Inventarisatie Cyberveiligheid

Veilige woon- en leefomgeving: alledaags, in de wijk en omgeving	Veilig Ondernemen	Jeugd en Veiligheid	Fysieke Veiligheid	Integriteit en Veiligheid
Sociale kwaliteit (woonoverlast, alcohol- en drugsoverlast, etc.) *Digitale criminaliteit* • Hacking/phishing/malware/spam/ ransomware, waarbij burgers zelf slachtoffer worden *Veiligheid met een digitaal component* • Woonoverlast: het continueren van treitergedrag, pesten en stalken van buren etc. online • Oplichting via marktplaats, identiteitsfraude • Kwetsbare doelgroep: LVB, ouderen die slachtoffer kunnen worden van digitale oplichting	**Veilige winkelgebied** *Digitale criminaliteit* • Oplichting bij koop/verkoop via websites, bijv. van winkels of Marktplaats • Beveiliging van digitale transacties. • Verstoring van websites. • Hacking/phishing/malware/spam/ ransomware, waarbij ondernemers zelf slachtoffer worden	**Jeugdoverlast** *Veiligheid met een digitaal component* • Digitaal pesten	**Verkeersveiligheid** *Digitale criminaliteit* • Beveiliging van verkeerssystemen tegen hacken/beïnvloeding van buiten. • Beveiliging van voertuigen	**Polarisatie en radicalisering** *Veiligheid met een digitaal component* • Haatzaaiende websites • Online extremisme • Opruiing • Online mobiliseren grote groepen mensen (demonstratie, project X)
Fysieke kwaliteit (vernielingen, verloedering etc.) *Digitale criminaliteit* • Veiligheid openbare wifi-spots. • Vernieling en verloedering: verstoring ICT door criminelen • Hacken internet of things (camera's, thermostaat, brandmeldsystemen etc.) *Veiligheid met een digitaal component*	**Veilige bedrijventerreinen** *Digitale criminaliteit* • Zie ook veilige winkelgebied. • DDOS-aanvallen op bedrijven. • Digitale spionage of verkoop van informatie. • Verstoring van systemen die noodzakelijk zijn voor bedrijfsvoering.	**Jeugdcriminaliteit** *Digitale criminaliteit* • Van sexting naar sextortion (afpersen van groepsgenoten) • Grooming van bijvoorbeeld jonge kinderen via online vriendschappen • Jeugdgroepen zijn digitaal actiever en kunnen zich schuldig maken aan gedigitaliseerde criminaliteit of treitergedrag	**Brandveiligheid** *Digitale criminaliteit* • Hacken van brandweerwagen- • systemen	**Georganiseeerde criminaliteit** *Digitale criminaliteit* • Darkweb om wapens, drugs etc te kopen en verkopen • Bitcoins • Witwassen van geld: link virtuele en fysieke wereld

- Digitale criminaliteit is Cybercrime + gedigitaliseerde criminaliteit. Cybercrime is criminaliteit met ICT als middel én doelwit. Gedigitaliseerde criminaliteit is 'ouderwetse' criminaliteit die een nieuwe impuls heeft gekregen door de opkomst van computertechnologie. Denk hierbij onder meer aan fraude, bedreiging of het witwassen van geld via digitale betaalmethoden. https://www.politie.nl/themas/cybercrime.html
- Veiligheid met een digitaal component is de verbinding tussen de digitale en fysieke wereld waarin de digitale wereld zich op een dergelijke manier organiseert of manifesteert wat impact kan hebben op de openbare orde en veiligheid in de fysieke wereld.

