FOI MEMO

Projekt	Sidnr
Asien och Mellanöstern	1 (22)
Projektnummer	**Kund**
A11903	Försvarsdepartementet
FoT-område	

Handläggare	Datum	Memo nummer
Johan Englund	2019-03-22	FOI Memo 6698

Kinas industriella cyberspionage

Huvudsakliga slutsatser

- Kinas cyberspionage syftar till att främja politiska, strategiska och ekonomiska intressen. Enligt sina nationella strategier eftersträvar den kinesiska staten att avancera i de globala värdekedjorna och bli en stormakt inom avancerad tillverkning.
- Kina avser att i högre grad bli teknologiskt självförsörjande och uppnå en världsledande position inom avancerade teknologier. Militärt siktar Folkets befrielsearmé (PLA) på att bli en av världens främsta försvarsmakter som är modern och högteknologisk.
- En stor del av det kinesiska cyberspionaget är inriktat på industrier och sektorer som den kinesiska regeringen identifierat som strategiska genom att de är kopplade till statens utvecklingsmål. Detta gäller bl. a nästa generations informationsteknologi, robotteknik samt rymd- och flygteknik.
- Kinas cyberspionage kan betraktas som en delkomponent för att stödja de strategiska utvecklingsmålen, där både lagliga och olagliga medel för informationsinhämtning ingår. Liksom strategiska investeringar och förvärv utgör medel för att uppnå industriella utvecklingsmål, kan även cyberintrång användas för att uppfylla dessa ambitioner.
- Kommunistpartiet har en alltmer framträdande roll i kinesiska företag. Därmed är gränsdragningen mellan privata och statliga verksamheter allt otydligare.
- Med sin öppna och innovationsbaserade ekonomi, en stark industri och världsledande företag är Sverige en attraktiv måltavla för kinesiskt cyberspionage.
- Kinas cyberspionage har till synes ökat i omfattning under senare år. Därtill har kinesiska cyberoperationer blivit mer avancerade och uthålligare.
- För såväl svenskt som europeiskt vidkommande bedöms kinesiska cyberoperationer fortsätta i ökad takt, i synnerhet inom industrier som anses vara avgörande för Kinas utvecklingsmål. På sikt kan detta komma att utmana svensk konkurrenskraft.
- Cyberoperationer prioriteras av den kinesiska staten. Cybersäkerhet anses centralt för nationell säkerhet samtidigt som cyberoperationer likställs övriga delar av militären.
- Utöver regerings- och arménsponsrade cyberaktörer kan även privata aktörer agera utifrån kinesiska statliga intressen. Detta kan grumla skiljelinjerna mellan statsstödd och självständig hackeraktivitet.
- Ministeriet för statssäkerhet (MSS) har till synes övertagit rollen för kommersiellt cyberspionage, medan PLA står för det politiska och militära spionaget. Då spionaget rör teknologier med både civila och militära användningsområden är skiljelinjerna mellan kommersiellt och försvarsinriktat cyberspionage otydliga.

Akronymer

APT	Advanced Persistent Threat
BFV	Bundesamt für Verfassungsschutz
DDos	Distributed denial of Service
FoU	Forskning och Utveckling
FRA	Försvarets radioanstalt
IT	Informationsteknologi
MSS	Ministeriet för statssäkerhet
NCIX	Office of the National Counterintelligence Executive
PLA	People’s Liberation Army (Folkets befrielsearmé)
SSF	Strategic Support Force (Strategiska stödstyrkan)
Säpo	Säkerhetspolisen

1 Inledning

Folkrepubliken Kina ägnar sig sedan länge åt cyberaktiviteter riktade mot kommersiella mål i utlandet.[1] Målsättningen bakom Kinas cyberspionage är att förbättra sin ekonomiska konkurrenskraft samt främja landets strategiska intressen, bland annat genom att tillskansa sig avancerad teknologi. För att inhämta teknologisk *know-how* finns olika tillvägagångssätt såsom företagsförvärv, forskningssamarbeten, påtvingad teknologiöverföring, riktad talangrekrytering, samt spionage. Cyberbaserat industrispionage utgör ett sätt för den kinesiska staten att komma åt känslig kommersiell information samt skaffa sig otillbörligt tillträde till immateriell egendom.

Cyberspionage kan definieras som ”bruket av datanätverk för att få otillbörlig tillgång till konfidentiell information, generellt hos en statlig eller annan organisation”.[2] Enligt öppen information har kinesiska regeringsstödda cyberintrång ökat 2018, mot såväl mål i USA som i Asien och Europa.[3] Angrepp mot företag och stölder av affärsinformation har tilltagit.[4] I synnerhet har en ökning skett i cyberspionage riktat mot IT-bolags molntjänster, telekommunikationsföretag och juristfirmor. Därtill ser kinesiska cyberaktörer ut att ha förhöjt sin förmåga att genomföra mer uthålliga intrång utan att bli upptäckta.[5]

2013 bedömdes Kina ligga bakom mellan 50 och 80 procent av världens gränsöverskridande stölder av immateriell egendom.[6] Samma år uppskattades Kina stå för över 90 procent av cyberrelaterat ekonomiskt spionage i USA.[7] Enligt beräkningar förlorar USA årligen mellan 225 och 600 miljarder USD på grund av stöld av immateriell egendom, varav Kina ligger bakom omkring 70 procent av dessa förluster.[8] Den amerikanska kongressen har fastslagit att kinesiskt spionage utgör det största enskilda hotet mot landets teknologi, vilket ställer stora krav på amerikanskt kontraspionage.[9] Kina hävdar dock konsekvent att regeringen och Folkets befrielsearmé (PLA) inte är involverade i cyberspionage och framhäver istället att landet är ett offer för cyberangrepp.[10]

För svenskt vidkommande bedömer Säkerhetspolisen (Säpo) i sin årsbok 2018 att hotbilden kopplad till Kina ökar.[11] Kina anses bedriva systematisk underrättelseinhämtning genom både uppköp av teknologiskt eftertraktade företag och cyberangrepp mot företag och myndigheter. Enligt Säpo är omfattningen så stor att det kan innebära risker för säkerheten i Europa.[12] I Försvarets Radioanstalts (FRA) årsrapport 2017 nämns ingen stat vid namn, men det Kina-härledda cyberangreppet Cloud Hopper beskrivs som en ny form av cyberangrepp där Sverige var ett av flera angripna länder,[13] och där ett flertal privata IT-säkerhetsföretag identifierat kinesiska aktörer som ansvariga för intrången.[14] Enligt FRA:s bedömning ligger stater och statsunderstödda organisationer bakom de mest avancerade angreppen, som därmed utgör de allvarligaste cyberhoten mot Sverige.

Syftet med detta memo är att belysa motiven till Kinas cyberspionage mot kommersiella och industriella mål, vilka målbilder och intresseområden som driver dessa aktiviteter samt vad som kan förväntas framöver i dessa sammanhang.

---

[1] Eftimiades (2018).
[2] Översatt från “The use of computer networks to gain illicit access to confidential information, typically that held by a government or other organization.” i Oxford Dictionaries (2019).
[3] Office of the United States Trade Representative (2018) s.11, 19-21; FireEye (2018) s.49.
[4] Johnson (2018).
[5] Johnson (2018); South China Morning Post (2018a).
[6] Blair and Huntsman, Jr. (2013) s.3.
[7] Verizon (2013) s. 21.
[8] Cooper (2018a).
[9] U.S.-China Economic and Security Review Commission (2007) s. 6.
[10] China Daily (2010).
[11] Säkerhetspolisen (2019) s. 20-21, 33.
[12] Säkerhetspolisen (2019) s. 20.
[13] Försvarets Radioanstalt (2018) s. 23.
[14] Sallinen (2018a).

Memot fokuserar på Kinas industrispionage via cyberoperationer, det vill säga det kinesiska cyberspionaget mot kommersiella och industriella mål. Det berör inte Kinas cyberaktiviteter med politiska förtecken som t.ex. kan syfta till kontroll av meningsmotståndare och att påverka narrativ om Kina. Memot omfattar inte heller angrepp såsom *distributed-denial-of-service*-attacker (DDos) eller tillgänglighetsattacker som syftar till att störa informations- och kommunikationsflöden, eller så kallade *Internet Hijacking Attacks* där angriparen övertar kontrollen över en kommunikationskanal.

Memot inleds med en kort översikt av Kinas cyberoperationer och hur dess cyberspionage har blivit allt mer sofistikerat. Därefter presenteras bakomliggande motiv och strategier för Kinas cyberoperationer, vilka kopplas till den kinesiska statens övergripande utvecklingsmål. Avslutningsvis diskuteras hur dessa motiv och mål förhåller sig till Sverige och Europa.

