11 FORENSISCH ONDERZOEK: ONDERZOEK NAAR CYBERCRIME

11.1 MINDSET & TECHNISCHE VAARDIGHEDEN

-> Georganiseerde cyberaanvallers omzeilen met gemak veiligheidsmaatregelen en stelen daardoor makkelijk geld en informatie. Geavanceerde aanvallen tonen de kwetsbaarheden in draadloze netwerken waardoor gegevens gestolen kunnen worden.

-> criminelen 'vermommen' zich als gewone gebruikers om zo geen argwaan op te wekken, om hier tegen op te treden is doorgewinterd leiderschap en kennis nodig

-> helaas worden binnen de overheid kritische positites vaak ingevuld door mensen met weinig technische kennis

-> wanneer je echt wil optreden tegen deze criminelen, zou je juist moeten denken als deze criminelen en dus met de tijd meegaan

-> ook is het van belang mensen met een forensische achtergrond te behouden, omdat je juist een andere kijk hebben op een onderzoek

-> van belang is ook dat er genoeg goede mensen zijn met verschillende kwaliteiten die elkaar kunnen versterken. Het is wel lastig om zulke teams te hebben en te behouden, vanwege de bezuinigingen

-> men moet over een rijtje 'hard skills' en 'soft skills' beschikken die ze in praktijk kunnen brengen:

-> **soft skills:** communicatief, rationeel, samenwerkend, intuïtief, samenhangend, veerkrachtig, stipt, kieskeurig, gedisciplineerd en strategisch

-> **hard skills:** onderzoekend, bewust, kennis van bewijs, forensische voorstelling, netwerk architectuur, hardware, bestandsystemen, gestructureerde data analyse, ongestructureerde data-analyse, semigestructureerde data-analyse, hoe de software wordt ontwikkeld, programmering en scripting, virtualisatie en hoe je technische rapporten moet maken

11.2 WAT IS TOEGESTAAN BIJ ONDERZOEK?

-> Cybercrime onderzoek kan inhouden dat er gericht gezocht wordt, dat er wordt gesurveilleerd en het monitoren van activiteiten

-> huiszoekingen en inbeslagname is een bepaalde manier van onderzoek, wat het ontdekken van bewijs, het identificeren van verdachten, aanhoouden van de daders en getuigen interviewen inhoudt

-> er zijn een aantal wetten die zorgen voor een minimale norm waar landen aan moeten voldoen, deze hebben te maken met privacy en vrijheid van meningsuiting

-> toch is het lastig om deze toe te passen op de cyberspace, omdat het relatief nieuw gebied is en er in elk land andere regels en wetten gelden

-> in de meeste landen heb je een bevelschrift nodig voordat je iemands spullen mag doorzoeken

-> in sommige gevallen wanneer er snel gehandeld moet worden omdat er anders data verloren gaat mag er op dat moment direct gezocht worden, maar wel met een beperking, regels hangen af van het land en de situatie

-> vastleggen van cybercrime roept nog wel eens problemen op aan administratieve kant, er is nog weinig op ingericht om dat goed vast te leggen en veel mensen zijn onwetend

-> als voorbeeld wordt gegeven dat een rechter dacht dat cybercrime het stelen van een computer was

- **Opgeslagen communicatie:**

  -> onderzoek vindt meestal plaats na de misdaad, rechercheurs moeten dan ook informatiestromen zien terug te brengen naar de basis

  -> een IP-adres is hier fnudamenteel en kan veel informatie opleveren, met de juiste autorisatie kan ook andere informatie worden opgevraagd, waaronder telecommunicatie, er kan bv gekeken worden welke telefoons op een bepaald moment aan een bepaalde mast waren verbonden

  -> welke informatie de rechercheurs uiteindelijk krijgen hangt voor een groot deel af van de bevoegdheden, maar ook van de tijd die ergens in wordt gestopt.

    -> soms kan je veel data hebben maar maar dit moet je ook kunnen analyseren, die capaciteit moet wel beschikbaar zijn

  -> de bewaarplicht van data blijft een controversieel ding, hier is ook nog geen oplossing voor gevonden. **Want wanneer is dit strict noodzakelijk?**

    -> wat eerst niet belangrijk leek kan nadien van cruciaal belang zijn

    -> hoe ga je hier mee om zonder dat je de privacy schaadt? Een vraagstuk waar nog geen kant-en-klare oplossing voor is gevonden

- **Bewaken en onderscheppen:**

  -> sommige nationale wetten zorgen ervoor dat wanneer politie en veilighheidsdiensten een gerechtelijk bevel krijgen, ze de communicatie tussen computers mogen onderscheppen

  -> dit gebeurt in principe alleen bij dringende en uitzonderlijke gevallen

  -> de regels omtrent interceptie verschillen per land. Als voorbeeld wordt het Verenigd Koninkrijk gegeven waarin de volgende dingen mogelijk zijn:

    -> **Interceptie communicatie:** het verkeer en de inhoudelijke gegevens

    -> **Indringende surveillance**: heimelijke in particuliere gebouwen en voertuigen

    -> **Gerichte surveillance:** heimelijk op een openbare plaats

    -> **Gebruik geheime menselijke intelligentiebronnen:** undercover agenten

    -> **Monitor communicatiegegevens:** opnames gerelateerd met communicatie, maar niet de inhoud van dergelijke communicatie

  -> het is lastiger wanneer blijkt dat data over de internationale grenzen gaat omdat elk land andere regelgeving heeft. Het is dus belangrijk dat de rechercheurs kennis hebben van regels in en verdragen met andere landen

  -> In België en Nederland is dit nog een onderwerp van discussie:

    -> op dit moment mag de politie onder bepaalde voorwaarden computers, telefoons en andere apparatuur hacken als ze daar fysiek bij kan

    -> het mag alleen om communicatie te onderscheppen, maar de regering wil ook dat de politie dit vanop afstand kan doen

    -> bovendien moeten agenten op afstand foto's kunnen maken met telefooncamera's, gesprekken kunnen afluisteren of bepaalde informatie zelfs ontoegankelijk maken

  -> Volgens de autoriteit Persoonsgegevens wordt de privacy daarbij niet voldoende gewaarborgd. Hacken zou alleen moeten kunnen bij georganiseerde misdaad, terrorisme of levensbedreigende zaken. Ook moet er beter controle op gebruik van de bevoegdheden komen

  -> In België wordt een wetsontwerp voorbereid over de modernisering van de bijzondere opsporingsmethoden. Speuren naar digitaal bewijs van misdrijven moet makkelijker worden met de nieuwe wet

-> de wetgeving die bepaalt hoe politie en justitie bewijs van misdrijven mogen verzamelen, is niet aangepast aan de digitalisering van het dagelijkse leven

-> het legt onder meer vast wanneer en hoe de politie berichten, foto's en andere informatie op je smartphone mag bekijken, toegang mag nemen tot je facebook- of Instagramprofiel of (vanop afstand) in je laptop mag inbrekene om gegevens te zoeken of om stiekem te volgen wat u op uw computer doet

-> de maatregelen moeten enkel mogelijk zijn wanneer ze ook echt nodig zijn om misdaad te bestrijden

-> het toezicht van een rechter is een van de centrale waarborgen in het Belgisch rechtsysteem

-> wanneer politie of parket bijvoorbeeld een huiszoeking of telefoontap wil regelen, moeten ze dat aan de onderzoeksrechter voorleggen

-> alleen met rechterlijk akkoord kan zo'n indringende maatregel worden uitgevoerd

-> maar de controle door de onderzoeksrechter wordt de laatste jaren systematisch teruggeschroefd en die trend zet zich in het nieuwe wetsontwerp duidelijk verder.

