den kinesiska exilen har inte bara MOS utan också den mycket omfattande kinesiska enhetsfrontorganisationen spelat en viktig roll.[25]

Enhetsfronten

Den kinesiska enhetsfronten, officiellt känd som Centrala avdelningen för enhetsfronten, är en avdelning inom Kinas kommunistiska parti (KKP) som har till uppgift att främja partiets intressen genom samarbete och påverkan, både inom landet och internationellt. Den är ett centralt verktyg för Kinas kommunistiska parti för att säkerställa makt och inflytande både nationellt och internationellt. Genom opinionspåverkan, samarbete med olika aktörer, rekrytering av stödjande individer och strategisk infiltration arbetar Enhetsfronten för att främja KKP:s mål och hantera kritik mot regimen. Enhetsfrontsarbetet, som under Xi Jinping upplevt något av en renässans, fungerar särskilt bra för spioneri eftersom frontens organisationer täcker många verksamheter för kineser utomlands, vilket ger spioner en utmärkt täckmantel.[26]

Privata aktörer

Organisationer liknande Enhetsfronten är ovanliga i andra länder än de leninistiskt organiserade. Ett andra kännetecken för kinesiskt spioneri, vid sidan av enhetsfronten, är hur den kinesiska staten, ofta via MSS, anlitar privata cyberföretag för att komplettera sin underrättelseverksamhet.[27] Detta upplägg ger kinesiska säkerhetsbyråer exklusiv tillgång till sårbarheter som identifierats av Kinas främsta civila hackare och gör att partiet kan lägga ut sin spionageverksamhet på privata entreprenörer. Den omfattande internetläckan från it-företaget I-soon 2024 gav detaljerad information som beskrev hur den kinesiska statliga säkerhetstjänsten lade ut beställningar på informationsinhämtning via hackning.[28] Den anonyma hackergruppen Intrusion Truth har också, genom åren, låtit publicera många av sina stora avslöjanden om denna statlig-privatkommersiella cyberspioneriverksamhet som Kina bedriver mot utlandet.[29] Framför allt har de, med namn och allt, lyckats avslöja ett antal av de personer som ligger bakom attackerna.

Sammanblandningen i Kina mellan vad som är statlig offentlig verksamhet och vad som är privat går dock mycket längre än så här. År 2017 införde Kina en ny ”nationell underrättelselag” som syftar till att stärka det nationella underrättelsearbetet och skydda den nationella säkerheten samt nationella intressen. Lagen fastställer en rättslig grund för underrättelsemyndigheter att genomföra operationer både inom landet och utomlands. Lagen betonar att alla organisationer och medborgare är skyldiga att stödja och samarbeta med nationella underrättelseinsatser. Denna breda skyldighet väcker oro över hur den kan tillämpas på individer och organisationer, inklusive utländska enheter som verkar i Kina. MSS-chefen Chen Yixin förtydligade den 15 april 2024 (på Kinas nationella

säkerhetsdag) att det var nödvändigt att ”mobilisera hela samhället och föra ett folkets krig för att upprätthålla nationell säkerhet”.[30] Kanske är beskrivningen av Kina som en ”underrättelsestat” av tidigare operations- och underrättelsechefen för MI6, Nigel Inkster, inte så extrem som den först kan verka.[31]

Cyberspionage

Inom forskningen kring underrättelseverksamhetens historia brukar man tala om ett ”Dreadnought moment”.[32] Detta skulle ha inträffat när internet gjorde cyberspionage möjligt och nästan över en natt helt ändrade huvudmetoderna för spioneri, påverkansarbete och sabotage.

Även om klassiska underrättelse- och påverkansaktiviteter i utlandet fortfarande är vanligt förekommande från kinesisk sida så har cyberspionage blivit den alltmer dominerande formen av informationsinhämtning. Det är så mycket mer effektivt än mer traditionella metoder. Enligt European Repository of Cyber Incidents – ett oberoende forskningskonsortium som tillhandahåller vetenskaplig analys av cyberincidenter – var Kina det land i världen som stod för det största antalet cyberattacker mellan 2005 och 2023.[33] Den svenska säkerhetspolisen har på ett liknande sätt beskrivit det kinesiska cyberspionaget som närmast industriellt.[34]

