Cybercrime og forsikring

I. Innledning

Cyberspace er vår tids ramme for informasjons- og kommunikasjonsteknologi (IKT). Stater, internasjonale og nasjonale organisasjoner og institusjoner, offentlig virksomhet, næringsvirksomhet og enkeltindivider er avhengig av en velfungerende og sikker bruk av cyberspace.

Omfanget av straffbare handlinger i cyberspace er i voldsom vekst, og særlig alvorlig for enkeltlandene er industrispionasje og cyberangrep på viktige infrastrukturer for samfunnsfunksjoner. Et hovedproblem er at disse handlinger kan finne sted uten at det eksisterer internasjonal lovgivning eller en domstol som kan stille aktørene til ansvar med rettsforfølging og straff.

Cyberspace er i dag den siste gjenværende arena der globale straffbare handlinger kan gjennomføres uten nevneverdig risiko. Alle andre områder, det være seg på land, til sjøs, og i luften er underlagt internasjonale lover og regelverk.
Lov og orden må også sikres og utvikles i cyberspace, som i det globale samfunn for øvrig. De rettigheter som har et strafferettslig vern offline må også få et strafferettlig vern online.

The United Nations Human Rights Council (UNHRC),[1] har i en Resolusjon av 29. Juni 2012, om " *the promotion, protection and enjoyment of human rights on the Internet"* uttalt blant annet:

"Reaffirming the human rights and fundamental freedoms enshrined in the Universal Declaration of Human Rights and relevant international human rights treaties, including the International Covenant on Civil and Political Rights, and the International Covenant on Economic, Social and Cultural Rights,

Noting that the exercise of human rights, in particular the right of freedom of expression, on the Internet is an issue of increasing interest and importance as the rapid pace of technological development enables individuals all over the world to use new information and communications technologies,

Affirms that the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one´s choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights."

[1] http://www.un.org/en/rights/index.shtml

II. Internasjonale lovtiltak

Europarådets konvensjon om cybercrime av 2001[2] er en historisk milepæl i kampen mot cybercrime. Alle medlemsstater og andre stater som ønsker en ratifikasjon eller slutte seg til konvensjonen, må tilpasse sine straffe- og straffeprosessuelle bestemmelser til konvensjonens bestemmelser. Andre land og regionale organisasjoner har brukt konvensjonens bestemmelser som helt eller delvise retningslinjer. I tillegg har mange medlemsland og andre land som følge av den teknologiske utvikling etter 2001, vedtatt ytterligere bestemmelser til vern mot cybercrime som ikke antas omfattet av konvensjonen.

Basert på Europarådets konvensjon og anbefalingene fra andre regionale organisasjoner blant annet fra Organization of American States (OAS), Asian Pacific Economic Corporation (APEC), Det britiske samveldet, Association of Southeast Asian Nations (ASEAN), Shanghai Cooperation Organization, The League of Arab States, European Union, og arbeidet gjennom slike FN organisasjoner som International Telecommunication Union (ITU) og United Nations Office on Drugs and Crime (UNODC), skapes nå muligheter for regionale og globale lovtiltak for cybercrime.

UNODC etablerte i 2010 en arbeidsgruppe som gjennomførte en undersøkelse av situasjonen for cybercrime i medlemslandene, og mottok svar fra 69 medlemsland samt fra 67 non-governmental organizations (NGO).

Arbeidsgruppen hadde flere møter og det siste ble holdt i Wien i februar 2013. Det ble oppnådd enighet om anbefalinger for "technical assistance and capacity building". Forslag om internasjonale lovtiltak for cybercrime oppnådde ingen muligheter for consensus.

To av hovedkonklusjonene fra UNODC arbeidgruppen skal nevnes:

1. *Reliance on traditional means of formal international cooperation in cybercrime matters is not currently able to offer timely response needed for obtaining volatile electronic evidence. As an increasing number of crimes involve geo-distributed electronic evidence, this will become an issue not only for cybercrime, but all crimes in general.*
2. *In a world of cloud computing and data centres, the role of evidence "location" needs to be conceptualized, including with a view to obtaining consensus on issues concerning direct access to extraterritorial data by law enforcement authorities.*

[2] Se www.conventions.coe.int

Et effektivt internasjonalt samarbeid er avgjørende for etterforskingen av den globale cybercrime og sikring av elektroniske bevis i slike saker. Dette gjelder standarder for det internasjonale rettslige samarbeid og prosedyrer for anmodninger om bistand fra andre lands etterforskingsorganer. Særlig viktig er dette for nye utfordringer som globale cyberattacks, sosiale nettverk, og "cloud computing".

