Bekjempelse av ulovlig innhold på nettet

Er det behov for et internasjonalt regelverk?

Sorenskriver Stein Schjølberg

UNINETT seminar i Oslo, 22. november 2016.

Sikkerhetsbloggen NSM, 1. juli 2016

Roar Thon (fagdirektør NSM): **Dette er et ran**

”Det begås digital utpressing, ran, tyveri og underslag hver eneste dag i Norge. Statistikkene over hvor utbredt dette er, eksisterer etter min mening foreløpig ikke i en troverdig form. (…) Hackernes uønskede aktiviteter må motarbeides på en rekke områder på samme måte som det ble gjort når det gjaldt fysiske ran, men samtidig er det viktig å forstå at enkelte faktorer ikke er de samme.

Hackerne påvirkes ikke av at bedrifter ikke lenger oppbevarer kontanter. Verdiene de går etter er digitale. **De bedriver kriminell aktivitet som ikke er et lokalt eller nasjonalt problem**. Hackeren sitter som oftest bak en kontorstol et helt annet sted i verden. Skjult bak teknologiske, juridiske og sågar politiske hindre er det heller ikke lett å straffeforfølge dem.”

Dyn cyberattack

The **2016 Dyn cyberattack** took place on October 21, 2016, and involved multiple denial-of-service attacks (DDoS attacks) targeting systems operated by Domain Name System (DNS) provider Dyn which made major Internet platforms and services unavailable to large swaths of users in Europe and North America.

As a DNS provider, Dyn provides to end-users the service of mapping an Internet domain name, when entered into a web browser, to its corresponding IP address. The DDoS attack was accomplished through a large number of DNS lookup requests from tens of millions of IP addresses.

Sikkerhet i sneglefart

Sofie Nystrøm (direktør NTNU Gjøvik juli 2016):

"**Landegrenser er for lengst visket ut i det digitale rom og gjør at samarbeid det satses på i NATO, EU, FN og Interpol er ekstra viktig**. Dette er den eneste måten å takle de massive problemstillingene vi står ovenfor på tvers av myndighetene, leverandører og private virksomheter."

Litt internasjonal historie

- The Ribicoff Bill, USA (1977)
- INTERPOL (1981)
- OECD (1986)
- Council of Europe (1989)
- United Nations (1990)
- Council of Europe (1995)
- The G-8 Group (1997)
- The Commonwealth (1999)
- Organisation of American States (OAS) (1999)

Internasjonal bakgrunn etter 2000

- The Council of Europe Convention on Cybercrime of 2001
- The Shanghai Convention on Combating Terrorism, Separatism and Extremism (2001)
- OECD Policy Guidance on Online Identity Theft (2008)
- The League of Arab States Convention on Combating Information Technology Offences (2010)
- The Shanghai Cooperation Organization Agreement in the Field of International Information Security (2011)

Internasjonal bakgrunn etter 2012

- HIPCAR – Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean (2012)
- The European Union Directive on attacks against information systems (2013)
- UNODC Expert Group to conduct a comprehensive study on cybercrime (2013)
- African Union Convention on Cybersecurity (AUCC) (2014)
- The Commonwealth – Report of the Working Group of Experts on Cybercrime (2014)

EU Direktiv 2011/92 av 13 desember 2011: on combating sexual abuse and sexual exploitation of children, and child pornography

- *Article 25: Measures against websites containing or disseminating child pornography.*
- *1) Member States shall take the necessary measures to ensure the prompt removal of webpages containing or disseminating child pornography hosted in their territory and to endeavour to obtain the removal of such pages hosted outside their territory.*
- *2) Member States may take measures to block access to webpages containing or disseminating child pornography towards the Internet users in their territory.*

Veien til Forente Nasjoner (FN)

- WSIS Geneva 2003 and Tunis 2005
- ITU High-Level Experts Group (HLEG), 2007-2008
- The United Nations Human Rights Council Resolution of June 29, 2012
- The Intergovernmental Expert Group to conduct a Comprehensive Study on Cybercrime (UNODC), 2013
- ITU Plenipotentiary Conference in Busan, 2014
- The Doha Declaration (2015)
- Working Group on responsible behaviour of States (2016)

Internasjonal forpliktelse for straffeloven

- Internasjonale forpliktelser - Europarådets konvensjon om cybercrime
- Extradite or prosecute – Article 22 nr. 3
- Straffelovens stedlige virksomhet – Rt. 2004 s. 1619: *"det utslagsgivende må være at alle nødvendige handlinger for å bryte beskyttelsen fant sted i Norge."*

Europarådets konvensjon om cybercrime

Substantive criminal law:	Straffeloven av 2005:
Article 2 – Illegal access	§ 204
Article 3 – Illegal interception	§ 205 b
Article 4 – Data interference	§ 351
Article 5 – System interference	§ 351 og § 192
Article 6 – Misuse of devices	§ 201
Article 7 – Computer-related forgery	§ 361
Article 8 – Computer-related fraud	§ 371
Article 9 – Offences related to child pornography	§ 311 og § 310

