

## Online veiligheid

- De speurders van de *Internet Referral Unit* (i2-IRU) hebben hun steentje bijgedragen in 1034 dossiers, voornamelijk rond terroristische propaganda en aanverwante gewelddadige extremistische activiteiten op het internet.
- Ransomware blijft een groot deel van de aandacht van de Federal Computer Crime Unit (FCCU) opeisen.
- Na een pauze van enkele jaren heeft de FCCU de opleiding tot het behalen van het functioneel brevet 'Computer Crime Unit' opnieuw georganiseerd.

### Internetrecherche

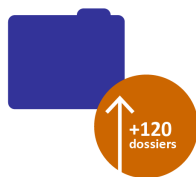
De sectie i2-IRU van de Directie van de bestrijding van de zware en georganiseerde criminaliteit (DGJ/DJSOC) voert verschillende opdrachten uit:

- internetrecherche;
- het blokkeren van websites en/of content;
- communicatie over preventie;
- opleiding, het geven van informatie en het delen van expertise;
- deelname aan de acties van Europol.

Dit team focust onder meer op terroristische propaganda en aanverwante gewelddadige extremistische activiteiten op het internet. Deze opdracht kadert binnen de Internet Referral Unit opgericht door Europol (IRU EU). In concreto wordt de opgespoorde propaganda ontoegankelijk gemaakt in samenwerking met de providers.

Wat de steun van de cel aan de eenheden betreft, ging het in 2019 om 1 034 dossiers. Dat is een stijging met 120 dossiers ten opzichte van 2018.

**1 034**



Dossiers

| Fenomenen                           | 2019 |
|-------------------------------------|------|
| Terrorisme                          | 314  |
| Informatie                          | 132  |
| Fraude                              | 118  |
| Diefstal                            | 91   |
| Poging tot zelfmoord                | 66   |
| Seksueel misbruik van minderjarigen | 54   |
| Mensenhandel                        | 47   |

|               |    |
|---------------|----|
| Openbare orde | 40 |
| Cyberhaat     | 37 |
| Cybercrime    | 31 |
| Wapens        | 26 |
| Verdwijningen | 23 |
| Hormonen      | 13 |
| Moord         | 2  |

## Federal Computer Crime Unit

De opdracht van de Federal Computer Crime Unit (FCCU) bestaat erin de strijd aan te gaan met ICT-criminaliteit (*Information and Communication Technology*), onder andere om de burgers te beschermen tegen nieuwe criminaliteitsvormen in de virtuele maatschappij. Die opdracht omvat ook de ondersteuning van de strijd tegen andere criminele fenomenen dankzij gespecialiseerde onderzoeken in ICT-omgevingen.

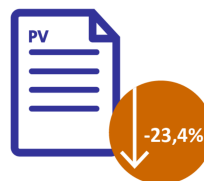
De FCCU heeft in 2019:

121



121 dossiers cybercrime behandeld;

