JOHAN ÖSTLUND
är grundare och ägare av, samt vd för, Ganeida Security Consulting. Johan har en ek. mag i företagsekonomi från Uppsala universitet, med inriktning mot informationssystem.

PONTUS WINSTÉN
är utredare och riskanalytiker på Ganeida Security samt verksam i arbetsgruppen ASIS Young Professionals. Pontus har en fil. kand. i sociologi med inriktning på risk och krishantering.

Johan Östlund och Pontus Winstén skriver en unik artikelserie om industrispionage för Skydd & Säkerhet. I detta nummer avslöjar de en händelse som tidigare inte varit allmänt känd och i nästa nummer tittar de närmare på de metoder som angripare använder för att optimera möjligheterna att komma åt forskningsdata och företagshemligheter.

Industrispionage

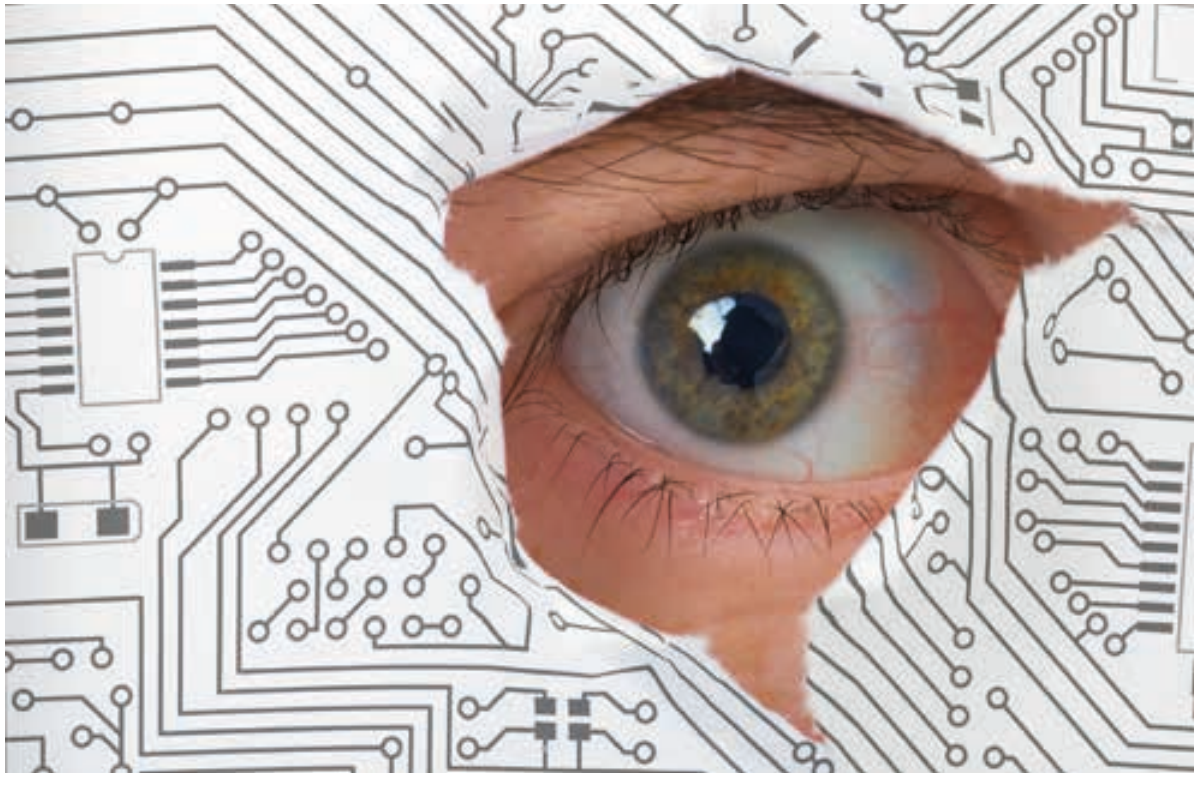
– ett globalt spel med enorma insatser

Industrispionage mot svenska företag och akademiska institutioner är mer vanligt förekommande och mer omfattande än många tror och hotet är stadigt tilltagande. Om den saken är den svenska underrättelseapparaten helt överens.

