Sikkerhet og sårbarhet i IP-basert infrastruktur

av

Ivar Brådland
Per Øyvind Hodøl

Hovedoppgave til mastergraden i informasjons- og kommunikasjonsteknologi

Høgskolen i Agder
Fakultet for teknologi
Grimstad, mai 2006

Sammendrag

Etter hvert som Internett har utviklet seg til å bli en bærer for samfunnskritiske tjenester, er det interessant å se helhetlig på robustheten til disse tjenestene ifra et teknologisk og samfunnsmessig perspektiv. De siste årene har fokuset på beskyttelse av kritiske infrastrukturer økt betraktelig. Begrepet som benyttes i internasjonal sammenheng er CIIP (Critical Information Infrastructure Protection).

I og med den økte mengden tjenester som er totalt avhengige av Internett for å fungere, er det vesentlig å kartlegge og forstå sårbarheter, sikkerhetstiltak og avhengigheter mellom aktørene i infrastrukturen. Den vanligste metoden for å forenkle forståelsen av slike komplekse problemstillinger, er å anvende modeller. Ulike modeller har ulike egenskaper, og ved å bruke flere modeller på det samme problemet, kan man visualisere flere aspekter.

Vi har tatt for oss de eksisterende modellene innen området, og konkludert med at ingen av dem tilfredsstiller behovet for å tydeliggjøre sammenhengene mellom aktører, ansvarsområder og sårbarheter på Internett i Norge. Modellen vi har utviklet i løpet av oppgaven har nettopp disse egenskapene, og den kanskje beste siden ved den er at den på en oversiktlig måte sammenfatter helhetsbildet av de involverte aktørene som infrastrukturen hviler på.

Mot slutten av oppgaven har vi belyst modellens sterke sider ved å eksemplifisere fremgangsmåten i et case study. Selve eksempelet er et tenkt tilfelle av et norsk sykehus som beslutter å gå over fra tradisjonell ISDN-telefoni til IP-telefoni basert på en eksisterende Internett-forbindelse. Resultatene fra case study går i stor grad ut på en aktualisering av de komplekse sammenhengene som oppstår når man er avhengig av mange aktører for å transportere samfunnskritiske tjenester.

Forord

Denne oppgaven er den siste delen av mastergradsstudiet i IKT ved Høgskolen i Agder, Grimstad, fakultet for teknologi. Oppgaven ble gitt av Post- og teletilsynet på grunnlag av deres deltakelse i BAS-prosjektet (Beskyttelse Av Samfunnet). Underveis har vi også vært i kontakt med FFI (Forsvarets Forskningsinstitutt) på Kjeller av samme grunn.

Vi vil rette en spesiell takk til vår veileder professor Vladimir A. Oleshchuk ved HiA for verdifull hjelp underveis. I tillegg takker vi Frank Reichert (HiA), Håkon Styri (PT) og Håvard Fridheim (FFI).

Grimstad, mai 2006.

Ivar Brådland Per Øyvind Hodøl

Innholdsfortegnelse

Figurliste

Forkortelser

ADSL	Asynchronous Digital Subscriber Line
AMS-IX	Amsterdam Internet Exchange
ARIN	American Registry for Internet Numbers
ARP	Address Resolution Protocol
ARPANET	Advanced Research Projects Agency Network
AS	Autonomt System
ASN	Autonomt System Nummer
ASP	Application Service Provider
ATM	Asynchronous Transfer Mode
BAS	Beskyttelse Av Samfunnet
BGP	Border Gateway Protocol
BIX	Bergen Internet Exchange
CATV	Cable TV
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
CRN	Comprehensive Risk Analysis and Management Network
CSD	Circuit Switched Data
DARPA	Defense Advanced Research Projects Agency
DCCP	Datagram Congestion Control Protocol
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DNS	Domain Name System
DNSSEC	DNS Security Extensions
DoS	Denial of Service
DPF	Distributed Packet Filtering
DSB	Direktoratet for Samfunnssikkerhet og Beredskap
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
EDGE	Enhanced Data rates for GSM Evolution
EMP	Elektromagnetisk Puls
ETSI	European Telecommunications Standard Institute
FFI	Forsvarets Forskningsinstitutt
FSA	Forsvarets Sikkerhetsavdeling
FSP	Fixed Access Service Provider
FTP	File Transfer Protocol
GAO	Government Accountability Office
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HSCSD	High Speed Circuit Switched Data
HSPDA	High Speed Downlink Packet Access
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System

IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IIS	Internet Information Server
IKT	Informasjons og kommunikasjonsteknologi
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPS	Intrusion Prevention System
IRC	Internet Relay Chat
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITU	International Telecommunication Union
IX/IXP	Internet Exchange Point
JD	Justisdepartementet
KPN	Koninklijke KPN N.V.
LAN	Local Area Network
LEO	Low Earth Orbit
MIMO	Multiple Input Multiple Output
MOD	Moderniserings-departementet
MPLS	Multiprotocol Label Switching
MSP	Mobile Access Service Provider
NAP	Network Access Provider
NFR	Norsk Forskningsråd
NFS	Network File System
NIX	Norwegian Internet Exchange
NS	Nederlandse Spoorwegen
NSM	Nasjonal Sikkerhetsmyndighet
NSR	Næringslivets Sikkerhetsråd
NTNU	Norges teknisk-naturvitenskapelige universitet
NTP	Network Time Protocol
NVE	Norges Vassdrags og Energidirektorat
OD	Oljedirektoratet
OED	Olje og Energi Departementet
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PAN	Private Access Network
POP	Point Of Presence
POP3	Post Office Protocol version 3
POS	Packet Over SDH/SONET
PPPoE	Point-to-Point Protocol over Ethernet
PT	Post- og teletilsynet
RARP	Reverse Address Resolution Protocol
RIP	Routing Information Protocol
RIR	Regional Internet Registry
ROS	Risiko Og Sårbarhet
SCTP	Stream Control Transmission Protocol
SD	Samferdselsdepartementet
SDH	Synchronous Digital Hierarchy

SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SPF	Single Point of Failure
SS7	Signalling System 7
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Spesielle Samfunnspålagte Oppgaver
TCP	Transmission Control Protocol
TNO	Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek
TNP	Transport Network Provider
TRDIX	Trondheim Internet Exchange
TTP	Tiltrodd tredjepart
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
USIT	Universitetets Senter for Informasjonsteknologi
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
VOIP	Voice Over IP
VPN	Virtual Private Network

1 Innledning

1.1 Bakgrunn for oppgaven

PT (Post- og teletilsynet [33]) er et frittstående forvaltningsorgan som ligger under Samferdselsdepartementet. Hovedansvarsområdet for etaten er å regulere og overvåke post- og telekommunikasjonssektoren i Norge. PT er selvfinansiert, og driften blir primært finansiert gjennom gebyrer.

Sikkerhet og beredskap i nett er en seksjon i avdeling for Strategi, Adressering og Sikkerhet. Arbeidsområdet til seksjonen omfatter blant annet: Sikring av prioriterte brukeres tilgang til robuste telekommunikasjonsløsninger, samlokalisering av operatører i fjellanlegg, beskyttelseskrav mot fysiske trusler og EMP (elektromagnetisk puls), samt å sikre samfunnskritiske institusjoner (Totalforsvaret) tilgang til sikre og robuste telekommunikasjonsløsninger. Sårbarhet og beredskap knyttet til Internett kommer også inn under seksjonens arbeidsområde.

Kritisk infrastruktur og beskyttelse av denne har vært en god del omtalt. På nasjonalt nivå finner vi BAS-prosjektet (Beskyttelse Av Samfunnet) [39], som omhandler beskyttelse av kritiske infrastrukturer i Norge. I USA er det opprettet et eget departement – DHS (Department of Homeland Security) [38], som koordinerer all nasjonal innsats innen blant annet kritiske infrastrukturer. I denne sammenhengen har man sett på sårbarhet og risiko ved ulike infrastrukturer i samfunnet, som for eksempel telefonnettet, vannforsyningen, transportsektoren og elektrisitet.

Flere samfunnsaktører samarbeider i BAS under ledelse av FFI (Forsvarets Forskningsinstitutt). BAS5 er den delen som er relevant i forhold til temaet vårt og omhandler CIIP (Critical Information Infrastructure Protection) [11]. PT ønsker at vi skal se nærmere på sårbarheten til Internett i Norge. Bakgrunnen for dette er blant annet tilsynets oppgaver med å sikre landets informasjons-infrastruktur, samt påpeke svakheter som må utbedres.

Internett begynte som et forskningsnett og var ikke tiltenkt den rollen det har fått idag. Eksempler på dette er IP-telefoni, eHandel og banktjenester. Det har derfor ikke vært like mye fokus på Internett som kritisk informasjons-infrastruktur før de siste årene.

Målgruppen for arbeidet vårt er deltakerne i BAS5-prosjektet, inkludert PT, som har ansvaret for SSO (Spesielle Samfunnspålagte Oppgaver) [25] overfor telekombransjen. Resultatene fra masteroppgaven kan brukes til å påpeke sårbarheter i forbindelse med Internett i Norge.

1.2 Oppgavebeskrivelse og mål med arbeidet

Etter hvert som Internett har utviklet seg til å bli en bærer for samfunnskritiske tjenester, er det interessant å se helhetlig på robustheten til disse tjenestene ifra et teknologisk og samfunnsmessig perspektiv. De siste årene har fokuset på beskyttelse av kritiske infrastrukturer økt betraktelig. Begrepet som benyttes i internasjonal sammenheng er CIIP (Critical Information Infrastructure Protection).

Hovedfokuset i oppgaven vil være å komme frem til en god fremgangsmåte for å vurdere og behandle sikkerheten og sårbarheten i en IP-basert infrastruktur. Denne fremgangsmåten skal i etterkant kunne brukes for å få oversikt over, samt å vurdere og fatte beslutninger i forbindelse med

en gitt konkret IP-basert infrastruktur. Det er ikke meningen å gjøre noen uttømmende sårbarhetsanalyse av Internett i Norge, da dette krever omfattende tilgang til data som vi ikke nødvendigvis har tilgang til under oppgaven.

Det finnes allerede en del arbeid innen kartlegging og vurdering av kritiske infrastrukturer internasjonalt. Dette arbeidet bærer preg av at forskjellige arbeidsgrupper har hvert sitt fokusområde og mangler helheten innen fagfeltet. Vi vil studere metodene og modellene i dybden og introdusere og anvende en lagdelt tankegang. Hensikten er på en oversiktlig og angripelig måte å få med de viktigste aspektene ved sikkerheten og sårbarheten knyttet til bruken av et IP-basert nettverk som informasjons-infrastruktur. Vi skal se på samspillet mellom noder i nettet og identifisere og vurdere sammenhenger mellom nøkkelressurser som infrastrukturen er avhengig av på forskjellige nivåer.

I fortsettelsen av oppgaven vil det være interessant å ta for seg et case study hvor man legger inn data om en reell IP-infrastruktur i Norge eller en fiktiv infrastruktur. Vi vil arbeide med en konkret anvendelse av lagdelt tankegang. Dersom vi får tilgang til data fra en virkelig infrastruktur, er det også spennende å se hvorvidt fremgangsmåten vår bidrar til en bedre oversikt. Vi kommer til å se på svakheter og sammenhenger mellom ressurser i infrastrukturen ved hjelp av lagdelt tankegang.

1.3 Avgrensninger

CIIP inngår i Homeland Security. Homeland Security omfatter alt som har å gjøre med «*domestic governmental actions*» og inkluderer mobilisering i nødssituasjoner, overvåking, spionasje, beskyttelse av infrastruktur og grensekontroll. Vi begrenser oss til informasjons-infrastruktur og kun det som har med IP-nett å gjøre. Dette omtales i flere sammenhenger som CIP (Critical Infrastructure Protection), og CIIP. CIIP er en del av CIP. Når vi omtaler Internett, er det CIIP som er aktuelt [5], [37].

Information Security er et felt innen Security Engineering, som er et gammelt fag med røtter flere hundre år tilbake i tid. Fra å omfatte fysisk sikring med låser og lignende, omfatter området nå i tillegg mange former for teknologisk sikring og analyse av sikkerhet. Vi kommer ikke til å legge vekt på andre typer sikkerhet enn det som har med analyse og vurdering av sårbarheten i infrastrukturen til Internett i Norge – transportnettet, stamnettet og aksessnettet ut til brukerne. Fokuset ligger på transporten av IP (Internet Protocol), ikke hva som skjer på hver enkelt bruker sin maskin. Det vil ikke bli gjort studier av samfunnssektorer, men de er helt klart en del av helhetsbildet og kommer derfor til å bli nevnt. Sikkerhet og sårbarhet på fysisk nivå, det vil si miljøet og strømnettet, kommer vi ikke til å ta for oss.

Det vil ikke bli gjort fullstendig sårbarhetsanalyse eller risikovurdering av Internett i Norge som helhet. Det vil bli fokusert på å komme frem til metoder og modeller som i ettertid kan brukes til sårbarhetsanalyse og komme med pekepinner på sårbarhetsreduserende tiltak.

På grunn av et bredt problemområde og oppgavebeskrivelse fra oppdragsgiver, ble tittelen ganske omfangsrik. Vi presiserer at vi i modellen ikke kommer til å legge mye vekt på IP-nett/intranett i bedrifter. Disse aspektene kommer til å bli nevnt, men hovedfokuset tar for seg Internett i Norge helt frem til brukerne, det vil si til og med aksessnettet.

1.4 Rapportens oppbygging

I fortsettelsen av rapporten tar vi for oss teorigrunnlaget. Først blir det en innføring i fagområdet. Det er nødvendig med god innsikt i hvordan Internett er bygd opp, samt hvordan man i IP-verdenen deler opp i ulike lag; jamfør OSI/ISO-modellen (Open Systems Interconnection / International Organization for Standardization). Sikkerhet og sårbarhet blir også behandlet i dette kapittelet.

Kapittel tre tar for seg større organisasjoner og myndighetene i vårt eget og andre land. Det har blitt gjort en del relevant arbeid innen fagområdet. For å danne et grunnlag for vårt arbeid, er det interessant å studere de andre arbeidene i dybden, samt gjøre en vurdering av disse.

I kapittel fire presenterer vi modellen og fremgangsmåten vi har kommet frem til. Det vil bli gitt en detaljert gjennomgang og forklaring av modellen. Vi vil også beskrive hvordan vi har gått frem for å løse oppgaven.

Kapittel fem tar for seg et case study hvor vi tester modellen på et sykehus tilkoblet en IP-infrastruktur og trekker inn viktige elementer fra Internett i Norge. I tillegg blir det en oppsummering med drøfting både av case study og vår egen modell.

Rapporten avsluttes med kapittel seks, som inneholder konklusjon og videre arbeid innen området.

2 Innføring og bakgrunn

I mye av litteraturen vi har studert, virker det som mange av forfatterne har telekom-bakgrunn. Derfor oppstår det av og til litt uklarheter om hva et IP-nett er, hvordan det fungerer og hvordan det er oppbygd. For å klare opp i slike uklarheter og for å ha en god forståelse om hva vi snakker om senere i rapporten, mener vi det er viktig å ta en gjennomgang av oppbyggingen og funksjonaliteten til Internett.

I oppgavebeskrivelsen ble det sagt at vi skulle introdusere og anvende en lagdelt tankegang. For å forstå hva lagdelt tankegang er og hvordan det fungerer, er det hensiktsmessig å studere det klassiske eksempelet; OSI/ISO-modellen. Det vil også bli gjennomgått kjente tema tilknyttet sikkerhet og sårbarhet i Internett-infrastrukturen.

2.1 Introduksjon til fagområdet

I forbindelse med temaet har vi satt oss inn i fagområdet og relevant arbeid både på nasjonalt og globalt plan. Etter 11. september 2001 har fokuset og tankegangen fått en betydelig justering. Det samme gjelder aktualiseringen av temaet med påfølgende ressurser til forskning og utbedring av infrastrukturer. Information Security har eksistert en stund som fagområde, men området Homeland Security er nytt de siste årene. Det er ulike syn på hvorvidt Homeland Security kan regnes som et eget fagområde; i og med de klare ulikhetene mellom dette og data- og nettverkssikkerhet generelt, har vi valgt å gjøre det slik.

Den største forskjellen mellom Information Security og den teknologiske disiplinen innen Homeland Security, er fokuset på informasjons-infrastruktur. USA er trolig det landet som er mest etablert innen fagområdet. De tydeligste eksemplene på det er DHS' opprettelse av et National Cyber Security R&D Center [5] som skal være en overordnet finansierings-instans for all slik forskning i USA.

2.1.1 Historisk bakgrunn

På midten av 1990-tallet innledet Clinton-administrasjonen en kartlegging av kritisk infrastruktur i USA. Dette ble i liten grad fulgt opp, men etter 11/9-01 ble fokuset rettet mot alt av samfunnskritiske tjenester. I ettertid ble det opprettet et eget departement, DHS [38], som nå koordinerer alt slikt arbeid på nasjonalt nivå. Dette inkluderer bedrifter og organisasjoner som ikke er statlige, men som bidrar gjennom et frivillig nettverk styrt av DHS. GAO (Government Accountability Office [36]) har lignende oppgaver som Riksrevisjonen her til lands, men går tilsynelatende grundigere til verks i omtalen av konkrete prosjekter som forskjellige samfunnsaktører er med på. Deriblant har de utarbeidet en tilstandsrapport [28] som beskriver DHS' visjoner, mål, ressurser og gjeldende status.

På verdensbasis var det noen få land som hadde slikt arbeid før 2001, og Norge har hatt et eget prosjekt helt siden 1994 (BAS). Ifølge en rapport fra Nederland fra 1999/2000 [51], var følgende land igang med analyser og studier med hensyn på infrastruktur og sårbarhet: USA, Canada, Tyskland, Storbritannia, Frankrike, Sverige, Norge, Danmark, Finland, Sveits, Israel, Japan, Singapore og Australia. Disse initiativene var nesten utelukkende begrenset til de enkelte lands problemområder, og oppdragene var for det meste bestilt av det enkelte lands forsvarsdepartement.

I senere tid er det imidlertid satt igang større globale forskningsprosjekter, og hvert år holdes det flere konferanser som blant annet tar opp temaer innen beskyttelse av teknologisk infrastruktur (CIIP). ISI/WISI06 (Workshop on Intelligence and Security Informatics, [53]) er et eksempel på en konferanse som kun tar opp sikkerhetsspørsmål i forbindelse med nasjonale og internasjonale tjenester og anvendelser. Tema som tas opp der inkluderer «*data management, data and text mining for ISI applications, terrorism informatics, deception detection, terrorist and criminal social network analysis, crime analysis, monitoring and surveillance, policy studies and evaluation, information assurance*».

Det store fokuset på terrorisme og organisert kriminalitet har også ledet oppmerksomheten inn på DDoS-angrep (Distributed Denial of Service). Mye forskning tar for seg oppgradering av rutere og forskjellige IDS-algoritmer (Intrusion Detection System) for tidlig deteksjon og motvirkning av DDoS-angrep. Dette faller også delvis inn under Homeland Security, selv om fokuset er mer på tjeneste-nivå enn på infrastruktur-nivå.

CRN (Comprehensive Risk Analysis and Management Network) er et sveitsisk-svensk initiativ som ble stiftet i 2000. I 2002, 2004 og 2006 har de utgitt en bok som heter CIIP Handbook. Den tar for seg en oversikt over arbeid innen CIIP i forskjellige land og hvilke metoder og arbeid de har gjort i forbindelse med CIIP og CIP [6]. Post- och telestyrelsen har også gjort en del arbeid innen sikkerhet og robusthet på Internett i Sverige. Spesielt interessante er rapportene «*Strategi för ett säkrare Internet*» [2] og «*Är Internet i Sverige robust?*» [3].

Nederland er en av pionerene innen CIIP i Europa. Internett i Nederland fungerer som en hub for Internett i Europa. AMS-IX (AMSterdam Internet eXchange) kobler sammen amerikanske, skandinaviske og flere europeiske ISPer [35]. Man har derfor i Nederland gjort en del arbeid på Internett som kritisk infrastruktur og utviklet modeller og metoder for å vurdere sårbarheter. Et par av de viktigste arbeidene er KWINT-rapporten [10], [43] og BITBREUK [9]. Også i Canada har man utviklet modeller og metoder som er interessante å kikke på, jamfør Canadian Layer Model [6], [26], som tar for seg kritisk infrastruktur og problemer knyttet til år-2000-skiftet.

I Norge har det blitt gjort en del arbeid innen Internett, sårbarhet og organisert kriminalitet. BAS5 (IKT infrastruktur) [11] er et prosjekt fra høsten 2004 til høsten 2006 med et budsjett på 12 millioner kroner og inkluderer følgende deltakere: NSR (Næringslivets Sikkerhetsråd), DSB (Direktoratet for Samfunnssikkerhet og Beredskap), NSM (Nasjonal Sikkerhetsmyndighet), OED (Olje- og Energi-Departementet), NVE (Norges Vassdrags- og Energidirektorat), OD (Oljedirektoratet), Statnett, JD (Justisdepartementet), MOD (Moderniserings-departementet), SD (Samferdselsdepartementet), PT, Telenor, NSR (Norsk Forskningsråd), FFI, FSA (Forsvarets Sikkerhetsavdeling). I tillegg er Universitetet i Stavanger, Høgskolen i Gjøvik og NTNU (Norges teknisk-naturvitenskapelige universitet) med. Det er likevel verdt å merke seg at det ikke finnes noe overordnet statlig departement som styrer utviklingen slik DHS gjør i USA.

Det siste tilskuddet til arbeidet med informasjons-infrastrukturer i Norge er NOU 2006:6 «*Når sikkerheten er viktigst*»; utarbeidet for Justis- og politidepartementet. I tillegg er BAS5 inne i sitt siste virkeår, og den endelige rapporten skal etter planen foreligge innen utgangen av desember 2006.

2.1.2 Internett i forhold til samfunnet og infrastrukturer

I forbindelse med studiene av Internett i Norge, er det til stor hjelp å ha en god forståelse av infrastrukturer generelt, samt hvordan Internett fungerer som infrastruktur. Grunnen til dette er at

flere av mekanismene som er i drift på Internett har fellestrekk med infrastrukturer generelt. Et eksempel på dette er prinsippet om redundans i kommunikasjonskanaler og -utstyr.

2.1.2.1 Infrastrukturer generelt

Infrastrukturer er et bredt tema som inkluderer:

- Transport
- Offentlige tjenester (brann, politi, søppelhåndtering, hjelp ved oversvømmelser)
- Offentlig regulerte tjenester (elektrisitet, drikkevann, kloakk, offentlig transport, telekommunikasjon)
- Nasjonale tjenester (forsvaret, postvesenet, pengesystemet)
- Myk infrastruktur (utdannelse, helse, biblioteker, velferd)

Informasjons-infrastruktur er definert slik: *«A physical communications network, particularly of national or global scope»* [41]. Kritisk infrastruktur er definert slik: *«[In security,] those physical and cyber-based systems essential to the minimum operations of the economy and government»* [5], [27]. Vi skal behandle kritisk informasjons-infrastruktur, som innebærer *«fysiske/elektroniske kommunikasjonsnettverk som er essensielle nasjonalt for økonomien og myndighetene»*.

2.1.2.2 Internett som infrastruktur

Den norske delen av Internett er i mye større grad enn telenettene desentralisert og derfor vanskeligere å regulere og ha oversikten over. Dette gjør det mye vanskeligere å forutsi konsekvensene av en eventuell krisesituasjon, selv om man har foruroligende pekepinner fra nordvestlandet ved kraftig uvær. Det ser ikke ut til at redundansen er utbygd i stor grad, og i alle fall ikke tatt i betraktning at de forskjellige ISPene (Internet Service Provider) sjelden samarbeider seg imellom med hensyn på redundans og kundens opplevelse av oppetid. Dette kan synes noe merkelig, da landet som kjent er særdeles langstrakt og periodevis relativt ufremkommelig og svært kostbart å bygge nettverk i.

2.2 OSI/ISO-modellen

2.2.1 Introduksjon til OSI/ISO

OSI-modellen (Figur 1) er en standard utviklet av ISO og de største aktørene i markedet på slutten av 1970-tallet og begynnelsen av 1980-tallet. Det som i begynnelsen så ut til å være en god tilnærming til standardisering av nettverkskommunikasjon, falt i 1996 fullstendig ifra hverandre. Forklaringen på dette var sammensatt, og de viktigste momentene hadde med implementasjonen å gjøre. Flere motstridende interesser i standardiseringsorganet hadde sørget for et utall valgmuligheter, som i sin tur gjorde utstyr inkompatibelt selv om det benyttet den samme standarden. I tillegg mente mange aktører at selve modellen var for tungvint.

Figur 1: 7-lags OSI-modell

Parallelt med dette arbeidet hadde det imidlertid vokst frem et annet alternativ med lignende egenskaper: TCP/IP-stakken (Transmission Control Protocol / Internet Protocol, se Figur 2). Dette arbeidet begynte som et behov i 1972, da man ønsket å koble sammen flere forskjellige nettverk – både satellitt-baserte og forskjellige bakkebaserte nettverk. Arbeidet foregikk som en del av DARPA (Defense Advanced Research Projects Agency) / ARPANET (Advanced Research Projects Agency Network) -prosjektet, og var allerede i 1984 gjort til den eneste standarden for all militær kommunikasjon i USA. Grunnet økende kommersiell interesse, ble TCP/IP-stakken mest populær også i utstyret som ble produsert.

Figur 2: 5-lags TCP/IP-stakk

Den mest iøynefallende forskjellen på OSI-modellen og TCP/IP-stakken er de to ekstra lagene mellom transportlaget og applikasjonslaget; sesjonslaget og presentasjonslaget. Flere mener imidlertid at OSI-modellen mangler funksjonaliteten til ARP/RARP-protokollen ((Reverse) Address Resolution Protocol) mellom lag to og tre, og ICMP-protokollen (Internet Control Message Protocol) og IGMP-protokollen (Internet Group Management Protocol) mellom lag tre og fire.

I den videre behandlingen av OSI-modellen refererer vi imidlertid kun til TCP/IP-stakken (se Figur 2) – ikke OSI-modellen med syv lag. Hensikten med å behandle modellen er ikke først og fremst å gi noen innføring i nettverksteori for IP-nett, men å bygge et teoretisk fundament for lagdelt tankegang innen infrastrukturer [42], [14].

2.2.2 Fundamentale egenskaper ved lagdeling og IP-nett

I motsetning til telefonnettet som er forbindelsesorientert, er IP-nett forbindelsesløse i bunnen. Det innebærer at det ikke forhandles om noen forbindelse før man kan sende data ut på nettverket. For protokollstakken betyr det at det ikke finnes noe motstykke til samtalestyringen som foregår i telekom-verdenen. Samtalestyringen er byttet ut med ende-til-ende prinsippet, hvor hver enkelt endeterminal er utrustet med intelligens nok til å adressere hver enkelt pakke til deres endelige destinasjon. Prinsippet er helt tilsvarende adresseringen av et brev som blir tatt hånd om av postvesenet; man trenger mottakerens fullstendige adresse før man kan poste brevet.

Et fundamentalt prinsipp ved lagdeling er tanken om at man kan bytte ut et hvilket som helst lag uten at det får konsekvenser for lagene over og under. Det krever imidlertid klart spesifiserte grensesnitt. IP-protokollen er bygd med tanke på nettopp dette; jamfør begrepet *«Alt over IP, IP over alt»* [22]. Utbredelsen av Ethernet har gjort at man spøkefullt har sagt det samme om denne protokollen.

2.2.3 Beskrivelse av lagene i TCP/IP-stakken

2.2.3.1 Lag 1: Fysisk lag

Fysisk lag er en fellesbetegnelse for alle elektriske og fysiske egenskaper for utstyr og medier som benyttes til å frakte digitale samband. Dette inkluderer polaritet, spenning og kabelspesifikasjoner. Hovedfunksjonene på fysisk lag er:

- Oppretting og terminering av en forbindelse til et kommunikasjonsmedium.
- Deltakelse i delingen av ressurser mellom flere brukere – så som konflikthåndtering og flytkontroll.
- Modulasjon eller konvertering mellom digital representasjon av data og korresponderende signaler sendt over en kommunikasjonskanal. Dette er signalene som sendes over det fysiske mediet – enten det er kabel eller luft.

På fysisk lag er det fornuftig å ta med teknologier som oppringt modem / xDSL (Digital Subscriber Line) over tvunnet parkabel (kobber), kabelmodem over koaksialkabel, fibermodem over fiberkabel og forskjellige typer trådløs aksess (for eksempel Wi-Fi og WiMAX (Worldwide Interoperability for Microwave Access) med korresponderende termineringsutstyr).

Protokoller som arbeider på dette nivået inkluderer Ethernet, ATM (Asynchronous Transfer Mode), Token Ring, IEEE 802.11 (Wi-Fi), IEEE 802.16 (WiMAX), Frame Relay og SDH (Synchronous Digital Hierarchy).

2.2.3.2 Lag 2: Datalink-laget

Dette laget sørger for den funksjonelle delen av dataoverføringen mellom nettverksenheter og kollisjonsdeteksjon og -håndtering fra fysisk lag. Adresseringen er fysisk; det vil si at den er hardkodet inn i utstyret under produksjonen. Denne metoden for adressering er flat, som betyr at det ikke er noen sammenheng mellom adressen og lokasjonen i nettverket. Utstyr som arbeider på dette laget inkluderer svitsjer og broer.

Den mest brukte protokollen på datalink-laget er Ethernet, som i økende grad benyttes både i

lokalnett, aksessnett og transportnett. I tillegg har telekom-verdenen frem til nå hatt tradisjon for å bruke ATM, SDH og enkelte steder Frame Relay. Tidligere var også Token Ring en mye brukt standard innen lokalnett. Leverandører av xDSL benytter i stor grad PPPoE (Point-to-Point Protocol over Ethernet), som også er en protokoll som arbeider på dette laget.

Nyere teknologier inkluderer imidlertid også trådløs aksess, som tar i bruk protokoller som IEEE 802.11 (Wi-Fi) og 802.16 (WiMAX). Wi-Fi er best kjent som trådløst PC-nett, og har relativt kort rekkevidde (opptil 90 meter ved fri sikt, mer ved bruk av MIMO-teknologi (Multiple Input Multiple Output). WiMAX er en standard for datanettverk over lengre avstander, og er basert på Wi-Fi. I tillegg kan det nevnes at det finnes protokoller som arbeider både på lag to og tre, og eksempler på disse er ARP/RARP og MPLS (Multiprotocol Label Switching).

