«Spaceflight will never tolerate carelessness, incapacity, and neglect. Somewhere, somehow, we screwed up. It could have been in design, build, or test.

Whatever it was, we should have caught it.

We were too gung ho about the schedule and we locked out all of the problems we saw each day in our work.»

(Gene Kranz - NASA Chief Flight Director)






Trusselbildet – hvordan jobbe med det og hvorfor?

– samfunnets og rikets sikkerhet

Storm Jarl Landaasen
Head Of Intelligence |Telenor Norge

All the business of war, and indeed all the business of life,
is to endeavour to find out what you don't know by what you do;
that's what I called «guessing what was at the other side of the hill.»
Arthur Wellesley, 1st Duke of Wellington

Telenor Norge

Eier og forvalter:
- Den ene av to *sivile* samfunnskritiske digitale nasjonale transportnettinfrastrukturer

Har
- Skjermingsverdige objekter

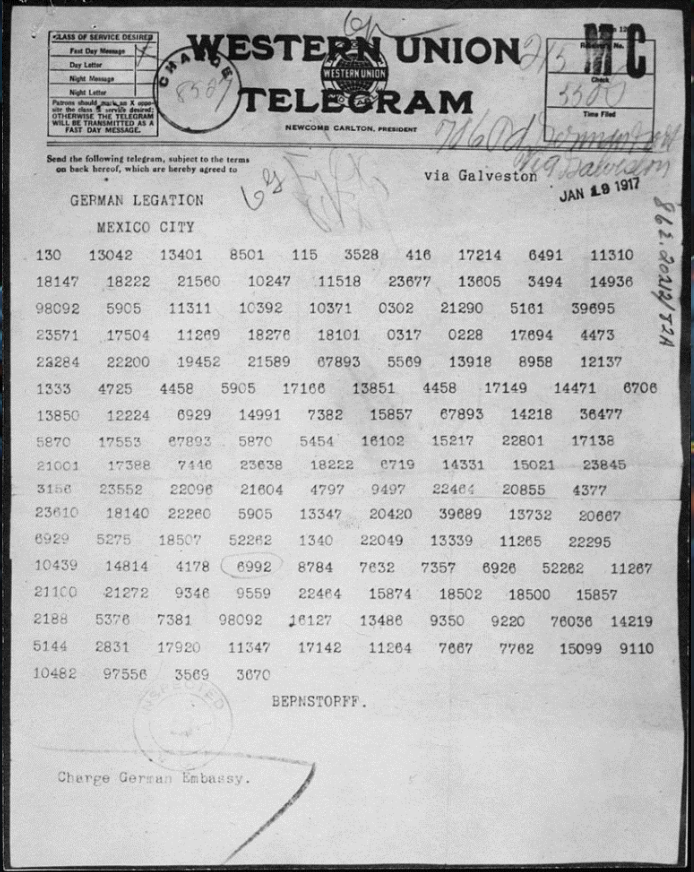
Transporterer:
- 80% av all datatrafikk i Norge

Operations
- – Network Operations Centre (NOC) 24/7/365:

Security:
- Både stopper stopper og leter – men bare i egen infrastruktur

Regulert sikkerhetsmessig:
- Sikkerhetsloven
- Ekomloven

…lenge før Internet og Snowden



CLASS OF SERVICE DESIRED
Fast Day Message
Day Letter
Night Message
Night Letter
Patrons should mark an X opposite the class of service desired; OTHERWISE THE TELEGRAM WILL BE TRANSMITTED AS A FAST DAY MESSAGE.

WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Receiver's No.
Check
Time Filed

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

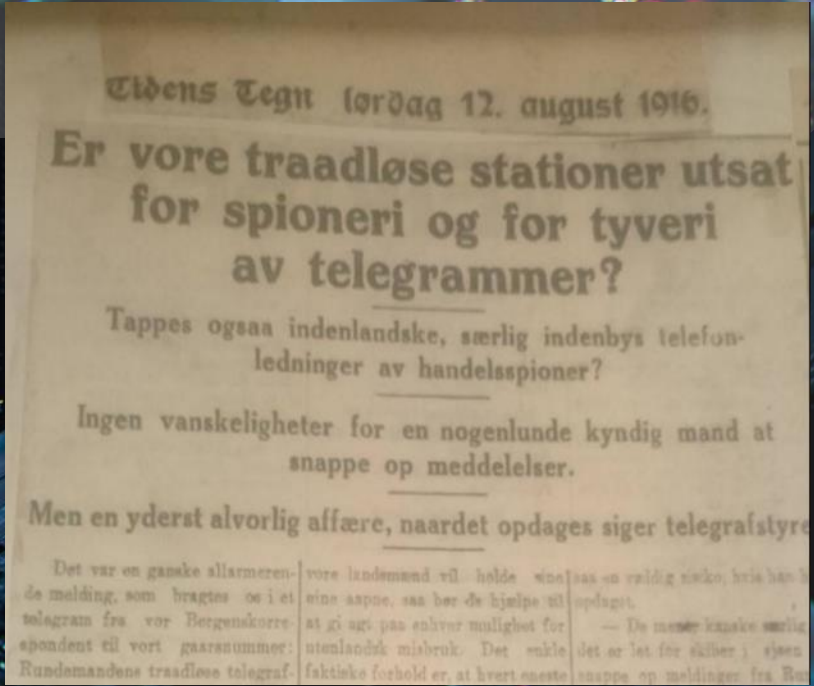
GERMAN LEGATION

MEXICO CITY

130	13042	13401	8501	115	3528	416	17214	6491	11310
18147	18222	21560	10247	11518	23677	13605	3494	14936	
98092	5905	11311	10392	10371	0302	21290	5161	39695	
23571	17504	11269	18276	18101	0317	0228	17694	4473	
22284	22200	19452	21589	67893	5569	13918	8958	12137	
1333	4725	4458	5905	17166	13851	4458	17149	14471	6706
13850	12224	6929	14991	7382	15857	67893	14218	36477	
5870	17553	67893	5870	5454	16102	15217	22801	17138	
21001	17388	7446	23638	18222	6719	14331	15021	23845	
3156	23552	22096	21604	4797	9497	22464	20855	4377	
23610	18140	22260	5905	13347	20420	39689	13732	20667	
6929	5275	18507	52262	1340	22049	13339	11265	22295	
10439	14814	4178	6992	8784	7632	7357	6926	52262	11267
21100	21272	9346	9559	22464	15874	18502	18500	15857	
2188	5376	7381	98092	16127	13486	9350	9220	76036	14219
5144	2831	17920	11347	17142	11264	7667	7762	15099	9110
10482	97556	3569	3670						

BEPNSTOPFF.

Charge German Embassy.



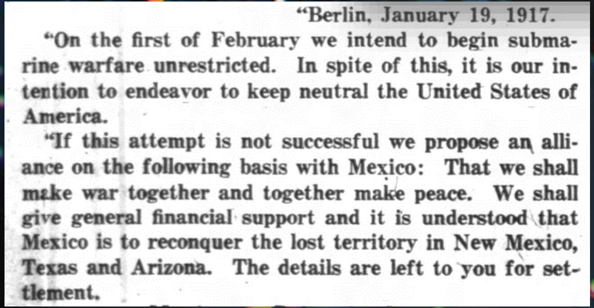
Tidens Tegn lørdag 12. august 1916.

Er vore traadløse stationer utsat for spioneri og for tyveri av telegrammer?

Tappes ogsaa indenlandske, særlig indenbys telefonledninger av handelsspioner?

Ingen vanskeligheter for en nogenlunde kyndig mand at snappe op meddelelser.

Men en yderst alvorlig affære, naardet opdages siger telegrafstyre



"Berlin, January 19, 1917.

"On the first of February we intend to begin submarine warfare unrestricted. In spite of this, it is our intention to endeavor to keep neutral the United States of America.