1.1 Metod

Detta memo är baserat på öppna källor och intervjuer med företrädare för akademin och näringslivet som arbetar med frågor rörande cybersäkerhet. Källorna inkluderar rapporter och uppgifter från säkerhetstjänster, cybersäkerhetsföretag, medierapportering, akademiska artiklar samt nationella strategidokument och rapporter från regeringsinstanser.

Analyser av cyberspionage försvåras av en generellt bristfällig tillgång till källor, vilket även gäller för framtagandet av detta memo. Följande faktorer innebär att uppgifter är svåra att verifiera, och att litteraturen ofta refererar till samma enskilda källa.

För det första vilar analysen till stor del på amerikanska källor, i och med att huvuddelen av den information om Kinas cyberspionage som finns öppet tillgänglig just härrör från USA. Därmed finns en risk för ett ensidigt fokus på amerikanska perspektiv och problemformuleringar.

För det andra präglas forskningsområdet av brist på heltäckande öppen information. Cyberoperationer är till sin natur känsliga och hemliga, vilket innebär att tillgången på officiellt bekräftade uppgifter är begränsad. De flesta cyberintrång rapporteras alltjämt inte av bolag och myndigheter som drabbats, i och med risken för att det kan föranleda anklagelser om säkerhetsbrister och skada verksamhetens rykte. Dessutom förblir många företag ovetandes om att de överhuvudtaget har blivit utsatta för angrepp. Således finns sannolikt ett betydande mörkertal för omfattningen av cyberspionage.

För det tredje är analysen befattad med svårigheter som rör härledning av cyberspionage till en särskild aktör och geografisk plats. Att attribuera en aktör ansvar för ett cyberintrång är en komplicerad process som kräver noggrann insamling av bevismaterial över tid, där hänsyn tas till faktorer såsom typ av teknik och taktik för en cyberoperation, dess omfattning, och operationella detaljer, exempelvis språkinställningar och tid för utförda intrång.[15] Dessutom krävs förberedelser innan en incident äger rum för att kunna lagra relevant data genom att sätta upp datorsystem så att de lagrar sådan aktivitet. Få civila organisationer har tillräcklig forensisk kompetens inom cyberområdet och budget för att underlätta utredningar.

Detta memo är skrivet med ovanstående faktorer i beaktande och därmed med förbehållet att översikten av det kinesiska cyberspionaget på intet sätt är uttömmande utan byggt på indikationer och kvalitativa bedömningar.

[15] FireEye (2016) s.12.

2 Översikt av kinesiska cyberoperationer

Kina har en lång historia av industriellt spionage och cyberintrång.[16] Cyberspionage härlett till Kina har involverat ett brett spektrum av branscher, sektorer och geografiska mål. Angrepp har exempelvis riktat in sig mot hälso-, utbildnings- och finansrelaterade sektorer, men även mot industrier såsom energi, försvar, IT, rymd, samt myndigheter.[17] USA har varit en återkommande måltavla, men även länder i Europa och Asien har drabbats av kinesiska cyberattacker.

Tabell 1. Urval av uppmärksammade cyberangrepp härledda till Kina-baserade aktörer[18]

Årtal	Aktör	Angripna länder	Urval av angripna sektorer
2006-2013	APT1/Enhet 61398	USA, Kanada Frankrike, UK, Belgien, Norge, Singapore, Japan m.fl.	Elektronik, transport, IT, finans, media, jordbruk, kemikalier, energi, rymd, hälsa, utbildning
2009	Night Dragon	USA, Taiwan, Grekland, Kazakstan	Energi
2009	Elderwood	USA, Kanada	Försvar, rederi, flygindustri
2010	APT17/Aurora Panda	USA	Teknologi, finans, försvar
2010-2012	N/A	USA (Westinghouse Electric) och Tyskland (SolarWorld)	Energi
2012	Shady RAT	USA, Kanada, Taiwan, Japan, Sydkorea, UK	Regeringsmål, försvar, teknologi, industri
2014	Axiom	UK, Tyskland, Nederländerna, Italien	Teknologi, telekom, miljö och energi, infrastruktur
2014	APT18	USA	Hälsa, medicin
2015	Emissary Panda	UK, Frankrike	Rymd, fordon, energi, försvar
2016	N/A	USA	Elektronik
2016	APT10 (Cloud Hopper)	USA, Norge, Finland, Sverige, UK, Japan m.fl.	IT, energi, gruvverksamhet, finans, medicin, försvarsindustri, offentlig verksamhet
2018	APT10	Finland, Frankrike, Tyskland, Sverige, UK m.fl.	Flyg, rymd, medicin, finans, elektronik, telekom

I samband med ett avtal som USA och Kina slöt i september 2015 avtog de upptäckta kinesiska cyberintrången i USA.[19] I överenskommelsen åtog sig båda sidor att avstå från att stödja cyberrelaterad stöld av immateriell egendom, såsom handelshemligheter eller annan känslig kommersiell information. På senare tid verkar dock Kinas cyberoperationer i USA åter ha tagit fart. De amerikanska cybersäkerhetsföretagen Crowdstrike och FireEye noterade i slutet av 2018 att statliga kinesiska cyberangrepp har ökat i omfattning, samt att tidigare inaktiva kinesiska hackergrupper hade

[16] Cooper (2018b) s.6.
[17] Racicot (2014).
[18] Racicot (2014); Mandiant (2014); PwC (2017); Cooper (2018b); Lee-Makiyama (2018).
[19] Cooper (2018b) s.7.

återaktiverats.[20] Samtidigt som de kinesiska angreppen mot USA avtog under 2015-16 ökade cyberattackerna mot andra mål, däribland Japan.[21] Det är troligt att Kinas angrepp helt enkelt omdirigerades till asiatiska och europeiska länder.[22]

2.1 Cyberoperationer med förbättrad förmåga

De kinesiska cyberoperationerna har enligt amerikanska cybersäkerhetsföretag blivit alltmer avancerade. FireEye hävdar att det kinesiska förfarandet tyder på att angripare har blivit mer precisa och beräknande, samt mer framgångsrika att infiltrera företagsnätverk.[23] Istället för att urskillningslöst ”dammsuga” det man lyckas komma åt, ägnar sig kinesiska aktörer numera åt att mer strategiskt precisera och inrikta sina cyberintrång. FireEye noterar också en ökning av kinesiskt cyberspionage som inriktar sig mot tjänstesektorn som leverantörer av molntjänster, telekomföretag och advokatbyråer.[24] Som en följd har den civila rådgivningskommittén till amerikanska försvarsdepartementet, Defense Science Board, varnat för att den kinesiska offensiva cyberförmågan numera överstiger USA:s förmåga att försvara kritisk infrastruktur.[25]

Kinesiska hackare har utvecklat sin förmåga att obemärkt ta sig in och operera inom andra system, vilket möjliggör tidsmässigt längre intrång innan de blir upptäckta. I november 2018 bedömde det amerikanska cybersäkerhetsföretaget Carbon Black att kinesiska statliga aktörer förbättrat sina metoder för dold infiltration genom öppet tillgängliga och egenutvecklade verktyg.[26] Genom att variera sina intrångsverktyg efter tillträde lämnar de få eller inga unika spår, vilket förhindrar forensiska efterforskningar. Således har de avsevärt förbättrat sina metoder att oupptäckt utföra cyberangrepp.

Kinesiska grupper har vidare uppvisat en markant förbättrad förmåga att kunna utföra så kallade *Advanced Persistent Threat* (APT)-operationer. En APT-operation är en sofistikerad process för att under lång tid utföra riktade cyberintrång. Operationen kan pågå i flera månader eller år, där angriparen stjäl information över tid och fördjupar sitt otillbörliga tillträde till sina måltavlor. Mycket kortfattat utförs en APT-attack generellt i sju steg: rekognosering, beväpning, sändning, exploatering, installation, styrning, och slutförande.[27] Kinesiska cybergrupper har visat sig utvecklat teknisk kapacitet i deras verktyg att komma åt flera klienter samtidigt och röra sig mellan dem under lång tid för att därigenom infiltrera deras data.