Det internasjonale samarbeidet er sterkt svekket og tidkrevende ved manglende enighet, og den eneste mulighet utenom de bilaterale og multilaterale avtaler, er samarbeidet gjennom INTERPOL.
INTERPOL har på sin side inngått et samarbeid med globale private partnere. I tillegg ser vi en utvikling av *"Global Virtual Taskforces for Cyberspace with the private sector for the investigation and prosecution".*

Spesielt skal nevnes "cloud computing", som kan beskrives som:

"Data in the "clouds" is data that is constantly being shifted from one server to the next, moving within or access different countries at any time. Also, data in the "clouds" may be mirrored for security and availability reasons, and could therefore be found in multiple locations within a single country or in several countries. Consequently, not even the cloud computing provider may know exactly where the requested data is located."[3]

Denne utvikling nødvendigjør fortsatte forsøk på å etablere globale lovtiltak på FN-nivå for å forebygge, etterforske og pådømme global cybercrime.

III. International Court 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 eller tribunal for cyberspace foreslås etablert. En internasjonal domstol eller tribunal er nødvendig for å forebygge og straffeforfølge de mest alvorlige globale handlinger i cyberspace. En internasjonal straffedomstol har blitt betegnet som "the missing link" i den globale rettshåndhevelse.
Den tidligere FN generalsekretær Kofi Annan har uttalt: *"In the prospect of an international criminal court lies the promise of universal justice."*

[3] INTERPOL European Working Party on Information Technology Crime (EWPITC) – Project on cloud computing, 2011.

Traktaten for Den internasjonale straffedomstol i Haag er ikke ratifisert av Kina, Russland, og USA. Det er derfor nødvendig å etablere et tribunal etter vedtak i FN.

Forslaget til en slik FN traktat bør også omfatte kontroll med den internasjonale overvåking eller "Electronic Communications Surveillance".

Presentasjonen av en demonstrasjons rettsak "Mock Trial" kan være et nyttig prosjekt, som vil demonstrere hvordan en global domstol for cyberspace kan fungere med hjemmel fremtidige FN traktater. Jeg arbeider med et prosjekt om dette, og håper å kunne gjennomføre en slik demonstrasjons rettssak i 2015.

Forslaget om en internasjonal domstol eller tribunal for cyberspace baseres blant annet på følgende prinsipper for rettshåndhevelse:

1. The judiciary is one of the three powers of any democratic state. Its mission is to guarantee the very existence of the Rule of Law and thus, to ensure the proper application of the law in an impartial, just, fair, and efficient manner. [4]
The International Criminal Tribunal for Cyberspace shall be a treaty based, fully independent international tribunal established to promote the rule of law similar or almost a parallel to a Supreme Court.
The International Criminal Tribunal for Cyberspace[5] *is established by the United Nations General Assembly, or by the United Nations Security Council acting under Chapter VII of the Charter of the United Nations. The purpose is to prevent serious and organized global cybercrime, protect the peace and ensure that the most serious international crimes in cyberspace do not go unpunished.*
2. Any intentional electronic communications surveillance in investigations of criminal cases across jurisdictional boundaries needs the consent of the International Criminal Tribunal for Cyberspace or the Prosecutors Office, whenever there is probable cause to believe that anybody is suspected of having committed or attempt to commit cyberattacks and other cybercrimes of the most serious global concern.

[4] See The Magna Carta of Judges (Fundamental Principles) Article 1, adopted by the Consultative Council of European Judges in 2010.

[5] The Statute of the International Criminal Tribunal for The Former Yugoslavia has been used as a Model Statute. Article 19 on the Electronic Communication Surveillance is based on models in the Norwegian Criminal Procedure Act Chapter 16a, and in the US Foreign Intelligence Surveillance Act (FISA), as required in 50 USC § 1805 (Issuance of order, that does not apply outside the United States.)

3. A permanent appointed defense attorney shall be present at the Court hearings and be a protector of the basic legal and procedural rights of the offender.

