PLATFORM IVZ

SAMEN STERK VOOR EEN VEILIG TWENTE

Opdrachtnaam Project Cybercrime Twente

Aanleiding	Cybercrime omvat strafbare feiten die worden gepleegd via een ICT middel én die gericht zijn op een ICT middel, zoals hacking, DDoS-aanvallen, en ransomware. Gedigitaliseerde criminaliteit bestaat uit strafbare feiten waarbij gebruik gemaakt wordt van een ICT middel, zoals bijvoorbeeld online fraude. Zowel in de Veiligheidsstrategie Oost-Nederland als in het Platform IVZ in Twente ligt de focus van de aanpak op zowel cybercrime als gedigitaliseerde criminaliteit. Cybercrime en gedigitaliseerde criminaliteit samen wordt ook wel 'digitale criminaliteit' genoemd. Echter, omdat zowel in de professionele context als in de communicatie richting samenleving vaak de term 'cybercrime' wordt gebruikt waar eigenlijk digitale criminaliteit bedoeld wordt, hanteren we in dit project ook de term 'cybercrime' als brede definitie. Waar we dus spreken over de term cybercrime, omvat deze term zowel hierboven gegeven definitie van cybercrime als gedigitaliseerde criminaliteit. Waar we enkel cybercrime in enge zin bedoelen (dus waarbij zowel middel als doel van criminaliteit ICT betreft), staat dat er specifiek bij. De samenleving digitaliseert, en de ontwikkelingen volgen elkaar in een razend tempo op. Het digitaliseren van de samenleving brengt ook met zich mee dat de criminaliteit zich in de digitale samenleving nestelt. Het plegen van stafbare feiten met behulp van informatietechnologie (ICT) is een groeiend fenomeen waar de ogen niet voor gesloten kunnen worden, en waar veel mensen slachtoffer van worden. Van de Nederlanders van 12 jaar en ouder maakt 97,7% gebruik van internet, waarvan 92,6% dagelijks voor privé doeleinden online is. Van deze doelgroep zegt 8,5% in 2018 slachtoffer te zijn geweest van één of meerdere vormen van digitale criminaliteit (Bron: CBS en VNG). Hoewel cybercrime voor de coronacrisis al de snelst groeiende vorm van criminaliteit was, is het probleem tijdens de corona-crisis alleen nog maar urgenter geworden. Tijdens de corona-crisis is het aantal politie-registraties van cybercrime, zowel landelijk als in Twente, flink gestegen. De meest waarschijnlijke oorzaak hiervan is het intensievere gebruik van digitale (communicatie)middelen door thuiswerken en het wegvallen van fysiek contact. Daar komt bij dat het aantal geregistreerde gevallen nog maar het topje van de ijsberg is; het werkelijke aantal cybercrime-incidenten en dus slachtoffers hiervan, ligt vele malen hoger. De veiligheidspartners erkennen het belang van de aanpak van cybercrime. Het thema is geprioriteerd in de Veiligheidsstrategie Oost-Nederland, en Politie en Openbaar Ministerie (OM) zetten stevig in op de aanpak van cybercrime. Ook gemeenten onderkennen het belang van lokale inspanningen en zien een verschuiving in de lokale criminaliteit van traditionele misdrijven naar criminaliteit met een digitaal component. Uit cijfers van het CBS blijkt dat tussen 2012 en 2018 het slachtofferschap van hacken zelfs hoger lag dan dat van fietsendiefstal. Het DVO wil de komende jaren samen met de partners gezamenlijk de strijd aan gaan tegen cybercrime via een aanpak zoals dat in dit document wordt beschreven.
Betrokken partners	Politie , OM, Veiligheidsregio, gemeenten, Saxion Hogeschool, Ministerie J&V, Centrum voor Criminaliteitspreventie en Veiligheid (CCV), bedrijfsleven, onderwijs, maatschappelijke organisaties en burgers.

