FORSVARET

Cyberkrig og cyberforsvaret

Kapt. Jarle Kittilsen
INI OPS / BKI

FORSVARET

Agenda

- Cyberkrig - Hvorfor trenger vi et cyberforsvar?
  - Cybertrusler
  - Utvikling
  - Hendelser

- Forsvarets tilnærming til cyberforsvar.
  - Gammelt konsept
  - Nytt konsept

FORSVARET

Cyberkrig

Hvorfor trenger vi et cyberforsvar?

Vitale samfunnsfunksjoner blir i stigende grad avhengige av at kommunikasjonssystemer og datanettverk fungerer, og at verdifull og sensitiv informasjon kan beskyttes mot systemfeil, sabotasje og angrep.

Stater og andre aktører har allerede tatt i bruk datanettverk og informasjonsteknologi [...] Gjennom operasjoner i cyber vil ulike aktører kunne rette angrep mot kritisk samfunnsinfrastruktur, næringsliv, akademia, og myndigheter.

Forsvarssjefens fagmilitære råd, 2011

FORSVARET

Cyber

Fra gresk *Kybernét (es)*. - styrmann eller navigatør, *den som styrer*.

Cyberkrig - Cyberangrep

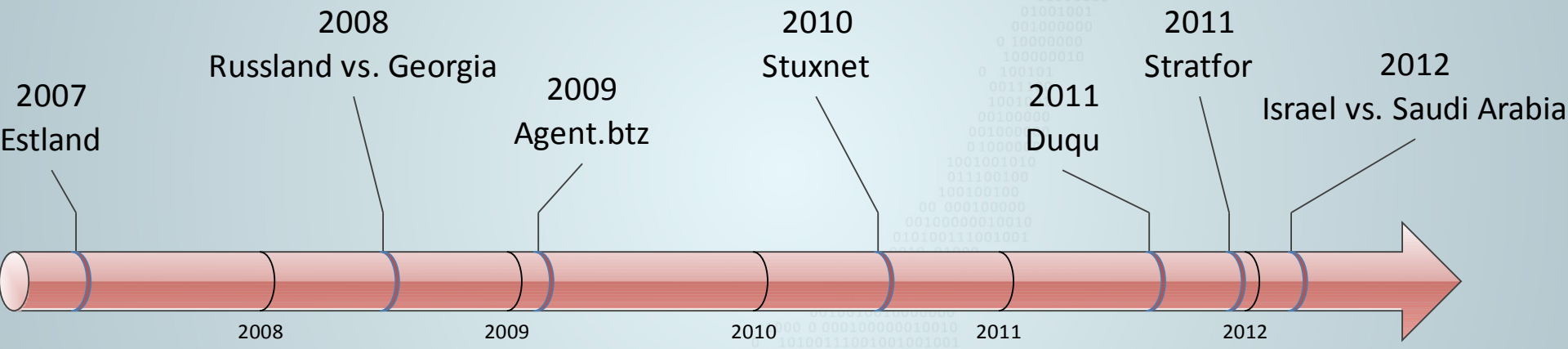
"The unauthorized penetration by, on behalf of or in support of, a government into another nation's computer or network, or any other activity affecting a computer system, in which the purpose is to add, alter or falsify data, or cause the disruption of or damage to a computer, or network device, or the objects a computer controls"

Richard A. Clarke (tidligere sikkerhetsrådgiver i det hvite hus)

