Stefan Kristiansson

OM UNDERRÄTTELSE-HOTET MOT SVERIGE

Spionerі eller underrättelseverksamhet har ökat världen över under de senaste decennierna. Det säkerhetspolitiska läget har skärpts och många länder förbereder sig för väpnade konflikter. Misstron mellan de största aktörerna är betydande och säkerhetspolitiska bedömare använder ofta termer som *oförutsägbarhet*, ökande komplexitet och *snabba förändringar* för att beskriva dagens geopolitiska tillstånd.

Det är inte bara inom de rent säkerhetspolitiska områdena som problemen ökar. Även inom den internationella handeln har läget blivit mer kritiskt; frihandeln ifrågasätts och protektionismen breder ut sig samtidigt som hotet om handelskrig finns där som ett mörkt moln. Vidare hårdnar konkurrensen och kampen rörande teknikutvecklingen är påtaglig. Industrispionage och affärsunderrättelseverksamhet är utbredd.

Förutom stora satsningar på olika former av väpnade angrepp utvecklas förmågor att i fredstid eller i skedet mellan fred och krig kunna destabilisera och utöva påtryckningar för att uppnå politiska mål på egen hand. Denna gråzonsproblematik är inte på något sätt ny men den ger anledning till ökande oro.

Även Sverige drabbas av det försämrade säkerhetspolitiska läget. Vi berörs av motsättningarna mellan Ryssland och västvärlden. Östersjöområdet och Arktis är områden där stormaktsintressen kolliderar. Det säkerhetspolitiska klimatet har under de senaste åren försämrats; Ryssland upplever sig hotat av väst och har genomfört en omfattande upprustning av sina väpnade styrkor. Samtidigt har de inrikespolitiska problemen ökat och den ryska ekonomin stagnerat till följd av fallande oljepriser och internationella sanktioner. Levnadsvillkoren för en stor del av befolkningen har försämrats och stödet för president Putin minskar.

Utöver de säkerhetspolitiska aspekterna rörande Rysslands agerande så påverkas vi allt mer av utvecklingen i Kina. Regimen har en tydlig ambition att bli en ledande

Stefan Kristiansson, generalmajor, är seniorrådgivare för IBM och var chef för militära underrättelse och säkerhetstjänsten (MUST) mellan 2007–12 och dess ställföreträdande chef 2004–07.

global stormakt och *The Belt and Road Initiative* handlar inte främst om handelsvägar utan om en ny världsordning. Kinas tydliga intresse för Arktis och möjliga farleder genom Norra Ishavet innebär att en ny aktör med stora resurser påverkar läget i vårt närområde. Utvecklingen av en stark försvarsmakt anses vara en förutsättning för att bli en ledande global aktör. Samtidigt som Kina gör stora satsningar på det militära området så vidareutvecklas landets cyberförmåga ytterligare från en redan hög nivå.

Spionerі har dock funnits i alla tider. Furstar och andra makthavare har alltid ansett sig behöva information om sina fiender. Underrättelser har inhämtats på många olika sätt. Man har kommit över och läst brev, knäckt koder, avlyssnat samtal, skickat ut spioner, värvat agenter och utnyttjat insiders, förhört avhoppare och fångar, använt olika former av teknisk inhämtning och utnyttjat informationsläckor. I tider av oro och krigsrisk har informationsbehovet ökat och man har tvingats att ta större risker.

Vilka intressen står då på spel för Sverige? Försvarsberedningens delrapport ”Motståndskraft” (2017:66) konstaterar att ”Spionage och angrepp från statliga och statsunderstödda aktörer mot skyddsvärd verksamhet i Sverige eller mot svenska intressen i utlandet kan syfta till att tillskansa sig information om svenska ekonomiska intressen, företag, forskning, försvarsförmåga och planering, våra säkerhetspolitiska avsikter, samhällsviktig verksamhet och kritisk infrastruktur. Det kan också handla om att en motståndare vill vilseleda, binda begränsade resurser eller försvåra effektivt beslutsfattande inför ett väpnat angrepp och på det sättet försämra våra förutsättningar att sätta oss till motvärn.”[1]

Därtill är EU-politiken, vårt förhållande till Nato och våra bilaterala relationer på försvarsområdet av intresse för en potentiell motståndare. Insikten om att Sverige inte kommer att klara sig undan en konflikt i närområdet ökar också intresset för hur vi kommer att agera i en sådan situation. Våra säkerhetspolitiska vägval, särskilt den militära alliansfriheten, leder till ett ökat behov av underrättelser rörande politiska inriktningar och militära förberedelser för en konflikt. Utvecklingen av vår militära och civila försvarsförmåga – dess styrkor, svagheter och sårbarheter – är också av intresse, särskilt i ett gråzonsscenario. Detta gäller hela samhället: centralt, regionalt och lokalt.

Underrättelseinhämtning i Sverige syftar även att främja geopolitiska mål bortom Sveriges närområde och inrikespolitiska agendor. Stater strävar efter att tillskansa sig teknologiskt övertag genom att stjäla företagshemligheter, uppköp och ta del av vårt lands universitetsforskning för att höja sin militära kapacitet. Därtill försöker auktoritära stater motverka politisk opposition genom flyktingspionage.

Denna rapport syftar till att ge en aktuell bild av hur underrättelsehotet mot vårt land ter sig idag och hur de viktigaste aktörerna agerar. Vissa utländska underrättelse- och säkerhetstjänsters bedömningar, erfarenheter och kapacitet redovisas i syfte att illustrera hur hot även kan drabba oss.

