Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken

AI & Cybersecurity

In dialoog met de toezichthouder

Max Landkroon

Bob van der Meulen

Inhoudsopgave

Wie kent de RDI?

Toezicht op cybersecurity & AI

Een juridisch perspectief

De schutterij werd in de middeleeuwen opgericht als plaatselijke militie/toezichthouders die de orde en veiligheid van de burgers moest garanderen.

- Bestaat dat eigenlijk wel, toezicht op cybersecurity?
- Hoe ziet dat toezicht er dan uit?
- En welke scope hebben we het dan over?

Wetgeving AI en cybersecurity

Tegenstrijdige tendens

- Ene kant: “deregulering” (zie: Omnibus / politiek)
- Andere kant: enorme waslijst aan wet- en regelgeving, die vooralsnog niet lijkt te stoppen

Scope…

Overzicht alle wetgeving waarin eisen worden gesteld aan cyberbeveiliging

- DORA (2022/2554) – zie art. 1, 6, 9, etc. etc.
- Data act (2023/2854) - zie art. 4, 19 en 25.
- Data governance act (2022/868 - zie art. 12 en 22.
- eIDAS / eIDAS 2.0 (2024/1183) – zie art. 5quater, 12bis.
- NIS-2/CBW (2022/2555) – (helemaal).
- AI-act (2024/1689) – art. 15 en 55.
- EHDS (2025/327) – art. 73.
- CER/wwke (2022/2557) – art. 13.
- CSA (2019/881) – (helemaal).
- CRA (2024/2847) - (helemaal).
- Cyber solidarity act (2025/38) – (helemaal).
- RED (RED 3.3.) (2014/53, wijziging 2025) – (art. 3.3).
- Netcode on cybersecurity (2024/1366)- (helemaal).
- AVG (2016/679) – art. 5 en 32.
- EU digital networks act (in initiatief).
- Richtlijn inzake de digitalisering van reisdocumenten (in initatief).
- Crypto assets / digital finance act (2023/1114) – art. 68.
- GPSR (2023/988) – art. 6
- Etc. etc. etc.

Toezicht op AI is ook toezicht op cybersecurity, maar andersom geldt hetzelfde!

- Toezicht op AI-act
- Toezicht op AI (vanuit open normen in andere wetgeving)
  - Stelling: >95% van alle AI-producten / diensten valt niet onder AI-act, maar onder ‘toezicht op AI’ (lees: al het voorgaande)

Wat staat er dan in die (open) normen ?

- *(..) door het nemen van **passende technische** of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een **passende beveiliging** ervan gewaarborgd is (AVG)*

- *De lidstaten zorgen ervoor dat essentiële en belangrijke entiteiten **passende en evenredige technische**, operationele en organisatorische **maatregelen nemen om de risico's voor de beveiliging van de netwerk- en informatiesystemen** die deze entiteiten voor hun werkzaamheden of voor het verlenen van hun diensten gebruiken, **te beheren** en om incidenten te voorkomen of de gevolgen van incidenten voor de afnemers van hun diensten en voor andere diensten te beperken. (NIS-2)*

- *AI-systemen met een hoog risico **worden op zodanige wijze ontworpen** en ontwikkeld dat deze een **passend niveau** van nauwkeurigheid, robuustheid en **cyberbeveiliging bieden**, alsook consistente prestaties gedurende de levensduur met betrekking tot deze aspecten (AI-act)*

- *Wanneer de aard van het product dit vereist, **de gepaste cyberbeveiligingskenmerken** die nodig zijn om het product te beschermen tegen externe invloeden, waaronder kwaadwillende derden, indien een dergelijke invloed gevolgen kan hebben voor de veiligheid van het product, waaronder het mogelijke verlies aan onderlinge verbondenheid; (GPSR)*

Rijksinspectie Digitale Infrastructuur

Toezichthouder/uitvoerder op basis van o.a. deze (cybersecurity)wetgeving:

- Telecommunicatiewet (Tw)
- Wet beveiliging netwerk- en informatiesystemen (Wbni)
- Richtlijn Radioapparatuur (RED) / RED 3.3 (cyberbeveiliging)
- Toegankelijkheidsrichtlijn
- eIDAS / eIDAS 2 - verordening
- Markttoezichtsverordening
- Europese Cyber Security verordening (CSA)
- Wet Digitale Overheid (WDO)
- Algemene productveiligheidsverordening (GPSR)