Cyberkrig vs. Konvensjonell krig

FORSVARET

Oppsiktsvekkende cyberangrep



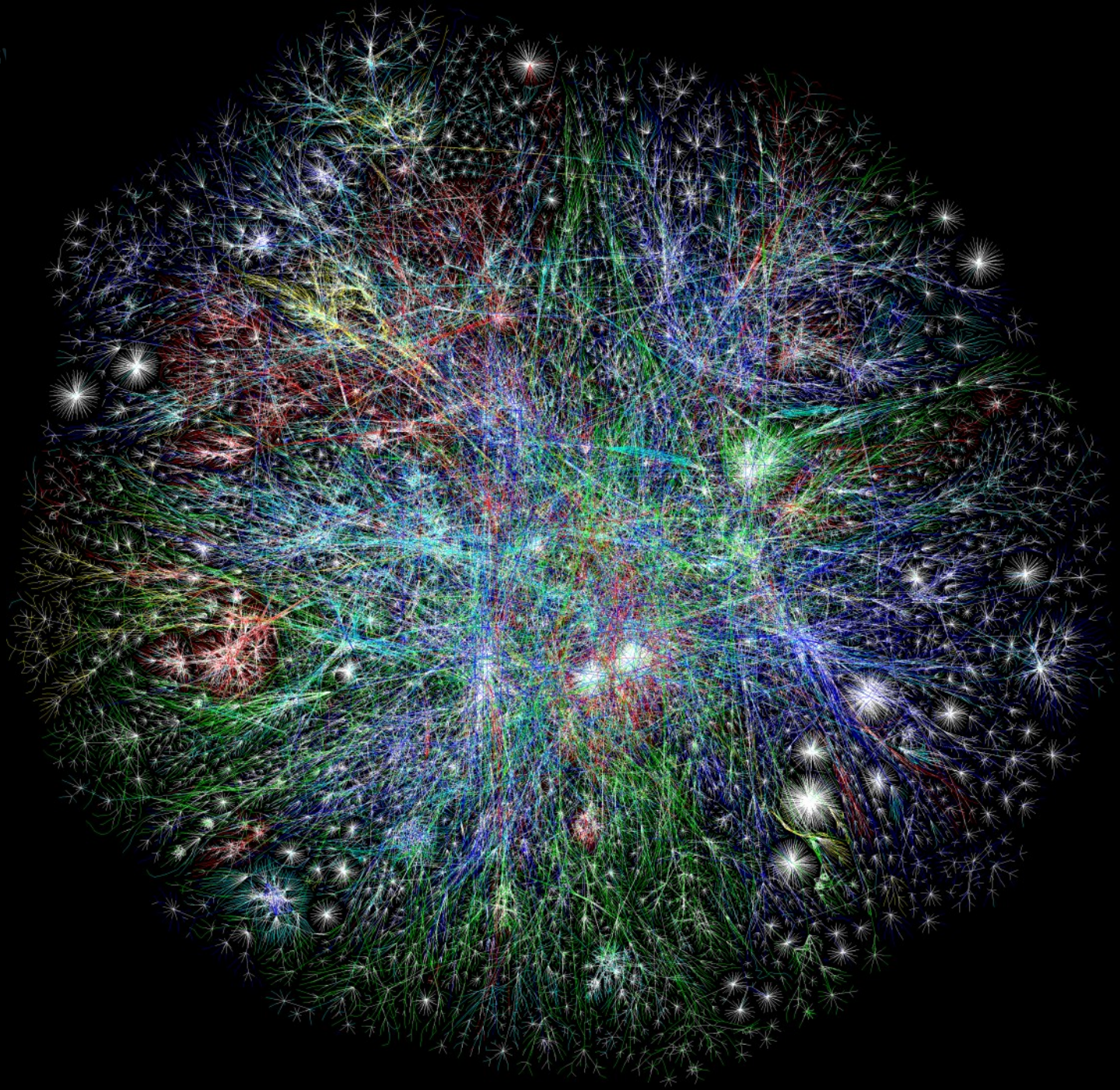
Cyberterrorisme

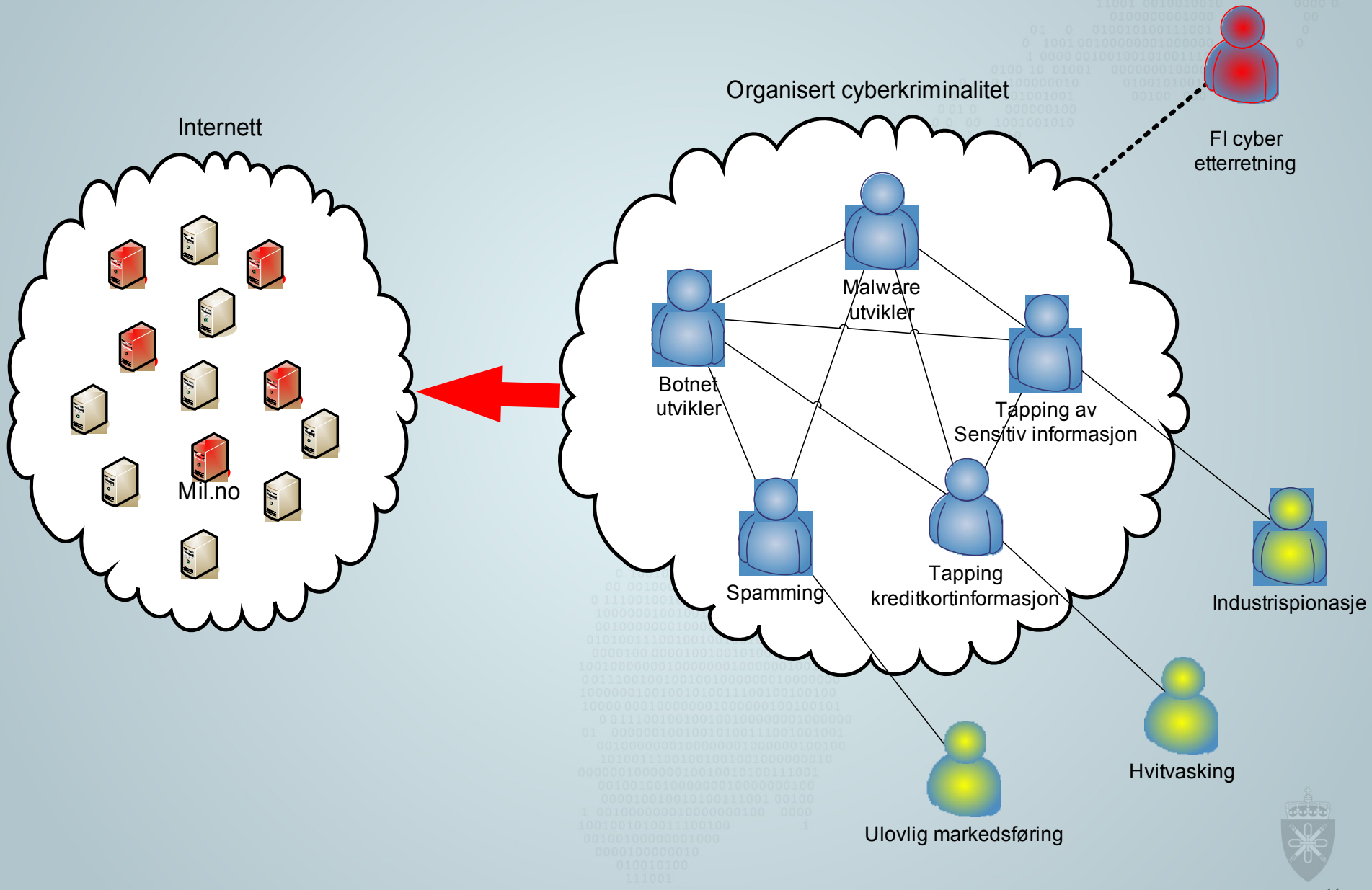
Cyberspionasje

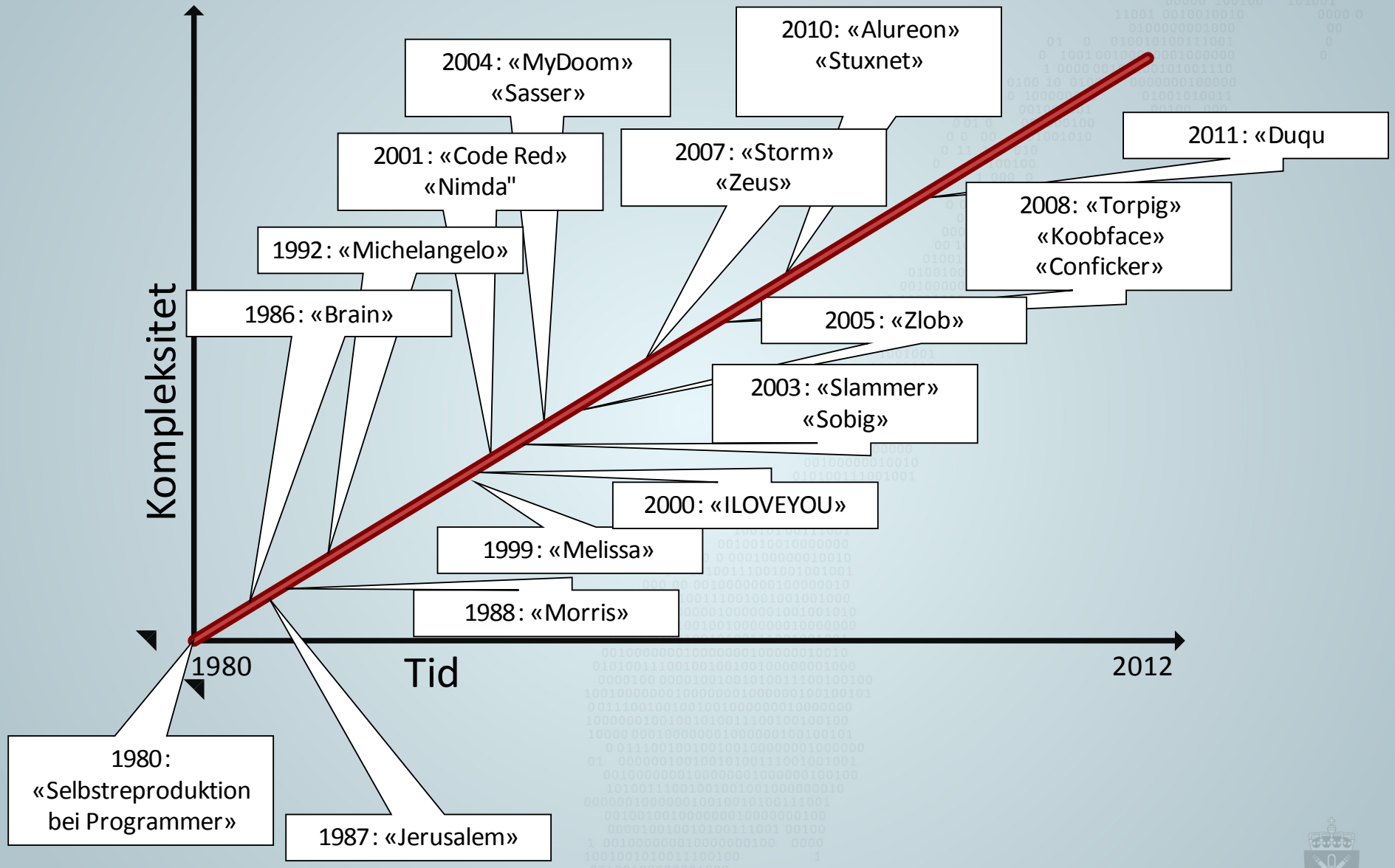
Cyberkrig

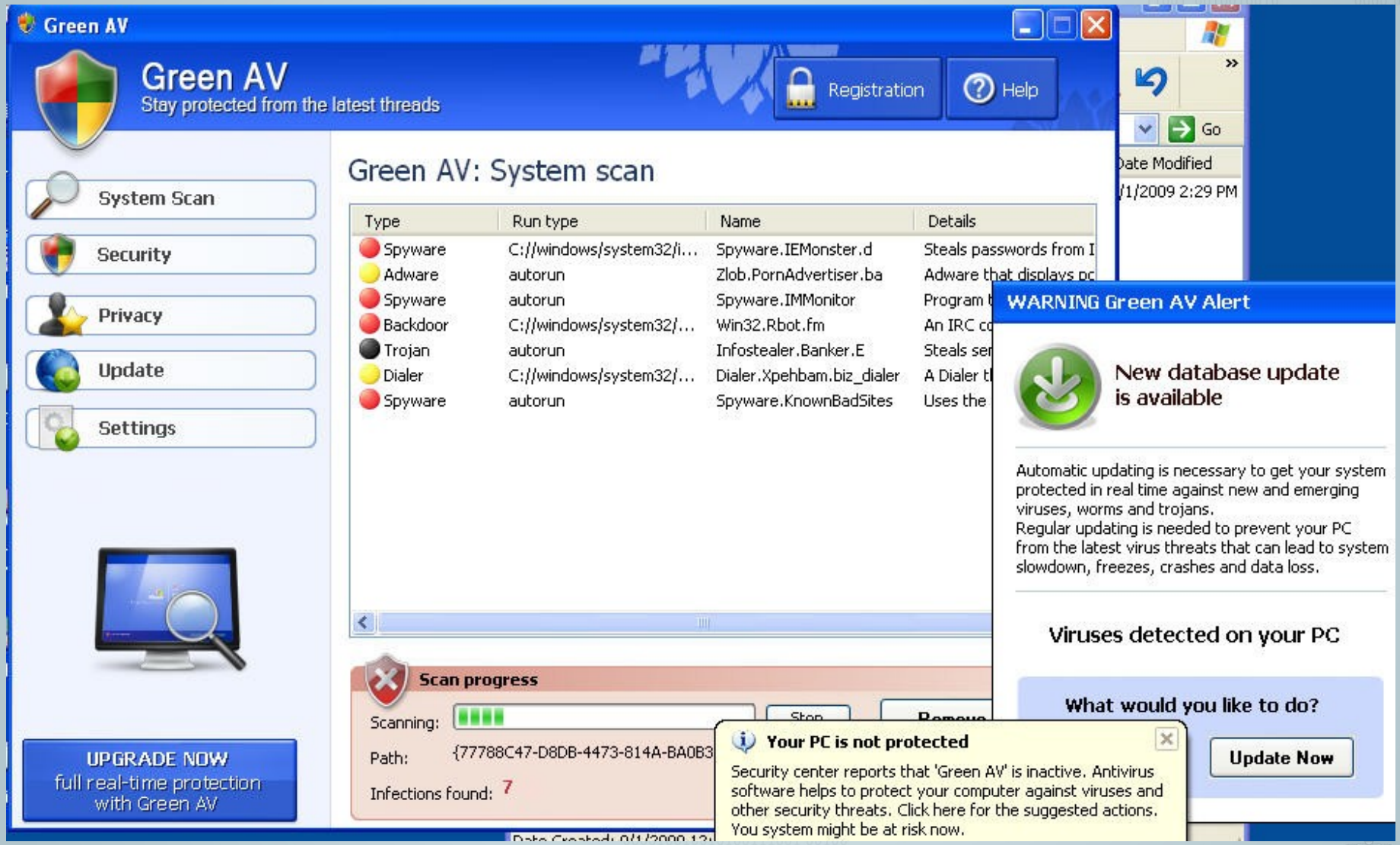
Cyberkriminalitet

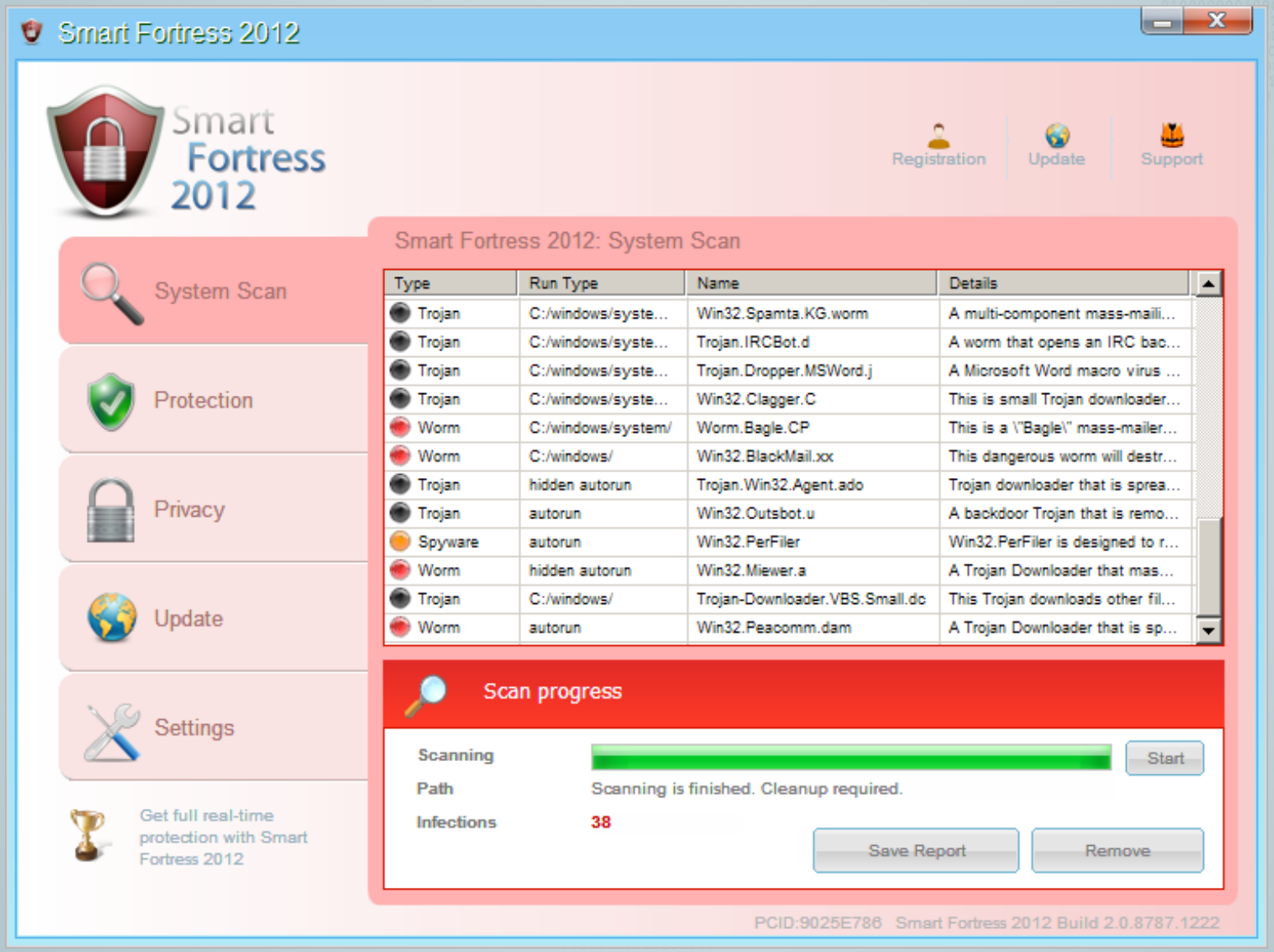
Hacktivisme




Internett
Mil.no
Organisert cyberkriminalitet
FI cyber etterretning
Malware utvikler
Botnet utvikler
Tapping av Sensitiv informasjon
Spamming
Tapping kreditkortinformasjon
Industrispionasje
Hvitvasking
Ulovlig markedsføring


Kompleksitet
Tid
1980
2012
1980: «Selbstreproduktion bei Programmer»
1986: «Brain»
1987: «Jerusalem»
1988: «Morris»
1992: «Michelangelo»
1999: «Melissa»
2000: «ILOVEYOU»
2001: «Code Red» «Nimda"
2003: «Slammer» «Sobig»
2004: «MyDoom» «Sasser»
2005: «Zlob»
2007: «Storm» «Zeus»
2008: «Torpig» «Koobface» «Conficker»
2010: «Alureon» «Stuxnet»
2011: «Duqu


Green AV
Green AV
Stay protected from the latest threads
Registration
Help
System Scan
Security
Privacy
Update
Settings
UPGRADE NOW
full real-time protection
with Green AV
Green AV: System scan
Type
Run type
Name
Details
Spyware
C://windows/system32/i...
Spyware.IEMonster.d
