1 INLEIDING IN CYBERCRIME

1.1 CYBERCRIME / OVERZICHT & ONTWIKKELING

- **Cybercrime:**

We spreken van cybercrime wanneer we spreken over misdaden die zijn gepleegd met behulp van computers en/of internet.

- **Cyberspace:**

Cyberspace is de ruimte die wordt gevormd door een netwerk van verbonden computers.

- **Internetcriminaliteit:**

De term internetcriminaliteit is een minder precieze term omdat niet voor elke misdaad met de Computer een internetconnectie nodig is.

- **ICT-criminaliteit:**

De beste en meest brede term is ICT (internet en computertechnologie) -criminaliteit.

- **Hightechcriminaliteit:**

Dit bevat zowel cybercrime (misdaden gepleegd met behulp van ICT) als computercriminaliteit. Dit zijn misdaden gepleegd met behulp van ICT, waarbij computers het expliciete doel zijn van de criminaliteit.

- **Wat is cybercrime?**

Cybercrime omvat elke strafbare gedraging waarbij voor de uitvoering het gebruik van geautomatiseerde werken bij de verwerking en overdracht van gegevens van overwegende betekenis is.

1.2 GESCHIEDENIS

- **Hacking:**

Een hacker is iemand die zwakheden vindt in een computer of computernetwerk. Hacking kan gemotiveerd worden door winst, protest of uitdaging. Een hacker breekt in in een afgelegen computer met behulp van een netwerk.

- **Local area networks & bulletin board services:**

Om informatiewisseling makkelijker te maken werden er local area networks (LAN) opgezet. Op één locatie, zoals bij een bedrijf, waren alle computers aan elkaar verbonden door ethernetkabels. Een kwaadwillig iemand die toegang had tot 1 pc had dus toegang tot alle pc's.

- **Bulletin board service (BBS):**

Vrij snel werd het mogelijk om pc's op verschillende locaties met elkaar te verbinden via modems en telefoonlijnen. De BBS zorgt ervoor dat pc's op afstand informatie konden uitwisselen. In deze periode verschenen de eerste versies van malware.

- **Worm:**

Een worm is een set van codes en verspreidt zichzelf van de ene pc naar de andere pc waar het connecties mee heeft (via de mailbox bijvoorbeeld), waar het zichzelf weer kopieert.

- **Virus:**

Een virus is verbonden met een file en wordt actief bij het openen hiervan. Virussen verhullen zichzelf vaak door zich voor te doen als nuttige programmma's.

- **White hats:**

De handhaving van politie & security experts op het internet.

- **Black hats:**

Criminele hackers met criminele doeleinden.

- **Grey hats:**

Heldhaftige, politiek gemotiveerde personen die vermeende wandaden van de overheid opsporen en bekend maken.

- **Profliferatie (vermenigvuldiging) en het internet:**

ARPAnet -> deze werd gecreëerd in 1969 door de defensie van amerika om pc's van universiteiten, labo's en bedrijven die met defensie te maken hebben, te verbinden.

National Science Foundation network (NSFnet) -> Dit was het begin van het internet zoals we dat nu kennen: een wereldwijd netwerk van onderling verbonden computers.

Spam -> spam is junk mail, wat in grote hoeveelheden een systeem kan vertragen. Probeert een reactie van de geadresseerde te krijgen.

Dos -> probeert effectief een systeem neer te halen door overflooding. Dit kan door veel emails te zenden (emailbommen) of malware.

- **Commodoficatie (commercieel maken), verfijning en penetratie (2000 – heden):**

Er doen zich 3 trends voor in de cybercrime sinds 2004: verfijning, commercialisering en organisatie. Verschillende soorten cybercrime:

Type 1 Klassieke misdaden waarbij een pc gebruikt wordt (kan zonder computers)

-> ging via krant of supermarktkaartjes

-> normale criminaliteit waarbij gebruik gemaakt wordt van een computer.

-> oplichting en bedreigingen, misdrijf tegen eigendom, personen en organisaties.

-> contact verloopt via mail, chat, online aankopen.

-> worden onder het klassieke strafrecht geclassificeerd.

CYBERCRIME IN RUIME ZIN (INSTRUMENT/MIDDEL)

-> bedreiging

-> smaad / laster

-> fraude

-> oplichting

-> heling

-> witwassen

-> relschoppen

-> valsheid in geschrifte

Type 2 Misdaden waar ICT ook het doelwit is (kan niet zonder computers)

-> criminele activiteiten waarbij ICT het doel is

-> misdaden die niet bestonden voordat er computer of internet was.

