Cybersecurity in verkiezingsprogramma's TK 2021

CONCEPT 0.3

Centre for the Law
and Economics of
Cyber Security

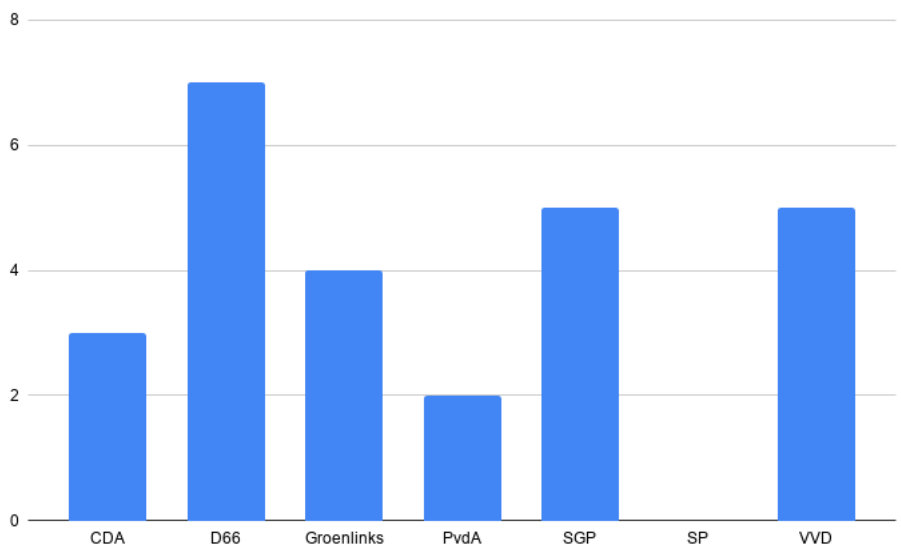
Burgermeester Oudlaan 50
3062 PA
Rotterdam

010-4082186
clecs.eu

Erasmus School of Law **Erasmus University Rotterdam**

Cybersecurity in verkiezingsprogramma's

Dit document bevat een analyse van de aan cybersecurity gerelateerde standpunten in de conceptverkiezingsprogramma's van een aantal partijen in de tweede kamer. Het gaat hier om een analyse van de standpunten die primair over cybersecurity gaan. Standpunten waar 'cybersecurity' zijdelings wordt genoemd, zijn niet meegenomen. Het doel is om een bondig overzicht te hebben van de verschillende afzonderlijke standpunten van diverse partijen. Het document beoogt uitdrukkelijk niet om een diepgravende analyse te geven van de wijze waarop verschillende politieke partijen invulling willen geven aan beleid rondom cybersecurity. In de onderstaande figuur zijn het aantal standpunten over cybersecurity per partij weergegeven.



Figuur 1: aantal standpunten over cybersecurity in conceptverkiezingsprogramma's, per partij

Dit document bevindt zich nog in de conceptfase. De resultaten veranderen mogelijk nog. Zo kunnen de verkiezingsprogramma's kunnen nog wijzigen en worden sommige programma's pas in een later stadium verwacht. Ook doen wij nog een aantal iteraties op de inhoud. Op de volgende pagina's worden per partij de standpunten genoemd in de verkiezingsprogramma's die cybersecurity behandelen.

CDA

“Wij zijn bezorgd over de cybersecurity in ons land. Volgens onze eigen diensten liggen we dagelijks onder vuur. Kennis wordt gestolen, vitale systemen aangevallen en desinformatie verspreid. Om de digitale weerbaarheid te vergroten, willen wij een meerjarig cybersecurityprogramma onder leiding van een aparte Nationale Cybersecurity Coördinator.”

“Nederland moet zich beter voorbereiden en oefenen op een massieve verstoring van het digitale domein door een technische storing of cyber-aanval. Als knooppunt in het internationale dataverkeer kan een storing in Nederland leiden tot grote economische en maatschappelijke ontwrichting.”

"De inlichtingen en veiligheidsdiensten moeten worden versterkt om Nederland te beschermen tegen de groeiende digitale en geopolitieke dreigingen uit landen als Rusland en China. De gezamenlijke huisvesting moet worden aangegrepen om voor de diensten een Cyberhub te creëren, waar het Defensie Cyber commando en het Nationale Cybersecurity Centrum deel van uit maken. Waar nodig wordt de WIV aangepast om de effectiviteit van de diensten te vergroten. "

D66

“We investeren het extra geld dat we beschikbaar stellen voor de politie en het OM in de aanpak van nieuwe vormen van criminaliteit, zoals cybercriminaliteit, en in effectieve bestrijding van ambtelijke corruptie.”

"Er komen fors meer investeringen in onderzoek op het gebied van digitale techniek, zoals kunstmatige intelligentie, cyber security, quantum computing en fotonica"
“Om deze rol te kunnen uitbouwen, hebben we echt één duidelijke aanpak nodig. Om cybercriminaliteit en

internationale cyberconflicten te kunnen bestrijden, moet investeren in onze digitale veiligheid een gewoonte worden."

"Het Nationale Cyber Security Centrum (NCSC) mag ook relevante beveiligingsinformatie van nietvitale sectoren gaan delen met Computer Emergency Response Teams."