Steals passwords from I
Adware
autorun
Zlob.PornAdvertiser.ba
Adware that displays pc
Spyware
autorun
Spyware.IMMonitor
Backdoor
C://windows/system32/...
Win32.Rbot.fm
Trojan
autorun
Infostealer.Banker.E
Dialer
C://windows/system32/...
Dialer.Xpehbam.biz_dialer
Spyware
autorun
Spyware.KnownBadSites
Uses the
Scan progress
Scanning:
Path:
{77788C47-D8DB-4473-814A-BA0B3
Infections found: 7
Stop
Remove
Go
Date Modified
/1/2009 2:29 PM
WARNING Green AV Alert
New database update
is available
Automatic updating is necessary to get your system protected in real time against new and emerging viruses, worms and trojans.
Regular updating is needed to prevent your PC from the latest virus threats that can lead to system slowdown, freezes, crashes and data loss.
Viruses detected on your PC
What would you like to do?
Update Now
Your PC is not protected
Security center reports that 'Green AV' is inactive. Antivirus software helps to protect your computer against viruses and other security threats. Click here for the suggested actions.
You system might be at risk now.


Smart Fortress 2012
Smart Fortress 2012
Registration
Update
Support
System Scan
Protection
Privacy
Update
Settings
Get full real-time protection with Smart Fortress 2012
