

De digitale stad vergt nieuwe vorm van oorlogsvoering

27 november 2025



Niet alleen om privacy bezorgde burgers en overheden houden zich bezig met de digitalisering van de stad. Ook de militairen zien nieuwe kansen en uitdagingen. Een oriëntatie van de militaire adviseurs van het elitaire Amerikaanse militaire opleidingsinstituut Westpoint* kan ook heel leerzaam zijn voor burgers die zich willen voorbereiden op de stad waar privacy een illusie is geworden.

Foto: [Claudio Schwarz](#) on [Unsplash](#)

All-digital

Digitalisering is in een stroomversnelling gekomen. Onze communicatie met elkaar, met bedrijven en overheden verloopt nu grotendeels digitaal. Vermaak en informatie komt ook in overgrote mate via online communicatie tot ons. Onder kritische burgers is bezorgdheid ontstaan over de privacy bij gebruik van al die online activiteiten. Met speciale browsers, VPN en wijs gebruik van het achterlaten van eigen gegevens, proberen zij hun 'digitale footprint' zo klein mogelijk te houden. Anderen kiezen voor een 'ouderwetse' telefoon, zonder internet en/of laten de smartversie thuis in de lade.

Die 'strategie' om zoveel mogelijk de privacy beschermen, wordt echter steeds minder effectief. In hoog tempo wordt de openbare ruimte ingericht met alle mogelijke nu beschikbare vormen van digitale volgtechnieken. De smartphone thuislaten zal niet meer helpen om digitaal onopgemerkt te blijven.

Het Amerikaanse elitaire militaire opleidingscentrum Westpoint plaatste onlangs een [analyse op haar website](#). Onder de kop: 'Urban Warfare in the age of smart cities' beschrijft zij de kansen en uitdagingen voor oorlogsvoering in gedigitaliseerde steden. Daarbij spreekt men van '[pervasieve surveillance](#)', dat zoveel betekent als de integratie van computers en het gebruik ervan in de dagelijkse omgeving, in tegenstelling tot de computer als een apart object. Hierbij wordt de computer op elke denkbare plek ingezet en in alle omstandigheden waarin de gebruiker zich bevindt. In het Engels spreekt men van 'ubiquitous computing' of 'ubicomp'.

In de afgelopen twee decennia zijn wereldwijd stedelijke gebieden digitale technologieën geïntegreerd in bijna elk aspect van het dagelijks leven, van energienetten en transportsystemen zoals in het openbaar vervoer tot openbaar bestuur en maatschappelijke interactie. Al in 2023 waren er wereldwijd meer dan duizend actieve smart city-projecten in ontwikkeling, groeiend met ongeveer honderd nieuwe 'slimme' steden per jaar. Niet in de laatste plaats vindt digitalisering plaats op het terrein van bewaking en surveillance van de publieke ruimte.

In het Westpoint-artikel constateert de auteur dat de Amerikaanse defensie nog te weinig kennis draagt van deze technieken in relatie tot 'urban warfare', oorlogshandelingen in een stedelijke omgeving: *"Terwijl steden evolueren naar*

digitale terreinen, vormt het ontbreken van militair begrip en bereidheid om zich aan deze nieuwe stedelijke realiteit aan te passen blinde vlekken.”

Steden meer conflictgebied

Volgens Westpoint zullen stedelijke conflicten [vaker voorkomen](#). En ook in toenemende mate in gedigitaliseerde steden. Men verwacht dat vooral in steden in het globale zuiden, waarbij digitalisering en snelle groei van de bevolking samenvallen, zich dergelijke conflicten zullen voordoen. In veel gevallen zijn steden in niet-Westerse landen verder in deze ontwikkeling dan de ‘ontwikkelde’ landen. Mondiaal kun je stellen dat deze ontwikkelingen de wereldwijde trend onderstrepen om stedelijke agglomeraties te herconfigureren in datagedreven ecosystemen.

Waar steden vooral een configuratie waren van gebouwen, straten en open ruimten is er nu een onzichtbare laag overheen gekomen: de digitale stad. De oriëntatie op enerzijds grote open ruimten waarbij privacy geen optie is, en anderzijds meer gesloten structuren als steegjes en hofjes, is in een gedigitaliseerde stad niet meer van nut. Met duizenden camera’s en andere vormen van detectie, is privacy niet meer zonder meer veilig te stellen, als dat überhaupt nog zou kunnen.

Veel steden zijn vandaag de dag al bedekt door talrijke, onzichtbare, bewakingssystemen. Westpoint: *“Schattingen suggereren dat Moskou tussen de 230.000 en 250.000 CCTV-camera’s telt, waaronder ongeveer 217.000 gekoppeld aan een AI-aangedreven systeem dat gezichtsherkenning mogelijk maakt. In Rusland bestaan naar schatting eenentwintig miljoen camera’s.*

In Azië is de schaal nog groter. China alleen al heeft naar verluidt tot zeventienhonderd miljoen CCTV-camera’s, met Beijing met 11,2 miljoen – ongeveer één voor elke twee van zijn inwoners. Het enorme bewakingsapparaat van China combineert CCTV, gezichtsherkenning, drones, microfoonarrays, ‘slimme’ lantaarnpalen en mobiele AI-platforms in de hele stad. Samen transformeren ze stedelijke ruimtes in bewakingsomgevingen die het tijdsvenster comprimeren voor manoeuvreren, verhulling, misleiding en – misschien wel het meest kritisch – besluitvorming.”