Den mest uppmärksammade APT-operationen hittills var Cloud Hopper, som har spårats till kinesiska statsaktörer och som drabbade minst 15 länder, däribland Sverige. Måltavlorna för operationen var verksamma inom sektorer såsom industriell tillverkning (t.ex. verkstad, mekanik och kemikalieindustri), *life science*[28], IT, gruvindustri och försvarsindustri. Cloud Hopper uppdagades och kartlades i en rapport framtagen 2017 av PwC i samarbete BAE Systems och brittiska National Cyber Security Centre.[29] En kinesisk hackergrupp benämnd APT10 som upptäcktes 2016 hade sedan ett antal år tillbaka infiltrerat leverantörer av molnbaserade övervakningstjänster av nättrafik hos kunder.[30] Hackergruppen nästlade sig in genom dessa IT-tjänsteleverantörer för att därefter inom IT-systemen sprida skadlig kod samt variera intrångsverktygen och hoppa mellan IT-leverantörers kunder, dvs. angriparens slutliga måltavlor. Därmed kunde hackergruppen kartlägga bolag och sedan angripa nyckelindivider via e-post,

[20] Johnson (2018).
[21] Intervjuer i Tokyo, mars 2019.
[22] South China Morning Post (2018a); Office of the United States Trade Representative (2018).
[23] FireEye (2016) s.4, 15.
[24] FireEye (2018) s.49.
[25] Defense Science Board, (2017) s.4.
[26] Carbon Black (2018) s. 13.
[27] Sallinen (2018b).
[28] Life science är ett tvär- och mångvetenskapligt samlingsbegrepp för studier av liv och hälsa, vilket bl.a. inkluderar bioteknik, läkemedelsindustri och medicinsk vetenskap.
[29] PwC (2017).
[30] Gruppen fick namnet APT10 av utredare på cybersäkerhetsföretaget Mandiant och är en av över 20 identifierade APT-grupper.

s.k. *nätfiske* (*spear phishing*). Angriparen kunde röra sig obemärkt inom systemen och därigenom genomföra en systematisk dammsugning av måltavlornas data och system för att extrahera information från dem. Intrången riktade sig mot företag och olika offentliga verksamheter i totalt 15 länder.

3 Kinesiska motiv och mål för cyberspionage

För att identifiera motiven bakom Kinas cyberspionage bör statens politiska, strategiska samt ekonomiska intressen och mål beaktas i en nationell och internationell kontext. Kinas industriellt motiverade cyberspionage sker mot måltavlor som är av betydelse för landets ekonomiska och militära utveckling.

Cybersäkerhet har tydlig prioritet för Kina och har beskrivits av kommunistpartiets generalsekreterare Xi Jinping som fundamental för den nationella säkerheten och statens modernisering.[31] Detta understryks av att staten etablerat nya cybersäkerhetsrelaterade instanser sedan Xi kom till makten 2012. En av de viktigaste av dessa är den *strategiska stödstyrkan* (*Strategic Support Force*, SSF[32]) som upprättades i slutet av 2015 och ansvarar för PLA:s cyberuppdrag, tillsammans med den elektroniska och rymdrelaterade krigsföringen. Genom grundandet av SSF likställs cyberoperationer med de andra vapenslagen. Enligt amerikanska bedömare ingår i SSF:s uppdrag att stödja militär utveckling genom att centralisera underrättelseinhämtning samt att förbättra informationsoperationer genom att integrera rymd, cyber och elektronisk krigföring, däribland genom medel som cyberspionage.[33] Upprättandet av SSF återspeglar ett skifte till en struktur där olika typer av uppdrag och domäner som rekognosering, attack och försvar integreras för att möjliggöra ett ”fullt spektrum av krigförande kapaciteter”, där cyberspionage kan aktiveras såväl defensivt som offensivt i PLA:s cyberuppdrag.[34]

3.1 Cyberspionage med ekonomiska och strategiska syften

Det kinesiska kommunistpartiets yttersta mål är att behålla sitt grepp om makten i Kina. Därmed måste det infria löften till den kinesiska befolkningen om ekonomisk utveckling, högre välstånd och global stormaktstatus. Militärt strävar Kina efter att på sikt ha en av världens främsta försvarsmakter som är modern, högteknologisk och internationellt konkurrenskraftig.[35] Ekonomiskt genomgår Kina en omställning från en investerings- och exportorienterad ekonomi till en mer innovativ och konsumtionsdriven ekonomi. Ett av det kinesiska ledarskapets mål är att staten ska avancera i de globala värdekedjorna och gå från tillverkning till inhemsk teknologiutveckling. Enligt nationella strategier ska innovation och högteknologisk utveckling utgöra grundbultar i Kinas ekonomiska omstrukturering, som slutligen syftar till att bygga den ”kinesiska drömmen”, där landet har förverkligat ”den nationella pånyttfödelsen”[36] och blivit en global stormakt.[37]

Därmed vilar både den militära och ekonomiska utvecklingen på teknologiska framsteg. Användningsområdena för dessa teknologier är ofta såväl kommersiellt som militärt relevanta. Detta innebär i sin tur att det industriella spionaget riktar sig mot både civila sektorer och försvarsindustri.

Kinas strategier för ekonomisk utveckling och teknologiska framsteg bottnar i partiets syn på att landet behöver förstärka sin innovativa förmåga samt en strävan efter att i högre grad bli teknologiskt självförsörjande.[38] År 2006 utfärdade regeringen en långsiktig plan för forskning och teknikutveckling

[31] Theoretical Studies Center Group (2017).
[32] På kinesiska zhanlüe zhiyuan budui, 战略支援部队.
[33] Costello och McReynolds (2018) s. 1.
[34] Kania och Costello (2018) s. 109-110.
[35] Xi Jinping (2017) ” 决胜全面建成小康社会 夺取新时代中国特色社会主义伟大胜利——在中国共产党第十九次全国代表大会上的报告” [Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era – Report Delivered at the 19th National Congress of the Communist Party of China], 27 oktober 2017.
[36] Den ”kinesiska drömmen om den nationella pånyttfödelsen” syftar bl.a. på det övergripande kinesiska målet att till mitten av 2000-talet ha utvecklats till en modern nation med avancerad teknologi och en innovativ ekonomi, med förmåga att vara i militär paritet med USA och där Taiwan har införlivats i Folkrepubliken Kina.
[37] Information Office of the State Council of the People’s Republic of China (2015); Central Committee of the Communist Party of China (2015).
[38] The State Council of the People’s Republic of China (2006); Chinese Academy of Sciences (2016); Zhang Yue (2018).

som prioriterar sektorer såsom energi, jordbruk, tillverkning, transport, IT och nationellt försvar.[39] Kinas 13:e femårsplan för 2016-2020 fokuserar starkt på innovation och identifierar strategiska industrier som ska bidra till Kinas framtida ekonomiska tillväxt och styrka.[40] Bland industrierna märks bland annat IT, avancerad tillverkning, ”gröna” fordon, bioteknik, rymd- och flygteknik och jordbruksmaskiner.

År 2015 utfärdade den kinesiska centralregeringen den nationella strategin *Made in China 2025*, som klargör att Kina ska minska sitt beroende av utländsk teknologi och bli en stormakt inom avancerad tillverkning, liknande Tyskland och Japan.[41] Strategin lägger fram industripolitiska intressen och målsättningen att uppgradera landets industrier. Kina ska bli världsledande inom teknologiskt avancerade områden såsom nästa generations IT, robotteknik samt flyg- och rymdteknik. Strategin identifierar tio teknikområden som Kina ämnar dirigera investeringar till, vilka även överlappar med ovan nämnda strategier.

Tabell 2. Tio breda teknikområden identifierade i strategin ”Made in China 2025”

Made in China 2025: 10 teknikområden	
1.	Nästa generations informationsteknologi
2.	Datorstyrda verkstadsmaskiner och robotteknik
3.	Flyg- och rymdteknik
4.	Teknik för sjöfart och högteknologiska fartyg
5.	Avancerad järnvägsutrustning
6.	Energibesparing och gröna fordon
7.	Energiutrustning
8.	Maskineri för jordbruk
9.	Innovativa material
10.	Biomedicin och högeffektiv medicinsk utrustning

Mot bakgrund av denna strävan att modernisera sin ekonomi och militär riktar sig också en stor del av Kinas cyberspionage mot de sektorer och industrier som den kinesiska regeringen har identifierat som strategiska.[42]

Enligt en analys av Nicholas Eftimiades som publicerades 2018 fokuserar nära hälften av Kinas totala spionage på amerikansk militär- och rymdteknologi, medan omkring 25 procent av spionaget sker mot kommersiella intressen.[43] Eftimiades, som har en bakgrund i den amerikanska underrättelsetjänsten och USA:s utrikes- och försvarsdepartement, drog denna slutsats efter att ha undersökt 274 dokumenterade fall av världsomspännande kinesiskt spionage sedan år 2000.

