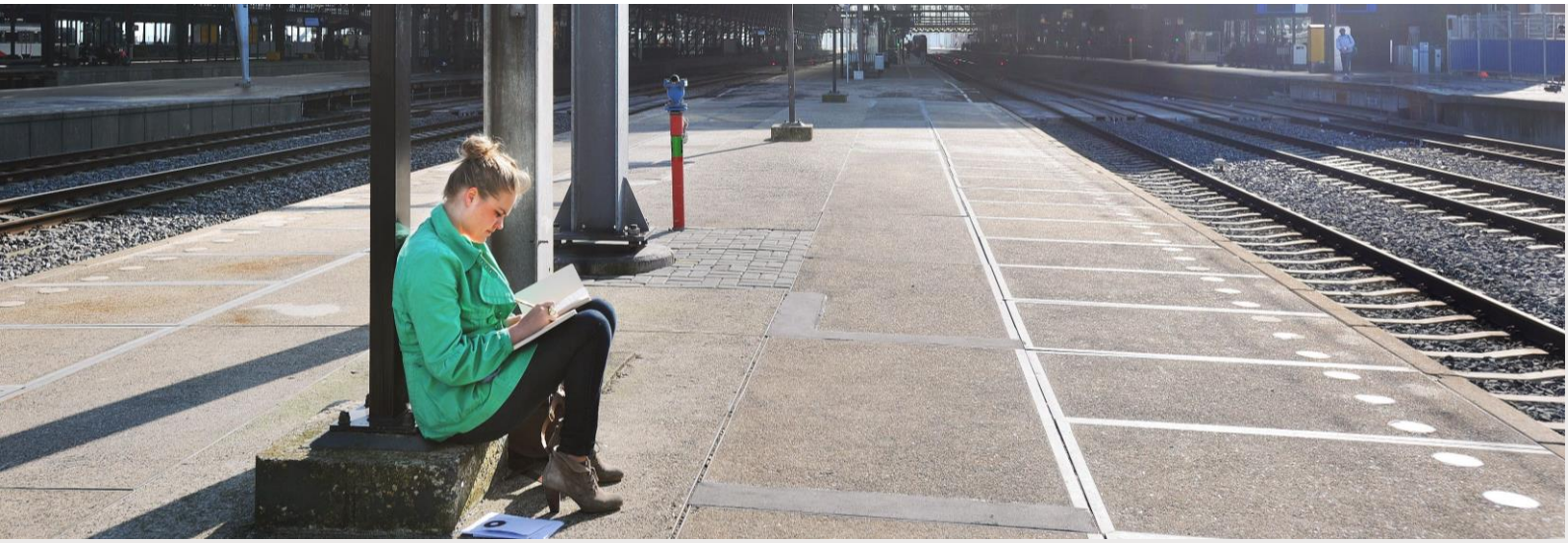
Rathenau Instituut

5 acties voor cybervrede



Bericht aan het Parlement

Steeds meer landen kunnen cyberaanvallen uitvoeren die grote schade aanrichten aan bedrijven, overheidsinstellingen en burgers. Vrijwel alle landen gebruiken deze cyberwapens ook. Ze bespioneren elkaar en proberen in elkaars digitale systemen te infiltreren; sommige staten saboteren de digitale systemen van civiele instellingen, zoals ziekenhuizen en energiecentrales, of verspreiden desinformatie.

Door middel van informatietechnologie ontstaat zo een nieuw conflict, waarbij juist de burger in het kruisvuur staat. In dit bericht formuleren we daarom vijf acties om het internationale informatieconflict te de-escaleren. Deze acties zijn gebaseerd op ons rapport Cyberspace zonder conflict.