Avsikten är inte att ge en detaljerad bild av hur till exempel värvning av informatörer genomförs eller ge en uttömmande beskrivning av IT-hotet. Den som är intresserad av dessa utmaningar kan läsa de årsrapporter som underrättelse- och säkerhetsmyndigheterna ger ut. Underlaget i denna rapport bygger uteslutande på öppna källor.

De viktigaste aktörernas underrättelsekapacitet

Ryssland

Underrättelsetjänst bedrivs av SVR, som är den ryska statens organ för utrikes underrättelsetjänst, samt GRU som är de väpnade styrkornas underrättelsetjänst.[2] Vidare bedriver den ryska säkerhetstjänsten FSB säkerhetsunderrättelsetjänst och kontraspionage i Ryssland samt i de

1 Försvarsberedningen, 2017.

2 Benämningen GRU ändrades officiellt 2010 till GU. Trots detta används GRU fortfarande i dagligt tal.

forna sovjetstaterna. Cheferna för SVR respektive FSB rapporterar direkt till presidenten medan chefen för GRU rapporterar till generalstabschefen samt till försvarsministern. Cheferna för SVR respektive FSB är adjungerade ledamöter av Nationella säkerhetsrådet. De ryska underrättelsetjänsterna har global räckvidd och opererar världen över där det anses finnas ryska intressen. Underrättelseförmåga och cyberkapacitet tillmäts mycket stor betydelse.

Det har under lång tid varit uppenbart att de ryska underrättelsetjänsterna förutom traditionell inhämtning och analys av information också används för utföra offensiva operationer. I januari 2019 införde EU sanktioner mot viceamiral Igor Kostyukov som är chef för GRU och organisationens andreman Alexander Alekseyev för mordförsöket på Sergei Skripal och hans dotter Yulia den 4 mars 2018 i Salisbury. De båda är dessutom upptagna på den amerikanska sanktionslistan sedan 2016 för påverkansoperationer riktade mot det amerikanska presidentvalet.[3] 2016 gjorde Ryssland ett sista försök att hindra Montenegro från att ansöka om medlemskap i Nato. 2017 dömdes två GRU-officerare i sin frånvaro till långa fängelsestraff för att ha rekryterat inhemska Nato-motståndare i uppdrag att mörda premiärministern och förhindra en omröstning i parlamentet. GRU-officerarna ska ha försett Nato-motståndarna med stora summor pengar för inköp av vapen samt tillhandahållit kvalificerad sambandsutrustning.[4] Ryssland har använt och kan förväntas fortsätta använda sina underrättelsetjänster för att uppnå politiska mål på utländskt territorium.

GRU

GRU är betydligt större än SVR och har både underrättelsepersonal, så som försvarsattachéer och annan personal med diplomatisk täckmantel, och avancerade tekniska resurser såsom spaningssatelliter, signalspaningsflygplan och fartyg. Det finns uppgifter som tyder på att organisationen har ett stort antal spaningssatelliter. GRU har också ett mycket nära samarbete med de ryska specialförbanden, Spetsnaz. Förutom personbaserad underrättelseinhämtning har GRU en ledande roll i cyberkrigföring. APT 28, även kallad Fancy Bear, är organiserad inom GRU:s sjätte direktorat.[5]

Enligt många bedömare har GRU bland mycket annat utfört attacker mot The World Doping Agency (WADA), Organisationen för förbud mot kemiska vapen (OPCW) samt mot den organisation som utredde nedskjutningen av MH17.[6] Dessutom anses GRU ligga bakom ett intrångsförsök i ett laboratorium i närheten av Bern som analyserar biologiska och kemiska stridsmedel, bland annat nervgiftet Novitjok som användes i mordförsöket på Sergej Skripal och hans dotter i Salisbury.[7] Bellingcat, ett kollektiv för grävande journalism, fann dessutom att GRU sannolikt varit delaktig i vissa faser av nedskjutningen av MH17.[8]

GRU anses ta betydande risker. Mark Galeotti vid University College London menar att ”att inte ertappas är inte deras främsta prioritet. Vägledningen från Kreml till GRU är ‘få jobbet gjort, oroa er inte om de politiska kostnaderna’.”[9]

SVR

SVR är Rysslands civila utrikes underrättelsetjänst som bedriver inhämtning företrädesvis mot civila mål. SVR-chefer rekryteras vanligtvis ur partieliten eller från den högsta tjänstemannanivån. Den nuvarande chefen,

3 Peel, M., 2019.

4 Farmer, B., 2019.

5 APT – Advanced Persistent Threat är en beteckning på planerade cyberoperationer som genomförs under lång tid mot specifika mål med avancerad teknik i syfte att till exempel tränga in i ett nätverk för att stjäla information. Ofta riktas operationerna mot ett företag genom dess IT-leverantör.

6 Faulconbridge, G., 2018.

7 Ny Teknik, 2018.

8 Bellingcat ”Identifying the Separatists Linked to the Downing of MH17. Juni 19 2019.

9 Smith, B., 2018.

Sergey Naryshkin har varit talman i Duman. Mikhail Fradkov var premiärminister 2004–2007 och var därefter chef för SVR fram till 2016. Chefen för SVR rapporterar direkt till presidenten och har därmed en betydande möjlighet att påverka dennes uppfattning om omvärldsutvecklingen. SVR-chefen Sergey Naryshkin omfattas, likt GRU-chefen, av amerikanska sanktioner. Naryshkin togs upp på sanktionslistan efter Rysslands annektering av Krim 2014.

SVR bedöms inte ha samma cyberkapacitet som GRU men bedriver operationer med APT 29 även kallad Cozy Bear främst mot civila mål[10]. APT 29 anses ligga bakom en attack 2017 bland annat mot Norges utrikesdepartement, underrättelsetjänst och försvarsmakt.