Slutsatserna i analysen stämmer överens med bedömningar om kinesiskt cyberspionage från amerikansk underrättelsetjänst, som anger att kinesiska cyberoperationer har fokuserat på måltavlor i den offentliga och privata sektorn inom försvar, teknologi och kommunikation.[44] Enligt en tidigare chef för USA:s

[39] The State Council of the People’s Republic of China (2006).
[40] Central Committee of the Communist Party of China (2015).
[41] The State Council of the People’s Republic of China (2015).
[42] Office of the Director of National Intelligence & Office of the National Counterintelligence Executive (2011) s. 7-9; Mandiant (2014) s.4, 24; iDefense (2017) s. 5; Cooper (2018b) s.19.
[43] Eftimiades (2018).
[44] Office of the Director of National Intelligence & National Counterintelligence and Security Center (2018) s. 7.

nationella kontraspionage (NCIX), Michelle Van Cleave, riktar kinesiska cyberattacker in sig på i det närmaste alla typer av teknologier som krävs för militär överlägsenhet.[45] Både privata och statsägda kinesiska företag är aktiva inom industriellt spionage, där de statsägda företagen primärt har inhämtat avancerad militär teknologi.[46] Ett liknande mönster märks i andra utsatta stater. En representant för den tyska säkerhetstjänsten uppgav 2009 att de kinesiska cyberattacker främst riktade sig mot kommunikations- och fordonssektorerna, samt förnybar energi och teknologi.[47]

Historiskt sett har Kinas cyberoperationer ofta syftat till att inhämta information och utländsk teknologi med relevans för de industrier som lyfts fram i kommunistpartiets femårsplaner som strategiskt viktiga.[48] Samtliga sektorer är potentiella måltavlor för kinesiska cyberoperationer, men utländska företag verksamma i vad Kina identifierar som strategiska sektorer har visat sig vara särskilt utsatta för cyberangrepp från kinesiskt statsstödda hackare.[49] De branscher som uppges ha varit föremål för flest angrepp överensstämmer väl med de teknologier som officiella dokument identifierar som strategiskt viktiga.[50]

Denna korrelation utmärkte även de två mest uppmärksammande fallen av kinesiskt cyberspionage som avslöjades 2014 av amerikanska cybersäkerhetsföretaget Mandiant respektive PwC i samband med Cloud Hopper-kampanjerna 2017.[51] Mandiants avslöjande visade att måltavlorna för angrepp under 2006-2013 till stor del var verksamma inom branscher som den 12:e femårsplanen betecknade som centrala för Kinas tillväxt, inklusive fyra av de sju identifierade strategiska industrierna.[52] Likaså hävdar PwC i sin granskning av Cloud Hopper att cyberintrången riktade sig mot såväl politiska organisationer med koppling till Kinas geopolitiska intressen som kommersiella verksamheter av betydelse för Kinas ekonomiska strategier.[53]

3.1.1 Cyberspionage en del av Kinas övergripande utvecklingsmål

Kinas satsningar på att avancera inom högteknologiska områden och att klättra i de globala värdekedjorna kräver stora satsningar på forskning och utveckling (FoU). År 2016 investerade Kina över 410 miljarder USD i FoU, näst mest i världen efter USA.[54] I enlighet med sina nationella strategier investerar Kina i teknologier som bedöms vara centrala för utveckling av såväl civila som militära sektorer. Framförallt sker satsningarna inom områden kopplade till informations- och kommunikationsteknologi, exempelvis chip- och halvledarsektorn. Andra intresseområden inkluderar artificiell intelligens, robotteknik och *Big Data*, vilket förklaras av att den kinesiska regeringen identifierat smart tillverkningsteknologi som central för Kinas möjligheter att utmana den rådande teknologiska dominansen bland industriländer.[55]

Därutöver uppmuntras kinesiska investerare av staten att förvärva internationella företag med teknologier och kompetenser som är relevanta för de strategiska sektorerna. Förvärven har såväl kommersiella som strategiska syften, och får delvis understöd och styrning av den kinesiska staten.[56]

Cyberspionage som syftar till att förvärva nödvändiga kunskaper och teknologier kan utgöra en effektiv metod för den kinesiska staten att driva sina intressen. Långsiktigt vill Kina vara världsledande inom de globala produktionsnätverkens mest högteknologiska segment. Kinesiska cyberintrång handlar således

[45] Van Cleave (2016).
[46] Eftimiades (2018).
[47] Connolly (2009).
[48] iDefense (2017); PwC, (2017).
[49] The National Bureau of Asian Research (2017).
[50] Office of the Director of National Intelligence & Office of the National Counterintelligence Executive (2011).
[51] Mandiant (2014); PwC (2017).
[52] Mandiant (2014).
[53] PwC (2017).
[54] OECD (2019).
[55] Wübbeke et al. (2016) s. 11.
[56] Ibid. s.7.

om mer än att endast komma över konsumentdata. Det handlar även om tillträde till regeringsnätverk samt att få tillgång till information om patenterad teknologi, tillverkningsprocesser och affärsplaner. Genom cyberspionage kan Kina spara in på FoU-utgifter och inhämta data för att komma ikapp andra industrinationer i strategiska sektorer. Samtidigt kan det leda till att andra länders konkurrenskraft hämmas, vilket i längden understödjer Kinas strävan om globalt teknologiskt ledarskap.

Med andra ord använder Kina cyberspionage som en del i att stödja sina strategiska utvecklingsmål.[57] Kinas cyberoperationer kan betraktas som en delkomponent i en komplicerad och mångfacetterad teknologisk utvecklingsplan där såväl lagliga som olagliga metoder ingår, exempelvis förvärv och forskningssamarbeten eller olika typer av spionage. Uppdagade kinesiska spionagefall – såväl cyberintrång som personbaserad inhämtning – har haft tydliga kopplingar till industrier kritiska för målbilder som formuleras i *Made in China 2025*.[58] Liksom strategiska investeringar utgör ett medel för att uppnå industriella utvecklingsmål, kan kinesiska cyberhackare identifiera sårbarheter i cyberrymden i syfte att bistå dessa ambitioner.

3.1.2 Otydliga gränsdragningar mellan statlig och privat verksamhet

Strukturen i den kinesiska ekonomin underlättar för staten att dra fördelar av industriellt spionage. Gränserna mellan statlig och privat kommersiell verksamhet är ofta otydliga, vilket innebär att intressen i båda sektorer kan sammanflätas och följaktligen underlätta för genomförande av cyberspionage.[59] Kinas underrättelselag från 2017 (art. 7) ställer krav på kinesiska företag, organisationer och medborgare att ge tillträde till samt samarbeta med kinesisk underrättelseinhämtning.[60] På så sätt kan privata och statliga intressen i vissa fall vara sammanlänkade och svåra att särskilja. Att lagen dessutom omfattar medborgare innebär att främjande av dessa intressen även kan involvera enskilda individer. Detta medför en problematik som förvisso inte nödvändigtvis berör cyberområdet, men som reflekterar den kinesiska regeringens möjligheter att ställa krav på enskilda medborgare att bidra till underrättelseinhämtning – inklusive anställda på utländska företag.

Vidare medför Kinas cybersäkerhetslag, som trädde i kraft 2017, försvårande omständigheter för utländska företag verksamma i Kina. Regleringar i lagen innebär att den kinesiska regeringen kan kräva att företag delar med sig av känslig information och teknologi samt källkoder som en del av Kinas säkerhetsprövning av ett företags produkter.[61] Lagen stipulerar också att företagsdata som berör kritisk infrastruktur ska lagras och bearbetas i Kina, vilket berör branscher såsom kommunikationsteknologi, energi, transport, och finansiella tjänster.

Den kinesiska underrättelselagen innebär naturligtvis inte att alla kinesiska företag eller medborgare automatiskt är agenter åt kommunistpartiet. Kinesiska bolag fattar alltjämt sina egna företagsbeslut och kommersiella drivkrafter utgör grundpelare. Däremot har gränsdragningarna mellan partiet och privata företag blivit alltmer otydliga. Kinas lagstiftning, utplacerade particeller och kommittéer i företag samt oskrivna regleringar, försvårar möjligheterna att skilja på privata och statliga verksamheter.[62]

Vad gäller inhämtning genom cyberspionage av teknologier med såväl civila som militära användningsområden kan det vara svårt att avgöra om syftet är militärt eller kommersiellt. Enligt FireEye sker ofta cyberattacker som potentiellt kan tjäna både militära och ekonomiska mål, exempelvis navigationsteknik.[63] Då det saknas information om vad den stulna informationen slutligen ska användas till blir det svårare att klassificera ett angrepp.

[57] National Counterintelligence and Security Center (2018).
[58] Sanger och Lee Myers (2018); Eftimiades (2018).
[59] Heilmann (2017).
[60] Standing Committee of the National People's Congress (2017).
[61] Sacks och Manyi (2018).
[62] Feng (2019).
[63] FireEye (2016) s. 14.

Kinas koncept om militär-civil fusion karaktäriseras just av otydlig gränsdragning.[64] Syftet med konceptet är att fördjupa samarbetet mellan militära och civila institutioner för att förbättra och mobilisera teknologi med civila, militära eller dubbla användningsområden, inom sektorer som exempelvis informations- och kommunikationsteknologi och rymd- och flygindustrin. Därmed integreras de militära och industriella sektorerna i ökad utsträckning, vilket också kan resultera i att den industriella sektorn kan komma att inrymma en avsevärt större strategisk betydelse ur ett militärt perspektiv för Kinas nationella säkerhet. Detta bör därtill ses i ljuset av att såväl privata som statsägda bolag är under långtgående kontroll av den kinesiska staten och därmed kommunistpartiet, vars intressen och prioriteringar trumfar det enskilda företagets.[65] Därigenom uppblandas ofta kommersiella intressen med nationalekonomiska och militära intressen i det kinesiska militär-industriella komplexet.

