

Samfunnssikkerhet, sårbarhet og IKT

Jan Audestad

- Hva kan gå galt? Ulykker, hackere, denial-of-service, programvarefeil...
- Hva er infrastruktur? – om kritisk infrastruktur. Sårbarhet og robusthet
 - Eksempel: DebtRank
- Vekselvirkninger mellom forskjellige infrastrukturer
 - Definisjoner
 - Eksempler
 - Strømutfall på østkysten av USA
 - Flom i Gøteborg
 - Brann i Oslo S
 - Brann i Stockholm 2013
- Beskyttelse

Når vi skal lage et system, må vi ta hensyn til hva som kan gå galt

- Ulykker og katastrofer: flom, jordskjelv, storm, brann, solaktivitet...
 - Brann på Oslo S, Brann i Stockholm
- Terrorisme og krig – landsanalyse før man etablerer seg
- Informasjonssikkerhet
 - Hackere: stjele, modifisere, lure...
 - Organisert: Se egen slide (New Scientist)
 - Største botnet – største kjente nett: 30 millioner maskiner!
 - Denial-of-service (DoS): Georgia, Pentagon, navnenodene i internett...
 - Datavirus, ormer, trojanere, bakdører, bomber, spam, spionprogram ...
 - Spredning av falsk informasjon
- Programvarefeil og maskinvarefeil
 - Østkysten av USA, flykaos i USA
- Systemfeil
 - Flash crash på NASDAQ i 2010
- Politisk uro og streik

Ofte uhyre vanskelig å skille mellom de forskjellige årsakene.

Informasjonssikkerhet

Cyber security

Informasjonssikkerhet (rapport fra norSIS 2013):

- Flere ledere overvurderer sikkerhetsmodenheten og kontroll i egen virksomhet (!)
- Flere organisasjoner melder om høye kostnader per sikkerhetshendelser, mens ledelsen i organisasjonen oppgir kostnadene til å være lave (!)
- Virksomhetene sliter fortsatt med å definere hva deres mest verdifulle informasjon er (!)
- Virksomhetene erkjenner behov for økte budsjetter og økt engasjement fra ledelsen som middel for å beseire hindringene mot bedre sikkerhet
- Europa har hatt en økning i økonomiske tap grunnet sikkerhetshendelser (uhyre vanskelig å finne tall – mange hendelse oppgis ikke, for andre er det vanskelig å beregne tap (f. eks. ved informasjonstyveri))

Konsekvenser for virksomheter

- Tyveri av informasjon
- Pengetyveri: Lede betalingen for varene på avveier
- Hindre legitim bruk av systemet (DoS)
- Spredning av negativ reklame
- Gjøre pålogging plundrete slik at folk går lei
- Gjøre tjenestetilbudet dårlig/ubrukelig
- Spionasje
- ...

Svakeste ledd i et system er PCen og smarttelefonen – det er her hackerne går inn!

Ikke i f. eks. bankens e-bank-servere.

New Scientist, 28 September, 2013

Hackers for hire

Professional gangs of computer hackers are available - for the right price



IMG_0001.pdf

Hva er et botnet?

Andre tar kontroll over din datamaskin og bruker den til

- Spam
- Reklame
- Denial-of-service-angrep
- Lese andres kort i nettpoker!
- Storskaladistribusjon av spionvare
- Lagring av illegal informasjon (f. eks. barneporno)
- Og mye annet!
- Se:
 - <http://en.wikipedia.org/wiki/Botnet>
 - http://en.wikipedia.org/wiki/Zombie_computer
- Største kjente nett: 30 millioner maskiner (delvis tatt ned i 2010); mange nett med mer en 1 million maskiner

Eksempler på sikkerhetsangrep

Denial-of-Service (DoS)

- DoS-angrep på Georgia (krig med Russland i 2008)
- DoS-angrep på den irske nasjonalbanken
- Mange DoS-angrep på Pentagon og Det hvite hus
- DoS-angrep på navnenodene i internett – **problemet løst ved å opprette mange toppnoder som gjensidig holder hverandre oppdatert**
- DoS-angrep på første aksjemegler på internett – ble lagt ned
- DoS-angrep på websider