PLATFORM IVZ
SAMEN STERK VOOR EEN VEILIG TWENTE

Opdrachtnaam **Project Cybercrime Twente**

Doelstelling en maatschappelijke effecten	**Doelstelling** Om cybercrime tegen te gaan, is het nodig om het 'nieuwe' fenomeen eigen te maken. Er is nog veel onbekend over het thema bij de overheid en de samenleving. De uitdaging zit daarom voornamelijk in kennisopbouw en bewustwording. De politie en het Openbaar Ministerie (OM) zijn gestart met kennisopbouw en bewustwording en de strafrechtelijke beoordeling van strafzaken. Duidelijk is: de aanpak van cybercrime komt niet tot stand door alleen een traditionele strafrechtelijke aanpak: samenwerking is essentieel. Met de Twentse aanpak van cybercrime willen we bijdragen aan: 1. Een weerbare overheid en maatschappij tegen cybercrime 2. Keten brede samenwerking en deskundigheidsbevordering. 3. Creëren ongunstig klimaat voor cybercrime door het opwerpen van barrières en het verhogen van het (ervaren) risico van daderschap. <u>Ad 1) Weerbare overheid en maatschappij</u> Om een effectieve weerbaarheid te creëren, is het nodig dat de overheid en maatschappij urgentie ervaren en dat zij weten waar risico's en bedreigingen bestaan. Een weerbare overheid en maatschappij begint dan ook met bewustwording van de gevaren. Dat vraagt inzet op het thema door middel van communicatie over het fenomeen, bij voorkeur op een wijze die cybercrime aan de keukentafel brengt. Mensen zijn namelijk minder geneigd om actie te ondernemen als zij onvoldoende urgentiebesef hebben. De direct daarop volgende stap is die van preventie. Als overheid én maatschappij zich bewust zijn van de risico's, staan zij open voor handelingsperspectief en kan gerichte preventie activiteit worden ingezet. Daarbij is het van belang om dit per doelgroep effectief te richten. In de aanpak van deze doelstelling, is het zeer zinvol om publiek-private samenwerking aan te gaan. Daarmee creëren we een direct bondgenootschap met (één of meerdere) doelgroepen. <u>Ad 2) Keten brede samenwerking en deskundigheidsbevordering</u> De bestrijding van cybercrime zal niet tot stand komen door de klassieke, strafrechtelijke aanpak. Slachtoffers zijn vaak onwetend en daders zijn moeilijk traceerbaar. In onze (netwerk)samenleving hebben partijen en organisaties elkaar nodig om de gezamenlijke kennis en expertise in te zetten bij maatschappelijke vraagstukken, zo ook bij cybercrime. Om cybercrime effectief aan te kunnen pakken is het essentieel dat er voldoende kennis en expertise aanwezig is bij partijen die een rol hebben in de aanpak van het fenomeen. Hier is nog veel winst te behalen. Door kennis en expertise bij overheid en veiligheidspartners en bedrijfsleven en maatschappelijke organisaties te vergroten en door elkaars kennis en expertise te benutten door samen te werken, kunnen we effectief slagen maken in de aanpak van cybercrime. <u>Ad 3) Creëren ongunstig klimaat door opwerpen barrières en verhogen (ervaren) risico van daderschap</u> Naast bewustwording, preventie en kennisbevordering, is er wel degelijk een rol weggelegd voor handhaving en opsporing. Gelet op de omvang van het fenomeen is het echter niet realistisch te veronderstellen, dat alle daders en strafbare feiten kunnen worden opgespoord. Een verhoogde pakkans is een factor die het gevolg is van effectieve opsporing. Het verhogen van de *ervaren* pakkans kan potentiële daders afschrikken. Dit vraagt van politie en OM om te laten zien wat we doen: het vraagt om expliciete communicatie over inzet op het thema en de opbrengst. Neveneffect daarvan zou kunnen zijn dat er een extra bewustwording ontstaat in de