4. The Prosecutor, as a separate organ of the International Criminal Tribunal for Cyberspace, shall be responsible for the investigation and prosecution of cyberattacks and other cybercrimes of the most serious global concern.
The Prosecutors Office shall act independently of the Security Council, of any State, or any international organization, or of other organs of the International Criminal Tribunal for Cyberspace.
5. The Prosecutors Office shall have the power to seek assistance in the investigation by global law enforcements coordinated by INTERPOL, and the global private sector.
6. The principle sources for the protection of individual rights, the Universal Declaration on Human Rights, the International Covenant on Civil and Political Rights, and the International Covenant on Economic, Social and Cultural Rights, are fundamental rights that support the right of every person to exercise the freedom to hold opinions without interference and to seek, receive and impart information and ideas through any medium regardless of frontiers. The same rights that people have offline must also be protected online.

IV. Internet of Things (IoT) – M2M

Konsekvensene av en global etablering av Internet of Things (IoT) må utredes.

Internet of Things (IoT) er betegnet av statsminister David Cameron som "The new industrial revolution." Dette kan endre vårt globale og nasjonale samfunn betydelig, enkelte eksperter mener allerede om 2-3 år.

"Internet of Things (IoT)" er beskrevet som tingenes Internet.[6] Tingene får sensorer, som er små datamaskiner, og kan dermed kommunisere med hverandre uten at mennesker er direkte involvert.

Dette kan også beskrives som "Internet of Everything (IoE)" [7] som er nettverkstilgang mellom "people, process, data, and things".

Jeg viser til et utdrag av min bok "The History of Cybercrime 1976-2014":

"The term "Internet of Things" was introduced in 1999, and refers to uniquely identifiable objects and their virtual representations in an Internet-like structure. The potential of a global system covering interconnected cyber systems and networks, sensors, and devices that all are using the Internet protocol, opens for communications among physical objects. This

[6] Se http://www.microsoft.com/windowsembedded/en-us/internet-of-things.aspx

[7] Se http://www.cisco.com/web/about/ac79/innov/IoE.html

development may change the technology world to such an extent that it has been described as the Internets next generation, or that the world is on a brink of "a new industrial revolution."

Internet of Things (IoT) may be described as the concept where all kinds of smart objects are seamlessly integrated to the information and communication technology (ICT) networks. The term "Internet of Everything" has therefore also been introduced. It will change the way the global population live, interact, and work in the future.

The term "Machine to Machine (M2M)" has also been introduced, and refers to technologies that allow both wireless and wired systems to communicate with other devices of the same type. M2M is considered as an integral part of the Internet of Things (IoT)."

(Stein Schjolberg: The History of Cybercrime 1976-2014, to be published in September 2014)

V. Forsikringsselskaper

Spesielle tilbud om forsikringsdekning av computer crime har vært tilbudt fra forsikringsselskaper siden 1980 årene.[8]

1. De første forsikringstilbud

I United States tilbød flere selskaper i 1980 årene slik forsikringsdekning, blant annet Surety Association of America (fra 1976), St. Paul Fire and Marine Insurance Company, AETNA Casualty and Surety Company, CHUBB GROUP of Insurance Companies, Fireman's Fund Insurance Companies, og Shand, Morahan & Company.
I West Germany ble slik dekning tilbudt fra Hermes Kreditversicherungs AG.

Men det var i Storbritannia den viktigste utvikling fant sted, med Lloyds Electronic and Computer Crime Policy (LECCP) fra 1981 og revidert fra 1983.[9]
The Lloyds Policy LECCP 83 tilbudet omfattet dekning beskrevet i syv "Insuring Agreements", blant annet:

[8] With regard for information on insurance policies in this section, see Stein Schjolberg: Datakriminalitet og forsikring (page 16-29), COMPLEX 7/86, Universitetsforlaget, Norway. (Norwegian text)

[9] Introduced by K.F.Alder Syndicate in New York, December 1981, especially directed at the US markets of banks and finance companies. The Policy was revised in 1983 and described as LECCP 83. It was also presented by Robert B. Budelman at the American Bar Association, Section of Tort and Insurance Practice, Fidelity and Surety Law Committee 1985 London Meeting, July 17, 1985.

"Insuring Agreement 1
Computer Systems

By reason of the Assured having transferred, paid or delivered any funds or property, established any credit, debited any account or given any value as the direct result of the fraudulent input of Electronic Data directly into:

(1) The Assured´s Computer Systems, or
(2) A Service Bureaus Computer System, or
(3) An Electronic Funds Transfer System, or
(4) A Customer Communication System,

or the fraudulent modification or the fraudulent destruction of Electronic Data stored within or being run within any of the above systems or during electronic transmission through data communication lines to the Assureds Computer Systems or a Service Bureaus Computer System which fraudulent acts were committed by a person who intended to cause the Assured to sustain a loss or to obtain financial gain for himself or any other person."