3.2 Kinas aktörer för cyberspionage

Kina använder en blandning av inhemska hackare, traditionella underrättelseagenter och infiltratörer anställda i utländska företag för att infiltrera datanätverk och otillbörligt tillskansa sig kommersiell och teknologisk information.[66] Spionaget utförs av individer inom regeringsinstanser, militären, statligt ägda företag, privata företag samt universitet. Enligt bedömningar från amerikanska FBI består det kinesiska nätverket av över 30 000 militära cyberspioner samt cirka 150 000 dataexperter inom den privata sektorn.[67]

Det kinesiska cyberlandskapet är dock inte helt monolitiskt och strikt statsdrivet. Bland aktörerna finns även enskilda patriotiska hackergrupper, privata säkerhetsentreprenörer och kriminella grupper.[68] Alla dessa kan arbeta utifrån liknande nationalistiska eller ekonomiska intressen, vilket innebär att skiljelinjerna mellan statssponsrad och självständig hackeraktivitet kan vara otydliga. Exempelvis finns uppgifter om att en självständig patriotisk organisation vid namn Red Hacker Alliance består av så många som 300 000 personer.[69]

Gruppen APT10 bedriver spionage som riktar in sig på immaterialrätt och annan känslig information. Enligt PwC har APT10 omfattande personal- och logistikresurser som stadigt har ökat under senare år.[70] Gruppen bedöms i sin tur bestå av ett flertal olika undergrupper med varierande ansvar, såsom utveckling av skadlig kod, domänregistrering, analysfunktioner och översyn av infrastruktur. APT10 har kopplats till ett antal olika cyberoperationer och har genomgått många förändringar sedan den avslöjades som APT1 i Mandiants rapport 2014.[71] Gruppen utgjorde en av åtminstone 20 APT-grupper med ursprung i Kina och beskrevs av Mandiant som en av Kinas mest framstående statssponsrade cyberaktörer. I rapporten kartlades hur APT1 sedan 2006 hade angripit minst 141 företag inom 20 olika industrier i ett flertal olika länder.

APT1/APT10 benämns i Mandiant-rapporten även som *enhet 61398*, vilket är PLA:s beteckning på samma grupp.[72] APT1/APT10/enhet 61398 och *enhet 61486* (även känd som APT2) är de två grupper som närmast associeras med kinesiska cyberattacker. Enhet 61486/APT2 antas bl. a stödja Kinas rymdövervakningsnätverk.

[64] Xinhua (2018).
[65] Hornby (2017); Lucas (2018).
[66] Van Cleave (2016) s.5-6; Eftimiades (2018); South China Morning Post (2018a).
[67] Van Cleave (2016); Gallagher (2018); Wilkes (2017).
[68] Intervjuer i Tokyo, mars 2019.
[69] Feakin (2013).
[70] PwC (2017).
[71] Mandiant (2014); PwC (2017).
[72] APT1/enhet 61398 har sedermera genomgått en förändring och fått sin nya beteckning APT10. Gruppen antas ha ökat avsevärt i kapacitet och omfattning i sina operationer, samt utvecklat nya intrångsverktyg. Dessutom antas APT10 ha omorganiserats från PLA till MSS. Se PwC (2017).

Mandiant bedömer att APT1/APT10 ägnar sig åt skadliga datornätverksoperationer som primärt fokuserar på politiskt, ekonomiskt och militärt relaterad underrättelseverksamhet.[73] Utöver dessa två enheter finns även en lång rad andra identifierade grupper som är kopplade till PLA, exempelvis APT3 (Gothic Panda), APT12 (Numbered panda), APT15 (Vixen panda), APT19 (Deep Panda), APT30, Aurora, Shady RAT och Night Dragon.[74]

Cloud Hopper-operationen härleddes till en enhet under ministeriet för statssäkerhet (MSS), den kinesiska säkerhetstjänsten. APT10 antas ha opererat från MSS-enhetens kontor i Tianjin. Således verkar åtminstone enhet 61398/APT10 ha flyttat från PLA till MSS. Detta utgör en förändring från tidigare förmodad struktur för statlig kinesisk cyberaktivitet mot kommersiella verksamheter, då enhet 61398 utgjorde PLA:s huvudsakliga organisation för cyberintrång mot kommersiell verksamhet. MSS – som är Kinas huvudsakliga civila underrättelseorgan – antas nu ha övertagit ledarskapet för det kommersiella cyberspionaget. PLA, som tidigare stod för majoriteten av kinesiska cyberattacker, har till synes skiftat från kommersiella måltavlor till politiskt och militärt spionage, medan MSS bedriver cyberspionage mot kommersiella verksamheter. Detta återspeglas bland annat i hur aktiviteter från icke-militära aktörer och hackare kopplade till MSS har ökat.[75]

[73] Mandiant (2014).
[74] Cooper (2018a) s.16.
[75] Eftimiades (2018).

4 Cyberoperationer mot Europa och Sverige

I Europa är EU:s största ekonomi, Tyskland, en attraktiv måltavla för kinesiska cyberangrepp.[76] Tyskland har pekat ut Kina som en av de främsta aktörer som försöker stjäla industriell information via cyberintrång, och den tyska säkerhetstjänsten Bundesamt für Verfassungsschutz (BFV) har varnat för att de kinesiska cyberattackerna mot landets företag har ökat.[77] Enligt BFV:s årsrapport från 2018 är kinesisk underrättelseverksamhet i Tyskland fokuserad på fyra områden: industri, forskning, teknologi och militär. Den kinesiska planen *Made in China 2025* tycks ha hämtat mycket inspiration från den tyska regeringens strategi år 2011 för industriell utveckling, *Industrie 4.0*. De sektorer som Tyskland identifierat som strategiska återkommer i *Made in China 2025*, och utgör således även måltavlor för det kinesiska cyberspionaget. Tyska företag har i ökad grad utsatts för kinesiskt spionage, däribland telekomindustrin och fordonsindustrin som den kinesiska staten sedan länge ser som strategiskt viktiga sektorer.[78] Bland övriga europeiska länder som har anklagat Kina för cyberspionage märks exempelvis Storbritannien och Tjeckien.[79]

Europa har en avancerad industriell och akademisk bas inom sektorer av intresse för Kinas strategiska mål och är ett attraktivt mål för Kinas cyberspionage, som kan komma att bli mer aktivt framöver. Inom Europa finns en avancerad kunskap och teknologi inom tillverkningsindustri och attraktiva branscher såsom fordon-, bioteknik- samt flyg- och rymdindustrin. Europeiska länder anses dessutom tillhöra de utvecklade ekonomierna med svagast cyberförsvar.[80]

Bland nordiska länder har säkerhetstjänsterna i Finland, Norge och Danmark pekat ut Kina som en av de främsta aktörer som utför cyberspionage och underrättelseaktiviteter inom ländernas gränser.[81] I Norge och Danmark har även bolag härlett hackerattacker till Kina. I februari 2019 bekräftade exempelvis det norska programvaruföretaget Visma uppgifter om att det varit föremål för cyberangrepp från en kinesisk aktör.[82] I Danmark uppdagades år 2014 att Kina under ett flertal år hade utfört omfattande cyberattacker mot danska försvarsföretag.[83] Norden inrymmer innovativa ekonomier med högteknologiska industrier vars tillgångar kan vara av intresse för många aktörer och kopplar an till Kinas strategiska mål. Dessutom har de nordiska länderna transparenta regeringsskick och öppna ekonomier, vilket kan underlätta för angripare.[84]

4.1 Sverige

Sveriges industriella bas har betydande likheter med Tyskland och har beskrivits som ett land med bristfälligt cyberförsvar.[85] Den svenska ekonomin är öppen och innovationsbaserad, och omfattar världsledande företag inom områden som telekommunikation och försvarsindustri. Även flygindustri och bioteknikutveckling tillhör sektorer där Sverige ligger i framkant. Sverige uppfattas av kinesiska bedömare som lätt att ha att göra med, politiskt stabilt, positivt inställt till frihandel och mindre misstänksamt mot Kina än andra västländer.[86] Sammantaget är Sverige ett attraktivt land att bedriva cyberspionage mot, inte minst från ett kinesiskt perspektiv mot bakgrund av Kinas industriella utvecklingsintressen.

[76] Martin (2018); Weiss och Burger (2018); Cooper (2018a) s.20.
[77] Martin (2018); Federal Ministry of the Interior, Building and Community (2017) s.35-37.
[78] Office of the United States Trade Representative (2018); Cooper (2018a); Weber (2010).
[79] Deutsche Welle (2017); Cerulus (2018).
[80] Lee-Makiyama (2018) s.12; intervjuer i Stockholm, december 2018.
[81] Finnish Security Intelligence Service (2018); Politiets sikkerhetstjeneste (2019); Politiets Efterretningstjeneste (2018).
[82] Drægni (2019).
[83] Fastrup och Lund (2014).
[84] FireEye (2015) s.3.
[85] Lee Makiyama (2018) s.12; intervjuer i Stockholm, december 2018.
[86] Hellström (2016).

