Stuxnet,

Første steget i retning av digital krigføring.

Da atombomben eksploderte over Hiroshima 6. August 1945 ga det kinetisk krigføring en ny dimensjon. Oppdagelsen av Stuxnet i juli 2010 innledet igjen en ny dimensjon i internasjonal krigføring; cyber krig.

Øst – Vest konflikten i verden var ikke ny ved innledning til dette århundret. Pakistan hadde utviklet atomvåpen og eksporterte kunnskapen til Nord Korea. Indonesia fulgte opp, samt Iran med flere. Forsøket med å limitere spredning av atomvåpen synes tapt mens FN intensiverte sine anstrengelser for å opprettholde NPT fra 1995 gjennom IAEA's inspeksjoner av atomanlegg verden over.

Problemene i Midt-Østen eskalerte med Hizbollahs rotfeste i Libanon og Syria, godt støttet av Iran. Med Israels ekspansjon på Vestbredden, Golan Høydene i Syria, sør Libanon og kriger med Egypt i friskt minne tilspisset frontene seg. Den «Arabiske vår» skapte usikkerhet og spenning, og nye fronter etablerte seg mellom Sunni og Shia muslimer i henholdsvis Saudi Arabia og Iran. Iran, tynget av vestlige sanksjoner, uttalte et klart mål om utvikling av «atomkraft for fredelige mål» i samme åndedrett som «Israels utslettelse». Israel og USA ble nervøse. Iran var en stormakt i Midt-Østen og ingen enkel motstander. President Carters mislykkede raid for frigjøring av gisler i den okkuperte amerikanske ambassade i Teheran var ikke glemt. Her måtte man tenke nytt.

Datavirus, ormer, trojanske hester og annen «Spy Ware» var kommet for bli. Mon om det kunne appliseres militært? I all hemmelighet var det bygget opp avdelinger i USA, Kina, Russland, Nord Korea, Israel, England med flere som engasjerte seg profesjonelt i utnyttelsen av moderne datateknikk for spionasje, sofistikerte data angrep, ormer med mere. Dette var ikke bare guttestreker og kriminell hacking for egen vinning. Her var det mulighet for å avlytte, danne seg innsikt, raffinere sine militære strategier og muligvis dominere sine motstandere.

Oppdagelsen av Stuxnet i 2010 innledet et helt nytt kapittel. Her hadde man utviklet en helt nytt «multilayered malware» som angrep industrielle kontroll systemer (PLC). Angrepet var rettet mot Irans atomkraftverk som anriket uran. Frykten var at Iran skulle skaffe seg nukleær kapasitet til militært bruk og bruke det mot Israel. Israel planla et nytt militært bombeangrep mot Natanz anlegget for å hindre anrikningen. Problemet var at Iran hadde flere tusen sentrifuger for anrikningen, spredt over mange anlegg og noen gjemt i fjellanlegg som ikke lot seg destruere så lett. Da Israel informerte USA om sine militære planer, delte USA sine planer om cyberangrep mot Irans sentrifuger. Israels militær angrep ble stilt i bero og samarbeidet med cyberangrepet ble innledet.

Selvsagt var alt hemmeligstemplet og ingen utenom de innvidde hadde noen kunnskap om det som var i gjære. Selv ikke de som ble angrepet skjønte hva som foregikk. Sofistikeringen av ormen var så avansert at ingen oppdaget infiseringen av datamaskinene, ei heller endringer i datasystemene, utslag av alarmer på SCADA monitorene eller at sentrifugene

oppførte seg unormalt. De bare gikk i stykker, den ene etter den andre, noen her, noen der og til ulike tidspunkter.

Data-ormen Stuxnet var et resultat av årelang forskning i USA med kodenavnet «Operation Olympic Games» sanksjonert av den amerikanske president og derfor sikkert koordinert av NSA, CIA og i samarbeid med Mossad, MI5 med flere og bygget av dataforsknings-laboratorier, atomforskere og internasjonale industriselskaper. Data koden var tydelig laget av «Old School» programmerere med grunnlag i C og C-påbygg med inngående kunnskaper til Windows operativ systemer, deres svakheter, mulige bakdører gjennom link-lag, ispedd med «multi-Zero day triggers», evnen til å oppdatere seg selv, penetrere registrer-laget og spre seg fra datamaskin til datamaskin. Forskere hadde bygget komplette replikanter av Iranske atomanlegg med alle komponenter til sentrifuger. De hadde funnet at hexafluoridgasser til bruk i anrikningen av uran (U-235) solidifiserte seg ved høye omdreininger av sentrifugene og belegget på rotorbladene skapte ubalanse i rotoren. Ved redusert hastighet rystet rotoren sentrifugen i stykker, det samme vi ser når vaskemaskinen avslutter spinning. Problemet for Iranerne var at ingen kunne finne årsaken til at sentrifugene endret hastighet siden monitorene ikke ga utslag. Flere Iranske forskere ble likvidert for sin «udugelighet».

Om ikke Sergey Ulasen hadde oppdaget ormen som spredde seg til 100.000 datamaskiner med 12.000 identifisere infeksjoner og som senere ble omtalt som W32.Suxnet av Brian Krebs i VirusBlockAdas sin publikasjon den 15 juli 2010, hadde man kanskje ikke fått innsikt i dette hemmelige scenariet. Det ble øyeblikkelig gjennomført en «distributed denial-of-service» angrep på serverne til sikkerhets selskapene som publiserte saken for å hindre videre spredning av informasjon om ormen. Senere utviklinger av Duqu-ormen og liknende inneholdt ytterligere kompleksitet som blant annet gjennomføring av selvdestruksjon hvis noen søkte å indentifisere den, hvilket gjorde videre forskning umulig.

Dette er det lille vi vet blant mengder av motstridende informasjon på nettet. Hva med alt vi ikke vet siden 2010? Hvor lagt har man gått og hvor sofistikert er ormene blitt? Hvem sitter på hva og hvem kan angripe deg uten at du ved det? Kan de rekonfigurere automatisk en ny «Zero Day» etter eget forgodtbefinnende? Kan de allerede ha infisert atomanlegg over hele verden slik at disse blir nye «Chernobyl» ved despotiske leders forgodtbefinnende, eller styrte fly ved infisering av flyets datorer? Kanskje var det det som skjedde da SAABs Jas Gripen skulle presenteres for miltære kjøpere under sin demonstrasjon og som plutselig styret ut av kontroll. Var det ubehagelig for USA at en ikke NATO produsent kunne innvirke på USAs planer om salg av F35 til samtlige Nato-land? Blir neste krig en cyber krig av internasjonalt omfang? Er dagens spenning på Ukrainas grenser opptakten? Saken er at vi ikke vet og det kan gi spekulasjoner langt ut over det noen skrekkfilm kan visualisere.

Kilder:
Wikipedia https://en.wikipedia.org/wiki/Stuxnet
Kristiania TK2100-1 22V:
https://kristiania.instructure.com/courses/7866/files/787885?module_item_id=289340