

KODER.

Det er selvsagt fint å kunne sende meldinger uten at motstanderen kan lese dem, det gir økt sikkerhet. Men man må også selv enkelt kunne motta og dekode meldingene, slik at meldingene har sin verdi i behold innenfor de knappe tidsrammer, som for eksempel en strid gir.

Hvordan man koder, er selvsagt avhengig av hvilke forsendelses måter man kan bruke og tiden til rådighet. Er koden og verktøyet til å tolke den gode, bruker dine egne kort tid på å tolke meldingen og motstanderen så lang tid på løse den at meningen og meldingen ikke lenger har noen verdi for motstanderen.

Meldingen: “Angrip ved Lilleby i morgen kl. tolv.” Tolkningen av denne meldingen for motstanderen har ingen verdi når det har gått to dager, hvis ikke tolkningen kan brukes til å tolke andre senere meldinger raskere. Så hvis motstanderen har løst og dekodet en melding, må ikke dette gi ham nok kunnskaper til å løse andre meldinger raskt og effektivt. For koder, tolkeverktøy og meldinger vil regelmessig bli funnet eller falle i motstanderens hender på andre måter. Dette er en av livets sikreste sannheter. Derfor må metoder, koder og utstyr regelmessig endres. Man må heller aldri starte eller avslutte meldinger på samme måte hver gang, egentlig alltid ha en ny start og en ny avslutning hver gang. Sjekk også alltid om motstanderens reaksjoner og meldinger kan skyldes at han leser dine koder. Det er selvsagt også viktig at dine meldinger og reaksjoner ikke avslører at du leser deres koder. Man skal heller ikke dele viktig informasjon eller planer med mange. Ja, folk som driver med koder er ofte en smule paranoide. Det tiltar med årene. Hvis du ønsker at motstanderen skal bli litt frustrert og ha mye å gjøre, kan du sende meldinger som bare er søppel. Det er også mulig å sende meldingene i en beholder, som ødelegger budskapet, hvis den blir åpnet på en gal måte. Ueksponert film i en lukket beholder er et eksempel på dette, som ble brukt av mange illegale virksomheter, også i Norge.

Måter for oversendelse.

Post, brevdUER eller ordonnans.

De gamle metodene for leveranse og gammeldags kodemetodikk var fortsatt i bruk, som for eksempel at hver tredje bokstav i meldingen ble satt sammen til den kodete meldingen eller at man la med tegn, som hadde en skjult betydning, eller at hele meldingen måtte bli tastet inn i kodetolkningsmaskin. En ny metode var at meldinger ble nedfotografert og skjult som for eksempel et punktum eller i et hulrom i forsendelsen. Eller at hele meldingen består av tall, som referer til side, linjenummer og ordnummer eller bokstavnummer i en bok, som både mottager og sender har en kopi av. Man har m.a.o. mange muligheter. Eller man blander sammen flere måter for å forvirre motstanderen eller gjøre tolkningen enda vanskeligere, som at første og siste delen av den reelle meldingen er fullstendig meningsløs eller at hele meldinger er det. Ved å bruke slike taktikker håper man at motstanderen gir opp å bruke en ervervet nøkkel.

Radio eller trådløst samband.

Radio kan brukes til å sende telegrammer og til samtale. Telegrammer kan selvsagt krypteres på samme måte som meldinger over post, glem fotografier og sære tegn.

Samtaler kan gjøres uforståelige ved å bruke språk, som ikke er allment forstått. USA brukte indianske språk under krigen i Stillehavet. Finnene blandet sammen finsk og svensk sammen med bruk av kallenavn under Vinterkrigen. Fordelen ved å bruke et eget språk er at mottageren raskt kan forstå meldingen, ulempen er at meldingen raskt kan tolkes av motstanderen, hvis denne forstår språket. Nå var det vel få japanere som var gode på indianske språk og få russere som var gode nok på både svensk og finsk. Det er også mulig å legge kodete samtaler oppe på en vanlig samtale over radio eller telefon, ved å modulere den kodete samtalen, slik at den går i en eller flere frekvenser, som ikke kan høres av det menneskelige øret.

Telegrafi eller telefon, såkalt fast samband.

I prinsippet er det ingen forskjeller fra radio. For man trenger ikke å koble seg til kabelen for å avlytte slikt samband, det er nok at man bruker en annen kabel eller spole med tråd i nærheten, som fanger opp de elektriske svingningene i kabelen. Så denne formen formkommunikasjonen bør også her være kodet, hvis kabelen ligger nær fienden eller det kan tenkes av fiendens soldater eller agenter kan oppholde seg i nærheten. Allerede under første verdenskrig var begrepet «i nærheten» en avstand på 100 meter. Denne avstanden økte utover århundret, så mannen i skyttergraven der borte kan høre hva du sier over din nedgravde telefonlinje.