"If this attempt is not successful we propose an alliance on the following basis with Mexico: That we shall make war together and together make peace. We shall give general financial support and it is understood that Mexico is to reconquer the lost territory in New Mexico, Texas and Arizona. The details are left to you for settlement.

Livsviktig sikkerhetsarbeid

Vi lever i en verden hvor trusselbildet er i stadig endring og trusselaktørene er mer avanserte enn tidligere. Angriperne er internasjonale, ressurssterke aktører som ofte har lange operasjonslinjer og kan angripe hvem som helst. Når dette skrives, er det irske helsevesenet på fjerde døgnet sterkt rammet av et alvorlig dataangrep.

Gro Jære
Administrerende direktør
Sykehuspartner HF

telenor

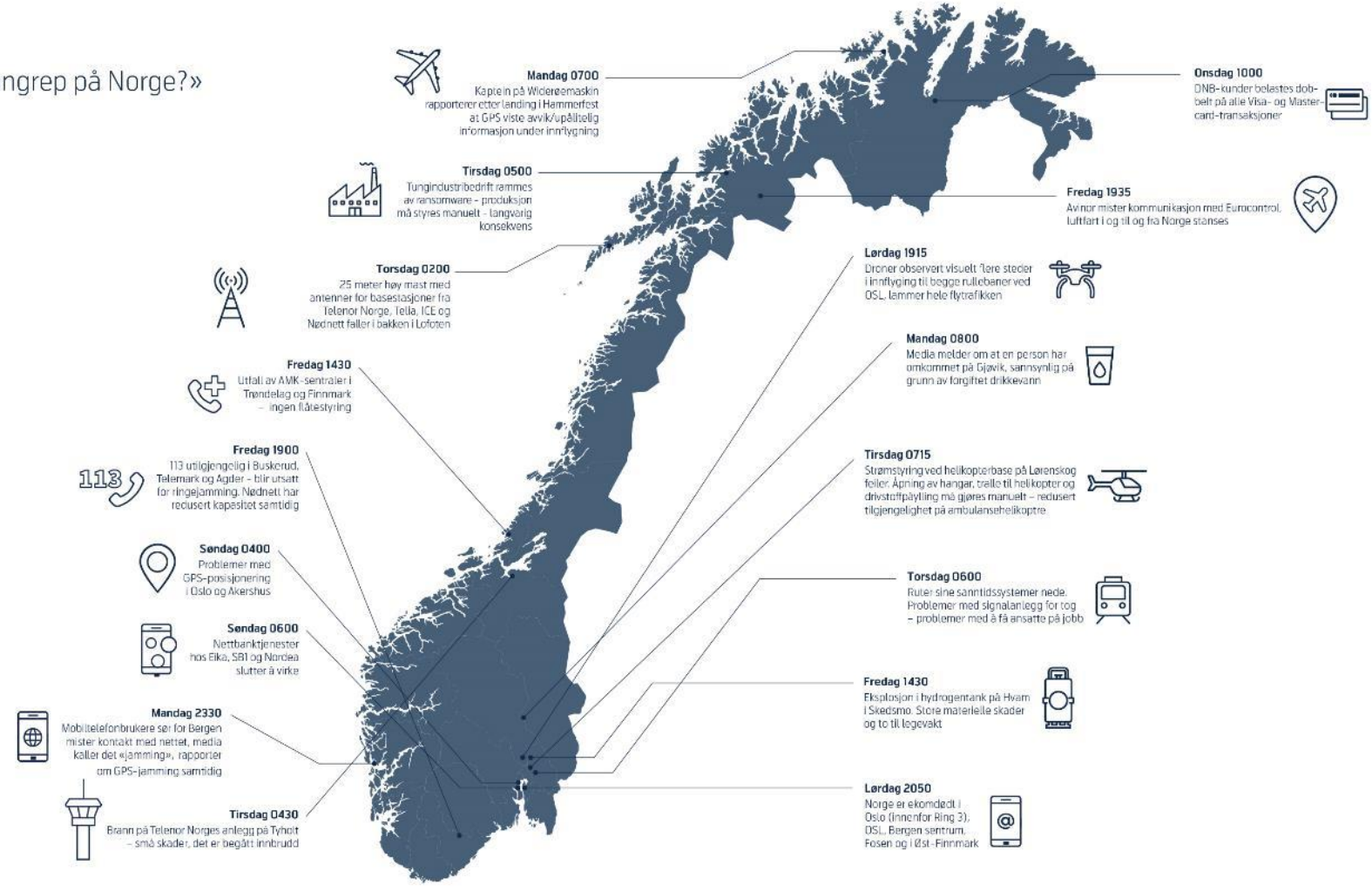
Angrepet på Østre Toten kommune

Natt til 9. januar 2021 ble Østre Toten kommune rammet av et hackerangrep på våre datasystemer. Dette ble oppdaget på omsorgssenteret vårt umiddelbart og på morgenen ble det raskt klart at alle våre systemer var nede og kommuneledelsen satte krisestab. Hackerne hadde på forhånd forberedt angrepet inne på våre systemer slik at de denne natta kunne låse oss ned. De lastet over våre data til seg og slettet våre **backuper**. Vi våknet opp til en ny dag denne morgenen der internett og fagsystemer ikke var tilgjengelige. Det var svarte skjermer rundt i tjenestene våre.

Bror Helgestad
Ordfører
Østre Toten kommune

telenor

«Et angrep på Norge?»



Når nettene blir lange del 2 – et faglig dypdykk:

Leveransekjeder – en kjent risiko som krever bevisste valg