2.2.3.3 Lag 3: Nettverkslaget

Nettverkslaget omfatter overføring av datapakker med variabel lengde fra ende til ende via ett eller flere nettverk. Opphavet til navnet er «*internetworking layer*», som henviser til lagets opprinnelige hensikt; evnen til å koble sammen forskjellige nettverk. Laget utfører ruting, flytkontroll, segmentering/desegmentering av pakker, samt feilsjekking av meldingshodet.

Adresseringen på nettverkslaget er i motsetning til datalinklaget, logisk og hierarkisk. Verdiene er inndelt etter det samme prinsippet som telefonnumre, hvor sifferne i økende grad åpenbarer lokasjonen til endeterminalen.

På dette laget snakker vi i oppgaven utelukkende om IP-protokollen – som definert i oppgavetittelen. Utstyr som benytter dette laget, er rutere og svitsjer med ruting-funksjonalitet (såkalte lag-3 svitsjer).

2.2.3.4 Lag 4: Transportlaget

Det er vanskelig å beskrive laget generelt, siden funksjonaliteten er avhengig av hvilken protokoll som blir benyttet. På transportlaget finnes funksjonaliteten for transparent dataoverføring mellom endeterminaler. Påliteligheten til en gitt forbindelse blir også kontrollert på dette laget. Alle de vanligste transportlagsprotokollene tilbyr feilsjekking av oversendte data og port-multipleksing. Sistnevnte er nødvendig for at flere applikasjoner skal kunne benytte protokollen samtidig. Dette er analogt med den første linjen i postadressen, som gjør at flere mennesker kan benytte den samme postkassen. Noen transportlags-protokoller er tilstands- og forbindelsesorienterte (TCP, SCTP (Stream Control Transmission Protocol), som betyr at transportlaget kan holde orden på pakkene som blir sendt og retransmittere de som måtte feile. De mest brukte protokollene er TCP og UDP (User Datagram Protocol).

TCP er den mest omfattende av de to, og støtter:

- Feilsjekking av meldingshodet og nyttelasten
- Port-multipleksing
- Tilstands- og forbindelsesorientert transport
- Pakkelevering i riktig rekkefølge
- Flytkontroll – for at mottakeren skal kunne begrense senderaten
- Metningskontroll – for at metning i nettverket indirekte skal kunne redusere senderaten
- Strøm-basert pakketransport (bitstreams)

UDP er svært enkel med følgende funksjonalitet:

- Feilsjekking
- Port-multipleksing

I tillegg finnes det et fåtall andre protokoller på transportlaget – så som SCTP og DCCP (Datagram Congestion Control Protocol). Sistnevnte er fremdeles under utvikling av IETF (Internet Engineering Task Force), mens SCTP er ferdig standardisert. De særskilte behovene som telekom-verdenen hadde i forbindelse med transmisjon av signaleringstrafikk (SS7 (Signalling System 7)) over IP-baserte samband, medførte at IETF-arbeidsgruppen SIGTRAN opprettet en egen protokoll til dette formålet [23].

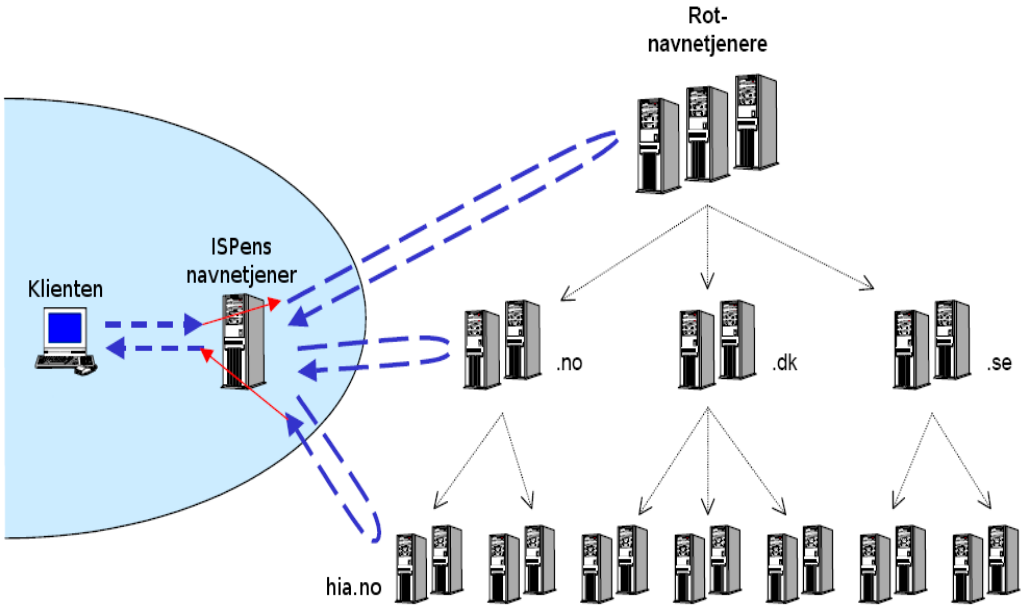
2.2.3.5 Lag 5: Applikasjonslaget

Applikasjonslaget er det mest avanserte laget og benyttes av de fleste brukerapplikasjonene. Her finner vi protokoller som HTTP (Hypertext Transfer Protocol), DNS (Domain Name System), FTP (File Transfer Protocol), SSH (Secure Shell), NFS (Network File System), SSL (Secure Socket Layer), POP3 (Post Office Protocol version 3), SMTP (Simple Mail Transfer Protocol), IMAP (Internet Message Access Protocol) og BitTorrent. Vanlige brukere er sannsynligvis mer kjent med begreper som nettleseren, programvare for overføring av filer, nettbanken, epost-leseren og fildelingsprogrammet – som naturligvis benytter seg av de foregående protokollene for å få jobben gjort. Før nettverksteknologien ble tatt i bruk, var applikasjonene lokale og kommuniserte kun med hverandre på den samme vertsmaskinen. Applikasjonslaget gjør imidlertid at dataprogrammer kan spres over så mange vertsmaskiner man ønsker – og dermed samarbeide om å utføre svært avanserte oppgaver. Det som for brukeren fortoner seg som et enkelt lokalt dataprogram, kan i virkeligheten være et kompleks og distribuert nettverkssystem spredt over hele verden.

Initiativene som har blitt gjort for å knekke koder og analysere store mengder data i sanntid er gode eksempler på dette, jamfør «*[Enigma] M4 Message Breaking Project*» [34] og «*Berkeley's Space Sciences Laboratory – Search for Extra Terrestrial Intelligence [SETI@home]*» [48]. Førstnevnte prosjekt ble offisielt igangsatt 9. januar 2006 for å knekke tre beskjeder snappet opp fra tyske ubåter i Nord-Atlanteren mellom februar og desember 1942. De to første beskjedene ble knekt henholdsvis 20. februar og 7. mars. Det sistnevnte prosjektet har sin bakgrunn fra Berkeley-universitetet i USA 17. mai 1999 og er et initiativ for å analysere radiobølger fra verdensrommet. SETI@home er det største «*distributed computing*»-prosjektet på verdensbasis med imponerende 250 TFLOPS (billioner flyttalls-operasjoner per sekund). I fortsettelsen vil vi se nærmere på to essensielle prokotoller som befinner seg på applikasjonslaget – henholdsvis DNS og BGP (Border Gateway Protocol).

2.2.3.5.1 DNS

DNS er både en protokoll og et system for lagring og utveksling av domeneinformasjon på Internett. Protokollen hører hjemme på applikasjonslaget. De to primære oppgavene til DNS er sammenknytning av IP-adresser og domenenavn samt informasjon om tilknyttede epost-servere. Begge deler betegnes som essensielle og kritiske funksjoner på nåtidens Internett. DNS bruker UDP som primærtransport for forespørsler, med unntak av større informasjonsmengder – som eksempelvis sonefiler, som gjerne benytter TCP.



Figur 3: Eksempel: DNS-forespørsel (modifisert utgave fra [22])

Systemet av navnetjenere er distribuert og hierarkisk oppbygd, og ICANN (Internet Corporation for Assigned Names and Numbers) styrer toppnivå-tjenerne (også kalt rot-tjenerne). Disse peker videre til neste nivå med navnetjenere, som for eksempel *com*, *org* og *no*. Slik fortsetter hierarkiet nedover, helt til man kommer til den endelige adressen. Adressen www.hia.no kan derfor teoretisk bli oversatt til en IP-adresse på denne måten (se Figur 3):

- Klienten spør ISPens navnetjener om www.hia.no-domenets adresse
- Siden ISPens navnetjener ikke betjener denne adressen, går forespørselen videre til toppnivået i hierarkiet. Den spør derfor rot-tjenerne om www.hia.no-domenets adresse
- En av rot-tjenerne svarer: Snakk med .no-tjenerne på følgende adresse ...
- Klienten spør .no-tjenerne om www.hia.no-domenets adresse
- En av .no-tjenerne svarer: Snakk med hia.no-tjenerne på følgende adresse ...
- Klienten spør hia.no-tjenerne om www.hia.no-domenets adresse
- En av hia.no-tjenerne svarer med IP-adressen til www-tjeneren

Denne prosedyren er tidkrevende og båndbreddekrevende, og antallet forespørsler har økt dramatisk med den eksplosive utbredelsen av Internett. Man har derfor for lengst implementert mellomlagring av DNS-informasjon. Dette fungerer ved at man både på den lokale datamaskinen, hos Internett-leverandøren og på nasjonalt plan mellomlagrer DNS-oppføringer. I tillegg har gjerne bedrifter sine egne mellomlagre.

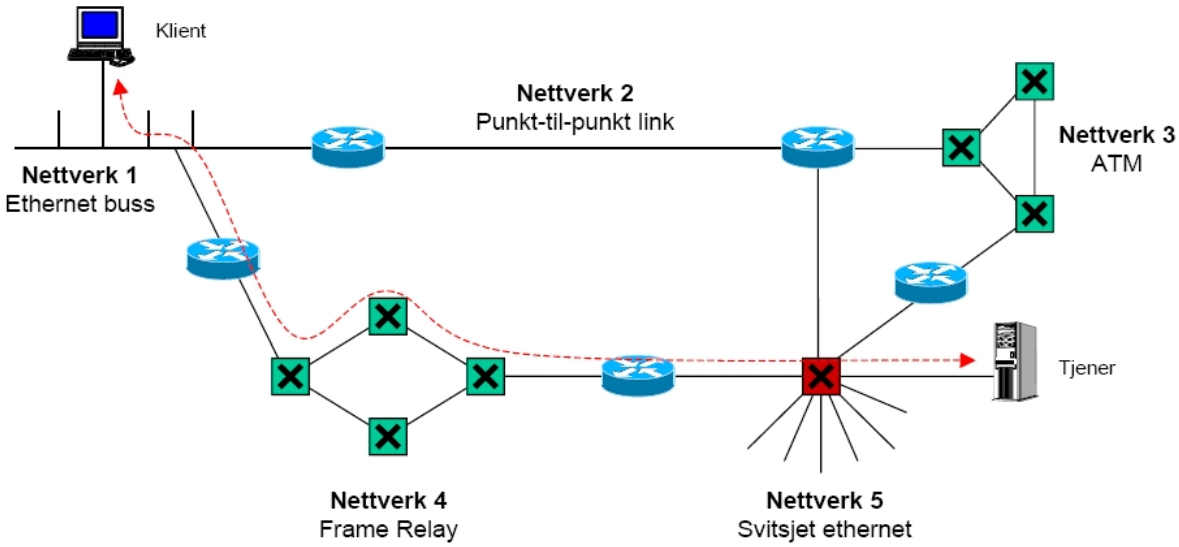
For å sikre at mellomlagret informasjon blir oppdatert ved endringer, er det innført gyldighetstid på DNS-informasjonen. Det er opp til den enkelte DNS-tjeneren å legge ved slik informasjon; som i sin tur gir eieren av domenet friheten til å bestemme tidsintervallet selv. Dersom man eksempelvis ønsker å bytte IP-adressen på et domene, bruker man gjerne en teknikk som går ut på å redusere gyldighetstiden på DNS-informasjonen til et svært kort intervall. Når den opprinnelige gyldighetstiden er utløpt, kan man så bytte IP-adressen uten at en stor brukergruppe opplever å surfe lenge på en utdatert nettadresse. Internett er svært avhengig av DNS-funksjonaliteten [14], [22], [30].

2.2.3.5.2 BGP

BGP er rutingprotokollen som anvendes mellom ulike AS (Autonome Systemer). BGP blir ofte omtalt som en protokoll på nettverkslaget. Ser man på transportmetoden, som består av TCP-forbindelser, kan man like godt plassere BGP på applikasjonslaget. Hovedfunksjonen til BGP er å utveksle en liste over tilgjengelige nettverk og hvilke AS man må gjennom for å nå disse nettverkene. Videre benyttes informasjonen som utveksles til å danne en graf over de forskjellige ASene og nettverkene [22].

2.3 Oppbyggingen og funksjonaliteten til Internett i Norge

Internett og andre IP-baserte nettverk er egentlig internettverk; det vil si nettverk av nettverk. Vi kan si at Internett er en samling av AS, som består av mange ulike nett med forskjellige teknologier; jamfør Figur 4. Internet Protocol er spesifisert med tanke på å kunne transporteres over alle typer underliggende teknologier. Alt som sendes over Internett blir lagt i en IP-pakke. Pakken blir sendt fra ruter til ruter som ved hjelp av en rutingtabell finner ut hvor pakken skal sendes på Internett slik at den kommer frem til den adressen som er spesifisert i destinasjonsfeltet. Et slagord som brukes om IP er: *«Alt over IP, IP over alt»* [22].



Figur 4: Internett består av mange ulike nettverk med ulike teknologier [22]

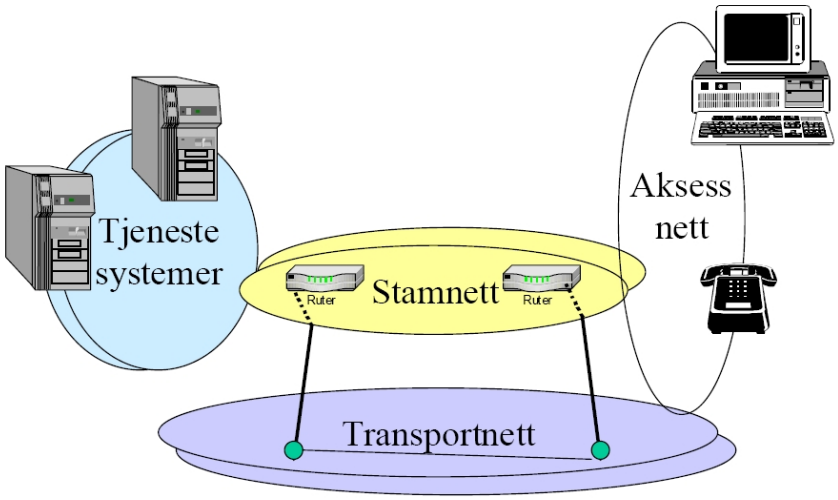
Internett baserer seg på ende-til-ende prinsippet. Det vil at at intelligensen finnes i endeutstyret og nettet er «*dumt*». I telenettet er terminalene «*dumme*», og man finner intelligensen i nettet. Siden Internett er «*dumt*» vil nettets funksjon kun være å finne ut hvor pakker skal og sende de til neste hopp. Man har altså ingen oppkobling slik som i telenettet. Internett er forbindelsesløst og bruker pakkesvitsjing, mens telenettet er forbindelsesorientert og bruker linjesvitsjing. Når man sier at Internett er komplekst, mener man ikke at funksjonaliteten til selve nettet er det, men at Internett er blitt komplekst fordi det er så mange aktører involvert på alle nivåer [10].

Telenettet har lokale sentraler som er knyttet sammen med hverandre. Internett derimot er mer stjerneformet. Det er fordi nesten all trafikken går innom de nasjonale samlingspunktene i Oslo hvor de største ISPene er tilkoblet.

En ISP er en organisasjon som eier og organisere sitt eget AS og tilbyr Internettjenester slik at man

kan surfe på web-en, lese epost og laste ned og opp filer. ISPen er selv fri til å organisere nettet sitt [20].

Skillet mellom ulike komponenter og roller på Internett blir stadig mer sammenslått og uklart. Før, mens Internett bygde mye på teleinfrastrukturen, delte man gjerne inn i aksessnettverk, stamnett (ryggrad + regionale nett), transportnett og tjenestesystemer – se Figur 5. Aktører kan ha en eller flere av disse rollene. Aksessnettet ble som regel levert av Telenor, og det var Telenor og et par andre aktører som hadde transportnettet. ISPer leide da aksessnettet av Telenor, mens transportnettet ble leid av Telenor og de andre aktørene. Nå har flere ISPer egne transportnett, og det blir derfor vanskeligere å skille mellom transportnettet og stamnettet til en ISP [20].



Figur 5: Komponenter på Internett [20]

Vi vil ta for oss aksessnett som en egen del og transport av IP som en egen del under *«2.3.2 Transport av IP på Internett»*. Den siste delen omfatter det som kalles transportnettet og stamnettet. Denne delen tar også for seg oppbyggingen av en ISPs nett, samt AS og samtrafikk.

2.3.1 Aksessnett

NAP (Network Access Provider) er en leverandør som tilbyr nettverksaksess til Internett [20]. De ulike aksessteknologiene tilbyr linker mellom brukerens utstyr og Internett. Aksessnettene transporterer meldinger fra brukerens endeutstyr til og fra ISPens nett. ISPen sørger for videre tilknytning mot resten av Internett. Først kommer en liten oversikt over de ulike teknologiene, deretter presenteres en mer detaljert beskrivelse [22].

Det finnes mange typer aksessnettsteknologier; både kablede og trådløse varianter. En vanlig bruker vil typisk få aksess over samme kobberkabel som vanlig telefoni går over, eller ved bruk av kabelen som leverer kabel-tv.

2.3.1.1 Kabelbaserte aksessnett

Telefonnettet i Norge er digitalt, men tilbyr både analoge og digitale aksesslinjer. Det kan høres ut som dette er to fysisk forskjellige linjer, men det er samme kabel med ulik teknologi for overføring av data. Har man ikke ISDN (Integrated Services Digital Network) må man bruke modem for å

kunne overføre digitale datasignaler som IP-pakker over en analog linje. Med ISDN har man digital aksesslinje til telenettet. Både modem og ISDN er oppringte forbindelser hvor man som vanlig privatperson må betale tellerskritt som for en samtale. Ved bruk av modem blokkerer man telefonlinjen slik at man ikke kan ringe samtidig. Ved bruk av ISDN har man en linje til Internett og en til telefoni. Ved bruk av modem vil man få hastigheter opp mot 57 kbit/s, mens ISDN gir 64 kbit/s ved bruk av en linje og det dobbelte hvis man og bruker begge linjene samtidig [22].

Den nyeste teknologien for bruk av kobberkablene er xDSL. DSL finnes i symmetriske og asymmetriske hastigheter. For å kunne bruke ADSL (Asynchronous Digital Subscriber Line) trenger man et ADSL-modem. ADSL-splitteren gjør at man kan bruke samme linja til telefoni og Internett samtidig ved å bruke ulike frekvenser til data og tale. Flesteparten av bredbåndskundene har ADSL, som gir størst hastighet ned, da man som regel har mest nedlasting. Hastighetene er opp mot 8 mbit/s ned og 1024kbit/s opp. ADSL2+ kan gi hastigheter opp mot 24 mbit/s ned. Disse hastighetene blir lavere jo lengre vekk man er fra telefonsentralen [22].

Får man Internettaksess over telefonkabelen er det Telenor som er NAP, da det er de som eier telefonnettet. Men hvis man for eksempel har LOS som ISP, er LOS også virtuell NAP. Har man ikke telefonabonnement hos Telenor, må man betale et ekstra gebyr for leie av kobberkabelen.

I mange byer er det utbygd kabel-tv. For å kunne bruke slike nettverk til Internett, må kabelleverandøren tilby Internettjenester. I tillegg trenger man et kabelmodem. Hastigheten er omtrent som for ADSL.

Fiber er vanlig som aksessmetode for bedrifter. En bedrift har da ofte direkte tilknytting fra sitt intranett til en ruter i nettet til ISPen. Aksessforbindelsen til bedriften trenger ikke å bruke de tidligere omtalte tradisjonelle aksessnettene. Det er også mulig å få fiber direkte hjem til seg selv som privatperson. Mange store ISPer tilbyr dette; da ofte i forbindelse med «*triple play*», som gir både TV, Internett og telefoni over fiberkabelen. Ved bruk av fiber i bedrift og privat er det gjerne Ethernet som er transportteknologi.

2.3.1.2 Trådløse aksessnett

Av trådløse aksessteknologier har vi Wi-Fi, WiMAX, UMTS (Universal Mobile Telecommunications System), GSM/GPRS (Global System for Mobile Communications/General Packet Radio Service) og satellitt. Noen av disse er mobile, det vil si at man kan bevege seg rundt uten å miste forbindelsen, mens andre er faste og andre igjen er nomadiske, som innebærer bevegelse innenfor et gitt område. Wi-Fi og den opprinnelige versjonen av WiMAX er fast eller nomadisk. Mobiltelefonsystemene UMTS og GSM/GPRS og den mobile versjonen av WiMAX er mobile systemer [22], [49].

Wi-Fi kan være en vanlig aksessmetode, men den kan også høre til PAN (Private Access Network). Hastigheter på Wi-Fi er teoretisk 54 mbit/s med 802.11g [22] og 540 mbit/s på 802.11n [13]. Hastigheten varierer med rekkevidden. Maksimal rekkevidde på Wi-Fi er cirka 90 meter ved fri sikt, men gjenstander som vegger og lignende gjør rekkevidden mindre. En bedrift får som regel Internett-aksess gjennom fiber eller ADSL fra en ISP. Når de ansatte i bedriften skal få aksess til Internett, skjer dette typisk gjennom intranettet – det bedriftsinterne nettet, som er bygd på LAN (Local Area Network) eller WLAN (Wireless Local Area Network). Man kan derfor si at en ansatt i en bedrift får tilgang til Internett gjennom et privat aksessnettverk, mens bedriften typisk får Internett-aksess over fiber eller ADSL. I bedriftssammenheng vil ikke Wi-Fi regnes som en vanlig aksessteknologi, men som en privat aksessteknologi.

Wi-Fi kan brukes som en vanlig aksessmetode istedet for ADSL, fiber og kabel. I den senere tid er det blitt vanligere og vanligere med offentlige Wi-Fi hotspots; det vil si trådløse Internettsoner eller IP-soner hvor brukere kan koble seg til og få aksess til Internett [22]. Telenor tilbyr slike IP-soner på diverse flyplasser, tog- og bensinstasjoner. En bruker må da betale et visst beløp for å få tilgang. I slike trådløse IP-soner vil Wi-Fi være aksessteknologien som gjør at brukeren får aksess til Internett. Et annet eksempel er i Storbritannia, hvor man tilbyr Wi-Fi som aksessteknologi. I toppen av lyktestolper monterer man trådløse basestasjoner som kommuniserer seg imellom og gir trådløs Internettilgang til privatpersoner. Dette kalles mesh-nettverk.

WiMAX er en teknologi som har fått mye omtale det siste året. Man snakker om trådløs bredbåndsaksess i områder der det er dyrt å legge kabler. WiMAX har rekkevidde fra 5 til 8 km og kan i praksis tilby delt hastighet opp mot 60 mbit/s. Det vil si at hver enkelt bruker kan få ADSL-hastighet. Den nyeste standarden for WiMAX støtter i tillegg mobilitet. Dette går under betegnelsen mobil trådløs bredbåndsaksess. I tillegg til å oppnå høye hastigheter har man muligheten til å bevege seg rundt som i mobilnettet. Det krever selvsagt at det er støtte for mobilitet i basestasjonene [49].

GSM tilbyr både linjesvitsjede (CSD (Circuit Switched Data)) og pakkesvitsjede (GPRS) tjenester. Ved bruk av CSD må man betale tellerskritt for tiden man bruker, mens det for GPRS er betaling i forhold til overført datamengde. IP-pakkene fra mobilen blir da sendt over radionettet og tunnelert gjennom kjernenettet i mobilnettet og frem til en gateway som står mellom Internett og mobilnettet. Når pakkene kommer ut på Internett, blir de rutet rundt som alle andre IP-pakker. Tredje generasjons mobilnett, kalt 3G eller UMTS, tilbyr kun pakkesvitsjing for dataoverføring. Dette fungerer på samme måten som i GSM-nettet. Hastighetene man oppnår på mobilnettet avhenger av hvilken teknologi og hvor mange brukere som overfører data samtidig. Ved bruk av CSD er man sikret 9.6 kbit/s uansett. Med HSCSD (High Speed Circuit Switched Data) slås flere datakanaler sammen for å gi opptil 57.6 kbit/s linjesvitsjet. Siden Internett er pakkebasert, vil det sannsynligvis være billigere å benytte seg av GPRS, som kan gi teoretiske hastigheter opp mot 160 kbit/s – og 473.6 kbit/s ved implementasjon av EDGE (Enhanced Data rates for GSM Evolution [29]) i nettet. 3G-nettet tilbyr enda høyere hastigheter med opp mot 1920 kbit/s, og ved implementasjon av HSDPA (High Speed Downlink Packet Access [40]) kan dette komme opp imot fem ganger høyere hastighet enn vanlig 3G. Siden alle disse er mobile teknologier, har man dekning over alt hvor det er utbygd basestasjoner [17].

Den siste aksessteknologien vi tar med er satellitt. Satellitter blir plassert i forskjellige avstander fra jorden. Geostasjonære satellitter vil befinne seg på samme punkt hele tiden. Fordi de er langt oppe, trenger man store antenner for å få inn signalet. For eksempel trenger man parabolantenne for å ta inn satellitt-TV. Bruker man geostasjonære satellitter til Internettaksess, kan man kun laste ned. For opplasting pleier man ofte å benytte seg av ISDN. Grunnen til at man bruker satellitt og ikke kun ISDN, er at satellitt tilbyr mye høyere nedlastingshastigheter. Lavbane-satellitter går i lavere bane rundt jorda, og man trenger en god del slike for å få full dekning. Bruker man slike satellitter, er det mulig med både nedlasting og opplasting uten bruk av andre aksessmetoder [22].

2.3.2 Transport av IP på Internett

For at IP-pakkene eller trafikken på Internett skal komme frem, er de avhengige av et underliggende transportnettlag. Det finnes mange teknologier for transport av IP, men det går mer og mer i retning av at man bruker Ethernet over fiber til å transportere IP-pakker. Man kan si at transportnettet består av et fysisk medium og en kommunikasjonsprotokoll som sørger for at det man sender inn på

mediet kommer frem.

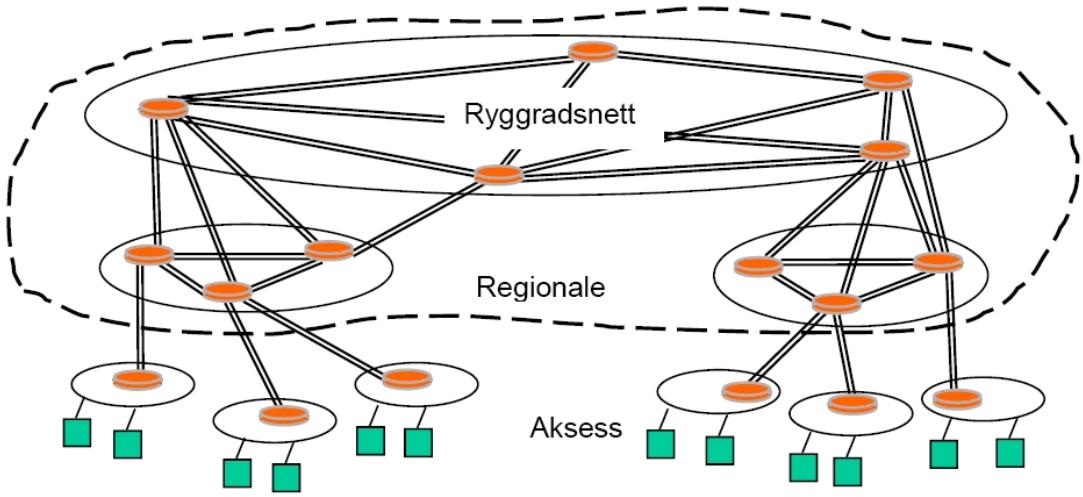
En ISP som drifter sitt eget nett, kan enten leie transportnett eller ha sitt eget. Rundt år 2000 var det ikke mange store ISPer. Da var det vanlig at ISPer leide transportnett av eksempelvis Telenor. Nå har mange ISPer egne fiberkabler som de bruker til å transportere IP-pakker rundt i landet. En leverandør som tilbyr leie av transportlinjer hvor man kan overføre data – enten i form av faste eller svitsjede linjer, kalles en TNP (Transport Network Provider). Eksempler på TNPer er Telenor, UPC, Bredbandsfabrikken, El-Tele og Jernbaneverket/Banetele.

Før Internett ble populært, hadde man en fullt utbygd telenettinfrastuktur i Norge. Denne infrastrukturen bestod hovedsaklig av fiberoptiske kabler som benyttet SDH og ATM til overføring av tale. Når man skulle bygge ut Internett, fant man ut at det ikke var nødvendig å bygge et eget dedikert transportnett; men man ville heller bruke den enorme kapasiteten som fantes på ATM- og SDH-linjene. Dermed ble både tale og Internettrafikk fraktet over det samme transportnettet [20].

2.3.2.1 En ISPs Nett

Små ISPer har kanskje ikke råd til å ha sitt eget transportnett. De kan da leie transportnett av en TNP. I starten var det vanlig å leie kapasitet på en ATM-, Frame Relay- eller SDH-linje. SDH og ATM er telekommunikasjonssystemer laget for å transportere tale – ikke IP-pakker, selv om det finnes løsninger som POS (Packet over SONET/SDH) og ulike tilpasningslag til ATM for å transportere IP-pakker. Dessuten finnes mange av de funksjonene som ATM og SDH tilbyr i andre Internett-protokoller på høyere lag over IP. Derfor har man begynt med andre muligheter for leie av transport. Det vanligste nå er at TNPen legger en fiberkabel mellom de punktene/ruterne som ISPen vil ha transport imellom. Dette gir ISPen to valg. Første mulighet er at den får tilgang til det vi kaller «*mørk fiber*». ISPen må da selv sørge for det elektro-optiske grensesnittet i hver ende for tilkobling av endeutstyr. På denne måten får ISPen muligheten til å utnytte de enorme kapasitetene fiberkabelen tilbyr. Den andre muligheten er at TNPen tilbyr et bølgelengde-multiplekset grensesnittet til ruterne. ISPen abonnerer da på en viss kapasitet og får tilgang til en liten del av det optiske spekteret som kan sendes gjennom fiberen.