-> Het Openbaar Ministerie kan echter zonder voorafgaande rechterlijke controle je persoonlijke informaticasystemen, zoals uw smartphone of laptop, openlijk uitlezen

-> Verder voorziet het wetsontwerp in een bevoegdheid om heimelijke laptops, smartphones en andere IT-systemen binnen te dringen en te doorzoeken, ook in België zijn hierover de nodige discussies gaande

- **Proactieve strategieën:**

-> steeds meer gespecialiseerde eenheden die zich bezig houden met misdaden via het web

-> door de relatieve anonimiteit op het web kan het vertrouwen van een verdachte worden gewonnen en op die manier informatie worden uitgelokt. Wel is het belangrijk dat de rechercheurs veel kennis hebben over de wet zodat er wel een zaak kan worden opgebouwd

- **Crime Scene en Forensische Diensten:**

  -> digitale onderzoeksmogelijkheden zijn de afgelopen jaren sterk verbeterd

  -> digitaal forensisch onderzoek is een onderdeel van de forensische wetenschap

  -> het is een langdurig proces en het doel is niet pure kennis verkrijgen, maar praktische veronderstelling krijgen

  -> de onderzoeksuitdaging is één van lokaliseren, identificeren, vergelijken en interpreteren van diverse bronnen van potentiële bewijsmateriaal

- **CONCLUSIE:**

  -> Cybercrime is heel complex, kennis van regels en wetten is erg belangrijk, ook omdat het zo wereldwijd is en je met andere landen te maken hebt. Verder is ook specifieke technische kennis van belang, anders loop je altijd achter de feiten aan. Het zal ook altijd complex blijven, want het wordt nu eenmaal steeds complexer met steeds meer gebruikers en steeds nieuwe mogelijkheden. Het is dus belangrijker om zelf ook te blijven ontwikkelen.

11.3 BELEMMERINGEN BIJ HET VINDEN EN ANALYSEREN VAN BEWIJSMATERIAAL

-> de hoeveelheid ruwe data die tijdens opsporingsonderzoek verzameld wordt legt grote druk op analisten om betrouwbare resultaten te leveren binnen zeer korte tijd. De ruimte op interne en externe harde schijven neemt heel snel toe

-> Wetshandhavingsautoriteiten lopen achter de feiten aan, hebben een grote achterstand aan apparaten die geanalyseerd moeten worden.

  -> binnen haalbare grenzen van arbeidskracht en prioriteitenverschuiving is het niet haalbaar om alle gegevens die op een plaats van delict worden ontdekt te onderzoeken.

  -> deze knelpunten worden verergerd door het ontbreken van prioriteitsstrategieën en inadequente budgetten voor personeel en opleiding

-> Als de politie bedrijfsruimten betreedt tijdens inbeslagnames en draaiende elektronische apparaten losgekoppelt om **ESI (electronically stored information)** te kunnen verzamelen, kunnen er juridische gevolgen zijn

-> Verstoren of belemmeren van bedrijfsvoering kan opsporingsinstanties blootstellen aan langdurige rechtszaken en aansprakelijkheid

-> schadevergoedingen voor belemmerde commerciële activiteiten kunnen zeer kostbaar zijn, waardoor de politie ontmoedigd wordt om goed onderzoek te doen

-> jarenlang was het de standaard om gewoon de stekker eruit te trekken

-> tegenwoordig hebben veranderingen in hardware- en softwareafhankelijkheden een doordachte aanpak van de politie noodzakelijk gemaakt

-> **Live Forensics:**

-> bestaat uit een analysetechniek van het verkrijgen van bewijsstukken uit een actief draaiend apparaat

-> vergankelijke data die blijft bestaan in het RAM en randapparatuur moet live worden vastgelegd om ervoor te zorgen dat de informatie wordt bewaard.

-> ook bij volledige schijfencryptie en externe verbindingen met IT-processen kan een live forensische procedure nodig zijn.

->Elke live procedure uitgevoerd op een actief apparaat zorgt voor wijzigingen in het systeem.

-> daarom wordt iedere activiteit die gegevens op een systeem verandert ontmoedigd

-> deze informatie vormt doorgaans het oorspronkelijke bewijs en de eventuele wijziging van het bestand en metadata is verwant aan het besmetten van een delict

-> Cloud Computing & Data mapping:

-> Persoonlijke, publieke en private domeinen worden steeds meer met elkaar verbonden door middel van netwerkinfrastructuur, variërend van een klein aantal aangesloten apparaten tot duizenden apparaten verbonden door middel van virtual private networks

-> de populariteit van clouud computing heeft grensoverschrijdende opsporings- en privacykwesties aangewakkerd, omdat de binnenlandse wetgeving lokaal is en de cloed globaal. In hun datacenters bieden **Cloud Service Providers (CSP's)** toegang tot krachtige netwerkinfrastructuren

- **Wat is Cloud-Computing?**

-> bij cloud computing wordt via een netwerk, doorgaans op het internet, op aanvraag hardware, software en gegevens beschikbaar gesteld voor een netwerk met alle computers die erop aangesloten zijn

-> het vormt een 'wolk van computers' waarbij de eindgebruiker niet weet op hoeveel of welke computers de software draait of waar die computers precies staan

- **Wat is Data-Mapping?**

  -> Mapping betekent letterlijk: in kaart brengen. Hierbij gaat het om het in kaart brengen van gegevens

- **De kwetsbaarheid van de cloud:**

  -> Aan gebruiukers worden middelen geleverd als een dienst, welke die op afstand toegankelijk zijn via een netwerk

  -> cloud computing heeft een groeiend klantenbestand en biedt cybercriminelen wereldwijd zowel een gecentraliseerde groep slachtoffers, als ook nieuwe wegen om digitale bronnen te exploiteren en detectie te ontwijken

  -> Clouddiensten kunnen het doelwit zijn van criminele activiteiten zoals onbevoegde toegang, systeem sabotage, diefstal van gegevens, spionage, etc

  -> kunnen worden ingezet als een middel voor het plegen van criminele activiteiten, bv afleverplaats voor gestolen gegevens, verspreidplaats van kindermisbruik materiaal, platform voor het plegen van fraude, etc.

  -> onderzoekers komen tijdens inbeslagname regelmatig apparaten tegen die verbonden zijn met clouddiensten. Vanwege geautomatiseerde cloud back-ups en synchronisatie tussen verschillende apparaten wordt data vaak gerepliceerd over verschillende cloud-computingomgevingen

  -> deze informatie kan belangrijke aanwijzingen bieden over slachtofferschap, hoe een dader een misdrijf pleegt en het bewijs van eerdere handelingen aantonen

    -> procedures voor onderschepping van gegevens kunnen toegang tot gegevens die zijn opgeslagen via clouddiensten vereenvouudigen.

