Bilaga 3

Teknisk utveckling och Hybridkrigföring

av Marcus Dansarie

ARTIKELN SAMMANFATTAR HUVUDDRAGEN av mitt föredrag vid Kungl krigsvetenskapsakademiens symposium om hybridkrigföring den 21 maj 2019 och tar upp den tekniska utvecklingen med anknytning till symposiets ämne. Här berörs ett antal löst kopplade teman som alla har anknytning till den tekniska utvecklingen under 2000-talet och som på något sätt kan påverka hur moderna konflikter kommer att föras.

Radikal förändring

Den tekniska utvecklingen sedan 2000-talets början har medfört samhällsförändringar som är större än vad de flesta nog inser. Anledningen till att det inte är omedelbart uppenbart hur stora förändringarna har varit är att de har varit små och stegvisa, snarare än paradigmskiften.

Mycket av den teknik vi idag ser som självklar är relativt ung. Skatteverket började ta emot deklarationer via internet 2002. Inledningsvis var det endast möjligt att kontrollera och godkänna den förenklade självdeklarationen. Året efter kom den första versionen av BankID. I år (2019) deklarerade 6,3 miljoner personer digitalt och 97,5% av alla svenskar mellan 21 och 50 års ålder har ett eller flera BankID. Enligt uppskattningar från företaget bakom BankID kommer tjänsten användas fyra miljarder gånger i år. BankID i mobiltelefonen kom först 2011 och året efter kom betalappen Swish. I januari 2019 använde 68% av svenskarna Swish minst en gång i månaden. Smarta mobiltelefoner, som vi är vana att se dem idag, gjorde sitt intåg med iPhone som började säljas av Apple 2007.

Även sociala medier, som har förändrat vårt sätt att kommunicera och utbyta idéer med varandra, är en väldigt ung teknik. Facebook och Twitter öppnade för allmänheten 2006 och Instagram kom först 2010. Detta återspeglar sig även i förändringar i mediekonsumtionen. 2015 passerade internet såväl TV som dagstidningar som det populäraste dagliga mediet i Sverige.

Vad har hänt?

Förändringarna i hur vi utför våra dagliga sysslor har både möjliggjorts av teknikutvecklingen och drivit den. Jag lyfter här fram fem aspekter av dessa förändringar.

Den första är att datornätverk är tillgängliga praktiskt taget överallt. Den revolutionerande idén med internet är att det är en generell teknik för överföring av godtycklig data mellan vilka ändpunkter som helst. Överföringen är snabb och har hög tillgänglighet. Det gör det möjligt att ge vilken apparat som helst tillgång till vilken information man vill.

Nästa aspekt är en övergång från specialiserade till generaliserade system och hårdvara. Framgångarna inom integration och produktion av elektronik tillsammans med stora produktionsvolymer har gjort generaliserade datorsystem billiga. Det har medfört att i stort sett alla moderna IT-system består av generaliserade komponenter. För 20 år sedan bestod de flesta militära tekniska

system huvudsakligen av specialprodukter. Militära system som designas och tillverkas idag, bortsett från vissa specialsystem och specialdelar, består istället i huvudsak av generella komponenter. Ofta är dessa framtagna för industribruk och klarar därmed militära krav på exempelvis miljötålighet.

Tillgången på beräkningskraft och minne är ytterligare en bidragande faktor till samhällsförändringarna. Idag finns processorer och datorer som är små och billiga nog för att lösa praktiskt taget alla upptänkliga problem. Tillsammans med utvecklingen av beräkningsförmåga har även utvecklingen av effektivare algoritmer för många grundläggande datavetenskapliga problem gett såväl ökad effektivitet som minskade krav på beräkningskapacitet inom en stor bredd av applikationer.

Även sensorer har blivit mindre och billigare. Det har gjort att även dessa har hamnat i flera nya typer av produkter med nya möjligheter som följd. En modern mobiltelefon kan exempelvis innehålla en eller flera högupplösta kameror, satellitnavigeringsmottagare, accelerometrar, gyron, magnetometer och barometer. Kombinationen med relativt stor beräkningskraft och snabb internettillgång har skapat synergieffekter.

En avslutande faktor är automation. Att fler datorer, sensorer och system kopplas ihop har möjliggjort en ökad grad av automation i de flesta applikationer. Maskiner har ersatt människor i utförandet av många uppgifter. Detta har så klart medfört stora samhällsvinster, men också ökad sårbarheten.

Risker

Automatisering och komplexa system har fört med sig nya risker. Information från ett system kan börja användas i ett annat system på sätt som skaparna av det första systemet aldrig förutsett. Systemberoenden blir också svåröverblickbara och många gånger är det inte ens möjligt att bilda sig en uppfattning om ett systems beroenden. Exempelvis visade sig skyltarna i Stockholms tunnelbana nyligen vara beroende av en webbtjänst för att fungera.

Så kallade felkritiska systemdelar eller svaga länkar, på engelska kallade *single points of failure*, kan uppstå utan att någon är medveten om det. Många till synes oberoende system i samhället är gemensamt beroende av ett fåtal andra system. När något av de systemen slutar fungera nedgår också funktionaliteten i alla beroende system. Ett konkret exempel är GPS-systemet som utvecklades för att lösa militära navigeringsbehov. Genom att signalerna är gratis tillgängliga för alla i hela världen har systemet kommit att nyttjas i en mängd olika applikationer. En av dessa är tidsförsörjning. Väldigt många system i samhället är beroende av noggrann tid och får detta genom en GPS-mottagare. Det är inte fullt ut känt vad konsekvenserna av fel i tidsförsörjningen via GPS, även under en kortare tidsperiod, skulle vara på samhällsnivå.

