CYBER CRIME MONITOR NETHERLANDS 2026

Summary

OPENBAAR MINISTERIE POLITIE

01/02

Summary

The insights from the Cybercrime Monitor Netherlands 2026 lead to three key conclusions. These conclusions provide starting points not only for identifying and prosecuting individuals within the cybercrime ecosystem, but also for systematically disrupting underlying structures and revenue models.

1. The different types of offenders are becoming increasingly interconnected, leading to hybrid forms of crime. Criminal groups are becoming intertwined with state actors; young Western cybercriminals are involved in nihilistic violent extremism.

2. Cybercrime should no longer be seen as a collection of separate offences, but as a criminal ecosystem. Behind almost every attack lies a chain of mutually cooperating offenders, resources and criminal services that reinforce one another - a criminal supply chain that enables and sustains cybercrime.

3. Artificial intelligence (AI) is a catalyst for cybercrime: it increases the speed and scale at which attacks take place. Criminal use of AI is no longer hypothetical and has potentially disruptive consequences.

The capacity for investigation and prosecution is limited. The Public Prosecution Service and the police will therefore have to make choices about which cases they invest time, energy and expertise in. This continuously challenges them to be agile and innovative in their approach. The broad response to combating cybercrime consists of prosecuting suspects, victim and offender prevention, disrupting criminal activities and informing victims.

The complex cybercrime threat landscape requires both a broad and integrated response. Tackling cybercrime is not solely the responsibility of the specialised investigation teams within the Public Prosecution Service and the police. The private and public sector, academia, government and individual citizens all have their own role to play in protecting our digital security. Practice has now shown that digital security can no longer be viewed separately from physical security. A sense of urgency alone is therefore no longer sufficient; everyone must take responsibility for their societal role and actively contribute to strengthening the digital resilience of society. Scientific research provides important tools and insights to support this.

Action points for the Public Prosecution Service and the police

Intensify cooperation

To remain effective in investigating and prosecuting crime, the Public Prosecution Service and the police should, first, strengthen cooperation with public and private parties and international law enforcement agencies. Only by working together across borders, exchanging information and sharing analytical capacity can they effectively identify and prosecute suspects, trace criminal money flows and sustainably strengthen their investigative and information position.

Increase innovation

Secondly, it is important to develop innovative and alternative investigative and intervention methods. These are needed to effectively disrupt the interconnected international offender structures. Financial investigation should structurally be part of cybercrime investigations. If the Public Prosecution Service and the police map cryptocurrency flows at an early stage, focusing on the seizure of criminal assets and disrupt financial infrastructures, they can effectively tackle the criminal revenue model of cybercrime.

02/02

Summary

Strengthen specialisation and disseminate knowledge more broadly
Thirdly, the Public Prosecution Service and the police must continue to invest in specialist knowledge, particularly in areas such as cryptocurrency and AI. At the same time, this expertise remains too concentrated within a small group of specialists. It is essential that a broader foundation of knowledge is embedded across the relevant organisations, so that they are not dependent on a select group of experts. A strong information position is essential for combating cybercrime.

Action points for the wider ecosystem

Agile legislation
For future-proof investigation and prosecution, it is important that laws and regulations keep pace with a digitised world that is rapidly evolving. Criminal networks operate online, while laws and regulations are often still based on the physical world. To use information from relevant public and private parties, the Public Prosecution Service and the police need appropriate legal bases, such as those now established in the Cybersecurity Act (Cbw). For the National Cyber Security Centre, it is now easier to share information with the police without a formal request always being required.

Tackling bad hosting
Measures are needed to combat bad hosting. Know-your-customer policies should therefore be made mandatory, the first payment in cryptocurrency should be prohibited, and the registration of hosting companies with the Chamber of Commerce should be specified. Administrative law should also be used effectively to combat bad hosting.

More prevention
Public and private parties have a major role to play in prevention. To combat cybercrime broadly, it is essential that citizens receive appropriate information about how foreign powers engage in digital influence operations. Citizens must be aware of the risk that they may be used by foreign powers. Parents, schools and other stakeholders all have an important role to play in preventing young people from becoming online offenders, either knowingly or unknowingly. By knowing what is happening online and by making young people digitally resilient to online influence, they can prevent young people from becoming involved in cybercrime.

To prevent victimisation, the individual citizen's online consumer behaviour also deserves particular attention: downloading a wide range of apps and devices and purchasing cheap, often Chinese-made, equipment that is connected to the home network without due consideration poses a significant risk. The principle 'if it is free or cheap, you are the product' applies here without exception: such devices and apps can, without the user's knowledge, turn home networks into part of a proxy network.

Take basic measures
Companies and organisations can increase their resilience to digital threats with relative ease. Basic cybersecurity measures often make a significant difference. Make this a policy priority. Train staff to strengthen resilience against social engineering and improve data management. Assume that malicious actors are already in your network, or may gain access one day, and limit their access by avoiding storing all data in one place. Where the potential physical consequences are high, securing systems must be an absolute priority.

Report it, do not pay
And: report cybercrime if you become a victim. Involving the police at an early stage increases the likelihood of criminals being identified and prosecuted. Do not pay a ransom; this is a direct investment in more and more dangerous cybercrime. For some organisations, such as government organisations, reporting cybercrime should even be mandatory.

The Cybercrime Monitor Netherlands is a publication of the Netherlands Public Prosecution Service and the Netherlands Police.

For substantive questions, please contact *ccbn@om.nl*.
For media enquiries, please contact the National Head Office