    -> wanneer echter CSP's actief zijn die meerdere landen omvatten, kunnen gegevens van individuele gebruiukers geografisch verspreid zijn en mogelijk gepoold met gegevens van andere gebruiukers. Dit belemmert het opsporingsonderzoek aanzienlijk

    -> behoud van bewijs kan complex zijn, als zowel opgeslagen als verzonden gegevens kunnen worden opgehaald uuit verschillende punten van oorsprong binnen de cloud-computing infrastructuren bv. Grensoverschrijdende datastromen, data back-up, synchronisatie, enz.

    -> dit is van invloed op de wettelijke bepalingen inzake toegang tot de gegevens en de openbaring

- **Openbaar Cloudbeheer:**

  -> met meerdere beheerders kan een mijnenveld aan technische en privacy-kwesties veroorzaken voor onderzoekers.

  -> problemen ontstaan wanneer de gegevens die door het doelwit van onderzoek zijn opgeslagen op een fysiek apparaat, worden gedeeld met andere cloudcomputers

  -> vanwege potentiële impact op derden verbiedt dit het in beslag nemen of aflezen van het apparaat.

  -> ook zijn veel digitale forensische tools niet geschikt voor het aflezen van gegevens van cloud-computing-omgevingen

  -> de politie vereist gewoonlijk de hulp van systeembeheerders in datacenters om de toegang tot de gegevens te vergemakkelijken

  -> datareplicatie en het gebruiuk van gedistribueerde bestandssystemen door datacenters voor load balancing kan ook kwesties opwerpen gerelateerd aan data-mapping, omdat deze politie-informatie over de nationale grenzen heen kan worden verspreid

  -> de moeilijkhijd voor de opsporingsinstanties ligt in het in kaart brengen van de locatie waar de data word gehost, het opsporen van het geografische traject waarlangs de gegevens zich bewegen, en een vaststelling van de wetten over gegevensbehandeling binnen deze rechtsgebieden

- **Op internet gebasseerde en satelietcommunicatie:**

  -> Voordat er smartphones waren met communicatie via het internet, ging de meeste digitale telecommunicatie via vaste lijn schakelaars of mobiele communicatietorens.

  -> deze gecentraliseerde routing configuraties voorzagen opsporingsinstanties van informatie over de abonnee en de verkeersgegevens.

  -> opslag en gelokaliseerde transmissies van telecommunicatiegegevens vergemmakelijkte toezicht en onderscheppingsactiviteiten konden met relatief gemak worden aangevraagd bij de rechter

  -> na verloop van tijd werd het bereik van instrumenten zoals CALEA en RIPA uitgebreid naar **Voice over Internet Protocol (VoIP)** en faciliteiten op basis van breedbandinternet modaliteiten die volledig verbonden zijn met het publieke telefoonnetwerk

-> door wijzigingen in de wet zijn de autoriteiten in de VS, mits bij de rechtbank aangevraagd, gemachtigd tot elektronische bewaking van de inhoud van gegevens die via internetgebasseerde communicatie wordt verzonden

-> lokale bedrijven en buiitenlandse bedrijven met zakelijke activiteiten in de VS moeten zich schikken als er een aftap-bevel wordt ingediend.

-> dit geldt ook voor versleutelde e-maildiensten, sociaal netwerksites, en aanbieders van spraak en videoconferenties, instant messaging en file sharing software.

-> het meewerken strekt zich uit tot het maken van veranderingen in de structuuur van hun diensten om toezicht en onderscheppen makkelijker te maken

-> de autoriteiten kunnen serviceproviders ook dwingen om de cryptografische sleutels die ze gebruiken voor het beveiligen van gegevens af te staan

-> echter, deze juridische instrumenten zijn vooral gericht op telecommuunicatiebedrijven die mobiele telefoondiensten en traditionele telefonie leveren, hebben geen betrekking op populaire en opkomende internet gebasseerde communicatiediensten

-> de komst van peer-to-peer netwerken, die communicatie via vaste breedband internetverbindingen en draadloze toegangspunten kunnen uitzenden, is een fikse uitdaging voor opsporingsinstanties.

> -> surveillance is hierbij veel moeilijker omdat zuiver peer-to-peer-netwerken geen centrale server hebben

-> onderschepping wordt ook problematisch, omdat communicatieprotocollen encryptie gebruiken om privacy te behouden.

-> de nationale veiligheidsdiensten hebben gelobbyd dat de mogelijkheid om strafrechtelijke en terreurverdachten af te luisteren achteruit gaat als mensen in toenemende mate online communiceren in plaats van via de telefoon. Dit is deels te wijten aan de private structuur van sommige peer-to-peer-netwerken

BELANGRIJK:

De mobiliteit en geheimhouding die door gecodeerde sattelietcommunicatiesystemen wordt geboden heeft deze technologie populair gemaakt onder georganiseerde criminele groepen

-> sommige satelietcommunicatie providers stellen gebruuikers in staat om hun dienstverlening te configureren zodat abonnee en inhooud van data wordt opgeslagen in een rechtsgebied van hun keuze

-> Als zodanig opgeslagen data wordt onderworpen aan de wetten van het land waar de sateliet gebasseerde abonementsdienst is gevestigd, wordt het bewijs vaak buiten het bereik van de wetshandhaving geplaatst

-> ongetwijfeld hebben zowel breedband en stateliet-telefonie ingrijpend invloed op de capaciteit van de opsporingsinstanties om gegevens te onderscheppen en de communicatie te controleren

-> de encryptie technologie is wijdverspreid en wordt immuun voor controle door de nationale staten. Gedecentraliseerde open source beveiligde communicatieplatforms zijn in opkomst

-> Deze tools integreren beveiligde instant messaging, voice- en videoconferencing klanten zonder de noodzaak voor signaleren of centrale servers

-> de effectiviteit van deze instrumenten en protocollen wordt beïnvloed door de betrouwbaarheid van elke betrokkene

-> indien 1 van beide partijen worden geïnfiltreerd en de basis besturingssysteem in het gedrang komt, kunnen transmissies met gemak worden onderschept

- **Anonimiteit:**

-> e-maildata is vaak een belangrijke bron van bewijs voor politieonderzoek

-> titelinformatie binnen e-discussies kan de politie helpen bij het identificeren van de oorsprong van bepaalde communicatie en zelfs kan de fysieke locatie van een verdachte worden vastgesteld

-> de inhoud van berichten en e-mailbijdragen kunnen ook persoonlijke gegevens over daders en co-samenzweerders blootleggen, met inbegrip van:

  - Financiële transacties
  - Direct bewijs in verband met criminele activiteiten
  - Evenals gedetailleerde verslagen van de commuunicatie tussen daders en slachtoffers

- **Remailers:**

  -> criminelen die die geavenceerde misdaden plegen zijn zich terdege bewust van de zwakke plekken in normale e-transmissies

  -> in plaats daarvan zullen ze veilige web-based e-mail diensten, remailers en andere anonimiserende methoden gebruiken om discreet te communiceren

  -> anonimiserende remailers zijn eigenlijk intermediaire mailservers die functioneren als een poort tussen de afzender van de e-mail en de ontvanger ervan

  -> wanneer email door de remailer service gaat, kun je geen informatie meer detecteren uit de e-mail header. De inhoud van berichten, inclusief bijlagen, kan dan anoniem doorgestuurd naar de ontvanger. Ook dit vormt een struikelblok voor opsporingsdiensten

- **Deaddropping:**

  -> is een techniek die web-mail diensten exploiteerd om geheime communicatie mogelijk te maken.

