STUDIECENTRUM RECHTSPLEGING

TRAINING AND STUDY CENTRE FOR THE JUDICIARY

AANBOD CYBERCRIME EN DIGITAAL BEWIJS/ DIGITALE OPSPORING JUNI 2022

SSR aanbod Cybercrime

Cybercrime vormt een belangrijk onderdeel van de juridische realiteit in ons dagelijkse werk. Kennis over deze vorm van criminaliteit verdient dan ook een vaste plek in de spreekwoordelijke gereedschapskist van elke strafrechtelijk georiënteerde professional.

In deze flyer sommen we daarom het SSR-aanbod cybercrime voor zowel de Rechtspraak als het Openbaar Ministerie op. Het schematische overzicht laat je in één oogopslag zien waar je uit kunt kiezen op basis-, verdieping- en masterniveau.

Verdere informatie over de inhoud en de leervorm (contactonderwijs op locatie/online of zelfstudie via webcollege/e-learning module) staat per titel beschreven in deze flyer. De meest actuele informatie en uitvoeringsdata zijn te vinden op onze website.

Vragen over ons cybercrime-aanbod kun je stellen via email:

KLIK HIER OM EEN EMAIL TE STUREN

Wat is er nog meer?

Kenniscentrum Cybercrime ZM

Het Kenniscentrum Cybercrime verzamelt, beheert en verspreidt kennis en informatie met betrekking tot cybercrime, digitale opsporing en digitaal bewijs. Het kenniscentrum heeft een pagina op Intro (het intranet van de Rechtspraak). Hier zijn nieuwsbrieven, kennispagina's, en diverse publicaties te vinden.

KLIK HIER OM NAAR DE INTRO-PAGINA TE GAAN

Kennis- en Expertisecentrum Cybercrime (KEC) OM

Het Kennis- en Expertisecentrum Cybercrime (KEC) van het Openbaar Ministerie is ondergebracht binnen het cluster High Tech Investigations bij het Landelijk Parket in Rotterdam. Het KEC houdt zich bezig met digitale opsporing, high tech crime en interceptie. Ook geven zij leiding aan de opsporingsonderzoeken van Team High Tech Crime van de Landelijke Recherche. Het KEC heeft een pagina op ZoOM (het intranet van het Openbaar Ministerie) en brengt periodiek een nieuwsbrief uit.

KLIK HIER OM NAAR DE INTRANET-PAGINA TE GAAN

Schema aanbod cybercrime en digitaal bewijs/digitale opsporing juni 2022

1. Introductie cybercrime

Basis:

1a Cyber 101 **ZM**

1b Cybercrime **ZM**

1c Digitale opsporing **ZM**

1d Cyber voor RC's: toezicht op verzamelen van digitaal bewijs **ZM**

1e Basics101: criminaliteit in een digitale wereld **OM**

1f Webinars Ressortsparket Cyber **OM**

Verdieping:

1g Webcolleges introductie cybercrime **OM/ZM**

2. Informatie en opsporing

Basis:

2a Digitale opsporing **ZM**

2b Strafrechtspleging in een digitale wereld **OM/ZM**

2c Interceptie: vorderen voor (niet) gevorderden **OM**

Verdieping:

2d Digitale kinderpornografie **OM/ZM**

2e Forensische expertise (digitaal onderzoeken voor **OM/ZM**)

2f Digitale opsporing en digitaal bewijs **ZM**

2g Lezing themadag Kenniscentrum Cybercrime 2020 **OM/ZM**

2h Crypto-communicatie en datasets, actualiteiten **ZM**

3. Diverse onderwerpen

Verdieping:

3a High tech cybercrime **ZM**

Master

3b Professionele ontmoeting / Masterclass Cybercrime **OM/ZM**

3c Themadag Kenniscentrum Cybercrime 2022 **OM/ZM**

3d Cybercrime, masterclass **OM**

3e Uniting forces against cyber challenges of terrorism **OM/ZM**

Internationaal

3f Aanbod ERA / EJTN **OM/ZM**

4. Podcasts SSR Meestervertellers

Plaats delict: internet

De Rotterdamse webcamhacker
Jacqueline Bonnes

Ethisch hacken
Brenno de Winter

Cybercrime of cyborg crime?
Wytske van der Wagen

Encrochat
Jan-Jaap Oerlemans

Ransomware
Jacqueline Bonnes

Digitale bewijsvoering
Brenno de Winter

1.Introductie cybercrime (basis)

Basis

1a) Cyber 101 (ZM)

In deze e-learning module doet je essentiële basiskennis op over computers, internet en sociale media. Daarbij komen ook bredere vraagstukken aan bod, zoals de invloed van kunstmatige intelligentie op het recht.
Meer info

