Government of the Netherlands

AI is accelerating the threat: *action is needed* ***now***

The General Intelligence and Security Service (AIVD), the Defence Intelligence and Security Service (MIVD), the National Cyber Security Centre (NCSC-NL), the National Coordinator for Counterterrorism and Security (NCTV), the Public Prosecution Service (OM), CIO Rijk and The Police observe that Artificial Intelligence (AI) is significantly changing the threat landscape. AI is accelerating threats and enabling a broader range of malicious actors to carry out attacks. Vulnerabilities are identified and exploited more quickly. Long-standing weaknesses are being amplified by the influence of AI. Artificial intelligence is used by actors to identify as well as exploit vulnerabilities before defenders are aware of their existence. Action is needed now to prepare for this.

We regularly see the consequences of cyber incidents when appropriate defences are lacking: prolonged outages of critical systems and large numbers of citizens falling victim to the theft of names, addresses and citizen service numbers (BSNs), with all the resulting privacy and financial implications. The impact of cyber attacks may not be immediately apparent. State actors engage in espionage targeting Dutch businesses, government bodies and citizens, and may obtain sensitive or classified information without being detected. This position could also potentially be used to cause damage at a later stage.

We therefore call on those in leadership positions to take responsibility and give cybersecurity priority: make the necessary resources available, prioritise cybersecurity and give experts the scope they need to strengthen the Netherlands' resilience.

Changes in the threat landscape

Cybersecurity is a continuous contest between attack and defence. AI lowers the barrier to entry for attackers and enables a broader range of malicious actors to carry out cyber attacks. Vulnerabilities are identified and exploited increasingly quickly by AI. This creates a new reality which we must adapt to.

Malicious actors primarily use AI to automate, accelerate or enhance the efficiency of their attack techniques: cyber attacks are becoming more advanced and remain undetected for longer. By leveraging AI, they can conduct attacks more quickly, develop malware more easily, write better phishing emails and personalise disinformation on a large scale. Moreover, attackers do not need to use the most advanced frontier models. Attacks can already be carried out using existing and readily accessible AI models.

Why this requires different leadership

Digital security is no longer an issue solely for CISOs and IT professionals. Its dependence is too great, too complex and too risky for organisations. Strengthening the Netherlands' digital resilience is a shared responsibility that requires action by public and private stakeholders alike.

To remain digitally resilient, it is essential to incorporate the risks of AI into cybersecurity policy. This applies to the use of AI models by malicious actors, but also to how AI models are deployed within your organisation, both for everyday applications and for defensive cybersecurity capabilities.

Organisations that have their fundamentals in order, with cybersecurity prioritised by their leadership, effective patch management, a small attack surface, logging and monitoring, allied with insight into their IT landscape, are significantly better positioned in this new reality.

The most important step we need to take is not a technical one, but creating a culture of cyber awareness. Cybersecurity is not an IT problem that can be solved somewhere in a basement or datacentre. It is a broad organisational issue, a governance issue and, ultimately, a societal issue. We are only as strong as our weakest link, and that weakest link is often not a matter of technology but of awareness amongst leadership as well as operational staff, who may lack sufficient understanding and recognition of cyber threats.

Leaders can take responsibility by owning the risks and making the appropriate financial and other resources available.

Three actions leaders can take today to fulfil their responsibility:

1. The fundamentals must be in order

Prioritise cybersecurity in the boardroom. Reducing the attack surface and replacing outdated systems that no longer receive security updates is a first step towards this. Make resources, such as funding, expertise and capacity, available for this purpose. It is not defensible that attacks should take place because the fundamentals are not in order and, for example, patches are either not installed or not installed in a timely manner. As the threat landscape grows increasingly complex, fundamental principles remain an effective barrier. You don't wear a seat belt because the law requires it, but because you want to get home safely. The same applies to basic measures. The human factor is vitally important in this: invest in awareness and behavioural and cultural change, and report incidents to the relevant authorities. Technology cannot solve everything, but with the right culture and training, your employees become your strongest line of defence.

2. Ask yourself: Is my security at an appropriate level?

For example, ensure adequate patch management so that your security is maintained at the required level. The race between releasing patches and exploiting vulnerabilities is not new, but low-barrier access to AI models is accelerating the pace of the contest. What once took weeks now takes days, and what took days now takes hours when it comes to deploying updates.

So, it is essential also to prepare for when things do go wrong. That is the principle behind Assume Breach: assume that an attacker can get in and ensure your organisation can respond when they do. Be prepared: know what you can do yourself, what you need help with, and make the necessary arrangements in advance. Think about it, develop a plan, and ensure that employees are educated, trained and practised in carrying out that plan.

3. Take signals seriously

Monitor developments and seek advice from technical experts. In a future where AI will play an increasingly important role for both attackers and defenders, the greatest risk lies not with AI, but with you, as a leader. It is essential, therefore, to adapt to the new reality.

Our shared responsibility

The Netherlands' digital resilience is constantly under pressure in the cat-and-mouse game between attackers and defenders. AI models accelerate this process and expose the existing weaknesses in our digital resilience even more clearly.

AI is changing the cyber landscape: cybercriminals and state actors are integrating AI into their strategies, making attacks faster, more complex and more widespread. Without adequate preparation and mitigation measures for these attacks, such as ensuring the fundamentals are in order, future cyber attacks could have significant consequences for organisations, certain sectors and society.

Preventing security incidents will remain a challenge for every organisation. Organisations that prepare effectively can detect and contain incidents more quickly and limit the impact on their operations and finances. These developments therefore require government bodies and organisational leaders to take responsibility. They must make the right decisions and ensure that sufficient resources are available. This in turn gives experts the scope they need to strengthen cybersecurity in the Netherlands. Only then can we minimise the impact of cyber attacks and the threat they pose to society.

Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

General Intelligence and Security Service (AIVD)
Simone Smit
Directeur-generaal

Ministerie van Defensie

Defence Intelligence and Security Service (MIVD)
Peter Reesink
Vice-admiraal

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

National Cyber Security Centre (NCSC)
Matthijs van Amelsfort
Algemeen directeur

Nationaal Coördinator Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

National Coordinator for Counterterrorism and Security (NCTV)
Marc Kuipers
Nationaal Coördinator Terrorismebestrijding & Veiligheid

POLITIE

The Police
Janny Knol
Korpschef

OPENBAAR MINISTERIE

Public Prosecution Service
Rinus Otte
Voorzitter College van procureurs-generaal

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

CIO Rijk
Art de Blaauw
CIO Rijk