

Secondant

THEMA'S: CYBERCRIMESOCIALE MEDIATECHNOLOGIE
RUBRIEK: ONDERZOEK & ANALYSE

INTERNETTROLLEN VERVUILEN HET WEB MET GEVAARLIJK GEDRAG



Foto: Inge van Mill



15 oktober 2018

AUTEUR: ARNOUT DE VRIES

Op het internet duiken steeds meer spookaccounts op, die nepnieuws verspreiden. Deze internettrollen zijn ook verantwoordelijk voor online haatuitingen en kunnen de rechtsorde bedreigen. Hoe kunnen online veiligheid en leefbaarheid gewaarborgd worden in de 21ste eeuw?

Sociale media zijn breed beschikbaar en worden door jong en oud en onschuldige maar soms ook kwaadwillende personen gebruikt. We kennen sociale media vooral als een geweldig middel om met elkaar verbonden te raken via chat en door (vakantie)foto's te delen. Toch kan je niet alleen je

hart luchten met andere gebruikers, maar ook mensen isoleren, van anderen vervreemden en vernederen. Dit varieert van kleine pesterijen tot regelrechte oorlogsvoering. Want kinderen gamen online, maar in dezelfde spelletjes zitten vaak ook neonazi's, zoals in het online oorlogsspel Clash of Clans. Soms zitten zij in eenzelfde chatsessie met jonge, zeer beïnvloedbare kinderen. Toezicht op de online normoverschrijdingen is beperkt, of afwezig.

Het zogeheten trollen als vorm van normoverschrijdend gedrag online neemt toe. Trollen kan beginnen met pesten, maar verergeren tot intimideren en stalken. Het kan slachtoffers zelfs tot zelfmoord drijven. Als dit online gedrag de veiligheid en leefbaarheid schaadt, komt het als verschijnsel in beeld bij de overheid.

VEILIGHEIDSCONFERENTIE

In mei dit jaar werd in Londen een internationale veiligheidsconferentie gehouden over 'trolling'. Onderzoekers en specialisten uit bedrijfsleven en overheden vanuit meer dan 15 Europese landen kwamen bijeen om de kansen voor een vernieuwde aanpak te bespreken. Ook de bedreigingen van deze ontwikkelingen kwamen aan bod. Al deze partijen uit de veiligheidssector hebben als doel om het internet veiliger en leefbaarder te maken.

Twitter heeft last van miljoenen spookaccounts

De techniek heeft zich in de afgelopen jaren zodanig ontwikkeld dat internet een vanzelfsprekendheid is voor veel mensen. Echter, ook anonimiteit door encryptietechnieken en het gebruik van kunstmatige intelligentie worden steeds normaler. De internetgedragscodes veranderen sinds het ontstaan ervan mee, maar: Wat is acceptabel en wat niet? Wat staan we met moderne technologie toe en wat niet? Nieuwe ontwikkelingen bieden nieuwe kansen, maar vormen ook nieuwe bedreigingen. Op het wereldwijde web zijn de meningen verdeeld over hoe ver vrijheid van meningsuiting mag gaan en elk socialemediaplatform hanteert hierbij zijn eigen huisregels. Socialemediaplatforms dulden bijvoorbeeld alleen echte mensen en toch duiken steeds meer valse en machinegestuurde accounts op om te trollen.

DILEMMA'S IN MOEIZAME AANPAK TROLLEN

De conferentie focuste op preventie en interventies in handhaving en vervolging met aandacht voor sociale en technologische innovaties. *Best practices* werden gedeeld, zoals die van John Donovan, werkzaam bij [The Online Hate Crime Hub](#) van de Metropolitan Police. Sinds 2017 pakken de

speciaal getrainde politieagenten online misstanden aan. De Hub onderzoekt meldingen van online haatmisdrijven, waaronder racisme en discriminatie gericht op beperking, religie, of geaardheid en acteren hierop, voor zover mogelijk. Donovan benoemde diverse juridische obstakels bij het trollen, zoals onduidelijke wettelijke kaders die de vervolging van trollen bemoeilijken. Ondersteuning van het slachtoffer staat dan wel centraal bij de Hub, maar als slachtoffers niet willen meewerken aan verdere actie blijven trollen vaak anoniem en ongestraft. Daarmee gaat dan weer geen afschrikkende werking uit tegen herhaling.