Kinesiska cyberspionageoperationer har global räckvidd och har riktats mot många länder, inklusive USA och europeiska nationer. De siktar oftast in sig på högteknologiska industrier och forskningsinstitutioner för att stjäla intellektuell egendom och teknologiska innovationer. Kina har här utvecklat och använt avancerade sabotageprogram – malware – som används för att infiltrera och kommunicera över säkra nätverk.[35]

I september 2024 uppgav amerikanska FBI att ett kinesiskt företag kopplat till kinesiska staten hackade 260 000 internetanslutna enheter, inklusive kameror och routrar, i USA, Storbritannien, Frankrike, Rumänien och på andra platser.[36] En av många allvarliga kinesiska cyberattacker med politiska implikationer genomfördes mot de amerikanska federala myndigheternas nätverk. Denna attack gjorde det möjligt för Storm-0558-gruppen – som sägs vara kopplad till den kinesiska regeringen – att 2023 bryta sig in i Microsofts e-postsystem. Hackare skaffade en digital nyckel så de kunde förfalska användaruppgifterna. Detta intrång drabbade 22 organisationer och över 500 individer globalt, inklusive högprofilerade tjänstemän som USA:s handelsminister och landets ambassadör i Kina. Enbart i det amerikanska utrikesdepartementet blev över 60 000 e-postmeddelanden utsatta för intrång.[37] Redan år 2015 kungjordes en dataläcka på 22,1 miljoner poster med säkerhetsklassificeringsuppgifter för statligt anställda i USA där man misstänkte att kinesiska aktörer låg bakom och att de kom över all personalinformation för varje statligt anställd inklusive pensionerade och tidigare anställda.[38] En annan allvarlig kinesisk cyberattack avslöjades för allmänheten i oktober 2024. Genom den hade aktörer kopplade till den kinesiska staten infiltrerat flera amerikanska bredbandsleverantörers nätverk, möjligen med åtkomst till system som används för domstolsgodkända avlyssningar. Verizon, AT&T och Lumen Technologies var bland de drabbade företagen.[39] Bland de telefoner som var måltavlor fanns enheter som användes av dåvarande presidentkandidat Donald Trump och hans vicepresidentkandidat, senator J.D. Vance från Ohio. Insatsen tros utgöra en del av en omfattande underrättelseinsamling som också riktade sig mot det demokratiska partiet, inklusive medarbetare i både vicepresident Kamala Harris kampanj och den för senator Chuck Schumer från New York.[40]

FBI och andra myndigheter menar att Kina kan använda AI för att samla in och lagra data om amerikaner i en omfattning som tidigare inte varit möjlig. Glenn Gerstell, tidigare chefsjurist vid National Security Agency, uttrycker farhågor om att ”Kina kan utnyttja AI för att sammanställa en dossier om praktiskt taget varje amerikan, med detaljer som sträcker sig från deras hälsoregister till kreditkort och från passnummer till deras föräldrars och barns namn och adress”.[41]

Säkerhet och risk i övervakningskapitalismen

Sedan en tid tillbaka lever vi i en alltmer uppkopplad värld, ett ”sakernas internet” som man har uttryckt det.[42] Detta ger tidigare oanade möjligheter till spionerі vilket ställer till problem i en värld där ekonomin samtidigt är så globaliserad. Om en handelsnation inte längre anses som pålitlig, ja, ett hot, ställer detta till stora problem. Det blev Kina varse när dess relationer med framför allt USA började gnissla. Det kinesiska företaget Huawei, som var på väg att dominera den nya 5G-standarden för mobilkommunikation, blev 2019 det första stora kinesiska företag som blev föremål för oron kring potentialen för kinesiskt spionerі.[43] Insikten om att ett kinesiskt företag skulle få kontroll över inte bara hur, och om, vi kommunicerar utan också vad vi kommunicerar satte i gång en febril USA-ledd verksamhet för att stoppa företaget från att sälja sin 5G-teknologi.[44] När det sedan gällde sociala medier-appen Tiktok handlade det inte bara om ett spionerі- och avlyssningshot utan om att våra beteenden och innersta fantasier kan läsas ur data och sedan vändas mot oss i form av algoritmer som styr våra beteenden och våra tankar.[45] Spionerі och påverkan i ett.

