

Fremtidens krige udkæmpes på nettet

KRIGSTEKNOLOGI: Cyberkrigen vil i fremtiden rase via massive hackerangreb og skjult cyberspionage. Kina har allerede en hær på titusindvis af militære cyberspioner, mens USA har en national cyberkommando, der udvikler våben til elektronisk krigsførelse. Vi står overfor et globalt elektronisk våbenkapløb.



21.02.2011 Af Otto Lerche Kristiansen

Angrebet på Estland kom klokken ti om aftenen. Uden bombefly. Uden tanks. Uden soldater. En hær af computere sendte i april 2007 den første bølge af elektroniske denial of service-angreb ind mod regeringens hjemmesider. Den estiske forsvarsminister, Jaak Aaviksoo, opdagede først angrebet, da han forgæves forsøgte at læse nyheder på landets største netavis, Postimees. Der skete ingenting. Som en lang række af landets andre hjemmesider var avisens overbelastet og brudt sammen. De følgende dage tog angrebene til i styrke. Mod regeringens hjemmesider. Mod bankers. Mod politiske partiers og avisers. Estland var under cyberangreb.

Angrebet mod Estland i 2007 var en af verdens første cyberkrige. Men ikke den sidste. Ifølge sikkerhedsvirksomheden McAfees seneste rapport forbereder en lang række lande sig på at skulle forsvare sig mod cyberangreb, mens USA, Rusland, Frankrig, Israel og Kina har tilføjet cybervåben til deres offensive arsenaler. Selv om våbnene hverken er atommissiler eller kampfly, men botnet og orme, så kan de smadre fiendens

rapport forbereder en lang række lande sig på at skulle forsvare sig mod cyberangreb, mens USA, Rusland, Frankrig, Israel og Kina har tilføjet cybervåben til deres offensive arsenaler. Selv om våbnene hverken er atommissiler eller kampfly, men botnet og orme, så kan de smadre fjendens infrastruktur og økonomi. Samtidig har Kina en hær med titusindvis af cyberspioner, og USA har oprettet en cyberkommando.

Truslen fra cyberspace stiger

Angrebet mod Estland varede tre uger og var af en hidtil uset størrelse og karakter. Selv om man helt tilbage til starten af 1900-tallet har kendt til elektronisk krigsførelse – i krigen mellem Rusland og Japan (1904 til 1905) forsøgte russerne at jamme japanernes telegraf og på den måde ødelægge deres kommunikation – så vakte verdens første internetkrig opsigt. Ikke mindst i NATO:

“Behovet for et center for cyberforsvar er påtvivende,” sagde det transatlantiske forsvarsfællesskabs general, James Mattis, da han et år senere mødtes med repræsentanter for medlemslandene for at underskrive papirerne for oprettelsen af et forskningscenter for cyberkrig. Det blev placeret i netop Estlands hovedstad Tallinn.

Siden er truslen i cyberspace ikke blevet mindre. I 2008 gik israelske og palæstinensiske hackere i krig med hinanden efter en israelsk militæroperation i det palæstinensiske selvstyreområde. Samme år invaderede Rusland nabolandet Georgien med tanks og kampfly. Samtidig angreb de også på internettet, hvor hjemmesider for blandt andet den georgiske regering blev lagt døde.

I 2009 bombarderede oppositionen i Iran regeringens hjemmesider som et led i flere protester mod valget. Samme år angreb et netværk af 50.000 computere, der var styret fra Nordkorea, sydkoreanske og amerikanske netsider.

I januar 2010 kom det frem, at kinesiske hackere havde hacket Google og skaffet sig adgang til en række mailkonti, som tilhørte menneskerettigheds-aktivister og journalister. Sagen lignede et opgør mellem mailudbyderen Google og nogle kinesere, men var ifølge fx USA's udenrigsminister, Hillary Clinton, langt mere end det.

“Så tæt forbundet som verden er, kan et angreb

Sagen lignede et opgør mellem mailudbyderen Google og nogle kinesere, men var ifølge fx USA's udenrigsminister, Hillary Clinton, langt mere end det.

“Så tæt forbundet, som verden er, kan et angreb på en nations netværk være et angreb på os alle,” sagde hun i en tale om internetfrihed sidste år, kort efter at Google havde offentliggjort angrebet.

Senere kom det frem, at angrebet på Google blot var en lille del af en større operation. Operationen – som ifølge McAfee gik under kodenavnet Aurora – var et koordineret angreb på minimum 34 amerikanske virksomheder og institutioner. Blandt andet antivirusproducenten Symantec, kemigiganten Dow Chemical og leverandører til Pentagon.

Eksemplet med Kina og Google er et af de seneste og mest kendte eksempler på politiske konflikter i cyberspace. Vi har endnu ikke været vidner til en regulær verdenskrig på internettet eller en cyberkrig mellem stormagter. Men:

“Den næste verdenskrig kan begynde i cyberspace,” sagde Hamadoun Touré, generalsekretær for FN's International Telecommunication Union (ITU), til FN's konference ITU Telecom World 2009 i Genève. Og forud for den amerikanske invasion af Irak i 2003 forberedte Pentagon faktisk et cyberangreb på Irak.