Smart Fortress 2012: System Scan
Type | Run Type | Name | Details
Trojan | C:/windows/syste... | Win32.Spamta.KG.worm | A multi-component mass-maili...
Trojan | C:/windows/syste... | Trojan.IRCBot.d | A worm that opens an IRC bac...
Trojan | C:/windows/syste... | Trojan.Dropper.MSWord.j | A Microsoft Word macro virus ...
Trojan | C:/windows/syste... | Win32.Clagger.C | This is small Trojan downloader...
Worm | C:/windows/system/ | Worm.Bagle.CP | This is a \"Bagle\" mass-mailer...
Worm | C:/windows/ | Win32.BlackMail.xx | This dangerous worm will destr...
Trojan | hidden autorun | Trojan.Win32.Agent.ado | Trojan downloader that is sprea...
Trojan | autorun | Win32.Outsbot.u | A backdoor Trojan that is remo...
Spyware | autorun | Win32.PerFiler | Win32.PerFiler is designed to r...
Worm | hidden autorun | Win32.Miewer.a | A Trojan Downloader that mas...
Trojan | C:/windows/ | Trojan-Downloader.VBS.Small.dc | This Trojan downloads other fil...
Worm | autorun | Win32.Peacomm.dam | A Trojan Downloader that is sp...
Scan progress
Scanning
Start
Path
Scanning is finished. Cleanup required.
Infections
38
Save Report
Remove
PCID:9025E786 Smart Fortress 2012 Build 2.0.8787.1222