Er leveransekjederisiko noe vi aktivt tar stilling til og er det en del av virksomhetens risikodiskusjoner? Er digital sikkerhet og leveransekjeder så krevende at ledere og beslutningstagere ikke evner å gå inn i diskusjonene? I **når nettene blir lange del 2** vil vi gå mer teknisk til verks for å vise at teknologikunnskap i samspill med kunnskap om hvordan teknologi kan utnyttes er viktig for å kunne ta bevisste valg. Det siste året har bydd på rikelig med eksempler på leveransekjedeangrep.

telenor

Vi måtte begynne å tenke det utenkelige

Trusselforståelse

Falske nyheter, angrep på demokratiet, verdikjedeangrep, digital opprustning, **ransomware** - det er vår nye hverdag. Det har aldri vært viktigere å forstå trussel-aktørene for å forstå hvordan vi skal sikre oss. Trusselaktører på jakt etter digital informasjon som kan stjeles, endres eller gjøres utilgjengelig, opererer ikke bare digitalt; et av trusselaktørens virkemidler kan være en kollega eller en konsulent.

Fra gammeldags security til security med INTEL-metoder for å forstå motstanderen

telenor

Etterretning = beslutningsstøtte

Arthur Wellesley, 1st Duke of Wellington
All the business of war, and indeed all the business of life, is to endeavor to find out what you don't know by what you do; that's what I called «guessing what was at the other side of the hill.»

Med andre ord:

- For å være i stand til å forstå og forutsi dine fienders oppførsel du må forstå hva du ikke vet
- For å forstå hvordan din fiende vil handle du må forstå hans kapasitet, kapabilitet, intensjon og *hans* ønskede slutt-tilstand for *sin* operasjon
- En trussel foreligger når *noen* har kapasitet, evner, motiv og en slutt-tilstand han ønsker å oppnå for *sin* operasjon

Vesentlige fasetter i E-terori: Secrets, mysteries and complexity?

