Signal letter 'Start the knowledge leap for AI-driven cyberattacks today'

To: Minister of Justice and Security and State Secretary for the Digital Economy and Sovereignty
cc: Minister of Economic Affairs and Climate Policy, Minister of Defence, Minister of Foreign Affairs, State Secretary for Kingdom Relations and Government Effectiveness

Your Excellency,

The Netherlands is not prepared for a new generation of cyberattacks in which artificial intelligence is deployed as a weapon. The Cyber Security Council (hereinafter the Council) is deeply concerned about this. These attacks are faster, larger in scale, and more difficult to detect than traditional cyberattacks, and are already being deployed autonomously by state actors. Our defenses are lagging. In this signal letter, the Council substantiates these concerns and makes three concrete recommendations.

Summary of the advice

The council advises:

- to recognize AI-driven cyberattacks as a full-fledged strategic threat and to adapt policies, budgets, and operational plans accordingly as soon as possible;
- To substantially close the knowledge gap of the Netherlands and the EU in this area in the coming years. In other fields, a so-called *Grand Challenge has* proven to be a good means for this: a competition aimed at stimulating knowledge building, in which (multidisciplinary) teams work on possible *dual use* solutions. The council offers to investigate the organization of these, together with business and academia, in a European context.

Cause

The consequences of threats from AI-driven cyberattacks are urgent, and the impact on national and public security can be significant. Although advanced cyberattacks using AI are still limited, many countries are rapidly developing knowledge and applications. It is therefore expected that such attacks will pose a major threat in the near future. Closing our knowledge gap in this area is consequently urgently necessary. The Netherlands' knowledge gap is widening every day, and the longer we delay building knowledge and developing applications, the greater the risk of damage from such attacks will be, and the more recovery capacity will be required.

These concerns apply not only to the Netherlands but are widely shared. For instance, leading researchers in Belgium, Germany, and the United States warn of the strategic implications of the knowledge gap for Western democracies. The European Commission also explicitly warns against AI-driven cyberweapons in the report *'Apply AI Strategy' , published in October 2025*.

> *"Terrorist and organized criminal organizations are increasingly using AI-based technologies to accelerate, upscale and broaden the reach of their illicit activities. Cybercrime, sabotage and terrorism are blended into hybrid attacks, where AI is often exploited by malicious actors. We therefore need to ensure the swift delivery of AI-based solutions for internal security and cyber security."*

Developments

The council notes three developments regarding the use of AI in cyberattacks:

1. Cyberattacks using AI are already taking place in practice

AI systems can quickly, on a large scale, and autonomously identify, analyze, and exploit vulnerabilities. Although these high-quality attacks are currently limited in scope, these developments have the potential to cause societal disruption. Concrete examples illustrate the urgency:

- a Russian state-affiliated hacking group (APT28) deployed sophisticated adaptive malware (LAMEHUG), in which AI converted simple text instructions into targeted cyberattacks on victims' computers.
- 2025 was also the year in which a hacking group affiliated with China carried out a cyber espionage attack in which AI autonomously attacked dozens of organizations (technology companies, financial institutions, and government organizations) around the world.
- AI technology is becoming increasingly easy to deploy for criminal activities. Solutions for cyberattacks similar to ChatGPT are appearing constantly: FraudGPT, WormGPT, DarkGPT, and similar tools are being deployed for both large-scale autonomous attacks and high-quality advanced attacks.
- AI-driven scanning and malware drastically shorten the time between the discovery of a vulnerability and its exploitation. As a result, organizations have less time to remedy vulnerabilities and are more frequently forced to implement hasty updates. The consequences of this became evident during the (non-AI-related) Crowdstrike incident in 2024, where a forced update caused major disruptions worldwide.

2. Current specialized knowledge is insufficiently available

Expertise regarding advanced AI applications for cyberattacks is currently concentrated in the hands of malicious actors – often states with offensive cyber programs and the intelligence and security services of other countries. Only those who understand how an adversary operates can effectively protect themselves against it. However, these actors share this knowledge little to none, not even with friendly nations or within partnerships such as NATO. Consequently, the Netherlands currently lacks the required specialized knowledge to fathom the nature, scope, and methodologies of AI-driven cyberattacks. The ability to develop sufficient defensive solutions and applications independently remains even further out of reach. To not only close the knowledge gap but to keep up, it is necessary to invest structurally in knowledge development and innovation surrounding this theme. Countries outside the EU are already fully engaged in this.

3. Defensive striking power falls short

Resilience against AI-driven attacks increasingly requires—in addition to knowledge about the nature of such attacks—the deployment of automated systems to detect attacks faster, predict exploitation, and develop more effective recovery methods. These are systems in which AI plays a key role. The Syzbot project, launched by Google for defensive purposes, illustrates this. Using a genetic algorithm (an older form of AI technology), it continuously searches for vulnerabilities in common operating systems. Although the AI application in Syzbot is not very advanced, the system is already finding more bugs than programmers can handle: hundreds to thousands of software errors are constantly awaiting fix.

Although computing power and expertise are present in the Netherlands and the EU, including in future AI factories, research institutes, and universities, there is a lack of a clear strategy to put these to use for our digital resilience. The innovation climate, investments, and business activity in this area are lagging, certainly compared to other leading countries.

Recommendations

The council has three recommendations to close the gap in AI cyberattacks and counter the threat:

1. **Incorporate AI-driven threats into government strategies and policy.** Recognize AI-driven cyberattacks as a full-fledged strategic threat and align policies, R&D budgets, and operational plans accordingly. Implement this through public-private and scientific collaboration, building upon existing coalitions where possible. Do not wait for the next Dutch Cybersecurity Strategy (NLCS): start now.
2. **Invest strategically in the Dutch business community in the field of AI and cybersecurity.** Increase defensive capabilities by developing innovative products for better detection of AI attacks, more sophisticated penetration testing — including for ethical hackers — and tools for active cyber defense. To this end, utilize the investment and innovation instruments from the Jetten -I coalition agreement.
3. **Request for political support for a European *Grand Challenge* in the field of AI and cybersecurity.** A Grand Challenge is a competition that stimulates knowledge building and innovation by mobilizing multidisciplinary teams of researchers and companies — including start-ups and scale-ups. By offering the solutions as open source, they are potentially commercially scalable within government organizations as well as the business sector. Within the EU, a challenge of this magnitude in the field of cybersecurity and AI has not previously been launched. Business and science, represented in the Council, see opportunities to organize this at the European level and wish to explore this. Your political support can help make this initiative a success.

The council calls on the cabinet to take concrete steps on each of the three recommendations above before the end of 2026. Delay increases the vulnerability of the Netherlands.

The council is more than willing to enter into a dialogue regarding our recommendations.

Yours faithfully,

Marc Kuipers
Co-chair public sector

Sylvia van Es
Co-chair private sector

The Hague, March 25, 2026