Ofte snakkes det om at ISPer har redundans i nettet sitt. Blir det brudd eller problemer på ett sted, kan trafikken sendes via et annet punkt i nettet. På Internett er slike alternative veier mer logisk enn fysisk adskilte. De alternative fremføringsveiene kan gå over samme fysiske kabel eller i en separat kabel, men da gjerne i samme kabelgrøft. Blir det brudd, er det stor sjanse for at det er brudd i de redundante veiene også. To ISPer kan også bruke den samme ISPen til å sende trafikken videre. Hvis en bedrift ønsker å sikre seg ved å bruke to forskjellige ISPer, må den undersøke at ikke begge ISPene bruker samme fremføringsvei for trafikken sin.



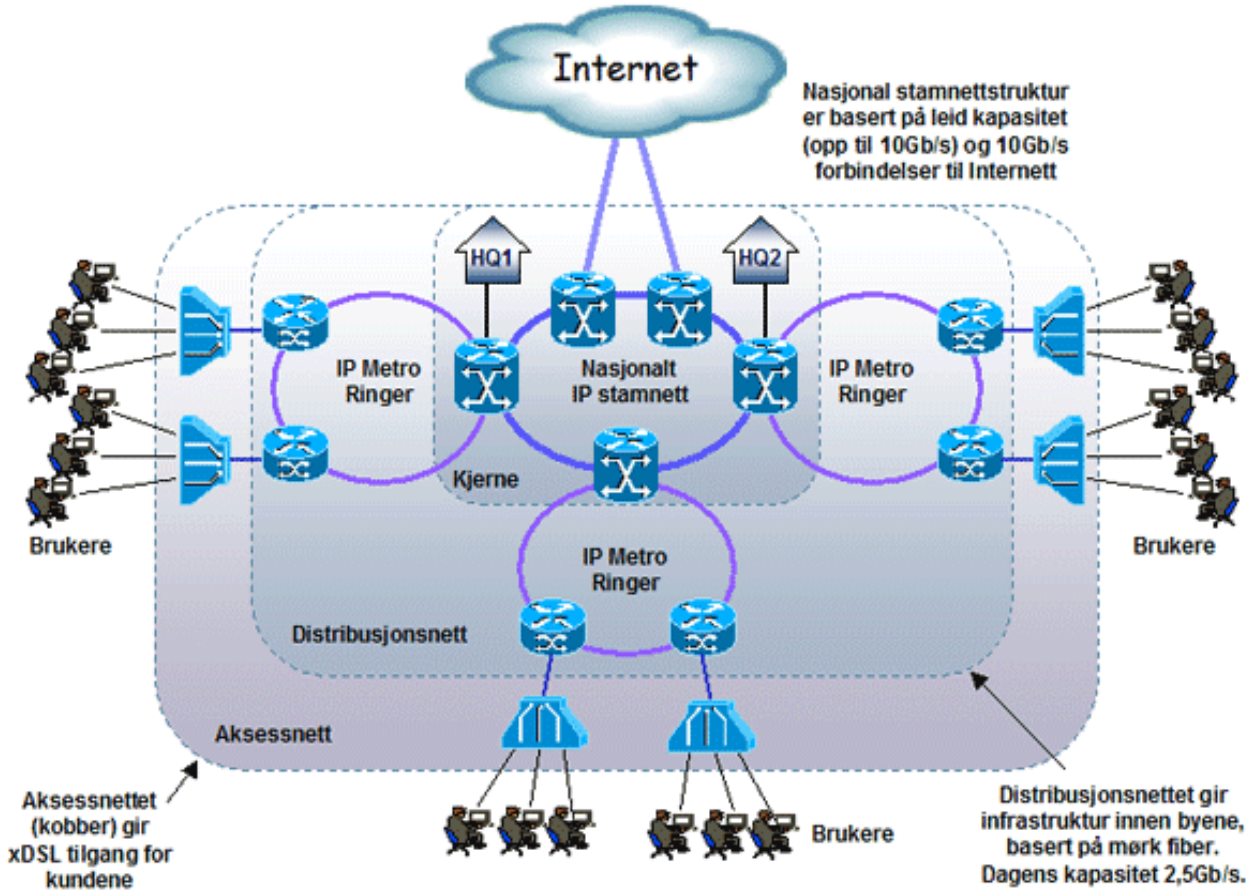
Figur 6: Oppbyggingen av et ISP-nett [20]

Hvordan en ISPs nett er strukturert og hvor omfattende det er oppbygd, avhenger av størrelsen på ISPen og om dekningsområdet er nasjonalt eller internasjonalt. Figur 6 viser hvordan et ISP-nett kan være bygd opp. Som man ser av figuren, er nettet ofte hierarkisk oppbygd med ett ryggradsnett, to eller flere regionale nett og et sett med aksessnett. Tidligere er ordet stamnett nevnt. En ISPs stamnett består av et ryggradsnett og de regionale nettene. En grunntanke er at det mellom to punkter i stamnettet skal være alternative transportveier for datatrafikk. Stamnettet vil kun bestå av noder, da ofte rutere, som enten kan være koblet sammen med egne transportlinjer eller ved å leie av en TNP som tidligere nevnt. Tilkobling av brukerne finnes nederst i hierarkiet; de er tilkoblet aksessnettet. Eksempelvis har Telenor et landsdekkende ryggradsnett med flere regionale nett og aksessnett for tilkobling av brukere [20].

Det er ikke enkelt å få en oversikt over hvordan de ulike ISPene organiserer nettene sine. TDC Song har et eget nordisk fibernett som dekker de største byene [45]. I Norge går dette fibernettet innom Oslo, Kristiansand, Stavanger, Bergen, Trondheim og diverse småbyer mellom de større byene; se Figur 7.

Figur 7: TDC Songs dekningsgrad [45]

NextGenTel har på sine nettsider [52] en liten nettverksoversikt, se Figur 8. Aksessnettet gir xDSL-tilgang til kundene, og baserer seg på kobberkabler mellom kunden og nærmeste telefonsentral. NextGenTel leier disse linjene av Telenor, som er eieren av kobberkablene man bruker til telefoni. Det er Telenor som eier telefonsentralene, og NextGenTel plasserer ut DSLAM-bokser (Digital Subscriber Line Access Multiplexer) som brukes til xDSL. Til dette leier de plass i sentralen. En sentral med DSLAM omtaler NextGenTel som en POP (Point of Presence). Mellom POPene blir det hovedsaklig benyttet leid fiber; da særlig mørk fiber. Distribusjonsnettet innen en by er også basert på mørk fiber, og for å knytte sammen byene, leies det samband med høy kapasitet av Telenor, BaneTele og andre. Kjernenettet eller det nasjonale stamnettet til NextGenTel, benytter seg også av leide høykapasitetslinjer. Tar man hele NextGenTels nettverk under ett, er det basert på IP-teknologi og MPLS.



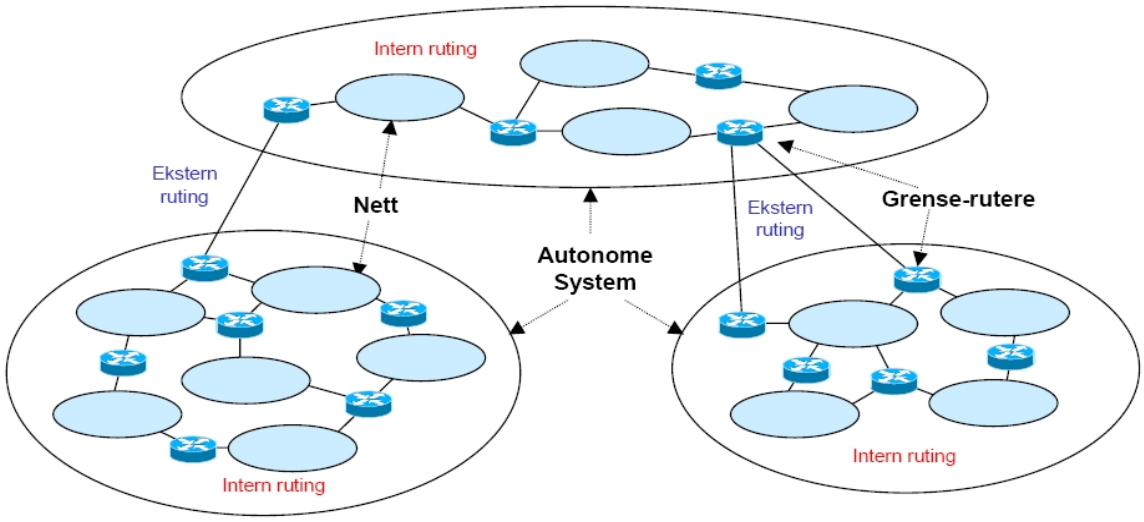
Figur 8: Oversikt over NextGenTels nettverksstruktur [52]

2.3.2.2 Autonome Systemer

For at en pakke skal komme frem på Internett, må ruterne ha rutingtabeller som spesifiserer hvor pakkene skal sendes. Internett blir stadig større, og det fører til større rutingtabeller og mer informasjon som må utveksles mellom ruterne. For å minske dette problemet, har man delt Internett inn i områder som kalles AS, som er en samling av IP-nett og rutere. Disse ASene eies og driftes av offentlige institusjoner, bedrifter og kommersielle operatører som Telenor og andre ISPer. Grunnen til at det kalles AS, er at eieren selv kan bestemme hvordan nettet skal bygges, hvilke kvaliteter nettet tilbyr og hvordan trafikken rutes internt. Man snakker da om to typer ruting: Intradomeneruting, som er vanlig ruting internt i et AS, og interdomeneruting, som er mellom AS. Se forøvrig Figur 9 [22].

Grenserutere eller kantrutere omtales ofte i sammenheng med AS. For at de ulike ASene skal kunne få kontakt med hverandre, må det være ruting mellom ASene. Dette tar kantruterne seg av, og begrepet som brukes er interdomeneruting. Kantruterne er gjerne koblet til flere interne rutere i ASet for å sikre redundans og robusthet [20]. Kantruteren fungerer som en vanlig intern ruter i ASet, men den annonserer også hvilke andre AS som kan nås gjennom ASet den selv er en del av. Internt i et AS rutes det på bakgrunn av IP-adressen som blir satt på pakken av avsenderen. I BGP som er rutingprotokollen for AS-ruting, bruker man ASN (AS-nummeret; en unik identifikasjon for AS på Internett), til rutingen. ASN deles ut av IANA (Internet Assigned Numbers Authority), som

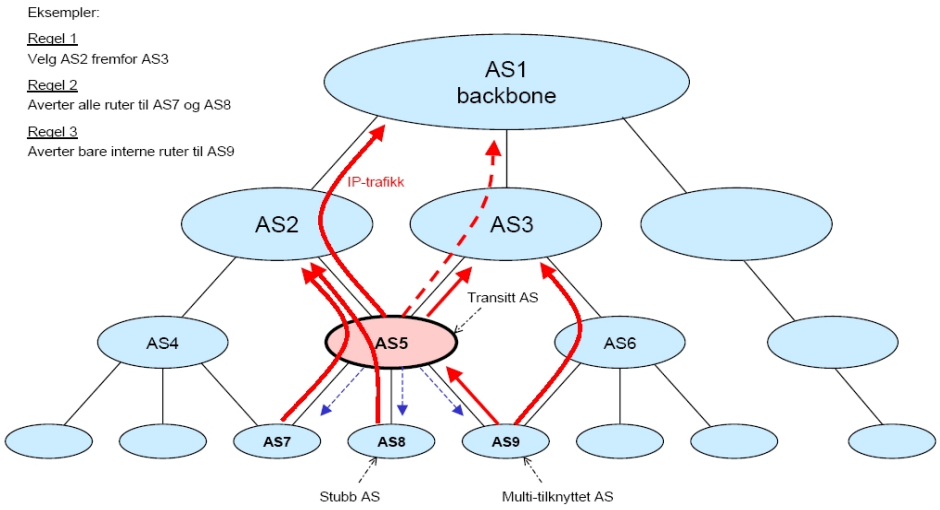
også deler ut IP-adresseområder til regionale Internett-registrarer (RIR) som RIPE NCC (Réseaux IP Européens Network Coordination Centre) og ARIN (American Registry for Internet Numbers) [22].



Figur 9: Ruting i og mellom AS [22]

Det er vanlig å dele inn AS i tre typer. Den første typen AS – et «*stub*», er et AS som kun er tilkoblet et annet AS. Et multitilknytttet («*multihomed*») AS er koblet til mer enn ett AS. Dette er sikrere hvis en tilkobling skulle gå ned eller andre feil skulle oppstå. Det transporterer imidlertid ikke trafikk mellom andre AS. Den tredje typen AS – transitt AS – er også tilkoblet flere AS som det transporterer trafikk mellom. Konseptuelt kan man si at AS A kan nå B gjennom C.

Figur 10 viser hvordan AS er tilkoblet hverandre basert på de tre AS-typene som er beskrevet. På figuren er det også beskrevet regler. Ruting-policy er blitt mer og mer viktig i en kommersiell verden. Her kan man bestemme hva slags trafikk som skal videresendes, hvilke AS som skal annonseres, samt styre trafikken til prioriterte AS [22].



Figur 10: Ulike AS-typer [22]

2.3.2.3 Rutere

Ruterne på Internett kan sammenlignes med telefonsentralene i telenettet. Ruterne finner ut hvor pakkene skal sendes ut ifra en rutingtabell, men de bygger også opp selve tabellen. Dette skjer ved hjelp av en rutingprotokoll. Rutere utveksler informasjon de har om ruter til andre rutere. På denne måten kan man sende en pakke ifra Norge, og den blir rutet riktig frem til USA. Ruterne på Internett kan deles opp i to kategorier; interne og eksterne. Innad i et AS det mange interne rutere som kjører rutingprotokoller som OSPF (Open Shortest Path First), RIP (Routing Information Protocol) og intern BGP. Her rutes pakker rundt basert på destinasjonsadressen. Den andre gruppen av rutere er det vi kaller eksterne. Ofte kalles de grense- eller kantrutere. De eksterne ruterne kjører de vanlige rutingprotokollene for intern ruting i tillegg til ekstern BGP for å annonsere ruter til andre AS. Kantruterne har en svært viktig funksjon på Internett. Skjer det noe galt med en eller flere slike i et AS, kan det få store følger for trafikken – litt avhengig av hvor viktig ASet er [22].

2.3.2.4 DNS

DNS-tjenesten er Internetts system for sammenkobling av domenenavn og IP-adresser. DNS fungerer begge veier; både navn til IP og IP til navn. Den inneholder også kobling mellom epost-servere og deres IP-adresser. DNS er en distribuert database som er spredd utover mange maskiner som blir omtalt som navnetjenere. Man kan kalle DNS for telefonkatalogen på Internett. Uten DNS hadde man ikke kunnet surfe på weben eller sende epost til hverandre uten å ha husket IP-adressene til alle websider og epostadresser man ønsket å benytte. I Norge er det UNINETT Norid som har ansvaret for registrering av .no-domener. Norid har toppnivå-serverne for .no-domener i Norge. For ytterligere informasjon om DNS, henviser vi til avsnitt 2.2.3.5.1 [32], [31].

2.3.3 Samtrafikk

Internett består som tidligere nevnt, av mange AS. Dette er separate nettverk som ofte benytter ulike teknologier. Alle skal kunne snakke med alle – som om man var på samme nettverk. Man må derfor knytte sammen ASene slik at informasjon kan utveksles. Utveksling av trafikk mellom to operatører kan foregå på tre måter: Enten ved at den ene er kunde av den andre, peering-avtaler eller gjennom knutepunkter [3].

2.3.3.1 Peering-avtaler

Når ISPer inngår avtaler, snakker man ofte om to typer avtaler; peering-avtaler eller avtaler om transitt. I begge tilfeller inngår begge partene en avtale eller kontrakt om vilkår og forpliktelser.

I en peering-avtale blir de to ISPene enige om å ha samtrafikk mellom seg og sine kunder. Men trafikk til og fra en tredje ISP – slik som i transittavtaler, er ikke tillatt. Ordet peering brukes egentlig som en kortform-referanse til uttrykket «*Settlement-Free Interconnection*», eller «*fri avtale om sammenkobling*». Dette betyr at ingen av partene betaler den andre for trafikken som blir utvekslet. Normalt er det to like store ISPer som inngår en peering-avtale, men peering-avtaler kan også inngås mellom en stor og en mindre ISP. I såfall må kanskje den mindre ISPen betale en avgift siden den store ISPen ikke får like mye utbytte som den mindre. Tilfeller der det betales en avgift for samtrafikk, kalles gjerne betalt peering.

I motsetning til en peering-avtale, tar en transittavtale seg av videresending av trafikk til og fra en tredje ISP. Den ene parten videreformidler sin egen og den andres trafikk til en tredje ISP. En

transittavtale inngås ofte mellom en liten ISP som vil nå resten av verden og en stor ISP som har nasjonale og globale forbindelser. I transittavtaler er det vanlig å betale avgift til den ISPen som videresender trafikken – enten en fast avgift eller en avgift basert på brukt kapasitet [3].

2.3.3.2 Samtrafikkpunkt

Samtrafikkpunkt eller IX/IXP (Internet eXchange (Point)) er samlingspunktet mellom ulike ISPer hvor det kan utveksles trafikk mellom AS. ISPene har da en avtale om at de kan sende trafikk seg imellom. Samtrafikkpunkter brukes typisk av ISPer til å redusere trafikkmengden på sin egen uplink ved å sende data gjennom andre transittnett. Dette øker effektiviteten og feiltoleransen. En IX er ofte en egen organisasjon som enten skal tjene penger eller som kun krever penger til å dekke utgiftene med samtrafikkpunktet. Normalt har hver IX egne avtaler og vilkår om hvem som får koble seg til og hvor mye dette koster [3].

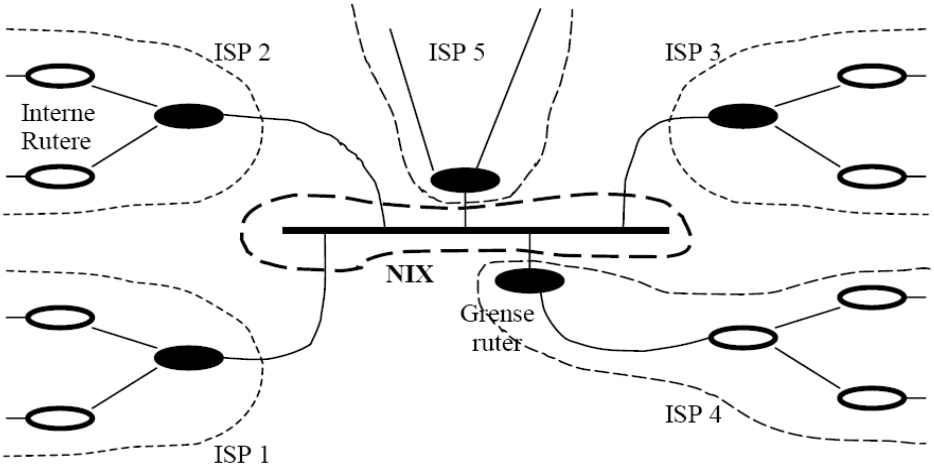
I Norge er det etablert to nøytrale sammenkoblingspunkter for å kunne ha åpen samtrafikk mellom ISPer. Disse punktene kalles NIX 1 og 2 (Norwegian Internet eXchange) og ligger i Oslo. De nasjonale samtrafikkpunktene eies og driftes av Universitetet i Oslo, og ansvarlig operatør er USIT (Universitetets Senter for Informasjonsteknologi). NIX er «*non-profit*», og de eneste avgiftene for en ISP er årlige driftsutgifter og eventuelle etableringsavgifter. Selve utvekslingen av trafikk over NIX er gratis. På NIX er det kun tilknyttet norske ISPer. ISPer som ønsker åpen samtrafikk, kan koble seg til et nøytralt medium – Cisco-svitsjer med 10/100/1000 mbit/s grensesnitt. For ytterligere informasjon om hvilke ISPer som er tilknyttet NIX, se Vedlegg B.

For at en ISP skal kunne koble seg på NIX, er det en del krav som må oppfylles. ISPen må ha fått tildelt et AS-nummer som skal benyttes til peering og annonsert dette minst et annet sted på Internett (utlandet). All ruting på NIX skal skje ved bruk av BGP4. ISPen må bestemme hvilket grensesnitt den vil bruke mot NIX og gi beskjed om hvilke ISPer tilknyttet NIX som ISPen har fått aksept for samtrafikk med.

En ISP kan koble seg til NIX på ulike måter; enten ved å plassere en ruter ved det nøytrale mediet, leie LAN-samband eller «*mørk fiber*» til det nøytrale mediet. Det er kun tillatt å plassere en ruter ved NIX for de som skal ha samband fra NIX til andre steder enn Oslo, eller i de tilfeller i Oslo hvor det er vanskelig å få LAN-samband [46].

Internett i Norge har fått en tilnærmet stjerneformet struktur, se Figur 11. Nesten all trafikken på Internett går innom de nasjonale samlingspunktene i Oslo. Derfor har NIX-punktene en svært viktig funksjon for landets Internett-funksjonalitet [20].

Av andre nasjonale sammenkoblingspunkter, finnes BIX (Bergen Internet eXchange) som har vært i drift i et par år, (3 ISPer tilkoblet) og TRDIX (Trondheim Internet eXchange – 2 ISPer tilkoblet). Sistnevnte har vært i drift siden 2005 [47].



Figur 11: Stjerneform på Internett i Norge [20]

2.4 Sikkerhet og sårbarhet

2.4.1 Introduksjon til datasikkerhet: Konfidensialitet, integritet og tilgjengelighet

Datasikkerhet hviler på konfidensialitet, integritet og tilgjengelighet, selv om tolkningen av disse aspektene varierer med sammenheng og behov. Vi skal nå gi en kort innføring i disse begrepene. For en mer omfattende beskrivelse henvises det til [4].

Konfidensialitet innebærer hemmeligholdelse av informasjon eller ressurser. Slike behov forekommer ofte når man benytter datamaskiner i industrien og hos myndighetene. Militære og sivile myndigheter har for eksempel som praksis at tilgang til informasjon er begrenset til dem som trenger og har rett til den aktuelle informasjonen. Mekanismer for aksesskontroll støtter konfidensialitet. Kryptografi og systemavhengige mekanismer er begge eksempler på metoder for å forhindre at uvedkommende får tilgang til informasjon. Noen ganger kan det å vite at en gitt type informasjon eksisterer, være et problem. Enkelte systemer har derfor også evnen til å skjule informasjonens eksistens. Fordi alle mekanismer på ett eller flere punkter gjør antakelser, er konklusjonen at antakelser og tillit utgjør grunnlaget for disse mekanismene.

Integritet refererer til påliteligheten til data eller ressurser, og omhandler vanligvis forhindring av feilaktige eller uautoriserte endringer. Integritet inkluderer dataintegritet, som omfatter innholdet i dataene, og opphavsintegritet, som tar for seg dataenes kilde. Sistnevnte blir ofte kalt autentisering. Mekanismene for integritet deles inn i to klasser: Motvirkning og deteksjon. Motvirkning kan videre deles inn i blokkering av uautoriserte forsøk på å endre data og forsøk på å endre data på uautoriserte måter. Førstnevnte sikter til eksterne angrep, mens sistnevnte omhandler autoriserte brukeres forsøk på å endre data på en ulovlig måte. Det å forhindre eksterne angrep er annerledes fra og mye mer trivielt enn å motvirke at autoriserte brukere foretar seg uautoriserte handlinger. La oss se på tilfellet med en bankansatt som har autorisasjon til å utføre pengetransaksjoner. Det er prinsipielt sett svært annerledes å designe mekanismer som beskytter mot angrep utenfra enn å forhindre den ansatte i å overføre bankens penger til sin egen konto i Sveits. På ett eller annet punkt må designeren av systemet gjøre antakelser i forhold til tilliten til den ansatte.

Deteksjonsmekanismer tar kun sikte på å rapportere integritetsbrudd. Slike mekanismer inkluderer

analyse av hendelser i systemet, samt analyse av innholdet i selve dataene. Evaluering av integritet er ofte vanskelig, da integriteten hviler på antakelser om dataenes kilde og tilliten til den kilden. Dette inkluderer dataenes korrekthet og pålitelighet, hvordan og fra hvem dataene ble mottatt, hvor godt dataene ble beskyttet før mottak, samt hvor godt dataene er beskyttet på gjeldende datamaskin.

Tilgjengelighet omfatter evnen til å gjøre bruk av den ønskede informasjonen eller ressursen. Tilgjengelighet er et viktig aspekt av såvel pålitelighet som systemdesign, da et utilgjengelig system er minst like ille som det å ikke ha noe system i det hele tatt. Den delen av tilgjengelighet som er relevant i forhold til sikkerhet, har å gjøre med tilsiktede handlinger for å gjøre data eller tjenester utilgjengelige. Systemdesign er vanligvis bygd på en statistisk modell for å analysere forventede bruksmønstre, og mekanismene garanterer tilgjengelighet så lenge den statistiske modellen holder vann. Dersom noen klarer å manipulere bruksmønstrene eller parametrene som kontrollerer bruken (for eksempel nettverkstrafikken), vil ikke antakelsene bak den statistiske modellen være gyldige lenger. Resultatet er ofte at tilgjengelighets-mekanismene feiler når de tvinges til å arbeide under omstendigheter de ikke var tiltenkt.

Forsøk på å blokkere tilgjengeligheten – kalt tjenestenekt-angrep – kan være svært vanskelige å detektere, fordi en analyse må finne ut hvorvidt de uvanlige bruksmønstrene kommer av miljømessige eller tilsiktede endringer. Vi har valgt å ta med et dypdykk i DDoS fordi det ikke bare rammer brukere i aksessnettet, men også til en viss grad stjeler kapasiteten til stamnettet og utgjør en potensiell fare for alle enkeltnoder i infrastrukturen.

2.4.2 Distribuert Denial of Service

2.4.2.1 Introduksjon

DoS-angrep, eller tjenestenekt-angrep, er en velkjent og utprøvd metode for å tvinge ned en tjeneste på IP-nett. DoS innebærer at en angriper oversvømmer et offer med unyttige data i et forsøk på å stenge ute legitime brukere av tjenesten. DDoS er når en samling angripere oversvømmer en tjeneste på den samme måten. I de senere årene har det vist seg at sikkerheten er så dårlig hos mange private Internett-brukere at det er lekende lett for en inntrenger å overta kontrollen over datamaskinen. Resultatet er at en angriper nå kan inneha kontrollen over en stor samling med slike «*tinnsoldater*» som går til angrep på bakmannens ordre. Et slikt nett kalles gjerne et bot-nett, og fjernstyres gjerne ved hjelp av IRC (Internet Relay Chat).

Senere tiders angrep har også hatt økonomisk formål, da bedrifter i en del tilfeller har betalt en bakmann for å angripe en konkurrerende bedrifts nettsider og forårsake store økonomiske tap. Mafiaen har også brukt lignende metoder for å tvinge særlig mellomstore bedrifter til å betale for å unngå angrep. Store pengesummer går tapt for hvert minutt en nettside er utilgjengelig, og dette kan forklare hvorfor en del bedrifter har gått med på å betale seg unna hele problemet.

Teknisk sett er det mye TCP-angrep som benyttes; da særlig mot webservere. TCP-forbindelser settes opp med treveis handshake, og siden angriperen gjerne forfalsker avsenderens adresse, har ikke angripende maskiner anledning til å være med lenger enn første runde. I første runde sendes en enkel pakke med SYN-flagget satt i headeren, noe som har bidratt til å gi denne typen angrep tilnavnet SYN-flooding. Angrep kan utføres på en hvilken som helst måte (TCP, UDP, ICMP), men dersom man ønsker å ramme tjenester på innsiden av brannmuren og ikke bare selve opplinken til offeret, benytter man gjerne TCP/SYN-flooding.

2.4.2.2 Hvorfor problemet ikke lar seg løse på en enkel måte

Det enkleste ville selvsagt vært og stengt ute all ondsinnet trafikk, men da må man klare å skille slik trafikk fra andre data. Mange metoder har blitt utviklet, og det pågår fremdeles forskning for å forbedre og utvikle slike metoder. Man kan eksempelvis abonnere på automatiske oppdateringer av angrepssignaturer, slik at brannmuren og IDS/IPS-løsningen (Intrusion Prevention System) til enhver tid er oppdatert.

Verre er det imidlertid at man selv med en perfekt metode for sortering av ondsinnet trafikk i de fleste tilfeller likevel vil ha store problemer under et DDoS-angrep. Forklaringen ligger i det faktum at selve Internett-forbindelsen ikke har ubegrenset båndbredde. Dersom et angrep stammer fra 10.000 ADSL-klienter med en samlet opplastingshastighet på 1.280 mbit/s (128 kbit/s * 10.000), vil det ta ned nærmest en hvilken som helst tjeneste her i landet. Et stort bot-nett kan i internasjonal sammenheng bestå av mer enn 30.000 klienter, og disse har ofte mer enn 128 kbit/s hver i opplastingshastighet. Eksempelvis får man nå 512 kbit/s opplastingshastighet på de fleste ADSL-pakkene, opptil 10 mbit/s over kabel-tv og opptil 100 mbit/s i enkelte tett befolkede områder.

2.4.2.3 Løsninger og pågående forskning

Det pågår en god del forskning rundt hvordan man skal ta det onde ved roten. Problemet er at når den ondsinnede trafikken kommer fra så mange kanter samtidig, er det vanskelig å skille legitime og ondsinnede brukere på mottakersiden. I tillegg tar det ofte for lang tid å konkludere med at en tjeneste eller bedrift er under angrep. En god del bedrifter har ingen varslingssystemer for slike angrep, og vet følgelig ikke om situasjonen før en eller annen tilfeldig bruker melder ifra om at tjenesten er utilgjengelig.

Som for å gjøre det hele fullkomment, er det slik at en del Internett-leverandører har spesifisert i avtalen at de uten forvarsel kan stenge ned Internett-forbindelsen dersom trafikken overstiger en viss grense. Man kan med andre ord bli straffet for å være under angrep.