Vi kan genom en mycket trovärdig källa avslöja att en kinesisk gästforskare vid Karolinska Institutet hösten 2012 överlämnade ett halvt års grundforskningsdata till hemlandet. En uppgift som tidigare inte varit allmänt känd. Säpo varnade redan 2005 för att kinesiska gästforskare utgjorde en säkerhetsrisk men fick inget gehör. Kanske borde svenska aktörer då ha varit mer lyhörda.

Enligt FRAs talesperson Fredrik Wallin skedde förra året ett tiotal målmedvetna och riktade angrepp mot myndigheter och statligt ägda bolag, som var så allvarliga att FRA fick gå in och hjälpa till med incidenthanteringen. Vad gäller det privata näringslivet – men kanske särskilt den akademiska världen – menar Wallin att de till stora delar är omedvetna om det hot som existerar.

DE ANGRIPARE SOM utgör det överlägset mest avancerade hotet mot svenska storföretag och svensk forskning är nationalstater som Ryssland, Kina och Iran. Dessa länder sitter på både know-how och avancerad teknologi och de kanaliserar stora ekonomiska resurser till spionage. Deras intresse riktas främst mot rymd-, flyg-, försvars- och verkstadsindustrin - men också mot industrier som läkemedel, telekom och IT.



Industrispionage mot svenska företag och akademiska institutioner är mer vanligt förekommande och mer omfattande än många tror.

En kinesisk gästforskare vid KI överlämnade hösten 2012 ett halvt års grundforskningsdata till hemlandet...

Sirpa Franzén från Säkerhetspolisen menar att de utländska underrättelse- och säkerhetstjänsterna och andra hotaktörer vill förvärva viktig strategisk information som är omöjlig eller mycket kostsam för det egna landet att ta fram, såsom framstående forskning eller civil och militär högteknologi.

Ett exempel på detta är den 46-årige man som 2003 dömdes till åtta års fängelse för grovt spionerи mot Ericsson, där han jobbade som ingenjör.

Med risk för skada för det svenska totalförsvaret och rikets säkerhet överlämnade mannen under åtta månaders tid ett stort antal konfidentiella dokument om mobiltelefoni till en rysk underrättelseofficer som han träffade på olika pendeltågstationer utanför Stockholm. Som en konsekvens utvisades senare två ryska diplomater.

DE UTLÄNDSKA underrättelsetjänsterna är dock inte det enda hotet. Den organiserade brottsligheten, hackergrupper, aktivister och konkurrerande företag är också ständigt närvarande.

Den organiserade brottsligheten är generellt mindre målinriktad och inhämtar gärna all typ av information som kan säljas vidare på den svarta marknaden. Den enorma mängd pengar som finns att hämta innebär att det är stora krafter i rörelse.

Där aktivisterna har en alltigenom altruistisk agenda med slutmålet att misskreditera organisationer de ser som onda, drivs hackergrupperna ofta av teknologisk bravado. De har vanligen teknisk kompetens men saknar resurser och uthållighet. I det aktuella sammanhanget förknippas hackers ofta med stöld av källkod och kunddatabaser.

KONKURRERANDE FÖRETAG saknar vanligtvis det kunnande som krävs för att bedriva spionage och nyttjar därför ofta ljusskygga säkerhetsföretag, hackers eller insiders på det aktuella målföretaget för sina syften. Deras fokus ligger helt på information som kan ge konkurrensfördelar vid upphandlingar samt vid utveckling av nya metoder och teknologier.

Konsekvenserna av hård konkurrens fick SAABs vd Håkan Buskhe uppleva under den pågående försäljningen av JAS 39 Gripen till Schweiz år 2012. Han berättade då i en intervju med SvD om hur hans telefon blivit avlyssnad, hur sms skickats iväg utan hans vetskap och hur tekniker på SAAB under sin fritid blivit kartlagda av utländska studenter. ”Det är så det fungerar”, menade Buskhe cyniskt.

JOHAN ÖSTLUND
PONTUS WINSTÉN