  -> verdachten delen accountgegevens en communiceren in het geheim via niet verzonden berichten, die worden opgeslagen in web-mail-accounts, gevestigd in rechtsgebieden buiten het bereik van de opsporingsautoriteiten.

  -> deze methode van uitwisseling laat toe dat informatie doorgegeven wordt tussen de partijen, zonder risico op onderschepping

  -> Criminelen hebben toegang tot deze ‘virtuele afleverplaatsen’ via openbare toeganf terminals en internet hotspots om detectie te omzeilen

  -> cybercriminelen exploiteren ook proxy servers om online activiteiten te verbergen. Via proxy-diensten kunnen gebruikers verbinding maken met een netwerk via een tussen-server

  -> gemeenschappelijke proxy-servers kunnen worden geconfigureerd voor toegangscontrole, cashing diensten en verbeterde informatiebeveiliging.

  -> een anonieme proxy staat toe dat gebruikers zich registreren met contant geld of Bitcoinbetalingen om hun identiteit te verbergen. Eenmaal geconfigureerd, kan een versleutelde ‘multi-hop’ proxydienst worden ingezet om een IP-adres te verbergen

- **Verduistering en encryptie:**

  -> bij inbeslagname kan het heel moeilijk zijn voor de politie om fysieke apparaten op een plaats van delict te vinden

    -> externe harde schijven worden vaak geïntegreerd in persoonlijke spullen zoals speelgoed, pennen, en sieraden. Micro-SD kaarten, moniele SD-kaarten en draadloze opslagapparaten kunnen worden verborgen in spouwmuren, onder dakpannen en in het plafond of de vloer

    -> zelfs als onderzoekers in staat zijn om verborgen apparaten te vinden, kan de inhoud van de gegevens die op deze apparaten staat zijn gecodeerd

    -> steganografie is een 'informatie-smokkel' techniek die informatie in gewone bestanden, zoals grafische afbeeldingen, documenten en audio-opnamen

  -> onderzoekers zijn in staat om het gebruik van teganografie te detecteren door het toepassen van 'steganalyse' die de ondertekening van een verdacht bestand vergelijkt met een bekend origineel om inconsistenties te vinden.

  -> zelfs steganalyse heeft weinig waarde wanneer steganografie gecombineerd is met cryptografie. Netwerk steganografie is erg moeilijk te detecteren vanwege heimelijke manipulatie van verloren, beschadigd, verborgen of ongebruikte gegevensvelden binnen netwerkverkeer. Een veelgebruikte techniek is 'steganograms' binnen VoIP-transmissies tijdens video of audio conferences te verbergen

  -> tijdens een gewoon VoIP-gesprek, kunnen paketten van gegevens stilzwijgend worden overgedragen tussen de deelnemers. Daarna knnen deze verzamelde datagrammen worden opgelost tot zinvolle gegevens

  -> het is gebruikelijk voor overtreders om particuliere netwerken te infiltreren om 'gekaapte' middelen voor dekking of camouflage te benutten.

    -> overtreders rekenen ook op openbare toegangspunten om anonimiteit en mobiliteit te verhogen en toezicht te voorkomen

  -> domeinen kunnen worden geregistreerd met holdings, die functioneren als dekmantel voor de gebruiker, en IP-adressen kunnen worden gehuurd en onderverhuurd.

    -> zo wordt het identificeren van de dader zeer complex voor opsporingsinstanties. Wijdverbreide gebruik van programma's en protocollen heeft het proces van het identificeren van eindpunten op het internet ook ingewikkelder gemaakt

    -> netwerkverkeer kan effectief worden verborgen met behulp van speciale netwerkprotocollen

- **Blijkbaar vormt sterke encryptie een enorme uitdaging voor onderzoek naar cybercriminaliteit**

  -> Wetshandhavers hebben steeds meer hun stem laten horen over hun zorgen dat toenemende gebruik van encryptie onderzoeken ernstig belemmert

  -> onderscheppen van netwerkverkeer en het in beslag nemen van apparaten is vaak een vruchteloze oefening als een verdachte krachtige encryptie op schijven in rust heeft geïmplementeerd, in combinatie met gecodeerde communicatiekanalen voor data in transit

  -> tijdens cybercrimeonderzoek is de politie er vaak in geslaagd om technologie op te sporen die wordt gebruikt bij het plegen van een misdrijf, maar ze zijn niet in staat om een overtreder ‘achter het toetsenbord’ te plaatsen

  -> in dergelijke omstandigheden kunnen door middel van keystroke monitoring (het volgen van de toetsen die worden ingeslagen) in combinatie met een verborgen camera wachtwoorden onthult worden, waardoor de dader kan worden geïdentificeerd

  -> echter, in sommige rechtsgebieden heeft de politie geen bevoegdheid tot het gebruik van toezicht voor cybercrime en veel wetshandhavingsinstanties bezitten niet over de technische middelen om sterke encryptie te omzeilen

  -> klein-versleutelde containers verborgen onder grote hoeveelheden gegevens kunnen moeilijk te identificeren zijn

  -> bovendien vergeten verdachten vaak het wachtwoord dat nodig is om gegevens te decoderen, zelfs wanneer openbaarmaking wordt bevolen door een rechtbank

  -> sommige gereedschappen ‘ontkennen encryptie-technologie', die gebruikers in staat stelt om meerdere containers met discrete wachtwoorden maken zodat de geheimhouding kan worden behoouden wanneer openbaarmaking wordt afgedwongen

  -> in reactie op de toenemende druk van de consument en de internationale gemeenschap, integreren multinationale bedrijven zoals apple en google encryptietechnologie op smartphones.

    -> dit vormt een belangrijk obstakel voor de rechtshandhaving, omdat de bedrijven zelf niet meer in staat zijn om telefoons, laptops, en tablets te openen.

    -> wetgeving kan bedrijven niet dwingen informatie door te spelen, als zij het wachtwoord van de consument niet langer bezitten

    -> diverse compromissen zijn voorgesteld, zoals het inbedden van achterdeuren in encryptie technologieën voor opsporingsonderzoek.

    -> als gevolg van een aanzienlijke toename in rekenkracht geboden door quantum computing, bestaat de mogelijkheid om bruut geweld op encryptie-algoritmen in de toekomst sterk te verbeteren

11.4 JURIDISCHE PROCEDURES IN BEWIJSMATERIAAL

- **Regels omtrent bewijsmateriaal**

  -> binnen de wet bestaan regels en procedures rondom de 'bewijsbaarheid' van een bepaalde reeks feiten in een zaak.