Opdrachtnaam Project Cybercrime Twente	
	maatschappij van deze vorm van criminaliteit. En tevens zou de verhoogde ervaren pakkans mogelijk nieuwe aanwas van jonge cyber criminelen afremmen. **Maatschappelijke effecten** De volgende maatschappelijke effecten willen we realiseren: 1. Weerbaarheid overheid, burgers en ondernemers 2. Creëren ongunstig klimaat voor het plegen van cybercrime 3. Het vertrouwen in de overheid behouden, ook in het digitale domein
Projectresultaat	Om bovengenoemde doelen en effecten te behalen, zetten we binnen de scope van dit projectplan de volgende 2 sporen uit: <u>Spoor 1: Vergoten inzicht in digitale criminaliteit breed</u> Zicht op aard, omvang en kwetsbare doelgroepen in Twente door: a) Op basis van beschikbare informatie(netwerken) en kennis zicht krijgen op de aard, omvang en doelgroepen bijv. door middel van dashboard, politiedata, CCV en Saxion Hogeschool. b) Zicht op governance van cybercrime. Inzicht geven in de keten en betrokken partijen door volgende vragen te beantwoorden en te beschrijven. Welke partijen houden zich (in Twente) bezig met cybercrime? Wie is waarvoor verantwoordelijk ? Wie doet wat? Welke partijen hebben we nodig en waarom? Wie heeft de regie? Inzicht in stand van zaken bij Twentse gemeenten op dit thema voor wat betreft o.a. beleid, capaciteit, etc. c) Zicht op bestaande tools voor bewustwording in afstemming met veiligheidspartners: inzicht in wat is er allemaal al, voor wie, hoe te gebruiken, effectiviteit etc. (beschikbaar stellen in soort gereedschapskist). d) Zicht op daders en daderprofielen: door kennis te vergaren over wat daders van cybercrime kenmerkt, kunnen gerichter interventies op daders worden bepaald en ingezet. <u>Spoor 2: Uitdragen van verworven inzicht</u> a) Vergroten kennis overheidspartijen via bijv. bijeenkomsten tutorials. b) Vergroten weerbaarheid kwetsbare doelgroepen, ondernemers en burgers: daadwerkelijk inzetten van bewustwordingsacties en bieden handelingsperspectief. Effect monitoren. c) Open kennisdeling. Vergelijkbaar met interne kennis vergrotende middelen, kunnen ook publieke acties worden ingezet. Denk bijvoorbeeld aan tutorials (Youtube-wise), challenges, preventietips. d) Gebruik maken van tussenpersonen met als boodschap: wees alert op cybercrime. Denk aan: medewerkers schuldsanering, sociale wijkteams, andere eerstelijnszorg, seniorenhuisvesting, scholen, banken etc. e) Aanpak van cybercriminelen, verhogen (ervaren) risico van daderschap: vooral Politie / OM / HALT: bijv. strafrechtelijke afhandeling zichtbaarder maken (communicatie)
Prestatie indicatoren	1. Inzicht in de hierboven beschreven verschillende facetten van Cybercrime 2. Vergrote kennis en expertise bij partijen die een rol hebben in de aanpak van cybercrime 3. Intensievere samenwerking op het thema *Gedurende het project bekijken we hoe we de prestatie-indicatoren meetbaar maken*

Opdrachtnaam **Project Cybercrime Twente**	
Monitoring / voortgangs-bewaking	1. Dit project kent een looptijd t/m 2022. We willen in 2020 een begin maken met voornoemde sporen. Voor de uitvoering worden aparte werkgroepen en uitvoeringsprogramma's opgesteld. 2. Expertgroep maandelijks. 3. Werkgroepen maandelijks. 4. Halfjaarlijks voortgangsbericht aan het DVO. 5. Elk jaar evalueren en doelen bijstellen. Fungeren als saté-prikker. Eens per half jaar met alle projectleiders van de IVZ projecten bij elkaar om voortgang en processen af te stemmen. 6. Hoe vaak afstemming met bestuurlijk portefeuillehouder?
Randvoorwaarden	1. Gezamenlijke aanpak in Twente door gemeenten, politie en OM. 2. De overheid moet de verantwoordelijkheid van inwoners en ondernemers niet overnemen. Uitgangspunten zijn dat de aanpak van cybercrime in gezamenlijkheid plaatsvindt (publiek en privaat) en dat burgers en bedrijven zelf maatregelen nemen om geen slachtoffer te worden (vergroten weerbaarheid). 3. Ruimte voor learning by doing 4. Financiële middelen. 5. Voldoende capaciteit en continuïteit
Afbakening	De expertgroep cybercrime Twente richt zich op: 1. De regionale activiteiten binnen Twente 2. Het vergroten van de weerbaarheid van Twente en het opwerpen van barrieres tegen cybercrime in Twente 3. Het ondersteunen en faciliteren van de Twentse partners die een rol hebben in de aanpak van cybercrime 4. Afstemming met het expertteam cybercrime Oost-Nederland (vallend onder het Veiligheidsnetwerk Oost-Nederland) Het CCV onderscheidt drie taken van gemeenten om cybercrime in brede zin aan te pakken en voorbereid te zijn: 1. Eigen huis op orde (intern): verantwoordelijkheid nemen voor het goed functioneren van de eigen digitale systemen. Dit is de eigen verantwoordelijkheid van iedere instantie en valt buiten de scope van dit projectplan. 2. Voorbereid zijn op cyberincidenten en cybercrises: cyberincidenten en cybercrises vormen een steeds grotere bedreiging voor overheden, veiligheidsregio's, bedrijven en burgers. Het regionale project Cyber-respons (Veiligheidsregio Twente) legt hier de focus op. Vanuit de expertgroep wordt verbinding gemaakt met het regionale project Cyber-respons, maar de voorbereiding op cyberincidenten in cybercrises valt buiten de scope van dit project. 3. Cybercrime en gedigitaliseerde criminaliteit (extern): weerbaar maken van bewoners en ondernemers. Zoals beschreven houdt de expertgroep cybercrime Twente zich zeker bezig met dit onderdeel van de aanpak van cybercrime.
Relatie andere initiatieven en ontwikkelingen	1. Veiligheidsstrategie Twente en Oost-NL. 2. We zoeken actieve afstemming met de andere expertgroepen van het Platform IVZ, zoals de expertgroep intelligence (over ontwikkelen dashboard cybercrime) en de expertgroep ondermijning 3. We zoeken aansluiting bij- en zorgen voor afstemming met het onderzoek van Saxion (geleid door Remco Spithoven) naar interventies om cyberweerbaarheid van burgers en bedrijven te vergroten.