Anna Chapman, som arresterades av amerikanska myndigheter 2010 tillsammans med ett tiotal andra andra ryssar, var SVR-spion. Hon var en av flera ryska underrättelseofficerare som följde och rapporterade om amerikansk politik och som senare blev utvisade.[11]

Kina

Kina har en långsiktig strategi rörande landets utveckling fram till 2050. *The Belt and Road Initiative,* eller Sidenvägsinitiativet, har nämnts tidigare. *Made in China 2025,* som handlar om utvecklingen av den kinesiska industrin till världsledande inom bland annat robotik och IT, är en annan viktig del i den kinesiska regimens stormaktsambitioner. President Xi Jinping har satt press på alla kinesiska aktörer att medverka till att visionerna förverkligas. Naturligtvis inkluderar detta också underrättelse- och säkerhetstjänsterna som genomför industrispionage och stöld av tekniklösningar inom strategiskt viktiga områden. För att nå det politiska ledarskapets olika mål verkar allt från nanoteknik till metoder inom jordbrukssektorn vara av intresse.

Att utveckla den kinesiska försvarsmakten, Folkets befrielsearmé (PLA), anses vara en av grundpelarna för att bli en global stormakt och har därmed en mycket hög prioritet. För att stärka landets militära kapacitet strävar Kinas ledare efter en långtgående integrering av landets militära och civila kompetens.[12] Detta innebär bland annat att civila företag i utlandet ska kunna inhämta och leverera teknik för utveckling av militära system.

Kinas civila underrättelseverksamhet drivs av ministeriet för statssäkerhet (MSS). Den nationella underrättelselagen ger MSS ett brett mandat att bedriva underrättelseverksamhet med olika metoder både i Kina och utomlands. Mandatet omfattar även ekonomiskt spionage. MSS bedöms enligt vissa ha cirka 100 000 anställda varav knappt hälften är stationerade utomlands. PLA har också en viktig roll i den kinesiska underrättelseapparaten. PLA driver bland annat personbaserad inhämtning, signalspaning och elektronisk krigföring.

Den 27 juni 2017 trädde den kinesiska nationella underrättelselagen i kraft. Lagen innebär att både statliga och privata kinesiska företag samt alla kinesiska medborgare kan åläggas att stödja underrättelse- och säkerhetstjänsterna. Lagen har ingen geografisk begränsning vilket innebär att även företag utomlands samt kinesiska medborgare boende i andra länder också omfattas av lagen.[13] Underrättelselagens tvång är ett av skälen till farhågorna att det kinesiska telekomföretaget Huawei kan användas för att inhämta känslig information. Rapportering om företagets verksamhet har visat att Huawei har spionerat på Afrikanska unionens högkvarter, utlämnat känslig information om klienter i Tjeckien och hjälpt regimerna i Uganda och Zambia att spionera på oppositionspolitiker.[14]

10 Estonian Foreign Intelligence Service, 2018. S.53.

11 National Intelligence Council, 2017.

12 Hellström, J., 2019.

13 E.g. Dackö, C., och Jonsson, L., 2019.

14 Cave, D., 2018; McEnchroe, T., och Kroupa, J., 2019; Parkinson, J., et al., 2019.

Med denna lag har Kommunistpartiet, MSS samt PLA skaffat sig ett formidabelt nätverk för inhämtning av underrättelser för att expandera politiskt inflytande, värna ekonomiska intressen samt öka den militära förmågan. Samtidigt har den kinesiska partistaten makt att agera bortom lagens skrivna ord.

I Sverige förknippar vi ofta kinesiskt underrättelsearbete med cyberspionage, men en stor del av inhämtningen sker med gamla välbeprövade metoder, bland annat personbaserad inhämtning. Etniska kineser som bor utomlands och kinesiska företag anlitas. Tankesmedjan Stratfor nämner i en rapport att en kinesisk underrättelseofficer arresterades i april 2018 när han försökte att rekrytera en amerikanska ingenjör som arbetade för ett GE Aviation.[15] Man använder dock inte bara etniska kineser utan rekryterar också informationslämnare med annan bakgrund. Stratfor ger flera exempel på hur kinesisk underrättelsetjänst rekryterar andra än etniska kineser. De exempel som redovisas är en före detta anställd på amerikanska utrikesdepartementet, två före detta underrättelseofficerare samt en verkställande direktör för ett teknikföretag i Ohio.[16]

Kinas cyberkapacitet har under de senaste åren utvecklats kraftigt och utgör en central roll i utvecklandet av ekonomisk och militär kapacitet. Operationerna har blivit svårare att upptäcka, mer precisa och långvariga. 2015 skapade PLA sin så kallade Strategic Support Force, en ny försvarsgren med ansvar för rymd- och cyberkrigföring. Cyberoperationer samordnas med rymdbaserade system och elektronisk inhämtning. Cybersäkerhetsföretaget FireEye bedömer att det finns fler än 20 APT-grupper med direkt anknytning till Kina.

Hackergruppen som kallas APT 10 arbetar på uppdrag av MSS.[17] Gruppen genomför spioneri och informationsinhämtning inom ett brett område och anses ligga bakom operation Cloud Hopper som 2016 drabbade bland andra USA, Norge, Finland, Sverige, Storbritannien och Japan. De sektorer som angreps var IT, energi, försvarsindustri och offentlig verksamhet. 2018 genomfördes ett liknande APT 10-angrepp mot Sverige och flera andra länder som drabbade flyg, rymd, medicin, finans, elektronik och telekom.[18] Information om attacken var mycket knapphändig både från myndighetshåll och från drabbade företag.

Samarbetet mellan Kina och Ryssland har fördjupats. Xi och Putin har träffats fler än trettio gånger sedan 2013 för att diskutera samverkan inom diplomati, handel och ekonomiska frågor men också gällande säkerhet och militär samverkan. Det är nog klokt att utgå från att det också finns ett samarbete inom underrättelseområdet.