  > -> Aan de hand daarvan wordt vastgesteld welke feiten wel of niet kunnen worden bewezen, het type bewijsmateriaal dat deze feiten kan ondersteunen en door wie en op welke manier het bewijsmateriaal bewezen kan worden

  -> de fundamentele vraag in een strafzaak betreft de schuld of onschuld van de verdachte. Ieder stuk dat kan helpen deze kwestie 'op te lossen', en toegestaan is in het betreffende rechtsgebied, kan gelden als bewijsmateriaal (feiten, getuigenissen, documenten en fysieke bewijsstukken)

  > -> bewijsmateriaal is het middel waarmee de aanklager de schuld van de verdachte probeert te bewijzen, en de verdediger juist de onschuld

  -> deze regelingen voor bewijsmateriaal fungeren als een soort poort: informatie moet de poort eerst passeren voordat het formeel erkend wordt als correct bewijs

  > -> als het niet mag passeren, wordt de informatie niet meegenomen in de overwegingen over de schuld of onschuld van een verdachte
  >
  > **-> waar ligt de grens voor toelaatbaarheid?** Bewijs is over het algemeen toelaatbaar indien het relevant is, de bewijskracht sterker is dan het nadelig effect (prejudicial effect) en het niet wordt uitgesloten door een wet.
  >
  > -> eenmaal geaccepteerd mag het bewijsstuk door de rechtbank gebruikt worden voor ieder legitiem doel

  -> in principe heeft de rechtbank aanspraak op het best beschikbare bewijs, dat de meeste zekerheid verschaft in een zaak.

  > -> kopieën worden niet geaccepteerd, tenzij het origineel aantoonbaar niet beschikbaar is of er gewoonweg niets beter is dan secundair bewijs zoals kopieën, notities of getuigenissen

- **Maar hoe zit dit bij digitale informatie in originele, binaire data-vorm?**

  -> een computerprogramma zal deze strengen van 1'tjes en 0'tjes moeten genereren naar menselijke taal, om te bepalen wat er met de data moet gebeuren.

  > -> de vraag is of deze gegenereerde menselijke taalvorm van de digitale informatie die aan de rechtbank gepresenteerd kan worden, een accurate representatie is van diezelfde informatie in originele binaire vorm

-> digitale informatie als bewijs is een vorm van getuigenbewijs en het meest complex met betrekking tot de uitsluitingsregels van bewijs in het recht

-> een verklaring betreft zowel verbale als geschreven verklaringen. Soms wordt ook bepaald gedrag van een persoon als verklaring gezien

-> in veel 'common-law' (gewoonterecht) hebben de rechtbanken geaccepteerd dat elektronisch bewijs (business records) wordt toegelaten als bewijs, indien aangetoond kan worden dat het document vertrouwbaar is

BELANGRIJK:

Het identificeren van cybercrimeovertredingen hangt vaak af van ander (indirect) bewijs. Om een specifieke verdachte te kunnen aanwijzen die op het moment van de overtreding de computer bestuurde, is vaak een gevolgtrekking van ander bewijs (circumstantial evidence). Dit 'andere' bewijs kan ontzettend belangrijk zijn in het verifiëren van auteurschap en auuthenticiteit van informatie (denk aan metadata)

-> wanneer de aanklager probeert om de schuld van de verdachte aan te tonen op basis van deze 'circumstantial evidence', moet dit bewijs alle mogelijke scenario's waarin de verdachte onschuldig zou zijn uitsluiten

> **-> ofwel:** de rechter moet in dit geval overtuigd zijn dat alle elementen van de overtreding daarmee worden , het bewijs moet in z'n geheel in acht genomen worden, losse 'items' tellen niet

- **Computer-Generated & Computer-Stored informatie:**

  -> sommige rechtsgebieden maken onderscheid tussen computer-generated archieven die op automatische basis door het bedrijfssysteem of programma worden gemaakt, en computer-stored archieven waarbij de informatie handmatig is ingevoerd.

  > **-> ofwel:** of een machine of een persoon de inhoud heeft gemaakt. Dit onderscheid is in de praktijk niet zuiver te maken

  -> ongeacht wie of wat de data heeft gemaakt, meestal is de metadata relevant voor onderzoekers en aanklagers wanneer zij onderbouwende elementen voor het delict zoeken.

  -> deze metadata kan gemakkelijk geconfigureerd, overschreven of verwijderd worden, ook zijn interne klokken en time zone instellingen in computers, camera's of in de email headers en dergelijke vaak niet accuraat, wat ze onbetrouwbaar maakt

-> de kwestie omtrent bewijs heeft betrekking op de betrouwbaarheid van het bedrijssysteem of programma dat de informatie heeft gemaakt, en of dat proces accuraat functioneerde.

-> dit heeft niet per se invloed op de toelaatbaarheid van het bewijs, maar eventueel het gewicht dat eraan wordt gehangen

- **Uitdaging voor digitaal bewijs op juridisch gebied:**

  -> in 1798 verklaarde Lord Kenyon: " it is a principle of natural justice, and of our law, that actus non facitreum nisi mens sit rea ". in andere woorden: de daad kan alleen verwijtbaar zijn indien de geest schuldig is: voor ernstige delicten moet de vervolger zowel de fysieke als mentale elementen van een delict vaststellen om de verdachte te veroordelen.

  -> fysieke element:

  -> het fysieke element, het strafbare feit, omvat de activiteiten die daadwerkelijk zijn uitgevoerd om het delict te plegen

  -> mentale element:

  -> het mentale element, de schuldige geest omvat de kennis, gedachten en intentie om het delict te plegen

  -> om verantwoordelijkheid te dragen voor een delict, is het noodzakelijk dat de wet en de intentie samenvallen

  -> het is de taak voor onderzoekers en vervolgers om de elementen van een delict met precisie te identificeren om zo de aanklacht accuraat af te bakenen. In veel rechtssystemen is een tekort aan mankracht en overload aan zaken om dit goed te kunnen aanleren en uitvoeren

  -> zoals eerder genoemd, kan het erg moeilijk zijn om een link tussen elektronisch bewijs en een verdachte vast te stellen. Elektronisch bewijs is normaalgesproken aangevuld met bewijs verkregen door traditioneel politieonderzoek dat aantoont dat een bepaald apparaat werd bestuurd door een verdachte op het moment van de overtreding

  -> elektronisch bewijs is vaak kortstondig en bestaat zelden in isolatie. Het is een product van een computerprogramma dat gebruikt is de informatie te genereren, en het computersysteem voor de gerichte handeling

  -> in cybercrime onderzoek komt vaak de vraag over auteurschap naar voren, in zaken omtrent diefstal van intellectueel eigendom tot witwassen, en allerlei fraudezaken

  -> wanneer een bedrijfsysteem of software-applicatie programmeringsfouten bevat, kan de authenciteit van alle computer gegenereerde bestanden worden betwijfeld

-> de authenticiteit van ESI (elektronisch bewaarde info) wordt vaak betwijfeld tot het auteursschap van computer-stored bastanden: nadat de bestanden zijn gemaakt kan de data gemanipuleerd of veranderd zijn

-> maar ook het compuuterprogramma kan obetrouwbaar zijn. De verdediging zal mogelijk proberen om de validiteit in twijfel te trekken om bewijs onderuit te halen door de beargumenteren dat niet met zekerheid vast te stellen is dat de verdachte achter de computer zat, maar dat dit mogelijk iemand anders was.