"Nederland was een van de eerste landen die samenwerking met ethische hackers stimuleerde door middel van een responsible disclosure richtlijn. Het is nu tijd om de volgende stap te zetten en de inzet van ethische hackers verder te professionaliseren door middel van actieve bug bounty programma's door de overheid en het stimuleren van responsible disclosure beleid bij bedrijven. Ook ondersteunen we initiatieven om jonge hackers op het rechte pad te houden."

"Er moet een procedure voor supersnelrecht komen om online content zo snel mogelijk - eventueel tijdelijk - van het internet te verwijderen. Slachtoffers van cybercrime zijn gebaat bij snel handelen. Platforms moeten worden verplicht om content te verwijderen indien nodig."

"Om onze vitale infrastructuur te beschermen tegen cyberaanvallen investeren we in cybercapaciteiten bij Defensie. Kennis hierover bij de Nederlandse krijgsmacht kan zowel in EU- als NAVO-verband worden ingezet."

Groenlinks

"De politie krijgt meer capaciteit en kennis om cybercriminaliteit en zaken als oplichting en kinderporno via internet op te sporen"

" Daarnaast zet Nederland in op het tegengaan van onlineoorlog ('cyberwar'), de beveiliging van informatie en versterking van de diplomatieke dienst. "

"Nederland streeft naar strikte internationale afspraken over de inzet van nieuwe wapensystemen, zoals bewapende drones, cyberaanvallen en hypersone raketten. "

"Technologie en apparatuur voor cybersurveillance gaan ook onder het wapenexportbeleid vallen"

PvdA

"Meer capaciteit voor bestrijding cybercrime. Criminaliteit verlegt zich voor een deel van de straat naar de cyberwereld. Daders blijven te makkelijk ongestraft. Daarom willen we meer en betere rechercheurs die cybercrime aanpakken."

“Beschermen tegen cyberaanvallen. In toenemende mate spelen conflicten zich af in cyber space. Militaire en industriële spionage vormen een directe bedreiging voor onze bedrijven en cruciale infrastructuur. Cyberaanvallen zijn aan de orde van de dag. Nederland geeft prioriteit aan bescherming op dit gebied.”

SGP

“We moeten rekening houden met het gevaar dat (digitale) oorlogvoering zich in de toekomst óók richt op cruciale (civiele) infrastructuur zoals elektriciteitscentrales, datacenters of waterkeringen. Om goed voorbereid te zijn op deze digitale oorlogvoering moet meer budget worden vrijgemaakt voor het defensie-cybercommando en de MIVD. Meer mensen kunnen zorgen voor meer kennis en slagkracht bij defensieve én offensieve inzet. Naast de operationele systemen moeten ook logistieke systemen volwaardig beveiligd worden. Waar nodig worden inlichtingen- en veiligheidsdiensten extra toegerust voor deze taak. Dit is ook van belang voor onze economische veiligheid.”

“Niet iedereen kan in een digitale samenleving goed meekomen. Hier moet aandacht voor zijn. Zo moet de overheid afspraken maken met het bedrijfsleven om kwetsbare groepen te beschermen tegen cybercrime.” “Overheidsdienstverlening dient in principe ook voor groepen met een achterstand in de digitale samenleving goed bereikbaar te zijn.”

“Ondernemers moeten ondersteund worden bij het werken aan meer cyberveiligheid. De inzet en capaciteit van het Digital Trust Centre moet versterkt worden.”

“Overheid en bedrijfsleven dienen afspraken te maken over de cyberveiligheid van kritieke infrastructuur. Hogere veiligheidsstandaarden voor de kritieke delen van de digitale processen zijn absoluut noodzakelijk. Cruciaal is het frequent en grootschalig testen van de beveiliging.”

“Het aantal cyberreservisten dient te worden uitgebreid om meer te kunnen profiteren van de kennis en expertise die onder burgers aanwezig is.”

SP

De SP heeft voor zover wij konden analyseren geen standpunten gerelateerd aan cybersecurity.

VVD

"Investeringen in het Defensie Cybercommando en de inlichtingendiensten. Succesvolle operaties tegen de Russische inlichtingendiensten laten zien dat Nederland hier sterk in is, en zo met unieke kennis en vaardigheden kan bijdragen aan de veiligheid van bondgenoten. "

“Versterken van de Nationale Politie met extra wijkagenten (basisteams), cyberexperts en recherche. Ook worden er

meer hooggeschoolden en specialisten aangenomen om de toegenomen werkdruk op te vangen en gecompliceerde misdaad, zoals cybercrime, te bestrijden."

"Meer vrijwilligers met cyberexpertise bij de Nationale Politie, Justitie, Defensie en de veiligheidsdiensten. Ook maken we het met betere arbeidsvoorwaarden aantrekkelijker voor cyberexperts om bij deze organisaties te werken."

"Versterking van de samenwerking tussen de overheid en het bedrijfsleven om vitale infrastructuur zoals het betalingsverkeer te beschermen tegen steeds agressievere cyberaanvallen. De overheid moet samen met organisaties die vitale infrastructuur beheren, de minimale beveiligingsstandaarden verhogen. Ook versterken we diensten zoals het Nationaal Cyber Security Centrum, het Defensi Cyber Security Centrum en de inlichtingendiensten om de digitale slagkracht en weerbaarheid te vergroten."

"Behoud van de grote economische waarde van de Nederlandse havens. Uitdagingen als cybersecurity, digitalisering en verduurzaming vragen om intensivering van samenwerking tussen de verschillende havens."