Mobiltelefoni, elsystem och kollektivtrafiksystem är ytterligare exempel på felkritiska systemdelar i samhället.

Cyber

”Cyber” och ”cyberkrigföring” är begrepp som ofta dyker upp i de här sammanhangen. I en artikel från 2002 för Thomas Rid fram den tes som också är artikelns titel: ”Cyber War Will Not Take Place”.[1] Han menar att det vi kallar för cyberkrigföring egentligen är sabotage, spionage och subversion som utförs med nya medel. Om ”cyber” inte är något nytt kanske skillnaden mot tidigare är den låga inträdeströskeln. Flera stater har förmåga att dolt genomföra bland annat avancerade inhämtnings- och sabotageoperationer,

men det finns fler aktörer på cyberarenan. Bokstavligt talat miljontals människor har den kunskap och de resurser som krävs för att komma över tröskeln, även om de saknar de avancerade förmågor som de välfinansierade och -organiserade aktörerna har.

En av de cyberoperationer som orsakat störst sidoskador är spridandet av ett program som har kommit att kallas NotPetya. Programmet spreds ursprungligen genom uppdateringsmekanismen för en ukrainsk bokföringsprogramvara. Det sprider sig vidare automatiskt och raderar all information på datorer det kommer i kontakt med. Avsikten verkar ha varit att slå brett mot det ukrainska näringslivet och flera länder har öppet anklagat Ryssland för att ligga bakom. NotPetya blev framförallt uppmärksammat för att det drabbade flera stora företag utanför Ukraina, bland annat FedEx, Maersk, Merck och Saint-Gobain. Sammantaget beräknas skadorna utanför Ukrania ha kostat över 10 miljarder dollar.

I en rapport[2] från amerikanska revisionsmyndigheten GAO i oktober 2018 beskrivs problematiken med cybersäkerhet i vapensystem. Rapportens underrubrik sammanfattar det läge som beskrivs tämligen bra: ”DOD Just Beginning to Grapple with Scale of Vulnerabilities”. Rapporten beskriver flera konkreta exempel på säkerhetsproblem i vapensystem, även om exakt vilka system det rör sig om har utelämnats av sekretessskäl. Bland annat sägs att nästan alla större vapensystem som testats under perioden 2012 till 2017 hade sårbarheter som kunde utnyttjas av en motståndare. Rapporten beskriver också att det inom det amerikanska försvarsdepartementet finns en syn på att cybersäkerhet inte är något som berör vapensystem och noterar att det sannolikt finns en hel generation system som har designats utan att ta hänsyn till cybersäkerhetsbehov.

Informationsexplosionen

I takt med teknikutvecklingen har mängden och typerna av information som är tillgänglig för de som är intresserade också ökat explosionsartat. De senaste två decennierna har flera tekniker och källor som tidigare bara har varit tillgängliga för stora länders underrättelsetjänster blivit allmänt tillgängliga. Här följer några korta exempel.

Inom ramen för EU:s Copernicus-projekt har ett antal jordobservationssatelliter utvecklats och skjutits upp i omloppsbana. Satelliterna samlar in data om jorden med flera olika metoder, däribland fotografiskt och med syntetisk aperturradar. Tanken är att den inhämtade datan ska användas för en mängd olika syften såsom grundforskning, samhällssäkerhet och räddningsarbete efter katastrofer. EU driver också projekt för att få företag att komma på nya idéer för hur informationen kan nyttjas. Ibland leder det till oväntade effekter. En israelisk bloggare upptäckte till exempel att störningar i Copernicusprojektets rymdbaserade syntetiska aperturradar går att använda för att lokalisera militära luftspaningsradarer. Bland annat har han publicerat positionerna på flera svenska PS-870-radarer.[3]

Projektet Openstreetmap[4] skapar en karta över jorden med hjälp av tusentals frivilliga. Underlaget kommer bland annat från satellitbilder och mätningar med GPS-mottagare på plats. Den underliggande databasen är fritt tillgänglig för nedladdning. Kartorna är noggranna även för platser och länder som är stängda för tillträde och där kartering generellt är otillåten, som exempelvis Nordkorea.

Tekniskspridningen har gjort att många nya aktörer bedriver verksamhet som tidigare har varit förbehållen stora länders underrättelsetjänster. Till dessa hör bland annat stater av alla storlekar, andra statsliknande

aktörer, företag, akademiska forskargrupper, ideologiskt drivna grupper (hackare, phreakers, säkerhetsforskare) och rent intressedrivna grupper (radioamatörer, amatörastronomer). Exempelvis har en amerikansk forskargrupp självständigt lokaliserat och identifierat produktionsanläggningar för delar i de nordkoreanska och iranska medel- och långdistansrobotsystemen.[5]

Författaren är kapten i flottan och doktorand i Militärteknik vid Försvarshögskolan.

Noter

1. Rid, Thomas: ”Cyber War Will Not Take Place”, *Journal of strategic studies*, vol 35, 1, 2012, s 5-32.
2. *Weapon Systems Cybersecurity*, United States Government Accountability Office, Washington DC 2018.
3. Dan, Harel: ”X Marks The Spot: Identifying MIM-104 Patriot Batteries From Sentinel-1 SAR Multi-temporal Imagery”, *https://medium.com/@HarelDan/x-marks-the-spot-579cdb1f534b*.
4. OpenStreetMap, *https://www.openstreetmap.org*.
5. Se exempelvis Lewis, Jeffrey: ”That Ain’t My Truck: Where North Korea Assembled Its Chinese Transporter-Erector-Launchers”, *https://www.38north.org/2014/02/jlewis020314/*.