Brukere av koder.

Selvfølgelig alle de fire våpengrenene, heimevernet, hær, marine og flyvåpen, men også diplomatiet, statsadministrasjonen, spioner og næringslivet er brukere.

Tolkere eller kodebrytere.

I hovedsak matematikere og folk med store språkkunnskaper. Briter og amerikanere brukte datamaskiner til kodebryting. Tyskerne var klar over at datamaskiner var fordelaktige i dette arbeidet, men de hadde ikke tilgang til slike i tilstrekkelig antall. Så britiske forskere hadde en fordel fordi de hadde tilgang til amerikanske datamaskiner i et stort antall, en fordel som de ikke klarte å utnytte før etter 1940, og da fortsatt i begrenset omfang og med varierende hell. Spesielt økte vanskelighetene når tyskerne utvidet antall kodehjul i sine Enigma kodemaskiner.

Hvem visste hva, når og hva brukte man?

Tyskerne baserte mange av sine meldinger på Enigma maskinen, som de regnet som sikker. Det beste med maskinen var at den kunne brukes i felt og at den var forholdsvis sikker fram til midten av 1941. I første rekke fordi tolkningen av de meldingene, som man klarte å løse, tok for lang tid. Etter 1941 begynte britene å tolke enkelte meldinger. Om lag 50.000 ble laget av denne maskinen.

I tillegg brukte tyskerne en del andre maskiner. G-skriveren eller Siemens & Halske T52, en slags kryptert fjernskriver. Koden ble brutt av både Sverige og Storbritannia. Rundt tusen stykker var i bruk innen strategisk nivå og diplomatiet. Tyskerne kunne også koble en Lorenz SZ40 eller SZ42 til den vanlige fjernskriveren for å kryptere meldingene. Færre en tusen ble lagd av disse, igjen kunne både Sverige og Storbritannia tolke meldingene.

Britene brukte en tilsvarende maskin til Enigma kalt Typex, de lagde rundt 5.000 av maskinen. Maskinen ble brukt på strategisk nivå og man tror ikke at koden ble brutt.

USA's militære brukte kodemaskinen M 209 på strategisk og operativt nivå. Man lagde 140.000 av maskinen. Koden ble etter hvert delvis lest av tyskerne. Maskinen var liten og behendig. I tillegg brukte de 10.000 Sigaba, også denne lik Enigma, på strategisk nivå innen hæren og på fartøyer innen marinen. Meldinger på denne maskinen ble ikke forstått av motstanderne.

USA diplomatiske koder var dårlige og meldingene ble forstått av Tyskland, Sverige, Storbritannia, Finland og Italia.

Tyskland konsentrerte mye av sine anstrengelser før krigen rundt tolking av kodemeldinger fra sine to antatt sterkeste motstandere, Frankrike og Storbritannia. Allerede i 1935 tolket de meldingene til det franske militæret, slik at de visste at innmarsjen i Østerrike og Rhinen området ikke ville bli møtt med angrep fra det franske forsvaret.

De kunne også i hovedsak tolke både den franske og britiske diplomatiske koden, hvilket er en del av forklaringene på München forliket og den senere okkupasjonen av Tsjekkoslovakia. Så Hitlers diplomatiske mesterstykker og dristige utenrikspolitikk på trettitallet er kanskje ikke så overraskende, målt opp mot denne bakgrunnen.

At de også kunne lese koden til den britiske marinen, sammen med dårlig vær og lavt skydekke, som hindret flyovervåking, forklarer hvorfor de praktisk talt uten uhell kunne opptre på den måten, som de gjorde i Nordsjøen i april 1940. De hadde et uhell og det var at den tyske krysseren «Hipper» ble oppdaget av den britiske destroyeren «Glowworm» utenfor Trondheim. Den britiske destroyeren hadde mistet en mann over bord i den grove sjøen og gikk tilbake i sin gamle kurs for å forsøke å finne vedkommende. Hvis vi antar at forespørselen om og tillatelsen til å gå tilbake ble sendt ved hjelp av lyssignaler, signalflagg eller høyfrekvent radio, hjelpemidler som ikke kunne fanges opp og tolkes av tyskerne, så kan dette være forklaringen på hvordan «Glowworm» kom overraskende på den tyske eskadren.

At en stor del av kodene til det franske militæret ble forstått, er og noe av forklaringen på hvorfor Tyskland nedkjempet Frankrike så raskt og stoppet alle franske motangrep i sin spede begynnelse i 1940. I tillegg kunne tyskernes B-dienst tolke hollandske og russiske meldinger fram til om lag 1943.

ETTERRETNING.

Tysk etterretning hadde de to første krigsårene den fordel at deres kodemaskiner var sikre. Etter hvert ble det snudd til en ulempe siden britene klarte med varierende hell å tolke disse kodemeldingene maskinelt.