62.76.190.87/SE/

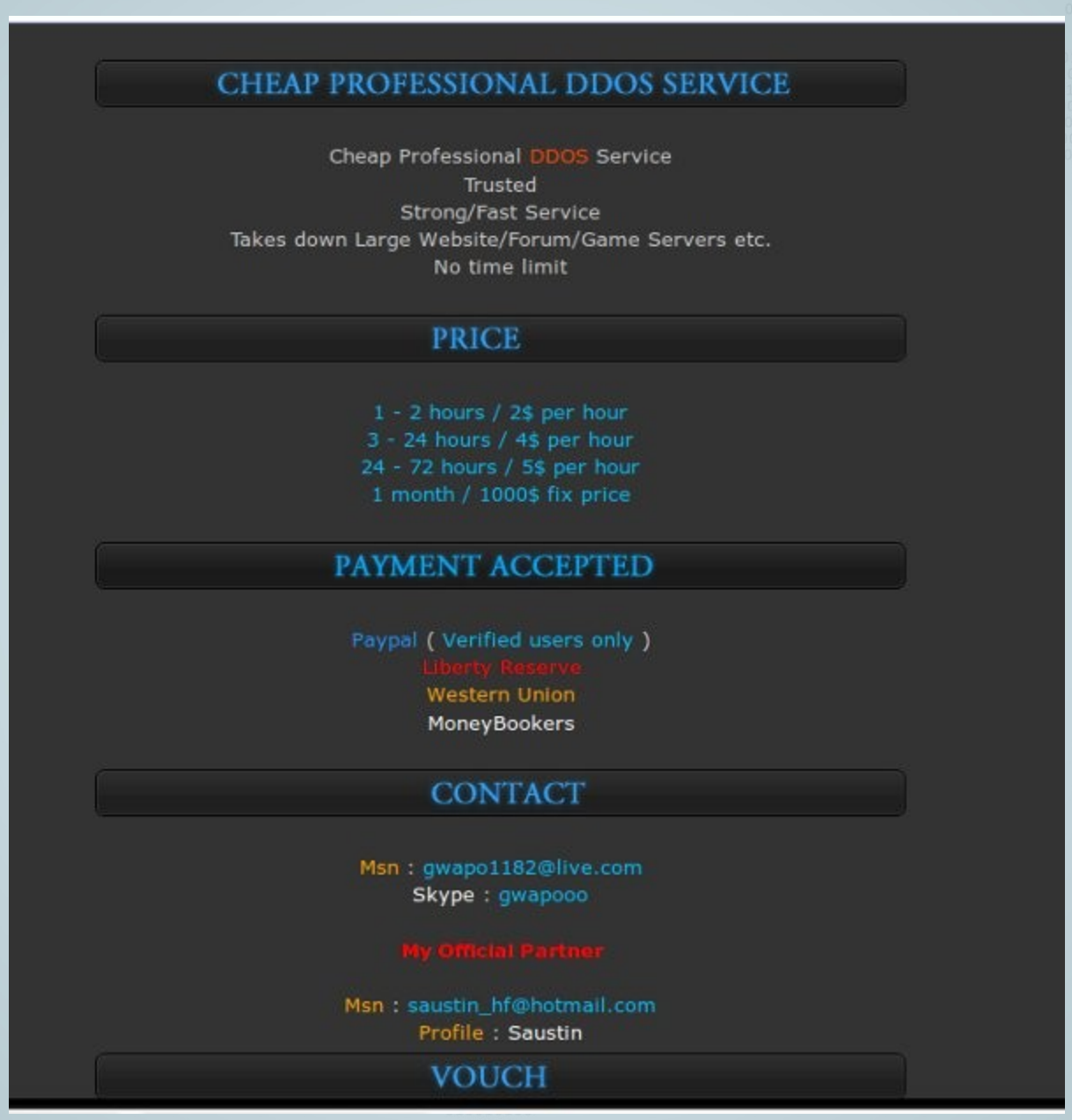
Blue Lace 16.bmp.EnCiPhErEd	2 KB	CRYPTED!
clock.avi.EnCiPhErEd	81 KB	CRYPTED!
Coffee Bean.bmp.EnCiPhErEd	17 KB	CRYPTED!
FeatherTexture.bmp.EnCiPhErEd	17 KB	CRYPTED!
Gone Fishing.bmp.EnCiPhErEd	17 KB	CRYPTED!
Greenstone.bmp.EnCiPhErEd	26 KB	CRYPTED!
OEWABLog.txt.EnCiPhErEd	2 KB	CRYPTED!
Prairie Wind.bmp.EnCiPhErEd	65 KB	CRYPTED!
Rhododendron.bmp.EnCiPhErEd	17 KB	CRYPTED!
River Sumida.bmp.EnCiPhErEd	27 KB	CRYPTED!
Santa Fe Stucco.bmp.EnCiPhErEd	65 KB	CRYPTED!
setuplog.txt.EnCiPhErEd	21 KB	CRYPTED!
Soap Bubbles.bmp.EnCiPhErEd	65 KB	CRYPTED!
winnt256.bmp.EnCiPhErEd	48 KB	CRYPTED!

HOW TO DECRYPT FILES.txt - Notepad

File Edit Format View Help

Attention! All your files are encrypted!
You are using unlicensed programms!
To restore your files and access them,
send code Ukash or Paysafecard nominal value of EUR 50 to the e-mail [redacted]@gmail.com. Duri

You have 5 attempts to enter the code. If you exceed this
of all data irretrievably spoiled. Be
careful when you enter the code!


CHEAP PROFESSIONAL DDOS SERVICE
Cheap Professional DDOS Service
Trusted
Strong/Fast Service
Takes down Large Website/Forum/Game Servers etc.
No time limit
PRICE
1 - 2 hours / 2$ per hour
3 - 24 hours / 4$ per hour
24 - 72 hours / 5$ per hour
1 month / 1000$ fix price
PAYMENT ACCEPTED
Paypal (Verified users only)
Liberty Reserve
Western Union
MoneyBookers
CONTACT
Msn : gwapo1182@live.com
Skype : gwapooo
My Official Partner
Msn : saustin_hf@hotmail.com
Profile : Saustin
VOUCH


Spy Eye v1.3
Find !NFO
Statistic
FTP accounts
Settings
2011 11/08 20:47:33
Screen shots
BOA Grabber
CC Grabber
Certificate Grabber
9505k +62740
E-Mail Grabber
Video Data
FTP Grabber
Loading...
Get Data from DataGrabber
Bot GUID :
Report date region :
06/11/2011 ... 08/11/2011
clean
Limit :
100
submit
Loading ...