-> dienovereenkomstig kan de verdediging beweren dat 'autonomous malicious code' (schade vanop afstand bestuurd RAT), ervoor gezorgd kan hebben dat een overtreding werd gepleegd zonder dat de verdachte hiervan afwist

-> met betrekking tot de kwaliteit van de processen die de integriteit van ESI bewaren, vanaf het moment dat het is aangemaakt tot het pnt dat het in de rechtzaal wordt aangedragen, moeten aantonen dat het bewijs betrouwbaar is.

-> het **'chain-of-custody'** proces wordt gebruikt om te verifiëren dat het bewijs geen geknoei of verandering bevat

-> in het geval van ESI, moet de continuïteit van het bewijs behouuden worden voor zowel het fysieke apparaat dat de data 'behuist', als de informatie opgeslagen op het apparaat zelf. Er moet kunnen aangetoond worden dat de informatie een echte en accurate representatie is van de originele data zoals gecodeerd in het apparaat (authenticiteit)

-> wanneer een partij specifiek de kwestie van de continuïteit van het bewijs aanvoert bij de rechter, dienen zich mogelijk vele bezwaren aan (denk aan: relevantie, geruchten, authenticiteit, integriteit)

-> gezien de kwetsbaarheid voor manipulatie wordt door rechtbanken de nadruk gelegd om de nauwkeurigheid van de computer aan te tonen bij het inhouden en opvragen van de betreffende informatie

-> in het geval dat de chain of custody incompleet is, kan het voorkomen dat het bewijs toch wordt toegelaten: dit beslist de rechter, afhankelijk van het belang van het missende stuk

-> de toelaatbaarheid van informatie met betrekking tot activiteiten op een computer, netwerk of ander apparaat, kan ook in twijfel worden getrokken indien het systeem dat de informatie genereert geen robuuste beveiliging heeft.

-> gebrek aan voorzorgsmaatregelen met betrekking tot de beveiliging kan informatiesystemen blootstellen aan manipuulatie. Deze kwetsbaarheid kan de betrouwbaarheid van de data ondermijnen

- **Rechters, deskundigen en de media:**

  -> de rechter is uiteindelijk verantwoordelijk voor het bepalen van de schuld of onschuld van de verdachte

  -> het principe is 'beyond a responsible doubt': de rechter moet overtuigd zijn van de schuld van de verdachte

  -> de rol van de rechtbank is om overzicht te houden in het aangedragen bewijs om te verzekeren dat dit rechtmatig is toegestaan

  -> desinteresse bij rechters over 'ontastbaar bewijs' heeft gezorgd voor tegenzin bij aanklagers om gebruik te maken van elektronisch bewijs

  -> de onderliggende factoren van deze tegenzin zijn moeilijk na te gaan, maar rechtssystemen wereldwijd zijn verontrust over het doordringen van cybercrime-overtredingen, dus ook elektronisch bewijs in de rechtzaal

  -> veel advocaten en rechters begrijpen weinig van het complexe elektronische bewijs

  -> sommige advocaten geven zelfs toe dat ze de gedetailleerde vragen zelfs vermijden

  -> ook zijn de middelen voor opsporing en vervolging kostbaar en tijdrovend. Er moet een selectie aan zaken worden gemaakt, en veel rechtzalen zijn niet voorzien van de technologie om elektronisch bewijs als middel te kunnen presenteren.

  -> Dit verklaart waarom waarom cybercrime zaken meestal gedropt worden voordat ze ooit een rechtzaal bereiken

  -> de mogelijkheid voor elektronisch bewijs hangt af van de houding van niet-technische stakeholders (politie, vervolgers, advocaten, rechters). Het is van belang dat zij op de hoogte zijn van de vormgeving van elektronisch bewijs en de beperkingen van cyber crime onderzoek

  -> niettemin hebben advocaten en experts de neiging om forensisch bewijs te presenteren op een manier waarbij ze eerder spreken in termen van waarschijnlijkheid dan in termen van gerede twijfel

  -> de manier waarop media een beeld schetst van de mogelijkheden en geschiktheid van forensische methoden via televisie, bioscoop en literatuur, schept onrealistische verwachtingen

  -> in werkelijkheid is forensisch onderzoek een langdurig proces, waarin ook menselijke fouten kunnen worden gemaakt. Een kwestie omtrent welzijn is bv. Dat medewerkers regelmatig worden blootgesteld aan onzedelijk materiaal

-> er wordt regelmatig beroep gedaan op getuigen deskundigen in strafzaken. Zij ondergaan pittige kruisverhoren, en moeten essentiële eigenschappen van het bewijs, toegepaste technieken en analyses en de interpretatie daarvan helder kunnen overbrengen

-> de mate waarin dit goed kan worden uitgelegd, bepaalt ook de waarde van de bevindingen, dit is cruciaal. In een rechtszaal kan de rapportage hiervan verwarrend zijn voor de 'fact finder' (onderzoeksrechter)

-> daardoor kan er twijfel ontstaan over de kwaliteit van de van de deskundige en misleidende invloed geven op de rechter, wat de gerechtigheid in gevaar brengt

-> sommige critici vinden dat forensisch onderzoek lijdt aan slechte documentatie en gebrek aan transparantie, of het vermijden van conclusies.

-> inadequaat taalgebruik kan leiden tot onrechtmatige veroordelingen.

-> er zijn universele kanttekeningen omtrent forensische disciplines die ettentieel zijn voor de rapportage van maten van zekerheid, om adequater een gewicht aan de resultaten te kunnen hangen. Denk aan dingen als: 'including but not excluding', 'possible but not certain'

- **Aanbevelingen:**

-> de ontwikkeling en promotie van het nationale, regionale en internationale beleid met betrekking tot het verzamelen van elektronisch bewijs, inclusief het verbeteren van de coördinatie tussen handhavingsinstanties (regionaal / nationaal / internationaal), is de afgelopen jaren vooruit gegaan

-> het netwerk van internationale telecommunicatiesystemen, welke een broedplaats zijn voor cybercrime overtredingen, eisen een universeel beleid. Dit zou ideaal gezien een bindend rechtsinstrument als een verdrag onder toezicht van de UN moeten zijn om de 'veilige haven' van cyber crime plegers te beperken

-> in veel common-law landen (gewoonterecht: gebasseerd op gewoonten) is er onderscheid tussen de wet in de praktijk en de wet in het boek

-> wetgeving moet meer aandacht schenken aan de mogelijkheden van de politie in de praktijk en de impact die technologie uitoefent op onderzoek, forensische onderzoeken en vervolgingen

-> wanneer er een aanzienlijk risico op vernietiging van bewijs bestaat, moet de politie bevoegd zijn om snel apparaten te kunnen onderzoeken zonder te hoeven wachten op een bevelschrift

-> door de bewijslast voor verdachten zodanig te wijzigen, dat er een duidelijke classifisering van cybercrime wordt ontwikkeld, kan zorgen voor een hogere 'conviction rate', maar ook een afschrikkende werking.

