CYBBAR COUNTRY PROFILE **THE NETHERLANDS**

www.cybbar.eu

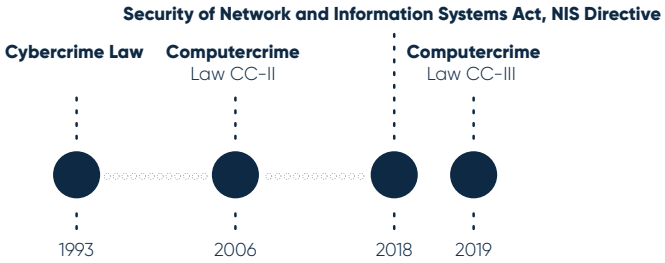
CYBER REPORTING MECHANISM

01 At a local police station, where the reporting party can ask a cyber expert to be present.

By calling the national police hotline. **02**

03 By reporting the crime anonymously at **www.meldmisdaadanoniem.nl**, albeit without pressing charges.

REGULATORY FRAMEWORK



REASONS FOR UNDERREPORTING

- **(Perceived) Reputational damage**
- **Costs of reporting**
- **Sensitivity of internal diagnostics data**
- **Lack of single point of contact for businesses at police**

DIVISION OF TASKS

NCSC National Cyber Security Centre

The NCSC protects the critical infrastructure of public and private entities involved in vital economic functions and has the mandate to act in case of immediate cyber threats. In addition, it is responsible for shaping and coordinating the Dutch policy framework for cybersecurity.

DTC Digital Trust Centre

The DTC is mandated to boost the digital resilience and security of non-vital businesses. In addition, it can share information about cyber threats with non-vital businesses at risk (Ministerie van Economische Zaken en Klimaat, 2021).

CYBER SECURITY COUNCIL

The Cyber Security Council is a national, independent advisory body consisting of representatives from academia, the public sector and businesses which observes the implementation of the country's Cyber Security Strategy and provides research and strategic advice (Timelex, 2019).

THTC Team High Tech Crime

The THTC is a special unit within the National Police that handles specific complex cybercrime cases characterized by, for instance, a high social impact, a strong international component or advanced methodologies.

FACTS

8%
OF THE REPORTED CHARGES ARE PRESSED IN CYBERCRIME CASES

Law enforcement statistics show that charges are only pressed in about **8%** of reported cybercrime cases (Nationale Politie, n.d.).

TWICE
CYBER INCIDENTS WITH INTERNAL CAUSE ARE TWO TIMES HIGHER IN BIG COMPANIES

In companies with over **250** employees, the number of reported cyber incidents with an internal cause is roughly twice as large as the number of cyber incidents with an external cause (CBS, 2021).

1.610
DDoS ATTACKS ARE REGISTERD IN 2020

The National Internet Providers Management Foundation (Stichting Nationale Beheersorganisatie Internet Providers, NBIP) registered **1.610 DDoS attacks in 2020**, as opposed to 919 recorded in 2019. The longest DDoS attack in the Netherlands in 2020 lasted over 20 hours (NBIP, 2021).

The project is funded by the European Union's Internal Security Fund - Police

ECORYS Answering tomorrow's challenges today | CSD CENTER FOR THE STUDY OF DEMOCRACY | FORENTEC