Fremtidens krige udkæmpes på nettet

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.

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 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 påtvingende," 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 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 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 spionage-sager 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 atomvåben-laboratorium, 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?

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 alliancens 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.

Angreb: Zombiehær slår it-systemet i gulvet

En af de mest alvorlige elektroniske angrebstaktikker er distributed denial of service (DDoS). Angrebet overbelaster modstanderens it-system og sætter det på den måde helt eller delvist ud af drift.

1. Den angribende part forbereder sig ved at samle et stort netværk af computere, et botnet, som skal bruges i angrebet. Zombierne, som de kaldes, er oftest tilfældige computere ejet af

almindelige mennesker. De hackes og inficeres med små programmer (attack tools), som gør det muligt på afstand at overtage kontrollen med dem.

2. Angrebet kan sammenlignes med en aktion fra den "rigtige" verden, med generaler, sergenter og soldater. Den angribende computer er generalen. Han giver ordrer til sergenterne, der sender ordren om angreb til soldaterne. På den måde er generalen (hovedcomputeren) i sikker afstand af "krigshandlingerne".

Et eksempel på en kommando fra hovedcomputeren til zombierne kunne være: !udp 207.71.92.193 9999999 0. Det betyder, at zombierne skal sende 9.999.999 meget store datapakker til IP-adressen 207.71.92.193. Det store antal tunge datapakker overbelaster offerets it-system, der til sidst bryder helt sammen.

Der findes flere forskellige angrebsmetoder. En af dem kaldes syndflod. De inficerede computere kontakter en webserver via en almindelig TCP-internetforbindelse. Det svarer lidt populært til en telefonsamtale. Man ringer op. Modtageren siger hallo og siger sit navn. Derefter kører snakken.

Angrebet går ud på, at browseren – fx Internet Explorer – kontakter web-serveren. Webserveren svarer, men står så og venter forgæves, idet browseren ikke fortsætter. Da webserveren ikke kan vide, om browseren blot er sløv eller ondskabsfuld, bliver webserveren nødt til at bevare forbindelsen, indtil den er sikker på, at der ikke er nogen. En er ikke et problem, men millioner af sådanne uafsluttede forbindelser opbruger serverens ressourcer.

3. Angrebet ødelægger ikke offerets system, men sætter det ud af funktion i en periode. Det kan dog have alvorlige konsekvenser, når angrebet er rettet mod fx forsvarets kommunikations-systemer, ministerier eller elnettet.

En hær af zombier lammer Estland

2007: Russiske computere angriber Estlands banker og ministerier med såkaldt distributed denial of service (DDoS). I tre uger bliver hjemmesider tilhørende estiske banker, aviser, politiske partier og ministerier angrebet, og adgangen til netbanker og handel på nettet er for mange borgere spærret.

Angrebene kommer efter alt at dømme som en reaktion på, at esterne har flyttet en mindestatue for de sovjetiske soldater, der var faldet under anden verdenskrig. Statuen er blevet flyttet fra den centrale del af Estlands hovedstad, Tallinn, til en militærkirkegård i udkanten af byen.

Det har vakt vrede i Rusland og Kreml, som ifølge den estiske udenrigsminister står bag angrebet. Selv om russernes skyld aldrig er bevist, så har en russer med forbindelse til Kreml påtaget sig ansvaret for angrebet.

Spionage: Trojanske heste sniger sig ind med USB-nøglen

Spionage er udbredt i cyberspace. It-sikkerhedshuller udnyttes af andre lande til at trænge ind og stjæle alt fra forretningshemmeligheder til politisk følsomme oplysninger. Et af cyberspionernes hemmelige våben er trojanske heste.

1. Den angribende part undersøger fjendens it-systemer, enten ved at skanne hele systemet for sikkerhedshuller (åbne porte) eller

ved at vælge ét bestemt mål (en computer) og forberede et målrettet angreb mod dette.