Opdrachtnaam **Project Cybercrime Twente**	
	4. We zorgen ervoor dat we afstemming zoeken en cross-overs maken met relevante andere (beleids)terreinen. 5. Er zit een digitale factor in vrijwel elk deel van ons leven. Daarmee is het ook van belang om in de diverse bestuurlijke portefeuilles en gezamenlijke projecten de digitale factor bewust te benaderen/beoordelen. Vervolgens kan er de keuze worden gemaakt om kennis te halen en meer of minder intensief te gebruiken. 6. Expertteam cybercrime Oost-Nederland (Veiligheidsstrategie Oost-NL 2019-2020) is ondersteunend aan Kerngroep Cybercrime Oost-Nederland waarin bestuurlijk portefeuillehouder, ambtelijk trekker, Cyberofficier v Justitie en een cyberspecialist van de politie onderdeel van uit maken. Vanuit de expertgroep cybercrime Twente zorgen we voor afstemming met- en actieve deelname aan het expertteam cybercrime Oost-NL. 7. OM heeft samen met politie een handelingskader: een soort selectiviteitskader welke cybercrimezaken wel/ niet opgepakt worden.
Risico's / onverwachte zaken /effecten	1. Meer aandacht leidt tot meer reactie en response. Dit kan tot meer meebewegen in de samenleving leiden (burgerinitiatief) of actieve betrokkenheid van het bedrijfsleven, waardoor het initiatief (nu vanuit de overheid) snel breder maatschappelijk gedragen wordt. 2. Een ander effect zou kunnen zijn dat mensen meer criminaliteit waarnemen en dus meer melden – dit kan van invloed zijn op het criminaliteitsbeeld en (on)veiligheidsbeleving van inwoners. 3. De 'digitale wereld' is snel, veelvuldig en continu in verandering en beweging, waardoor we flexibel moeten kunnen inspelen op onvoorziene zaken. Daarom moet er, wanneer de omstandigheden ernaar vragen, gemotiveerd afgeweken kunnen worden van dit projectplan.
Expertgroep	Burgemeester Wierden mw. Tigchelaar-Van Oene: DVO portefeuillehouder Susan Faal: projectleider Suzanne Coehorst: secretaris Mark Imbos: Openbaar Ministerie Manon Gregoire: Politie Remco Aagtjes: Politie Herald Arnold: gemeente Hellendoorn Mayke ten Bos: gemeente Hengelo Jane Slot: platform IVZ
Planning en mijlpalen	Project loopt tot 31 december 2022.
Communicatie	De communicatie naar betrokkenen en de samenleving zal in de uitvoeringsprogramma's van de verschillende onderdelen verder vorm krijgen. Het DVO zal halfjaarlijks worden geïnformeerd middels een voortgangsbericht.
Financiën	Zodra we scherper inzichtelijk hebben welke financiële behoefte er is voor de uitvoering van onze activiteiten, onderzoeken we de mogelijkheden voor het aantrekken van budget, bijv. door middel van Platform IVZ en subsidies.