FORSV

```
2848=C:\Program Files\[redacted].exe
2852=C:\Program Files\[redacted].exe
3068=C:\Program Files\[redacted].exe
3592=C:\[redacted].EXE
4060=c:\windows\[redacted].exe
1636=C:\Program Files\Internet Explorer\iexplore.exe
2292=C:\Program Files\[redacted].exe
1740=C:\Program Files\[redacted].exe
3368=C:\Program Files\[redacted].exe


ASP.NET Account
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
Pass: [redacted]


Windows RAS
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
Name: [redacted]


Internet Explorer
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
http://mail.[redacted].dk/@@@[redacted]:[redacted]
http://www.[redacted].dk/log-ind/@@@[redacted]:[redacted]
http://www.[redacted].dk/log-ind/@@@[redacted]:[redacted]
http://www.[redacted].dk/@@@[redacted]:[redacted]
http://www.[redacted].dk/@@@[redacted]:


Google Chrome
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
http://[redacted].dk/@@@[redacted]:[redacted]
http://www.[redacted].dk/@@@[redacted]:[redacted]
```

6.0.6001![redacted]!0E1E73B0

```
System Info
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
User: [redacted]
OS: Windows Vista Service Pack 1 (Build 6001) 64-bit
Computer: [redacted]-PC
Country: United States
Language: English
Time: 11/6/2011 6:38:30 AM
```

SUPPORT CENTER
TICKET TRACKING

SUPPORT TICKET SYSTEM

Home | New Ticket | Ticket Status

Please fill in the form below to open a new ticket.

Full Name: *

Email Address: *

Telephone: Ext

Help Topic: Select One *

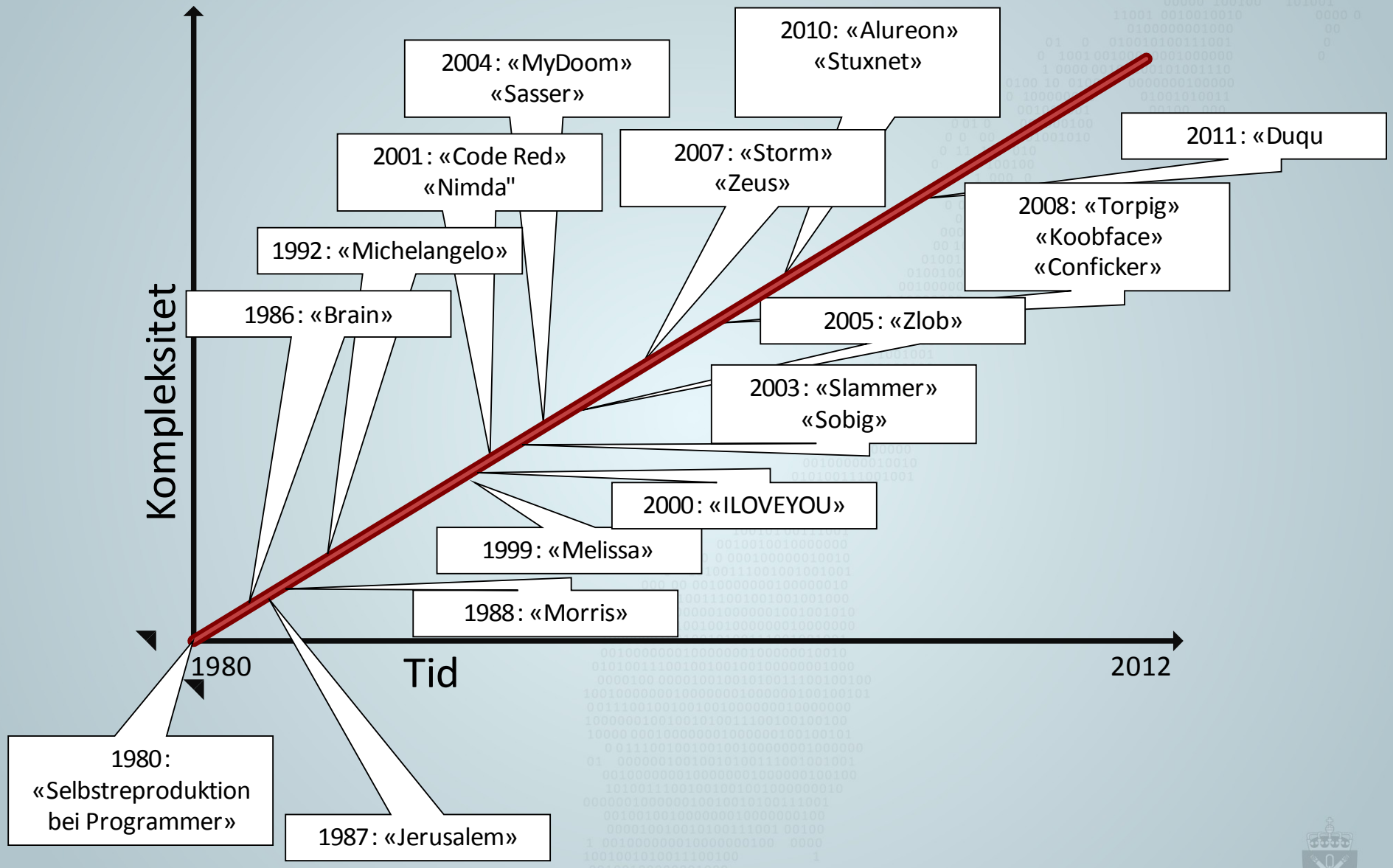
- Select One
- bugreport
- feature request
- help needed
- serial.txt needed

Subject: *

Message:

Captcha Text: 27528 *Enter the text shown on the image.*

Submit Ticket | Reset | Cancel


2010: «Alureon»
«Stuxnet»
2004: «MyDoom»
«Sasser»
2011: «Duqu
2001: «Code Red»
«Nimda"
2007: «Storm»
«Zeus»
2008: «Torpig»
«Koobface»
«Conficker»
1992: «Michelangelo»
1986: «Brain»
2005: «Zlob»
2003: «Slammer»
«Sobig»
2000: «ILOVEYOU»
1999: «Melissa»
1988: «Morris»
Kompleksitet
1980
Tid
2012
1980:
«Selbstreproduktion
bei Programmer»
1987: «Jerusalem»


UN
UN
UN
UN 01024


F310


98056


F310


UN

Aftenposten.no Nyheter Innenriks

Aftenposten

Alt innhold | Nyheter | Sport | Meninger | Økonomi | Kultur | Oslopuls | Arkivet | Reise | Mat og vin | Jobb | Bolig

Innenriks | Verden | Wikileaks | Politikk | Klima | Oslo | Fakta | Viten | Kongelige | Helse | Leve | Siste 100

FOTO: SCANPIX

PST: Sosiale medier en viktig arena for å spre ekstrem islam

- Gjennom moderne nettmedier kommer meningsfeller enkelt i kontakt med hverandre på tvers av etniske og geografiske skillelinjer, mener PST.