1b) Cybercrime (ZM)

In deze e-learning module doe je basiskennis op over cybercrime als vorm van (gedigitaliseerde) criminaliteit. Daarbij komen actualiteiten, nieuwe strafbaarstellingen en actuele jurisprudentie ruim aan bod.
Meer info

1c) Digitale opsporing (ZM)

In deze e-learning module doe je basiskennis op over het opsporingsproces op basis van digitale sporen zoals open bronnen, sociale media, inbeslagname van gegevensdragers en de hackbevoegdheid.
Meer info

Bovenstaande modules zijn ontwikkeld voor de ZM en kunnen in combinatie gevolgd worden. Tijdsbesteding is circa 2 uur per deel. De modules zijn 24/7 te volgen en tussentijds stoppen is mogelijk.

1d) Cyber voor RC's: toezicht op verzamelen van digitaal bewijs (ZM)

Een praktisch ingestoken cursusdag vanuit de gedachte dat elke zaak digitale aspecten kan bevatten en dat iedere rechter-commissaris hiermee te maken krijgt. Er wordt onder meer stilgestaan bij de doorzoeking (digitaal beslag, netwerkzoeking), de BOB-middelen (internettap, vorderen opgeslagen gegevens, hacken), grootschalig digitaal onderzoek (Ennetcom) en recente ontwikkelingen (inloggen op een account, analogievorderingen). Daarbij wordt ook aandacht besteed aan de schriftelijke afhandeling in proces-verbaal doorzoeking, machtiging dan wel beschikking (artikel 181/177 Sv). Het doorlopen van deze cursus (inclusief voorbereiding) duurt circa 3 dagdelen.
Meer info

1e) Basics101: criminaliteit in een digitale wereld (OM)

Deze e-learning module biedt basiskennis over de techniek achter de digitale wereld en over digitale criminaliteit.
Meer info

1f) Webinars Ressortsparket Cyber (OM)

Speciaal voor collega's van het Ressortsparket is in 2021 een start gemaakt met een serie webinars over cybercrime. De eerste drie delen Wat is cybercrime?, Cryptodata in opsporingsonderzoeken en Witwassen met cryptovaluta zijn terug te kijken in MIJN SSR voor collega's van het Openbaar Ministerie. In 2022 organiseert SSR opnieuw een aantal webinars met actuele onderwerpen.

Verdieping

1g) Webcolleges introductie cybercrime (OM/ZM)

In samenwerking tussen SSR/KCC en Fox-it zijn in ons Cybercrime-aanbod een aantal webcolleges tot stand gekomen en opgenomen. Enkele hiervan behoren tot het voorbereidingsmateriaal van de cursus High Tech Cybercrime. De overige webcolleges zijn interessant om kennis te nemen in het betreffende deelonderwerp.

- Phishing
- Computervredebreuk
- Witwassen met gebruikmaking van cryptovaluta
- Ransomware
- Metadata
- Bestandsreconstructie
- Windows bestandssysteem
- Basiskennis IP-adressen
- Data-extractie van mobiele telefoons

De webcolleges zijn hier te bekijken.

2. Informatie en opsporing

Basis

2a) Digitale opsporing (ZM)

In deze e-learning module doe je basiskennis op over het opsporingsproces op basis van digitale sporen zoals open bronnen, sociale media, inbeslagname van gegevensdragers en de hackbevoegdheid (deze e-learning staat ook onder 1c beschreven).

Meer info

2b) Strafrechtspleging in een digitale wereld (OM/ZM

Deze tweedaagse cursus is met name gericht op het opsporingsonderzoek. Voorafgaand aan de bijeenkomsten volg je een e-learning die meer informatie geeft over diverse vormen van criminaliteit in het digitale domein en de opsporing daarvan. Tijdens de eerste bijeenkomst wordt ingegaan op de wetgeving bij interceptie aan de hand van het Vademecum Interceptie, de opsporingsactualiteiten en ontwikkelingen in de nabije toekomst. Tijdens de tweede bijeenkomst wordt een aantal onderwerpen verder verdiept en worden individuele leervragen behandeld. Het doorlopen van deze cursus (inclusief voorbereiding) duurt circa 6 dagdelen.

Meer info

2c) Interceptie: vorderen voor (niet) gevorderden (OM)

Met deze e-learning krijg je de kans om kennis op te doen over diverse onderwerpen die het thema Interceptie omvat.