Er vindt een internationaal informatieconflict plaats

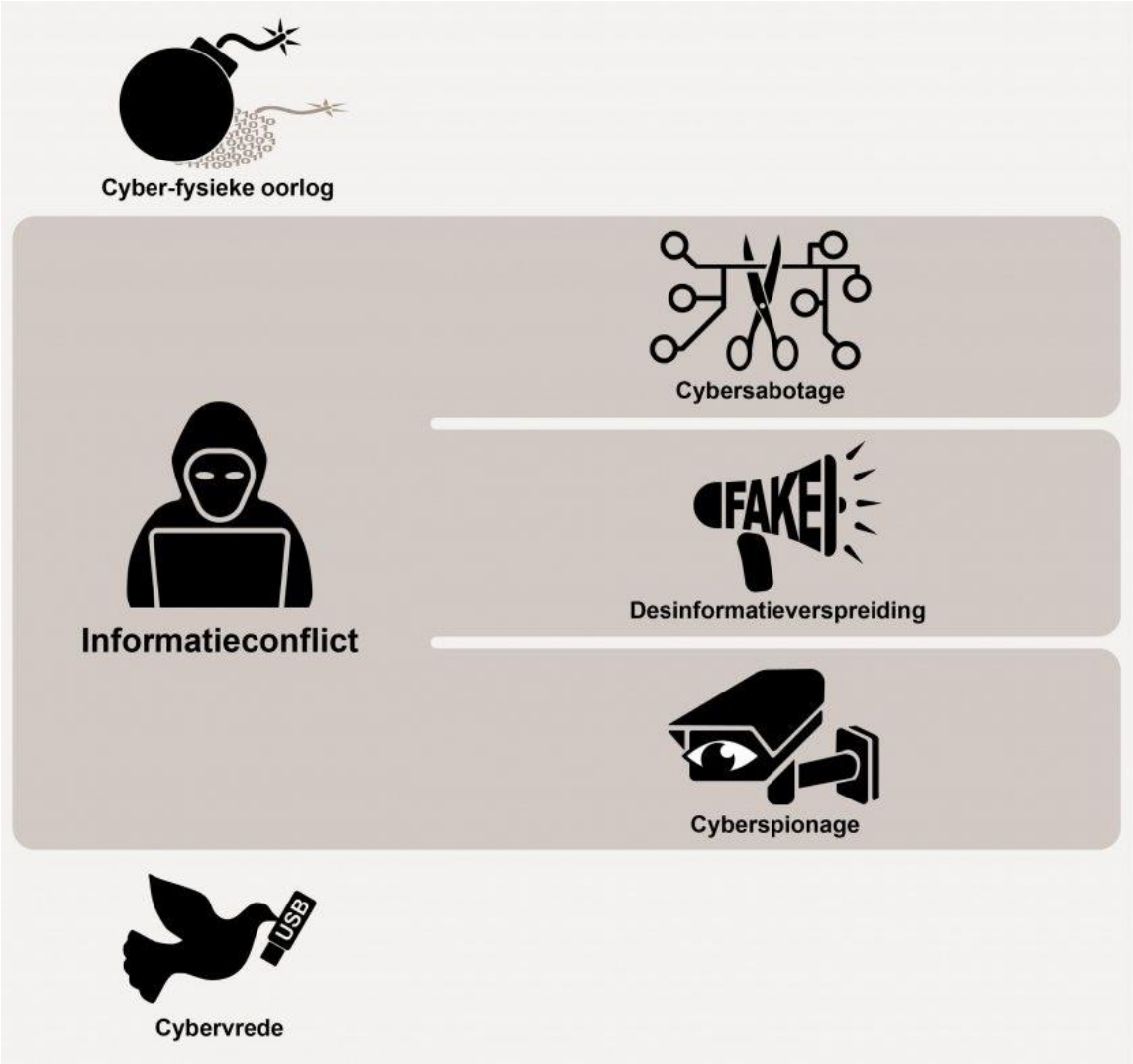
De digitalisering van de samenleving leidt tot nieuwe kwetsbaarheden. Door middel van cyberspionage kunnen gevoelige geheimen gestolen worden; cybersabotage kan de dienstverlening van een ziekenhuis of een bank verstoren en de online verspreiding van desinformatie ondermijnt een op waarheidsvinding gebaseerd democratisch debat. Bij elkaar creëren deze cyberaanvallen een nieuw conflict, dat het Rathenau Instituut omschrijft als een informatieconflict.