En av taktikkene for å bekjempe slike angrep, er å begrense trafikken innover i nettet. Dette fungerer både ved for mye legitim og uønsket trafikk. Mahajan et al ved AT&T Research Labs har utviklet en metode kalt «*Aggregate-based Congestion Control*» [15]. Denne metoden grupperer trafikken ut ifra hvilke kjennetegn pakkene har, og søker å identifisere typene strømmer. Dersom algoritmen ved oversvømmelse finner at for eksempel TCP/SYN-pakker holder høyest nivå, vil den begrense mengden slike pakker først. Dersom dette ikke er nok, vil den ta for seg resten av rekken etter tur. En annen metode går ut på at den oversvømte ruteren sender en pushback-melding til overordnede rutere, som begynner å strupe ned spesifisert trafikk. Dermed vil oversvømmelsen behandles lengre inn i nettet, hvor kapasiteten er større.

En metode går ut på at den siste ruteren før kundens nett begrenser all innkommende trafikk til det høyeste nivået som kundelinken kan klare. Dette er meningsfylt uansett om den innkommende trafikken er legitim eller ikke, siden pakkene vil bli kastet uansett. På denne måten kan ISPen forhindre at kundens forbindelse overbelastes utenfra – uansett hva årsaken måtte være.

For samfunnskritiske tjenester har Keromytis et al definert en arkitektur ved navn «*Secure Overlay Services*» [12], som tar sikte på å bygge et virtuelt nettverk over Internett beregnet på samfunnskritiske tjenester. Bakgrunnen for problemstillingen er den stadige utflyttingen av nødnetts-, infrastruktur- og lignende tjenester på det offentlige Internett. Dette innebærer i tillegg til de vanlige problemstillingene rundt konfidensialitet, at slike noder utsettes for

oversvømmelsesrisikoen som resten av nettet har problemer med. Ideen er at all trafikk som skal aksessere samfunnskritiske noder fra det vanlige Internett, først må verifiseres i kjernenettet hvor kapasiteten til å håndtere oversvømmelser er stor. Dette gjøres ved å utplassere såkalte gates som videresender all trafikken som skal til kritiske deler av nettet.

DPF (Distributed Packet Filtering) er et initiativ i retning av å kaste alle pakker med ugyldig avsender. IP-protokollen tillater slike pakker å flyte fritt i nettet, men med en oppgradering av kantrutere mellom de forskjellige leverandørene, kan dette bremses ned effektivt. Ruteren blir pålagt å inspisere trafikken på pakkenivå og sjekke at avsenderadressen er gyldig før videresending tillates. I motsatt fall kastes pakken umiddelbart. Route-based DPF [16] går ut på å innføre dette på kantruterne mellom de store ASene. I tillegg bemerkes det at man med fordel kan implementere slike metoder også på lavere nivå, som eksempelvis innen nettet til hver enkelt leverandør. Selv om et slikt initiativ kan ta tid å gjennomføre, vil selv en grovfiltrering på høyt nivå gjøre det mye vanskeligere for angripende datamaskiner å skjule sine adresser.

2.4.3 Sikkerhet og sårbarhet på lagene i TCP/IP-stakken

De fire laveste lagene i TCP/IP-stakken er det vanskelig å si noe generelt om, da valgt protokoll i stor grad bestemmer sikkerheten og sårbarheten. Vi nevner eksempler på noen slike sårbarheter:

- For ordens skyld: Fysisk lag i TCP/IP-stakken har ikke med sprengning av broer, graving med gravemaskin og sprengning av serverskap å gjøre. Sikkerhet og sårbarhet på fysisk lag omfatter kun alt innen kabling og signalforstyrrelser.
- På linklaget snakker man om rettede angrep mot ARP/RARP-protokollen og endring av rammestørrelser (Ethernet-protokollen) for å fremprovosere feil i nettverket.
- Nettverkslaget inneholder flere muligheter for ondsinnet aktivitet. Eksempler på dette er å forfalske avsender-adressen, samt å oversvømme offeret med ICMP-pakker. ICMP-protokollen brukes også til sporing av nettverksenheter (traceroute) og til sniffing etter aktive verter (ping).
- Ved angrep mot tjenester og servere stiller transportlaget i en egen klasse. Blant de mest brukte taktikkene, finner man portskanning, SYN-flooding (TCP) og UDP-flooding (de klassiske tjenestenekt-angrepene).

På applikasjonslaget er det et utall med muligheter – så vel proprietære, lukkede som åpne og standardiserte protokoller. Alle disse kan ha hittil uoppdagede svakheter, i tillegg til programmeringsfeil og sårbarheter i de enkelte applikasjonene som benytter protokollene. Svært mange av sikkerhetshullene som oppdages, har målskive nettopp på dette laget. Dette inkluderer:

- Webservere (som Internet Information Server og Apache)
- Epost-programvare (som Outlook og Thunderbird)
- System-tjenester for deling av filer (som Windows fil- og printerdeling)
- Programvare for filoverføring (FTP- og SSH-programmer)
- Autentiseringstjenester (som «*Windows Network Logon*»)
- Trivielle protokoller som DHCP (Dynamic Host Configuration Protocol) (Eksempel: Blaster-viruset benyttet blant annet ServiceHost-tjenesten i Windows for å trenge seg inn på datamaskinen. Denne tjenesten tar seg blant annet av DHCP-forespørsler.)
- BGP-protokollen

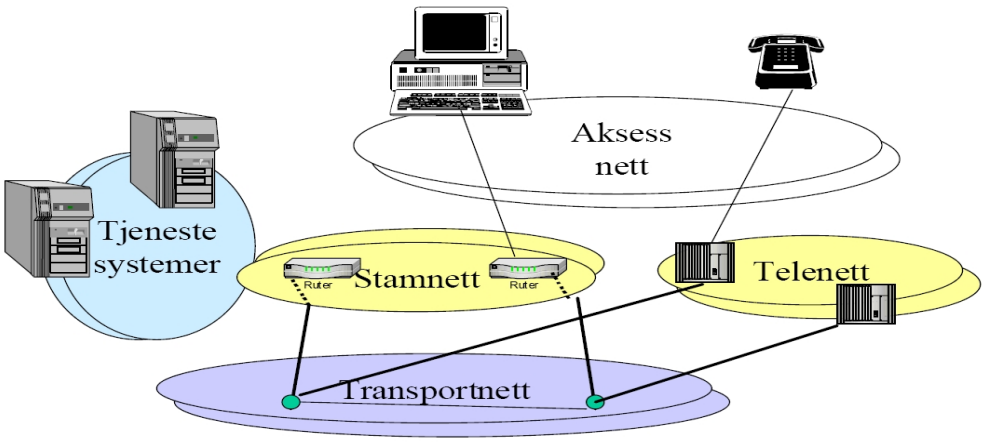
BGP-protokollen styrer all trafikken mellom ASene på Internett. Det er ingen beskyttelse av dataene

som overføres. Ruteformidlingen inneholder ingen autentisering, og dermed kan man verken vite hvor den kommer fra eller om den er endret underveis. Det antas at et ondsinnet AS kan få til et angrep med alvorlige konsekvenser [19].

Applikasjoner som utvikles kan bli utsatt for slurvete arbeid. Men selv om slurv ikke var til stede under utviklingen, er det likevel bortimot umulig å sikre en applikasjon mot alle typer feil og svakheter. Det medfører at man hele tiden må være på vakt overfor angrep mot programvaren, og at det i mange tilfeller er nødvendig å spre feilrettinger og programvare-oppdateringer til brukerne av applikasjonen. Likevel vil det alltid være et moment av usikkerhet til stede, for man kan ikke vite med hundre prosent sikkerhet om en sofistikert inntrenger har klart å skjule sin tilstedeværelse samtidig som vedkommende har klart å utnytte et hittil ukjent sikkerhetshull i programvaren.

2.4.4 Sårbarhet relatert til Internett

Scandpower-rapporten har tatt utgangspunkt i Figur 12 og sett på sårbarhetene knyttet til aksessnett, transportnett, stamnett og tjenestesystemer. Alle disse elementene er i større eller mindre grad sårbare for tekniske feil, uhell, kabelbrudd, sabotasje og cracker-virksomhet (populært kalt «*hacking*»). Vi vil ta for oss sårbarhetene til de ulike komponentene på Internett i Norge slik som Scandpower har beskrevet dem – det vil si aksessnettet, transportnettet, stamnettet, DNS og NIX [20].



Figur 12: Sårbarheter i forhold til komponenter på Internett [20]

2.4.4.1 Aksessnett

Det finnes flere ulike aksessnett og tilbydere av aksessnettjenester (NAPer). For en privatkunde er ofte aksessnettet til Internett det samme som for vanlig telefoni. Det vil si at man har et stjerneformet aksessnett (en vei til/fra hver enkelt bruker). Blir det brudd på denne kabelen eller det skjer andre uønskede hendelser, vil det som oftest kun ramme en enkelt kunde. Hvilke konsekvenser dette får, er avhengig av hva slags tjenester kunden gjør bruk av.

Ser man på vanlige kabelbaserte aksessnett, er det gravearbeid som er den største årsaken til brudd. Det skjer ofte at en gravemaskin får med seg et par fiberkabler i grabben. Andre trusler er hærverk og sabotasje. Radiobaserte aksessnett har ikke fysiske kabler som kan bli ødelagt, men de kan få problemer med radiostøy, enten i form av tilfeldige støykilder eller bevisst jamming. Alle med litt

innsikt i radioverdenen, kan fange opp radiosignaler og lese innholdet. Siden radiobaserte aksessnett er mer utsatt for avlytting enn kabelbaserte, er det nødvendig å sikre radiosambandet med sikkerhetsmekanismer.

Ser man på redundans og sikkerhet, vil det for private kunder ikke være aktuelt med flere aksesslinjer. Større bedrifter har ofte flere leverandører for å ha redundans og øke robustheten til Internett-tilknytningen.

2.4.4.2 Transportnett

På samme måte som med aksessnettet, finnes det flere transportnett. Telenor er ennå den største leverandøren med et landsdekkende transportnett. Hvor stort omfang brudd i transportnettet gir, avhenger av hvor skaden har skjedd. Blir det brudd på et sentralt punkt hvor det går mye trafikk, kan det få store konsekvenser. Ofte deler man opp i landsomfattende, regionale og lokale konsekvenser. Dette er avhengig av robustheten i transportnettet.

Trafikken på Internett er annerledes enn i det vanlige telenettet. I telenettet er det mye trafikk mellom kunder på lokalt og regionalt nivå. Blir det brudd i telenettet og en region blir avskåret fra resten, kan kundene fremdeles få kontakt med hverandre i den samme regionen dersom de tilhører samme teleselskap. På Internett er det ikke mange lokale forbindelser mellom kunder. Andelen langdistansetrafikk er mye større. Derfor vil brudd i transportnettet føre til at store områder blir uten Internettforbindelse.

Siden Internett i Norge i stor grad baser seg på at all trafikk mellom ISPer skal innom NIX, vil man ikke få lokal eller regional autonomi (som i telenettet) dersom det skulle bli brudd i transportnettet.

Ser man på robustheten og redundansen i transportnettet, er det slik at TNPer ikke bygger ut kapasiteten før de trenger den. De tenker lite på mer overordnede interesser som nasjonal robusthet og befolkningens tillit til informasjonssamfunnet. Redundansen i transportnettet er i mange tilfeller ikke helt bra. Ofte blir det lagt ut nye fiberkabler i samme kabelgrøft som den gamle for å sikre redundans og alternative fremføringsveier. Skjer det et graveuhell, er det liten nytte i en kabel som ligger ved siden av den kabelen den var ment å være backup for.

I de tilfeller hvor transportnettet er basert på teleteknologi (separate nett for drifts- og signaleringsdata), er det ikke stor fare for logiske angrep – bortsett fra den overføringskapasiteten angrepet legger beslag på.

2.4.4.3 Stamnett

Tidligere er det nevnt at Internett er en sammenkobling av flere AS; det vil si ISPer med sine stamnett. I Norge er de fleste ASene koblet sammen i de nasjonale samlingspunktene NIX 1 og 2 i tillegg til en utenlandsforbindelse. Svikt i stamnettet kan få større konsekvenser enn i aksessnettet. Det verste som kan skje, er at alle kundene til ISPen blir berørt og at eventuelle tjenester ISPen tilbyr, blir utilgjengelige.

I stamnettet går drifts- og signaleringsdata i det samme nettet som brukerdataene. Muligheten for logiske angrep er derfor større enn i aksess- og transportnettet. Grunner til svikt i stamnettet, kan være logiske anslag, feil eller ondsinnede driftsfunksjoner, svikt i utstyr og strømforsyninger eller andre påvirkninger fra omgivelsene. Beskyttelse mot ondsinnet bruk av driftsfunksjoner er det

normalt beskyttelse for i ruterne, samt utveksling av rutinginformasjon mellom ruterne. I verste fall kan slike angrep sette hele stamnettet ut av drift.

Den siste tiden har det blitt vanligere å sende kunstig trafikk mot et sted i nettet slik at denne trafikken tar opp all kapasiteten. Dermed blir fremkommeligheten redusert eller helt blokkert. Dette kalles tjenestenekt. Ved distribuert tjenestenekt blir det sendt data fra mange steder mot det samme målet. Dette kan føre til metning i nettet og at den aktuelle tjenesten blir utilgjengelig. Til nå har det vært vanligere at tjenester blir utilgjengelige enn at kapasiteten i stamnettet blir brukt opp.

Skal man gardere seg mot angrep i stamnettet, kan det gjøres ved fysisk og logisk sikring av noder og protokoller. Mange protokoller inneholder svakheter – for ikke å nevne protokollene med totalt fravær av sikkerhetsmekanismer. Et skremmende scenario er at en hacker med god innsikt i en ISPs nett skal få tilgang til en ruter for så å plante et virus som sprer seg fra ruter til ruter inntil ISPen er ute av drift.

2.4.4.4 DNS og NIX

Hvis DNS-tjenesten skulle gå ned, vil det ikke være mulig å surfe, sende epost og bruke IP-telefoni. Et DDoS-angrep kan gjøre DNS-tjenesten utilgjengelig. DNSSEC (DNS Security Extensions) legger til sikkerhetsmekanismer i DNS-tjenesten, men hjelper ikke mot tjenestenekt [47]. En kjent angrepsteknikk mot DNS-tjenesten er «*cache poisoning*». DNS-serveren blir lurt til å tro at den har mottatt autentisk informasjon. DNS-informasjon som mottas, blir typisk «*cachet*» en stund på serveren, og dermed blir feil informasjon spredt rundt til brukerne av nettopp den DNS-serveren [4].

Hvis NIX-punktene blir utsatt for fysiske angrep, kan det få store følger for Internett i Norge, da nesten all trafikken kommer innom der. Feil og angrep kan skje på selve NIX-punktene, men også på transportnettet. Det har vært eksempler på at brudd på en fiberkabel mellom NIX og en ISPs ruter noen hundre meter fra NIX har ført til at all nasjonal trafikk knyttet til denne ISPen har stoppet opp [20].

3 Relevant arbeid innen CIIP

Når man skal lage modeller og fremgangsmåter for sikkerhet og sårbarhet i IP-basert infrastruktur, er en viktig del av arbeidet å se på det som allerede er gjort på fagområdet. Vi vil ta for oss arbeid og metoder som vi synes er viktig bakgrunn for vårt arbeid.

3.1 BITBREUK – «In Bits And Pieces»

Følgende er hentet fra BITBREUK-rapporten – oversatt til engelsk versjon: «*In Bits And Pieces*» [9].

3.1.1 Introduksjon

Forsvaret i Nederland skrev i et whitepaper i 2000: *«However, given the Armed Forces' high level of dependence on information and communication technology, it cannot be ruled out that in the future, attempts will be made to target the Armed Forces in precisely this area.»* Denne påstanden og lignende problemstillinger innen andre sektorer i samfunnet satt igang en prosess på høyt nivå i Nederland. Aktører fra flere samfunnslag – både innen offentlig og privat sektor – begynte å samles for å samtale om de nye problemstillingene. TNO (Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek) ble utnevnt til å studere disse sammenhengene nærmere og lage et paper som utgangspunkt for de videre samtalene.

Man begynte med å stille spørsmål om hvorvidt slike svakheter faktisk eksisterte, og hva som ville skje dersom ulike skrekkscenarier skulle inntreffe. Deretter begynte man å forestille seg hvordan en opprydningsaksjon ville ta seg ut og hvilke parter som måtte involveres for å få samfunnet på beina igjen. Underveis oppdaget man at det kanskje ikke var nok med en større nasjonal innsats, men at man muligens måtte samarbeide med internasjonale myndigheter og kommersielle aktører for å få systemene fullstendig tilbake i drift igjen. Internetts multinasjonale og sammensatte struktur respekterer ikke landegrenser, og informasjons-infrastrukturer burde derfor behandles globalt analogt med politiets innsats mot kriminalitet.

I de videre studiene ble det også kartlagt kryssavhengighet mellom kritiske infrastrukturer og samfunnsaktører. Et skremmende eksempel på dette ble presentert i «*Strømløs*»-rapporten [21]; hvor det ble sagt om strømbrudd at *«After eight hours, disruption of society as a whole can assume disastrous proportions, especially if the disruption affects a large area and there are signs that it will last for more than 24 hours.»*.

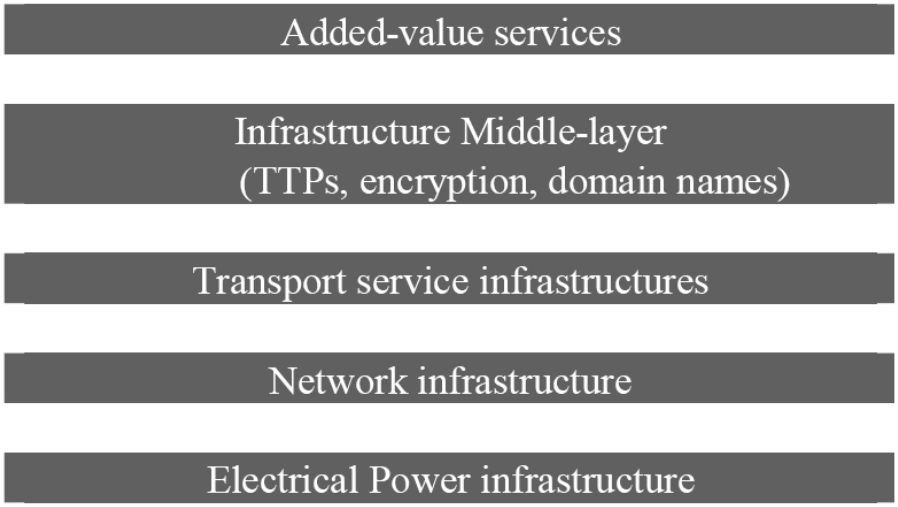
3.1.2 Definisjoner

I forbindelse med samarbeidet med aktører med liten innsikt i sikkerhetsmessige og teknologiske begreper og mekanismer, trengte man forenklede definisjoner av essensielle begreper. Innen sikkerhet er det sentralt med tilgjengelighet, integritet og konfidensialitet. I tillegg er sårbarhet essensielt for infrastrukturer. Tilgjengelighet ble definert som *«the extent to which an information system is functioning at the moment the organisation needs it».* Integritet ble *«the extent to which an information system is error-free»*. Definisjonen av konfidensialitet ble *«the extent to which access to, and consultation of, an information system and the information contained therein is restricted to a specified group of authorised persons or processes running on their behalf»*. Sårbarhet ble definert som *«the effects of the manifestation of threats on the functioning of an information system or an area of responsibility»*.

I tillegg fant man det hensiktsmessig å utdype tilgjengelighet med begrepet overlevelsesdyktighet: *«Survivability is a measure of the extent to which availability can be re-established in extreme circumstances (serious disruptions).»*.

3.1.3 BITBREUK-modellen

År-2000-problemet demonstrerte for nederlenderne det moderne samfunnets akutte avhengighet av og svært begrensede innsikt i IKT og underliggende infrastrukturer. For å få en helhetlig forståelse av alle former for elektroniske informasjons- og transmisjons-infrastrukturer, ble det laget et forslag til lagdeling i form av en grovskisse med følgende innhold (se Figur 13).



Figur 13: Lagene i BITBREUK-modellen [9]

Det mest grunnleggende i denne lagdelingen, er den elektriske strømforsyningen, som utgjør grunnlaget for all IKT. På nivået over finner vi alle nettverks-infrastrukturer som for eksempel telekom-utstyr, fibre- og andre kabler, radio- og TV-sendere, satellitter og de lokale aksessnettene. Slikt utstyr benytter seg i tillegg av IKT-komponenter og programvare til overvåking og styring.

På neste lag finner vi transmisjonstjenester av forskjellige slag: Telefoni, faks, Internett-transmisjon og -ruting og distribusjon av TV- og radio-signaler. Slike tjenester tilbys av forskjellige leverandører som i mange tilfeller benytter den samme nettverks-infrastrukturen. Laget over er ikke fullt så lett å gjenkjenne, men tilbyr alt av teknologiske sammenknytninger som trengs for å gjøre bruk av mer avanserte tjenester. Dette mellom-laget inneholder for eksempel TTPer (Tiltrodd Tredje-Part), DNSer, SMS-tjenester (Short Message Service), Internett-servere, lokasjonsinformasjon til lokasjonsbaserte tjenester og så videre.

Verdiskapende tjenester inkluderer eHandel, statlige 24-timers informasjonstjenester, automatisert innsamling av skatt, automatisert prosessering av lisenser og lignende. I de følgende avsnittene blir disse lagene behandlet i mer detaljert form.

3.1.3.1 Network infrastructure layer

Dette laget håndterer transporten av bits og består følgelig av elementære nettverksprotokoller og

-komponenter. Luiijf og Klaver har nevnt følgende eksempler:

- Aksessnettene: Det leddet som kobler forbrukere og operatører sammen. Består oftest av kobberkabler, CATV-kabler (Cable TV), fiberkabler eller mikrobølge-forbindelser.
- Bunter med glassfiber og i enkelte tilfeller svitsje-utstyr tilhørende aktører med enerett på slikt utstyr – som eksempelvis NS (Nederlands jernbaner) og forsvarsdepartementet.
- Nasjonale transportnettverk og svitsjing-/routing-laget til telekom-operatørene – som KPNs (Koninklijke KPN N.V.) (Universal Transport Network (tilsvarende Telenors transportnett i Norge).
- Infrastruktur i tilknytning til basestasjoner for mobilkommunikasjon.
- Internasjonale og transkontinentale transmisjons-infrastrukturer for bakkenett (som PTAT)
- Radio- og TV-sendere; opplink ifra studio til sendemast
- Satellitt-kommunikasjon; opplinks- og nedlinks-fasiliteter (Eutelsat, Inmarsat, lavbane-satellitter – LEO (Low Earth Orbit)).
- Infrastruktur knyttet til satellittnavigasjon

3.1.3.2 Transmission service infrastructures

Følgende er eksempler på transmisjonstjenester:

- Datatjenester som faks, Internett og annen datatrafikk over modem, ISDN, ADSL, X.25, leide linjer og mørk fiber (leide fibersamband).
- Mobile datatjenester over oppringt samband (9600 bps), GPRS, UMTS. SMS hører også hjemme her.
- Radio- og TV-frekvenser som samtidig benyttes til informasjonstjenester (tekst-TV med aksjekurser og lignende)
- Tetra/C2000 og personsøkere som benytter en separat infrastruktur til transmisjon
- Sammenknytninger av ryggradsnettet til Internett ved at ISPer benytter nettverks-infrastrukturer

3.1.3.3 Information infrastructure middle-layer

Dette laget gjør bruk av transmisjonstjenestene på forrige lag og inkluderer:

- Domenetjenester
- TTP-tjenester for eHandel
- TTP-tjenester for sikker epost mellom myndighetenes avdelinger (Nederlands Utenriksdepartement, 1999)
- Transparente gateway-tjenester mellom diverse nasjonale og internasjonale infrastrukturer
- Store-and-forward -tjenester for meldinger (epost, voicemail, SMS)
- Sikker datakommunikasjon (konfidensialitet og integritet) for sikre finansielle transaksjoner
- VPN (Virtuelle Private Nettverk) tilhørende organisasjoner
- Infrastrukturen for elektroniske pengeoverføringer (kortlesere og minibanker)
- Alarmtjenester (for eksempel tyveri- og brannalarmer)
- GPS-tjenester (Global Positioning System) som forsyner mobile enheter med nøyaktig posisjon og tidspunkt

3.1.3.4 Added-value services infrastructure

Et fungerende mellomlag gir muligheter for mer avanserte verdiskapende tjenester som eHandel, automatisert innsamling av skatt, automatisert prosessering av transportlisenser, informasjonstjenester basert på lokasjonsinformasjon og Internett-tjenester.

3.1.3.5 Horisontale informasjonsflyter

Under studiene av verdiskapende tjenester fant nederlenderne ut at tjenestene i tillegg til å være fullstendig avhengige av underliggende nettverksfunksjonalitet, også var avhengige av horisontale informasjonsflyter. Dette innebærer at informasjonstjenester ofte må betraktes som en del av en informasjonskjede mellom bedrifter, organisasjoner, myndigheter, samfunnet generelt og private brukere.

Telekom-tjenester, distribusjon av elektrisk kraft, elektroniske betalingstjenester, distribusjon av drikkevann, nødtjenestene, mediene og transportsektoren er alle eksempler på vitale tjenester som i dagens samfunn hviler på IKT-løsninger. De fleste av disse løsningene er videre helt avhengige av ulike kombinasjoner av horisontale (samme lag) og vertikale (underliggende lag) infrastrukturer. På dette grunnlaget definerer BITBREUK «*vitale infrastruktur-kjeder*».

Erfaringene fra år-2000-problematikken viste nederlenderne at deres egne kunnskaper omkring denne komplekse sammenhengen av kjeder var dårlige. Avbrudd i en infrastruktur kan føre til uforutsette dominoeffekter hvor også andre infrastrukturer rammes. Det å håndtere slike problemer krever en klar forståelse av kryssavhengighetene, samt en effektiv og gjennomtenkt handlingsplan. En ytterligere kompliserende faktor er det at kryssavhengighetene i noen tilfeller krysser landegrenser.

3.1.4 IKT-infrastrukturenes kjede-sårbarheter og -avhengigheter

BITBREUK tok videre for seg sårbarhetene og avhengighetene på de forskjellige lagene i detalj.

3.1.4.1 Sårbarhet lag 1: Electrical power infrastructure

Det var blitt gjort en del arbeid med å kartlegge konsekvensene av strømbrudd i Nederland allerede på 1990-tallet; «*Strømløs*»-rapporten [21] er den mest omfattende av disse.

Det er vanlig å dele inn strømforsyningen i to deler; henholdsvis medium- og lavspennings-nettverk (distrikter) og produksjonssystemer, svitsjesystemer og høyspent-nettverk. Det vanligste er forstyrrelser og brudd i distriktene som en følge av skader på kabler og tekniske feil. Slike brudd har varighet fra noen timer og inntil noen dager. Ved brudd på høyspentnettet, er det oftest overbelastede kabler, tekniske forstyrrelser eller administrative feil som har skylden. I slike tilfeller vil IKT-infrastrukturene slutte å fungere eller oppleve overbelastning av trafikk i de komponentene som er utstyrt med nødspenning.

Det er uklart hvor Nederland står i forhold til sikringen av elektronisk overvåking og kontroll av det elektriske strømnettet. I USA er trenden at man i stadig økende grad tar i bruk kommersielt utstyr for å utføre administrative oppgaver. I tillegg benytter man ofte offentlige kommunikasjonsnett til transport av slike data. På denne måten oppstår det nye sårbarheter.

I Nederland er det kun det nasjonale nødnettet (National Emergency Network) og telefonnettet som er utstyrt med nødspenning. En av konsekvensene ved større strømbrudd, er derfor at størsteparten av mobilnettet vil falle ut umiddelbart. Grunnet uventet stor etterspørsel etter elektrisk kraft i og rundt Amsterdam, har man valgt å øke utnyttelsesgraden i det allerede eksisterende strømnettet. Dette øker risikoen for at telekom-operatører kan oppleve varige utfall av tjenester.

3.1.4.2 Sårbarhet lag 2: Network infrastructure layer

Sårbarheten på dette laget er direkte knyttet til tilgjengeligheten av tjenesten, da denne infrastrukturen tar seg av transporten av bits over kabel. Kabelbrudd er derfor den vanligste årsaken til problemer på dette laget. I og med at kabler ofte bærer mange forskjellige typer tjenester, kan det ventes at kabelbrudd vil medføre omfattende konsekvenser.

- Det nederlandske telenettet KPN Telecom var allerede i år 2000 utrustet med dublert kabling i alle retninger, slik at et hvilket som helst kabelbrudd ville være fullstendig transparent for nettverksfunksjonaliteten.
- Et tilfelle i Nederland i 1999 hvor fire av KPN Telecoms fiberkabler ble brutt samtidig, medførte ni timers bortfall av både mobil- og linjetelefoni, faks, datatrafikk, elektroniske betalingstjenester, Internett og nødtjenestene. Konkurrerende mobilnett falt også ut da de delvis var basert på KPNs fiberkabler. Samtidig ble også databasen for registrering av bilnummer satt ut av spill, og den trådløse reserveløsningen (mikrobølger) ble ikke aktivert fordi det ikke ble ringt inn noen klager fra det mørklagte området.

Selv om det finnes alternative ruter ved kabelbrudd, viser erfaringene at konsekvensene gjerne inkluderer en god del forsinkelse.

- Fire fiberkabler på 10 gigabit per sekund ble ødelagt i Ohio, USA, i 1999. Internett-trafikken mellom øst- og vestkysten i USA ble omdirigert via London og København – med lange forsinkelser som konsekvens.

På grunn av presset med å få ut produkter på markedet så fort som mulig, hender det at produsentene ikke rekker å teste utstyret grundig nok før det blir satt i produksjon. Det kan derfor hende at man vil oppleve uforutsette forstyrrelser også fra programvaren på svitsjing- og ruting-lagene ved alvorlige forstyrrelser i nettet. I tillegg er Nederland et massivt termineringspunkt for transatlantiske forbindelser. Man lurer på om brudd på så lite som en enkelt slik forbindelse vil kunne medføre store ringvirkninger for de andre nettverkene.