AV JON DAGSLAND HOLGERSEN

Oppdatert: 28.02.11 kl. 13:55 Publisert: 28.02.11 kl. 11:39

Epost:

IMDi Aarsrapport 2010

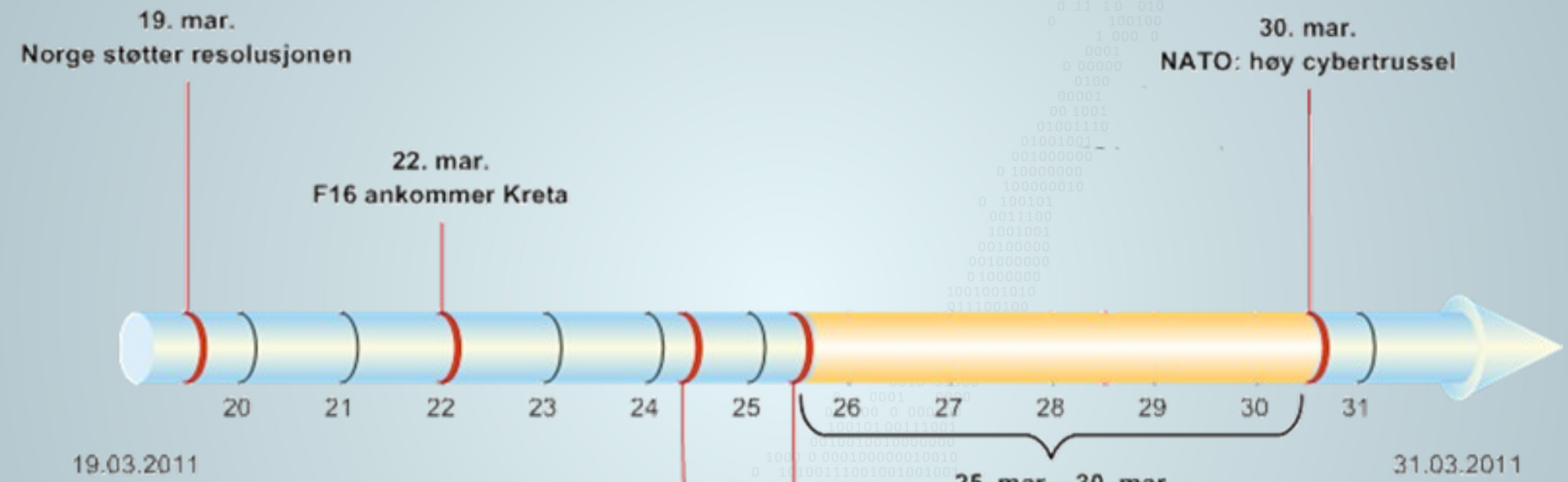
”Sosiale medier en viktig arena for å spre ekstrem islam. Gjennom moderne nettmedier kommer meningsfeller enkelt i kontakt med hverandre på tvers av etniske og geografiske skillelinjer, mener IMDI.

Thor Bjork
Seniorrådgiver
Integrerings og mangfoldsdirektor atet (IMDi)
Postboks 8059 Dep., 0031 Oslo”

Vedlegg:
IMDI_Aarsrapport_2010_hele.pdf

FORSVARET

Forsvaret:



Trusselaktør:

24. mar.
Angrep klargjort

25. mar.
Epost sendes ut

FORSVARET

Cyberforsvar

Forsvarets tilnærming til cyberforsvar

Nettverksbasert Forsvar (NbF)

- Økt militær effekt gjennom nettverksorganisering av militære kapasiteter
- Endring i prosesser, organisasjon og teknologi
- Fra "Need to know" til "Responsibility to share"; et paradigmeskifte

Coalition forces within Afghanistan cannot communicate effectively and share theatre related operational Commander's guidance, information and intelligence. These communication gaps increase risks to life, resources and efficiency.

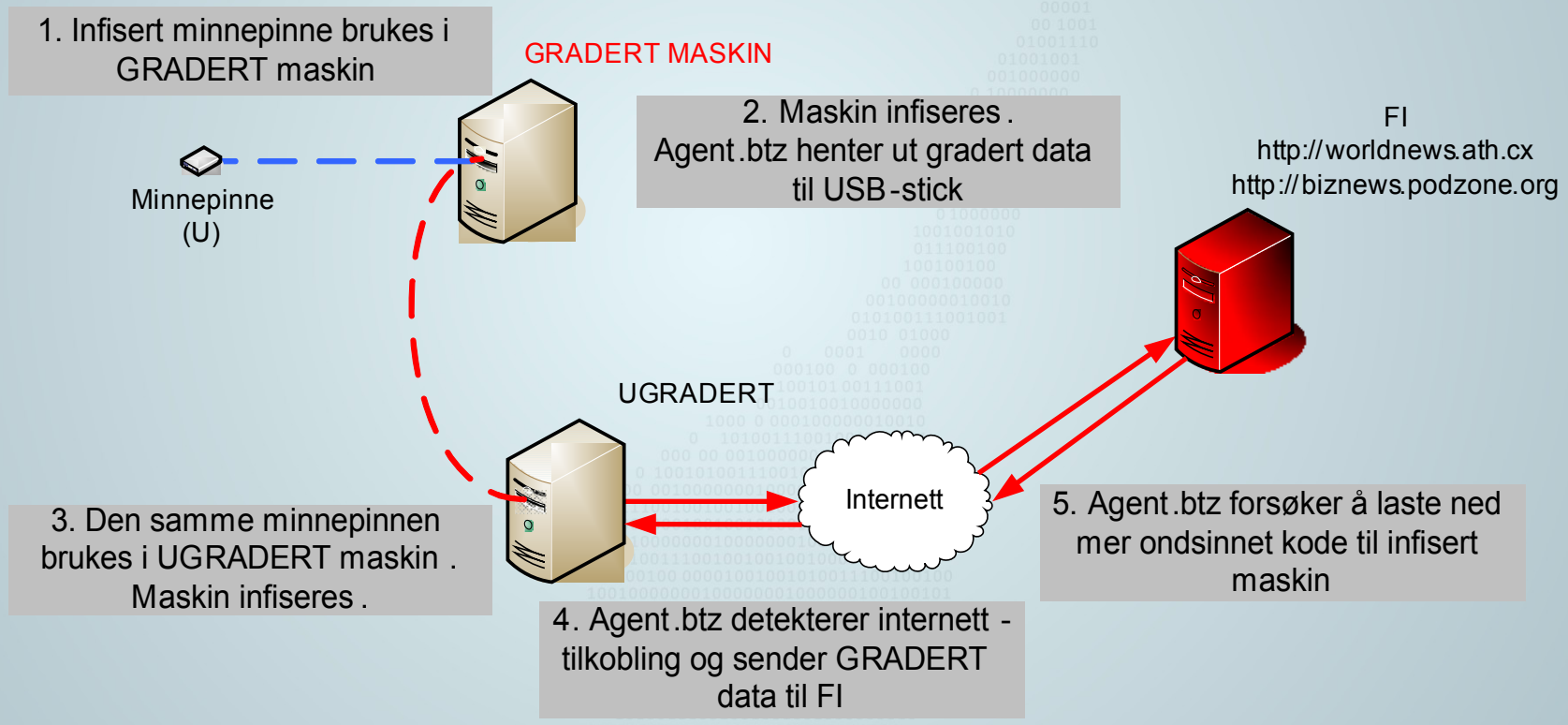
GEN McChrystal, COMISAF

IKT i Forsvaret

- Mål: Informasjonsoverlegenhet
- Integrert del av planlegging og gjennomføring av militære operasjoner.
- Omfattende og kompleks infrastruktur