2. Forsikringstilbud idag
Forsikringstilbud i 2014 omfatter også spesiell dekning av cyberspace. I denne rapport skal bare to globale tilbud omtales.

Lloyds Cyber Insurance
Lloyds[10] har i 2014 advart mot en økning av cybercrime, som er ventet å kreve flere spesielle forsikringstilbud.[11]Lloyds underwritere utvikler derfor nye forsikringstilbud for markedene i Europa, Asia og Latin Amerika. Spesielt skal nevnes Beazley som har lansert en internasjonal versjon av sin USA Beazley Breach Response Insurance. Dette forsikringstilbudet kan også gi spesialdekning for følgende cybercrime:

- Phishing scams;
- Telephone hacking;
- Loss of future sales caused by a privacy breach or a network security event;
- Cyber terrorism;

[10] Se www.lloyds.com
[11] http://www.lloyds.com/news-and-insight/news-and-features/market-news/industry-news-2014/lloyds-underwriters-look-to-address-the-growing-threat-of-cybercrime

AIG CyberEdge Insurance
Forsikringsselskapet AIG i USA har et tilbud som kalles CyberEdge[12] og inkluderer CyberEdge Mobile App og CyberEdge PC. Forsikringstilbudet inkluderer:

- Third-Party Loss Resulting From a Security or Data Breach;
- Direct First-Party Costs Resulting From a Breach;
- Lost Income & Operating Expense Resulting From a Security or Data Breach;
- Threats to Disclose Data or Attack a System to Extort Money;
- Online Defamation & Copyright Trademark Infringement;

I tillegg tilbyr AIG en 24/7 service med tilgang til og assistance fra "The CyberEdge Breach Resolution Team", som inkluderer et nettverk av eksperter.

VI. Hvordan kan forsikringsselskaper bistå?

1. Styrebehandling av datasikkerhet
Den tidligere styreleder i Lloyds, Lord Levene har i 2010 uttalt følgende:

"A discussion of digital risks should be on the agenda of board meetings everywhere as cyber attacks become more frequent, more creative and more disruptive. Cybercrime is an international business aided by those countries without the legislation framework to tackle it.
If we are serious about combating cybercrime, we need to increase international communication and collaboration between governments and businesses, and move towards uniform global regulation."

Lord Levene, Chairman of Lloyds (2010)

Det bør således kreves fra forsikringsselskaper i forsikringsavtalen at bedriftens eller institusjonens datasikkerhet alltid må være på agendaen til alle styremøter, og at styret alltid skal oppdateres og behandle redegjørelser om disse spørsmål.

2. Endring av forebyggende tiltak
Forebyggende tiltak bør endres fordi teknologitilbud og løsninger endrer seg. De nye risikoer som følge av "smart-teknologien" med IoT, IoE, og M2M må forebygges.

[12] Se www.aig.com/CyberEdge_3171_417963.html

Forsikringsdekning bør inneholde krav til å sikre data i seg selv, og ikke bare ved hjelp av brannmurer o.l.

Et nytt krav til forsikringstaker kan være innstallering av "Keyless Signature Infrastructure (KSI)"[13]:

"The Keyless Signature is an electronic stamp or digital fingerprint which enables the properties of the data to be verified using hash functions – cryptographically secure one-way operations that take arbitrarily-sized data as input and generate a hash value – a unique fixed-size bit sequence.
KSI provides an early warning system for the integrity breaches of any data by constant re-verification of existing signatures, making it possible to discover and remedy any vulnerabilities before large-scale damages can occur and ensuring business continuance and preventing hackers from covering their tracks."

VII. Konferanse i Singapore

Her er lenker til nærmere informasjon om "Asia Cyber Liability Conference" i Singapore 2-3. juli 2014. Konferansen var organisert av Asia Insurance Review, som er en ledende journal for forsikringsbransjen i Asia.

1. Profiles of Speakers & Sponsors
Se www.asiainsurancereview.com/aircyber

2. Omtale og referat fra konferansen
se www.asiainsurancereview.com av Charles Chau: *Prevention must complement insurance (August 2014)*
http://www.asiainsurancereview.com/Magazine/ReadMagazineArticle/aid/35317/Cyber-insurance-focus-Prevention-must-complement-insurance

Stein Schjølberg

[13] Se David Piesse, Insurance Lead & Advisory Board Member of Guardtime, Hong Kong & Ambassador, APAC, International Insurance Society; david.piesse@guardtime.com