-> het verplicht stellen voor het nemen van voldoende voorzorgsmaatregelen voor informatiebeveiliging door individuen en organisaties zal ook de kwetsbaarheid voor cyber crime reduceren

-> het reguleren van cybercrime met louter nationale wetgeving en internationale instrumenten, zal niet toereikend zijn vanwege het transnationale karakter. Een betere samenwerking tussen internationale politie-eenheden is cruciaal om cybercrime trends en mechanismen op te sporen

-> Organisaties als Interpol, Europol, de FBI, etc. Moeten deze samenwerking faciliteren, bijvoorbeeld door internationale conferenties

-> lokale politiekorpsen ondervinden hier een probleem met betrekking tot competentie voor technische expertise. Er is een effectief mechanisme nodig om kennis over te dragen over hoe je cybercrime moet surveilleren en onderscheppen om geen overtredingen te missen.

> -> ook is er een barrière tussen de politie en de communicatie industrie. Het delen van informatie en verbeteren van de samenwerking is noodzakelijk.
>
> -> industrieleiders zijn de sleutel voor het ontwikkelen van een robuuster systeem binnen wetgeving en technologie

-> Gegeven de neiging van veel advocaten om het technische aspect te vermijden bij het bouwen van een zaak, is het van belang om cursussen/trainingen te ontwikkelen voor juristen om bewust te worden van de impact van technologie op de manier van delicten plegen op het gebied van oa fraude, corruptie of andere 'data-driven' handelingen die persoonlijke schade aanbrengen. Het is onvermijdelijk voor bv rechters om enigszins te begrijpen wat het elektronisch materiaal met betrekking tot online criminaliteit en het DarkNet inhoudt. Dit zouu al in juridisch onderwijs aangeboden moeten worden

-> de impact van globalisering dwingt nationale rechtssystemen zich ook bezig te houden met zaken transnationaal niveau. Logischerwijs zou de verantwoordelijkheid hiervoor meer pluratisch moeten zijn.

> -> rechters moeten bv extensieve ervaring met cybercrime zaken, zouden bevoegd moeten zijn om op internationaal niveau te helpen, door videovergaderen om het betaalbaar te houden, of bevoegdheid via de International Criminal Court (ICC) of International Court of Justice (ICJ)

-> tijdens de meeste strafzaken moet de vervolging in staat zijn aan te tonen dat alle wegen zijn bewandeld te aanzien van het bewijs tijdens het opsporingsbericht.

-> daarvoor moet nauw samengewerkt worden tussen aanklagers, tipgevers en forensisch onderzoekers om de rechtbank een accuraat overzicht te kunnen bieden bij een strafzaak. Ervaren aanklagers en onderzoekers zijn nodig om erop toe te zien dat alles correct volgens het juridisch proces verloopt

-> vergaderingen voorafgaand aan de strafzaak worden door advocaten en experts vaak over het hoofd gezien vanwege tijdgebrek. Deze ronde tafelgesprekken zijn echter wel ettentieel voor gesprekken tussen de verdediging, forensisch analisten en andere getuigen, waarbij mogelijk tegen kwesties op technisch of rechtsgebied wordt aangelopen.

-> zo verloopt de strafzaak zelf een stuk soepeler en zullen technische aspecten van bewijs beter worden begrepen

BELANGRIJK:

Het ontwikkelen van heldere standaard procedures zal het afwijzen van elektronisch bewijs verminderen. Bij een duidelijk beleid wordt de betrouwbaarheid voor getuigendeskundigen verbeterd, het kan als handvat dienen en het gebruik van digitale forensische methoden in de rechtszaal makkelijker maken. Ook kan adequater gemeten gemeten worden wat de betrouwbaarheid en toelaatbaarheid van een elektronisch bewijsstuk is

-> meer kennis nodig over wat voor onderzoekers wel en niet mogelijk is in de aanpak van cyber crime en het pakken van daders

-> ook het trainen van leidinggevenden binnen hadhavingsinstanties, over het gebruik en werking van digitale forensische methoden

-> zowel managers, die vaak eindverantwoordelijk zijn, als het trainen en het inzetten van specialisten binnen een team is belangrijk

-> Eerlijkheid staat voorop, en daarom moeten onafhankelijke forensische faciliteiten beter toegankelijk worden, er moet een mogelijkheid zijn voor verdachten die duidelijk in het nadeel zijn vanwege de hoge kosten van forensische ondersteuning, sponsoren voor forensische hulp is noodzakelijk

-> sterke cryptografie is onmisbaar voor het succes en de ontwikkeling van een open systeem zoals het internet.

-> veiligheidsmaatregelen die de overheid heeft opgezet om gevoelige en **Persoonlijk Identificeerbare Informatie (PII)** te beschermen zijn blijkbaar ontoereikend

-> het met opzet in gevaar brengen van versleuteling in dit kwetsbare technologische milieu, zelfs voor het publiek belang, verzwakt bescherming en veiligheid voor iedereen.

-> overheidsregulering van cryptografie ondermijnt globale cyber security, heeft negatieve invloed op het publieke beeld van de integriteit van de politie, vermindert de rapportage van cybercrime en resulteert in het 'minst vertrouwde land' probleem.

-> beperkingen in de kracht van versleuteling of enige consessies naar opsporingsautoriteiten dmv achteringangen of 'master decryption keys' zal resulteren in een situatie waar de veiligheid van de internationale gemeenschap aanzienlijk wordt verzwakt door de beveiligingssituatie in het minst vertrouwde land

-> wanneer landen toegang tot effectieve encryptie vergemakkelijkt, ontstaat er een veilige haven voor cybercrime daders en een bloeiende zwarte markt voor encryptie

-> andere oplossing: daders die niet in staat of niet bereid zijn om mee te werken aan een rechterlijk bevel tot decodering zouden een straf in verzuimboete moeten krijgen

-> de ontmoedigende waarde van deze aanpak is voelbaar en individuen en organisaties stimuleren om beveiliging te implementeren om decoderingssleutels te beschermen

> -> deze oplossing lijkt misschien zeer dwingend voor individuele verdachten, maar de aanpak is veel minder totalitair dan de methoden die momenteel worden voorgesteld in de uitvoerende macht. Deze laatste hebben namelijk invloed op de veiligheid van de samenwerking als geheel

-> er is behoefte aan een uniform en gedegen cybercrime rapportage mechanisme

-> strategieën om mensen aan te moedigen te rapporteren includeert bewustwordingscampagnes, online rapportage portalen en cybercrime hotlines. Echter, om adequaat te kunnen reageren op meldingen van cybercriminaliteit, moet de politie uitgerust worden met de nieuwste technologie en getraind worden in de beste manieren om ESI aan te pakken

-> om multidisciplinaire teams op te stellen, moeten wethandshavingsautoriteiten investeren in vakexperts, opleidingen en inkoop-budgetten. Om de opspoorders zo goed mogelijk te assisteren moeten rechtzalen worden uitgerust met multimedia technologie zodat resultaten effectief gepresenteerd kunnen worden

