**Hoofdvraag: Welke concrete stappen moeten er gezet worden om de cyberveiligheid van mensen, bedrijven en overheden te vergroten?**

De problemen rondom cyberveiligheid zijn niet eenvoudig op te lossen. Vrijwel alle cyberveiligheid problemen vereisen discipline, samenwerking en goede coördinatie om opgelost te worden. Daarnaast zijn de “grenzen” tussen landen in de cyberwereld niet of nauwelijks aanwezig. Iedere oplossing die wij vanuit Nederland in willen zetten zal ook breder binnen de Europese of zelfs in wereldwijde kringen moeten worden gedragen. In het algemeen geldt dat op basis van risico-inschattingen stapsgewijs de cyberveiligheid moet worden verhoogd. Er zal altijd een bepaald risico aanwezig blijven, dus er moeten prioriteiten worden gesteld. Op hoofdlijnen, moeten naar mijn inzicht, de volgende concrete stappen worden genomen:

* Internationale samenwerking vereenvoudigen en stimuleren richting cybercriminaliteit en cyberwarfare.
* Het financieel aantrekkelijk maken voor bedrijven om een hoge mate van cyberveiligheid te hebben.
* Het weren van zwak beveiligde apparatuur en dienstverleners op de Nederlandse markt.
* Verantwoordelijkheid van bedrijven (zowel in de vitale sector als daar buiten) eisen en dit ook handhaven door het opleggen van boetes wanneer er geen verantwoordelijkheid wordt genomen.
* Het aanmoedigen van ethisch hacken middels bug-bounty programma’s, officiële erkenning e.d.
* De individuele burger trainen om zichzelf te “verdedigen” in de digitale wereld.

**Deelvraag 1: Welke stappen moet de overheid nemen op het gebied van wetgeving, certificering, standaarden en beleid, en voor het beveiligen van de vitale infrastructuur?**

De overheid moet op gebied van cyberveiligheid een faciliterende, beschermende en controlerende rol spelen. Allereerst moet er gezorgd worden voor een nauwe internationale samenwerking om de pakkans van cybercriminelen te vergroten en cybercriminaliteit te ontmoedigen. Daarnaast moet er uit oogpunt van de veiligheid van de Nederlandse maatschappij actief gecontroleerd worden op cyberveiligheid.

Cyberwarfare en cyber terrorisme begint een steeds groter risico te worden in onze maatschappij en wij moeten ons hier, in alle redelijkheid, tegen kunnen verdedigen. Waar naties onderling altijd een afweging moeten maken rondom het inzetten van cyberwapens, het valt immers ook in handen van de tegenstander, geldt dit voor extremisten niet. Het cyberwapen valt in handen van de tegenstander en kan niet tegen de extremisten partij worden ingezet. Denk bijvoorbeeld aan een aanval op de waterzuivering. Ook zien we dat cyberaanvallen die niet gericht zijn op Nederland (bijvoorbeeld Petya) nu al extreme economische schade veroorzaken. Dit is simpelweg “nevenschade”. Een gerichte aanval kan ook levens kosten of een maatschappij ontwrichtende situatie veroorzaken. We moeten nu op defensief vlak actie ondernemen.

Er moet een controlerende dienst worden gecreëerd die het recht heeft om steekproefsgewijs te controleren en boetes uit te delen aan bedrijven en overheidsinstanties die structureel onveilig zijn op cybersecurity vlak. Op deze manier zijn er financiële consequenties voor bedrijven die structureel onveilig zijn, voordat er daadwerkelijk iets “mis” gaat.

Ook zou er naast de huidige veiligheidscertificeringen zoals brandveiligheid, spanningsveiligheid en dergelijke, gekeken moeten worden naar de cyberveiligheid van apparaten in de vitale infrastructuur. Daarmee bedoel ik het zoeken naar cyber kwetsbaarheden in het algemeen, evenals het proberen middels cyberaanvallen fysieke schade te veroorzaken aan of met het apparaat.

Voor overige apparatuur zoals IoT-devices, zou een optionele certificering moeten komen die zich richt op de basale cyberveiligheid. Denk aan het gebruik van encryptie, sterke authenticatie mechanismes, mogelijkheid tot ‘responsible disclosure’ enzovoort. Nederlandse bedrijven die aantoonbaar apparatuur met een dergelijk certificaat leveren, verkopen of gebruiken zouden kunnen worden beloond met een stukje fiscaal voordeel. Dit maakt het zowel voor consumerende als producerende bedrijven aantrekkelijk om een hoog basis cyberveiligheidsniveau te behalen en behouden. Het blijft wel mogelijk om niet gecertificeerde producten aan te bieden of te gebruiken, maar dit is simpelweg minder interessant.

Ook moet er wetgeving komen die bedrijven dwingt naar redelijkheid apparatuur te blijven ondersteunen als het gaat om security updates. Er zou bijvoorbeeld aan de hand van hoe populair een apparaat en/of bepaalde software is een minimale hoeveelheid jaren support moeten worden geleverd. Naarmate de populariteit van het apparaat afneemt kan het apparaat na verloop van tijd alsnog ‘end of life’ verklaart worden. De huidige situatie staat leveranciers en 3e partijen toe niet ondersteunde apparatuur te verkopen en dus gebruikers bloot te stellen aan een aanzienlijk cybersecurity risico.