Iran

Öppet tillgänglig information om den iranska underrättelsetjänsten är hårt begränsat. Det är dock allmänt känt att Ministry of Intelligence and Security, även känt som MOIS eller VEVAK, är en mäktig och fruktad aktör både i Iran och utomlands. Chefen för MOIS, som ska utses bland prästerskapet och vara en högt utbildad teolog, rapporterar direkt till Irans högste andlige ledare och statschefen, Ali Khamenei. MOIS har en omfattande organisation och stor budget. Myndighetens uppdrag är att värna både nationell och regional säkerhet. Verksamheten i utlandet sker vanligtvis från ambassaderna eller från muslimska centra. Även Air Iran, studenter och affärsmän används för spioneri och inhämtning av information om individer.

Förutom underrättelsetjänsten som är inriktad mot hoten från utlandet där givetvis USA, Israel och Saudiarabien står högt i prioritet så ägnas omfattande resurser mot dissidenter och andra som anses utgöra hot mot regimen. MOIS driver fängelser och genomför brutala mord för att avskräcka regimkritiker.

15 Stewart, S., 2019.

16 Ibid.

17 E.g. PwC UK och BAE Systems, 2017.

18 Englund, J., 2019, s. 5.

Spioneri mot Sverige

Enligt Säkerhetspolisens (Säpo) bedömning har främmande makters underrättelseinhämtning i Sverige ökat under de senaste åren. Verksamheten har breddats både avseende antalet aktörer och vilken information som dessa är ute efter. De metoder som används är allt från traditionellt spioneri och värvning av informatörer till satellitspaning, signalspaning, nätverksoperationer och andra former av teknisk inhämtning. Inhämtning via sociala medier ökar.

Säpo har vetskap om att ett femtontal länder bedriver underrättelseinhämtning i Sverige.[19] Ryssland, Kina och Iran pekas särskilt ut. Redan i april 2014 konstaterade Säpo att den underrättelseverksamhet som Ryssland bedriver kan ses som krigsförberedelser.[20] Säkerhetspolisen bedömer att var tredje rysk diplomat[21] i Sverige verkar under täckbefattning vilket innebär att dessa i själva verket arbetar för någon av underrättelsetjänsterna. Till detta kommer givetvis ett okänt antal underrättelseofficerare som verkar utan diplomatisk täckmantel till exempel affärsmän och journalister.

Utländsk underrättelseverksamhet riktas också mot Försvarsmakten enligt den Militära underrättelse- och säkerhetstjänstens årsöversikt 2018.[22] Syftet är exempelvis att kartlägga Försvarsmaktens personal, bedöma Sveriges operativa förmåga eller vår tekniska utveckling. Ryssland och Kina nämns i årsöversikten.

FRA har rapporterat att det pågår omfattande teknisk inhämtning från främmande makt i Sverige. Den övervägande delen av dessa aktiviteter består av rena underrättelseoperationer där syftet är att komma åt vital information och att kartlägga landets kritiska infrastruktur. Cyberhotet ökar årligen och det gäller inte bara stormakternas aktiviteter, aktörer med mer blygsamma resurser kan också utgöra ett hot förutsatt att den tekniska kompetensen finns.

Samtidigt som hotet ökar så ökar även våra sårbarheter. Teknikutvecklingen och digitaliseringen bidrar till att det blir lättare att komma åt känslig information. Säkerhetsarbetet hänger inte med i den snabba tekniska utvecklingen och insikten om att allt som kopplas upp mot internet kan hackas är inte tillräckligt utbredd.

Kartläggning av personer, inte minst personer med nyckelbefattningar, kan enkelt ske med information från sociala medier såsom Facebook, Instagram och särskilt LinkedIn där många generöst presenterar både omfattande CV och anställningsförhållanden.

Främmande makter bedriver personbaserad underrättelseverksamhet i Sverige. I mars 2019 slog Säkerhetspolisen till mot en restaurang i Stockholm och arresterade en svensk teknikkonsult som hade ett möte med en rysk underrättelseofficer. Enligt Dagens Nyheter handlar det om Jevgenij Umerenko, som vid tiden för tillslaget var ambassadråd vid ambassaden i Stockholm. Umerenko utpekas som SVR:s Sverigechef.[23]

Kina bedriver bland annat flyktingspionage i Sverige. 2010 dömdes en uigurisk man för att ha spionerat på andra exil-uigurer i Sverige, på uppdrag av en diplomat vid Kinas ambassad i Stockholm.[24] En man dömdes i juni 2018 av Södertörns tingsrätt för grov olovlig underrättelseverksamhet efter att ha spionerat på tibetanska flyktingar och sålt informationen vidare till kinesiska myndigheter. Med

19 Säkerhetspolisen, 2018, s. 33.

20 Tillkännagivandet skedde i samband med presentationen av Säpos Årsrapport för 2013. SvD 2014-04-07

21 Säkerhetspolisen, 2017, s. 25. Enligt Stockholm Diplomatic List, 17 juli 2019, finns det finns det totalt 28 ackrediterade diplomater vid ambassaden i Stockholm och ytterligare fyra vid generalkonsulatet i Göteborg. Utöver de ackrediterade diplomaterna finns 20 anhöriga noterade i listan.

22 Militära underrättelse- och säkerhetstjänsten, 2019, s. 37.

23 Carlsson, M., och Holmström, M., 2019.

24 Sveriges Radio, 2015.

största sannolikhet kartlägger den kinesiska säkerhetstjänsten flyktingar och dissidenter för att förhindra kritik mot Kina samt för att kunna utöva hot mot flyktingarnas släktingar i hemlandet.