131



131 pv's met modus operandi ransomware\*

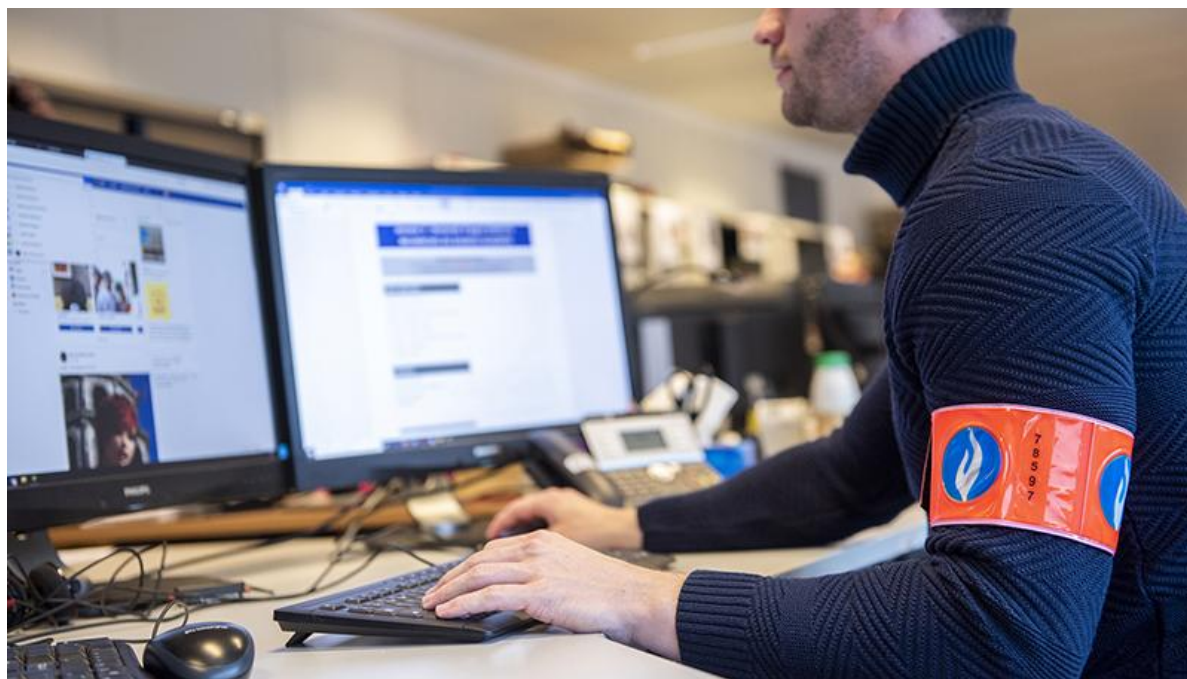
\* Bij de modus 'ransomware' installeren oplichters op een slinkse manier een virus op een toestel buiten het medeweten van de eigenaar om. Het virus houdt het toestel en de bestanden 'gegjzeld' (geëncrypteerd) en de oplichters vragen losgeld.

### Opleiding en expertise

Het afgelopen jaar heeft de FCCU na een intermezzo van enkele jaren opnieuw de opleiding tot het behalen van het functioneel brevet 'Computer Crime Unit' georganiseerd. Intussen hebben 60 personen de basismodule gevolgd. De examens worden pas in 2021 afgenomen.

Voorts leverde de FCCU een substantiële bijdrage aan meerdere Europese opleidingsprojecten rond het *darkweb*. De feedback op de trainingen die onder de koepel van het Europees Politiecollege CEPOL werden georganiseerd – twee trainingssessies waar een 60-tal politiemedewerkers uit verschillende Europese landen aan deelnamen – was positief.

Ten slotte heeft de FCCU het concept en de werking van de Quick Reaction Force op punt gesteld. Dit team staat in voor de politionele respons in het kader van het cybernoodplan van het Centrum voor Cybersecurity België (CCB). Zowel medewerkers van de FCCU als van de regionale CCU's zijn voorzien in het team. Sinds de oprichting van de Quick Reaction Force zijn er nog geen incidenten geweest die aan de voorwaarden voor een inzet voldeden (opschaling volgens het cybernoodplan).



Success Story

## Hackerstool wereldwijd offline na internationale politieactie

Een gevaarlijke hackerstool IM-RAT (*Imminent Monitor Remote Access Trojan*) is offline gehaald als resultaat van een onderzoek dat vorig jaar is opgestart door de Australische federale politie. Als de hackerstool eenmaal was geïnstalleerd op een computer, gaf deze tool de cybercriminelen de vrije hand over de machine van het slachtoffer. De opsporingsdiensten vermoeden dat er tienduizenden slachtoffers zijn. Bij een internationale politieactie verrichtte de FCCU drie succesvolle huiszoekingen bij verdachten die leidden tot de inbeslagnames van bewijsmateriaal en één voorlopige hechtenis.

### Federale Politie

✉ [federal.contactcenter@police.belgium.eu](mailto:federal.contactcenter@police.belgium.eu)

🌐 [www.federalepolitie.be](http://www.federalepolitie.be)

### Archief

[Jaarverslag 2018](#)

[Jaarverslag 2017](#)

### Taalkeuze

[Nederlands](#)

[Français](#)