**Deelvraag 2: Welke stappen moet het bedrijfsleven nemen? Is er bij het bedrijfsleven voldoende aandacht voor cyberveiligheid en het tegengaan van bedrijfsspionage? Wat moeten bedrijven beter doen?**

Binnen het bedrijfsleven zien wij langzaam steeds meer aandacht voor cybersecurity. Bedrijven beginnen in te zien dat een zwak cybersecurity niveau de continuïteit van het bedrijf in gevaar kan brengen. Een probleem hierbij is dat bedrijven door concurrentie een steeds kortere time-to-market hebben waardoer er geen tijd is voor beveiliging. Bovendien willen consumenten niet betalen voor beveiliging.

Veelal is het probleem niet een gebrek aan weten wat er gedaan zou moeten worden, maar een gebrek aan de benodigde specialisten, security mentaliteit/cultuur, middelen en kennis om de problemen daadwerkelijk structureel op te lossen. Door trainingen, cursussen, inhuur van specialisten et cetera kunnen bedrijven hun gehele cybersecurity awareness verhogen en de kennis om problemen aan te pakken in huis halen via medewerkers of derde partijen.

Daarnaast moeten bedrijven die technologische producten leveren hun verantwoording nemen voor het uitleveren van producten met een hoog cybersecurity niveau. Dit zou bij voorkeur ook ondersteunt dan wel bestraft moeten worden vanuit wetgeving (meer hierover bij deelvraag 1).

**Deelvraag 3: Welke rol spelen onderzoekers en (ethische) hackers bij het vergroten van de cyberveiligheid en zijn zij voldoende beschermd in hun werk?**

Goede beveiliging is niet gebaseerd op de kennis van het individu, maar op de kennis van de gemeenschap. Juist de ethische hackers dragen hier enorm aan bij. Zij proberen veelal ook non-profit instellingen, kleine bedrijven en andere bedrijven die geen groot budget voor security hebben te helpen.

Op dit moment zijn er richtlijnen rondom ‘responsible disclosure’. Deze worden nog niet gehandhaafd door wetgeving. Als een ethische hacker zich aan deze richtlijnen houdt, zou hij ook middels wetgeving moeten worden beschermd van verdere vervolging.

Veel bedrijven zien de ethische hacker als een lastpost, niet als iemand die ze probeert te helpen. De ethische hacker ziet dit meestal juist andersom en probeert bedrijven te helpen door hun security problemen aan te tonen. Doordat beloning of erkenning voor dit werk vaak uitblijft is het voor sommigen aantrekkelijker om het criminele pad op te slaan. Misdaad loont meer dan ‘responsible disclosure’. Bovendien is de pak-kans relatief klein. Door ‘responsible disclosure’ en ‘bug bounty’s’ aan te moedigen en wellicht zelfs te subsidiëren kunnen we het algemene cybersecurity-niveau verbeteren en ook technisch begaafden op het goede pad houden. Juist deze technisch begaafden kunnen in de huidige situatie een serieus gevaar vormen voor de maatschappij als ze het criminele of extremistische pad kiezen.

**Deelvraag 4: Wat zijn aangrijpingspunten voor burgers om het bewustzijn van cybercrime te vergroten, om vervolgens door middel van preventie cybercrime te voorkomen?**

We kunnen en mogen niet van iedere burger verwachten dat zij zelf volledig verantwoordelijk zijn voor hun cybersecurity. Cybersecurity is al complex voor hoogopgeleide technici en bestuurders, laat staan voor mensen die niet dagelijks met cybersecurity of IT in het algemeen worden geconfronteerd.

Waar we wel op kunnen richten, is hoe mensen op een simpele manier veilig gebruik kunnen maken van internet. Zo kan er bijvoorbeeld worden aangestuurd op veilig wachtwoord gebruik en 2 factor authenticatie, het herkennen van phishing mailtjes, het controleren van beveiligde verbindingen et cetera. Dit zou moeten gebeuren via media-campagnes met simpele reclame-spotjes en documentaires/TV programma’s die verdieping bieden in het “waarom moet ik dit dan allemaal doen?”. Het veilig gebruik maken van internet moet bij voorkeur onderdeel worden van onderwijsprogramma’s in het basis-en voortgezet onderwijs. We leren kinderen en tieners nu al veilig te zijn in de echte wereld, het wordt tijd dat we dat ook doen in de digitale wereld.

Daarnaast moeten we als maatschappij toe naar een situatie waarbij hard- en of software veilig “uit de doos” komen en gebruiksvriendelijk zijn. Zoals eerder gezegd kunnen we niet verwachten dat iedereen een technisch expert is. Hard- en software moeten standaard over een redelijke mate van cybersecurity beschikken. Er is altijd kans op misconfiguraties, veranderende omstandigheden of zero days. We moeten van bedrijven verwachten dat niet iedere willekeurige robot of hackende puber zomaar op apparatuur kan inbreken en dat deze apparatuur ook gedurende zijn normale levensduur van updates wordt voorzien. In de huidige situatie is dit veelal niet het geval. Dit heeft vervelende gevolgen voor het individu, en kan ook voor de maatschappij als geheel enorme problemen veroorzaken.