Store forbedringer i protokollmaskinene på IP- og TCP-laget gjør DoS-angrepene stadig vanskeligere, men angriperne blir stadig smartere

- **Oversvømme inngangen (ping, SYN, INVITE, bruk av botnet), pakker med feil (lengde, overlappende), langsom lesing (svært lite TCP-vindu, langsom respons), få maskinen til å gjøre**
- **Ping-meldinger stoppes av brannmur, neglisjere masseanrop, filtrere, bruk av cookies (autentisering av kilde) ...**

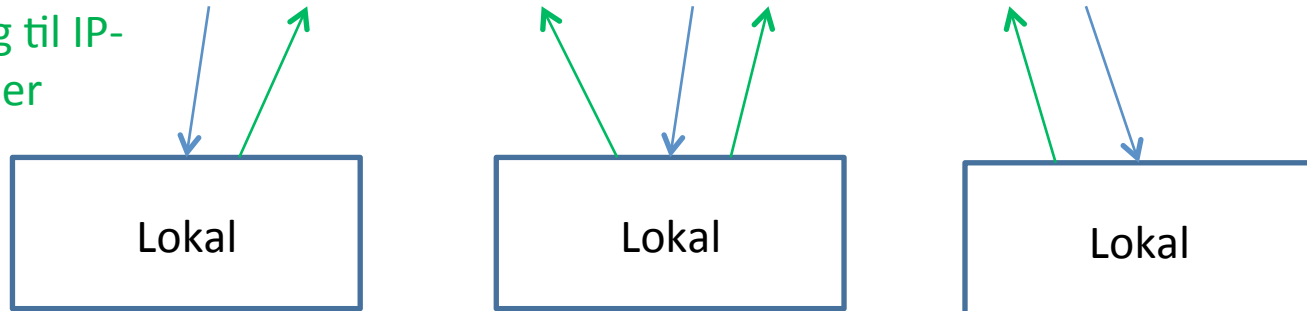
Ta ut Norge

Toppnode

~~no~~, se, us,..., com, org, mil,...

Oppdatering med jevne mellomrom

Forespørsel om
oversetting til IP-
nummer



Etter en stund: adresser x.y.no blir avvist som ugyldige

- Mange virus- og ormeangrep – dagens antivirusprogrammer pluss bedre epostrutiner (ikke automatisk videresending av eksekverbare vedlegg) synes å ha redusert faren
- Spam – spamfiltrene synes å fungere godt (i 2005 fikk jeg mer enn 5000 i uka, nå er det færre enn en).
- Phishing – filter som søker etter visse ord og uttrykk
- Spyware – uhyre vanskelig å stoppe – må ofte reboote operativsystemet
- Spesielle trussel 1: synkronisering av smarttelefoner og internt datasystem!!
- Spesiell trussel 2: la andre (f eks barn) bruke din jobbmaskin!

Infrastruktur

Infrastrukturer:

- Elektrisitet
- IKT (internett)/web
- Finans (bank)
- Logistikk (funksjonell: levering)
- Logistikk (fysisk: vei, fly, bane, båt)
- Vann og kloakk
- Forsvar
- Regjering
- Informasjonssystemer (nyheter)
- Etc

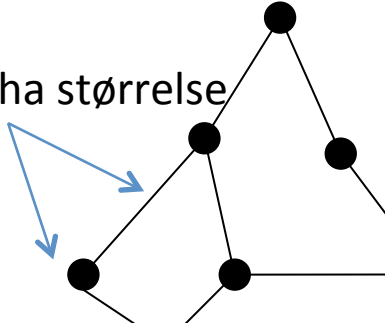
De mest kritiske

Alt går på strøm – alt bruker internett!

Uten elektroniske penger (bankkonti) stopper samfunnet!