Sverige – öppenhetens förlovade land

I underrättelsekretsar sägs det ibland att den bästa uppgiftslämnaren är den som inte förstått innebörden av det som hon eller han berättat. Vår medvetna eller omedvetna öppenhet gör att vi ibland tillgängliggör information som vi borde hålla för oss själva, information som en motståndare kan använda antingen för att skada vårt land i en krissituation eller för att utveckla sin egen ekonomi, tekniska kompetens eller militära förmåga. Underrättelsetjänster behöver ofta inte ta risker eller använda illegala, konspiratoriska metoder för att inhämta information som kan vara av stort värde.

Open Sources Intelligence (OSINT) är en inhämtningsmetod som fått en ökad betydelse, särskilt mot länder med stor öppenhet. I och med digitaliseringen och användandet av sociala medier ökar betydelsen av OSINT. Nedan finns några exempel på områden där främmande aktörer kan få tillgång till information utan att ta några risker.

Geografisk information är naturligtvis av stor betydelse när man genomför planering av militära operationer – både för den som ska försvara sig och för angriparen. Totalförsvarets Forskningsinstitut (FOI) har varnat för konsekvenserna av en alltför långtgående öppenhet med geografisk information. Dels handlar det om kommersiella företag som samlar in stora mängder av geografisk information. Dels handlar det om den offentliga sektorn som öppnar upp sina informationsbaser. Lantmäteriet har redan gjort det möjligt att hämta och använda väg- och terrängkartor som kan utnyttjas för operativ planläggning och för precisionsbekämpning av olika typer av mål.[25] Likaledes har vissa kommuner öppnat upp stora delar av sina databaser. Informationen i dessa databaser kan användas för kartläggning av sårbarheter (elförsörjning, dricksvatten, med mera) och man exponerar sig för cyberattacker.

PLA-forskare vid svenska universitet.

Alex Joske vid Australian Strategic Policy Institute har visat att kinesiska PLA bedriver omfattande samarbeten med utländska universitet.[26] Under de senaste åren har samarbetet med utländska universitet ökat radikalt och studien visar att mer än 2500 militära forskare och ingenjörer har studerat utomlands. Så gott som samtliga av dessa tillhör både PLA och Kommunistpartiet. I vissa fall har PLA-forskare varit verksamma utomlands under annan täckmantel, men ofta uppger de sin riktiga organisationstillhörighet. Täckmantel behövs i många fall inte eftersom mottagaruniversiteten i allmänhet inte skiljer mellan samarbete med personer från PLA:s forskningsinstitut och andra kinesiska läroverk. De länder som haft flest PLA-studenter är de så kallade Five Eyes-länderna (USA, Storbritannien, Kanada, Australien och Nya Zeeland). Sverige har under åren 2006 till 2017 varit den åttonde största mottagaren av PLA-forskare. 2017 gick vi upp till sjätte plats vilket är anmärkningsvärt.

Studien har också analyserat antalet referentgranskade forskningsrapporter som publicerats av PLA-forskare har publicerat tillsammans med forskare vid västerländska universitet mellan 2006 och 2017. Kartläggningen visar att det största antalet medförfattade artiklar publicerats med forskare från universitet i USA, Storbritannien, Kanada, Australien, Tyskland och därnäst Sverige.[27] Därefter följer Singapore, Nederländerna, Japan och Frankrike.

Rapporten går inte närmare in på vilka svenska universitet som haft kinesiska studenter från PLA eller vilka

25 Söderman, U., et al. 2017.

26 Joske, A., 2018.

27 Ibid, s. 8

forskningsområden som dessa varit verksamma inom.[28] Däremot nämns att en man som skulle doktorera i kvantfysik vid Uppsala universitet fick medskicket att ”hur skulle man kunna utveckla vapen utan framsteg i fysik?” Kinas utbildningsdepartement har också betonat att studenterna vid University of Cambridge ”kommer stärka nationens förmåga inom områdena nationellt försvar, kommunikationsteknologi, antistörningsutrustning för bilder och högprecisionsnavigering.”[29]

Kina strävar efter att utveckla en modern försvarsindustri som är oberoende av utlandet. För att uppnå detta har man stärkt samarbetet mellan civil och militär teknikutveckling.[30] Sverige underlättar Kinas utveckling av teknik med dubbla användningsområden genom att svenska universitet som accepterar PLA-forskare och -ingenjörer och bidrar därmed med svenska skattemedel till ökad operativ militär förmåga för Kina. Det vore rimligt att reflektera över huruvida detta ligger i svenskt intresse.[31] USA beviljar sedan en tid tillbaka inte visum till kinesiska forskare som har PLA- eller underrättelsebakgrund.

ESRANGE

Kina räknas till en av världens ledande rymdnationer och har förmåga till rymdkrigföring vilket innebär att man kan störa ut eller släcka andra länders satelliter. Rymdförmågan kan användas t ex som stödsystem för kommunikation, spaning och underrättelseinhämtning. Inom området finns både rent militära system, de som primärt är för civilt bruk samt de som har dubbla användningsområden.

Kina har, som tidigare framhållits, en långtgående integration av civila och militära förmågor och staten kan begära att civila företag ska bidra till den militära förmågeutvecklingen. Av den anledningen är det svårt att hävda att ett företag endast verkar inom den civila sektorn.

