Samenvatting

Verschillende factoren maken de bestrijding van cybercriminaliteit uniek en lastig. Cybercriminaliteit is intrinsiek grenzeloos en ontwikkelt zich snel, soms zo snel dat nationale autoriteiten het niet kunnen bijhouden. De horizontale aard van cybercriminaliteit zorgt voor extra complexiteit: bijna elk type misdrijf kan tegenwoordig via internet worden gepleegd. Vanwege het vluchtige karakter van gegevens kan het moeilijk zijn elektronisch bewijsmateriaal van dergelijke misdrijven te verzamelen, en is daarvoor mogelijk specifieke deskundigheid nodig. Justitiële samenwerking is essentieel voor het tijdig vergaren van elektronisch bewijsmateriaal dat toelaatbaar is in gerechtelijke procedures. Internationale justitiële samenwerking kan worden belemmerd door aanzienlijke verschillen tussen nationale rechtskaders (bijvoorbeeld wat betreft de strafbaarstelling van gedragingen of wetgeving inzake gegevensbewaring). Als gevolg van het fenomeen cybercriminaliteit is het traditionele juridisch begrip territorialiteit onderhevig aan verandering, aangezien het bewijsmateriaal dat vereist is om een succesvolle vervolging van cybercriminelen te kunnen waarborgen, supranationaal is.

Voor een doeltreffende nationale bestrijding van cybercriminaliteit is daarom vaak samenwerking op meerdere niveaus noodzakelijk. Nauwere internationale samenwerking is van cruciaal belang omdat cyberspace internationaal en grensoverschrijdend van aard is. De “Strategie inzake cyberbeveiliging van de Europese Unie: een open, veilige en beveiligde cyberspace” is gericht op het ontwikkelen van een cyberspace die de toegang tot het internet bevordert en zorgt voor marktgroei, maar is ook bedoeld om de cyberspace veerkrachtig te maken en cybercriminaliteit te bestrijden, met inachtneming van het evenwicht tussen de grondrechten van de burgers en de rechtsstatelijkheid ([1]). Bovendien wordt er in de strategie voor gepleit om instrumenten voor internationale samenwerking te benutten in de strijd tegen cybercriminaliteit en om op dit gebied te komen tot politiële en justitiële samenwerking met derde landen van waaruit cybercriminele organisaties opereren ([2]).

De conclusies van de Raad over “Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU” ([3]) vormen een aanvulling op de strategie inzake cyberbeveiliging van de EU door de nadruk te leggen op de noodzaak van het voorkomen, ontmoedigen en opsporen van en reageren op kwaadwillige cyberactiviteiten. In de conclusies wordt onderstreept dat overheidsinstanties moeten worden toegerust met instrumenten voor het opsporen, onderzoeken en vervolgen van cybercriminaliteit.

Eurojust richt zich op de bestrijding van cybercriminaliteit met het oog op de versterking van de justitiële samenwerking op dit gebied, met name door het faciliteren van de snelle behandeling van gerechtelijke verzoeken. Dit is essentieel gezien de vluchtigheid van gegevens en om lacunes te kunnen verhelpen die zich voordoen als gevolg van verschillen tussen nationale regels voor gegevensbewaring. Daarnaast kan deze samenwerking worden versterkt door de rechterlijke macht vroegtijdig te betrekken bij operaties tegen cybercriminaliteit, zodat gegevens tijdens de onderzoeksfase in overeenstemming met de toepasselijke voorschriften worden verzameld en deze in latere gerechtelijke procedures als toelaatbaar elektronisch bewijsmateriaal kunnen worden ingediend. Bovendien ontwikkelt Eurojust strategische producten op het gebied van cybercriminaliteit of levert het daaraan een aanzienlijke bijdrage, om zo beroepsbeoefenaren te helpen noodzakelijke cyberspecifieke vaardigheden verder te ontwikkelen ([4]).

([1]) Conclusies van de Raad over de gezamenlijke mededeling van de Commissie en de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid over de Strategie inzake cyberbeveiliging van de Europese Unie: een open, veilige en beveiligde cyberspace, Brussel, 27.7.2013 (12109/13).

([2]) Eurojust is betrokken bij verschillende projecten voor capaciteitsopbouw op het gebied van cybercriminaliteit, zoals het SIRIUS-project, (http://eurojust.europa.eu/Practitioners/Pages/SIRIUS.aspx), het EuroMed Justice-project (https://www.euromed-justice.eu/) en het GLACY+-project (https://www.coe.int/en/web/cybercrime/glacyplus).

([3]) Raad van de Europese Unie, conclusies van de Raad over de gezamenlijke mededeling aan het Europees Parlement en de Raad: Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU, Brussel, 20.11.2017 (14435/17).

([4]) Zie voor meer informatie het hoofdstuk “Projecten en publicaties van Eurojust op het gebied van cybercriminaliteit” in dit document.

In dit rapport wordt een overzicht gegeven van de werkzaamheden van Eurojust op het gebied van cybercriminaliteit. De operationele werkzaamheden van Eurojust geven een uitstekend beeld van de gemeenschappelijke uitdagingen waarmee beroepsbeoefenaars worden geconfronteerd, alsook van de beste praktijken om deze uitdagingen het hoofd te bieden. De door Eurojust behandelde zaken zijn een nuttige bron van informatie over specifieke problemen op het gebied van justitiële samenwerking en over de wijze waarop deze kunnen worden opgelost; deze informatie draagt bij aan de discussie over de wijze waarop cybercriminaliteit het best kan worden aangepakt. Daarna volgt een hoofdstuk met voorbeelden van zaken. Ten slotte wordt een lijst gegeven van de publicaties en relevante projecten van Eurojust op het gebied van cybercriminaliteit.