- Bank-lockout i 2006 stoppet med tvungen lønnsnemd før den startet – ingen penger fra bankautomatene – ingen kortbetaling i butikker

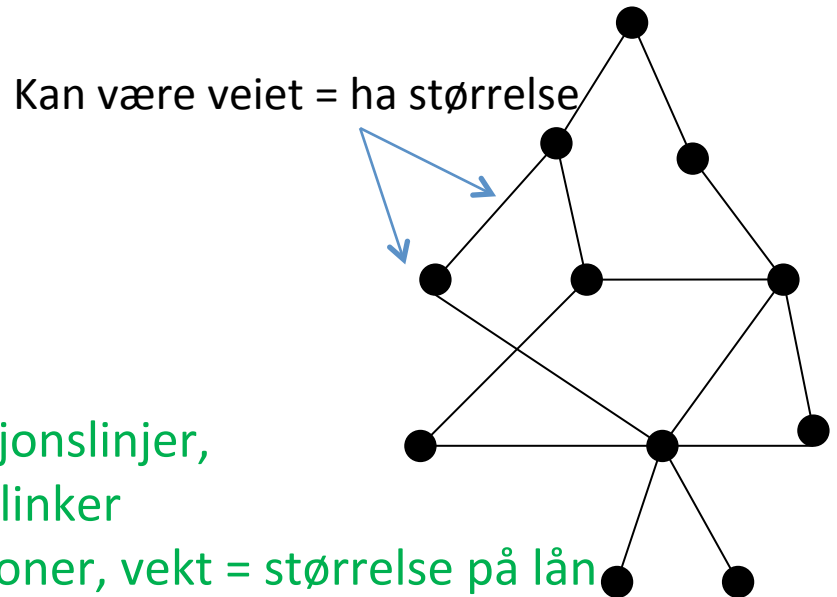
Infrastrukturene er nettverk (eller grafer)

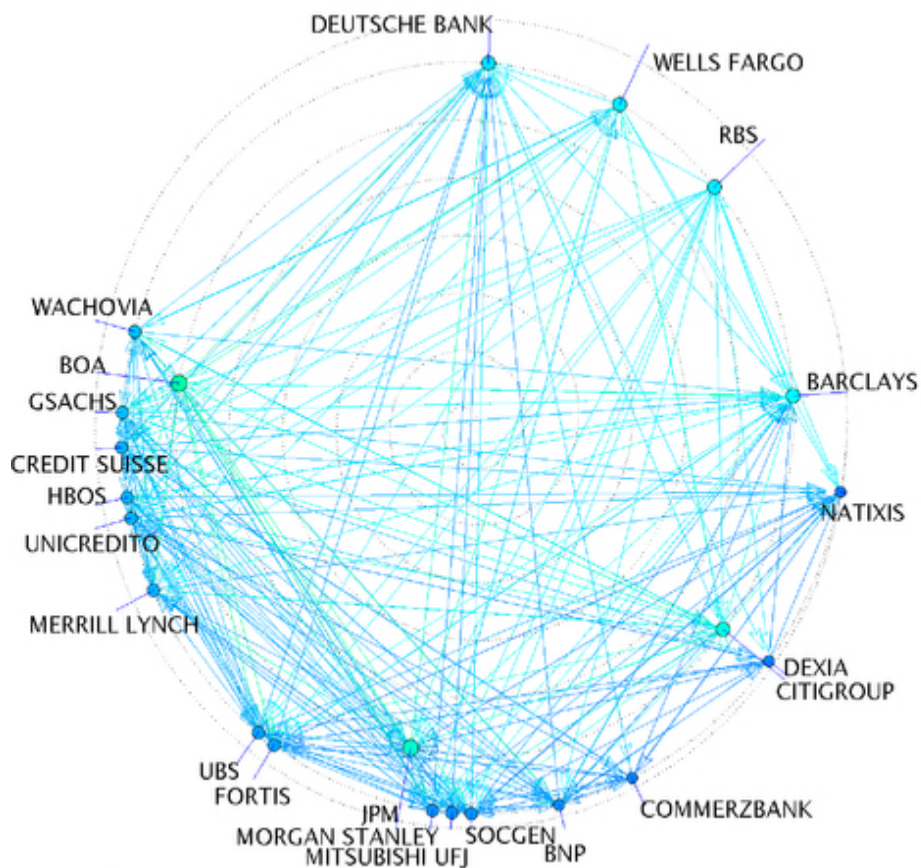
- Strømnettet
 - Telenettet
 - Finans: Bankenes pengeflyt + avhengigheter (f. eks. gjeld)
 - <http://www.nature.com/srep/2012/120802/srep00541/full/srep00541.html>
 - Viser hvordan bankene påvirker hverandre (DebtRank)
 - Veier, flyruter...
 - Vann- og kloakknettet
 - Nyheter – kilder, distribusjon
 - Web
 - ...
- Kan være veiet = ha størrelse
- 