Jerker Hellström, som är forskningsledare på FOI, menade i ett anförande vid Folk och Försvars Rikskonferens i Sälen i år att ”om en teknologi är tillgänglig för ett kinesiskt bolag så är den också tillgänglig för militären.”[32]

I en artikel i Svenska Dagbladet i januari i år sägs att det helstatliga Rymdbolaget, Swedish Space Corporation, 2008 ingick ett samarbetsavtal med den kinesiska uppskjutningsmyndigheten CLTC [33]. Avtalet undertecknades på den kinesiska sidan av Zhang Jianqi som är generallöjtnant. CLTC är enligt FOI[34] en militärt styrd myndighet som kontrollerar uppskjutning och styrning av satelliter. På ESRANGE finns en antenn som ägs av CLTC dessutom laddas information ner från tre antenner som ägs av Rymdbolaget[35].

Rymdbolaget hävdar att avtalen med de kinesiska kunderna är civila och att man har kontroll på hur antennerna används samt vilken typ av information som laddas ner och att man gör noggranna riskbedömningar. Därmed tycks både Rymdbolaget och dess uppdragsgivare i regeringen att det inte finns risk att information från ESRANGE bidrar till att öka den militära förmågan i Kina.

Bolaget har sedan våren 2019 ett nytt ägardirektiv som ålägger verksamheten att ta säkerhetspolitisk hänsyn.

28 Alex Joske uppger vid kontakt med honom att när det gäller antalet referentgranskade rapporter så ligger KTH på 70, Lunds Universitet 50, Karolinska Institutet 34, Linköpings Universitet 21, Uppsala Universitet 16, Stockholms Universitet 11, Malmö Högskola samt Handelshögskolan 9.

29 Joske, A., 2018, s. 6.

30 Sandklef, K., 2018.

31 Olsson, J., 2019.

32 Hellström, J., 2019.

33 Forsberg, 2019.

34 Ibid.

35 Swedish Space Corporation, Appendix for SSC Chinese Customers”

Kunskapsöverföring genom förvärv

Uppköp av utländska företag är en viktig del i Kinas strategi för att tillskansa sig teknologi med militära användningsområden.[36] Även i Sverige har kinesiska företag förvärvat teknologi som kan ge Kina en starkare roll i den militära maktbalansen. Särskilt anmärkningsvärt köpte kinesiska företag tre svenska företag, varav två var statligt ägda, som producerar halvledare, vilket används i allt från mobiltelefoner och bilar till militära system.[37]

Efter en tilltagande insikt att uppköp av strategiskt viktiga företag kan hota Sveriges säkerhet beslutade regeringen i augusti 2019 att låta en utredare ”föreslå under vilka förutsättningar utländska direktinvesteringar ska kunna hindras och vilka förbehåll för sådana investeringar som bör kunna ställas upp”.[38]

Hot mot svenska intressen i utlandet

Givetvis tilldrar sig Bryssel ett stort intresse för de som har anledning att närmare följa utvecklingen inom den Europeiska unionen respektive Nato. Enligt olika källor har Europeiska utrikestjänsten (EEAS) varnat unionens medlemsstater om underrättelsehotet i Bryssel. EEAS har, enligt *The Guardian*, bedömt att det finns cirka 250 kinesiska och 200 ryska underrättelseofficerare i staden.[39]

Underrättelsehotet mot EU i Bryssel gäller naturligtvis också EU-parlamentet i Strasbourg. Den estniska underrättelsetjänsten skriver i sin årsrapport från 2018 att Ryssland aktivt rekryterar EU-parlamentariker i Strasbourg både som ett led i att inhämta information och att påverka beslutsfattandet i unionen.

Det har dessutom rapporterats att ryska underrättelsetjänster har infiltrerat den belgiska militära underrättelsetjänsten, ADIV. Sekretessbelagd information har läckts till en serbisk kvinna med länk till den ryska underrättelsetjänsten.[40] Affären påminner om Herman Simms, en tjänsteman på Estlands försvarsministerium, som läckte 386 sekretessbelagda EU- respektive Nato-dokument till rysk underrättelsetjänst.

Svenskar på semestern och tjänsteresa

Att spionera och rekrytera agenter i utlandet innebär att man måste ta politiska risker dessutom är det resurskrävande och kostsamt. I den estniska säkerhetstjänstens årsbok för 2018 ägnas en betydande del till att beskriva hur de ryska underrättelse- och säkerhetstjänsterna rekryterar informatörer i Ryssland.[41] Att inhämta information på det egna territoriet är säkrare, mindre kostsamt och kan vara väl så effektivt som att bedriva verksamhet i utlandet. Dessutom är det svårare för utländskt kontraspionage att bedöma omfattning av och förhindra verksamheten. Därmed tenderar också denna typ av inhämtning att underskattas.

Den första fasen i processen i att värva utlänningar i Ryssland är, enligt den estniska rapporten, att grovsortera de inresande och bedöma vilka som kan ha intressant information. Detta sker genom rutinkontroll av till exempel information i inresevisum. De som bedöms vara av intresse analyseras djupare genom granskning av öppna källor såsom sociala medier, CV:n och Linkedin. De som efter denna inledande granskning anses vara intressanta kan komma att utsättas för värvningsförsök med traditionella metoder.[42]

Vid större evenemang i Ryssland, till exempel OS och VM, upprättas enligt den estniska rapporten särskilda operativa organisationer med personal från både underrättelse- och säkerhetstjänsterna i syfte att övervaka och rekrytera informatörer. De som förstår vad som pågår och

36 Brown, M., och Singh, P., 2018.
37 Forsberg, B., 2018.
38 Regeringen, 2019.
39 Boffey, D., 2019.
40 Rettman, A., 2019.
41 Estonian Foreign Intelligence Service, 2018.
42 E.g. Säkerhetspolisen, 2018, s. 35.

avvisar värvningsförsöket kan emellertid få problem vid såväl utresan som vid förnyad ansökan om inresevisum till Ryssland.