Meer info

Verdieping

2d) Digitale kinderpornografie (OM/ZM)

Wat zijn de belangrijkste opsporingstechnische, digitale en juridische aspecten van kinderpornofeiten? Tijdens deze cursus krijg je niet alleen inzicht in complicerende factoren die gepaard gaan met het behandelen van kinderpornofeiten (zoals de opsporing via het Dark Web en de maatschappelijke impact), maar word je ook geïnformeerd over de juridische basiskennis met betrekking tot deze feiten. Tevens worden de psyche van de pleger van kinderpornodelicten en de digitale wereld waarin hij zich begeeft, behandeld. De cursus biedt gelegenheid om met vakgenoten van gedachten te wisselen over de wijze waarop je dit soort zaken het beste kunt aanpakken. Het doorlopen van deze cursus (inclusief voorbereiding) duurt circa 3 dagdelen.

Meer info

2e) Forensische expertise (digitaal onderzoeken voor OM/ZM)

In de samenleving is digitalisering steeds meer zichtbaar. Apparaten zijn met internet verbonden en met smartphones bestuurbaar en via internet vindt in toenemende mate communicatie en handel plaats. Ook de onderwereld maakt hier gebruik van. Politie (en andere opsporingsdiensten) staan voor de uitdaging om bij te blijven en de juiste gegevensdragers in beslag te nemen en te onderzoeken. Het Openbaar Ministerie stuurt dit onderzoek aan en dient daartoe de onderzoeksmogelijkheden te kennen en doorzoekingen te kunnen aansturen. Van de Zittende Magistratuur wordt

verwacht dat zij bij de behandeling van deze zaken voldoende knowhow heeft om de zaken goed te kunnen beoordelen. Tijdens deze cursus krijg je zicht op wat digitaal materiaal ons kan vertellen (en ook wat je er niet aan kunt aflezen), waar je rekening mee moet houden bij het voorbereiden en behandelen van zaken, welke verweren met regelmaat gevoerd worden en hoe je daarmee om kan gaan. Het doorlopen van deze cursus (inclusief voorbereiding) duurt circa 3 dagdelen.
Meer info

2f) Digitale opsporing en digitaal bewijs (ZM)

Wordt in 2022 ontwikkeld en uitgevoerd. Nadere informatie volgt op de SSR-website.

2g) Lezing themadag Kenniscentrum Cybercrime 2020 (OM/ZM)

Tijdens dit webcollege wordt een overzicht gegeven van jurisprudentie op het gebied van onderzoek aan gegevensdragers. Het webcollege duurt circa 30 minuten.
Meer info

2h) Crypto-communicatie en datasets, actualiteiten (ZM)

Al enige jaren levert de opsporing van strafbare feiten met gebruikmaking van communicatie via versleutelde berichten discussies in de rechtszaal (en daarbuiten) op. Rechters worden geconfronteerd met nieuwe technieken en verweren van velerlei aard over de toegepaste opsporingsbevoegdheden en -methodes. Internationale aspecten en de onder meer daarmee samenhangende terughoudendheid van politie en OM om volledig inzicht te geven in de gang van zaken leidende tot het toevoegen van ontsleuteld berichtenverkeer aan het strafdossier leiden tot extra complicaties. De advocatuur laat zich niet onbetuigd met het verwijzen naar (informatie verkregen uit) buitenlandse rechtspraak. Nederlandse gerechten beslissen niet altijd in gelijke zin. Gezien dit alles lijkt de tijd gekomen voor het geven van een overzicht van de actuele stand van zaken, met een korte blik naar het recente verleden. De duur van deze actualiteitencursus is circa 2,5 uur.
Meer info

3. Diverse onderwerpen

Verdieping

3a) High tech cybercrime (ZM)

Een cursusdag waarbij wordt ingegaan op de juridische kaders met betrekking tot de wetgeving op het gebied van cybercrime en cyberdelicten (waaronder computervredebreuk, phishing, ransomware en witwassen/bitcoins). Ter voorbereiding worden video's aangeboden in MIJN SSR. Deze geven een introductie van de genoemde cyberdelicten (zowel qua fenomeen op zich als qua techniek). Het doorlopen van deze cursus (inclusief voorbereiding) duurt circa 3 dagdelen.
Meer info

Master

3b) Professionele ontmoeting / Masterclass Cybercrime (OM/ZM)

Ook in 2022 organiseert SSR weer masterclasses over cybercrime. Discussieer met collega's en professionals op specialistisch niveau over onderwerpen als: (digitale) kinderpornografie, deepfakes, resellers en vormen van hosting.
Meer info

3c) Themadag Kenniscentrum Cybercrime 2022 (OM/ZM)

De jaarlijkse themadag vindt plaats op donderdag 19 mei 2022 (9.45 tot 16.15 uur) in het Eye filmmuseum, Amsterdam. Dit jaar is het centrale thema: 'Digitale technieken: informatieve rijkdom'.