Telenett: noder = rutere, kanter = transmisjonslinjer,
eller: noder = websider, kanter = hyperlinker

Finans: noder = banker, kanter = lånerelasjoner, vekt = størrelse på lån
eller: noder = banker, kanter = transaksjoner, vekt = transaksjonsvolum

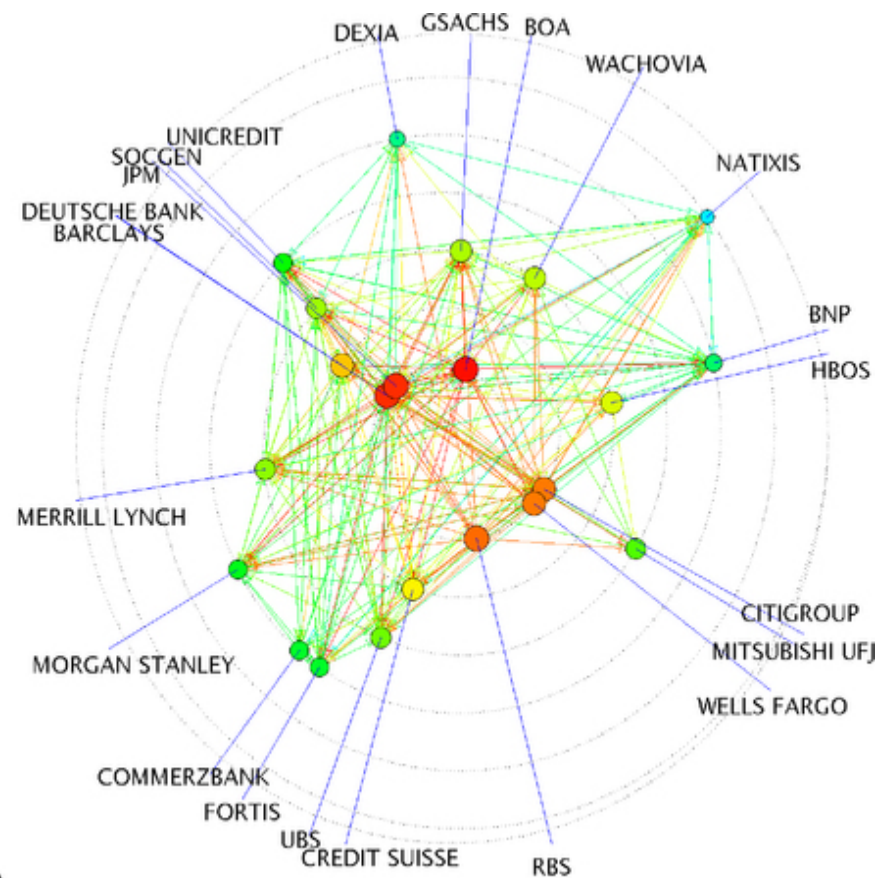
Hvor robust er nettverket? Hvor mye informasjon/gods kan flyte i det?





a)

August 2007



b)

Oktober 2010

Noder = banker, kanter = total gjensidig gjeld, avstand fra sentrum = hvor stor påvirkning noden har på stabiliteten til andre banker

DebtRank

Disse nettverkene inneholder noen store og meget viktige noder

- Web: Søkemotorene (Google...)
- Internett: store rutere, navneserverne
- Strømnettet: store trafostasjoner/kontrollsentre
- Logistikk: store flyplasser, store havner, store veisystemer
- Banker: de dominerende bankene

Se: Barabási, Albert-László, [Linked: The New Science of Networks](#), 2002.