Jamming av GPS- og GSM-kommunikasjon er mulig å få til med støysendere, men slike trusler er lokale av natur, og det å spore opp gjerningsmannen er relativt enkelt. Nederlenderne mener imidlertid at avlytting og misbruk av GPRS- og UMTS-data kan bli en lønnsom bedrift når disse tjenestene blir mer populære. Samtidig risikerer man at tilliten til mobil eHandel blir skadelidende.

3.1.4.3 Sårbarhet lag 3: Transmission service infrastructures

Den mest akutte sårbarheten på dette laget involverer aktivt ødeleggende handlinger og inkluderer fysiske og elektromagnetiske angrep, falske fasader (spoofing og phishing) og tjenestenekt fra utsiden. Grunnet den raskt voksende infrastrukturen, er det også en økende fare for tekniske feil og nettverksoperatører med mangelfull utdannelse og erfaring. I denne prosessen vil redundans bli oversett og SPF (Single Points of Failure) bli bygget inn. Kun gjennom omfattende analyser kan

slike faktorer bli avslørt på et tidlig stadium.

3.1.4.4 Sårbarhet lag 4: ICT-infrastructure middle-layer

På dette laget finner man elementære Internett-tjenester som eHandel, TTP, pålitelig meldingsutveksling (eksempelvis digitale signaturer), samt navngiving og adressering (eksempelvis domenenavn). Påliteligheten til disse tjenestene er essensiell for samtlige nettbaserte tjenester og berører særlig publikums og myndighetenes tillit til den overveldende integrasjonen av IKT-tjenester i samfunnet. I omtalen av sårbarheten til disse IKT-tjenestene, siktes det til sårbarheten til systemet som tilbyr den enkelte tjenesten, samt sårbarheten til infrastrukturen som tjenesten tilbys igjennom.

Beskyttelse av integriteten og konfidensialiteten til serverne som tilbyr disse tjenestene, er primært tjenestetilbydernes eget ansvar. Slike problemstillinger er sammenlignbare med innbrudd i et bankhvelv og kan stort sett forhindres ved korrekt anvendelse av sikkerhetsmekanismer. Konsekvensene av denne typen sikkerhetsbrudd omfatter blant annet økt skepsis til eHandel blant forbrukerne.

Atskillig verre er det dersom adresseringssystemet på Internett skulle feile. I lys av nylige hendelser har man funnet at DNS-tjenesten, som tilbyr slik adressering på Internett, er mer sårbar enn tidligere antatt. I tillegg finnes det ingen garantier for tilgjengeligheten til denne kritiske tjenesten. Teknisk sett er det flere utfordringer – så som eksistensen av SPF, mangel på redundans, overbelastning av domeneservere og risikoen for administrative feil. Det forekommer også stadige problemer i form av falske fasader, etterligning av andre nettsteder og feilsituasjoner i deler av navnestrukturen. De viktige navnetjenerne og deres backuper i Nederland kan gjøres utilgjengelige i noen timer gjennom rettede angrep.

3.1.4.5 Sårbarhet lag 5: Added-value services

Disse tjenestene baserer seg på at de underliggende basistjenestene og -infrastrukturene er pålitelige. Problemet ligger i det at de underliggende kjedene av IKT-tjenester er vanskelige å ha oversikten over. Derfor er det vanskelig å forstå og redusere avhengigheter og svakheter selv ved design av nye tjenester. I prinsippet kan en feil på en enkelt link ta ned hele tjenesten dersom den spesifikke avhengigheten ikke har redundans. Sårbarheten til disse tjenestene er følgelig i det store og hele avhengig av påliteligheten til de underliggende lagene, samt ekspertisen til personellet som gjenoppretter systemet etter feilsituasjoner. Dersom alvorlige feilsituasjoner kommer ut av kontroll, kan dette føre til at private brukere og finansverdenen mister tilliten til informasjonssamfunnet.

- Melissa-ormen spredte seg svært raskt i 1999. En US Air Force-base med ansvaret for å støtte Kosovo-operasjoner ble også rammet av denne ormen gjennom en leverandør. Resultatet var at hele basen ble stengt en hel dag.

3.2 KWINT – «The Vulnerable Internet»

Historisk sett har Nederland alltid hatt en sentral plass i europeisk sammenheng. De største havnene og samlingspunktene fant man i Nederland. Selv om skutetida er over og vi nå er i IKT-tidsalderen, har Nederland fremdeles en viktig posisjon; særlig for samtrafikken på Internett. AMS-IX knytter sammen ISPer fra USA, Skandinavia og resten av Europa. Nederland knytter altså sammen de europeiske landene og USA slik at de kan utveksle trafikk over Internett. Siden den nederlandske

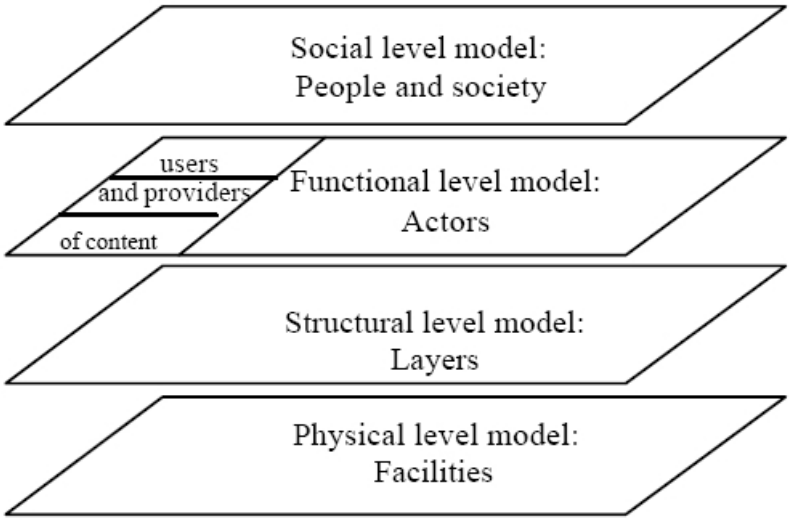
Internett-infrastrukturen er en såpass vital node i den europeiske informasjons-infrastrukturen, kan forstyrrelser på den nederlandske delen av Internett få store ettervirkninger for andre europeiske land. Stratix og TNO satt derfor igang prosjektet KWINT (Kwetsbaarheden van Internet) for å studere sårbarheten på den nederlandske delen av Internett. Prosjektet var ferdig 12. januar 2001.

KWINT-rapporten [43] er skrevet på nederlandsk. Luiijf har skrevet et engelskspråklig paper som er et sammendrag av KWINT; «*The Vulnerable Internet – A study of the critical infrastructure of (the Netherlands section of) the Internet*» [10]. Det vil bli gitt en gjennomgang av KWINT-prosjektet og Luiijf sitt paper.

Under arbeidet med rapporten, viste det seg at det ikke fantes mange brukbare modeller som kunne vise sammenhenger, avhengigheter, innvirkning på samfunnet, samt alle aktører som er involvert i Internett-sammenheng. Derfor ble det nødvendig for de involverte i KWINT-prosjektet å utvikle egne modeller for å kunne håndtere det komplekse problemet med sårbarhet på Internett, samt å få med alle aspekter som strømbrudd, feil i nettverksutstyr, nasjonal infrastruktur, kritiske tjenester og alle markedsaktører, brukere og tilbydere. Det ble utviklet fire modeller med forskjellige innfallsvinkler for å ta for seg og klargjøre de ulike aktørrollene, mangfoldigheten, gjensidige avhengigheter og sårbarheter. Man definerte Internett som ende-til-ende; det vil si at man inkluderte arbeidsstasjoner, private og offentlige IP-nettverk og informasjonssystemer på servere.

De fire nivåer av modeller som ble utviklet, se Figur 14, er:

- Modell av sosialt nivå: Mennesker og samfunn
- Modell av funksjonelt nivå: Aktører
- Modell av strukturelt nivå: Lagene
- Modell av fysisk nivå: Fasiliteter



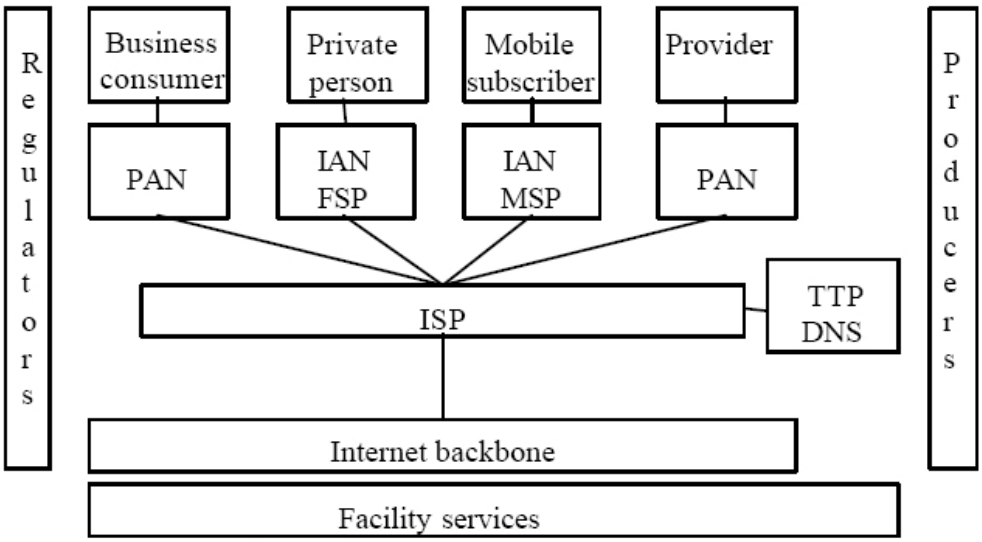
Figur 14: Fire nivåer av modeller [10]

3.2.1 Sosialt nivå: Mennesker og samfunn

Denne modellen ble benyttet for å drøfte motiver og økonomi til Internett-utviklingen. Den ble brukte til å forklare dynamikken bak Internett-utviklingen; hvordan tjenestekjeder fra organisasjonene i de ulike samfunnssektorene henger sammen, samt nye ideer som påvirker alle

aspekter ved Internett.

3.2.2 Funksjonelt nivå: Aktører



Figur 15: Modell av funksjonelt nivå - Aktører [10]

Den funksjonelle modellen viser de ulike aktørene som er tilknyttet Internett, se Figur 15. Man laget denne modellen som et mellomledd mellom brukererfaringer – det vil si organisasjoner, private brukere og bedrifter på toppnivå, og de mer abstrakte underliggende strukturelle og fysiske modellnivåene.

På toppen av Figur 15 ser man de ulike brukere, konsumenter og produsenter av informasjon – koblet til Internett via ulike aksessnett. Bedrifter og informasjontilbydere er som regel koblet til en ISP med forskjellige typer private aksessnettverk (PAN). De kobler seg ofte til en ruter i ISPens nett og får på den måten aksess til Internett. Vanlige private brukere får tilgang gjennom Internett Aksessnettverk. Disse aksessnettene tilbys av faste eller mobile tjenestetilbydere, FSP (Fixed Access Service Provider) og MSP (Mobile Access Service Provider). De ulike aksessnettene kobles til ISPens nett, som igjen er koblet til resten av Internett. Tjenester som DNS knytter man inn på ISP-nivå, da de fleste Internett-tjenester på brukernivå er avhengig av denne tjenesten for å fungere. Alle ISPer har sin egen DNS-server som ved behov kontakter DNS-servere på rotnivå.

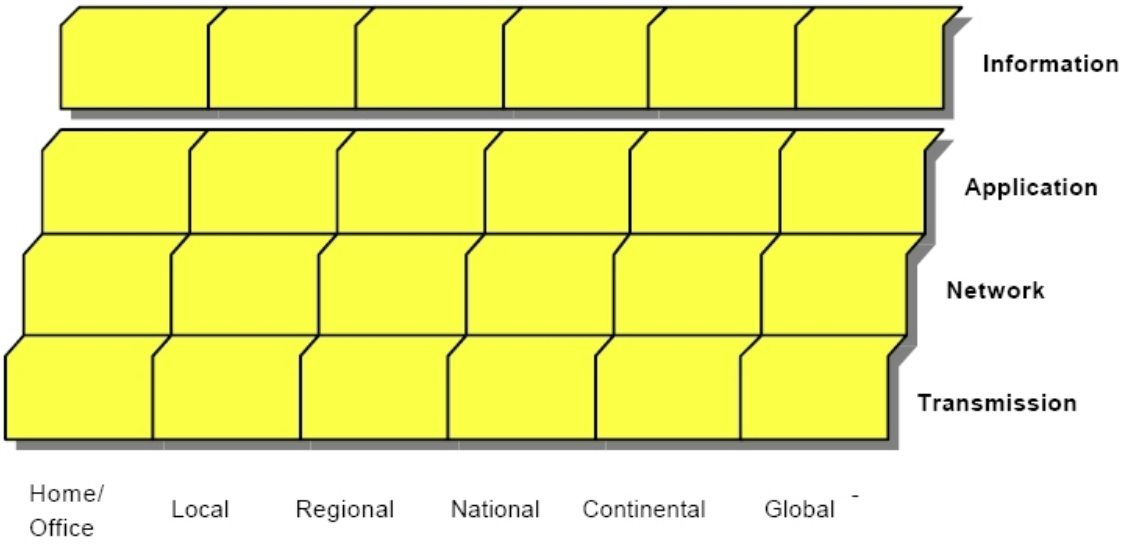
I KWINT-rapporten har man funnet ut at det er ni typer av aktører knyttet til Internett. De ni er:

- Brukere og konsumenter av informasjon
- Tilbydere av informasjons- og transaksjonstjenester
- Aksessnett-tilbydere
- Internett tjenestetilbydere
- Grunnleggende applikasjonstilbydere som DNS, ASP (Application Service Providers) og TTP
- Tilbydere av transportkapasitet i ryggradsnettet
- Regulatører som IETF, ITU (International Telecommunication Union), ETSI (European Telecommunications Standard Institute) og myndigheter
- Software- og hardwareprodusenter som sørger for Internett-funksjonalitet

- Fasiliteter som bygninger, strøm, sikkerhet, verdiskapende tjenester (eHandel), automatisert skatteinnsamling, GPS og så videre

3.2.3 Strukturelt nivå: Lagene

For å kunne undersøke markedsområdet til tjenestetilbydere og produktleverandører, ble Stratix' grunnleggende lagmodell utviklet, se Figur 16. Ser man på modellen horisontalt, er det definert ulike geografiske områder. Ikke alle aktører er aktive på alle områdene. Eksempelet som blir nevnt, er at en tilbyder som tilbyr .nl toppnivå-domenet er av nasjonalt omfang, mens en .com tilbyder har internasjonalt omfang. Et annet eksempel er utstyrsleverandører. Leverandører av intranett i bedrifter er ofte forskjellige fra transportnettleverandører på Internett.



Figur 16: Modell av strukturelt nivå - Lagene [10]

Modellen er delt inn i fire lag: Informasjons-, applikasjons-, nettverks- og transmisjonslaget. På informasjonslaget finnes brukerinformasjon og transaksjonsfasiliteter fra private og bedrifter. Applikasjonslaget omfatter DNS og protokollkonvertering. Eksempelvis VOIP, epost og SMS gateways. Standard applikasjonsprotokoller som IRC, IM (Instant Messageing), POP, IMAP og TTP finner man også på dette laget.

Nettverkslaget er IP- og rutinglaget. Her er det Internet Protocol som gjelder. IP-pakker utveksles mellom endesystemer og ISPer og mellom de ulike ISPene. For at pakkene skal finne frem til destinasjonen, er det nødvendig at rutingen fungerer. Rutere bygger opp rutingtabeller ved hjelp av rutingprotokoller. Eksempler på protokoller er OSPF, BGP og IGP Interior (Gateway Protocol). Internet eXchange sørger for at nasjonale og internasjonale ISPer kan utveksle trafikk seg imellom. I Nederland finner man AMS-IX som knytter Europa sammen med Amerika – og dermed utgjør en vital node i europeisk Internett-sammenheng. Transmisjonslaget sørger for den fysiske transporten av digital informasjon. Ofte er det teleoperatørene som eier og drifter linjene som utgjør transmisjonslaget.

3.2.4 Fysisk Nivå: Fasiliteter

Når man analyserer sårbarhet er det viktig å vite fysisk lokasjon til driftsmessige fasiliteter. På fysisk nivå finnes strøm, lokasjonen til rutere, IX og andre viktige noder. For aktører finnes det ofte

geografiske eller horisontale avhengighetskjeder. Et eksempel som er nevnt, er peering. Mange land sammenkobler nasjonalt Internett i USA. Hvis man ikke har tenkt på redundans, kan sammenknytningspunkter, peeringsentre og oppbevaring av data være potensielle SPF.

3.2.5 Sårbarhetsvurdering av den nederlandske delen av Internett

For å kunne utføre en høynivå sårbarhetsanalyse, fant de involverte i KWINT ut av man trengte enda en lagdelt modell. Denne modellen ble utledet ved å utvide Stratix' grunnleggende lagmodell med to nye lag slik at man fikk en modell med seks lag. Det første nye laget ble lagt til under transmisjonslaget og er logisk infrastruktur- og fysisk interaksjonslag (convergence and entanglement). Helt i bunnen av lagmodellen la man til fysisk miljø. I tillegg til de ulike lagene, delte man inn i tre ansvarsområder: Et enkelt håndterings- og ansvarsområde (eksempelvis en bank eller en ISP), et multi-ansvarsområde og forstyrrelser på nasjonalt nivå, (eksempelvis et fiberbasert ryggradsnett med flere parter) og forstyrrelser på globalt nivå (eksempelvis håndtering av virusutbrudd). Når man så gikk igjennom de seks lagene, kategoriserte man svakheter, truslenes sannsynlighet og deres mulige innvirkning etter de tre ansvarsområdene. Trusler og innvirkning ble kategorisert til høy, middels eller lav.

Når man skulle presentere de viktigste sårbarhetene på Internett i Nederland, ble de ulike sårbarhetene og innvirkningsnivå presentert i flere tabeller. Hvert lag ble gjennomgått og inndelt etter de tre ansvarsområdene. Deretter undersøkte man sårbarheter med tanke på sikkerhetsaspektene konfidensialitet, integritet og tilgjengelighet. I neste omgang tok man for seg aspekter som naturlige årsaker og tilsiktede angrep. Videre ble dataene presentert i tabeller for hvert lag.

3.2.6 Internasjonalt arbeid

Under arbeidet med KWINT-rapporten, tok man for seg aktiviteter, studier og arbeid fra myndigheter og internasjonale organisasjoner innen kritisk infrastruktur og informasjonsbeskyttelse. Dette ble gjort for å se hvilke fallgruver man må unngå og hvilke anbefalinger som kunne være vellykkede. CIIP-aktivitetene ble analysert og det ble laget en tabell som tok for seg de ulike organisasjonene, bedriftene og direktoratene som arbeidet med CIP og CIIP i Europa og Amerika. I rapporten ble det gitt en gjennomgang av arbeidet i Canada, USA, Tyskland, de skandinaviske landene og Storbritannia, samt enkelte internasjonale organisasjoner.

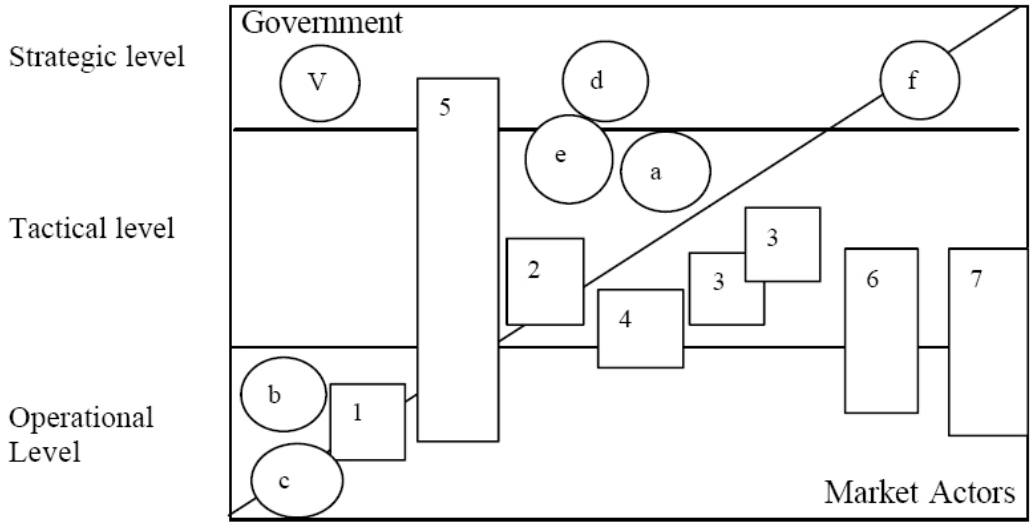
Ved å bruke det man hadde lært fra andre lands arbeid, fant man ut at det bortsett fra KWINT-studiet bare fantes et fåtall liknende initiativer, og disse verken samarbeidet eller kjente til hverandres arbeid. Blant annet kom det frem at Justis/Innenlandsministeren og Direktoratet for Telekommunikasjon og «*Post of the MoT*» begge sponset to forskjellige nettsteder med offentlige råd, og ingen av disse visste om hverandre. Ut ifra analysen av andre lands innsats innen CIP/CIIP, ble det laget en liste med konklusjoner.

3.2.7 Resultater og anbefalinger

KWINT utarbeidet policy-anbefalinger ut ifra kartleggingen av sårbarheter, konklusjoner og anbefalinger fra andre land. Før selve anbefalingen ble det laget prinsipper som måtte tas med i betraktingen i eventuelle anbefalinger. Det ble blant annet nevnt at det er umulig å sikre en Internett-basert infrastruktur 100 % på grunn av den åpne funksjonaliteten til Internett, stadig nye trusler, mange ulike aktører på alle lag rundt i hele verden og de høye kostnadene med å fjerne eller

redusere alle sårbarhetene. Et annet interessant punkt er «*outsourcing*». Mange bedrifter har erfart at outsourcing av oppgaver krever mer oppmerksomhet fra ledelsen enn før outsourcingen. Ledelsen bør prioritere de «*outsourcede*» tjenestene og gi en person i bedriften ansvar for å overvåke pris, gjennomføring og kvalitet på daglig basis.

Under utviklingen av «*KWINT draft policy*»–anbefalingene undersøkte man myndighetenes og markedsaktørenes oppgaver og ansvarsområder. Det ble laget en figur, se Figur 17 som viser en oppgave- og ansvarsfordeling på tre nivå. Hensikten med dette var å redusere sårbarheten og kontrollere krisesituasjoner på Internett. På toppen finner man strategisk nivå hvor myndighetene setter krav til sikkerhet og utførelse, legger frem langtidsvisjoner og bestemmer hva som er viktig. Det midterste nivået – taktisk nivå, er viktig for å få dialog og interaksjon mellom myndighetene på toppen og markedsaktørene på bunnen. Det laveste nivået er operasjonelt nivå, hvor markedsaktørene har sitt primære arbeidsområde. Her har myndighetene bare et fåtalls oppgaver – så som politietterforskning og nasjonale sikkerhetsoppgaver. Blir det forandring i trusler, ytelse eller kvaliteten på Internett, er det viktig at det blir gjort handlinger på det taktiske nivået; enten fra myndigheter eller markedsaktører. Men dette er hovedsaklig et felles ansvar.



Figur 17: Tre nivåer for ansvar og oppgaver [10]

Et samspill mellom offenlige og private aktører krever støtte, samarbeidsvilje og tillit. Dette er ikke alltid lett å få til, men KWINT kan være et første steg. KWINT presenterer anbefalinger for hvordan myndighetene skal gjøre sine vurderinger, syv primære mekanismer og et større antall støttemekanismer. Forfatterne av KWINT-rapporten håper at man ved å gjøre de foreslåtte handlingene vil få igang en prosess som bringer sammen myndighetene, de ulike markedsaktørene, telekom og ISPer på det taktiske nivået. Forhåpentligvis vil de samarbeidende partene fortsette å samarbeide for å minimere sårbarhetene på Internett.

De ulike tiltakene kan studeres i dybden i KWINT-rapporten [43] og det finnes et kort sammendrag i Vulnerabilities-paperet [10]. Kort sagt dekker anbefalingene alle delene av Figur 17, og viser at sårbarhet på Internett kun kan håndteres gjennom en bred felles privat og offentlig innsats på alle nivåer.

3.2.8 Konklusjoner

Konklusjonen fra KWINT-rapporten er at Internett i Nederland er sensitivt for et mangfold av sårbarheter. Siden Nederland har en hub-funksjon for Internett i Europa og transatlantiske forbindelser, er det ikke bare Nederland som ville blitt rammet ved større hendelser. Med bakgrunn i arbeidet, var det stor enighet om at Internett-infrastrukturen er mye mer kompleks enn andre infrastrukturer. Dette fordi det er mange ulike aktører som er involvert på ulike lag og over et geografisk område som strekker seg fra lokalt til globalt.

De mange modellene som ble utviklet, hjalp til å overbevise alle parter om at man ikke er istand til å øke påliteligheten av den Nederlandske delen av Internett på egenhånd. Partenes egne infrastrukturer avhenger av tjenester som leveres av andre aktører på Internett eller transmisjon- og kraftleverandører. Hvor suksessrike anbefalingene og tiltakene blir, er avhengig av villigheten og dyktigheten til myndigheter, markedsaktører, forbrukere og brukere. Gode resultater fordrer nasjonalt og internasjonalt samarbeid i håndteringen av problemstillinger rundt påliteligheten til Internett.

3.3 BAS5-prosjektet

I Norge har FFI siden 1994 samarbeidet med Justis- og politidepartementet og DSB om flere BAS-prosjekter. Det er FFI som har ledet prosjektene, og flere tilsyn, direktorater og institusjoner har hatt deltakende roller. Tidligere BAS-prosjekter har omtalt sårbarheter i telekommunikasjons-sektoren, kraftforsyningen og transportsektoren. Dette er kritiske infrastrukturer som alle er grunnleggende teknologiske nettverk i samfunnet. Tilnærmet samtlige samfunnsfunksjoner er avhengige av disse teknologiske nettverkene. BAS-prosjektene ble igangsatt for studere og evaluere sårbarheten i disse kritiske infrastrukturene [7].

3.3.1 Bakgrunnsinformasjon om BAS5

Tidligere ble IKT-systemer brukt som et tillegg eller en støtte til den normale virksomheten. Nå er dette snudd fullstendig om, og IKT-systemer har blitt kritiske for den normale virksomheten og for drift og opprettholdelse av infrastrukturene. I [7] er det laget en figur (se Figur 18) som gir et innblikk i hvilke sektorer som er avhengig av IKT.

Det siste BAS-prosjektet (BAS5) startet i 2004 og skal etter planene være ferdig i løpet av 2006. BAS5 omhandler sårbarhet i kritiske IKT-systemer. I internasjonal litteratur brukes gjerne begrepet CIIP. Formålet med BAS5 er å *«redusere sårbarheten av samfunnskritisk IKT, det vil si gjøre IKT-systemene mer robuste mot ulike trusler, villede handlinger og ulykker»* [44]. Viktige hovedmomenter er å *«Utvikle og anvende en ROS-metode (Risiko Og Sårbarhet) på samfunnsviktige IKT-systemer», «Utvikle og anvende en metodikk for å rangere tiltak som reduserer sårbarheten»* og *«Utvikle og anvende en metode for å rangere kritiske IKT-systemer og samfunnsfunksjoner».*

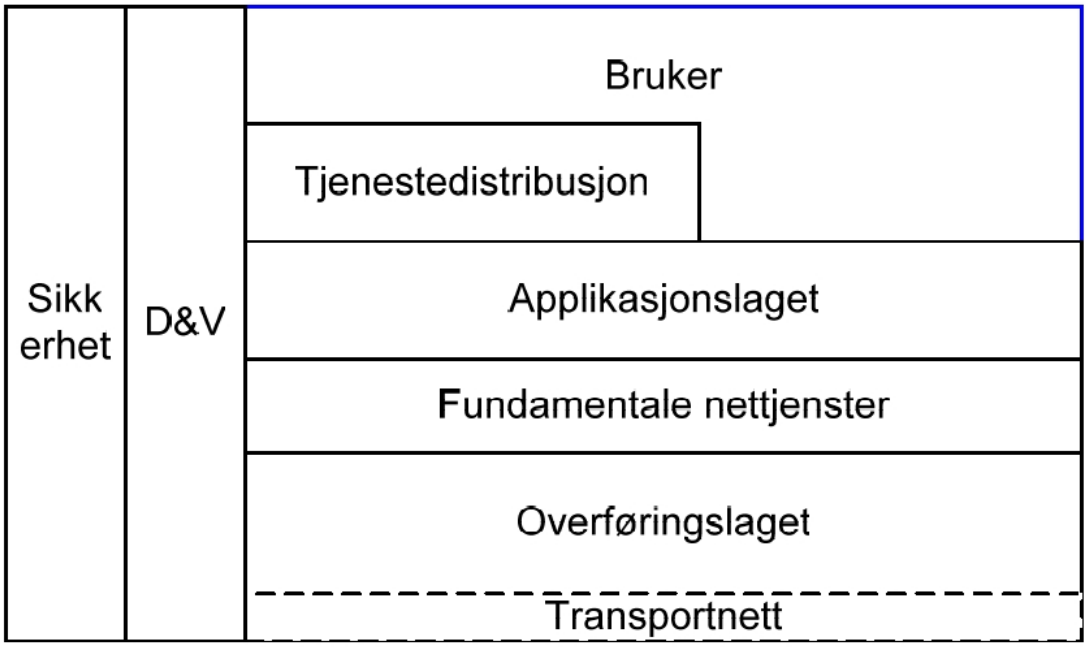
Figur 18: Sektorer avhengige av informasjons- og kommunikasjonsteknologi (IKT) [7]

Den endelige BAS5-rapporten var ikke ferdig under skrivingen av oppgaven vår, men FFI har vært generøse og gitt oss noen presentasjoner fra nåværende fase av prosjektet. I forbindelse med sårbarhetsvurderinger og andre aspekter knyttet til metodearbeidet i BAS5, har FFI opprettet det de kaller Internettstudien [18]. Formålet med dette delstudiet er at man skal utføre en sårbarhetsstudie og -analyse av Internettets infrastruktur med vekt på et «*anvendelsessyn*». Med anvendelsessyn menes i dette tilfellet et tjenestesyn; en innfallsvinkel som fokuserer på hvordan brukeren er knyttet opp mot tjenestene. Eksempler på dette er: Privat og offentlig migrering mot Internett, kundehåndtering over Internett (eksempelvis nettbank) og Internett som infrastruktur for digital kommunikasjon (IP-telefoni). Bakgrunnen for Internettstudien er at Internett nå blir brukt i stadig større grad som basis-infrastruktur for samfunnkritiske tjenester og prosesser [19].