Problematiken rör inte bara Kina utan även det globala skifte som forskare och samhällsdebattörer ibland beskrivit som övervakningskapitalism.[46] Det kinesiska övervakningssamhället och det västerländska algoritmstyrda och datainhämtande konsumtionssamhället förenas i samma kraftfulla nya tekniker. För datainhämtning öppnar de nya teknologierna oerhörda möjligheter. Framväxten av nya slags affärs- och marknadsföringssystem ställer inte bara hotet om spionerі och påverkan på sin spets utan öppnar samtidigt upp nya stora risker för företags- och tekniкspionage. Genom att vara i realtidskontakt med både sina leverantörer i Kina och sina kunder runt om i världen, och använda sig av de fakta om kundpreferenser, trender och produktionsmöjligheter detta spindelnät ger, kan till exempel det kinesiska företaget Shein oerhört snabbt ställa om produktionen och lansera nya garderober.[47] Den åtkomst av data rörande såväl producenterna och distributörerna som konsumenterna som detta upplägg möjliggör gör det möjligt för Shein att ständigt förbättra sina AI- och algoritmmodeller, vilket leder till effektivare verksamhet och bättre marknadsinformation. Ett sådant sofistikerat upplägg utgör inte bara en utmaning för etablerade klädjättar som H&M eller Zara. Det är - genom det ständigt pågående inhämtandet av information på olika nivåer om företag, individer och olika nätverk inom handel och transport - också ett potentiellt hot mot länders säkerhet eftersom det inte kan uteslutas att kinesiska myndigheter begär att få ta del av all denna information. Vi befinner oss alltså i en ny situation där den digitalt sammankopplade världen ger nya möjligheter att spionera på och hämta information om nästan vem eller vad som helst och från varsomhelst i världen. En fas i kapitalismens utveckling där data blivit själva drivmedlet – den nya oljan, menar vissa.[48] I skyddet mot kinesiskt spionerі upphör därför problemet inte vid ett visst kinesiskt företag, som Huawei, Tiktok eller Shein. Det handlar i slutändan i stället om en misstro mot Kina under Xi Jinping och en ständigt pågående konflikt mellan vad filosofen Karl Popper benämnde som ”det öppna samhället och dess fiender”.

Perry Johansson Vig

Oberoende forskare och tidigare analytiker vid Nationellt kunskapscentrum om Kina

Om Nationellt kunskapscentrum om Kina

Nationellt kunskapscentrum om Kina (NKK) vid Utrikespolitiska institutet (UI) bedriver forskningsbaserad och policyrelevant analys och rådgivning om Kinarelaterade ämnen. Fokuset ligger på frågor av särskild vikt för svenska intressen. UI:s publikationer genomgår intern kvalitetskontroll. Eventuella åsikter som uttrycks är författarens egna.

NATIONELLT KUNSKAPSCENTRUM OM KINA

UTRIKESPOLITISKA INSTITUTET

Referenser

1 Wray, Christopher, "China's attempt to influence U.S. institutions", videoframträdande, Hudson Institute, Washington D.C, 7 juli 2020, https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states.

2 Wray, Christopher, "Countering threats posed by the Chinese government inside the U.S", tal vid Ronald Reagan Presidential Library and Museum, 31 januari 2022, https://www.fbi.gov/news/speeches-and-testimony/countering-threats-posed-by-the-chinese-government-inside-the-us-wray-013122.

3 Corera, Gordon, "MI5 head warns of "epic scale" of Chinese espionage", BBC, 18 oktober 2023, https://www.bbc.com/news/uk-67142161.

4 För en bra översikt om vad underrättelseverksamhet är, se Lowenthal, Mark M, "Intelligence: From secrets to policy", Sage/CQ Press, Thousand Oaks, Kalifornien, 2019.

5 Kinas kommunistiska parti, KKP, ser detta som ett arbete för partiets säkerhet.

6 Det saknas en sådan översikt. Den vetenskapliga litteraturen i allmänhet är, med tanke på de senaste årens stora uppmärksamhet kring det kinesiska spionhotet, ganska mager. Joskes, Alex "Spies and lies: how China' s greatest covert operations fooled the world", Richmond, Victoria, Hardie Grant Books, 2022, är en bra blandning av forskningsarbete kring kinesiskt spionerі och hemligt påverkansarbete framför allt vad gäller USA. Se även Mattis,Peter & Brazil, Matthew, "Chinese communist espionage: an intelligence primer", Naval Institute Press, Annapolis, Maryland, 2019, för en akademiskt solid studie utifrån kinesiska öppna källor som fokuserar på personer, institutioner och historia gällande kinesisk underrättelseverksamhet.

7 Se till exempel Mark Lowenthal (2019). Det handlar alltså om säkerhet, och därför kan man omväxlande referera till säkerhetstjänster.