Disse nettverkene er ekstremt robuste overfor tilfeldige angrep:

- Du treffer stort sett små noder
 - Det er dette som skjer med de aller fleste dataangrep

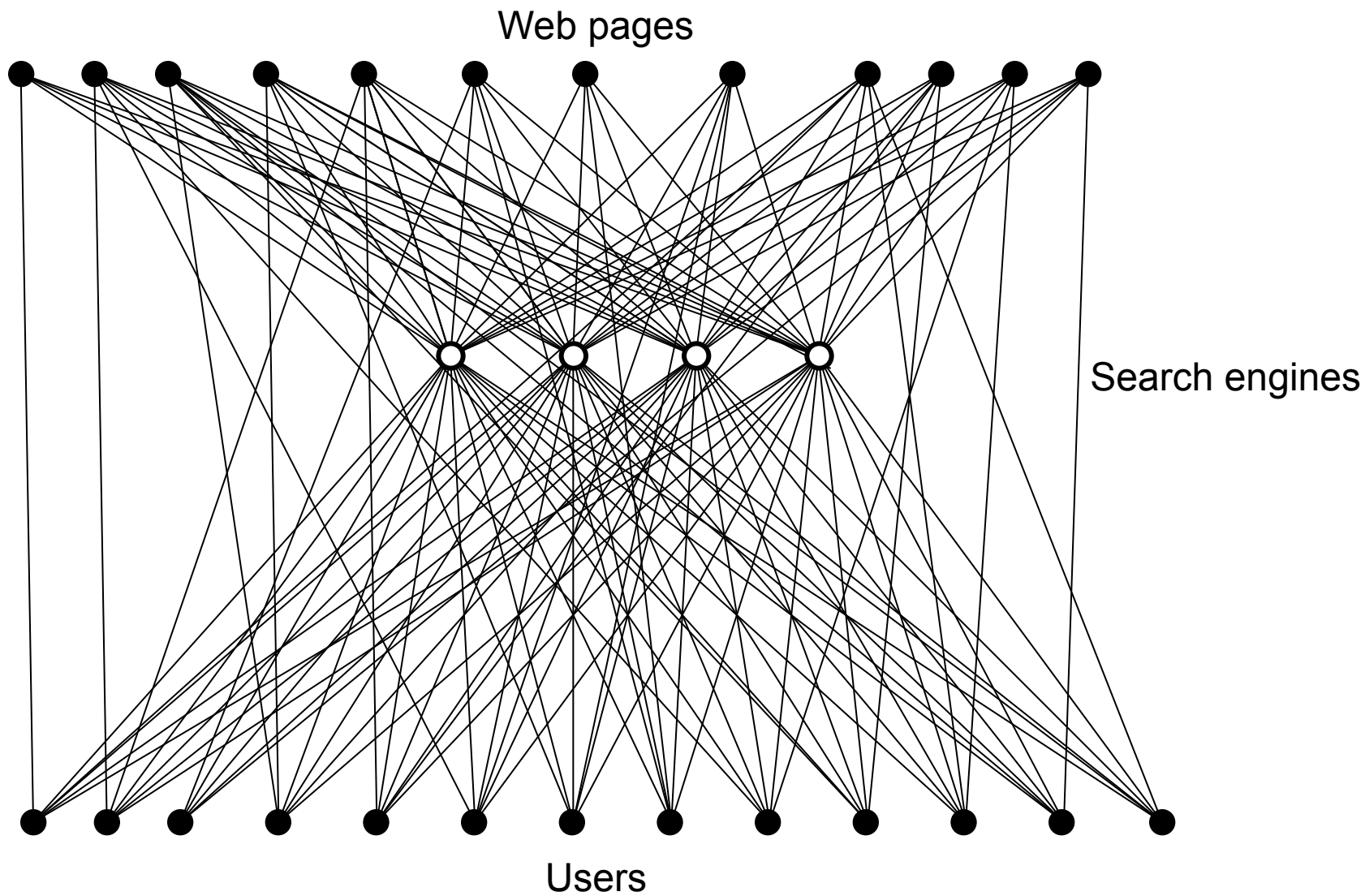
De er ekstremt sårbare overfor rettede angrep:

- De faller fra hverandre hvis du tar ut de store nodene
 - Dette skjedde med bankene i EU og USA i 2008 – ble reddet av staten
 - Kan ikke tillate at infrastrukturen går konkurs!!