De opkomst van het informatieconflict creëert ernstige veiligheidsrisico's, juist voor essentiële civiele voorzieningen en publieke goederen. Zo kunnen kwaadwillende actoren de persoonsgegevens van burgers gebruiken om de desinformatie die ze verspreiden precies op hen te richten. Cambridge Analytica maakte bijvoorbeeld in 2016 gebruik van 87 miljoen dataprofielen van Facebook en kon vervolgens zicht krijgen op groepen gebruikers met bepaalde psychologische kenmerken. Op basis van die profielen heeft het bedrijf geprobeerd het stemgedrag van Facebookgebruikers gericht te beïnvloeden.

Steeds meer landen voeren cyberaanvallen uit, en maken daarmee deel uit van het informatieconflict. Hoewel vrijwel alle landen cyberspionage uitvoeren, kenmerken sommige staten zich door een offensieve strategie. Zo voert China veel economische spionage uit en verspreidt Rusland veelvuldig desinformatie. Ook de Verenigde Staten willen zodanig dominant aanwezig zijn in cyberspace, dat zij de digitale systemen van aanvallers preventief kunnen saboteren.

Het informatieconflict kent vooralsnog alleen zeer algemene bindende regels. Dat komt deels omdat cyberaanvallen zelden zodanig schadelijk zijn dat ze de grens van een gewapende aanval overschrijden, en daarmee het internationaal humanitair recht activeren. Het informatieconflict vindt plaats tussen een staat van oorlog en vrede in. Of preciezer: tussen aan de ene kant een staat van cyber-fysieke oorlogsvoering, waarin de militaire troepen van staten elkaar met een gedigitaliseerd arsenaal bevechten en zware fysieke schade berokkenen, en aan de andere kant een staat van cybervrede, waarin landen elkaar niet schaden met cyberaanvallen (zie figuur 1).

In dit schemergebied zijn vooralsnog geen bindende internationale regels die specifiek zijn toegespitst op het informatieconflict. Dit gebrek aan concrete, bindende regels, en het gebrek aan internationale samenwerking en coördinatie dat daarmee verbonden is, vergroten het risico dat cyberaanvallen in ernst en in frequentie toenemen.



Figuur 1 Het informatieconflict

Vijf acties voor de-escalatie

Het is daarom hard nodig om het informatieconflict te de-escaleren. In dit bericht hebben we daarvoor vijf acties geformuleerd.

1. **Blijf samenwerken om de internationale cybersecurity te verhogen**
   Internationaal zijn er belangrijke initiatieven ontplooid om de veiligheid van cyberspace te verbeteren, zoals de IMPACT-coalitie, het Europese netwerk van Cyber Emergency Incident Response Teams en de NAVO-cyberoefeningen. Nederland heeft zich hierbij aangesloten. Deze samenwerkingen blijven van groot belang. Cyberaanvallen kunnen bijvoorbeeld onschadelijk worden gemaakt, als de software-updates die beveiligingslekken dichten snel tussen verschillende landen en bedrijven worden gedeeld.

2. Maak heldere internationale afspraken voor de-escalatie op het gebied van cybersabotage, desinformatie en cyberspionage

Hoewel Nederland en andere landen belangrijke stappen hebben gezet om internationale regels voor cyberaanvallen op te stellen, zoals het publiceren van het Tallinn Handboek en de Paris call for Trust and Security in Cyberspace, zijn de regels met een bindend karakter algemeen van aard.

Het is daarom belangrijk bindende afspraken te maken die zijn toegespitst op het informatieconflict. Daarbij kan worden gedacht aan een cyberverdrag. De bekendmaking dat Nederland vaker openlijk cyberaanvallen aan daders zal attribueren draagt ook bij aan de normontwikkeling. Daarnaast is het goed dat Nederland investeert in een netwerk van cyberdiplomaten. Maar meer beleidsontwikkeling en diplomatieke inzet is nodig om te komen tot breed gedeelde en concreet nageleefde afspraken.

3. Zorg dat het cyberarsenaal verantwoord wordt beheerd

Het is belangrijk verdere verspreiding (proliferatie) van cyberwapens tegen te gaan. Dit vraagt om een internationale coördinatie van de aanschaf van cyberwapens, en om een effectieve samenwerking met technologiebedrijven die kwetsbaarheden in hun producten kunnen verhelpen.