Mycket riktigt har Sverige också drabbats av kinesiska cyberintrång. Såväl Säkerhetspolisen som Försvarets radioanstalt (FRA) har direkt eller indirekt pekat ut Kina som en aktiv aktör vad gäller cyberspionage riktat mot svenska intressen.[87] Bland de mer uppmärksammade fallen på senare tid märks Cloud Hopper-kampanjen, där myndigheter och företag hade varit drabbade under ett flertal år. Det utdragna angreppet föranledde FRA att öppet bekräfta att en statlig aktör låg bakom attacken, dock utan att namnge staten ifråga.[88] Därutöver framkom amerikanska anklagelser i december 2018 att Sverige var ett av tolv länder där företag angripits kontinuerligt av APT10 i över ett decennium.[89] Måltavlorna för cyberangreppen var verksamma inom flygindustrin, rymd- och satellitteknologi, medicinsk utrustning, elektronik, bank- och finansväsendet, telekom samt myndigheter. Ett flertal av dessa nämns som strategiska sektorer i Kinas statliga planer.

Cyberangreppen föranledde utrikesminister Margot Wallström att på Twitter kommentera att hon ”dela[r] oron som uttryckts över statsstödd uppsåtligt skadlig cyberaktivitet.” Utrikesministern pekade inte direkt ut Kina, men hänvisade till hur ”kampanjer som den så kallade Cloud Hopper undergräver förtroendet för cyberrymden och hotar den globala anslutning som vi alla är beroende av”.[90]

Liksom i övriga Europa, USA och andra delar av världen är mörkertalet för kinesiskt cyberspionage sannolikt betydande även i Sverige. Cyberangrepp i andra europeiska länder ger en tydlig indikation på vad svenska företag troligtvis också är utsatta för. Framförallt har Europas största ekonomier – Tyskland, Frankrike och Storbritannien – utsatts, men även mindre länder är av intresse för kinesiska hackare.[91] Dessutom riktar attackerna sig inte enbart mot stora företag, utan även mot mindre bolag som kan ha än större svårigheter att skydda sig mot dessa typer av angrepp. Sett till sektorer och ekonomisk öppenhet bland ansatta europeiska länder är bedömningen och antagandet i detta memo att Sverige mycket väl vara drabbat i stor omfattning.

Kinas förhållningssätt till spionage i allmänhet och cyberspionage i synnerhet skiljer sig markant från andra länder. Kommunistpartiet betraktar ekonomisk tillväxt som ett kärnintresse för nationell säkerhet,[92] vilket innebär att staten tillåts ge stöd till privata bolag i syfte att förbättra deras konkurrensfördelar på ett sätt som inte anses acceptabelt i marknadsekonomier. Kina använder delvis cyberoperationer för att främja nationella och industriella intressen och ser dem som en integrerad domän tillsammans med land, hav, luft och rymd.[93] Alltså ses de som en delmängd i hela systemet, snarare än en enskild domän, vilket upphöjer cyberoperationers betydelse.

Den kinesiska partistaten har således en förmåga att exploatera de öppna marknaderna i USA och Europa i syfte att anskaffa högteknologi. Kinesiska investeringar från såväl statsägda som privata företag i smart tillverkningsindustri i Europa har ökat sedan *Made in China 2025* antogs 2015.[94] Vid sidan av företagsförvärv utgör cyberspionaget en metod för att uppnå Kinas övergripande utvecklingsmål och ge kinesiska företag stöd för att de ska bli världsledande i sina respektive sektorer. Därmed kan länder med framstående högteknologiska industrier vara attraktiva för kinesiska angripare. Områden som exempelvis robotteknik, avancerad maskinutrustning och halvledare utgör områden där Kina investerar stora resurser inom FoU.[95]

I synnerhet är avancerade halvledarkomponenter som exempelvis datorchip av stort intresse för Kina. Halvledarkomponenter kan användas såväl civilt som militärt, och Kina måste importera dem då dess egen förmåga att tillverka de mest avancerade havledarkomponenterna är otillräcklig. Nästintill alla stora amerikanska halvledarbolag har erhållit investeringserbjudanden från kinesiska statsstödda

[87] Säkerhetspolisen (2019) s. 20-21, 33; Försvarets Radioanstalt (2018) s. 23.
[88] Sallinen (2017).
[89] Xu Klein (2018).
[90] Svenska Dagbladet (2018).
[91] Lee-Makiyama (2018) s.14.
[92] Se artikel 2 i Standing Committee of National People's Congress (2015) *National Security Law of the People's Republic of China*.
[93] Information Office of the State Council of the People's Republic of China (2015).
[94] Wübbeke et al. (2016).
[95] Ibid.

företag. Även i Sverige har Kina visat intresse inom denna sektor. Sedan några år tillbaka äger kinesiska företag med koppling till försvarsindustrin tre svenska halvledarbolag, varav två delägdes av svenska staten.[96] Därmed har kinesiska aktörer med militär bakgrund inte bara intresserat sig för, utan även redan förvärvat svensk teknologi med dubbla användningsområden i linje med sina strategiska mål. Det är troligt att kinesiska aktörer har försökt att inhämta sådan teknologi även via cyberspionage i Sverige.

Säkerhetspolisen bedömer att Sverige befinner sig inom det kinesiska intresseområdet rörande såväl strategiska investeringar och förvärv som för samarbeten inom akademin och näringslivet, liksom för underrättelseverksamhet via cyberangrepp.[97] Mot denna bakgrund fastslog Säkerhetspolisen i sin årsbok att kostsamma förebyggande insatser krävs för att öka medvetenheten och reducera sårbarheten hos svenska myndigheter och företag.

4.2 Slutsatser

Det kinesiska kommunistpartiet avdelar stora resurser för sina strategier som syftar till att Kina ska bli en innovativ och världsledande stormakt. Teknologiska framsteg utgör centrala byggstenar för den kinesiska regeringens mål att avancera i de globala värdekedjorna samt att bli en modern och högteknologisk försvarsmakt. Givet hur Kina prioriterar cyberområdet som ett strategiskt viktigt instrument för att uppnå sina utvecklingsmål kan man förvänta sig att Kina kommer att fortsätta ägna sig åt rådande cyberoperationer, i synnerhet inom områden som bedöms som avgörande för landets industriella strategier. En stor del av Kinas cyberspionage är inriktat på sektorer och industrier som den kinesiska regeringen har identifierat som strategiskt viktiga, såsom nästa generations IT, robotteknik och rymd- och flygteknik. Därmed kan Kinas cyberspionage betraktas som en delkomponent för att stödja den kinesiska regeringens strategiska utvecklingsmål.

Cyberspionage är ett relativt kostnadseffektivt medel för Kina att uppnå sina strategiska mål, men är samtidigt förknippat med politiska risker. Kinas cyberspionage har ökat i omfattning under senare år. Dessutom har kinesiska cyberoperationer blivit alltmer avancerade och uthålliga.

För svenskt vidkommande utgör myndigheter och företag attraktiva måltavlor för de kinesiska cyberoperationerna. Innovativa ekonomier med högteknologiska industrier bedöms vara av största intresse för Kinas industriella cyberspionage. För länder med nischteknologier och världsledande företag som Sverige kan det kinesiska cyberspionaget komma att öka, mot såväl civila som försvarsrelaterade industrier. På sikt medför dessa aktiviteter betydande utmaningar för Sveriges konkurrenskraft, vilket i förlängningen kan påverka det svenska välståndet som helhet.

Ytterligare en aspekt, som inte tas upp i detta memo men som kan föranleda vidare forskning, rör de globala leveranskedjorna för elektroniska produkter, och i synnerhet frågan om komponenter tillverkade i Kina. Det finns idag farhågor om att den kinesiska staten kan exploatera de globala leveranskedjorna till att utveckla bakdörrar till utländsk mjukvara genom att placera innehåll på exempelvis kretskort som används i produkter och komponenter.[98] Problematiken aktualiserades under hösten 2018 då en artikel publicerad i *Bloomberg* uppgav att kinesisk militär placerat små sändare på moderkort tillverkade i Kina.[99]

Relaterat till detta område finns även anledning att vidare undersöka den problematik kring 5G-utbyggnad som debatterats aktivt under 2018-2019. Specifikt har debatten involverat misstänksamhet mot de kinesiska telekomföretagen Huawei och ZTE, och risken för att deras utrustning ska innehålla dolda bakdörrar och kunna användas för spionage av den kinesiska staten.[100] Frågan har även aktualiserats i Sverige i samband med utrullningen av 5G-nätverk i landet. Den kinesiska

[96] Feng (2019).
[97] Säkerhetspolisen (2019) s. 33.
[98] Beeny (2018) s. V.
[99] Bloomberg (2018).
[100] AFP (2019).

cybersäkerhetslagen (art. 28) förstärker denna farhåga då den specificerar att kinesiska nätverksoperatörer och telekomföretag vid behov ska förse polis och underrättelsetjänst med ”tekniskt stöd och assistans”.[101] Idag finns därmed en risk för angrepp utifrån mot känslig infrastruktur och inhämtning av information, men även infiltration inifrån. Frågan om kopplingen mellan statliga aktörer och leverantörer av telekominfrastruktur kan således bli föremål för vidare forskning.