2. Hackeren kan nu enten skaffe sig fysisk adgang til et it-system, fx via en insider, der indsætter en USB-nøgle, eller snyde brugeren af computeren til selv at installere den trojanske hest, fx ved at camouflere den som en softwareopdatering eller som en vedhæftet fil i en e-mail.

3. Hackeren kan herefter installere et såkaldt rootkit, der slører den trojanske hest. Ejeren kan så ikke opdage eller fjerne den trojanske hest.

4. Når computeren er infiltreret, har hackeren ofte total kontrol over offerets computer og kan fra sin egen computer fx følge ethvert tryk på tastaturet ved hjælp af såkaldte keylogging-programmer eller aktivere webkameraet. Infiltrationen gør det også muligt at kopiere fx adgangskoder og følsomme filer og stjæle dem. Ofte uden at offeret opdager, at det er sket.

Spioner smugler trojansk hest ind hos Dalai Lama

2009: Canadiske efterforskere afslører i 2009 en kinesisk spionring, som har brugt en trojansk hest til at infiltrere næsten 1300 computere i 103 lande.

Ifølge efterforskerne er spionagen rettet mod tibetanere medhenblik på at finde information af politisk eller militær interesse. Cyberspionerne skaffer sig blandt andet adgang til Dalai Lamas kontorer og installerer trojanske heste. På den måde får de direkte adgang til følsomme informationer.

Spionringen får navnet GhostNet efter den type trojansk hest, Ghost RAT, som den bruger. RAT er en forkortelse for remote access tool (fjern-adgangsværktøj) eller remote access trojan, som programmer, der giver fjernadgang til fremmede computere, kaldes.

Kontrol: Intelligente filtre styrer folket

Krig handler ikke kun om at vinde slaget på slagmarken. Det handler også om at styre tilgængelige informationer og folkets meninger. I cyberspace sørger blokering af hjemmesider og semantiske filtre for at holde folket i et jerngreb.
1. Borgeren sender en forespørgsel på en hjemmeside, enten ved at skrive en adresse i browseren eller ved at klikke på et resultat fra en søgemaskinesøgning.
2. Forespørgslen møder en firewall hos internetudbyderen. I praksis varetages blokeringen af internetudbyderen på ordre fra myndighederne.
3. Firewallens indbyggede semantiske filter analyserer forespørgslen. Det semantiske filter kan være en almindelig ordliste over forbudte ord, fx "porno" eller "våben". Det kan også være sofistikeret og indeholde fx ontologisk filtrering, hvor tilladte søgeord som "skyder" eller "lunte" blokeres, fordi de knytter sig til det forbudte ord "våben". Hvis søgningen ikke fanges i filteret, får brugeren adgang. Han opdager ikke, at hans forespørgsel har været gennem et filter.
4. Hvis forespørgslen fanges i filteret, sender firewallen en besked tilbage til brugeren, hvor adgangen nægtes.
5. Når firewallen fanger en søgning i sit filter, kan den indstilles til at sende besked til fx myndighederne med oplysninger om brugerens IP-adresse og indholdet af søgningen.

Iran og Kina blokerer folkets adgang til internettet

2009: I sommeren 2009 går tusinder på gaden i Teheran for at protestere mod det iranske præstestyre. Regimet slår hårdt ned på demonstranterne. Ikke kun med sikkerhedsstyrker på sorte motorcykler, som jagter demonstranterne gennem gaderne, men også med omfattende censur på internettet. Styret blokerer store dele af det iranske internet for at forhindre regeringskritikere i at kommunikere med hinanden og med omverdenen.
Kina har også længe rutinemæssigt blokeret bestemte søgninger i Googles søgemaskine. Kina blokerer også for Facebook, YouTube, Wikipedia og meget andet. Alt sammen for at styre befolkningens adgang til informationer.
Restriktionerne får i marts 2010 Google til at videresende søgninger i Kina til Google Hongkong, der har mere lempelige regler.

Af Otto Lerche Kristiansen
Illustreret Videnskab (21-2-11)