Veilige woon- en leefomgeving: alledaags, in de wijk en omgeving	Veilig Ondernemen	Jeugd en Veiligheid	Fysieke Veiligheid	Integriteit en Veiligheid
Objectieve veiligheid/HIC *Digitale criminaliteit* • (Woning)inbraak: hacken van privé computers/ telefoons of ander eigendom dat gekoppeld is aan internet (Internet of things) • Diefstal: Phishing • Ransomware • Vermogensdelicten via internet, bijv. heling • Bedreiging/stalken via digitale middelen • Diefstal: ID-fraude • Diefstal/roof van informatie of privé-gegevens • Prive computers gebruiken als onderdeel van botnet. *Veiligheid met een digitaal component* • Bedreiging: Personen online via verschillende kanalen bedreigen en treiteren	**Veilig uitgaan** *Veiligheid met een digitaal component* • Hoe om te gaan met spontane feesten via internet georganiseerd? • Hoe om te gaan met feesten die online gepromoot worden en een bepaalde doelgroep aantrekken die bekend staan om het veroorzaken van vechtpartijen en verstoring van de openbare orde?	**Jeugd, alcohol en drugs** *Digitale criminaliteit* • Online kunnen kopen van drugs via darkweb en verhandelen van drugs op en rond scholen.	**Externe veiligheid** *Digitale criminaliteit* • Beveiliging systemen opslag/ verwerken • gevaarlijke stoffen. • Vitale infrastructuren goed beveiligd tegen cyberaanvallen?	**Veilige publieke taak** *Gedigitaliseerde criminaliteit en Veiligheid met een digitaal component* • Digitaal pesten/cybertrollen waarbij bedreigingen worden geuit. • Bewustzijn van bestuurders en ambtenaren welke informatie ze op internet plaatsen.
Subjectieve veiligheid (veiligheidsgevoel) *Digitale criminaliteit* • Podia om voorbeelden van cybercriminaliteit te delen. • Aandacht voor handel in drugs via internet, aanbieden (thuis)prostitutie. • Toezicht- en handhaving op cybercriminaliteit: wat voor impact heeft cybercrime op het veiligheidsgevoel van de burger? Creëren van bewustzijn bij burger en verantwoordelijkheden van gemeenten, politie, OM en burger duidelijk maken.	**Veilige evenementen** *Veiligheid met een digitaal component* • Hoe om te gaan met spontane evenementen via internet georganiseerd? • Demonstraties: online worden oproepen gedaan om te gaan demonstreren, zonder dat de organisator zich heeft gemeld bij de gemeente. Hoe ga je hier als gemeente mee om? • Hacken van kermisattracties: hoe gaan gemeenten om met de verstrekking van vergunningen aan bedrijven? Hoe weet je als gemeente dat de systemen van de vergunning aanvrager "veilig" zijn?	**Veilig in en om school** *Cybercrime en Veiligheid met een digitaal component* • Digitaal pesten • Sexting • Gebruik van mobieltjes om te filmen in de klas maar ook in de kleedkamer, gymzaal etc. • Veiligheid van school ICT	**Rampenbestrijding en Crisisbeheersing** *Digitale criminaliteit* • Crisisorganisatie voorbereid op scenario's waarbij vitale infrastructuren onbruikbaar zijn of schade veroorzaken a.g.v. cyberaanvallen • Risico analyse crisisbeheersing van impact van hacking of DDOS aanval. Hoe vindt crisiscommunicatie in dergelijke situaties dan plaats?	**Informatieveiligheid** *Cybercrime* • Beveiliging van gemeentelijke en regionale systemen en digitale dienstverlening tegen hacken, cyberaanvallen en datalekken. (ondersteuning IBD van VNG en KING) • Opbouwen veiligheidsbewustzijn informatieveiligheid in de gemeentelijke organisatie • Vlotte incident detectie en coördinatie

- Digitale criminaliteit is Cybercrime + gedigitaliseerde criminaliteit. Cybercrime is criminaliteit met ICT als middel én doelwit. Gedigitaliseerde criminaliteit is 'ouderwetse' criminaliteit die een nieuwe impuls heeft gekregen door de opkomst van computertechnologie. Denk hierbij onder meer aan fraude, bedreiging of het witwassen van geld via digitale betaalmethoden. https://www.politie.nl/themas/cybercrime.html
- Veiligheid met een digitaal component is de verbinding tussen de digitale en fysieke wereld waarin de digitale wereld zich op een dergelijke manier organiseert of manifesteert wat impact kan hebben op de openbare orde en veiligheid in de fysieke wereld.

Veilige woon- en leefomgeving: alledaags, in de wijk en omgeving	Veilig Ondernemen	Jeugd en Veiligheid	Fysieke Veiligheid	Integriteit en Veiligheid
	Veilig toerisme *Digitale criminaliteit* • Veiligheid openbare wifispots			**Ambtelijke en bestuurlijke integriteit** *Cybercrime* • Bij inbouwen controlemechanismen aandacht besteden aan wie toegang heeft tot welke digitale informatiesystemen. • Mogelijkheden infiltratie systemen via personen (intern en extern)

Algemeen

Rol gemeente:

1. Beveiliging eigen systemen en organisatie.
2. Cyberveiligheid binnen de gemeente vergroten met daarin een regierol in bewustwording van gevaren van digitale criminaliteit en aandacht voor preventie.
3. Bestuurlijke handhaving in cyberspace. Momenteel wordt onderzoek gedaan naar de rol van burgemeesters in cyberspace.