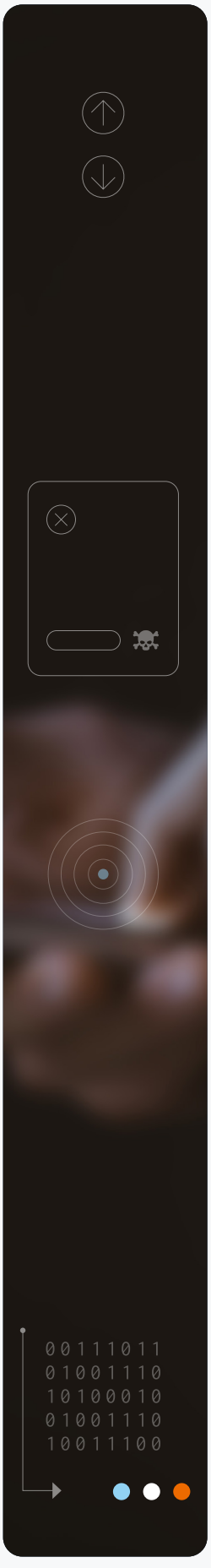
OPENBAAR MINISTERIE POLITIE

CYBER CRIME MONITOR NETHERLANDS 2024



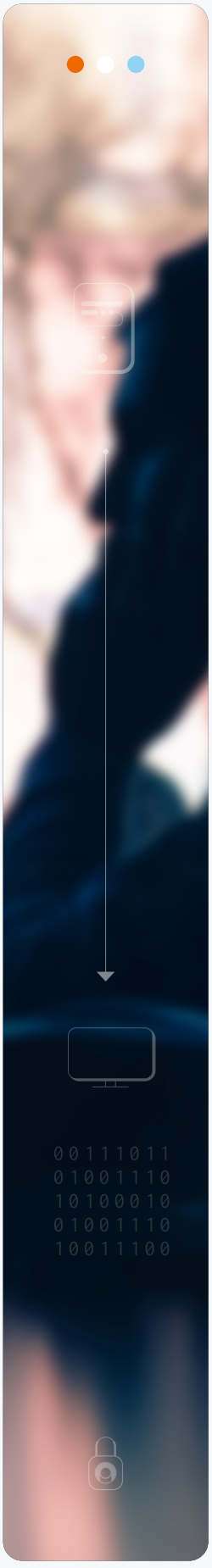
Summary

Cybercrime can only be fought effectively through extensive cooperation, with the Public Prosecution Service, the National Police, and public and private partners working closely together. Comprehensive counteraction against cybercrime involves investigation, detection and prosecution, but also disruption of criminal activity, mitigation of damage (through notification), prevention of victimisation, and offender deterrence. Therefore, it is essential that all stakeholders have a sense of urgency on the matter of countering cybercrime.

The Cybercrime Monitor Netherlands (CMN) tracks trends and developments within the cybercrime landscape, specifically from the unique perspective of the Public Prosecution Service and the National Police, supplemented with open source information. It is the first edition of a biennial publication. This first edition focuses on cybercrime aimed primarily at ICT: cyber-dependent crime. It serves as a resource for policymakers in both public and private sectors involved in the comprehensive efforts to counter cybercrime.

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

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



Key takeaways

Key takeaways from the Cybercrime Monitor Netherlands 2024:

01

The cybercrime landscape is complex

Because cybercrime knows many forms that are constantly evolving, counteraction requires an unconventional approach. Cybercrime is a global crime with a local footprint by default, and tackling it requires continuously developing specialized skills.

Whilst law enforcement and prosecution need knowledge, expertise, time, and focus to combat cybercrime, it takes less effort than ever before for criminals to enter into this field of crime.

One does not need to be tech savvy to become a cybercriminal, as technically skilled individuals offer their criminal services, products and knowledge readily online: cybercrime-as-a-service. This creates the opportunity for a wide variety of criminals to commit cybercrime.