- Secrets/hemmeligheter er informasjon som er kjent for noen, altså fakta, men som den samme *noen* ønsker å holde skjult for andre
- Mysteries/mysterier er informasjon som er ukjent, ofte fordi de som har informasjonen ikke har besluttet hvorledes de kommer til å benytte den eller respondere på et gitt sett hendelser
- Complexity/kompleksitet er det som kan bli resultatet av motstanderens handlemåte og intensjon – hans ønskede sluttsituasjon

telenor

Trusselbildet – en del av risikostyringen

Trendbildet

Endrede ramme-faktorer: Teknologi, vær, regulatorisk …

Sårbarhets-bildet

Sårbarheter i virksomhet som kan *utnyttes* av trusselaktør eller *utløses* av en eller flere årsaker/hendelser som eks. vær og vind, teknisk feil, menneskelig svikt, …

Trusselbildet

Ondsidnnede villede handlinger «Hostile intent»

- Skal gjøre organisasjonen bedre forberedt til å handle og forberede seg på mulige kommende hendelser, ikke bare reagere når hendelsen inntreffer
- **Arbeid med trusselbildet baseres på:**
  - Offisielle trusselbilder
  - Eget sårbarhetsbilde
  - Eget trendbilde
  - Åpne kilder - OSINT
  - Egne data i egne systemer
  - Dialog med kunder og partnere
  - …
- **Arbeidsfaser**
  - Etterretningsdialog
  - Styring (direction): Gitt i E-dialogen og følges så opp med påfølgende utledning av SIR/EEI – ledes av E-sjef
  - Innhenting (collection) – på bakgrunn av resulatat av e-dialog og styrings-steget; hente inn informasjon
  - Bearbeiding (processing) – produksjon og ferdigstilling
  - Fordeling (dissemination) – presentasjon og distribusjon

telenor

Innsidetrusselen

Han er sjarmerende og høflig...

Hun er elegant og har dyre smykker...

Begge er på konferanse; han som «deltaker» hun som «bartender» - begge har sannsynlig lønn fra en annen arbeidsgiver enn den som oppgis i skatteseddelen.

De beste i klassen bruker ikke malware…

telenor

Uansett: Beredskapen avgjør når det smeller

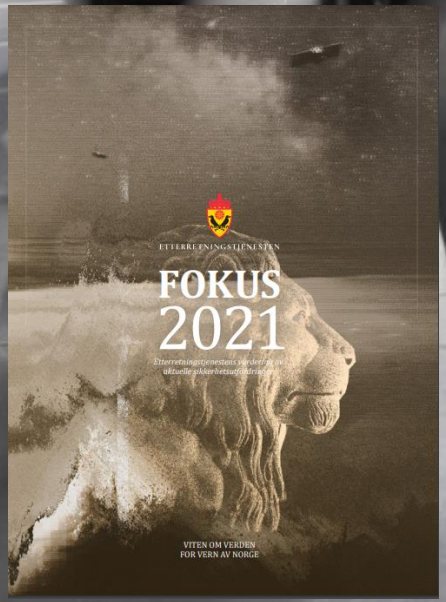
Forutsi, detektér, håndter, normaliser, lær, repetér

Forbered for analoge og digitale stormer

Tren organisasjonen på sosial manipulering

Du må ha kunnskap, beredskap og risikostyring
Det finnes ingen «silver bullet»

telenor



Samfunnssikkerheten under angrep

Vi har lagt bak oss et år med avanserte operasjoner mot både virksomhetsverdikjeder og demokrati. Avanserte aktører fortsette å utnytte enhver svakhet og sårbarhet og vi må erkjenne at samfunnssikkerheten, statssikkerheten og borgernes trygghet trues. Vi må ta bevisste valg om hva vi aksepterer av risiko og hva vi må gjøre noe med.

Foto: Ekaly / E+ / Getty Images

Telenor Norge legger til grunn:

De mest avanserte trusselaktørene Telenor Norge, våre kunder og andre totalforsvarsaktører står overfor har ikke noe krav på seg til å tjene penger; de skal tjene nasjonen de representerer og ikke en økonomisk bunnlinje.

Slike avanserte aktører har lange tidslinjer i sine operasjoner (måneder og år) og de ønskede effektene av operasjonene kan være svært langsiktige, slik som eksempelvis SolarWinds-operasjonen.