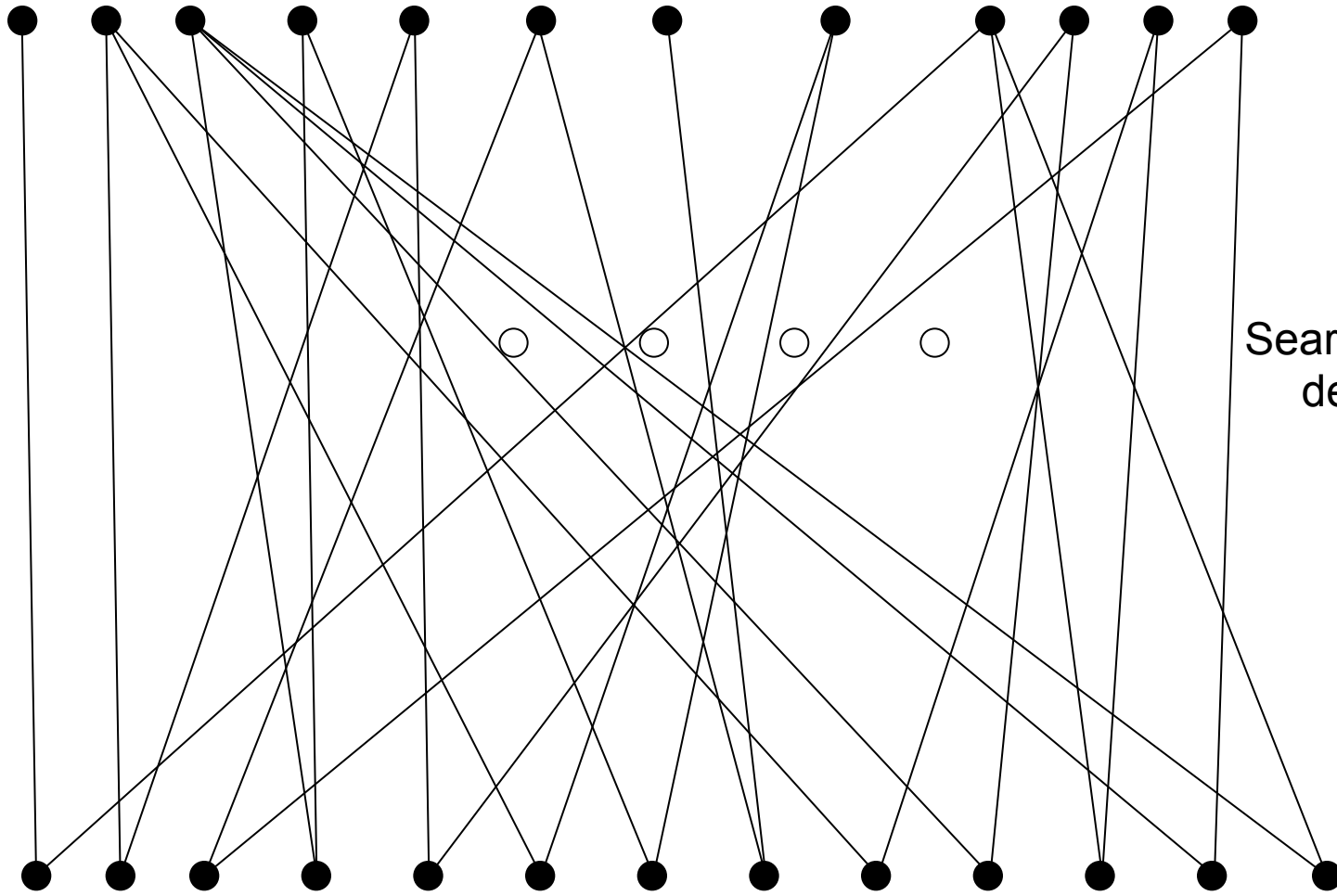
Kaskade: Faller én faller flere: finans, kraftlinjer, spredning av ormer

Spre de store nodene på mange enheter (Google, navneserverne...)