«Gammelt» konsept for informasjonssikkerhet

- Fokus på forebyggende tekniske tiltak og administrative rutiner
- Basert på statistisk prediksjon av trussel og evne til å identifisere egne sårbarheter
- Forutsetter:
  - at risiko vurderes og sikkerhetstiltak iverksettes på forhånd
  - en forutsigbar anvendelse av og trussel mot IKT


1. Infisert minnepinne brukes i GRADERT maskin
GRADERT MASKIN
2. Maskin infiseres . Agent .btz henter ut gradert data til USB-stick
FI
http://worldnews.ath.cx
http://biznews.podzone.org
Minnepinne
(U)
UGRADERT
Internett
3. Den samme minnepinnen brukes i UGRADERT maskin . Maskin infiseres .
4. Agent .btz detekterer internett - tilkobling og sender GRADERT data til FI
5. Agent .btz forsøker å laste ned mer ondsinnet kode til infisert maskin

FORSVARET

Sikkerhetskonsept for NbF

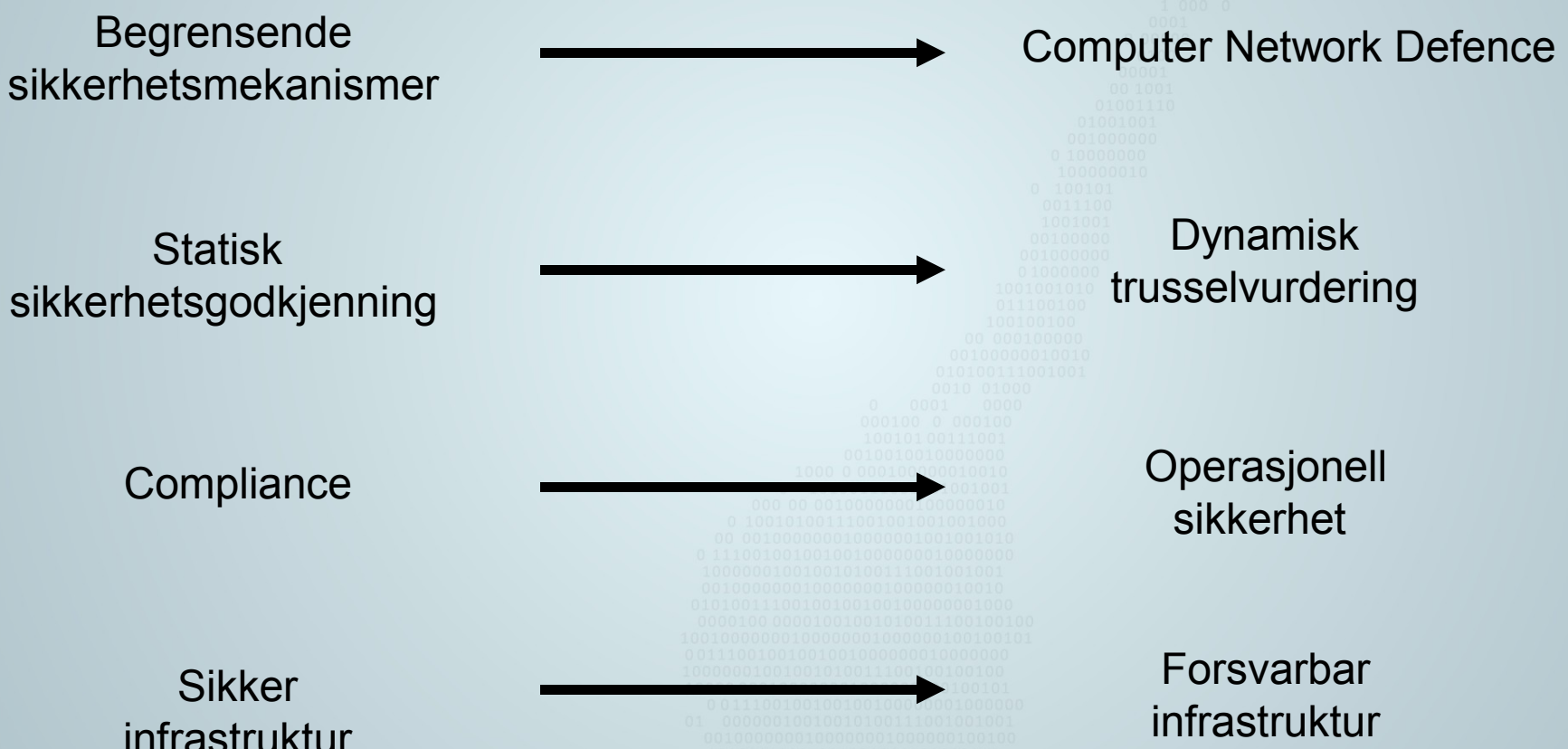
Risikohåndtering i et NbF

- Fleksibel; "Responsibility to share" betyr at risikohåndtering må skje på alle nivåer
- Sikkerhetstiltak må vurderes i operativ kontekst
- Forebyggende tiltak fokuseres inn mot å etablere en forsvarbar infrastruktur

FORSVARET

Computer Network Defence

- Detektere datanettverksangrep og -etterretning mot eller i Forsvarets informasjonssystemer
- Planlegge, lede og koordinere håndtering av sikkerhetstruende hendelser i informasjonssystemene
- Gjennomføre skadevurdering etter angrep


Begrensende sikkerhetsmekanismer
Computer Network Defence
Statisk sikkerhetsgodkjenning
Dynamisk trusselvurdering
Compliance
Operasjonell sikkerhet
Sikker infrastruktur
Forsvarbar infrastruktur

FORSVARET

Takk for oppmerksomheten!

jarle.kittilsen@gmail.com

http://no.linkedin.com/in/jarlekittilsen