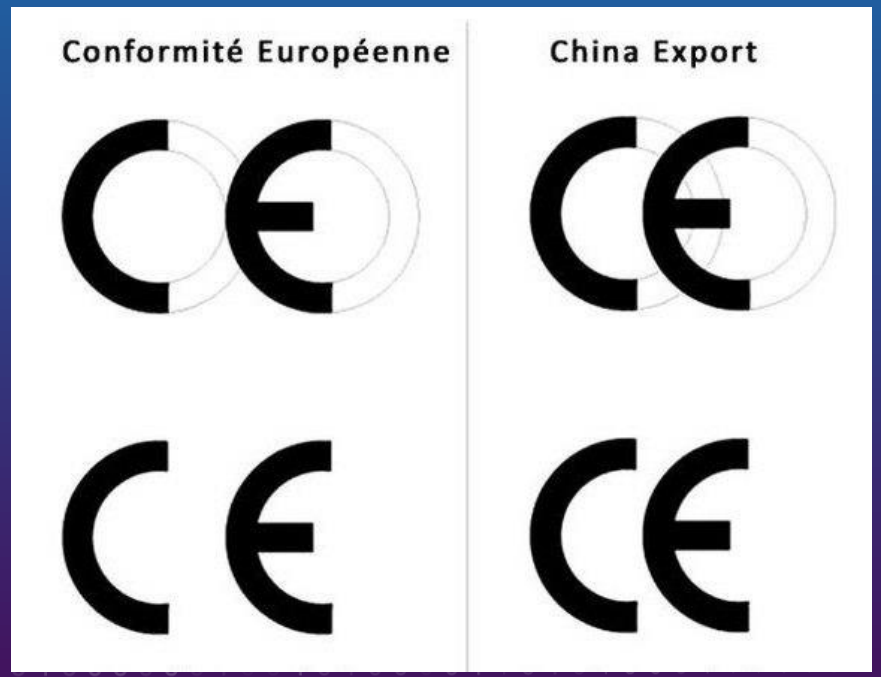
En dit komt er aan (of is er deels al):

- AI-verordening
- Cyberbeveiligingswet (Cbw) (NIS2-richtlijn)
- Wet weerbaarheid kritieke entiteiten (Wwke) (CER)
- Netcode Cybersecurity
- Energiewet
- Cyber Resilience Act (CRA)

Al deze wetten hebben één ding gemeen: eisen aan cybersecurity

- RDI is daarmee de facto een ‘cybersecurity toezichthouder’ (geworden)
- Niet elke regel is automatisch op elke sector / product van toepassing

Cybersecurity: 2 regimes, 1 gemene deler



- Producttoezicht – vallend onder EU 2019/1020 (markttoezichtverordening)
  - Bijvoorbeeld: AI-act, CRA, RED 3.3.
  - Alles waarvoor je een CE-markering nodig hebt.
- en ‘regulier’ toezicht
  - Bijvoorbeeld: eIDAS, NIS-2/CBW, WDO, WBNI

- In beide gevallen geldt, het wordt ingevuld door:
  - Open normen
  - standaarden

Speciale rol voor de cybersecurity act

- CSA: vreemde eend in de bijt, maar zeer relevant
  - **<u>Vermoeden van conformiteit</u>** onder.....
    - AI-act art. 42
    - CRA art. 27
    - NIS-2 art. 24
    - EIDAS 2 art. 12 bis.

Standaarden?

- Maar CSA heeft, vooralsnog, geen AI-specifieke normen (soms wel indirect), en de rest van al die verplichte standaarden ook niet.
  - Zie bijvoorbeeld onder de CSA:

ISO/IEC 27001/17/18	Geen AI-specifieke eisen	Security- en cloudnormen, geen AI
EUCC (EU Common Criteria)	Geen AI-specifieke eisen	CC-gebaseerd, geen AI-criteria
EUCS (EU cloud security)	Geen AI-specifieke eisen	Geen AI-specificaties
ISO/IEC 15408	Indirecte AI-specifieke eisen	Kan AI evalueren, maar bevat geen AI-vereisten

- Er bestaan echter wel standaarden die zien op AI (en deels cybersecurity), maar die zijn vooralsnog niet verplicht:
  - Zie bijvoorbeeld:

AI-specifieke norm	AI-eisen?	Toepassing
ISO/IEC 42001	Ja	AI Management System (AIMS): governance, monitoring, risk controls, datakwaliteit, fairness, explainability
ISO/IEC 23894	Ja	AI risk management, modelrisico's, model drift, adversarial attacks
ISO/IEC 38507	Ja	AI governance in organisaties
ISO/IEC 5338	Ja	AI engineering & lifecycle management
ISO/IEC 25059	Ja	AI quality model (accuracy, robustness, explainability)
ETSI EN 17640	Ja	Europese norm voor "Trustworthy AI"

- Verplichte normen komen waarschijnlijk vanaf **2026–2028** onder de AI Act (let op: dat hoeven niet bovenstaande te zijn!).