- Mal apropos: Terroristorganisasjoner gjør dette



Web pages

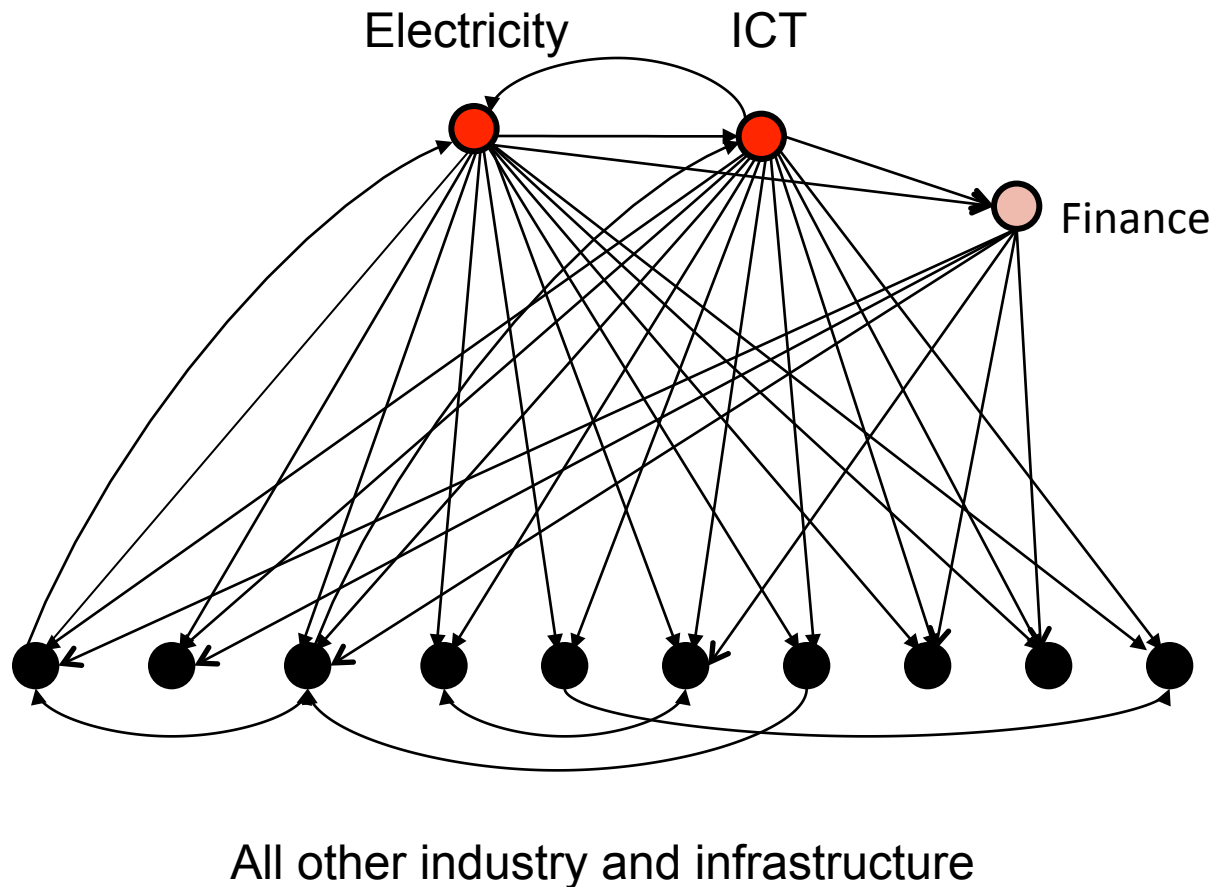


Users

Infrastrukturene henger også sammen i nettverk – de er avhengige av hverandre – i noen tilfeller er dette kritisk:

- Uten elektrisitet, ICT og penger stopper samfunnet

De tre mest kritiske: Alt annet er avhengig av disse



Vekselvirkninger mellom infrastrukturer

Eksempler

- Fysisk: strøm, kommunikasjonsnettverk, logistikk – enkel å forstå
- Logisk: IKT, f eks database, server som brukes til flere ting – veldig kompliserte sammenhenger
- Geografisk: samme sted (f eks strøm og fiber i samme kabelgate) – enkel å forstå, men ofte oversett)
- Menneskelig: f eks streik, opprør