Conflicten in steden zullen met deze ontwikkelingen met andere middelen worden

bestreden dan louter met patrouillerende mannen in legergroene pakken.

Alles met alles verbonden

De stad produceert onmetelijke hoeveelheden data. Niet alleen van camera's en sensoren, ook de via Wifi en Blue Tooth met het internet verbonden apparatuur (denk aan alles waar 'smart' voor staat) leidt tot een stortvloed aan data. Ook de toepassing van RIFD (radiofrequentie-identificatie) bijvoorbeeld in winkels, is een andere bron van data.

Om dat allemaal te verzenden, op te slaan en te verwerken zijn niet alleen supersnelle verbindingen nodig, maar ook AI (kunstmatige intelligentie) is onmisbaar om iets met deze datastroom te kunnen. Timing is in het geval van surveillance en bewaking cruciaal. Een signaal van een cluster van bewegingssensoren, enkele CCTV-waarnemingen van onbekende gezichten en een piek in het lokale telefoonverkeer kunnen in een samenhangend patroon worden waargenomen. Hieruit kan het systeem autonoom de aanwezigheid van een ongeautoriseerde groep signaleren die door een specifieke sector beweegt en onmiddellijk de bewaking waarschuwt. In geval van oorlogshandelingen kan een dergelijke signalering een zaak van leven en dood zijn.

Geen hekken of muren

Fysieke poortjes en bewakers om 'opvallende' gedragingen te signaleren en tegen te houden zijn of worden vervangen door AI-gebaseerde video-analyse, radiofrequentie patroon-of-life monitoring en anomalie detectie-algoritmen. De combinatie van data kan onmiddellijke een alarm geven – bijvoorbeeld wanneer individu tegen de stroom ingaat. Het gaat daarbij om het veel toegepaste principe bij het programmeren van algoritmes waarbij een 'normale' situatie wordt verondersteld, en alles wat daarvan afwijkt als een 'anomalie' wordt beschouwd.

Volgens Westpoint creëren 'slimme' verlichting en geïntegreerde cameranetwerken virtuele perimeters (digitaal afgebakende gebieden of zones). Deze adaptieve, gegevensgestuurde beveiligingszones kunnen hun bewakings- en reactieprotocollen dynamisch aanpassen aan de realtime dreigingsbeoordelingen. Deze technologieën vervangen fysieke toegangscontrole en andere vormen van fysieke sturing van menselijke bewegingen zoals door muren of

veiligheidshekken. Een ruimte kan er dan voor het oog vrij en onbewaakt uitzien, maar het tegendeel is dan waar.

Een militaire tactiek is bijvoorbeeld het preventief onklaar maken van de stroomtoevoer waardoor een gebouw onverlicht is en insluipen ongezien kan plaatsvinden. Maar volgens Westpoint kan het uitvallen van elektriciteit in een gedigitaliseerde stad juist argwaan oproepen en een alarm uitlokken. Westpoint: *“Als ze (militairen, red.) radiogebruik vermijden en zich stil verplaatsen (elektromagnetische en akoestische discipline), maar daarbij een verkeerscamera of een bewegingsdetector activeren, kan de missie nog steeds mislukken.”*

Zonder smartphone de stad in? Verdacht!

Gedragingen als tegen een menigte in lopen of het besturen van een ongemarkeerd voertuig, kan nu door AI-analyse als ‘onregelmatig patroon’ een waarschuwing uitlokken. Een groep mensen dat helemaal geen mobiele telefoons bij zich heeft, in een van mobiele telefoons verzadigde stad, kan zelfs een rode vlag zijn. In sommige autoritaire slimme steden waar de bevolking bio-gelabeld en gevolgd wordt, kunnen buitenstaanders onmiddellijk worden onderscheiden van de massa.

Machine learning- en trajectmodellen voorspellen waar en wanneer verdachte activiteit waarschijnlijk is, waardoor beveiligingspersoneel of politie (in geval van Westpoint, militairen) zich alvast kunnen posteren of gebieden sluiten voordat een event (demonstratie, conflict of geweld) begint. Deze technieken maakt de stad grotendeels transparent zonder *places-to-hide*. Vanwege lokale gebruiken, wetten en financiële mogelijkheden zal de configuratie per stad verschillen. Het volledig uniformeren en koppelen van alle dergelijke systemen zal dan ook nog lang op zich wachten, zo verwacht Westpoint.