Aan de ene kant vereist het tegengaan van wapenproliferatie een bepaalde mate van openheid tussen bondgenoten. Het is riskant als een land eigenstandig cyberwapens ontwikkelt en geheim houdt. Die wapens kunnen namelijk gestolen worden en tegen bondgenoten ingezet. Zo rapporteerde securitybedrijf Symantec onlangs dat China cyberwapens van de V.S. wist te stelen, en die vervolgens onder andere op Europese doelen heeft gericht.

Aan de andere kant is het belangrijk de kennis over gevaarlijke cybertechnologie af te schermen, en ervoor te zorgen dat bedrijven niet zomaar aan gevaarlijke regimes cyberwapens kunnen verkopen. En het is belangrijk dat buitenlandse studenten en onderzoekers niet te gemakkelijk toegang hebben tot gevaarlijke cybertechnologie.

Ook op dit gebied heeft Nederland stappen gezet om de wapenproliferatie tegen te gaan, bijvoorbeeld wat betreft het invoeren van exportvergunningen en het uitbreiden van toezicht op studenten en onderzoekers uit risicolanden. Bovendien wisselen de Nederlandse inlichtingendiensten informatie uit met bondgenoten en bedrijven. Maar landen voeren nog steeds hun eigen wapenbeheer; effectieve internationale coördinatie zal daarom een voortdurende diplomatieke inspanning vragen.

4. Bescherm de onafhankelijkheid van technologiebedrijven

Technologiebedrijven vervullen een cruciale rol in de beveiliging van de digitale omgeving. Zij dichten de gaten in hun software en kunnen robuuste digitale toepassingen op de markt brengen. Het is belangrijk om bedrijven te ondersteunen om zo veilig mogelijk te opereren. Overheden nemen een risico als ze van bedrijven eisen de veiligheid van producten, zoals de gebruikte encryptie, te verzwakken. In Australië en het Verenigd Koninkrijk is wetgeving aangenomen die het mogelijk maakt bedrijven te dwingen hun digitale beveiliging te verwijderen of aan te passen, en ook in de V.S. wordt hierover gedebatteerd. Tot dusver moedigt de Nederlandse overheid het gebruik van encryptie juist aan – het verzoek van de AIVD om Whatsapp-encryptie te beperken werd in 2016 afgewezen. Tegelijk geldt in Nederland een medewerkingsplicht voor bedrijven waar zorgvuldig mee moet worden omgesprongen. Uit het jaarverslag van de Toetsingscommissie Inzet Bevoegdheden (TIB) blijkt dat dit niet altijd het geval is.

5. Investeer in debat over internationale cyberveiligheid

Het informatieconflict is bij uitstek een onderwerp voor democratisch debat: juist burgers worden geraakt door cyberaanvallen. Zij worden misleid door desinformatie, vitale voorzieningen worden gehackt en bedrijven zoals banken worden bespied. Burgers moeten weerbaar zijn. Ook is het aan hen om richting te geven aan de digitale toekomst. Het zal daarom steeds belangrijker worden om zichtbaar te maken hoe cyberaanvallen onze veiligheid aantasten.

De-escalatie van het informatieconflict vraagt daarom om een maatschappelijk en politiek debat. Dat moet gaan over grote vragen, die niet van bovenaf beantwoord kunnen worden. Over vragen als: mag een democratische rechtstaat met cyberaanvallen terugslaan? Op het gebied van de verspreiding van desinformatie geeft de Nederlandse overheid voorlichting en voert het debat. Het is belangrijk dat op alle hierboven aangegeven punten te doen.

Meer onderzoek van het Rathenau Instituut over dit onderwerp

- Cyberspace zonder conflict – Op zoek naar de-escalatie van het internationale informatieconflict
- Een nooit gelopen race – Over cyberdreiging en versterking van weerbaarheid
- Digitalisering van het nieuws – Online nieuwsgedrag, desinformatie en personalisatie in Nederland
- Just ordinary robots: Automation from love to war