3.3.2 Lagdelt referansemodell

For å kunne studere sårbarheter, trusler, tjenester og aktører på Internett, ble det utarbeidet en lagdelt referansemodell over Internetts oppbygging og virkemåte, se Figur 19. Modellen består av fem hovedlag og et halvt lag mellom bruker- og applikasjonslaget. Samtidig ser man på sikkerhet, drift og vedlikehold på alle lagene. Vi har ikke fått noen utfyllende beskrivelse, men vi har fått slides som beskriver lagene med stikkord [18].

Laget som er i bunnen av modellen, er transportnettlaget. Dette laget tar for seg de noder og forbindelser som i kommunikasjons-infrastrukturen sørger for transport av informasjon mellom geografiske punkter. Her finner man beskrivelser av hvordan Internett er sammensatt av flere typer nett, og hvordan de ulike nettene er oppbygd. Nettverkselementer som nevnes er kjernenettet, distribusjonsnettet og aksessnettet. Andre stikkord som nevnes er ekstern kommunikasjonsstruktur, et utvalg av aktører og geografiske aspekter.

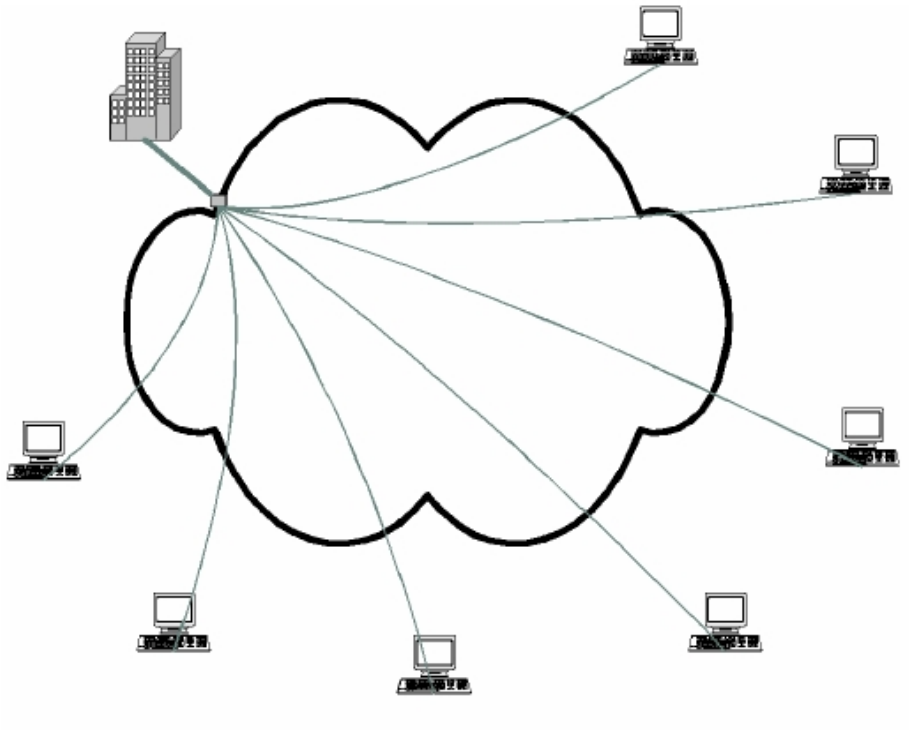


Figur 19: Lagdelt referansemodell for Internetts oppbygning og virkemåte [18]

Neste lag er overføringslaget. Dette laget tar for seg de protokollene og tjenestene som sørger for overføring av trafikk i nettet. Her behandles Internett-protokoller og rutingprotokoller. Viktige protokoller er IP, BGP og OSPF.

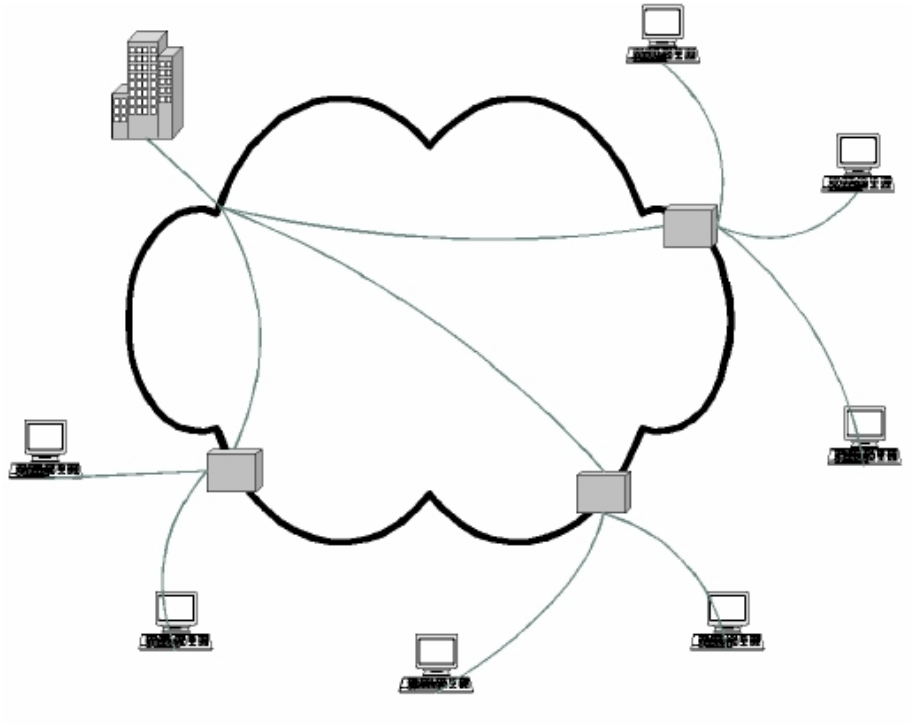
Laget fundamentale nettjenester beskriver tjenester som er nødvendig for at Internett som kommunikasjonsinfrastruktur skal fungere. Tjenester som nevnes er DNS og NTP (Network Time Protocol).

Det fjerde laget er applikasjonslaget. Systemer og tjenester som har direkte innholdsverdi for sluttbrukeren er på det øverste laget i modellen og inkluderer tradisjonelle applikasjonslags-protokoller for e-post, web og filoverføring.



Figur 20: Tradisjonell modell for tjenestelevering [19]

Tjenestedistribusjonslaget er et slags mellomlag mellom applikasjonslaget og brukeren. Tradisjonell tjenestedistribusjon kan beskrives som på Figur 20. Den baserer seg på at en node i nettet tilbyr for eksempel Windows-oppdateringer og websider. Dette skalerer ikke særlig godt globalt, og man trenger en alternativ leveringsmodell. En ny metode kalt Content Delivery Networks, er en nettverksinfrastruktur for desentralisert innholdsleveranse, se Figur 21. Dette nettverket er et distribuert nettverk av innholds-servere og fungerer i praksis ved hjelp av en intelligent DNS. Ut ifra hvor man er koblet på nettet, blir man sendt til den nærmeste serveren eller den nærmeste serveren med minst trafikk. Den største aktøren på dette området er Akamai som har mer en 15 000 servere i 69 land. Deres kunder er blant annet Microsoft, Yahoo, Trend Micro og ulike amerikanske departement [19].



Figur 21: Ny modell for tjenestelevering - Content Delivery Networks [19]

Sikkerhet og drifting blir trukket inn samtidig som hvert av lagene blir studert. Når det gjelder sikkerhetsaspektet, nevnes sikkerhetstjenester og sikkerhetsprotokoller. Det blir fokusert på mekanismer, løsninger og systemer for sikkerhet på tvers av de foregående lagene. Viktige mekanismer og systemer er tillitshåndtering, VPN og andre tunnelmekanismer. Når det gjelder driftsaspektene, er det aktørenes drift og styring av nettet og tjenestene det fokuseres på. Det blir tatt for seg hvordan kontroll og vedlikehold av nett og tjenester skjer på tvers av de foregående lagene [18].

3.4 Drøfting

Alle de tre arbeidene vi har gått gjennom i dybden omhandler CIIP. Vår innfallsvinkel og det vi konsentrerer oss om innen CIIP, er Internett. Siden vi har bakgrunn innen teknologi og sikkerhet og ikke samfunnsvitenskap, er det slike ting vi fokuserer på i motsetning til næringslivet og samfunnet. Under sammenligningen vil vi ha fokus på hvor bra disse er i forhold til vinklingen vår. Vi vil se på hva som er bra og dårlig i forhold til oppgavedefinisjonen og avgrensingene våre. Det viktige er å se på modellene som har blitt utviklet, hvordan disse er beskrevet og hvilket fokus de har. Viktige vurderinger vil være hvorvidt modellene beskriver alle typer informasjons-infrastrukturer eller om de kun tar for seg Internett, hvorvidt de tar opp sikkerhet og sårbarhet og hva slags fokus de har. Eksempler på forskjellig fokus kan være på teknologi, samfunn, økonomi, aktører eller blandinger av disse.

De tre arbeidene vi har gått gjennom er BITBREUK, KWINT og Internettstudien i BAS5.

3.4.1 BITBREUK

BITBREUK tar for seg sårbarheter i den nederlandske IKT-infrastrukturen og konsekvenser for informasjonssamfunnet. De har gjort et bra arbeid med å få laget en lagdelt modell (se Figur 13) som tar for seg alle former for elektroniske informasjons- og transmisjons-infrastrukturer. Metoden som går ut på å dele opp i flere lag, er en god måte å forklare og oppdele en kompleks problemstilling. For hvert lag blir det beskrevet hva slags tjenester og teknologier som brukes. Etter at alle lagene er beskrevet med tanke på tjenester og teknologier, blir det gjennomgått sårbarheter for hvert av lagene. Det er lettere for en leser å få overblikk og forståelse når man først deler opp i lag og beskriver teknologier og sårbarheter for hvert lag. Dersom alt slås sammen, er det lettere å miste oversikten over innholdet.

En av ulempene med BITBREUK i forhold til fokuset vårt, er at den tar for seg alle typer informasjons-infrastrukturer og ikke kun Internett. På nettverksinfrastruktur-laget som beskriver transport av fysiske bits, tar den med infrastrukturer til blant annet mobiltelefon-systemer, radio, TV, aksessnett og nasjonale transportnett. I forhold til oppgaven vår blir det altfor mye sammenblanding av elementer som ikke er relevante for Internett-infrastrukturen.

Det samme kan sies om transporttjeneste-laget. Her finner man for eksempel datatjenester som faks, Internett, modem, ADSL, ISDN og mobile datatjenester som GPRS, UMTS og SMS. Samtidig trekkes det inn radio- og TV-frekvenser som kan brukes til informasjonstjenester; eksempelvis tekst-TV. BITBREUK blander inn andre informasjons-infrastrukturer som telekom, radio og TV. Dette er ikke relevant for oss.

I BITBREUK er det identifisert horisontale informasjonsflyter. Med dette menes at tjenester på ett lag ikke bare er avhengige av underliggende tjenester, men også i økende grad er avhengige av andre tjenester på samme lag. Horisontal avhengighet er en viktig oppdagelse, og bruken av IKT har ført til nye problemstillinger som man ikke har måttet ta stilling til tidligere. For å kunne forstå helhetsbildet, er det etter vår oppfatning essensielt å ha dette i bakhodet.

Hovedfokuset i BITBREUK er på lagdeling, hvor man studerer teknologi og sårbarhet for hvert lag. Den fokuserer ikke mye på økonomi og samfunn. BITBREUK er et veldig godt utgangspunkt for arbeidet vårt.

3.4.2 KWINT

KWINT tar for seg sårbarheter på den nederlandske delen av Internett. Det fokuseres kun på Internett i motsetning til andre informasjons-infrastrukturer. Dette passer bra i forhold til oppgaven vår, hvor vi studerer Internett.

For å kunne håndtere det komplekse problemet med sårbarheter på Internett, ble det laget flere modeller med ulike innfallsvinkler. Ved å dele opp i flere modeller, prøver man å unngå at alt havner i en modell – noe som fort kan bli uoversiktlig. Istedet ble det laget modeller tilpasset til innfallsvinkelen. Disse omhandler samfunn og økonomi, aktører, teknologi på lagene og fasiliteter. De fleste av modellene ble kun brukt til å påpeke sammenhenger og å få et overblikk over en stor problemstilling.

Av modellene som KWINT bruker, er det særlig modellen av funksjonelt nivå med aktører (se Figur 15) og modellen av strukturelt nivå med grunnleggende lag (se Figur 16) som er interessante. Den første beskriver hvordan brukeren er koblet til Internett. Det blir også beskrevet hvilke aktører som

er involvert og deres funksjonalitet. Den strukturelle modellen er den mest teknologiske av disse og tar for seg protokoller og i hvilke områder en aktør kan være involvert.

Da KWINT skulle utføre en høynivå sårbarhetsanalyse, tok de utgangspunkt i den strukturelle modellen og la til to ekstra lag. Hvert lag ble tatt for seg, og sårbarheter ble studert. Det ser ut til at sårbarhetsstudiet er ganske bra beskrevet i rapporten på nederlandsk [43], mens det i det engelske sammendraget [10] blir relativt overfladisk behandlet. Vi synes det er bra at hvert lag blir beskrevet og at sårbarheter blir studert. Den utvidede strukturelle modellen er et godt utgangspunkt for oss, men den mangler en del om brukere av tjenester og hvordan avhengighetene spiller inn.

Hovedfokuset i KWINT er rettet mot å lage ulike modeller for flere vinklinger; særlig samfunn, økonomi og aktører. Rapporten er svak på teknologi, som vi ønsker å ha med i vårt arbeid. Tankegangen med flere modeller er bra i den forstand at man unngår å lage en unødvendig komplisert modell. Fokuset på aktører er også en av de sterke sidene til KWINT.

3.4.3 BAS5

Den delen av BAS5 som vi omtaler og har fått kjennskap til, er Internettstudien. Siden BAS5 er et norsk prosjekt, tar den for seg hva som er avhengig av IKT, samt hva som er relevant for Internett i Norge. Vår vurdering er at det er bra BAS5 omtaler avhengigheter av IKT, og dette er indirekte noe vi bygger videre på i arbeidet vårt.

Den lagdelte referansemodellen (se Figur 19) som benyttes i Internettstudien, tar kun for seg Internett. Det passer godt som utgangspunkt for oss. Modellen tar for seg oppbyggingen av Internett, hva slags protokoller som overfører trafikk i nettet og nettjenester som er nødvendige for at Internett skal fungere. Dette utgjør litt for mye detaljer om protokoller og deres svakheter.

I Internettstudien og beskrivelser av referansemodellen blir det lagt en del vekt på tjenestedistribusjon. Dette omhandler optimalisering av brukertjenester og fører blant annet til «raskere surfing». Arbeidet vårt handler mer om kritiske avhengigheter, og tjenestedistribusjon er derfor mindre aktuelt i modellen vår.

Referansemodellen innfører to vertikale lag som omhandler sikkerhet, drift og vedlikehold. Ved å legge til vertikale lag viser man at det bør fokuseres på sikkerhet på alle de horisontale lagene. Av den grunn er det interessant å trekke de vertikale lagene inn i arbeidet vårt.

Vi synes hovedfokuset til denne modellen er at man forsøker og lage en generell modell for å knytte sammen brukeren og nettverket; med andre ord hva som er nødvendig for at en bruker skal kunne benytte seg av de tjenestene Internett tilbyr. Modellen beskriver mange teknologier som er nødvendige for funksjonaliteten, men nevner ikke mye om aktører, som vi synes er viktig å ha med i en slik modell.

4 Vårt arbeid

I denne delen av rapporten vil vi gå gjennom arbeidet med den endelige modellen. Slutten av kapittelet gir en grundig beskrivelse av denne.

4.1 Introduksjon til arbeidet

I starten fant vi en del rapporter fra statlige organer i USA; blant annet en rapport fra GAO [28] og en fra DHS [5]. Disse beskrev gjeldende status for det amerikanske arbeidet innen fagområdet, samt fremtidige planer for forskning og koordinasjon av innsatsen på tvers av private og statlige aktører. Disse rapportene manglet det vi egentlig var på leting etter; referanser til og omtale av arbeid innen CIIP. Etter å ha funnet og studert CIIP Handbook 2004 [6], økte forståelsen betraktelig. Den inneholdt også en god del relevante referanser.

I CIIP Handbook 2004 var det arbeidet fra Nederland som interesserte oss mest. En pioneer innen CIP og CIIP i Nederland er Eric Luiijf. Han har skrevet mange papers og vært med på en del nasjonalt og internasjonalt arbeid. De mest betydningsfulle arbeidene for vår del var KWINT [43] og BITBREUK [9]. Luiijf sendte oss flere dokumenter og papers fra relevant arbeid innen området.

Det kanadiske arbeidet [26] vekket også interesse. Referansen var til et paper skrevet av Jacques Grenier. Utgangspunktet for det kanadiske arbeidet var å håndtere eventuelle kriser i forbindelse med år-2000-skiftet. Dessverre var fokuset mye mer på telekommunikasjon enn på Internett. Grenier fortalte at mye av det kanadiske arbeidet hadde blitt brukt som grunnlag da nederlenderne begynte sitt arbeid rundt år 2000. Av disse grunnene brukte vi ikke mye tid på å studere Canadas arbeid.

Videre har vi vært i kontakt med Håvard Fridheim, Janne Hagen og Tormod Sivertsen på FFI og fått utlevert dokumenter og papers fra BAS5-prosjektet.

4.2 Modeller for økt forståelse

Det er mange måter å tilnærme seg komplekse problemstillinger. De fleste er imidlertid enige om at forståelsen øker betraktelig dersom man introduserer en eller annen form for modeller. Ulike modeller dekker ulike behov, og vi vil kort presentere grafteori, UML og lagdeling.

4.2.1 Modeller som benytter grafteori

De siste årene har grafteori i økende grad blitt trukket inn i applikasjoner og modeller innen flere forskjellige fagfelt. Eksempler på dette finner vi innen biologi (genetikk, næringskjeder), datastrukturer i datamaskiner (stack, linked lists) og samfunnskunnskap (sektoranalyse, kryssavhengighet). I et FFI-notat [1] beskriver Jan Audestad hvordan man kan utnytte kunnskaper omkring forskjellige typer grafer også innen det teknologiske fagfeltet. Alle nettverk er grafer, og ved å gjøre en grundig jobb med å kartlegge nettverkenes egenskaper, kan man fastslå hvilke(n) graf(er) de har samsvarende egenskaper med. Resultatet er økt forståelse av mekanismer i nettverkene, samt evnen til bedre å kunne forstå komplekse egenskaper som sårbarhet og robusthet.

4.2.2 UML og statiske modeller

Utviklingen av komplekse databasestrukturer og klassehierarkier innen datateknologien har fremskyndet arbeidet med grafiske verktøy som gjør brukeren istand til å modellere den aktuelle strukturen før man lager den i praksis. Dette forenkler betraktelig arbeidet med å se sammenhenger og forstå de komplekse sammenhengene. I tillegg lukes menneskelige feil ut ved at designverktøyet genererer de endelige resultatene. Et eksempel på bruk av UML (Unified Modeling Language) finner vi i det EU-finansierte CORAS-prosjektet [50].

4.2.3 Nettverk og lagdeling

IP-nettverkene har tradisjonelt blitt modellert ved hjelp av TCP/IP-modellen. Dette innebærer at man ser på funksjonaliteten til enkeltdeler av strukturen ved å isolere disse fra hverandre. For å kunne arbeide på denne måten, har man definert grensesnitt mellom de forskjellige lagene. Dermed kan man studere og optimalisere funksjonaliteten på det enkelte laget uten å blande det sammen med andre deler av strukturen. I tillegg gjør man jobben enklere for programmererne, som slipper å implementere hele funksjonaliteten i hvert enkelt dataprogram. Istedet kan de støtte seg til skreddersydde biblioteker for underliggende deler av nettverksstrukturen.

4.3 Introduksjon til vår modell

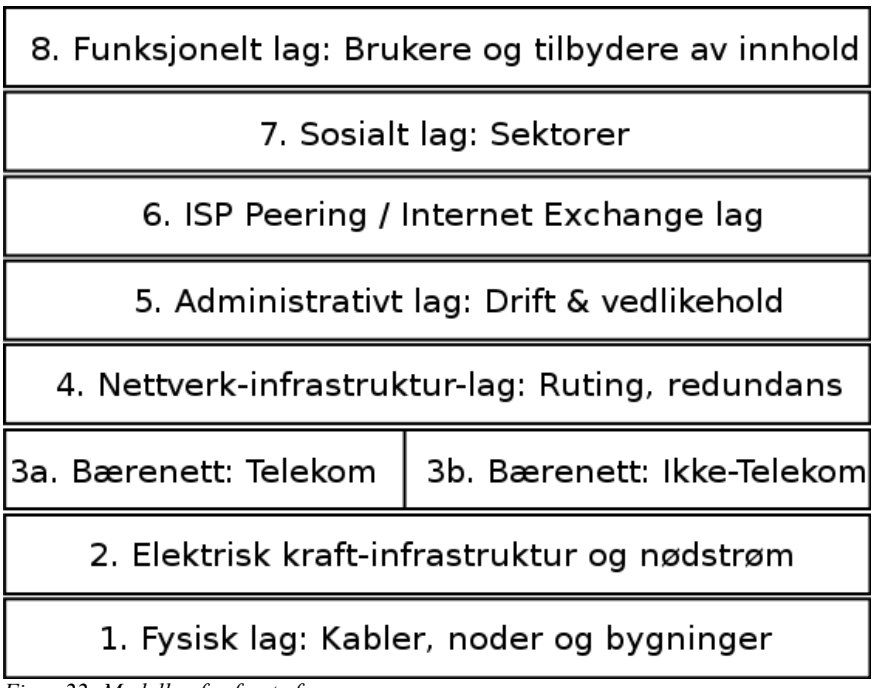
Vi valgte å se nærmere på lagdelingsmodellen fordi vi har mest erfaring med slik tankegang ifra IP-nettverk og nettverksteori generelt. Vi har gjort studier av de mest konkrete og innholdsrike internasjonale arbeidene innen fagfeltet i det forrige kapittelet. Modellene som er beskrevet i disse arbeidene, er laget med forskjellige hensikter i tankene.

Under arbeidet med de allerede eksisterende modellene, var den første tanken å utforme en modell som tok for seg alle aspektene ved IP-kommunikasjonen helt ifra brukerens PC til informasjonen forlot Norge. Det viste seg imidlertid svært komplisert å kombinere ruting, samtrafikk, diverse telekom-teknologier og momenter som elektrisitet og fysiske forutsetninger i en og samme modell. Det som ytterligere kompliserte bildet, var de horisontale informasjonsflytene vi oppdaget under arbeidet med den nederlandske BITBREUK-modellen.

Det er vår oppfatning at man ved å ta med personsøkertjenesten, opplink-stasjoner for satellittsamband og et utall analoge transmisjonstjenester, gjør en sammenblanding som neppe bidrar til å forenkle et allerede uoversiktlig bilde. I tillegg betrakter vi utviklingen rundt Internett som altoppslukende; det vil si at den synes å ta over for det meste av etablerte informasjons-infrastrukturer. De tydeligste signalene på dette finnes innen telekom-bransjen, hvor fokuset på pakkesvitsjet samband ser ut til å sluke allerede svært utbredte og tungt etablerte standarder basert på linjesvitsjing. I det videre arbeidet var det klart for oss at oppgaven kun burde ha fokus på Internett som informasjonsbærer. Samtidig bør det påpekes at Internett fremdeles er svært avhengig av eksisterende teknologier innen telekom-bransjen når det gjelder transporten av datatrafikk.

I første omgang ønsket vi å lage en modell som var så teknologisk nøyaktig og omfattende som mulig. Hensikten med dette var å kunne betrakte Internett som en selvstendig informasjons-infrastruktur og å forstå denne godt bare ved å studere en enkelt modell. Målgruppen for en slik modell vil hovedsaklig være beslutningsorganer med særlig ansvar for landets elektroniske infrastrukturer. Slike organer finnes innen offentlig sektor, og to av disse er PT og FFI.

I den første fasen endte vi derfor opp med en kompleks og uoversiktlig modell (se Figur 22) som viste seg ikke å favne alle aspekter likevel. I det videre arbeidet ble det klart at vi måtte kategorisere og prioritere annerledes for å oppnå det vi ønsket med modellen. Under studiet av KWINT-rapporten, kom det frem at nederlenderne hadde støtt på det samme problemet. Løsningen de hadde valgt gikk ut på å dele inn modellen i forskjellige innfallsvinkler.

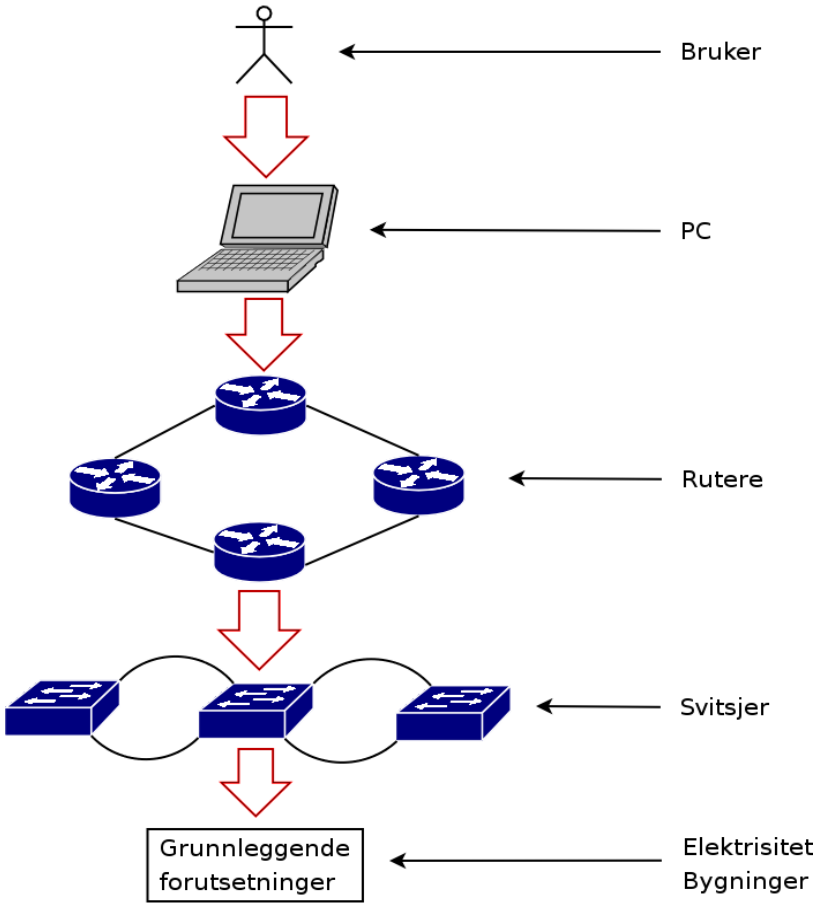


Figur 22: Modellen fra første fase

Selv om de andre arbeidene har tatt for seg sikkerhets- og sårbarhetsspørsmål, har modellene gjerne hatt en teknologisk eller samfunnsvitenskapelig innfallsvinkel. Det ble naturlig for oss å se videre på innfallsvinkelen sårbarhet, sikkerhet og avhengighet.

4.3.1 Sårbarhet, sikkerhet og avhengighet

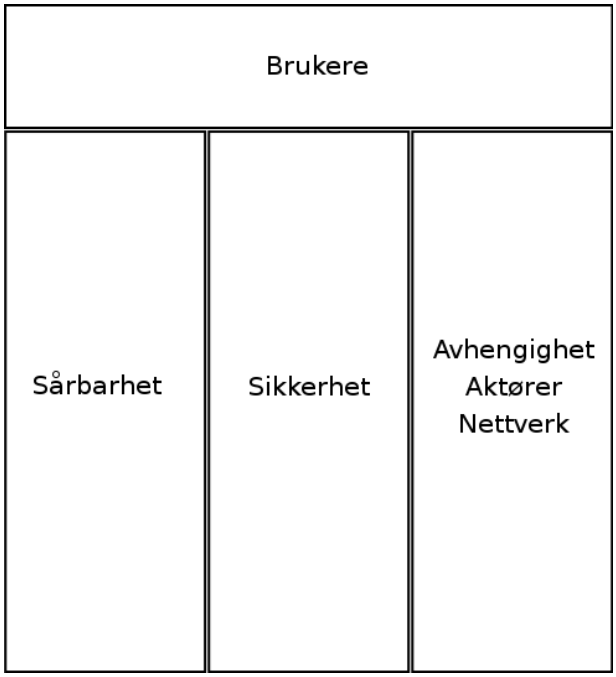
Det første perspektivet vi begynte å arbeide med, var avhengighet. I denne fasen var vi opptatt av å se på alle ressursene en Internett-bruker var avhengig av for at trafikken skulle komme uhindret gjennom Internett i Norge. En konseptskisse ble derfor utformet ut ifra denne tankegangen (se Figur 23). Figuren viser en bruker som er avhengig en PC til å kommunisere med Internett. Videre er PCen avhengig av ruting og svitsjing for at transporten av data skal kunne gjennomføres. Alt utstyret som er ibruk er videre avhengig av elektrisitet og visse fysiske forutsetninger.



Figur 23: Konseptskisse av avhengighetsmodellen

Innen informasjonssikkerhet er det grunnleggende å betrakte sikkerhet som en del av designet helt ifra starten av en utviklingsprosess. Dette omtales som «*secure by design*» [4]. Modellen vi arbeidet med, ble derfor utvidet til å dekke både sikkerhet og sårbarhet på alle lagene. En grov skisse som tilfredsstilte disse kravene, ble utformet (se Figur 24).

På toppen av modellen har vi for ordens skyld plassert menneskene som benytter seg av teknologien. Disse kan være private brukere eller arbeidstakere som jobber i en sektor. Det er særlig interessant å betrakte de brukerne som har samfunnskritiske oppgaver. I fortsettelsen skiller vi mellom sikkerhet og sårbarhet; sikkerhet er de mekanismene man anvender for å eliminere eksisterende sårbarheter. Et system uten kjente sårbarheter krever derfor ingen sikkerhetsmekanismer. Inspirasjonen til vertikale felt fikk vi ifra Internettstudien i BAS5-modellen, hvor det var tegnet inn sikkerhet vertikalt.