Angrebet kunne angiveligt have fastfrosset Saddam Husseins personlige bankkonti, stoppet lønudbetalinger til soldaterne og betalinger til militærets materiel og på den måde banet vejen for en fysisk invasion. Præsident George W. Bush valgte dog ikke at sætte angrebet i gang, angiveligt fordi risikoen var for stor. Cyberangrebet kunne nemlig muligvis lamme den finansielle sektor i andre lande.

Digital propaganda griber om sig

Truslen fra cyberspace stiger i takt med udbredelsen og afhængigheden af internettet. Mailsystemer. IP-telefoner. Banker og offentlige hjemmesider. Elnet og vandforsyning. Store dele af vores infrastruktur er afhængige af internettet og dermed et militært mål, som kan angribes fra en hvilken som helst computer et hvilket som helst sted i verden.

Samtidig åbner den stigende afhængighed af internettet nye muligheder for lande, som ønsker at bruge cyberspace til spionage, informationskontrol og propaganda. I krigen

sted i verden.

Samtidig åbner den stigende afhængighed af internettet nye muligheder for lande, som ønsker at bruge cyberspace til spionage, informationskontrol og propaganda. I krigen mellem Rusland og Georgien var russernes cyberangreb på georgiske hjemmesider ifølge Dmitri Alperovitch, direktør i McAfees afdeling for trusselsforskning, ikke kun et militært angreb, men i lige så høj grad et forsøg på at forhindre georgiske myndigheder og medier i at fortælle deres version af krigen. Selv om propaganda ikke er en direkte krigshandling, så er kontrollen med informationer stadig afgørende for, at krigen skal lykkes.

Det samme er spionage i cyberspace. Det amerikanske forsvarsministerium registrerede i 2006 seks millioner forsøg på at bryde ind i ministeriets computersystemer. I dag er det tal vokset til op mod seks millioner om dagen. I 2008 lykkedes det en ukendt udenlandsk regering at plante malware på en amerikansk computer på en militærbase i Mellemøsten via en USB-nøgle og efterfølgende få adgang til planer om militære aktioner. Og alene mellem 2002 og 2005 blev der ifølge det amerikanske forsvarsministerium downloadet mellem 10 og 20 terabytes information fra ministeriet i den såkaldte operation Titan Rain.

Titan Rain og flere andre spionagesager har spor til Kina. Landet er ifølge flere eksperter den førende nation inden for cyberspionage og har siden 2005 trænet målrettet i at hacke fjendtlige netværk. Blandt andet et amerikansk atomvåbenlaboratorium, USAs elnet og den tyske kansler Angela Merkels kontor. Kina har angiveligt titusindvis af cyberspioner og er ifølge en redegørelse fra den amerikanske U.S.-China Economic and Security Review Commission midt i en "radikal modernisering, som fundamentalt vil ændre landets evne til at udkæmpe teknologiske krige".

Missionen er angiveligt at stjæle bl.a. militære hemmeligheder. Kina benægter det dog.

Den ukendte krig raser på www

Der findes ingen definition på cyberkrig. Derfor rejser de mange eksempler en række spørgsmål: Er de eksempler på krigshandlinger? Kan man sammenligne et angreb i cyberspace med et angreb på landjorden? Er en krig uden fysiske ødelæggelser overhovedet en krig?

rejses de mange eksempler en række spørgsmål: Er de eksempler på krigshandlinger? Kan man sammenligne et angreb i cyberspace med et angreb på landjorden? Er en krig uden fysiske ødelæggelser overhovedet en krig?

Sikkerhedsekspert Eugene Spafford fra Purdue University er skeptisk:

“De cybervåben, vi har set til dato, er ikke i stand til at forårsage så stor skade, at det når et niveau af krig,” siger han i den seneste rapport fra McAfee. “Jeg siger ikke, at cyberkrig som betegnelse ikke giver mening, men den passer ikke på nogen af de begivenheder, vi har set indtil nu.”

Allerede i 1990'erne pressede Rusland på for at få international enighed om en definition af cyberkrig. De seneste ti år er der skrevet titusindvis af sider om cyberkrig, men vi mangler stadig egentlige internationale doktriner og traktater på området. Tidligere minister for det amerikanske sikkerhedsministerium Michael Chertoff sammenlignede for nylig behovet for at tilpasse sig den nye og ukendte trussel fra internettet med behovet for at tilpasse de militære doktriner til atombomben i halvtredserne.

NATO og det amerikanske militær er allerede i gang. I november 2010 vedtog NATO på et topmøde at udvide cyber-forsvaret:

“Vi vil medtage cyberspace i NATO's doktrin og forbedre mulighederne for at identificere, vurdere og forhindre trusler og reetablere alliansens centrale systemer i tilfælde af cyberangreb,” er ordlyden i rapporten fra topmødet.

Samtidig indgik EU og USA en aftale om et øget samarbejde på området. Og i 2010 udnævnte det amerikanske militær den første cyberkrigsgeneral og flyttede 30.000 soldater fra teknisk support til cyberkrigenes frontlinjer.