-> advocaten vragen om praktische kennis van de software die wordt gebruikt door de politie bij het verwerken ESI. Tot slot is een uuniforme taxonomie voor strafrechtelijke systemen en wetgevende organen onmisbaar voor het bereiken van een grotere harmonie tussen de nationale en internationale wettelijke kaders

-> definities van cybercriminelen moeten worden uitgedrukt met nauwkeurigheid en consistentie en moeten geformuleerd worden in overleg met de internationale gemeenschap om taalbarrières en culturele verschillen te overbruggen

- **CONCLUSIE:**

  -> Industrieleiders zijn zich bewust van de noodzaak om de veerkracht van de cyberverdediging te waarborgen

  -> Er zijn programma's ontwikkeld zoals informatiebeveiligingstechnologieën en advocaten specialiseren zich in data privacywetgeving

  -> Fysieke en virtuele beveiligingsmechanismen worden verbeterd en informatiesystemen worden getest op zwakke punten

  -> Er wordt wereldwijd veel aandacht besteed aan het onderzoeken en vervolgen van cybercrime door staten, private sectoren, politiediensten en universiteiten

  -> Om belemmeringen voor onderzoek en vervolging van cybercrime tegen te gaan zijn oplossingen dringend nodig

- **Enkele uitdagingen die cybercrime meebrengt voor het strafrecht:**

  1. **Identificatie**

     -> moeilijkheden bij toeschrijven bezit en auteurschap van elektronisch opgeslagen informatie, bij het identificeren van individuen die controle hebben over informatiesystemen/apparaten, onvermogen om relevante info te onderscheiden, ineffectiviteit bij opsporen criminele activiteiten wanneer data anoniem is, ruime bevoegdheid van consumenten die bewijsmateriaal op hun apparaten vernietigen

  2. **Toegang**

     -> onvermogen om toestemming te krijgen voor uitvoeren online onderzoek en verzamelen gegevens die op afstand zijn opgeslagen, vertraging bij behandeling verzoeken van wereldwijdse rechtshulp door bureaucratische struikelblokken, onvermogen om gegevens te verkrijgen als gevolg van ontwikkelingen in bescherming apparaten van consument, wettelijke regeling die fabrikanten en dienstverleners dwingt om opsporingsinstanties toegang te geven aan elektronisch opgeslagen info wordt overbodig

     -> het is technisch niet haalbaar om buitenlandse fabricanten te dwingen te voldoen aan lokale wetten, sancties die rechters opleggen aan verdachten die weigeren mee te werken en opdrachten bekend te maken zijn niet effectief

3. Welzijn

-> druk om te presteren en stressvolle werkomstandigheden kunnen leiden tot burn outs van personeel, langdurige blootstelling aan obscene materiaal kan zorgen voor psychische problemen voor onderzoekers , officieren en forensische ondervragers, welzijn personeel kan over het hoofd worden gezien en onderzoek kan worden ontspoord wanneer personen zonder ervaring op gebied van cybercrime zaken behandelen

4. Aansprakelijkheid

-> bemoeienis met commerciële activiteiten kan leiden tot schadeclaims, onbedoelde schade aan informatiesystemen/apparaten kunnen leiden tot rechtzaken bij de civiele rechter, openbaarmaking van prive en vertrouwelijke info tijdens een onderzoek kan leiden tot strafrechtelijke / civielrechtelijke / bestuurrechtelijke procedures

5. Processen

-> bereidbaarheid van wethandhavingsinstanties om middelen in te zetten tegen cybercrime is afhankelijk van beleidsvoorkeur en prioriteiten en de politieke agenda, gedocumenteerde procedures zijn nodig om de behandeling van elektronisch bewijsmateriaal te leiden naar opsporingsautoriteiten

6. Retentie

-> kortstondige bronnen van elektrische info die niet via live systemen worden verzameld verzwakken de zaak, kan leiden tot gerechtelijke dwaling, dienstverleners die niet reageren op toestemminigsverzoeken voor productie en behoud van gegevens kan leiden tot verlies essentieel bewijs

7. Ontvankelijkheid en billijkheid

-> documenten die onvolledig of onjuist zijn kunnen leiden tot niet-ontvankelijkheid van bewijsmiddelen, wetshandhavingsinstanties die niet kunnen verklaren dat de elektronische info betrouwbaar of echt is kan bewijsmateriaal in rechtzaken dwarsbomen, onderzoek van overheden en experts die onvoldoende objectief worden geacht kunnen geloofwaardigheid bewijs verzwakken. Analisten en onderzoekers die niet in staat zijn tijd te besteden aan het identificeren van ontlastend bewijs kan sterkte zaak verzwakken of leiden tot rechterlijke dwaling

8. Menselijk vermogen

-> wethandhavers en OvJ zonder technische expertise kunnen bijdragen aan vrijspraak van cybercriminelen, analisten die niet gekwalificeerd zijn om technische uitrusting of gegevens van informatiesystemen te onderzoeken kunnen de geloofwaardigheid ondermijnen van onderzoek

9. Technische middelen en financiering

-> politie die niet uitgerust is met gespecialiseerde tools om informatie te verwerken kan belangrijk bewijs missen, rechtzalen die niet zijn uuitgerust met moderne technologie die wel is vereist om het bewijs effectief te presenteren kan de overtuigingskracht van het bewijs ondermijnen

10. Training

-> politie, OvJ en rechters zijn niet voorzien van doorlopende trainingen die zich richten op nieuwe vormen van criminaliteit: bemoeilijkt het behandelen van cybercrime zaken

11. Rapportage en onzekerheid

-> misvattingen bij burgers omtrent de capaciteiten van de politie om iets aan cybercrime te kunnen doen, gaten in wetgeving en procedures kunnen ervoor zorgen dat het onduidelijk is voor onderzoekers om onderzoek te verrichten naar cybercrime. Getuige deskundige kan verkeerd informeren

12. Privacy en privelege

-> onderzoeken kunnen stuk lopen wegens schending van fundamentele mensenrechten, technische kennis bij de advocatuur kan het proces langzamer laten lopen, onderzoekers kunnen bepaalde informatie niet langer meer bereiken door wereldwijd geldende privacy wetgeving

13. Coöperatie/samenwerking

-> binnen de private sector wordt er langzaam en in mondjesmaten gereageerd op verzoeken van de politie of andere autoriteiten. Door het bestaan van grote internationale ondernemingen is het voor politie instanties moeilijk om binnen het grondgebied van de eigen staat te blijven waarover zij macht uitoefenen en die bevoegdheid hebben

14. Juridisch proces en framework

-> verschillen in internationale wetgeving tussen bv lidstaten van Europa. Wetgeving die niet rekening houdt met technologische ontwikkelingen

-> doordat het relatief makkelijk is om via het internet delicten te plegen en de baten hiervan hoog zijn, is er een sterke motivatie tot deze vorm van criminaliteit

-> Er moeten barrières worden opgeworpen om awareness te creëren en om deze steeds groter en beter georganiseerd wordende lucratieve vorm van criminaliteit te doen stoppen