Figur 24: Ny modell med et sterkere fokus på sårbarhet og sikkerhet

Den første kolonnen omhandler sårbarhet:

- *I hvilken grad tekniske og menneskelige feil, uhell og sabotasje kan redusere eller hindre nettets evne til å transportere data mellom brukerne. Et robust nett har høy tilgjengelighet og stor evne til å motstå feil, uhell og sabotasje som setter deler av nettet ut av drift [20].*

Sårbarheter er det man ønsker å sikre seg mot ved hjelp av ulike fysiske og logiske mekanismer. Sikkerhetshull i programvaren er typisk et problem for brukere og bedrifter, men det kan også forekomme i rutere, svitsjer og andre noder i nettet. Sårbarheter omfatter imidlertid også det fysiske aspektet; både fasiliteter, kabler og strømnett har naturlige sårbarheter.

Den andre av de tre vertikale kolonnene tar for seg sikkerhet:

- *Tiltak for å beskytte data, under transport og lagring, mot uautorisert innsyn og manipulering. Dette vil i hovedsak være basert på bruk av kryptografiske metoder, og vil være aktuelt for å beskytte både nettet selv (navnetjeneste, driftsinformasjon), brukerdata og brukertjenester [20].*

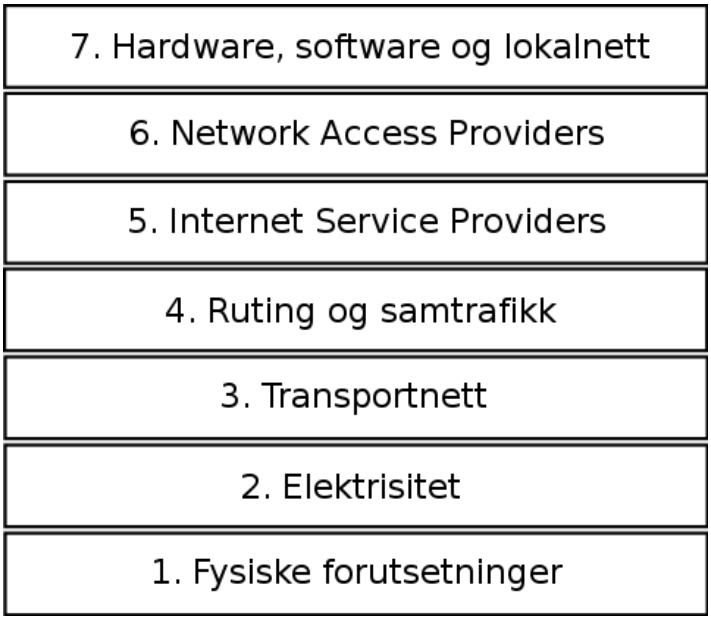
Sikkerhet og sikring av ressurser omhandler gjerne brukerens og bedriftens perspektiv; med andre ord drift. I modellen vår er dette tatt med, men fokuset er ikke på beskyttelsen av de interne ressursene til en privat bruker eller en bedrift. Eksempler på relevante sikkerhetsspørsmål i denne sammenhengen er alt ifra fysisk sikring av aksesslinjer og transportnett til logisk sikring og konfigurasjon av svitsjer og rutere.

Den tredje kolonnen tar for seg avhengighet for aktører og nettverk. Dette er de teknologiske avhengighetene som er til stede ved bruk av Internett som informasjons-infrastruktur. Hensikten er ikke å utforme en ny OSI-modell eller lignende for å beskrive innholdet i den elektroniske kommunikasjonen, men å synliggjøre alle aktører og teknologier som samspiller for at

kommunikasjonen skal nå frem til destinasjonen. For å synliggjøre sammenhengen mellom avhengighetene, er denne kolonnen delt inn i sju horisontale lag. Inspirasjonen til å tenke lagdelt på denne måten, fikk vi under studiene av BITBREUK-rapporten.

4.3.2 Kolonnen for avhengighet, aktører og nettverk

Da sikkerhet og sårbarhet er tema som berører hvert lag, har vi valgt å omtale disse aspektene sammen med den utdypende gjennomgangen av lagene. Grunnen til at vi valgte å modellere dem som egne kolonner, er at de altomfattende egenskapene til sikkerhet og sårbarhet lettest kan visualiseres ved bruk av vertikale lag. Den neste delen vil ta for seg lagene som vist på Figur 25.



Figur 25: Figuren viser alle lagene i kolonnen for avhengighet, aktører og nettverk

4.3.2.1 Hardware, software og lokalnett (lag 7)

Innholdet på dette laget omfatter alt av programvare, utstyr og kabling på brukerens eller bedriftens side; med andre ord alt på brukersiden og frem til aksessnettet. Under programvare faller både operativsystem, systemtjenester, brukerapplikasjoner. Eksempler på utstyr er lokale PCer, IP-telefoner, mobile enheter med Internett-tilkobling og ulike typer sensorer som kommuniserer over IP. Nettverksutstyr som svitsjer, rutere, brannmurer, virus walls og IDS/IPS-systemer – både på bedriftsnett og hos private brukere, hører hjemme på dette laget. I tillegg finnes det her horisontale avhengigheter: DNS-tjenester, webservere, servere for IP-telefoni og epost, PKI-tjenester (Public Key Infrastructure) og VPN. Hensikten med laget er å skille ut utstyr og nettverk i endepunktene fra selve Internett-infrastrukturen.

Sårbarheter inkluderer her sikkerhetshull og konfigurasjonsfeil i programvaren, samt fysiske svakheter i forbindelse med eksponering av utstyr og ressurser. Dersom utstyr er totalt avhengig av strøm fra kraftleverandøren, utgjør dette en sårbarhet. Horisontale sårbarheter inkluderer sentraliserte løsninger (DNS-tjenester, servere for IP-telefoni; Single Points of Failure).

Av sikkerhetstiltak kan nevnes installasjon av sikkerhets-oppgraderinger, utstyr for nødstrøm

(batteri, strømaggregat), korrekt konfigurasjon av utstyr og programvare, løsninger for desentralisering av kritiske ressurser.

4.3.2.2 Network Access Providers (lag 6)

Virtuell NAP har ikke eget utstyr, men driver videresalg av tjenester istedet. Vi konsentrerer oss om aktører som eier og drifter utstyret selv. Laget inneholder aksessnett som brukerens eller bedriftens lokale utstyr er tilkoblet. På dette laget transporteres meldinger fra brukerens endeutstyr til og fra ISPens nett. Det finnes flere typer aksessnett; som eksempelvis kabel-tv, xDSL, ISDN, Wi-Fi, WiMAX, UMTS, GPRS, Ethernet over fiber og satellitt.

Hensikten med å ta med dette laget, er å tydeliggjøre segmentet som sprer data ifra store distribusjonskanaler til et større antall endepunkter med lavere båndbredde. Fordelen med dette er at man får skilt ut NAP-aktørene, samt at man kan vurdere sårbarheten på dette segmentet separat.

På aksessnettet kan man dele inn i kategoriene fysiske og logiske sårbarheter. Under fysiske sårbarheter hører kabelbrudd, anslag mot noder og jamming og støy på radiosambandet. Dersom utstyr er totalt avhengig av strøm fra kraftleverandøren, utgjør dette også en sårbarhet. Logisk sårbarhet handler i all hovedsak om opphoping av trafikk på kundens forbindelse, samt programvare- og konfigurasjonsfeil i noder. Ved opphoping er det enten gyldig eller ondsinnet (DDoS) trafikk eller en kombinasjon av disse.

Enkelte fysiske sårbarheter er det vanskelig å sikre seg mot; så som gravearbeid, jamming og støy. Anslag mot noder kan forebygges ved fysisk sikring av fasiliteter, og problemene knyttet til kortere strømbrudd kan elimineres ved å ta ibruk utstyr for nødstrøm. Logiske sikkerhetstiltak inkluderer håndtering av oversvømmelse på kundeforbindelsen. Ved å håndtere dette problemet på ISP-laget, unngår man at aksessforbindelsen fylles opp fra utsiden. For DDoS har vi tidligere nevnt «*Aggregate-based Congestion Control*».

4.3.2.3 Internet Service Providers (lag 5)

På samme måte som for NAP, finnes det virtuelle ISPer. Siden disse ikke eier utstyret selv, er de heller ikke aktuelle for videre betraktninger. ISP-laget inneholder transportlinjer som ISPen selv eier og har fullstendig kontroll over, samt intern ruting-funksjonalitet. I tillegg kommer interne protokoller som RIP, OSPF, MPLS og Ethernet. Hensikten med ISP-laget er å skille ut ISPen som aktør og nettet den administrerer. Fordelen med det er å kunne betrakte sårbarhet og sikkerhet på dette segmentet separat.

Fysisk sårbarhet forekommer her i forbindelse med noder i nettet, samt ISPens transportlinjer og strømforsyningen. Logiske sårbarheter inkluderer tilgang til det administrative grensesnittet på nodene i nettet, mangel på alternative ruter for trafikken og programvare- og konfigurasjonsfeil i nodene. Tilgang til det administrative grensesnittet på nodene i nettet forekommer fordi det i IP-nett ikke er noen oppdeling mellom brukerdata og kontrolldata. I ekstreme tilfeller kan et DDoS-angrep utgjøre en trussel mot ISP-nettet dersom kapasiteten ikke er stor nok.

Når det gjelder logisk sikring av svitsjer og rutere, er det vanlig praksis med VLAN (virtuelle LAN-segmenter), som innebærer en logisk oppdeling av administrative forbindelser (management) og nyttedata. Ved bruk av VLAN oppnår man at vanlige brukere av nettet ikke har mulighet for å aksessere administrative IP-adresser på svitsjer og rutere i ISP-nettet. Denne løsningen er

tilsvarende den oppdelingen man finner i telekom-verdenen med et separat pakkesvitsjet nett til signaleringsdata. Håndtering av DDoS mot aksessnettet kan innføres ved begrensning av kjent angrepstrafikk til en forhåndsbestemt verdi («*rate limiting*» av eksempelvis ICMP, UDP og TCP-SYN).

4.3.2.4 Ruting og samtrafikk (lag 4)

Begrepet samtrafikk inkluderer både peering-avtaler og samtrafikk-punkter. IP-protokollen er hjørnesteinen for all trafikken. Det fjerde laget tar for seg NIX som sentralt knutepunkt for samtrafikk mellom alle større norske ISPer. Inkludert på dette laget er også peering-avtaler som ikke går innom NIX. Utenlandsforbindelser blir ikke sendt over NIX, men ivaretas gjennom at hver enkelt ISP har peering med utenlandske operatører eller gjennom et norsk transittnett. Rutingen mellom ISPenes AS styres ved hjelp av BGP-protokollen. På dette laget finnes det horisontale avhengigheter; et AS er avhengig av andre AS for at trafikken skal komme frem til målet. Hensikten med laget er å trekke frem NIXen som et viktig punkt i infrastrukturen.

BGP introduserer kjente sårbarheter. Disse inkluderer ondsinnet bruk av BGP-protokollen og rettede angrep mot BGP-noder. På samme måten som ved intern ruting, er det en sårbarhet dersom det ved bortfall av deler av nettet ikke finnes muligheter for omdirigering av trafikken til alternative ruter. Dette omhandler ruting mellom AS.

Fordi Internett i Norge er stjerneformet, er NIX i seg selv et sårbart punkt. Et eksempel på dette er to brukere som er tilkoblet i det samme geografiske området med ulike ISPer. Ved feilsituasjoner på NIX eller på forbindelsen til NIX, kan brukerne miste forbindelsen seg imellom. Denne situasjonen kunne vært unngått dersom ISPene hadde inngått lokale peering-avtaler. NIX har nødstrøm i form av UPS og strømaggregat.

4.3.2.5 Transportnett (lag 3)

Vi definerer transportnett til å være alle former for nett som er istand til å tunnelere IP-pakker. Dette inkluderer alle TNPer. Situasjonen i Norge er spesiell fordi to store TNPer, Telenor og BaneTele, er nærmest enerådende innen utleie av transportkapasitet. Ut ifra avhengighetsmodellen, kan man se at ISPene er avhengige av et underliggende transportnett. Dette laget omfatter de aktører og nett som ISPen ikke eier selv. Tradisjonelt har transportnett vært basert på telekom-baserte teknologier som SDH og ATM. De siste årene har det blitt vanligere å benytte rent pakkesvitsjede teknologier som for eksempel Ethernet. Hensikten med laget er å skille ut TNPen som aktør og betrakte dette segmentet separat.

I SDH- og ATM-baserte transportnett er det i all hovedsak fysisk sårbarhet som er aktuelt. Det finnes trolig også logiske sårbarheter, men man får ikke tilgang til selve nettet uten først å inneha kompetanse, kostbart utstyr og fysisk aksess. Ethernet-baserte transportnett har de samme logiske sårbarhetene som nevnt på ISP-laget. Dersom utstyr er totalt avhengig av strøm fra kraftleverandøren, utgjør dette også en sårbarhet.

Fysisk sikring av noder og kabler er trolig den beste måten å beskytte SDH- og ATM-baserte transportnett. For Ethernet-baserte transportnett er det mulig å sikre seg ved bruk av logisk oppdeling og VLAN som beskrevet på ISP-laget. Problemene knyttet til kortere strømbrudd kan elimineres ved å ta ibruk utstyr for nødstrøm.

4.3.2.6 Elektrisitet (lag 2)

Elektrisk kraft er grunnlaget for alle elektroniske enheter og utgjør følgelig basisen for alle IKT-systemer. På dette laget er det kun snakk om det elektriske kraftnettet. Nødstrøm til nodene i nettet behandles på de respektive lagene av hver enkelt aktør. Hensikten med dette laget er å illustrere at alle deler av informasjons-infrastrukturen over tid er totalt avhengig av kraftnettet.

Sårbarheten og sikkerheten på dette laget omhandler kraftlinjene. Vi tar ikke stilling til feil internt i kraftnettet, men henviser til annet arbeid innen området for slike studier [9], [25].

4.3.2.7 Fysiske forutsetninger (lag 1)

Dette laget tar for seg problemstillinger som er langt utover det som har direkte med informasjons-infrastrukturen å gjøre. Det er likevel tatt med for at man skal kunne vurdere helhetsbildet sett fra myndighetenes perspektiv. Problemstillingene her inkluderer områder som rikets sikkerhet og sivil og militær beredskap i forhold til fasiliteter og nøkkelressurser på nasjonalt nivå. Vi nevner villet og ikke-villet anslag mot fysiske fasiliteter som eksempelvis bygninger, rutere, svitsjer og kabler. Under kategorien villet finner vi hærverk, sabotasje og terror. Eksempler på ikke-villet er graveulykker, branner og naturkatastrofer.

5 Case study, resultater og drøfting

Dette kapittelet tar for seg et eksempel på anvendelse av modellen som ble beskrevet i forrige kapittel. Vi har valgt å slå sammen case study med resultatene, da resultatene i stor grad belyses gjennom dette eksempelet. Det er i mange tilfeller vanskelig å skille resultatene fra case study. Vi besluttet også å gjøre drøftingen i dette kapittelet. Det har sammenheng med at drøftingen av case study og modellen generelt bør sees i sammenheng.

5.1 Case study: Sykehus

Under arbeidet med case, ble det klart at vi ikke kunne benytte detaljerte opplysninger om infrastrukturer og ISPer i Norge. Det er flere grunner til dette; de mest åpenbare går på bedriftshemmeligheter og til en viss grad nasjonal sikkerhet. Opplysningene vi har benyttet er delvis tatt fra offentlig tilgjengelig informasjon og delvis fiktive data for å gjøre bildet komplett.

5.1.1 Hardware, software og lokalnett (lag 7)

I eksempelet tar vi for oss et norsk sykehus som benytter ISP1 som leverandør av Internett og Tjenestetilbyder1 som leverandør av IP-telefoni. På toppen av modellen finner vi sykehuset med brukere tilknyttet et intranett med lokalt driftet hardware og software (brukere og lag sju). Utstyret spenner ifra filservere, brannmurer og lokale PCer til IP-telefoner og servere for IP-telefoni.

Sårbarheter inkluderer sikkerhetshull som kan utnyttes av virus, trojanere, ormer og til «*cracking*» (populært kalt «*hacking*»). I tillegg introduserer bruken av IP-telefoni en ny sårbarhet; Tjenestetilbyder1 har en sentralt plassert nummerserver for IP-telefoni som benyttes for oppsett av samtaler. En feil i denne serveren, i DNS-hierarkiet eller på Internett-forbindelsen vil effektivt slå ut hele IP-telefonitjenesten. Nødstrøm havner inn under fysisk sårbarhet.

På dette nivået handler sikkerheten om brannmurer og kryptografiske mekanismer. Videre har sykehuset sikret eget nettverk og fiber-transceiveren med nødstrøm (batterier, strømaggregat).

5.1.2 Network Access Providers (lag 6)

ISP1 er ISP og virtuell NAP, mens et annet selskap, NAP1, er reell NAP. Forklaringen på dette er at NAP1 eier aksessnettet som ISP1 tilbyr tjenestene over. Sykehuset benytter fiberteknologi fra NAP1.

Det at ISP1 benytter NAP1 sitt aksessnett, kan innebære sårbarheter og nedetid for forbindelsen. Slike sårbarheter inkluderer opphoping av trafikken i aksessnettet og programvarefeil i nettverksnoder. Et særlig aktuelt problem i aksessnettet er DDoS-angrep som fyller opp Internett-forbindelsen til sykehuset. I tillegg har ikke ISP1 kontroll med hvor raskt feilsituasjoner i aksessnettet blir korrigert. NAP1 tilbyr fiber mellom sykehuset og ISP1; strømforsyningen til fiberutstyret i NAP1 sitt nett utgjør derfor en sårbarhet. Det er ikke mulig å adressere fiber-transceiverne, og det er dermed ingen fare for logiske angrep mot aksessnettet.

NAP1 har redusert sårbarheten ved å installere utstyr for nødstrøm. Opphoping av trafikk på aksessforbindelsen blir ikke håndtert av NAP1. Kabelbrudd i aksessnettet er også en sårbarhet som NAP1 må planlegge og ta høyde for; NAP1 har en service-avtale med et firma som har spesialisert

seg på reparasjon av kabler ved brudd. Nødstrøm er tatt ibruk for å sikre mot korte strømbrudd i strømnettet.

5.1.3 Internet Service Providers (lag 5)

På ISP-laget tilbyr ISP1 intern ruting i sitt eget nett, samt til og fra aksessnettet mot sykehuset. ISP1 har også egne linjer i de regionale nettene. For å opprettholde en viss kontroll med trafikken i nettet, har ISP1 valgt en MPLS-løsning.

DDoS-angrep kan i ekstreme tilfeller lamme hele eller deler av ISP1 sitt nett dersom angrepet overstiger nettkapasiteten til ISP1. En atskillig vanligere sårbarhet er imidlertid DDoS-angrep som slår ut en bestemt kunde. Angående intern ruting er det en skjult sårbarhet dersom det ikke er definert alternative ruter for trafikken. Logiske angrep mot administrative grensesnitt på rutere og svitsjer utgjør en annen sårbarhet.

Håndtering av DDoS-angrep mot brukeren innebærer inspeksjon og filtrering av innhold. Slik beskyttelse i form av utstyr og konfigurasjon, har ikke ISP1 tatt høyde for. ISP1 har imidlertid redusert sårbarheten ved å installere utstyr for nødstrøm, samt definert alternative ruter for alle kundene sine. Faren for logiske angrep er redusert til et absolutt minimum ved inndeling i virtuelle LAN-segmenter. Dermed er administrativ trafikk skilt ut fra vanlig brukertrafikk.

5.1.4 Routing og samtrafikk (lag 4)

ISP1 har samtrafikk med andre ISPer over NIX. I tillegg har ISP1 en utenlandsforbindelse til Sverige.

Under sårbarheter bør det nevnes at ISP1 er totalt avhengig av NIX for samtrafikk. Dersom det skulle bli brudd på en eller flere av linjene til NIX, vil ikke kundetrafikken i de berørte områdene komme frem; verken lokalt, regionalt, nasjonalt eller internasjonalt. BGP benyttes over NIX og introduserer sårbarheter for inntrengere som benytter målrettede angrep.

Et grep for å redusere NIX-avhengigheten, er å opprette regionale peering-avtaler, samt å delta i samtrafikk-punktene i Trondheim og Bergen.

5.1.5 Transportnett (lag 3)

ISP1 benytter en nasjonal transportnett-leverandør, TNP1, for å koble sammen de regionale nettverkene sine.

Sårbarheten på transportnettet er kun avhengig av termineringsutstyret hos ISP1, da ISP1 leier mørk fiber av TNP1. Dermed vil ikke eksempelvis et strømbrudd hos TNP1 ha noen innvirkning på nettverket til ISP1. Det er derfor klart at det er ISP1 sitt ansvar å sikre transportnettet med nødstrøm. Kabelbrudd i transportnettet er en sårbarhet som er omtalt i kapittel 2.4.4.2.

5.1.6 Elektrisitet (lag 2)

På dette laget snakker vi kun om det elektriske kraftnettet; samtlige aktører er tilkoblet strømnettet. Nødstrøm til nodene i nettet behandles på de respektive lagene av hver enkelt operatør. Sårbarheten

og sikkerheten på dette laget omhandler kraftlinjene. For utfyllende studier av det norske kraftnettet, henvises det til BAS3 [25].

5.1.7 Fysiske forutsetninger (lag 1)

Fysisk lag tar for seg villet og ikke-villet anslag mot fysiske fasiliteter som eksempelvis bygninger, rutere, svitsjer og kabler. Under kategorien villet finnes hærverk, sabotasje og terror. Eksempler på ikke-villet er graveulykke, brann og naturkatastrofer. Hver aktør må ta høyde for naturlige og enkelte målrettede forstyrrelser, mens myndighetene i landet har ansvaret ved større katastrofer og terrorangrep.

5.2 Drøfting

Post- og teletilsynet ga oss en bred oppgave. Under forarbeidet til masteroppgaven måtte vi derfor tolke og utforme detaljene rundt oppgaveteksten selv. Vi vurderte det til å bli en best mulig oppgave ved å gå for en teoretisk vinkling. I begynnelsen hadde vi sett for oss å trekke inn utstyr og ta for oss konkrete og målbare spesifikasjoner og data som en del av case study. Det viste seg imidlertid at vi ikke fikk tilgang til slike data. Drøftingen er todelt; den første delen tar for seg case study, og den andre delen drøfter resten av oppgaven.

5.2.1 Drøfting av case study

Case study tar for seg et sykehus som har Internett-forbindelse fra en ISP og IP-telefoni fra en tjenestetilbyder. Dette er et tenkt tilfelle som representerer en av flere utfordringer innen transport av kritiske tjenester over offentlige IP-nett i Norge. Mens det for det offentlige telenettet er få og store aktører som leverer de teknologiske løsningene til sluttbrukerne, er det i Internett-verdenen mange aktører av forskjellige størrelser og på forskjellige nivå i arkitekturen. Derfor er det mer omfattende å kartlegge sårbarheter og konsekvenser ved flytting av kritiske tjenester til IP-basert transport.

Sykehuset hadde tidligere en løsning med ISDN-utstyr og egen lokal hussentral. Telefonapparatene fikk da strøm fra hussentralen, og nødstrøm behøvdes kun i det ene punktet. Ved overgangen til IP-telefoni ble utplassert svitsjer med flere porter. I denne forbindelsen ble svitsjer plassert ut i avdelingene for å unngå å trekke mange kabler til et sentralt punkt. Konsekvensene av det er behov for nødstrøm på hver avdeling; ikke bare for svitsjene, men også for hvert enkelt telefonapparat. Vi tar utgangspunkt i at sykehuset har nødstrøm, men at denne kun dekker de aller nødvendigste funksjonene. Problemer knyttet til sårbarheten og tilgjengeligheten til telefoni internt i sykehuset, har følgelig blitt desentralisert og mer uoversiktlig enn tidligere. Videre er IP-telefonitjenesten avhengig av en ekstern nummerdatabase, og i den sammenheng også avhengig av DNS. Selv når alt fungerer utmerket internt i sykehuset, kan telefonien utad gå ned ved feil i DNS-tjenesten og nummerdatabasen.

Internett-forbindelsen involverer samarbeid mellom flere aktører for at trafikken skal komme frem. På aksessforbindelsen har ISP1 en egen leverandør av aksesstjenester, NAP1. I og med at sykehuset er plassert i et tettbygd strøk, er det mindre sjanse for kabelbrudd. Skulle det likevel skje, er service-tiden sannsynligvis kort før kabelen er reparert. Det må skje et strømbrudd med en viss varighet for å slå ut aksessnettet.

Sykehuset inngikk en avtale med ISP1 om leveranse av Internett-forbindelse. Avtalen inneholder en

SLA (Service Level Agreement) som blant annet spesifiserer krav til oppetid som ISP1 garanterer. I realiteten innebærer SLA at ISP1 også garanterer oppetiden til NAP1, TNP1 og NIX. Dersom disse aktørene har sammenfallende nedetid, vil sykehuset oppleve dette som et sammenhengende brudd. Sjansene er imidlertid større for at NAP1, TNP1 og ISP1 har nedetid på forskjellige tidspunkter, og dette vil oppfattes som flere brudd på forbindelsen. Fordi ISP1 altså er avhengig av oppetid hos de andre aktørene, har den svært små muligheter til å garantere samlet oppetid. Dersom dette hadde vært i telekom-verdenen, ville eksempelvis Telenor kunnet satt inn ekstra ressurser der det trengtes for å kunne garantere samlet oppetid.

ISP1 har ikke tatt høyde for håndtering av DDoS-angrep mot sykehusets aksessforbindelse. En foruroligende praksis er det når ISPen forbeholder seg retten til å bryte aksessforbindelsen ved oversvømmelser ut mot kunden. Slike avtaler gjør at ISPen i praksis straffer kunden for å ha blitt angrepet. Særlig for kritiske tjenester vil en slik praksis være uholdbar.

Med utgangspunkt i sykehusets behov for tjenester, er det rimelig å anta at servertjenester ikke er nødvendig lokalt. Et lettvint sikkerhetstiltak for å demme opp for DDoS-angrep på aksessforbindelsen, er å ta ibruk NAT på ISP1. Ved korrekt konfigurasjon av den lokale IP-telefoniserveren og NAT-serveren, vil ikke dette skape noen problemer for sykehuset. Selv ved *port forwarding* inn mot den lokale IP-telefoniserveren hos kunden, vil DDoS i stor grad kunne forhindres fra å nå kundeforbindelsen ved filtrering på kildeadresse på ISP1 sin side.

All samtrafikken til ISP1 blir sendt over NIX. Det er med på å illustrere at norske ISPer er svært avhengige av at NIX fungerer som den skal. Figur 26 illustrerer at NIX nærmest har fungert som et eget avhengighetslag på Internett i Norge. Det er ikke ønskelig at NIX skal være et Single Point of Failure for hele Internett i Norge. De to siste årene har det imidlertid blitt opprettet samtrafikkpunkter i Bergen og Trondheim for å forbedre denne situasjonen. I tillegg har det blitt vanligere med peering-avtaler mellom operatørene innenlands. Fra et sårbarhets-perspektiv er det klart at norske Internett-brukere er tjent med mange samtrafikkpunkter og utstrakt bruk av peering-avtaler mellom operatørene.

Figur 26: NIX som avhengighet for all Internett-trafikken i Norge

Det er vanlig at norske ISPer leier transport fra de store TNPene. Konsekvensene av kabelbrudd og

feil i transportnettet er derfor dramatiske. Dersom sykehuset ønsker å sikre tilgjengeligheten på Internett-forbindelsen ved å kjøpe tjenester fra flere ISPer, bør man først sjekke at ISPene ikke benytter seg av den samme TNPen. Ved et kabelbrudd i transportnettet er det liten hjelp i å kjøpe tjenester fra to ISPer som benytter kapasitet fra den samme transportleverandøren.

Bruk av innleide service-firma kan skape problemer ved større katastrofer eller hendelser hvor flere reparasjoner må skje samtidig. Under normale tilstander kan det være uproblematisk at flere nettleverandører benytter ett og samme firma til service og vedlikehold av kablene. Dersom det skulle skje en naturkatastrofe og flere ISPer og TNPer er avhengige av ett bestemt firma for å reparere viktige kabelstrekk, kan det ta lang tid før alle tjenestene er oppe igjen.

Det elektriske kraftnettet er ikke fullstendig stabilt, og variasjoner i spenningen kan skape store problemer for elektronisk utstyr. I tillegg er det vanlig med kortere strømbrudd grunnet kabelbrudd og menneskelige feil. Nødstrøm, overspenningsvern og utstyr for utglatting av spenningsvariasjoner er derfor viktige tema for samtlige aktører i den kritiske infrastrukturen.

En av de store norske ISPene har gitt oss informasjon om at det i tilfelle strømbrudd i nettet deres kun er tatt høyde for to timers nødstrøm. Dersom dette er representativt for de ulike aktørene på forskjellige nivå i infrastrukturen, er det betenkelig med tanke på kritiske tjenester med høye krav til oppetid og tilgjengelighet. I eksempelet med sykehuset er det rimelig å anta at det finnes atskillig mer enn to timers nødstrøm for telefonitjenestene. Hvis en ISP har planer om å tilby viktige tjenester til kritiske aktører, må denne forsikre seg om at både dens eget nett, samt alle andre aktører den er avhengig av, har tilfredsstillende backup-løsninger implementert.

5.2.2 Drøfting av modellene

Modellen som vi har utformet i dette arbeidet, er bygd på tidligere arbeid fra myndighetene i Nederland og FFI, Norge. Felles for modellene er at de baserer seg på en lagdelt forståelse av teknologi, sikkerhet og sårbarhet. En slik tilnærming virker fornuftig i og med data- og telekom-verdenens sterke fokus på lagdeling innen forståelse og funksjonalitet. Det positive med en slik tilnærming er at man får abstrahert seg bort fra teknologiske detaljer. Dermed kan ikke-teknologisk personell få oversikten og ta beslutninger uten å ha en dyptgående forståelse av teknologien. På den andre siden kan det lett bli for overfladisk til å kunne gi et representativt bilde av virkeligheten. I ytterste konsekvens kan man oppleve at den lagdelte modellen ikke fanger opp en del problemstillinger som kan være viktige.