8 Än svårare är att veta något om en i mitt tycke – särskilt i det kinesiska fallet – viktig och ofta förbisedd del av underrättelsejobbet, nämligen själva leveransen av information till ansvariga politiker. Når den rätta informationen fram till ledaren, eller är det i Kina som det sägs ha varit i Sovjetunionen, att underrättelsetjänsten inte vågar komma med information som motsäger ledarens världsbild?

9 Staffas Edström, Erika, "Ro med kommunistpartiets åror: en granskning av den kinesiska medienärvaron i Sverige", Nationellt kunskapscentrum om Kina, 2023, https://kinacentrum.se/publikationer/ro-med-kommunistpartiets-aror-en-granskning-av-den-kinesiska-medienarvaron-i-sverige/. Lundberg, Frida & Sundqvist, Gustav, "Statliga kinesiska påverkansoperationer mot demokratin i svenska kommuner", Nationellt kunskapscentrum Kina, 2022, https://kinacentrum.se/publikationer/statliga-kinesiska-paverkansoperationer-mot-demokratin-i-svenska-kommuner/.

Se även:

Nyrén, Pär, "Kinesiska kommunistpartiets enhetsfront", Frivärld, 2020, https://frivarld.se/rapporter/kinesiska-kommunistpartiets-enhetsfront/

Oksanen, Patrik, ”Kinas attacker för att tysta kritiker”, Frivärld, 2020, https://frivarld.se/rapporter/kinas-attacker-for-att-tysta-kritiker/

Letho, Jesper & Oksanen, Patrik, ”Draken som bytte taktik”, Frivärld, 2021, https://frivarld.se/rapporter/draken-som-bytte-taktik/

10 För en analytisk bakgrund, se Lowenthal, Mark M., ”Intelligence: From Secrets to Policy”, CQ Press, 2019.

11 För mer om detta, se Mattis, Peter & Brazil, Matthew, ”Chinese Communist Espionage: An Intelligence Primer”, Naval Institute Press, 2019.

12 För en bra översikt över Kinas leninistiska säkerhetsapparat, se Pei, Minxin, ”The sentinel state: surveillance and the survival of dictatorship in China”, Harvard University Press, Cambridge, Massachusetts, 2019.

13 Corera, Gordon, ”China’s spy threat is growing, but the West has struggled to keep up”, BBC, 15 maj 2024. https://www.bbc.com/news/articles/cmm33rm32veo. Alltså både internt och utomlands – det är viktigt att påpeka då denna siffra har felrapporterats av flera mindre nogräknade nyhetssajter som att Kina har 600 000 spioner.

14 Shirk, Susan, ”China: Fragile superpower”, Oxford University Press: Oxford, 2007.

15 Coleman, Maia, ”Queens man is convicted of spying on dissidents for China”, New York Times, 6 august 2024. https://www.nytimes.com/2024/08/06/nyregion/shujun-wang-conviction-spy-china.html?searchResultPosition=20.

16 Förra chefen för MSS har till exempel flyttats upp i politbyrån. Se Chestnut Greitens, Sheena, ”New leaders in ”national” security after China’s 20th party congress”, China Leadership Monitor, 30 november 2023, https://www.prcleader.org/post/new-leaders-in-national-security-after-china-s-20th-party-congress

17 Vid 2015 –2016 års reform av befrielsearmén tog Högkvarterets underrättelsebyrå (The Intelligence Bureau of the Joint Staff Department of the Central Military Commission) över huvuddelen av det som tidigare benämnts i litteraturen som 2PLA. För en historik, se Matthew Brazil och Peter Mattis (2019).

18 Kidwell, Deborah, ”Cyber espionage for the Chinese government”, Office of Special Investigations, 17 september 2020, https://www.osi.af.mil/.

19 Hsiao, Russell, ”Recent Chinese spy cases in Taiwan: knowns, unknowns, and implications”, Global Taiwan Brief, vol. 9, issue 17, 4 september 2024, https://globaltaiwan.org/2024/09/recent-chinese-spy-cases-in-taiwan/.

20 Ehrman, John, ”Toward a theory of CI: What are we talking about when we talk about counterintelligence?” Studies in Intelligence, vol. 53, no. 2, 2009.

21 Se A. Kuo, Mercy, ”State security departments: The birth of China’s nationwide state security system”, The Diplomat, 2023, https://thediplomat.com/2023/11/chinas-state-security-departments-and-nationwide-system/.