NORMLOOSHEID VAN GAMINGPLATFORMS

Gamingplatforms werden expliciet uitgelicht, omdat het normoverschrijdende gedrag hierin nóg prominenter lijkt. Cybercriminoloog Thomas-Gabriel Rüdiger vergeleek online games met een fysieke speeltuin: rond de spelende kinderen zien we borden met simpele gedragsregels en ouders die vanaf een bankje wat toezicht houden. Online houdt niemand zo toezicht. Via online '[speeltuinen](#)' zoals Minecraft, Roblox en MovieStarPlanet worden steeds meer kinderen het slachtoffer van *grooming*, terwijl ouders denken dat ze een onschuldig spelletje spelen.

Volgens sommige trendwatchers is 2018 het jaar van de 'social bot'

Online zijn gedragsregels op zijn minst anders te noemen, maar eigenlijk vaak afwezig. Wat vinden we van deze normloosheid? Rüdiger liet zien hoeveel online groepen met nazinamen in de game Clash of Clans te vinden zijn, hoe die gesprekken verlopen en ook met welk gebrek aan online normen het spel soms gespeeld wordt. Naast dit spel zijn er vele games waarin gecommuniceerd wordt, via tekst, maar ook via spraak, zoals bijvoorbeeld het populaire schietspel Fortnite: 100 spelers strijden tot de laatste overblijft. Een spel waarin de norm lijkt dat online alles geoorloofd is om maar die laatste te zijn.

STERKTE-ZWAKTEANALYSE

De conferentie resulteerde op grond van de vele voorbeelden in een sterkte-zwakteanalyse, waarbij kansen en bedreigingen werden benoemd voor een effectievere aanpak voor veiligheidspartijen die trollen willen bestrijden.

Figuur 1> SWOT-analyse van aanpak trollen door veiligheidsdiensten

SWOT-ANALYSE AANPAK TROLLEN DOOR VEILIGHEIDSDIENSTEN	
STERKTES	ZWAKTEN
S1 Handlingsperspectieven kenbaar maken en succesvolle aanpak delen S2 Slachtoffers centraal plaatsen en ervaringen delen, in de impact op slachtoffers verplaatsen S3 Verder ontwikkelen van best practices in veiligheidswerk waarin slachtoffers centraal staan S4 Bestaande relaties tussen doelgroepen (zoals jongeren) en veiligheidsinstanties versterken S5 Juridische kaders verder vormgeven ten behoeve van effectieve aanpak	Z1 Gebrek aan bewustwording omtrent belang van sociale media en gaming en weinig kennis Z2 Slechte voorbeelden van gedrag m.b.t. sociale media en trollen binnen veiligheidsdiensten Z3 Gebrek aan effectieve weegkaders om prioriteiten te stellen in trollenzaken Z4 Moeizame vervolgingsbeslissingen ondermijnen vertrouwen in aanpak. 'Eenzame gek' wordt vaker aangepakt dan georganiseerde groepen Z5 Lange en moeizame vervolgingsprocessen, gebrek aan 'ZSM-aanpak'
KANSEN	BEDREIGINGEN
K1 Nieuwe technieken om trollen uit anonimiteit te halen (deanonimisering) K2 Geautomatiseerde systemen die ongewenst gedrag herkennen (content- en accountmoderatie) K3 NGO's die slachtoffers en minder zelfredzame personen bereiken en stimuleren iets te doen K4 Platforms voor sociale media en gaming meer verbinden met overheidsinstanties, zoals de internationale gedragscode voor illegale haatuitingen op internet van de EU commissie (2016)	B1 Juridische kaders staan nog in kinderschoenen B2 Gebrek aan verantwoordelijkheid bij partijen rondom sociale media en gaming B3 Weerwoord kan olie op het vuur gooien; 'Don't feed the trolls' en toename van eigenrichting op het internet B4 Slachtoffers die weigeren mee te werken aan vervolging van daders ondermijnen online veiligheid en leefbaarheid B5 Trollen groeit: generatiekloof en trage tech-adoptie in veiligheidsdiensten maakt kloof groter B6 Trollen uit de anonimiteit halen is zeer moeilijk B7 'Ontremmingseffect', waardoor online andere (ontremde) normen en waarden gelden B8 Gebrek aan internationale samenwerking en prioriteiten in aanpak van trollen

TROLLEN BEDREIGEN DE RECHTSORDE

Trollen vindt niet alleen plaats op individueel niveau.

Uit [onderzoek](#) van NRC bleek dat Russische internettrollen op Twitter probeerden anti-islamsentimenten in Nederland aan te wakkeren. Dit gebeurde vanuit een '[trollenfabriek](#)' in [Sint-Petersburg](#), het beruchte Internet Research Agency (IRA). Dat beheerde zeker 3841 trol-accounts. Sommige tweets zijn door de nepaccounts verstuurd op de dag van de aanslagen in Brussel, 22 maart 2016, andere ten tijde van de Nederlandse verkiezingen.

