

KEYNOTE ON AI, CYBERCRIME AND RESILIENCE

Cybercrime in the AI Era

Criminals use AI to strike faster, on a larger scale and with more convincing tactics. This keynote shows what they do today, what lies ahead and how your organisation puts AI to work in its defence and builds resilience.

In this keynote, he shows how criminals use AI: cloned voices, fake online shops and AI agents that hunt for vulnerabilities on their own. He looks at where crime is heading and how organisations can defend themselves. He has spoken on these subjects to audiences working in policing, defence and international police cooperation.



RICHARD VAN HOOIJDONK

Most futurists study tomorrow's world from a distance. Richard van Hooijdonk already works in it: his research team consists of people and AI agents. He speaks about AI and new technology, the organisation of the future and leadership in the AI era.

3,000+

keynotes

650,000+

participants

30+

countries

Bestselling

author

The keynote in 22 topics

As attacks grow smarter and faster, defences must keep pace. AI makes cybercrime a challenge for the whole organisation.

THE THREAT

How criminals use AI

What AI changes about phishing, fraud, extortion and break-ins, and how criminals organise their operations.



01 Crime-as-a-service

Criminals have long paid for tools and know-how. AI adds convincing phishing in many languages and models stripped of their safeguards.



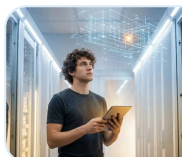
02 Deepfakes and voice clones

A fake voice or video of an executive or relative. Telling the real person apart from the imitation is getting harder.



03 Fraud on an industrial scale

Synthetic identities, fake online shops and investment scams in which chatbots help manipulate many victims at once.



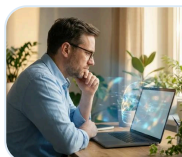
04 AI that finds vulnerabilities

AI reads code, probes systems and finds flaws that went unnoticed for years. Criminals are experimenting with it too.



05 The ransomware business

Criminal groups operate like businesses, using AI to research targets, negotiate and extort money with stolen data.



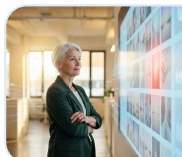
06 The fake job applicant

A remote applicant has a fabricated CV, a stolen identity and sometimes an AI-generated face. Once hired, they hold the keys.



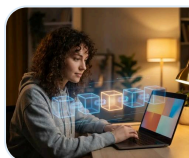
07 AI itself under attack

Hidden instructions, poisoned training data and stolen models. An organisation's own AI becomes a target.



08 Fake news as a weapon

A fabricated statement attributed to an executive or a fabricated disaster photo: AI disinformation can move share prices and damage reputations.



09 A way in through the supply chain

One infected update or software component can hit thousands of customers. AI helps attackers find a way into the supply chain.

THE FUTURE

The future of crime

Where crime could be in five to fifteen years: attacks that run themselves, broken encryption and crime that reaches beyond the screen.



10 The attack that runs itself

FUTURE SCENARIO

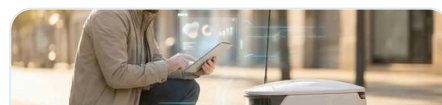
AI agents could run entire attacks: scouting, breaking in, finding data and negotiating, against thousands of targets at once.



11 When encryption breaks

FUTURE SCENARIO

A future quantum computer could break widely used encryption. Criminals and states are already collecting encrypted data.



12 Crime beyond the screen

FUTURE SCENARIO

Robots, drones and driverless cars will coordinate their own work. Hacking their controls could disrupt streets and warehouses.



DURATION

30, 45, 60 minutes or longer, with time for questions



LANGUAGE

Dutch or English



FORMAT

On location or online



FEE

From €3,500 (webinars)

THE OTHER SIDE

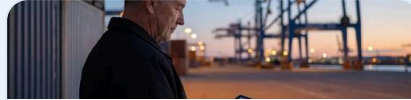
Critical infrastructure

Why power, water, healthcare and ports attract attackers, where crime meets conflict and how much surveillance a safe society will accept.



13 Critical infrastructure as a target

Power, water, hospitals, ports and networks partly rely on old control systems. Now connected to the internet, they can be reached remotely.



14 Criminals working for states

Governments use criminal groups to break in, sabotage and spy. To the victim, it looks like ordinary cybercrime.



15 Security and freedom

A safe society faces choices about surveillance. AI can track network traffic and human behaviour in ever greater detail.

THE ORGANISATION

The resilient organisation

How your organisation defends itself against criminals using AI: human-AI teams, new roles, a board that sets direction and partners around the world.



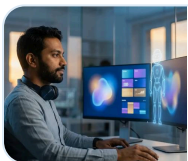
16 The AI-first organisation

In security, AI does the repetitive and predictive work, and spots threats faster than people ever could. The team judges and chooses.



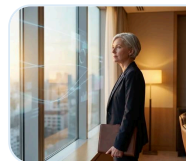
17 Defence with AI

AI spots unusual network behaviour, stolen accounts and misused supplier access, and can act within seconds.



18 New roles in security

Specialists who attack their own AI to test it, people overseeing defensive AI agents, and analysts working alongside AI.



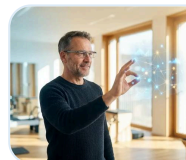
19 Resilience in the boardroom

Rules make boards responsible for digital security. In an AI-first organisation, they also decide what AI may do independently.



20 People as the first defence

Many attacks begin with a person. When reporting concerns is normal, every employee becomes a sensor.



21 A future academy for security

Attackers change tactics quickly. Organisations train their own people in a future academy where AI plays the attacker.



22 Stronger together against crime

Criminals cooperate globally. Defenders do too, through international ecosystems of businesses, researchers, police and governments.



“Richard succeeded excellently in waking up our leaders and setting them on the path to the future: after the lecture, discussions took place across various parts of the organisation about the topics covered, and initiatives have been set in motion.”

Aart van Haren Managing director,
PLUS



“A dazzling journey through new technology. The enthusiasm and energy during his presentation, combined with the visuals, provided a successful kick-off to our event.”

Patrick Steemers Partner, Deloitte



Cybercrime in the AI Era
for your event

EMAIL

talks@vanhooijdonk.com

PHONE

+31 85 303 0792

WEB

richardvanhooijdonk.com