Geografisk:

Flere infrastrukturer bruker samme trasé:

- Stockholm i oktober 2013: Brann i tunnel som ødela kabler for strømnettet og internett
- Brann på Oslo S i 2007 ødela signalanlegg for jernbanen, kommunikasjonslinjer mellom politikamre, internett og telefon i deler av Oslo, noen regjeringskontor:
 - 800 kansellerte tog
 - 25 000 døde internettlinjer

Reservesamband gikk gjennom samme rom!! – noen på samme mørke fiber fra Jernbaneverket!!!

Logisk

November 2009: en feil på et trykkretskort i en internettruter i Salt Lake City gjorde at flytrafikkontrollen falt ut i store deler av USA, både øst- og vestkyst - kanselering av hundrevis av avganger

Fysisk pluss logisk

August 2003: strømutfall på østkysten av USA (bl a New York) og i Canada (55 millioner innbyggere):

- Varighet: ca ett døgn
- Årsak:
 - Kortslutning av linje pga av varme og tilgrodde kraftgater – kaskade
 - Race condition bug i overvåkningsutstyr– gjorde at feilen ikke ble oppdaget
 - Backup-systemet gikk ned da det skulle overta
- Effekt:
 - Transport: Trafikklys, bensinstasjonspumper, tog, undergrunn, flyplasser...
 - Energi: Stenging av ni kjernekraftverk – en uke å starte opp igjen
 - Vann og kloakk: Pumpene stopper – forurensning (bl a kloakk i drikkevann)
 - Telekom: Nesten alt stoppet (mobil, trådløse telefoner, Tv, radio, internett, nødnett)
 - Helse: Air condition (varmt) – sykehusene hadde nok backup
 - Industri: Mange bedrifter både i og utenfor området måtte stenge pga stopp i varetransport – mange brukte flere dager på å starte opp igjen.
 - Nødetatene reddet av radioamatører!
 - 3000 branner pga stearinlys
 - Kostnad for New York: minst 6 milliarder dollar

Fysisk:

Oversvømmelse i Göteborg i mars 2006: – førte til oversvømmelse, bl a rundt bygningen til nødetatene

- Datamaskinrommet i kjelleren ble fullt av vann og maskinene satt ut av drift
- Backup-lagringen fungerte ikke
- Datamaskinrommet var opprinnelig vanntett, men da man bygget nytt garasjeanlegg glemte man dette
- Ibas klarte å gjenvinne 85% av dataene!
- Lærdom: Plasser aldri datautstyret i kjelleren!!

Logisk og menneskelig

Flash crash på NASDAQ 6. mai, 2010

- 9% fall i løpet av minutter – gjenopprettet i løpet av ca ett minutt
- Raske datamaskinalgoritmer føre til ekstremt raske salg og kjøp – raskere enn et menneske kan gjøre det
- Børsen altfor sårbar når det gjelder raske forandringer
- Børsen må ha bremses for å hindre at slikt skjer

Hackere la ut falsk opplysning om terrorangrep på Det hvite hus og at president Obama var skadet på Associated Press sine nettsider 23 april, 2013. Førte umiddelbart til 3% fall på børsen.

NorSIS: Virksomhetene sliter fortsatt med å definere hva deres mest verdifulle informasjon er (!) – mangel på sikkerhet kan bli dyrt

Beskyttelse:

- Brannmur
- Network translation server (NAT): alle maskiner i et firma vil ha samme IP-adresse utad: bruker avsenders portnummer til oversetting til internt IP-nummer – hindrer direkte tilgang til indre ressurser
- Stor båndbredde for å redusere faren for DoS
- Proxyer for å analysere TCP/UDP-pakker
- Automatisk backup
- Streng passordkontroll
- Krypterte filer
- Kryptering også av interne meldinger
- Aksesskontroll både for interne og eksterne meldinger
- Regler for bruk av mobilt utstyr og synkronisering
- Skal man tillate maskiner med kamera og mikrofon?
- ...