3d) Cybercrime, masterclass (OM)

Voor OM collega's met cybercrime/digitale opsporing in hun portefeuille organiseert SSR jaarlijks een aantal masterclasses. De doelgroep ontvangt hiervoor een uitnodiging.

3e) Uniting forces against cyber challenges of terrorism (OM/ZM)

Het gebruik van cyberspace voor terroristische activiteiten en verschillende vormen van misdrijven creëren een complexe omgeving voor autoriteiten die zich bezighouden met misdaadonderzoek. De steeds veranderende technische ontwikkelingen op het gebied van communicatie en de versleuteling hiervan zijn daarbij uitdagingen waar men in verschillende landen dagelijks tegenaan loopt. Voeg daarbij de aard van de dreiging, de locatie van de plaats delict, de anonimiteit van het wereldwijde web, het grensoverschrijdende aspect van de misdrijven en de complexiteit van procedures, complexe wetten en tijdrovende informatie-uitwisseling en er ontstaat een wirwar van vertragende omstandigheden. Over bovenstaande onderwerpen is in oktober 2019 de internationale conferentie 'Uniting forces against cyber challenges of terrorism' in Spa, België gehouden. Deze e-learning module (in de vorm van een e-book) bevat interviews, video's en presentaties van deze conferentie én de conclusies hiervan.
Meer info

Internationaal

3f Aanbod ERA / EJTN (OM/ZM)

Voor het internationale aanbod op het gebied van cybercrime, verwijzen wij je graag naar de websites van ERA en EJTN.

4. Podcasts SSR Meestervertellers – plaats delict: internet

Datalekken bij grote organisaties en gemeentes en universiteiten die digitaal gegijzeld worden; zijn we eigenlijk wel klaar voor cybercrime? In 2021 heeft SSR Meestervertellers een speciale serie over de aanpak van cybercrime gemaakt. Cyber-expert Chris van 't Hof (Tek Tok) ging daarvoor in gesprek met Brenno de Winter, Jacqueline Bonnes, Wytske van de Wagen en Jan Jaap Oerlemans. Over hacken, ransomware, encro-chat en de dilemma's waar de rechterlijke organisatie voor staat bij de aanpak van internetcriminaliteit.

Jacqueline Bonnes – De Rotterdamse webcamhacker

Jacqueline Bonnes doet als officier van justitie grote onderzoeken op het gebied van cybercrime. In deze aflevering kijkt ze met Chris van 't Hof terug op de zaak van de Rotterdamse webcamhacker. Bonnes legt uit waarom deze zaak bepalend is geweest voor de manier waarop we in Nederland computercriminaliteit benaderen.

Brenno de Winter – Ethisch hacken

In zijn rol als onderzoeksjournalist kaartte Brenno De Winter misstanden aan door het hacken van onder meer de OV-chipkaart. Tegenwoordig treedt hij op als expert in rechtszaken en adviseert hij organisaties over het verbeteren gegevensbescherming. Waar zit het verschil tussen computervredebreuk en ethisch hacken? Aan de hand van enkele bekende hacks geeft de Winter uitleg over subsidiariteit en proportionaliteit.

Wytske van der Wagen – Cybercrime of cyborg crime?

Wytske van der Wagen, assistent professor criminologie aan de Erasmus Universiteit Rotterdam gaat vanuit New York met Chris van 't Hof in gesprek over haar proefschrift From Cybercrime to Cyborg crime. In haar proefschrift gaat van der Wagen in op de interactie tussen dader en technologie bij het plegen van internetcriminaliteit.

Jan-Jaap Oerlemans – Encrochat

Jan-Jaap Oerlemans, bijzonder hoogleraar inlichtingen en recht, geeft in deze podcast tekst en uitleg over de zaak encrochat; de hack van versleutelde telefoonberichten van criminelen door de Franse en Nederlandse politie.

Jacqueline Bonnes – Ransomware

Als officier van justitie doet Jacqueline Bonnes grote onderzoeken op het gebied van cybercrime. Aan de hand van een voorbeeld geeft ze in deze podcast uitleg over de aanpak van afpersing met gijzelsoftware, beter bekend als ransomware.

Brenno de Winter – Digitale bewijsvoering

In zijn rol als onderzoeksjournalist probeerde De Winter misstanden aan te kaarten door hacks van onder meer de OV-chipkaart. Tegenwoordig helpt hij organisaties met het verbeteren van gegevensbescherming. Van 't Hof en de Winter praten in deze podcast over digitale bewijsvoering. Ze vragen zich af: "In hoeverre moet een rechter zélf ICT-kennis hebben en welke experts kan de rechter vertrouwen om een oordeel te vellen?"

de Rechtspraak

OPENBAAR MINISTERIE

SSR