[101] National People’s Congress of the People’s Republic of China (2016).

5 Källförteckning

AFP (2019) *Calls for Huawei boycott get mixed response in Europe,* 13 januari 2019. https://www.afp.com/en/news/15/calls-huawei-boycott-get-mixed-response-europe-doc-1c47ur2

Beeny, Tara (2018) "Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology", *U.S.-China Economic and Security Review Commission,* april 2018. s.V. https://docs.house.gov/meetings/IF/IF16/20180516/108301/HHRG-115-IF16-20180516-SD105-U105.pdf

Blair, Dennis C. och Huntsman, Jr. (2013) "The Report of the Commission on the Theft of American Intellectual property", *National Bureau of Asian Research,* maj 2013. http://ipcommission.org/report/IP_Commission_Report_052213.pdf

Bloomberg (2018) *The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies*, 4 oktober, 2018. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Carbon Black (2018) "Quarterly Incident Response Threat Report, Destructive Cyberattacks Increase Ahead of 2018 Midterm Elections", *Carbon Black,* november 2018. https://www.carbonblack.com/quarterly-incident-response-threatreport/november-2018/

Central Committee of the Communist Party of China (2015) *The 13th Five-Year Plan for Economic and Social Development of the People's Republic of China (2016-2020).* http://en.ndrc.gov.cn/newsrelease/201612/P020161207645765233498.pdf

Cerulus, Laurens (2018) "West accuses Beijing of 'extensive' cyber espionage", *Politico*, 28 december, 2018. https://www.politico.eu/article/china-cyber-espionage-uk-us-accuses-beijing/

China Daily (2010) *China 'biggest victim' of cyber attacks*, 25 januari 2010. http://www.chinadaily.com.cn/bizchina/2010-01/25/content_9369226.htm

Chinese Academy of Sciences (2016) *President Xi Says China Faces Major Science, Technology 'bottleneck',* 1 juni, 2016. http://english.cas.cn/newsroom/news/201606/t20160601_163827.shtml

Connolly, Kate (2009) "Germany accuses China of industrial espionage," *The Guardian*, 22 juli, 2009. http://www.theguardian.com/ world/2009/jul/22/germany-china-industrial-espionage

Cooper, Zack (2018a) "China's latest cyber offensive - and what to do about it", *New York Post*, 4 oktober, 2018. https://nypost.com/2018/10/04/chinas-latest-cyber-offensive-and-what-to-do-about-it/

Cooper, Zack (2018b) "Understanding the Chinese Communist Party's Approach to Cyber-Enabled Economic Warfare", *Foundation for Defense of Democracies*, september 2018

Costello, John och McReynolds, Joe (2018) "China's Strategic Support Force: A Force for a New Era*", Center for the Study of Chinese Military Affairs, Institute for National Strategic Studies, China Strategic Perspectives*, No. 13, oktober 2018. https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf

Creemers, Roger, Triolo, Paul, och Webster, Graham (2018) "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)", *New America*, 29 juni, 2018. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/

Defense Science Board, Department of Defense (2017) "Task Force on Cyber Deterrence", *Office of the Secretary of Defense*, februari, 2017. s. 4. https://www.acq.osd.mil/dsb/reports/2010s/dsb-cyberdeterrencereport_02-28-17_final.pdf

Deutsche Welle (2017) *China denies using social media to infiltrate German politics and business circles*, 11 december, 2017.
https://www.dw.com/en/china-denies-using-social-media-to-infiltrate-german-politics-and-business-circles/a-41733287

Drægni, Ingvill (2019) ”Visma utsatt for hackerangrep fra Kina”, *TV2*, 6 februari, 2019.
https://www.tv2.no/a/10396361/

Eftimiades, Nicholas (2018) “Uncovering Chinese Espionage in the US”, *The Diplomat*, 28 november, 2018.
https://thediplomat.com/2018/11/uncovering-chinese-espionage-in-the-us/

Fastrup, Niels & Lund, Michael (2014) ”Fremmede stater hacker sig ind i Danmarks største virksomheder”, *DR Nyheder*, 21 september 2014.
https://www.dr.dk/nyheder/penge/fremmede-stater-hacker-sig-ind-i-danmarks-stoerste-virksomheder

Feakin, Tobias (2013) “Enter the Cyber Dragon: Understanding Chinese intelligence agencies’ cyber capabilities”, *Australian Strategic Policy Institute*, Issue 50, 23 juni, 2013.

Federal Ministry of the Interior, Building and Community (2017) “Brief Summary 2017 Report on the Protection of the Constitution – Facts and Trends”, *Federal Ministry of the Interior, Building and Community*, 2017.

Feng, Ashley (2019) ”We Can’t Tell if Chinese Firms Work for the Party”, *Foreign Policy*, 7 februari, 2019.
https://foreignpolicy.com/2019/02/07/we-cant-tell-if-chinese-firms-work-for-the-party/

Feng, Emily (2019) ”How China acquired mastery of vital microchip technology”, Financial Times, 29 januari, 2019.
https://www.ft.com/content/7cfb2f82-1ecc-11e9-b126-46fc3ad87c65

Finnish Security Intelligence Service (Supo) (2018) *National Security review 2018*, 2018.
https://www.supo.fi/instancedata/prime_product_julkaisu/intermin/embeds/supowwwstructure/76777_2018_National_Security_Review_A4-www.pdf?34b9d3053367d688

FireEye (2015) *Cyber Threats to the Nordic Region*, maj 2015.

FireEye (2016) *Redline Drawn: China recalculates its use of cyber espionage*, juni 2016.

FireEye (2018) *M-trends 2018*, 2018.

Försvarets Radioanstalt (2017) *FRA Årsrapport 2017*.
https://www.fra.se/download/18.72cfabb316104f6be5a30/1518177844513/FRA-arsrapport-2017-highres.pdf

Gallagher, Sean (2018) “New Data Shows China Has “Taken the Gloves Off” in Hacking Attacks on US”, *Arstechnica*, 1 november, 2018.
https://arstechnica.com/information-technology/2018/11/new-data-shows-china-has-taken-the-gloves-off-in-hacking-attacks-on-us/

Heilmann, Sebastian (2017) “How the CCP embraces and co-opts China’s private sector”, *Mercator Institute for China Studies*, 21 november, 2017.
https://www.merics.org/en/blog/how-ccp-embraces-and-co-opts-chinas-private-sector

Hellström, Jerker (2016) ”Sounding boards and door-openers – China’s political priorities in the Nordic countries”, *FOI*, maj 2016.
https://www.foi.se/download/18.7fd35d7f166c56ebe0bdf16/1542369110802/Chinas-Political-Priorities_FOI-Memo-5701.pdf

Hornby, Lucy (2017) “Communist party asserts control over China Inc”, *Financial Times*, 3 oktober, 2017.
https://www.ft.com/content/29ee1750-a42a-11e7-9e4f-7f5e6a7c98a2

iDefense (2017) "2017 Cyber Threatscape Report – Midyear Cybersecurity Risk Review: Forecast and Remediations", *Accenture Security*, 2017.
https://www.accenture.com/t20170721T220639Z__w__/us-en/_acnmedia/PDF-57/Accenture-2017-cyber-year-threatscape-report.pdf

Johnson, Tim (2018) "China backed off from hacking U.S. companies. Now it is at it again.", *McClatchy*, 7 juni, 2018.
https://www.mcclatchydc.com/news/nation-world/national/national-security/article212666139.html

Kania, Elsa B. och Costello, John K. (2018) "The Strategic Support Force and the Future of Chinese Information Operations", *The Cyber Defense Review*, Vol. 3, No. 1 (SPRING 2018), pp. 105-122.

Lee-Makiyama, Hosuk (2018) "Stealing Thunder", *European Centre for International Political Economy*, Occasional Paper No. 2, 2018.

Lewis, James (2018) "Economic Impact of Cybercrime— No Slowing Down", *CSIS*, februari 2018.
https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf

Lucas, Louise (2018) "The Chinese Communist party entangles big tech", *Financial Times*, 19 juli, 2018.
https://www.ft.com/content/5d0af3c4-846c-11e8-a29d-73e3d454535d

Mandiant (2014) *APT1 – Exposing One of China's Cyber Espionage Units,* 2014.