Och så till sist … även vänner och allierade spionerar

Henry L Stimson var amerikansk utrikesminister mellan 1929 till 1933. Han är mest känd för att stänga ner utrikesdepartementets kryptoanalysavdelningen med motiveringen att ”gentlemen läser inte varandras brev”. Historien visar att han hade fel.

Den minnesgode erinrar sig avslöjandet 2013 att USA:s underrättelsetjänst avlyssnat Tysklands förbundskanslers mobiltelefon. En upprörd Angela Merkel förklarade i tv att ”Spionage vänner emellan – det händer bara inte”.

Den franske före detta utrikesministern Bernard Kouchner medgav att även Frankrike spionerar, men att man ”inte har samma resurser som amerikanarna”.

Två år senare avslöjades att den tyska underrättelsetjänsten Bundesnachrichtendienst (BND) avlyssnat ett stort antal ambassaders mejl- och telefonkommunikationer i Berlin, däribland den svenska. Reaktionerna varierade.

Avslutning: hur ska vi bemöta underrättelsehotet?

Ett viktigt steg för att motverka att olika aktörer ska kunna inhämta information i vårt samhälle är att det från och med den 1 april i år finns en ny säkerhetsskyddslagstiftning som skärper kraven på alla i samhället som bedriver någon form av verksamhet som är av betydelse för Sveriges säkerhet.[43] Sammanfattningsvis krävs bland annat att myndigheter, företag och kommuner gör säkerhetsanalyser som klarlägger om något inom deras ansvarsområden är skyddsvärt och hur detta i så fall ska skyddas. Åtgärderna kan handla om att säkerställa att information skyddas, att fysiskt skydda kritisk infrastruktur eller att utbilda personal. Det är verksamhetsutövaren som har ansvaret för att lagen följs. Hur arbetet ska genomföras framgår av Säpos föreskrifter och vägledning. Om den nya lagstiftningen följs av alla berörda så kommer säkerhetsskyddsnivån i landet att höjas rejält.

Ett viktigt steg i att höja säkerheten är också att chefer och verksamhetsansvariga måste ta ett ökat ansvar när det gäller säkerhetsfrågor. Det duger inte att låta en säkerhetschef ta ansvar för detta. Frågan som måste ställas är huruvida myndighetschefer, verkställande direktörer och andra chefer (de som i lagtexten kallas verksamhetsutövare) kan tillräckligt om hur de ska leda till exempel cybersäkerhetsarbete eller om det krävs någon form av utbildning.

Underrättelseverksamhetens konsekvenser är mycket större idag än förr i tiden. För att sätta den ovannämnda cyberattacken Cloud Hopper i proportion noterade Svenska Dagbladet att ”som jämförelse kan spionen Stig Berglings stöld av 20 000 dokument sägas motsvara 20 gigabyte, medan stölden av information i ett större ATP-angrepp kan bestå av 100-tals terabyte, alltså många gånger så mycket”.[44] Jämförelsen visar tydligt hur säkerhetshotet förändrats och förvärrats.

Slutsatsen blir också att vi måste ägna stor kraft åt att skydda oss mot cyberattacker. Det handlar bland annat om att utbilda personal. Enligt en amerikansk studie som citeras i SvD-artikeln så orsakas mer än hälften av alla dataintrång av den mänskliga faktorn och att en person släppt in angriparen. Personalen måste förstå hotet och veta hur de ska agera. Ett annat område som måste ses över är myndighetens processer och administrativa rutiner. Slutligen handlar det om teknologi. Det är industrin som leder utvecklingen av cybersäkerheten och därför krävs det ett nära samarbete mellan staten respektive företag och industrin. Tiden för hemmasnickrade lösningar är för alltid förbi.

43 Säkerhetsskyddslagen (2018:585), Säkerhetsskyddsförordningen (2018:658) och Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2019:2).

44 Pirttisalo Sallinen, J., 2018.

Vi svenskar har ett jämförelsevis lågt säkerhetsmedvetande och det går inte att lagstifta fram en bättre säkerhetskultur. Samhället präglas i stor utsträckning av naivitet eller aningslöshet när det gäller frågor om rikets säkerhet. Lagstiftning är ett sätt att höja säkerhetsskyddsnivån men den riktigt stora utmaningen är att förändra människors attityder till landets säkerhet. Landets underrättelse- och säkerhetstjänster bör vara mer öppna med information om säkerhetshotande verksamhet. Om medborgarna inte får konkret information om vilka hot som är riktade mot landet kommer inte den mentala beredskapen och säkerhetsmedvetandet att öka. Hur ska exempelvis cybersäkerheten höjas om man inte går ut med information om Cloud Hopper?

1939 inleddes det som kom att kallas Vaksamhetskampanjen med syfte att allmänheten skulle hålla tyst om allt som kunde skada landet. Symbolen för kampanjen blev *En svensk tiger* som på kort tid fick stort genomslag. Vi skulle behöva en motsvarande kampanj idag för att höja säkerhetsmedvetandet.

Sverige har av naturliga skäl under många år ägnat stor kraft åt att följa och analysera utvecklingen i Ryssland och dess konsekvenser för oss. Den politiska utvecklingen i Kina gör att vi får ytterligare en global aktör som vi måste ägna uppmärksamhet åt. Landet är inte en avlägsen aktör som inte angår oss. Därför bör vi öka kunskapen om Kina. Det ligger inte i svenskt intresse att den militära förmågan i Kina utvecklas med information som vi genom aningslöshet gjort tillgänglig.

