Het verspreiden van inzichten naar degenen die deze inzichten nodig hebben
In de voorgaande subparagraaf worden verschillende soorten onderzoeken naar voorvallen benoemd. De informatie die deze onderzoeken oplevert wordt in een beperkt aantal gevallen openbaar gemaakt: wanneer de organisatie daar bij uitzondering voor kiest of daartoe wordt bewogen door de toezichthouder. In de vorige subparagraaf worden als voorbeeld de universiteit van Maastricht, Universiteit/Hogeschool van Amsterdam, gemeente Lochem en gemeente Hof van Twente genoemd. Ook wordt beschreven dat de meeste onderzoeken naar voorvallen niet worden gepubliceerd, of alleen in besloten kring. Vaak is de informatie alleen begrijpelijk voor een beperkte kring van experts en lijkt het een abstracte technische gebeurtenis. Daarom is het belangrijk om bij het delen van inzichten uit cyberaanvallen, deze te demystificeren en de menselijke gevolgen ervan te benadrukken.[216]

Ook is er nog geen entiteit die informatie uit onderzoeken en meldingen verzamelt ten behoeve van wetenschappelijk en/of statistisch onderzoek. In het cyberdomein, dat een relatief nieuwe traditie heeft als het gaat om incidentenonderzoek, is behoefte aan een platform waar kennis wordt gedeeld, vastgehouden en waar organisaties op zoek kunnen naar relevante inzichten om hun informatiebeveiligingsbeleid beter te kunnen onderbouwen (*historic capture*). Overigens sluit dit aan bij de missie van het NCSC als Nationaal Cyber Security Centrum: begrijpen en duiden wat er gebeurt, het verbinden van partijen, kennis en ervaring met als doel om herhaling te voorkomen.[217]

In de huidige praktijk komen veel organisaties er niet voor uit dat ze zijn aangevallen. De onderzoeken bieden niet de verklaringen die nodig zijn om het systeem te verbeteren. Betrokken organisaties verspreiden lessen uit voorvallen meestal niet buiten de eigen organisatie of gemeenschap.

4.5 Beleid en internationale context

Op Europees niveau is er verschillende regelgeving op het gebied van cybersecurity, en zijn ook een aantal initiatieven in ontwikkeling. Deze regelgeving en initiatieven hebben ieder een verschillend doel en doelgroep. In de tabel hieronder zijn enkele kenmerken van de regelgeving opgenomen.

216 Schaake, M., *The Lawless Realm, Countering the Real Cyberthreat*. 2020. https://www.foreignaffairs.com/articles/world/2020-10-13/lawless-realm
217 https://www.ncsc.nl/over-ncsc, geraadpleegd op 13 september 2021.

Naam wetgeving	Soort wetgeving	Status	Inhoud
NIS *directive*/ NIB richtlijn	Richtlijn[218]	Dient vanaf 10 mei 2018 geïmplementeerd te zijn bij lidstaten.[219]	• Doelgroep: digitale dienstverleners en aangewezen aanbieders van essentiële diensten. • Samenwerking tussen lidstaten op het gebied van cybersecurity. • Stelt verplichtingen aan doelgroep om beveiligingseisen te implementeren en incidenten te melden.
NIS 2 *directive*	Richtlijn	Ontwerprichtlijn.	• Doelgroep: uitgebreid ten opzichte van de NIS met o.a. de voedselsector, openbaar bestuur, fabrikanten van kritische producten. • Verscherpte beveiligingseisen voor organisaties en versterking van Europese samenwerking.
Cyber Security Act	Verordening[220]	In werking sinds 27 juni 2019.	• Doelgroep: gehele Europese digitale markt. • Vergroot het mandaat van ENISA. • Introductie van cybersecurity certificeringskader (nog in ontwikkeling).
Digital Operational Resilience Act (DORA)	Verordening	Ontwerpverordening, naar verwachting eind 2022 in werking.	• Doelgroep: financiële sector. • Doel: harmoniseren regels digitale weerbaarheid in de EU. • Basiskader voor financiële organisaties, stelt basiseisen aan financiële organisaties o.a. op het gebied van risicomanagement en digitale incidenten.
Horizontale regulering software	Onbekend	Nog in ontwikkeling.	• Doelgroep: softwarefabrikanten.[221] • Horizontale wetgeving met betrekking tot cybersecurity eisen voor softwareproducten.

Daarnaast is er ook regelgeving (in ontwikkeling) op het gebied van *Internet of Things* (IoT), oftewel software die is opgenomen in producten. Dit betreft onder andere het voornemen om cybersecurityeisen te stellen aan draadloos verbonden apparaten via de *Radio Equipment Directive* en de regulering van apparaten die met elkaar communiceren via internet (*connected devices*) in de *Cybersecurity Resilience Act*. Daarnaast zijn er in 2017 een aantal EU verordeningen aangenomen waarbij cybersecurityeisen worden gesteld aan medische apparaten, en zullen er op VN niveau ook cybersecurityeisen worden opgenomen in regulering voor de auto-industrie. Op het gebied van productveiligheid wordt de algemene EU richtlijn voor productveiligheid herzien. Deze herziene richtlijn regelt onder andere de productveiligheid van producten met digitale