Je kunt nu al een bot maken die praat als president Trump

Volgens Facebook is 2 tot 3 procent van hun accounts vals, maar experts schatten dat het eerder 10 procent is. Ook Twitter heeft last van miljoenen spookaccounts. Bij de grote zomerschoonmaak verwijderde Twitter [70 miljoen nepaccounts](#). Facebook blokkeerde zelfs [1.3 miljard accounts](#).

INTERNETTECHNOLOGIE

Twitter-directeur Jack Dorsey beklagde zich er onlangs over hoe fictieve accounts zijn berichtendienst misbruiken. Hij wil weer een gezond debat met echte mensen, maar heeft geen idee hoe de klok terug te draaien. Internettechnologie ontwikkelt zich intussen verder. Volgens sommige trendwatchers is 2018 het jaar van de '[social bot](#)' (online robotaccounts die communiceren). Veel omarmen dat in hun klantgerichte dienstverlening. Nu al kan een computer kunstmatig aangemaakte portretfoto's genereren en voorzien van namen. Accounts aangedreven door kunstmatige intelligentie worden dan een *chatbot*. Je kunt nu al een bot maken die praat als president Trump en nieuwe 'Trump-uitspraken' doet op basis van oude uitspraken.

Onder kinderen zijn social bots enorm populair. Opeens kunnen ze chatten met Minions, die precies praten zoals in de film. Minion-bots bieden ook producten aan: 'Heb je al aan papa en mama verteld dat een nieuwe Minion-film uitkomt?' Chinese kinderen vertrouwen hun diepste geheimen toe aan dit soort [bots](#), terwijl kinderen vaak erg beïnvloedbaar zijn. Papa en mama weten ondertussen niet welke informatie hun kinderen delen en welke informatie gedeeld wordt.

Nederlandse trollen hadden in 2012 al een aantal keren flinke impact

Nederlandse trollen hadden in 2012 al een aantal keren flinke impact. Een jongen twitterde bijvoorbeeld tijdens Project X dat een meisje was overleden. Hij deed dit voor de lol en noemde zich 'hoax creator', maar dat wisten hulpdiensten, media en maatschappij niet, met alle gevolgen van dien. De jongen werd niet vervolgd, omdat wat hij deed dan wel niet ethisch, maar ook niet 'zomaar' strafbaar was.

OFFLINE EN ONLINE MAATSCHAPPIJ

We stevenen af op een kantelpunt waarin het onderscheid tussen echt of nep steeds lastiger wordt. De jeugd praat graag online met Justin Bieber, ook al weten ze ergens wel dat hij niet echt is. Vele partijen spelen, goed en kwaad, in op deze ontwikkelingen. Alleen met bewustzijn en verantwoordelijkheid, ook onder technologieaanbieders en overheden, kunnen online leefbaarheid en veiligheid in de 21ste eeuw geborgd worden. Samenwerking, juist internationaal, moet hierom volwassener worden. Passende wet- en regelgeving moet die samenwerking ondersteunen.

Door gebrekkige kennis van sociale media en gamen wordt de kloof tussen de offline en online maatschappij alleen maar verder vergroot, zolang hier niks mee gedaan wordt. Die kloof kan kleiner worden door relaties te

versterken tussen specifieke groepen en veiligheidsinstanties. Wat staan we toe en waar ligt de grens? Er bestaan al genoeg voorbeelden van bedreigingen die de leefbaarheid verminderen en die de grens al ver gepasseerd zijn. Gelukkig bestaan ook genoeg kansen. Als we deze samen aangrijpen hoeft het niet van kwaad tot nog erger te gaan. <<

Europees project

Het onderzoeksproject MEDI@4SEC brengt de kansen en bedreigingen in kaart die nieuwe communicatietechnologieën teweegbrengen voor de veiligheid en veiligheidsinstanties. Dit artikel is het derde van een serie artikelen over specifieke thema's binnen dit onderwerp als: [Do It Yourself \(DIY\) Policing](#); Rellen en massabijeenkomsten; Dagelijks politiewerk; Dark Web; Trolling en; Innovatieve marktoplossingen. Lees ook het inleidende [artikel](#) in Secondant over de kansen van nieuwe communicatietechnieken voor justitie en politie. Meer informatie over MEDI@4SEC is te vinden op de [projectwebsite](#). Hier zijn ook de volledige onderzoeksrapporten te downloaden zodra deze openbaar zijn.

Arnout de Vries is werkzaam bij TNO als senior scientist internet security. Hij is bereikbaar voor vragen en discussie via e-mail: [arnout.devries\(at\)tno.nl](mailto:arnout.devries(at)tno.nl).