Slutligen måste vi ägna större uppmärksamhet åt gråzonsproblematiken – tillståndet mellan fred och krig. Den försvarspolitiska debatten i Sverige handlar till övervägande del om hur vi ska försvara oss mot ett väpnat angrepp men inte i tillräcklig omfattning om hur vi ska kunna motstå påtryckningar i skedet mellan fred och krig. En fungerande försvarsmakt behöver fungerande samhällsfunktioner såsom livsmedelsförsörjning, drivmedel, el, fungerande kommunikationer med mera.

Francis Walsingham , som var underrättelsechef i 1500-talets England menade att ”det är farligare att frukta för lite än för mycket.” Vi svenskar borde i större utsträckning tänka som Walsingham.

Referensförteckning

Bellingcat, 2019, ”Identifying the Separatists Linked to the Downing of MH17”.

Boffey, D., 2019, “I’ll talk, but then I have to talk to Putin’: steakhouse at centre of EU spy alert”, *The Guardian*, den 12 februari.

Brown, M., och Singh, P., 2018, ”China’s technology transfer strategy: How Chinese investments in emerging technology enable a strategic competitor to access the crown jewels of U.S. innovation”, Defense Innovation Unit Experimental, USA:s försvarsdepartement.

Carlsson, M., och Holmström, M., 2019, ”Hög rysk diplomat pekas ut som spionhef i Sverige”, *Dagens Nyheter*, den 14 mars.

Cave, D., 2018, ”The African Union headquarters hack and Australia’s 5G network”, *The Strategist*, Australian Strategic Policy Institute, den 27 december.

Dackö, C., och Jonsson, L., 2019, ”Applicability of Chinese National Intelligence to Chinese and non-Chinese Entities”, Mannheimer Swartling.

Englund, J., 2019, ”Kinas industriella cyberspionage”, FOI Memo 6698, Totalförsvarets forskningsinstitut.

Estonian Foreign Intelligence Service, 2018, “International Security and Estonia 2018”.

Farmer, B., 2019, ”Russian spies sentenced in Montenegro coup plot”, *The Telegraph,* den 9 maj.

Faulconbridge, G., 2018, “What is Russia’s GRU military intelligence agency?”, *Reuters*, den 5 oktober.

Forsberg, B., 2018, ”State sålde spjutspetsbolag till Kina – under radarn”, *Svenska Dagbladet*, den 18 december.

Forsberg, B., 2019, ”Statliga Rymdbolaget skrev avtal med kinesisk militär”, *Svenska Dagbladet*, den 18 januari.

Hellström, Jerker (2019), ”Kinas politiska prioriteringar: militär-civil fusion och konsekvenser för Sverige”, FOI MEMO 6649, Totalförsvarets forskningsinstitut.

Lindström, S., och Rydqvist, J., 2019, ”Kinas rymdprogram och rymdförmågor”, FOI-R--4718--SE, Totalförsvarets forskningsinstitut.

Joske, A., 2018, “Picking flowers making honey”, Report Nr. 10/2018, Australian Strategic Policy Institute

McEnchroe, T., och Kroupa, J., 2019, “Former Huawei Employees Say Client Information Was Discussed at Chinese Embassy”, Radio Praha, den 22 juli.

Militära underrättelse- och säkerhetstjänsten, 2019, ”Årsöversikt 2018”.

National Intelligence Council, 2017, ”Assessing Russian Activities and Intentions in Recent US Elections”.

Ny Teknik, 2018, ”Ryssar utvisas efter påstått spioneri”, den 4 oktober.

Parkinson, J., Bariyo, N., och Chin, J., 2019, “Huawei Technicians Helped African Governments Spy on Political Opponents”, *Wall Street Journal*, den 15 augusti.

Pirttisalo Sallinen, J., 2018, ”Så angrep Kina ”naiva” Sverige i det fördolda”, *Svenska Dagbladet*, den 21 april.

PwC UK och BAE Systems, 2017, ”Operation Cloud Hopper”.

Olsson, J., 2019, ”De forskar för Kina militär”, *Universitetsläraren*, den 13 februari.

Peel, M., 2019, “EU imposes sanctions on Russian military intelligence chiefs”, *Financial Times,* 21 januari.

Regeringen, 2019, ”Ett system för granskning av utländska direktinvesteringar inom skyddsvärda områden”, Dir. 2019:50.

Rettman, A., 2019, "Belgian spy scandal puts EUand Nato at risk", *EU Observer*, den 15 februari.

Rymdbolaget, n.d., "Appendix for SSC's Chinese Customers".

Smith, B., 2018. "Russian intelligence services and special forces", briefing paper nr. CBP 8430, House of Commons Library.

Sandklef, K., 2018. "Kinas globala investeringar: Ekonomiskt verktyg för politiskt inflytande?" Frivärld rapport nr. 2 2018.

Stewart, S., 2019. "Common Misconceptions About China´s Corporate Espionage Tactics", Stratfor, den 18 juni 2019.

Sveriges Radio, 2015, "Spionfallet på kinesiska ambassaden", den 17 april.

Swedish Space Corporation, "Appendix SSC's Chinese Customers".

Säkerhetspolisen, 2017, "Säkerhetspolisen 2017".

Säkerhetspolisen, 2018, "Säkerhetspolisen 2018".

Söderman, U., Ahlberg, S., och Tolt, Gustav, 2017, "Geografisk information – en vital resurs i förändring" i red. Hull Wiklund, C., Faria, D., Johansson, B., och Öhrn-Lundin, J., Strategisk Utblick 7: Närområdet och nationell säkerhet, Totalförsvarets forskningsinstitut.

Taylor, D., 2018, "Study reveals North Korean cyber-espionage has reached new hights", *The Guardian*, den 20 februari.

Försvarsberedningen, 2017, "Motståndskraft: Inriktning av totalförsvaret och utformning av det civila försvaret 2021 – 2025", Ds 2017:66, Försvarsdepartementet.