-> voorbeeld: hacken en infectie met malware, en ook een DDOS (distributed denial of service) dit houdt in dat een pc of netwerk wordt aangevallen met het doel het functioneren van het systeem te stoppen.

-> Niet al deze misdaden kunnen onder het klassieke strafrecht begrepen en geclassificeerd worden. Bv illegale toegang tot een computer (computervredebreuk) kan vergeleken worden met huisvredebreuk.

CYBERCRIME IN ENGE ZIN (ICT ALS DOEL/OBJECT)

-> computervredebreuk (hacking)

-> Malware (virus, botnet, spyware, ransomware)

-> verwijderen / aanpassen van gegevens

-> ICT sabotage (DDOS)

-> grootschalige auteursrechtinbreuk/softwarepiraterij

-> spam

-> phishing

1.3 DE EVOLUTIE VAN CYBERCRIME (2004 –HEDEN)

- **De wet van Moore:**

De wet van Moore stelt dat de capaciteit van computers elke 2 jaar verdubbelt.

- **3 fundamentele trends: geraffineerdheid, marketing & de organisatie**

-> **geraffineerdheid**: de complexiteit van methoden van cybecrime.

-> **marketing:** verwijst naar de winst en markten en de motivaties voor cybercrime.

-> **organisatie:** ogenschijnelijke diversiteit van de organisatorische vorm die de huidige cybercriminaliteit aanneemt.

- **Geraffineerdheid (verfijning)**

-> **botnets**: kunnen gebruikt worden voor verschillende illegale doeleinden, zoals spam, denial of service of versprijding van malware ter bevordering van een reeks financiele misdrijven. In p2p botnets communiceren besmette computers met elkaar en niet met een centrale commandolocatie. Hierdoor wordt de veerkracht en bestendigheid vebeterd.

-> na de evolutie van briefpost naar faxen naar emails waren de eerste fraudeverzoeken relatief ruw en zaten vol fouten in spelling en grammatica. Tegenwoordig zijn er betere technieken waardoor de uitnodigingen verfijnd zijn en erg overtuigend.

-> Vaak zijn toenaderingspogingen gericht op accademici, ze worden uitgenodigd om een conferentie te houden in een exotische locatie en worden gevraagd de registratie te betalen.

-> **Scareware:** scareware is een boodschap die meldt dat je computer in gevaar is gebracht in combinatie met een aanbod van een technologische oplossing voor een ‘goedkopere prijs’

-> **targeting**: er wordt contact gelegd met leden van een organisatie door het verkrijgen van toegang tot websites van de betreffende organisatie of door het identificeren van andere geselecteerde groepen van mensen met iets gemeenschappelijks (blogs / social networks). Dit zorgt voor een betere geloofwaardigheid van een verzoek.

-> **trojan horses:** zijn er al meer dan 3 deccenia, maar de verfijning waarmee ze tegenwoordig ontworpen zijn is groter dan ooit.

-> **kits:** huidige kits genereren alle informatie over de browsers en besturingssystemen die de slachtoffers gebruiken. Exploitkits worden ook steeds meer verfijnd.

-> **TOR-technologie**: op basis van multi layer codering zorgt ervoor dat internetgebruuikers kunnen internetten zonder hun locatie of identiteit te onthullen.

- **Commercialisatie (marketing):**

-> **botnets:** tegenwoordig worden botnets gebruikt voor een breed scala aan hebzuchtige misdaden (bijvoorbeeld pay-per-click), pay per downloadfraude, shareware en elektronisch betaalmiddelfraude.

-> **hacking tools:** tegenwoordig kunnen hackers ingehuurd worden, hackertools zijn gemakkelijk te downloaden, maar de betere tools (meestal uitdrukkelijk bedoeld voor kwaadaardige doeleinden kun je kopen of huren.

-> **Botnets kopen:** gemakkelijk te kopen of te huren. Deze bevatten versleutelde malware zodat ze moeilijk op te sporen zijn. Ze geven toegang tot servers om aanvallen te lanceren, waarborgen anonimiteit in de communicatie en leveren distributed denial of service aanvallen.

-> het zoeken naar en vervolgens verkopen van onontdekte fouten in computercodes.

-> **pre-commerciele groepen**: anonymous, een los collectief van anarchisten dat grotendeels gebaseerd is op een gedeelde ethos van onheil en wrok ten opzichte van het gezag.

- **Organisatie:**

-> veel cybercriminelen werken alleen.

-> **botnets**: kunnen gemaakt en ingezet worden door individuen of groepen, maar indien gebruikt voor illegale doeleinden. ze worden beschouwd als vorm van georganiseerde criminaliteit. Wanneer grote aantallen pc's worden aangetast en en ze onder controle staan van een botmaster dan worden de eigenaren van de aangetaste pc's onwetend medeplichtig aan een criminele onderneming.

