**Korte introductie t.b.v. rondetafelgesprek Tweede Kamer over Geïntegreerde Buitenland- en Veiligheidsstrategie, thema cybersecurity**

*Sico van der Meer, onderzoeker Instituut Clingendael*

Vanuit cybersecurity-perspectief juich ik de Nederlandse geïntegreerde aanpak van buitenlands- en veiligheidsbeleid toe. Nog te vaak worden de in de Geïntegreerde Buitenland- en Veiligheidsstrategie geschetste activiteiten voorkomen, verdedigen en versterken als geïsoleerde ‘eilandjes’ gezien.

Wat betreft cybersecurity ben ik van mening ik dat qua hoeveelheid de meeste dreigingen uit niet-statelijke hoek komen, met name door toedoen van cybercriminelen. De dreiging van statelijke actoren is echter de gevaarlijkste. Deze actoren kunnen grote schade toebrengen aan de Nederlandse maatschappij. Alleen staten en door staten gesteunde groeperingen hebben de financiële en personele slagkracht om werkelijk grootschalige cyberoperaties uit te voeren. Waar niet-statelijke actoren vooral economische schade en ongemak veroorzaken, kunnen staten aanzienlijker schade aanrichten door cyberoperaties gericht op bijvoorbeeld politieke, militaire en economische spionage, manipulatie van publieke opinie (inclusief ondermijnen van vertrouwen in instituties) en het aantasten van vitale infrastructuur.

In internationale context zien we momenteel een cyberwapenwedloop plaatsvinden waarin veel landen flink investeren in defensieve en offensieve cybercapaciteiten. Deze investeringen richten zich vooral op (actieve en passieve) verdediging. Helaas is er wereldwijd naar mijn mening te weinig inzet op het voorkomen van cyberaanvallen en het versterken van internationale samenwerking. Het cyberdomein is vanuit internationaal-politiek perspectief nog teveel het ‘Wilde Westen’ waar het recht van de sterkste zegeviert.

Vanuit mijn optiek is juist de versterking van de internationale rechtsorde en samenwerking wat betreft cybersecurity cruciaal, zeker voor de grote meerderheid van landen die zich geen cybergrootmacht kan noemen. Omdat in het cyberdomein nauwelijks fysieke grenzen bestaan, kunnen landen zich uiteindelijk niet in hun eentje verdedigen tegen cyberdreigingen. Hoeveel je ook investeert in verdediging, cyberaanvallers zullen altijd een stap voor lopen in hun zoektocht naar zwakheden. Verdediging door afschrikking en door het preventief aanvallen van mogelijke vijanden werkt misschien op korte termijn, maar veroorzaakt op lange termijn vooral escalatie.

Helaas komt internationale samenwerking over cybersecurity nog niet goed van de grond. Het overleg hierover binnen de Verenigde Naties is vastgelopen, en ook andere fora zoals de Internationale Telecommunicatie Unie bieden weinig positief perspectief. Natuurlijk betreft het ingewikkelde materie met erg veel dimensies, maar ook heb ik het idee dat de grootmachten met hun aanzienlijke militaire cybercapaciteiten hun handen nog niet willen binden zolang ze nog een ruime voorsprong op de rest van de wereld hebben. De recente Command Vision van het US Cyber Command vind ik wat dat betreft een zorgelijke ontwikkeling; de VS claimen daarin openlijk het recht om preventief digitale netwerken van potentiële vijanden binnen te dringen en te manipuleren om zo de Amerikaanse ‘digitale superioriteit’ te heroveren. Dit soort beleid creëert een nieuwe norm in de internationale betrekkingen waarin het recht van de sterkste zou gelden.

Daarom ben ik blij dat Nederland wel nadrukkelijk inzet op cyberdiplomatie en het versterken van de internationale rechtsorde in dit domein. Een geïntegreerde benadering van de problematiek is nodig om ook op langere termijn te kunnen blijven profiteren van de grote voordelen die het cyberdomein de wereld biedt.