Kryptering

- Kryptering
- *A warrant-proof encryption: "to describe a situation where a service provider has implemented encryption in a way that prevents them from producing usable, unencrypted information even if they are served with a valid court order."* Leslie R. Caldwell, US DoJ, (Juni 2016)
- Høyesterett kjennelse 30. august 2016
- Dataavlesing – straffeprosessloven § 216 o og § 216 p
- Kommunikasjonkontrollforskrift av 9. september 2016

Høyesterett 30. august 2016

Førstvoterende uttalte blant annet:

*"Jeg finner for min del klart at **bruken av siktedes finger til å få tilgang til bevismidler utenfor kroppen – her innholdet i en mobiltelefon, språklig sett er noe annet enn en kroppslig undersøkelse**. Etter ordlyden gir § 157 med andre ord ikke hjemmel for det inngrep som er tema i saken."*

Et nytt trussel- og risikobilde

- Cyberangrep og alvorlig cyberkriminalitet mot våre nasjonale interesser
- Styrke cybersikkerheten i Norge
- Nasjonal Sikkerhetsmyndighet – Sikkerhetsfaglige råd (2015)
- Etterretningstjenestens rapport – FOKUS 2016
- Nasjonal kommunikasjonsmyndighet – nasjonal cyberøvelse (desember 2015)
- Riksrevisjonens Dokument 1 (2015)

A Geneva Convention or Declaration for Cyberspace

A global framework on cybersecurity and cybercrime, and a contribution for peace, security and justice in cyberspace.

Judge Stein Schjolberg, Norway, and Professor Solange Ghernaouti, Switzerland

(VFAC Review, No 12, October 2016)

https://eng.kic.re.kr

www.cybercrimelaw.net

A Geneva Convention or Declaration for Cyberspace

"It is no longer a question of a nation protecting its own security, it is a question of the global community protecting itself." *Kapil Sipal, India, Former Minister for Communications and Information Technology, (2012)*

- Standarder for internasjonale tiltak om cybersikkerhet
- Internasjonal koordinering og samarbeid i etterforsking av cyberkriminalitet gjennom INTERPOL
- Standarder for globalt partnerskap med den private sektor i etterforsking av cyberkriminalitet
- Harmonisering av landenes straffebestemmelser
- Etablere en internasjonal domstol eller Tribunal for Cyberspace

Etterforsking av global cyberkriminalitet

- INTERPOL Global Complex for Innovation (IGCI) i Singapore
- Cyber Fusion Centre
- Public Private Partnerships med globale aktører i privat sektor og akademia
- Spesielt samarbeid med World Economic Forum
- INTERPOL-Europol Cybercrime Conferences 2013, 2014, 2015
- Singapore 28.–30. september 2016

INTERPOL-Europol Cybercrime Conference
28.–30. september 2016

Det ble fremhevet behov for:

- *Law enforcement agencies and private sector companies to consider and find solutions to address respective constraints when investigating cybercrime.*
- *Supporting user-focused initiatives such as 'No more ransom', a multi-stakeholder project which aims to help victims of ransomware retrieve their encrypted data without paying their attacker.*
- *INTERPOL and Europol to support existing entities in their establishment of regional cyber centres via capacity building and information sharing.*

Public-Private Partnerships

- PPP organisert av politiorganisasjoner
- Interpol
- Europol
- FBI
- A Memorandum of Understanding (MoU)
- PPP organisert av privat sektor
- Microsoft Cybercrime Center – Digital Crimes Unit
- Microsoft 30 regionale kontorer globalt
- International Cyber Security Alliance, UK
- Project 2020 sammen med Europol

Harmonisering av enkeltlandenes lovtiltak mot cyberkriminalitet

- Støtte til enkeltland for en bedre forståelse av behovet
- Fremme internasjonal koordinering og samarbeid
- Forsikre at personvern og menneskerettigheter ivaretas
- Etablere klare og entydige strafferettslige standarder
- Et av de viktigste formål er å forebygge cyberkriminalitet
- Utvikle og etablere straffebestemmelser i internasjonale traktater og regelverk

En internasjonal domstol eller tribunal for cyberspace

"There can be no peace without justice, no justice without law and no meaningful law without a Court to decide what is just and lawful under any given circumstances". Benjamin B. Ferencz, former US Prosecutor

- En internasjonal domstol er en "missing link"
- De mest alvorlige globale cyberkriminalitet straffeforfølges
- Etterforsking koordineres gjennom INTERPOL
- *The Third Pillar for Cyberspace*
- En FN domstol eller tribunal, som inkluderer påtalemyndighet

Takk for oppmerksomheten!

www.cybercrimelaw.net