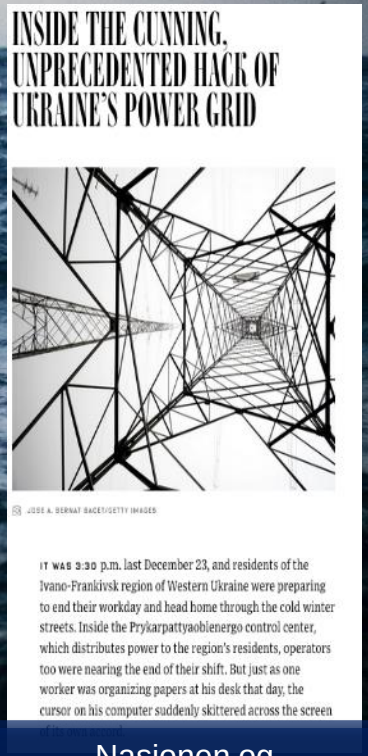
- Hybride operasjoner pågår; privat infrastruktur brukes til å utføre cyberoperasjoner, informasjonsoperasjoner og påvirkningsoperasjoner.
- Fremmed etterretning, spesielt russisk og kinesisk som E og PST fremhever, ønsker å drive etterretnings-, påvirknings- og informasjonsoperasjoner mot Telenor Norge og våre kunder.
- Som totalforsvarsaktør vil vi bli forsøkt utnyttet og utsatt for målrettede etterretningsoperasjoner.
- Avanserte trusselaktører bruker kombinasjoner av handlemåter for å oppnå sine intensjoner; både teknologiske og menneskelige, fysiske og logiske.
- Fremmed etterretning vil forsøke å misbruke tjenester hvis de finner det formålstjenlig. • Fremmed etterretning ønsker meget sannsynlig å benytte statssponsede organisasjoner og organiserte kriminelle miljøer, i tillegg til egen kapasitet, for å drive cyberoperasjoner mot Telenor Norge og enkelte av Telenor Norges kunder.
- Avanserte aktørers ønske om å rekruttere innsideaktører er økende.
- Telenor Norge og våre kunder vil bli utsatt for aktører som benytter utpressing som virkemiddel, både i forbindelse med DDoS og med å ønske å ta kontroll over informasjon ved å benytte ransomware.
- Direktørsvindel vil bli enda mer spisset og målrettet, kriminelle miljøer vil fortsette å utnytte teknologi og avansert manipulering for å få tilgang til e-postsystemer (BEC).
- Helt nye angrepsformer vil sannsynlig komme etter hvert som IoT-utviklingen virkelig skyter fart og kriminelle miljøer også på dette området kan «arve» metoder fra statlige aktører.
- Store hendelser i samfunnet slik som for eksempel store russiske militærøvelser eller øvelser der NATO-land øver i Norge vil kunne medføre økt aktivitet fra fremmede stater og kriminelle miljøer som kan påvirke Telenor Norge.
- Hacktivisme pågår, men fenomenet har blitt mye mindre synlig.
- Ekstreme grupperinger av alle politiske valører er avhengig av kommunikasjon, men ikke en stor trussel i cyberspace.

telenor

Vi trenger: Felles situasjons- og konsekvensforståelse

Forsvarbarhet

Kommando&kontroll



INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID

JOSE A. BERNAT BACETI/GETTY IMAGES

IT WAS 3:30 p.m. last December 23, and residents of the Ivano-Frankivsk region of Western Ukraine were preparing to end their workday and head home through the cold winter streets. Inside the Prykarpattyaoblenergo control center, which distributes power to the region's residents, operators too were nearing the end of their shift. But just as one worker was organizing papers at his desk that day, the cursor on his computer suddenly skittered across the screen

Nasjonen og virksomhetene

Up Guards and at them again

Arthur Wellesley, 1st Duke of Wellington

Sikkerhet er ikke valgfag og det går ikke over!

«Det er imidlertid ikke nok at vi snakker om det. Vi må også ta bevisste valg og gjennomføre det vi må for å beskytte oss.»

Hanne Tangen Nilsen – Sikkerhetsdirektør bedriftsmarked – Telenor Norge

telenor