Rol RDI – toezicht op AI (en cybersecurity)

- Toezicht (maar hoe?)
  - In gesprek / handhaven / uit de markt halen etc.
  - Prioriteren / risked based approach (?)
- Guidance
  - Communicatie met markt
  - Bijdragen aan standaarden
  - Interpretatie geven aan open normen
- Relatief nieuwe rol m.b.t. AI en toezicht: pionieren en expertise opbouwen (AISSL)
- Doel: een veilig verbonden Nederland

AI & cybersecurity

Zonder kennis geen toezicht mogelijk

- AI speelt een grote rol en gaat een steeds grotere rol spelen in cybersecurity
- Daarmee gaat AI als verdedigingsmechanisme binnen cybersecurity ook een steeds grotere rol spelen in het toezicht van de RDI
- Zodoende: wat valt ons op op het gebied van AI gebruik binnen de cybersecurity?

AI Safety & Security Lab

Een verkenning van de impact van AI

AISSL // **AI Safety & Security Lab**

Ondersteuning Toezicht

Observatorium	**Forensisch**	**Dialoog**
• Up-to-date blijven met de AI ontwikkelingen • Interpreteren en classificeren van (systeem) risico's	• Ondersteuning RDI • Ondersteuning andere toezichthouders	• AI Act Sandboxes • AICC • **AI36** • EU WG • GNAIS

Focus op **complexe** & **nieuwe** AI Risico's

Ontkoppelde Infrastructuur

Publicatie

AIVD & RDI

Aanval **op** GenAI	Aanval **met** *GenAI*
Verdediging **van** *GenAI*	Verdediging **met** *GenAI*

Publicatie

AIVD & RDI

Aanval **op** GenAI	Aanval **met** *GenAI*
Verdediging **van** *GenAI*	Verdediging **met** *GenAI*

Attack **on** *GenAI*	Attack **with** *GenAI*
Defence **of** *GenAI*	Defence **with** *GenAI*

Disrupting the first reported AI-orchestrated cyber espionage campaign

13 nov 2025

Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’

By Heather Chen and Kathleen Magramo, CNN

2 min read · Published 2:31 AM EST, Sun February 4, 2024

LILY HAY NEWMAN MATT BURGESS SECURITY AUG 27, 2025 8:36 AM

The Era of AI-Generated Ransomware Has Arrived

Cybercriminals are increasingly using generative AI tools to fuel their attacks, with new research finding instances of AI being used to develop ransomware.

ESET researcher discovers the first known AI-written ransomware: I feel thrilled but cautious

Ransomware will likely become more sophisticated, faster spreading, and harder to detect.

Roman Cuprik

27 Aug 2025 • 2 min. read

4MIN • SECURITY

Kwaadaardige LLMs verlagen drempel voor cybercrime

GTIG AI Threat Tracker: Advances in Threat Actor Usage of AI Tools

November 5, 2025

Google Threat Intelligence Group

LAMEHUG: The First AI-Powered Malware Shaking Up Cybersecurity in 2025

CoreSecurityInfo Follow 6 min read · Aug 1, 2025

Overzicht cyberdomeinen

Attack **on** *GenAI*

Attack **with** *GenAI*

Defence **of** *GenAI*

Defence **with** *GenAI*

Overzicht is niet uitputtend

Cyber domains by Henry Jiang

Impact non-generatieve AI

Attack **on** *GenAI*

Attack **with** *GenAI*

Defence **of** *GenAI*

Defence **with** *GenAI*

Verkennend onderzoek – open voor discussie

Cyber domains by Henry Jiang

Impact generatieve AI

Attack **on** *GenAI*

Attack **with** *GenAI*

Defence **of** *GenAI*

Defence **with** *GenAI*

Verkennend onderzoek – open voor discussie

Cyber domains by Henry Jiang

In dialoog met de toezichthouder

De techniek verandert snel, wil ik dan:

- Wel compliant zijn, maar feitelijk niet veilig

- Wel veilig zijn, maar niet compliant

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken

Max Landkroon

max.landkroon@rdi.nl

AI Safety & Security Lab

meindert.kamphuis@rdi.nl