Martin, Michelle (2018) "German security office warned German firms about Chinese hacking – report", *Reuters*, 19 december, 2018.
https://uk.reuters.com/article/uk-germany-security/german-security-office-warned-german-firms-about-chinese-hacking-report-idUKKBN1OI0HS

National People's Congress of the People's Republic of China (2016) *中华人民共和国网络安全法* [Folkrepubliken Kinas internetsäkerhetslag], 11 juli, 2016.
http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm

New Europe (2018) *Finnish intel says Russia and China continue to actively deploy assets*, 11 december, 2018.
https://www.neweurope.eu/article/finnish-intel-says-russia-and-china-continue-to-actively-deploy-assets/

OECD (2019) *Gross Domestic Spending on R&D*, (Hämtat 8 januari 2019).
https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm

Office of the Director of National Intelligence & Office of the National Counterintelligence Executive (2011) *Foreign Spies Stealing US Economic Secrets in Cyberspace*, oktober 2011.
https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf

Office of the Director of National Intelligence & National Counterintelligence and Security Center (2018) *Foreign Economic Espionage in Cyberspace*. 26 juli, 2018

Office of the United States Trade Representative (2018) *Update concerning China's acts, policies and practices related to technology transfer, intellectual property, and innovation*, 20 november, 2018.
https://ustr.gov/sites/default/files/enforcement/301Investigations/301%20Report%20Update.pdf

Oxford Dictionaries (2019) *Cyber espionage*. Hämtat 15 mars 2019.
https://en.oxforddictionaries.com/definition/cyberespionage

Politiets Efterretningstjeneste (2018) *Årlig Redogørelse 2017*, 2018.
https://www.pet.dk/~/media/Aarsberetninger/rligredegrelseforPET2017WEBpdf.ashx

Politiets sikkerhetstjenestes (2019) *Trusselvurdering 2018*, 2019.
https://www.pst.no/globalassets/artikler/trusselvurderinger/psts-trusselvurdering-2018.pdf

PwC (2017) *Operation Cloud Hopper*, April 2017.

Racicot, Jonathan (2014) "The Past, Present and Future of Chinese Cyber Operations", *Canadian Military Journal*, Vol. 14, No. 2, 2014.

Sacks, Samm och Manyi, Kathy Li (2018) "How Chinese Cybersecurity Standards Impact Doing Business in China", *Center for Strategic & International Studies*, augusti 2018.
https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180802_Chinese_Cybersecurity.pdf?EqyEvuhZiedaLDFDQ.7pG4W1IGb8bUGF

Sallinen, Jani Pirttisalo (2017) *"FRA: Statlig aktör bakom massiv cyberattack", Svenska Dagbladet*, 4 juni, 2017.
https://www.svd.se/fra-delger-statlig-aktor-bakom-massiv-cyberattack

Sallinen, Jani Pirttisalo (2018a) "Hultqvist vill inte peka ut Kina för cyberangrepp", *Svenska Dagbladet*, 24 april 2018.
https://www.svd.se/hultqvist-vill-inte-peka-ut-kina-for-cyberangrepp

Sallinen, Jani Pirttisalo (2018b) "Så angrep Kina "naiva" Sverige i det fördolda", *Svenska Dagbladet*, 22 April 2018.
https://www.svd.se/sa-angrep-kina-naiva-sverige-i-det-fordolda

Sanger, David E. och Lee Myers, Steven (2018) "After a Hiatus, China Accelerates Cyberspying Efforts to Obtain U.S. Technology", *New York Times*, 29 november 29, 2018.
https://www.nytimes.com/2018/11/29/us/politics/china-trump-cyberespionage.html

Sebenius, Alyza and Grant, Nico (2018) "China Violating Cyber Agreement With U.S., NSA Official Says", *Bloomberg*, Nov. 8, 2018.
https://www.bloomberg.com/news/articles/2018-11-08/china-violating-cyber-agreement-with-u-s-nsaofficial-says.

South China Morning Post (2018a) *China 'has taken the gloves off' in its thefts of US technology secrets*, 1 November, 2018.
https://www.scmp.com/news/world/united-states-canada/article/2173843/china-has-taken-gloves-its-thefts-us-technology

Standing Committee of National People's Congress (2015) *National Security Law of the People's Republic of China*, 1 juli 2015. Available in English at
https://www.chinalawtranslate.com/2015nsl/?lang=en

Standing Committee of the National People's Congress (2017) *National Intelligence Law of the People's Republic of China (国家情报法)*, 27 juni, 2017.
http://www.npc.gov.cn/npc/xinwen/2017-06/27/content_2024529.htm

Svenska Dagbladet (2018) *Sverige pekas ut som mål för kinas cyberattacker*, 20 december, 2018.
https://www.svd.se/usa-kineser-stams-for-hackerattacker

Säkerhetspolisen (2019) *Årsbok 2018*.
https://www.sakerhetspolisen.se/download/18.6af3d1c916687131f1fae5/1552543607309/Arsbok-2018.pdf

Theoretical Studies Center Group, Cyberspace Administration of China "深入贯彻习近平总书记网络强国战略思想 扎实推进网络安全和信息化工作" [Fördjupad implementering av Generalsekreterare Xi Jinpings strategiska tänkande om en stark internetmakt, och att driva internetsäkerhets- och informatiseringsarbetet framåt med beslutsamhet], *Qiushi*, 15 september, 2017.
http://www.qstheory.cn/dukan/qs/2017-09/15/c_1121647633.htm

The Information Office of the State Council of the People's Republic of China (2015) *China's Military Strategy*, 27 maj, 2015.
http://english.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm

The National Bureau of Asian Research (2017) *Update to the IP Commission – The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy*, februari 2017.
http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.pdf

The State Council of the People's Republic of China (2006) *The National Medium- and Long-Term Plan for the Development of Science and Technology (2006-2020)*
https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/China_2006.pdf

The State Council of the People's Republic of China (2015), *Made in China 2025（中国制造 2025), 7* juli, 2015.
http://www.cittadellascienza.it/cina/wp-content/uploads/2017/02/IoT-ONE-Made-in-China-2025.pdf

U.S.-China Economic and Security Review Commission (2007) *2007 Report to Congress: Executive Summary*, 2007.
https://www.uscc.gov/sites/default/files/annual_reports/2007-Report-to-Congress-Executive%20Summary.pdf

Van Cleave, Michelle (2016) "Chinese Intelligence Operations and Implications for U.S. National Security," *Statement for the Record: Testimony before the U.S.-China Economic and Security Review Commission*, 9 juni, 2016.
https://www.uscc.gov/sites/default/files/Michelle%20Van%20Cleave_Written%20Testimony060916.pdf

Verizon (2013) "2013 Data Breach Investigations Report," *Verizon*, 2013.
http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

Weber, Joshua (2010) "Industrial espionage threatens German companies and jobs", *Deutsche Welle*, 26 juni, 2010.
https://www.dw.com/en/industrial-espionage-threatens-german-companies-and-jobs/a-5645869

Weiss, Patricia & Burger, Ludwig (2018) "Exclusive: German prosecutors charge Chinese-born engineer in industrial espionage case", Reuters, 15 november, 2018.
https://www.reuters.com/article/us-germany-chemicals-espionage-exclusive/exclusive-german-prosecutors-charge-chinese-born-engineer-in-industrial-espionage-case-idUSKCN1NK0UT

Wilkes, William (2017) "Hit by Chinese Hackers Seeking Industrial Secrets, Germans Manufacturers Play Defense", *Fox Business*, 23 september, 2017.
https://www.foxbusiness.com/features/hit-by-chinese-hackers-seeking-industrial-secrets-german-manufacturers-play-defense

Wübbeke, Jost., Meissner, Mirjam., Zenglein, Max J., Ives, Jaqueline., och Conrad, Björn. (2016) "Made in China 2025 – The making of a high-tech superpower and consequences for industrial countries", *Mercator Institute for China Studies*, No. 2, december 2016.

Xi Jinping (2017) " 决胜全面建成小康社会 夺取新时代中国特色社会主义伟大胜利——在中国共产党第十九次全国代表大会上的报告" [Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era – Report Delivered at the 19th National Congress of the Communist Party of China], 27 oktober 2017.
http://www.xinhuanet.com//politics/19cpcnc/2017-10/27/c_1121867529.htm

Xinhua (2018) *Xi calls for deepened military-civilian integration*, 12 mars, 2018.
http://www.xinhuanet.com/english/2018-03/12/c_137034168.htm

Xu Klein, Jodi (2018) "China accused by US and allies of 'massive hacking campaign to steal trade secrets and technologies'", *South China Morning Post*, 22 december, 2018.
https://www.scmp.com/news/world/united-states-canada/article/2178981/us-and-more-dozen-allies-condemn-china-economic

Zhang Yue (2018) "More reform to encourage innovation", *China Daily*, 12 juni, 2018.
http://www.chinadaily.com.cn/a/201812/06/WS5c085d4ba310eff30328f56c.html