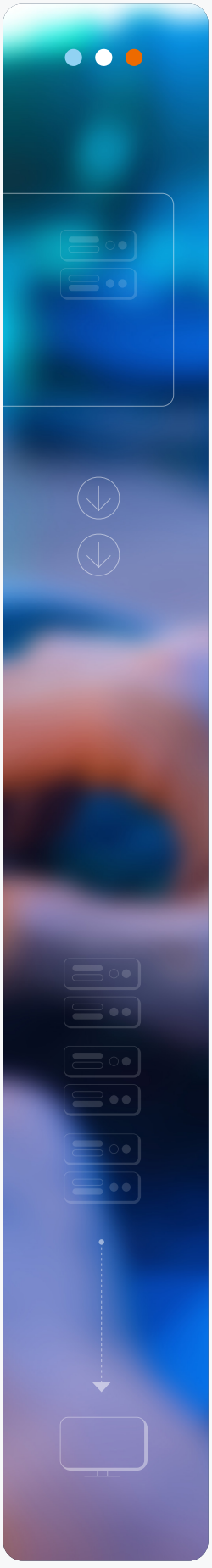
02

Trends and developments 2024

Criminal investigations and prosecutions show the following trends and developments contributing to the scale and impact of cybercrime:

I. Worrying proportion of young cybercrime suspects
The Public Prosecution Service and National Police are concerned about the proportion of young cybercrime suspects; half of the number of cybercrime suspects who appear before a judge are younger than 25.

II. Rise of data theft and data commodification
Cybercriminals increasingly shift their extortion tactics from encryption to data theft and leakage as a means of extortion. Stolen data is then refined and enriched and sold to other criminals for further criminal activity.



Key takeaways

Key takeaways from the Cybercrime Monitor Netherlands 2024:

02

Trends and developments 2024

III. Blending of traditional and cyber crime
The world of cybercrime and traditional crime are increasingly blending together. Cybercrime suspects do not exclusively commit cyber offences; weapons, ammunition and explosives are also found in the possession of - sometimes even juvenile - suspects. The notion that cybercriminals just arm themselves with a keyboard is therefore not always accurate.

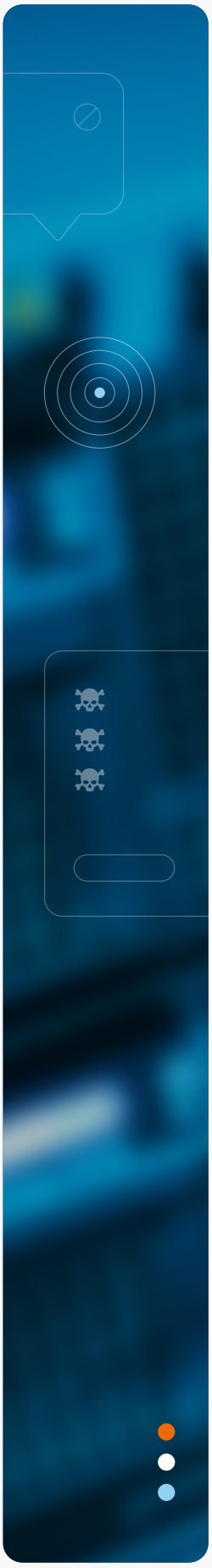
IV. The Netherlands as a host country for criminal infrastructure
Netherlands-based data centers and hosting providers play an important part in countering cybercrime. Some data centers and hosting providers present themselves as legitimate, but take little to no responsibility for minimising the amount of illegal content on their servers, and advertise their services on the criminal market, thus actively facilitating cybercrime. Despite improved legislation that the Digital Services Act (DSA) provides, room for questionable business models persists.

03

The impact on victims is underestimated

Research shows that individual victims of cybercrime suffer more emotionally than financially. It also turns out that in some cases victims of cybercrime experience more acute stress than victims of comparable traditional crimes.

Furthermore, criminal damage to businesses and other organisations does not only consist of initial material losses, but could also include secondary harm like reputational damage, or violations of privacy, and persistent mental health issues among employees. Finally, the criminal justice system is not equipped to effectively handle mass victimisation; a result of the inherent scalability of cybercrime, where one push of a button can create many victims in one go.



Key takeaways

Key takeaways from the Cybercrime Monitor Netherlands 2024:

04

A comprehensive approach is crucial for effectively countering cybercrime

Public and private partners play a crucial part in combating cybercrime. The cybercrime ecosystem is both flexible and resilient. Local interventions are important where they are possible, but they are not necessarily of great impact on the system as a whole.

Counteraction therefore requires a comprehensive and systemic approach, in which various stakeholders have their own expertise and responsibility. Law enforcement and prosecution are important parts of that comprehensive counteraction, but other public and private stakeholders play a crucial role as well.

A comprehensive, integrated and systemic approach does not only involve prosecution of cybercriminals, but needs to include disruption of their criminal activity, victim notification and prevention that focuses both on victims as well as offenders.