5 WETGEVING

5.1 BELANGEN

- **Inbreuken op cybersecurity schaden individuele, organisatorische en maatschappelijke belangen.**
- **Verminderd vertrouwen in digitale diensten en werkt als rem op de bedrijvigheid.**
- **Door berichtgeving over datalekken, uitval van ICT etc. Zijn mensen terughoudender met het gebruik van systemen.**

  -> rem op economische groei.

  -> nieuwe toepassingsgebieden leveren kwetsbaarheden en een debat op.

  -> door nieuwe manier van toepassing ICT, ook nieuwe manieren van trespassing

- **Gedigitaliseerde mobiliteit vergt gescheiden netwerken**

  -> auto's vliegtuigen en andere vervoersmiddelen worden voorzien van ICT-mogelijkheden.

  -> ontwikkeling bij de bestrijding van 'gedigitaliseerde mobiliteit' = gescheiden netwerken

  -> niet de bedoeling dat fout in entertainmentsysteem van vliegtuig de besturing aantast.

- **Analoge alternatieven verdwijnen:**

  -> wanneer ICT-systemen uitvallen vaak geen analoge alternatieven meer, kan leiden tot ernstige gevolgen

  -> ICT-systemen zijn op hun beurt veel complexer dan de analoge alternatieven, dat maakt ze sneller vatbaar voor uitval.

  -> overheid streeft naar digitaal contact met de burgers, betalingsverkeer kent steeds minder analoge alternatieven.

  -> hoewel het beveiligen van informatie en systemen telkens nieuwe uitdagingen creëert, zijn de achterliggende redenen voor het beveiligen nauwelijks verandert.

- **Vooruitblik:**

  -> betrouwbaarheid van software wordt belangrijker nu ICT-systemen op meer plaatsen worden toegepast.

  -> belangen van de vitale sectoren blijven ook de komende jaren gelijk.

  -> de organisaties in deze sectoren zijn door hun ervaring beter in staat om voor deze belangen in te staan.

- **Achtergronden:**

  -> **begripsbepaling:**

  Cybercriminaliteit kan worden omschreven als strafbare feiten ‘gepleegd door gebruikmaking van elektronische communicatienetwerken en informatiesystemen of tegen dergelijke netwerken en systemen.

  -> cybercriminaliteit kan onderscheidt worden in 3 typen

  a. Computergerichte delicten: strafbare feiten gepleegd tegen computers, computernetwerken of computergegevens, hierbij fungeren computers of gegevens als doel
  b. Computer-gerelateerde delicten: strafbare feiten gepleegd met gebruikmaking van computers, netwerken of gegevens. Hierbij fungeren computers of gegevens als substantieel hulpmiddel, speelt relevante rol bij plegen van het delict
  c. Computer-relevante delicten: strafbare feiten waarbij computers, netwerken of gegevens relevant zijn als omgevingsfactor, hierbij zijn computers en gegevens een niet substantieel hulpmiddel.

- **Criminologische context:**

  -> **criminologe factoren:**

  -> internet is wereldwijd, er is sprake van deterritorialisering (uitroeing van sociale, politieke, of culturele praktijken uit geboorteland plaatsen en volkeren)

  -> flexibelere netwerken tussen daders

  -> interactie tussen dader en op afstand, beperkte ‘capable guardianship’

  -> anonimiteit, manipuleerbaarheid van programmatuur

  -> data, automatisering van aanvallen, grotere schaal om misdrijven te plegen

  -> grote winst behalen door aggregatie

  -> informatie-economie waarin gegevens geld waard zijn

  -> snelle ICT-innovatiecycli

  Al met al betekent dit dat het internet een ‘opportunity structure’ schept voor het plegen van criminaliteit.

-> emperische kennis over omvang van cybercriminaliteit is niet groot:

-> hoog 'dark number' omdat slachtoffers vaak geen aangifte doen of zelfs niet weten dat ze betrokken zijn bij een aanval

-> dark number is een term die door criminologen en sociologen wordt gebruikt om de hoeveelheid niet gerapporteerde of niet ontdekte criminaliteit aan te geven.

-> drie types hackers:

-> jeugdige crimineel: voor de lol, nieuwschierigheid, indruk maken

-> ideologische hacker: is veelal intelligent, soms obsessief en anti-sociaal

-> financieel gemotiveerde hacker: e-fraudeurs die geld rieken

5.2 WELKE STAPPEN HEEFT DE EU ONDERNOMEN?

- Wetgeving ronde cybercriminaliteit stimuleren en te harmoniseren dit leidde tot het CCV (CyberCrime Verdag)
- Strafbaarheid over racistische uitlatingen werd door de vrije meningsuiting hierin niet opgenomen door de VS
- Seksueel misbruiken van minderjarigen werd geregeld in het verdrag van lanzarotte

-> **drie kamerbesluiten opgenomen (inmiddels vervangen door richtlijnen):**

-> fraude met niet chartaal geld

-> aanvallen op computersystemen

-> seksuele uitbuiting van kinderen en kinderpornografie

- **In 2017 EU-brede regels opgesteld ter bestrijding van aanvallen op informatiesystemen:**

-> **volgende overtredingen worden geconfronteerd met strafrechtelijke sancties:**

a. Illegale toegang tot systemen
b. Systeeminterferentie
c. Onderschepping strafbare feiten
d. Makers van botnets
e. Makers van malware

-> **richtlijn betreffende aanvallen tegen informatiesystemen:**

Nieuwe regels opgesteld om een snellere samenwerking tussen de wetshandhavingautoriteiten van de lidstaten te versterken.

