Barrièremodel digitale criminaliteit en cybercrime

Op dit thema zijn veel innovatieve ontwikkelingen en pilots gestart in Oost-Nederland die veel belovend zijn. Sommige bevinden zich in de fase van planvorming, andere interventies worden al uitgeprobeerd of toe gepast.
In grote lijnen zijn er twee sporen: bewustwording en betekenisvolle interventies.

- *Bewustwording* is van belang vanwege het preventieve effect dat hiervan uitgaat. Daarnaast is het erg belangrijk dat ketenpartners weten wat ze moeten doen als ze getroffen worden door een cyberaanval (bijvoorbeeld: het voorkomen van datavernietiging door een verkeerde aanpak, wat te doen als een cyberaanval de oorzaak is van een GRIP-situatie, wat zijn dan de do's en dont's en wat betekent dat voor de crisisorganisatie?).

- *Betekenisvolle interventies* (geen uitputtende opsomming maar slechts enkele voorbeelden):
  - Een vernieuwende publiek-private samenwerking is een *digitale authentieke handtekening-app* die door politie, OM, enkele gemeenten, de Radboud Universiteit samen met grote webshops, brancheorganisaties en postorderbedrijven ontwikkeld wordt.
  - In IJsselland Zuid loopt de pilot 'betekenisvol handelen bij aangiften van fraude en onlinehandel'.Verdachte rekeninghouders (katvangers/moneymules) die hun bankrekening (laten) gebruiken ten behoeve van internetoplichting worden thuis door de politie bezocht (stopgesprek) en krijgen de mogelijkheid om een schuldbekentenis te ondertekenen en het slachtoffer terug te betalen (civiele overeenkomst). Indien men niet mee werkt kan er een strafrechtelijk onderzoek gestart worden. De pilot draagt bij aan genoegdoening, het stoppen van het strafbare feit en het vergt geen extra opsporingscapaciteit van het basisteam.Landelijk is er grote belangstelling voor deze aanpak.