”Studies in Chinese Communist Party external work”, Deserepi, Issue 0, 2023.

Inkster, Nigel, ”The Xi files: how China spies”, The Spectator, 27 april 2024, https://www.

spectator.co.uk/article/the-xi-files-how-china-spies/?ut%20%20m_medium=email&utm_source=CampaignMonitor_Editorial&utm_campaign=WEEK%20%2020240425%20%20AL+CID_5208de9c42aeb7f58702c946cc45c9d2.

22 Se Mattis och Brazil (2019) för detta.

23 Barnes, Julian E. & Sanger, David E., "As China expands its hacking operations, a vulnerability emerges", New York Times, 22 februari 2024, https://www.nytimes.com/2024/02/22/us/politics/china-hacking-files-risk.html.

24 Operation Fox Hunt är en av det kinesiska kommunistpartiet ledd hemlig global operation vars officiella syfte är antikorruption. De hemliga polisstationerna verkar ha varit en del i det arbetet. Safeguard Defenders avslöjade detta i två rapporter 2022.:

"110 Overseas - Chinese Transnational Policing Gone Wild", Safeguard Defenders, 2022, https://safeguarddefenders.com/en/publications/110-overseas.

"Patrol and Persuade", Safeguard Defenders, 2022, https://safeguarddefenders.com/en/publications/patrol-and-persuade

25 Ewe, Koh & Binger, Laura, "United Front: China's magic weapon caught in a spy controversy", BBC News, 18 december 2024, https://www.bbc.com/news/articles/c878evdp758o. Se också Hamilton, Clive, "Silent invasion: China's influence in Australia", Hardie Grant Books: Richmond, Victoria, 2018, för en detaljerad genomgång av Enhetsfrontens olika användningsområden.

26 Mattis beskriver väldigt pedagogiskt i en artikel hur kinesiska spioner utger sig för att vara ambassadanställda, journalister, vetenskapsmän och forskare, företagare, ja till och med politiker. Se Mattis, Peter, "Five ways China spies: not as different as you might think", National Interest, 6 mars 2014, https://nationalinterest.org/commentary/five-ways-china-spies-10008. Alex Joske (2022) har också rikligt med exempel på vilka slags täckmantlar som MSS använder sig av för sina spioner.

27 En ledande forskare beskriver det i en rapport som att "Den kinesiska regeringen har skapat ett utarbetat mångfasetterat ' hack-for-hire'-ekosystem som inte liknar något vi tidigare sett". Se Benincasa, Eugenio, "From Vegas to Chengdu: hacking contests, bug bounties, and China's offensive cyber ecosystem", Center for Security Studies (CSS), ETH Zürich, 2024, https://css.ethz.ch/en/publications/risk-and-resilience-reports/details.html?id=/f/r/o/m/from_vegas_to_chengdu_hacking_contests_b.

28 Till exempel hur man hade gjort intrång på webbplatser eller e-postservrar tillhörande statliga myndigheter i Kinas grannländer, som Kirgizistan, Thailand, Kambodja, Mongoliet och Vietnam.

29 Zetter, Kim, "Intrusion truth – five years of naming and shaming China's spies", Zero Day, 29 mars 2022, https://www.zetter-zeroday.com/interview-with-intrusion-truth/. Intrusion Truth är ett globalt nätverk av anonyma bidragsgivare med det gemensamma målet att avslöja kinesiska APT (advanced persistant threats) på sin blogg: https://intrusiontruth.wordpress.com/?ref=zetter-zeroday.com.

30 Ministeriet för statssäkerhet (april 2024),《求是》杂志刊发陈一新署名文章：全面贯彻总体国家安全观-中国长安网. http://www.chinapeace.gov.cn/chinapeace/c100007/2024-

04/15/content_12723018.shtml?utm_so.

31 Inkster, Nigel, "The Xi files: how China spies", the Spectator, 27 april 2024, https://www.spectator.co.uk/article/the-xi-files-how-china-spies/?utm_medium=email&utm_source=CampaignMonitor_Editorial&utm_campaign=WEEK%20%2020240425%20%20AL+CID_5208de9c42aeb7f58702c946cc45c9d2.

32 Dreadnought var ett nytt slags pansarbåtar som brittiska imperiet byggde och som över en natt gjorde alla andra krigsskepp på haven harmlösa i jämförelse. Skeppet ändrade helt spelreglerna för den tidens maritima krigföring.