Verdenking op basis van algoritmen

“In de afgelopen jaren hebben wetshandhavingsinstanties een baanbrekende aanpak van misdaadpreventie en -voorspelling omarmd. Voorspellend politiewerk, een datagestuurde methode, is een krachtig hulpmiddel om de openbare veiligheid te verbeteren en de toewijzing van middelen te optimaliseren. Door historische misdaadgegevens te analyseren en patronen te identificeren, stelt

deze innovatieve technologie wetshandhaving in staat om op potentiële criminele activiteiten te anticiperen en middelen effectiever in te zetten.”

[Dit schrijft](#) het in Dubai (de stad met een wijk met de naam Internet City) gevestigde beveiligingsbedrijf IGNESA.

Voorspellend politiewerk is gebaseerd op geavanceerde analytische technieken van de datastroom die een stad met alle ‘slimme’ apparaten aanlevert. Doel is om criminele activiteiten door voorspelling te voorkomen. Deze werkwijze combineert gegevensanalyse, criminologische theorieën en technologische hulpmiddelen teneinde de handhavingsstrategieën te verbeteren. Hierbij richt zich de methode op geografie en omgevingsfactoren in plaats van specifieke criminaliteitsgebeurtenissen.

Volgens het bedrijf kan het systeem geweldsmisdrijven, terroristische incidenten, verkeersincidenten, drugscriminaliteit en georganiseerde misdaad voorspellen. Zelfs kindermishandeling. Met dat laatste worden misdrijven achter de voordeur bedoeld. We weten inmiddels dat bij elke surveillancewetgeving, online en offline, kindermisbruik wordt opgevoerd als legitimatie voor massa-surveillance.

Via de zogenaamde ‘Social Network Analysis (SNA)’ worden netwerken van individuen en groepen mensen geanalyseerd. Het systeem presenteert de gegevens op een visuele manier die *“snel en gemakkelijk te begrijpen is voor minimaal opgeleid personeel.”* Dat laatste sluit dus uit dat ervaren personeel zelf een oordeel velt over de aangeleverde analyse. De visualisatie van de netwerken, bekend als een sociogram, is gebaseerd op complexe berekeningen afgeleid van de grafiektheorie.

Wat er mis kan gaan weten we inmiddels bij het Toeslagenschandaal waarvan de overheid bij monde van toen nog premier Mark Rutte verwacht dat de toedracht nog jaren onduidelijk zal blijven. De rol van het datasysteem van Palantir is daarbij vrijwel zeker.

[Hoe Palantir in ieders leven sluipt](#)

Concluderend

De snelle ontwikkeling van de digitale transparante stad mag voor ordehandhavers een positieve ontwikkeling zijn, het berooft de burger wel van een fundamenteel recht: het recht op privacy. Enkelen zullen betogen dat in de publieke ruimte er geen recht op privacy kan bestaan. Daar is wat voor te zeggen. De keuze om de straat op te gaan is een eigen beslissing.

Toch is er verschil tussen sociale controle door omstanders en een rondlopende agent of BOA, en een 24/7, 100% ruimtedekkend systeem van digitale ogen en sensoren. Ook wie niets crimineels van plan is, voelt zich toch bespiedt en past gedrag aan aan wat vermoedelijk door 'het oog' wordt verlangd. Dan kan zijn dat het thuislaten van je smartphone al tot verdenking kan leiden, zoals bovenstaand is te lezen. Een controle door een menselijk oog zal dat niet waarnemen, waarmee de telefoon dus thuis kan blijven (om welke reden dan ook).

Een algoritme bepaalt of gedragingen 'afwijkend' en daarmee 'verdacht' zijn. Iemand die in een winkelstraat 'te lang' stilstaat, wijkt af van de voorbysnellende passanten. In het Verenigd Koninkrijk kunnen in bepaalde gebieden uit geïnstalleerde luidsprekers gerichte aanwijzingen volgen, van een echte persoon of vanuit AI.

Vooraf de combinatie met het dubieuze Palantir (zie artikel boven) is reden voor zorg. Een bedrijf met de ethiek van een struikrover dat over uw en mijn data gaat, daar zijn eigen mix van maakt en bepaalt of u een keer een huisbezoek van de wijkagent moet krijgen. Er zijn regimens uit het verleden die hiervan hebben gedroomd.

Sommigen spreken van een tijd van dehumanisering. Deze vorm van bespieden van publiek, in de publieke ruimte, online of achter de voordeur, roept associaties op met duistere regimens uit het verleden en autoritaire regimens uit het heden. Als deze vorm van maatschappelijke sturing door middel van ontmenselijke surveillance in combinatie met de propagandistische brainwash doorzet, gaat er meer verloren dan gebruiken en cultuur. Dan verliest de samenleving haar menselijkheid.

*The articles and other content which appear on the Modern War Institute website are unofficial expressions of opinion. The views expressed are those of

the authors, and do not reflect the official position of the United States Military Academy, Department of the Army, or Department of Defense.