- **Structuren:**

-> **Proxy servers:** door dit omgeleid verkeer via andere computers met het doel om de echte locaties van leden te maskeren was het voor onderzoekers moeilijk om de online activiteiten van leden op te sporen.

-> **dark market:** forum voor uitwisseling van gestolen creditcard- en bankgegevens, malware en gerelateerde technologie. Gegevens worden illegaal verkregen door bv skimmingapparaten, onbevoegde toegang tot informatiesystemen of door technieken van 'social engineering' waar de slachtoffers waren overgehaald om gegevens af te staan aan een ogenschijnlijke legitieme bron.

-> **anonymous:** minder formele organisatie en meer een los collectief van anarchisten. De groep houdt zich bezig met hacktivisme. Concentreerde zich op amerikaanse ministerie van justitie.

-> **Oekraïense ZeuS group:** software engineers uit oost-europa met malware beter bekend als verfijnd Zeus virus. Deze kwaadaardige code werd gebruikt om toegang te krijgen tot pc's van mensen die werkzaam zijn in kleine bedrijven, gemeenten en niet-overheidsorganisaties in de vs. Wanneer gebruiker bericht opent, krijgen de hackers toegang tot bankrekeningnummers en wachtwoorden.

- **Meest verfijnde cybercrime organisaties (aard en rollen die een frauduleuze samenzwering kan meebrengen:**

-> **codeurs / programmeurs**: schrijven malware, exploits en andere tools

-> **distributeurs of verkopers**: verhandelen / verkopen gestolen gegevens.

-> **technici**: onderhouden de criminele infrastructuur en onderstaande technologieën (bijvoorbeeld servers, ISP's, en encryptie

-> **hackers**: zoeken kwetsbaarheden in applicaties, systemen en netwerken met als doel toegang te krijgen tot beheer of loonlijsten.

-> **fraudespecialisten**: ontwikkelen en maken gebruik van van social engineering regelingen (zoals phishing, spammen en domeinbeheer kraken)

-> **hosts**: bieden veilige faciliteiten van illegale servers en sites. Meestal dmv botnets of proxy-netwerken

-> **cashers**: beheren drop accounts en geven de namen en rekeningen door aan andere criminelen voor geld. Beheren ook vaak geldkoeriers (money mules)

-> **money mules**: fungeren als derde partij voor de overdracht van de opbrengst van fraude door deze over te brengen naar een veilige locatie.

-> **tellers**: helpen bij het overdragen en witwassen van illegale opbrengst van fraude dmv digitale valuta diensten en het verwisselen van verschillende nationale munteenheden.

-> **uitvoerders van de organisatie**: selecteren doelen, werven leden en wijzen leden een van de bovengenoemde taken toe. Beheren de verdeling van de criminele opbrengsten.

- **De staat en door de staat gesponsorde cybercrime:**

-> toename in het volume van illegale activiteiten gepleegd door overheden of hun gevolgmachtigden

-> **actieve sponsoring door de staat**: stilzwijgende aanmoediging van niet-statelijke criminaliteit. De staat die een oogje dichtknijpt betreffende de betrokken activiteiten.

-> de aard en de omvang van deze activiteiten wordt verzwegen voor het publiek

-> **enkele voorbeelden**:

Russische regering steunde cyberaanvallen tegen estland en georgie. De term 'patriotic hackers' werd gebruikt om aanvallen van burgers van een land tegen een vreemde tegenstander aan te duiden.

Aanvallen tegen de website van het presidentieel kantoor en een aantal andere officiële media-sites in Zuid-korea. Wsl gecoördineerd vanuit Noord-korea.

- **Nog meer organisatievormen: er is een typologie opgesteld van cybercrime groepen, deze bestaat uit 6 groepen. 3 hoofgroepen telkens onderverdeeld in 2 subgroepen**

-> **type 1:**

Deze groepen werken online en kunnen onderverdeeld worden in 'swarms' en 'hubs' zijn meestal virtueel en verkrijgen vertrouwen via hun reputatie in online illegale activiteiten.

SWARMS: ongeorganiseerde organisaties met een gemaanschappelijk doel, zonder leiderschap. Minimale bevelen, opereren in virale vormen. Ze zijn ideologisch gedreven (anonymous)

HUBS: meer georganiseerd duidelijke commandostructuuur, het gaat om een centraal punt (hub) van de kern waar medewerkers zich omheen verzamelen. Online activiteiten zijn divers: bijvoorbeeld piraterij, phishing-aanvallen, botnets, scareware distributie en online seksuele misdrijven.