33 Zettl-Schabath, Kerstin & Hemmelskamp, Jonas, "APT Profile – Volt Typhoon vs. Flax Typhoon: In the eye of the Chinese typhoons", European Repository of Cyber Incidents, 20 augusti 2024, https://eurepoc.eu/publication/apt-profile-volt-typhoon-vs-flax-typhoon/.

34 Andersson Åkerblom, Tobias, "Säpo: Västsverige mål för storskaligt kinesiskt spionage", Göteborgs-Posten, 22 september 2020, https://www.gp.se/ekonomi/sapo-vastsverige-mal-for-storskaligt-kinesiskt-spionage.2cf6ac48-6ec4-4aa1-a54e-4e2cf88ae2ab.

35 Howell O'Neill, Patrick, How China built a one-of-a-kind cyber-espionage behemoth to last. A decade-long quest to become a cyber superpower is paying off for China. MIT Technology Review, 28 februari 2022, https://www.technologyreview.com/2022/02/28/1046575/how-china-built-a-one-of-a-kind-cyber-espionage-behemoth-to-last/.

36 Colchester, Max & Michaels, Daniel, "Scale of Chinese spying overwhelms Western governments", Wall Street Journal, 14 oktober 2024, https://www.wsj.com/politics/national-security/scale-of-chinese-spying-overwhelms-western-governments-6ae644d2.

37 Lyngaas, Sean & Atwood, Kylie, "Chinese hackers breached US ambassador to China's email account", CNN, 21 juli 2023, https://edition.cnn.com/2023/07/20/politics/chinese-hackers-us-ambassador/index.html.

38 Fruhlinger, Josh, "The OPM hack explained: Bad security practices meet China' s Captain America", CSO Online, 2 december 2020, https://www.csoonline.com/article/566509/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html.

Se också "The OPM data breach: how the government jeopardized our national security for more than a generation", Committee on Oversight and Government Reform, U.S. House of Representatives 114th Congress, https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf.

39 Krouse, Sarah, Volz, Dustin, Viswanatha, Aruna & McMillan, Robert, U.S. wiretap systems targeted in China-linked hack, Wall Street Journal, 5 oktober 2024, https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b.

40 Barret, Devlin, "What to know about the Chinese hackers who targeted the 2024 campaigns", New York Times, 26 oktober 2024, https://www.nytimes.com/2024/10/26/us/politics/salt-typhoon-hack-what-we-know.html.

41 McMillan, Robert, Volz, Dustin & Viswanatha, Aruna, "China is stealing AI secrets to turbocharge spying, U.S. says", Wall Street Journal, 25 december 2023, https://www.wsj.com/tech/ai/china-is-stealing-ai-secrets-to-turbocharge-spying-u-s-says-00413594.

42 För en kort diskussion om konsekvenserna, se ”The ethical implications of the Internet of Things (IoT)”, Unesco, 2021, https://unesdoc.unesco.org/ark:/48223/pf0000387201.

43 ”Investigative report on the U.S. national security issues posed by Chinese telecommunications companies Huawei and ZTE”, U.S. House Permanent Select Committee on Intelligence, 2012.

44 Berman, Noah, Maziland, Lindsay & Chatzky, Andrew, ”Is China’s Huawei a threat to U.S. national security?”, The Council on Foreign Relations, 8 februari 2023, https://www.cfr.org/backgrounder/chinas-huawei-threat-us-national-security.

45 Staffas Edström, Erika, ”Kan vi lita på Tiktok?”, Nationellt kunskapscentrum om Kina, 21 juli 2023, https://kinacentrum.se/publikationer/kan-vi-lita-pa-tiktok/.

46 Zuboff, Shoshana, ”Övervakningskapitalismen: Vid maktens nya frontlinjer”, Ordfront, 2021.

47 Företaget har nu, i ett försök att inte framstå som ett kinesiskt företag, flyttat sitt huvudkontor till Singapore. För affärsidén och hur Shein och liknande postorderupplägg med anknytning till Kina kan utgöra ett hot kring informationsinhämtning, se Ann LaRocco, Lori, ”Amazon’s Asian rival Shein wants to be supply chain giant, but some fear Chinese cyber spying inside global trade links”, CNBC, 8 juli 2024, https://www.cnbc.com/2024/07/08/shein-to-build-supply-chain-giant-fear-china-cyber-spy.html.

48 ”The world’s most valuable resource is no longer oil, but data”, Economist, 6 maj 2017, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.