-> Europese agenda voor beveiliging:

- **Duidt cybercrime aan als één van de drie topprioriteiten voor het huidige mandaat van de europese commisie op het gebied van veiligheid:**

  -> gebruikers hebben het recht om zich veilig te voelen online

  -> fundamentele rechten van de EU-burgers mogen niet geschonden worden

  -> onze economie mag niet geschaadt worden door cybercrime

  -> daders mogen niet denken dat ze straffeloos mogen handelen

  -> vertrouwen in online diensten moet versterkt worden

- **Cybercrimes zorgen voor aanzienlijke kosten voor de EU-economie:**

  -> bezorgdheid van gebruikers over online veiligheid is de afgelopen jaren gestegen

  -> 85% is van mening dat het risico op slachtofferschap vergroot zal worden

  -> 73% bezorgd over hun persoonlijke informatie die online te vinden is

  -> 42% bezorgd over de beveiliging van online bankieren

  -> 13% koopt geen goederen online uit wantrouwen

  -> 12% is nog niet klaar om online te bankieren

- **Victimisatie is ook toegenomen:**

  -> 14% had beperkte tijd geen toegang tot online diensten wegens cyberaanvallen

  -> 12% zag hun sociale media- of email accounts gehackt worden

  -> 16% ervaarde online fraude op e-commerce websites

  -> 8% slachtoffer van ransomware en malware

  -> 8% slachtoffer van creditcard- of bankfraude online

  -> 7% diefstal van identiteit

  -> 7% zegt dat ze per ongeluk kinderpornografie zijn tegengekomen online

- **Richtlijnen zorgen voor een effectieve reactie op deze bedreigingen in de EU**

  -> strafrechtelijke regels zorgen voor een nieuw offensief tegen cybercrime

  -> het versterkt ook de samenwerking tussen rechterlijke macht en de politie

  -> verplichting voor lidstaten om beter gebruik te maken van het 24/7 netwerk van contactpunten door dringende verzoeken binnen bepaalde termijn te behandelen

  -> 10 van de 28 staten staten bevestigd dat ze de richtlijnen hebben opgenomen in hun nationale wetgeving

  -> EU-commisie heeft ook een specifiek Europees Cybercrime Center in Europol opgericht om wetshandhavingsinstanties van de lidstaten te ondersteunen en de operaties te coördineren.

  -> Wereldwijde alliantie tegen seksuele misbruik van kinderen online (54 landen)

- **Volgende stappen:**

  -> 2 vlaggenschipstrategieën:

  -> Europese agenda voor veiligheid

  -> strategie voor digitale interne markt

  -> wijzen op noodzaak om beter cyberdreigingen aan te pakken en de inzet van de EU voor de hoogste normen voor privacy en gegevensbescherming

  -> toekomstige initiatieven omvatten het herzien van het toepasselijke juridische kader voor specifieke overtredingen zoals:

  a. Fraude en vervalsing van niet-contante betalingsmiddelen
  b. Opsporen van belemmeringen voor strafrechtelijke onderzoeken
  c. Regels inzake toegang tot bewijsmateriaal en informatie
  d. Effectievere rechtshandhavingsrespons
  e. Versterken van het opbouwen van acties op het gebied van de capaciteit van buitenlandse hulpverlening

5.3 EUROPOL

-> op 11 mei 2016 is de nieuwe verordening van kracht gegaan

-> europol het middelpunt van bestrijding tegen terrorisme, cybercriminaliteit en andere ernstige en georganiseerde vormen van criminaliteit

-> een versterkt europol is vanaf heden een politieke prioriteit en zal europa in staat stellen een vuist te maken tegen terroristen en criminelen

- Nieuwe verordening zal het europol gemakkelijker maken om gespecialiseerde eenheden op te stellen die onmiddelijk kunnen reageren op opkomende terroristische dreigingen:

  -> Europees Counter Terrorism Center (ECTC)

  -> European Union Internet Referral Unit (EU IRU)

  -> deze worden beiden door europol gehost.

  -> deze nieuwe bevoegdheden van europol zullen het vermogen van europol vergroten om te fungeren als informatiehub van de EU in de strijd tegen terrorisme en ernstige georganiseerde misdaad

  -> er wordt gestreefd naar verhoogde beveiligingsmaatregelen voor gegevensbescherming, democratische beheersing en parlementaire beheersing.

  -> het toezicht op europol wordt vanaf 1 mei 2017 door de europese toezichthouder voor gegevensbescherming uitgevoerd.

- Hoofdkantoor in den haag

- Is het agentschap voor wetstoepassing van de EU

- Staat de nationale autoriteiten bij door informatie-, inlichtingenanalyses en bedreigingen uit te wisselen

- Behandelt terrorisme en internationale criminaliteit, zoals cybercriminaliteit, drugssmokkel en mensenhandel