Infrastrukturer og lagdeling innen sårbarhet og sikkerhet fører gjerne til et behov for å skille ut det som har med nettverksdrift å gjøre. Med det sikter vi til konfigurasjon av utstyr, valg av teknologier, oppsett av brannmurer og lignende på bedriftsnivå. Når man videre skal beskrive infrastrukturen og sårbarhets- og sikkerhetsspørsmål i forbindelse med denne, står teorien i fare for å bli tynn og virkelighetsfjern. Etter vår oppfatning er hensikten med sårbarhets- og sikkerhetsvurderinger nettopp at man skal ha nytte av vurderingene, og da ser vi et klart behov for å gå noe dypere enn de store linjene.

Den store forskjellen mellom modellene går på utgangspunkt, hensikt og innfallsvinkel. Vårt utgangspunkt var teknologi, sikkerhet og de tre andre modellene BITBREUK, KWINT og BAS5. Hensikten med arbeidet var å utvikle en nyttig modell som skulle kunne brukes til å forstå, vurdere og fatte beslutninger i forbindelse med kritisk IP-basert infrastruktur. Innfallsvinkelen vi valgte ut ifra dette, var sårbarhet, sikkerhet og avhengighet for aktørene på de forskjellige nivåene i infrastrukturen.

5.2.2.1 Drøfting av BITBREUK, KWINT og BAS5

CIP-arbeidet som har blitt gjort i Nederland etter år 2000, har som utgangspunkt The Canadian Layer Model [26]. Det er derfor rimelig å anta at BITBREUK [9] og KWINT [10], [43] har blitt influert av tankegangen fra det kanadiske arbeidet. Hensikten med arbeidet med BITBREUK var å ta for seg sårbarheter i den nederlandske IKT-infrastrukturen og konsekvenser for informasjonssamfunnet. Rapporten skiller imidlertid ikke mellom Internett-baserte og andre typer infrastrukturer som telekommunikasjon og kringkastings-systemer. Innfallsvinkelen til BITBREUK er teknologi og sårbarhet, men fordi det blandes inn flere systemer, skiller den seg en del fra modellen vår. Når man forsøker å omtale ulike teknologier samtidig og på det samme laget, tvinges man til å abstrahere seg bort fra forskjellene. Dette er trolig den viktigste årsaken til at BITBREUK-modellen i perioder oppleves noe virkelighetsfjern i forhold til hvordan teknologien fungerer i praksis.

Utgangspunktet for KWINT-arbeidet er at markedsaktørene satt seg ned for å beskrive statusen til Internett i Nederland. Ut ifra dette ble det laget modeller og gjort studier på disse modellene. Hensikten arbeidet var å finne ut kartlegge sårbarheter, prøve å forutse utvikling i nærmeste fremtid, forutse konsekvensene av truslene, forstå hvilke aktører som spiller hvilke roller, samt hvilke tiltak som bør tas ibruk for å redusere sårbarhetene ble funnet. KWINT-rapporten beskriver fire ulike innfallsvinkler: Sosialt nivå, funksjonelt nivå, strukturelt nivå og fysisk nivå. Funksjonelt og strukturelt nivå er de to innfallsvinklene som er mest relevante i forbindelse med betraktninger av infrastrukturen. Den funksjonelle modellen trekker inn avhengighet mellom aktører og regulatører, men behandler ikke teknologi, sårbarhet og sikkerhet. I den strukturelle modellen behandles utstyrs- og programvareleverandører, samt teknologi på lagene (ulik geografisk rekkevidde).

Utgangspunktet for BAS5 var at man i de foregående BAS-arbeidene stadig hadde støtt på avhengighet i forhold til telekommunikasjon og IKT. Det er uklart hvorvidt selve modellen i Internettstudiet baserer seg på annet arbeid innen fagfeltet. I og med at denne delen av BAS-prosjektet er i en tidlig fase, er det vanskelig å si hva det ender opp med. Hensikten med studiet ser ut til å være å utvikle en generell modell for å knytte sammen brukerne og nettverket; med andre ord hva som er nødvendig for at en bruker skal kunne benytte seg av de tjenestene som Internett tilbyr. Overfor oss har de involverte i prosjektet presisert at de «*ikke ser på Internett fra en ISPs (eller tilsvarende) ståsted. Målgruppen er primært snittet mellom teknologer og beslutningstakere i offentlig forvaltning, samt sikkerhetsansvarlige innen kritisk infrastruktur [24].*»

5.2.2.2 Drøfting av vår modell

De forut nevnte modellene er laget av markedsaktører og myndigheter med den hensikt at de skulle brukes i bestemte konkrete tilfeller. Modellen vår er laget for å kunne brukes generelt på IP-baserte infrastrukturer – med enkelte tilpasninger spesifikke for Internett i Norge.

Modellen som vi har utviklet i løpet av oppgaven, slår sammen sårbarhet, sikkerhet og avhengighet med aktørene på hvert enkelt lag. Hensikten med modellen er å belyse ansvarsområder ved å sette fokus på problemstillingene som finnes på hvert nivå med aktører. Dermed får modellen også en indirekte hensikt; det å hjelpe aktører med å identifisere problemstillinger på sitt eget nivå, samt å gi pekepinner på hvordan man kan gjøre noe med disse.

Med hensyn på hvordan Internett i Norge er bygd opp, klarer modellen i tilfredsstillende grad å

belyse ansvarsområder for aktører som Internett-infrastrukturen er avhengig av. Dette inkluderer både tradisjonelle tjenestetilbydere og aktører som ikke er direkte tilknyttet infrastrukturen, som eksempelvis tilbydere av elektrisk kraft. Vi har også tidligere vært innom at aktørene på hvert nivå selv har ansvaret for å opprettholde sine egne tjenester og sikre seg mot eventuelle trusler. Dette stemmer godt overens med et sentralt begrep innen norsk samfunnssikkerhet og beredskap; nærhetsprinsippet.

I case study har vi tatt for oss et tenkt sykehus som har byttet ut tradisjonell telefoni med IP-telefoni over Internett-forbindelsen. Da vi anvendte modellen ble det klart at den utgjorde en god oppskrift for å få med de viktigste aktørene, samt sårbarheter og sikkerhetstiltak på hvert nivå i infrastrukturen. Det viser at modellen kan brukes til å forstå, vurdere og fatte beslutninger.

Resultatet er at vi har utformet en modell med et klart fokus på sikkerhet, sårbarhet og avhengighet. Modellen vår er oversiktlig i forhold til de andre modellene – den samler mye informasjon og mange aktører på en oversiktlig måte. Den er detaljert beskrevet med fremgangsmåte og eksemplifisert i et case study. Der blir det skissert hvordan et tenkt norsk sykehus med IP-telefoni over Internett-forbindelsen ville se ut i et sikkerhets-, sårbarhets- og avhengighetsperspektiv. I modellen blir det identifisert og vurdert sammenhenger mellom nøkkelressurser som infrastrukturen er avhengig av på forskjellige nivåer. Et konkret eksempel på resultater fra anvendelsen av modellen, er at alle tjeneste-kritiske aktører blir tatt med og vurdert. Sammenhengene mellom aktørene kommer også frem. Sårbarheter, sikkerhetsmessige tiltak og ansvarsområder blir grundig belyst for hvert lag i modellen.

5.2.2.3 Drøfting av valg underveis

I første runde ble det utformet en modell som forsøkte å ta med alle aspekter av teknologi, sikkerhet og sårbarhet, samt aktører og samfunnssektorer (se Figur 22). Det ble etter hvert klart at en slik modell introduserte unødvendig mye kompleksitet, i tillegg til at den manglet enkelte aspekter. Vi reviderte derfor modellen ved å kutte ut tungvint oppdeling og introdusere vertikale lag. I tillegg forandret vi fokus i forbindelse med noen av lagene i modellen.

Sektor-laget ble fjernet fordi det ikke ble ansett som relevant for infrastrukturen. Det administrative laget ble spredd over de enkelte aktørene. Laget som i første omgang ble kalt bærenett, inneholdt både aksess- og transportteknologier. I forbindelse med revisjonen forsvant aksessteknologiene ifra bærenett-laget, og navnet på laget ble omdefinert til transportnett. Dessuten forsvant oppdelingen mellom telekom og ikke-telekom på dette laget. Årsaken til omgjøringene på dette laget var behovet for å skille ut operatørene i aksessnettet og deres rolle som mellomledd mellom brukere og ISPer. Elektrisitet ble omdefinert til ikke lenger å omfatte nødstrøm. Fysisk lag ble redusert slik at det ikke lenger omfattet bygninger, noder og kabler tilknyttet de enkelte aktørene på høyere lag i modellen.

Forandringene på fysisk lag, elektrisitetslaget og det administrative laget var alle på grunn av endring i fokus angående ansvarsområder. I første omgang var planen å skille ut funksjonaliteten på de forskjellige lagene, men under det videre arbeidet føltes det mer naturlig å distribuere ansvaret ut på hver enkelt aktør. Eksempler på dette er ansvaret for kabler og nødstrøm.

Introduksjonen av vertikale lag var inspirert av besøket på FFI og modellen som var utviklet i Internettstudien til BAS5. Grunnen til at vi ikke tok med drift og vedlikehold (tilsvarende administrativt lag) som et eget vertikalt lag, er at modellen skal ha det sammen fokuset som masteroppgaven; sårbarhet og sikkerhet. De tre vertikale kolonnene er alle med for å belyse de viktigste momentene i infrastrukturen sett ifra synsvinkelen til masteroppgaven. De horisontale

lagene ble satt inn i kolonnen for aktører, nettverk og avhengighet. Sårbarhets- og sikkerhetskolonnene skulle tydeliggjøre fokuset på disse temaene på hvert enkelt horisontalt lag.

6 Konklusjon

Vi har laget en modell som tar for seg Internett som infrastruktur. Den tar for seg infrastrukturen på høyt nivå, drar inn aktører og er mer konkret enn de andre modellene på lavt nivå. I case study har vi tatt med bruker-perspektivet for å illustrere sårbarhets- og sikkerhetsperspektiver i forbindelse med transport av kritiske tjenester over IP-basert infrastruktur. Bruker-perspektivet er ikke sentralt i oppgaven, men det er ofte meningsfylt å trekke det inn for å få med de viktige aspektene.

Arbeidet vårt er basert på tre tidligere studier; BITBREUK og KWINT (TNO Defence, Security and Safety, Nederland) og BAS5 (FFI, Norge). Samtlige av disse studiene er basert på lagdelt tankegang. De to nederlandske arbeidene er utført ved at ledende markedsaktører og nasjonale myndigheter samlet seg og utarbeidet modeller og anbefalinger angående deres kritiske informasjons-infrastrukturer. BAS5-arbeidet tar for seg kritisk informasjons-infrastruktur i Norge, og Internettstudien er den delen som er direkte relevant i forhold til arbeidet vårt. I motsetning til de nederlandske modellene, er arbeidet vårt i likhet med BAS5, forskningsbasert. Vi presiserer at Internettstudien var i en tidlig fase da vi var i kontakt med FFI, og at modellen vi refererer i oppgaven ikke nødvendigvis vil se slik ut i den endelige BAS5-rapporten.

Under arbeidet med modellen var det nødvendig å trekke inn og vurdere en del aktuelle protokoller og teknologier. I motsetning til OSI/ISO-modellen og TCP/IP-stakken hvor protokollene er i sentrum, har modellen vår fokus på aktørene på de forskjellige nivåene, samt de protokollene og teknologiene som benyttes av hver enkelt aktør. Parallelt med behandlingen av teknologi, blir det for hvert lag i modellen også gjennomgått sårbarhet og sikkerhet.

Masteroppgavens hensikt er i henhold til oppgavebeskrivelsen «*å komme frem til en god fremgangsmåte for å forstå, vurdere og behandle sikkerheten og sårbarheten i en IP-basert infrastruktur*». Oppgaveteksten er fullstendig besvart fordi man ved å benytte modellen vår både kan få oversikt over, vurdere og fatte beslutninger i forbindelse med sårbarheten og sikkerheten til en gitt konkret IP-basert infrastruktur. Fremgangsmåten er eksemplifisert under gjennomgangen av case study.

I oppgavebeskrivelsen ble det sagt at vi skulle identifisere og vurdere sammenhenger mellom nøkkelressurser som infrastrukturen er avhengig av på forskjellige nivåer. Gjennom lagdelingen i modellen har vi fått frem aktører, ressurser og avhengigheter som er essensielle for Internett i Norge. Dette blir godt eksemplifisert gjennom case study hvor alle aktørene og ressursene som sykehuset er avhengig av, blir behandlet.

Innfallsvinkelen «*sårbarhet, sikkerhet og avhengighet for aktører og nettverk*» har gjort at modellen vår belyser problemstillingene fra andre vinkler enn hva de tidligere modellene gjør. Dette går særlig på sammenhengene mellom aktørenes ansvarsområder innen sårbarhet og sikkerhet. Nytteverdien av modellen er størst for de ulike aktørene i BAS-prosjektet, men det kan også tenkes at bedrifter kan ha bruk for den i forbindelse med planlegging av bedriftens Internett-forbindelse.

«*CIP is the underpinning of our society, our safety and our security*»

«*You cannot manage what you don't know*»

- Jacques Grenier, [8].

6.1 Videre arbeid

Modellen vår er spesifikk med hensyn på innfallsvinkel og hensikt. Det kan vise seg hensiktsmessig i fremtiden å videreutvikle modellen gjennom dialog med aktuelle regulatoriske myndigheter nasjonalt og internasjonalt. I tillegg kan det oppstå andre behov og hensikter som gjør det nødvendig å utforme nye modeller innen fagområdet. I de tidlige fasene av oppgaven var vi innom en helt annen innfallsvinkel; bruken av teknologier og nettverk på Internett i Norge. I den sammenhengen laget vi en modell for nettverk og teknologi på Internett i Norge (se Vedlegg A) som det kan være interessant å bygge videre på.

7 Referanser

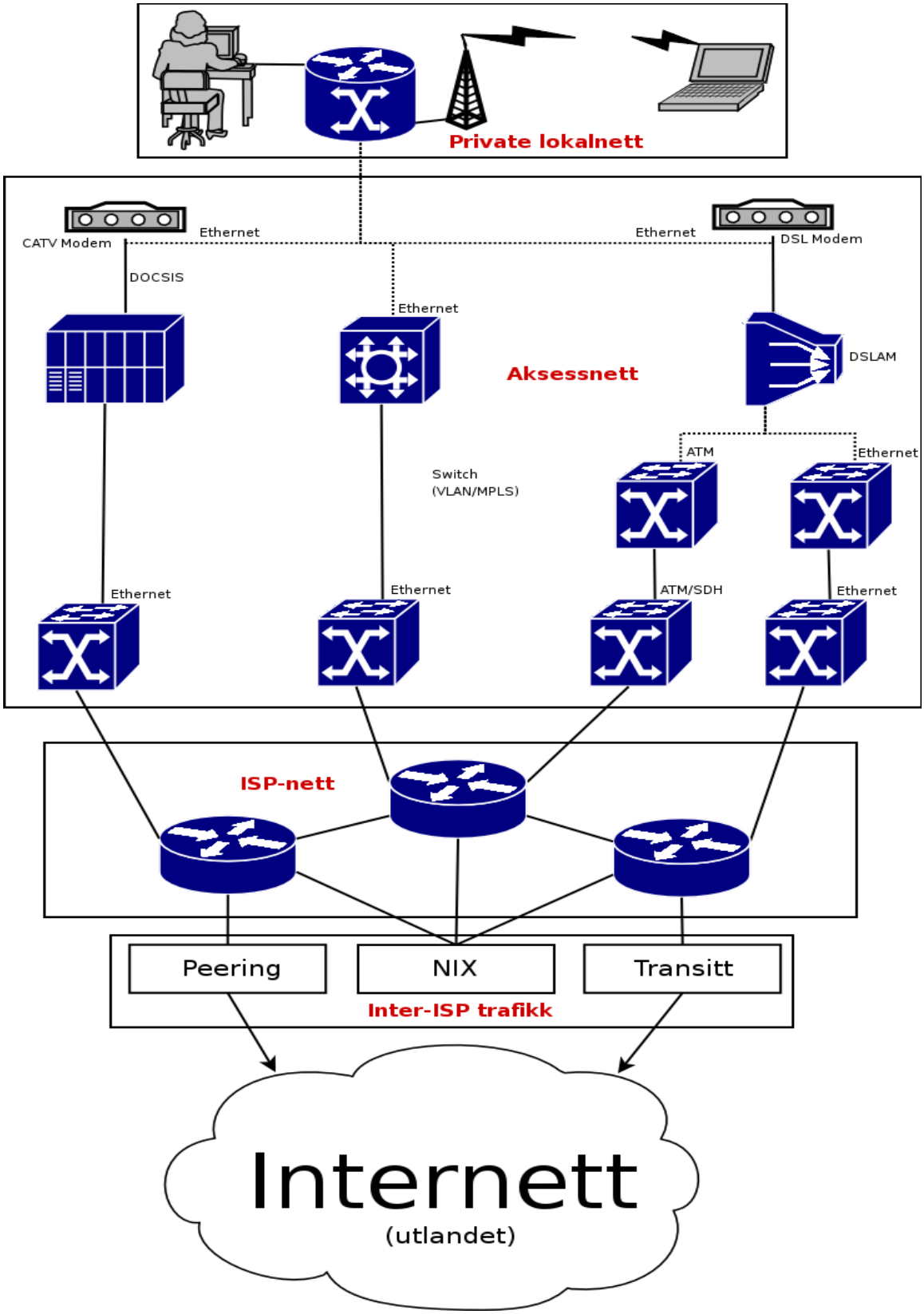
[1] Audestad, Jan, "E-BOMBER OG E-GRANATER", FFI, FFI/NOTAT-2005/00938, 2005.
[2] Billinger, Nils-Gunnar, "Strategi för ett säkrare Internet", Post- och telestyrelsen, PTS-ER-2004:37, 2004.
[3] Billinger, Nils-Gunnar, "Är Internet i Sverige robust?", Post- och telestyrelsen, PTS-ER-2003:1, 2003.
[4] Bishop, Matt, "Computer Security: Art and Science", Addison-Wesley Professional, ISBN: 0201440997, Sider: 1120, 2002.
[5] Chertoff, Michael; Marburger, John H., Department of Homeland Security, "2004 National Critical Infrastructure Protection R&D Plan", 2004.
[6] Dunn, Myriam; Wigert, Isabelle, "International CIIP Handbook 2004", Center for Security Studies, ETH Zurich, ISBN: 3-905641-92-5, Sider: 403, 2004.
[7] Fridheim, Håvard, "Samfunnssikkerhet - Er det mulig å redusere sårbarheten i krit. infrastrukt", FFI, Presentert på FFI-Forum 28.03.2006, 2006.
[8] Grenier, Jacques Pauline, "Critical Infrastructure Protection and Emergency Preparedness", PSEPC, Canada, Presentert på Swedish Emergency Management Agency, Mars 2004.
[9] H.A.M. Luiijf, M.H.A. Klaver, Infodrome, "In bits and pieces (BITBREUK)", http://www.iwar.org.uk/, 2000.
[10] H.A.M. Luiijf, M.H.A. Klaver, J. Huizenga, "The Vulnerable Internet", TNO, http://citeseer.ist.psu.edu/713100.html, 2001.
[11] Hagen, Janne, "BAS5 Critical Information Infrastructure Protection (CIIP)", FFI, http://www.forskningsradet.no/, presentert IKT-SOS workshop, Gardermoen 01.03.05, 2005.
[12] Keromytis, Angelos D.; Misra Vishal; Rubenstein, Dan, "SOS: Secure Overlay Services", http://citeseer.ist.psu.edu/, 2002.
[13] LeClaire, Jennifer, "TechNewsWorld: 802.11n Ratified as Draft Spec for Next-Gen WiFi", http://www.technewsworld.com/story/48410.html, 20.01.2006.
[14] Loshin, Pete, "TCP/IP Clearly Explained", Morgan Kaufmann Publishers, ISBN: 0-12-455826-7, Sider: 512, 1999.
[15] Mahajan, Ratul et al., "Controlling High Bandwidth Aggregates in the Network", http://citeseer.ist.psu.edu/, 2001.
[16] Park, Kihong; Lee, Heejo, "Effectiveness of Route-Based Packet Filtering for DDoS Attack Prevention", http://citeseer.ist.psu.edu/, 2001.
[17] Schiller, Jochen, "Mobile Communications", Addison Wesley, ISBN: 0-321-12381-6, Sider: 416, 2003.
[18] Sivertsen, Tormod, FFI, "Internettstudien (PowerPoint)", 2006.
[19] Sivertsen, Tormod; Nystuen, Kjell Olav; Windvik, Ronny, FFI, "Sårbarhetsstudie av Internett (PowerPoint)", 2006.
[20] Spilling, Pål; Johnsen, Ole-Arnt; Silkoset, Ove, Scandpower AS, "Sårbarhet og beredskap relatert til Internett", 2000.
[21] Steetskamp, I.; A.J.M. van Wijk, "STROOMLOOS: Vulnerability of the society, impacts of disturbances in elect.", , ISBN: 90-346-311-76, Sider: 263, 1994.
[22] Sørensen, Frode, "Innføring i nettverk", IDG Norge Books, ISBN: 82-7772-284-2, Sider: 485, 2004.
[23] Sørensen, Frode, "Moderne IP-nett", IDG Norge Books, ISBN: 82-7772-279-6, Sider: 464, 2004.
[24] Tormod K. Sivertsen, FFI, "Definisjon av målgruppe for Internettstudien (privat korrespondanse)", 2006.

[25] Østby, Eirik; Hagen, Janne; Nystuen, Kjell Olav, "Finansiering og organisering av beredskap innen telekom og kraftforsyning", FFI, FFI/RAPPORT-2000/00131, 2000.
[26] "Canadian Infrastructures and their Dependencies", National Contingency Planning Group, 2000.
[27] "Critical Infrastructure", ATIS Committee T1A1, http://www.atis.org/, Sist besøkt 04.05.2006.
[28] "DHS Faces Challenges in Fulfilling Cybersecurity Responsibilities", Government Accountability Office, GAO-05-434, 2005.
[29] "EDGE", Tech FAQ, http://www.tech-faq.com/edge.shtml, Sist besøkt 05.05.2006.
[30] "Electronics Research Group: Naming and Addressing", University of Aberdeen, http://www.erg.abdn.ac.uk/, Sist besøkt 04.05.2006.
[31] "FAQ", NORID, http://www.norid.no/domeneregistrering/faq.html, Sist besøkt 05.05.2006.
[32] "Forvaltningsmodellen for .no i korte trekk", NORID, http://www.norid.no/bakgrunn/forvalt-oversikt.html, Sist besøkt 05.05.2006.
[33] "Hjemmeside", Post- og teletilsynet, http://www.npt.no/, Sist besøkt 04.05.2006.
[34] "Hjemmeside", Enigma M4 Message Breaking Project, http://www.bytereef.org/m4_project.html, Sist besøkt 04.05.2006.
[35] "Hjemmeside", Amsterdam Internet Exchange, http://www.ams-ix.net/, Sist besøkt 04.05.2006.
[36] "Hjemmeside", Government Accountability Office, http://www.gao.gov/, Sist besøkt 04.05.2006.
[37] "Hjemmeside", Asia Homeland Security, http://www.safetysecurityasia.com.sg/ahs/home.html, Sist besøkt 04.05.2006.
[38] "Hjemmeside", Department of Homeland Security, http://www.dhs.gov/, Sist besøkt 04.05.2006.
[39] "Hjemmeside", Forsvarets Forskningsinstitutt, http://www.ffi.no/, Sist besøkt 23.05.2006.
[40] "HSDPA", UMTSWorld, http://www.umtsworld.com/technology/hsdpa.htm, Sist besøkt 05.05.2006.
[41] "Information Infrastructure", Labour Telematics Centre, http://www.christlinks.com/glossary2.html, Sist besøkt 05.05.2006.
[42] "International Organization for Standardization", International Organization for Standardization, http://www.iso.ch/, Sist besøkt 04.05.2006.
[43] "Kwetsbaarheid van het Internet (KWINT)", Stratix/TNO-FEL, http://www.tno.nl/, 2001.
[44] "Møte med BAS5-ROS 22.03.2006 (PowerPoint)", SEROS, 2006.
[45] "Nettverket vårt", TDCSong, http://tdcsong.no/, Sist besøkt 05.05.2006.
[46] "NIX homepage", Universitetet i Oslo, http://www.uio.no/nix/, Sist besøkt 05.05.2006.
[47] "Referat fra møte nr 7 i Internettgruppen", Post- og teletilsynet, http://www.npt.no/, 17.01.2006.
[48] "SETI@HOME", UC Berkeley, http://setiathome.berkeley.edu/, Sist besøkt 04.05.2006.
[49] "Technology", WiMAX Forum, http://www.wimaxforum.org/technology, Sist besøkt 05.05.2006.
[50] "The CORAS Project", The CORAS Consortium, http://coras.sourceforge.net/, Sist besøkt 11.05.2006.
[51] "The reliability of the Netherlands Internet: Consequences and measures", Stratix/TNO-FEL, http://citeseer.ist.psu.edu/664007.html, 2000.
[52] "Virksomheten", NextGenTel, http://www.nextgentel.no/nextgentel/virksomheten/, Sist besøkt 05.05.2006.
[53] "WISI 2006", Intelligence and Security Informatics, http://isi.se.cuhk.edu.hk/index.htm, Sist besøkt 04.05.2006.

8 Vedlegg

A. Modell for nettverk og teknologi på Internett i Norge
B. ISPer tilknyttet NIX

Vedlegg A: Modell for nettverk og teknologi på Internett i Norge



Vedlegg B: ISPer tilknyttet NIX, hentet fra [46]

Navn	**Peering-informasjon**	**IP-adresse på NIX1**	**IP-adresse på NIX2**	**AS-nummer på NIX**
UNINETT	http://www.uninett.no/info/uninett/samtrafikk	193.156.90.1	193.156.120.1	224
Telenor	peering@telenor.net	193.156.90.2	193.156.120.2	2119
Catch Communications AS	peering@catch.no	193.156.90.3	193.156.120.3	2116
Tele2 Norge AS	peering@tele2.no	193.156.90.4	193.156.120.4	1257
Infostream Services AS	nettdrift@infostream.no	193.156.90.5		3293
PowerTech Information Systems AS	peering@powertech.no	193.156.90.6	193.156.120.6	5381
Equant	peering@equant.com	193.156.90.7		2874
ErgoGroup	peering@ergo.no	193.156.90.8	193.156.120.8	5619
AT&T Global Network	peering@attglobal.net	193.156.90.9		2686
BaneTele AS	peering@banetele.net	193.156.90.10	193.156.120.10	3307
		193.156.90.11		
alfaNETT		193.156.90.12		8394
Telenor Mobil AS	lirmaster-mobil@telenor.com	193.156.90.13		8786
Whitebird New Media AS	peering@newmedia.no	193.156.90.14		9173
Netpower	peering@netpower.no	193.156.90.15		8896
TDC	peering@tdc.dk	193.156.90.16	193.156.120.16	3292
Bergen Nett og Media as	http://peering.bgnett.no/	193.156.90.17		6709
UPC Broadband	peering@aorta.net	193.156.90.18 193.156.90.70		6830
		193.156.90.19		

UUNET Norge AS	peering@mci.com	193.156.90.20		702
Song Networks AS	peering@sn.net	193.156.90.21	193.156.120.21	3246
Domeneshop AS	peering@domeneshop.no	193.156.90.22	193.156.120.22	12996
NetCom GSM AS	nix-ops@netcom.no	193.156.90.23		12929
DataGuard AS	http://www.dataguard.no/peering/	193.156.90.24		13069
		193.156.90.25		
		193.156.90.26		
Ementor AS	nix-peering@comace.net	193.156.90.27		13243
EDB Teamco	peering.tco@edb.com	193.156.90.28		15688
Priority Telecom	peering@prioritytelecom.no	193.156.90.29	193.156.120.29	13646
Saunalahti Group Oyj / EUnet Finland	peering@eunetip.net	193.156.90.30		6667
NextGenTel AS	driftssenter@nextgentel.com	193.156.90.31	193.156.120.31	15659
Broadnet Norge AS	peering@broadnet.no	193.156.90.32	193.156.120.32	25351
COLT	peering@colt.net	193.156.90.33		8220
MIMER AS	nix@mimer.no	193.156.90.34		15765
		193.156.90.35		
Net Fonds ASA	hostmaster@netfonds.no	193.156.90.36		21201
SSC Networks Norge AS	noc@ssc.net	193.156.90.37		16186
EasyNet AS	nix-ops@easynet.no	193.156.90.38		16065
Utfors AS	peering@telenor.se	193.156.90.39	193.156.120.39	8434
INN AS	lir@inn.no	193.156.90.40		16180
ID Comnet	peering@idcomnet.no	193.156.90.41		13212
		193.156.90.42		
		193.156.90.43		
		193.156.90.44		

		193.156.90.45		
Bredbandsbolaget	peering@bredband.com	193.156.90.46		8642
IT Connect AS	peering@itconnect.no	193.156.90.47		16175
Schibsted ASA	nix-ops@schibsted.com	193.156.90.48	193.156.120.48	21171
WAN Norge AS	noc@wan.no	193.156.90.49		21119
NRK	peering@nrk.no	193.156.90.50		21293
		193.156.90.51		
NC-Systems AS	peering@smarti.no	193.156.90.52		15560
Direct Connect AS	drift@directconnect.no	193.156.90.53		29300
Teleglobe	peering@teleglobe.net	193.156.90.54		6453
Registrar AS	peering@registrar.no	193.156.90.55		29517
IP-Only	peering@ip-only.net	193.156.90.56		12552
Workzone AS	peering@workzone.no	193.156.90.58		31005
Bredbåndsallian sen	05123@bkk.no	193.156.90.59		30950
Stim Computing AS	hostmaster@stim.no	193.156.90.60	193.156.120.60	31264
Smartcall ASA	peering@smartcall.no	193.156.90.61		25400
Ventelo Norge AS	peering@ventelo.no	193.156.90.62		6844
Labs2	peering@labs2.com	193.156.90.63		29518
DCS	peering@dcs.net	193.156.90.64		21202
FastHost AS	peering@fasthost.no	193.156.90.65	193.156.120.65	31283
Lyse Tele AS	nix-ops@lyse.no	193.156.90.66		29695
Port80 AB	noc@p80.net	193.156.90.67		16150
Basefarm AS	peering@basefarm.no	193.156.90.68	193.156.120.68	25148
nianet a/s	noc@nianet.dk	193.156.90.69		31027
RBnet AS	peering@rbnet.no	193.156.90.71		30737
Oslo ISP DA	peering@osloisp.no	193.156.90.72		39783