218 Een richtlijn moet door lidstaten geïmplementeerd worden in nationale wetgeving.
219 In Nederland is dit vastgelegd in de WBNI.
220 Een verordening is wetgeving direct van toepassing in alle EU lidstaten.
221 Het is nog niet duidelijk voor welke specifieke doelgroep deze wetgeving ontwikkeld wordt.

componenten. Ook op het gebied van consumentenrecht en IoT zijn er Europese ontwikkelingen waarin onder andere zaken rondom het recht op updates zijn opgenomen. Het tegengaan van kwetsbaarheden in software, evenals het opsporen van strafbare feiten ten behoeve van handhaving en vervolging als ook de afspraken over hoe staten onderling met elkaar omgaan als het gaat om cyberaanvallen, vragen om internationale samenwerking.[222]

De handel in software is een internationale markt in vraag en aanbod. Fabrikanten en afnemers bevinden zich over de hele wereld. Zoals in paragraaf 4.1 is beschreven, wordt software als product en de totstandkoming ervan tijdens de levensduur als proces op dit moment alleen gereguleerd vanuit wet- en regelgeving die van toepassing is op de domeinen waarbinnen software wordt toegepast, zoals software in voertuigen en software in zorginstellingen. Op software zelf is geen product- of procesregulering vanuit de overheid van toepassing. Wel zijn er industrienormen, waartegen een fabrikant zijn software of zijn processen kan certificeren, om daar tegenover afnemers bijvoorbeeld verantwoording over te kunnen afleggen.

Ook de actoren die kwetsbaarheden in software misbruiken om de digitale systemen van organisaties aan te vallen komen overal vandaan. Het gaat daarbij zowel om criminele actoren als om actoren die werken voor natiestaten en combinaties of tussenvormen van beide. Zo worden *ransomware* aanvallen vaak uitgevoerd door criminele organisaties, maar kunnen ze ook een dekmantel zijn voor een actie van een inlichtingendienst of een manier zijn voor een land om inkomsten te verkrijgen. Internationale samenwerking is gecompliceerd mede doordat landen niet alleen slachtoffer zijn van onveiligheid door cyberaanvallen, maar ook baat hebben bij kwetsbaarheden in software voor hun eigen activiteiten.[223] Daarnaast belemmeren ideologische verschillen tussen landen internationale samenwerking, bijvoorbeeld over hoe de staat zich verhoudt tot het internet en welke afschrikwekkende acties tegen aanvallers (*deterrence*) toelaatbaar zijn.[224]

Desondanks hebben de lidstaten van Europese Unie de afgelopen jaren echter laten zien in staat te zijn door samen te werken strenge eisen over gegevensbescherming en buitenlandse investeringen te kunnen afdwingen. Ook roepen landen elkaar vaker (in de openbaarheid) tot verantwoording na grootscheepse cyberaanvallen.

222 Zie onder andere Schaake, M., *The Lawless Realm, Countering the Real Cyberthreat.* 2020. https://www.foreignaffairs.com/articles/world/2020-10-13/lawless-realm

223 Perlroth, N. *This is how they tell me the world ends: the cyberweapons arms race*, 2021.

224 Henriksen, A. The end of the road for the UN GGE process: The future regulation of cyberspace, *Journal of Cybersecurity*, Volume 5, Issue 1, 2019. Fischerkeller, M.P. en R.J. Harknett, Deterrence is Not a Credible Strategy for Cyberspace. *Orbis,* Volume 61, Issue 3, 2017, Pages 381-393, 2017. Daniel, M., Closing the Gap: Expanding Cyber Deterrence. *Cyberstability Paper Series,* 2021.

Multistakeholder groepen leveren een bijdrage aan het verbeteren van de internationale samenwerking. Zo werkte de *Global Commision on the Stability of Cyberspace* aan voorstellen voor normen en beleid die de internationale cybersecurity en stabiliteit verbeteren. Daarbij gaat het om normen voor verantwoord gedrag van zowel staten als niet-statelijke actoren in *cyberspace*. In deze commissie is een groot aantal stakeholders betrokken uit verschillende landen en vanuit verschillende soorten organisaties, zoals overheden, universiteiten en fabrikanten. Zij kwamen tot acht normen, waaronder de volgende:[225]

- Niet-statelijke actoren mogen geen cyberaanvallen uitvoeren en staten moeten dit voorkomen en erop reageren als dit wel gebeurt;
- Staten moeten kwetsbaarheden waar zij kennis van hebben in principe melden aan de fabrikant en een transparant raamwerk hanteren voor wanneer ze besluiten om dat niet te doen;
- Fabrikanten van producten en diensten moeten cybersecurity en stabiliteit prioriteit geven en alles doen wat redelijkerwijs mogelijk is om er zeker van te zijn dat deze geen kwetsbaarheden bevatten. Ook moeten zij maatregelen nemen om kwetsbaarheden die bekend worden te mitigeren en daar transparant over zijn. Alle actoren hebben een plicht om informatie over kwetsbaarheden te delen om zo cyberaanvallen te voorkomen en de gevolgen ervan te beperken;
- Landen moeten maatregelen nemen, waaronder wet- en regelgeving, zodat de basis cyberhygiëne op orde is.

225 GCSC, *Advancing Cyberstability*, 2019.https://cyberstability.org/report/