-> **type 2:**

Combineren online en ofline misdrijven en worden beschreven als 'hybride' die 'geclusterd' of 'extended' kan zijn.

GECLUSTERDE HYBRIDE: misdaad opgebouwd rond een kleine groep individuen, specifieke activiteiten of methoden, vergelijkbaar met hubs, maar ze bewegen feilloos tussen online en offline misdrijven. Bijvoorbeeld: ze skimmen creditcards en gebruiken gegevens voor online aankopen of verkopen de gegevens door middel van netwerken.

EXTENDED HYBRIDE: minder gecentraliseerd, veel medewerkerkers en subgroepen, voeren verschillende criminele activiteiten uit. Voldoende mate van coördinatie om succes van hun activiteiten te waarborgen.

-> **type 3:**

Deze groepen functioneren vooral offline, maar gebruiken online technologie om hun ofline activiteiten te vergemakkelijken. Worden onderverdeeld in 'hiërarchieën' en 'aggregaten'

HIËRARCHIEËN: traditionele criminele groepen (bv families) die deel van activiteiten online exporteren. Bv porno-websites, online gokken, afpersen/chanteren/bedreigen met het afsluiten van systemen. Bv de familie Gambino in de VS die valse barcodes en creditcards produceren.

AGGREGATEN: zijn tijdelijk en losjes georganiseerd. Vaak hebben ze geen duidelijk doel. Ze maken 'ad hoc' gebruik van digitale technologieën, die schade toebrengen. Bv gebruik van mobiele telefoons om bendes of misdrijven te coördineren, zoals de britse rellen in 2011.

-> **RECENTE TECHNOLOGISCHE ONTWIKKELINGEN:**

Mobiele telefoons: worden gezien als instrument voor diverse criminele activiteiten. Het ontsteken van explosieven op afstand, voor transmissie van frauduleuze bezoeken, verspreiding van illegale beelden van kinderen, kan gebruikt worden als afluisterapparaat, SIM-kaarten kunnen worden gecloned. Er worden nepapplicaties gemaakt, waarin malware verwerkt zit.

Draadloos internet: biedt strafrechtelijke mogelijkheden.Met de term 'war driving' wordt bedoeld het lokaliseren en het inloggen in hotspots (draadloze toegangspunten). Persoonlijke gegevens komen zo op een onbeveiligd netwerk van grote retailers.

Near-field technologieën: hierbij worden gegevens tussen apparaten uitgewisseld als de apparaten dicht bij elkaar in de buurt komen. Zo kunnen ook contactloze betalingen gedaan worden. Gebruik van speciale portemonees zou hiervoor wenselijk zijn.

Cloud computing: externe opslag van gegevens, besturingssystemen en applicatierdiensten. Online e-mailsystemen zijn het meest voorkomend. Cloud computing zorgt voor kostenbesparing op infrastructuren. Bestanden, computerkracht en software is toegankelijk via het web in plaats van via de individuele desktop. Clouds worden ook vaak gebruikt om illegale software te hosten zoals malware, illegale software en entertainment zoals kinderporno.

Voice over internet protocol (VOIP): technologie die spraakcommunicatie ondersteunt via internet in plaats van een openbaar telefoonnetwerk. SKYPE is 1 vd grootste.kon eerst moeilijk gemonitord worden maar tegenwoordig kunnen overheden deze data opslaan en analyseren.

Social media: dit kan de productiviteit van werknemers verminderen en kan kwetsbaarheid voor industiële spionage vergroten. Er kunnen zeer veel persoonsgegevens op iemands facebookpagina staan. Deze kunnen worden uitgebuit door afpersers en stalkers. Accounts kunnen worden gehackt. Inbrekers halen hier ook hun info uit wanneer iemand op vakantie is.

- **Internet of things (IOT):**

Het internet of things betreft de verbinding van apparaten (anders dan computers en smartphones) die via het internet worden vastgelegd. Auto's, keukenapparatuur en zelfs hartmonitoren. Simpel voorbeeld is de relatie van een kassascanner in de supermarkt om de inhoud van voorraad bij te houden. De mens wordt door nieuwe technologieën gesurveilleerd en dat maakt diverse criminele activiteiten mogelijk. Bijvoorbeeld diefstal, inbraak, afpersing en terrorisme.

-> verder in de toekomst:

‘Brain-to-brain' technologie of ‘computer-to-brain’ technologie kunnen kwetsbaar zijn voor criminele uitbuiting, men kan stellen dat deze technologieën niet langer behoren tot science fiction.