



samen tegen cybercrime
NICC

The National Infrastructure against Cybercrime (NICC) is the Dutch approach to fighting cybercrime. The NICC programme is a public-private partnership.

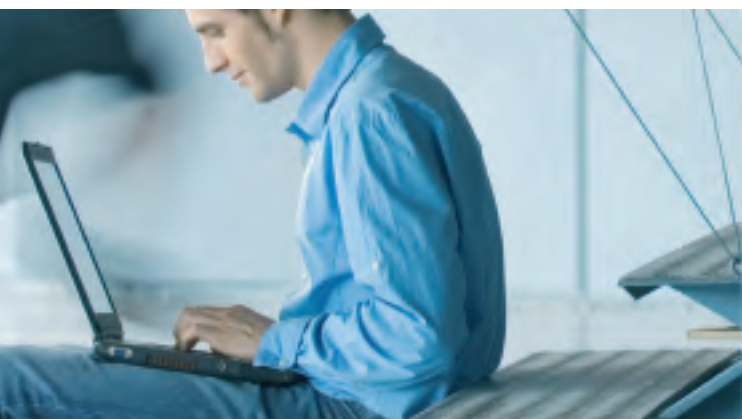
United against cybercrime

The Dutch approach: results through partnership

In our digital world, we want to be able to work securely, and prevention is the key. We certainly need to investigate and prosecute cybercrime, but this alone is not the solution. Only when government, investigatory authorities and the private sector join forces and exchange information about new threats will we be able to keep up with the cybercriminals.

An infrastructure is needed to integrate separate activities and establish and facilitate collaboration between all the parties involved. Embracing the principle of 'learning by doing', the Dutch government and the private sector took the first steps towards developing a successful strategy against cybercrime in 2006 with the establishment of the National Infrastructure against Cybercrime (Nationale Infrastructuur ter bestrijding van Cybercrime, NICC).

The NICC programme is charged with the responsibility of creating this infrastructure – not only by developing new features, but by collaborating with others as much as possible and by integrating existing initiatives in order to create the National Infrastructure.



The NICC is not involved in the actual fight against cybercrime – this is the responsibility of all the public and private stakeholders involved. So what is the purpose of the NICC? The programme supports, facilitates and finances initiatives by other public and private organizations that contribute to safer computer-supported work processes. The NICC brings these organizations together so that they can continue to build the National Infrastructure. They bring their own knowledge and experience to the table. The NICC's role is to monitor the entire process, to gather and disseminate information and to encourage public and private organizations to share their knowledge.

The NICC listens to its stakeholders and responds to their demands, working closely with organizations that propose concrete, viable initiatives. The NICC programme works in a dynamic and flexible way. We realize that what is essential today may be outdated tomorrow. We keep track of developments and continuously adapt our efforts on the basis of the latest information. The NICC supports practical, well-organized projects, pilots and trials. We believe in getting the project started – no long lead times, complex structures or endless meetings, but learning by doing and making any adjustments as and when needed.

National Infrastructure against Cybercrime

The time has come for public and private organizations to jointly assess the electronic security measures they have adopted, and to align them and implement additional measures where necessary. The National Infrastructure is a partnership between professionals drawn from all the disciplines involved in fighting cybercrime.

A number of Dutch organizations involved in the fight against cybercrime are already in place, such as the Cybercrime Reporting Unit (Meldpunt Cybercrime), the High Tech Crime Team of the National Police Services Agency (Korps Landelijke Politiediensten, KLPD) and the National Alerting Service (Waarschuwingsdienst.nl) of GOVCERT.NL, the government's Computer Emergency Response Team. Other organizations are currently in the development stage, while managers of the critical infrastructure are also developing in-house security measures. The fight against cybercrime at the national level is currently still fragmented however, as there is no comprehensive overview available of all the initiatives. It is not clear who is responsible for what, and there is no common, public-private, integrated approach. The map of the fight against cybercrime has overlapping features and 'blind spots'. The NICC assesses the status of the fight against cybercrime, identifies overlaps and supports activities that help fill in these blind spots.

The National Infrastructure consists of several components: a contact point, reporting unit, trend watching, monitoring and detection, information distribution, education, warning, development, knowledge sharing, surveillance, prevention, termination and mitigation.



The NICC further strengthens this infrastructure in two ways:

1. By hosting the Cybercrime Information Exchange, the heart of the National Infrastructure.
2. By developing and supporting practical projects and trials that both solve concrete problems and generate knowledge about cybercrime.

The result is an integrated public-private approach to secure electronic work processes – a single, balanced National Infrastructure against Cybercrime.

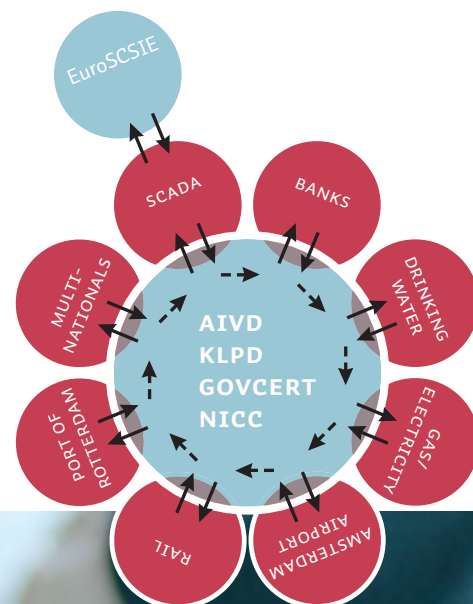
Cybercrime Information Exchange

The Cybercrime Information Exchange is the beating heart of the National Infrastructure, in which public and private organizations share sensitive information.

The information-sharing model adopted by the Dutch Cybercrime Information Exchange is based on that used by the UK's Centre for the Protection of National Infrastructure (CPNI). As part of this model, a select group of government services consults with representatives of critical industry sectors on the risks of cybercrime and the measures to be implemented. The sectors themselves select representatives to participate in these meetings. Trust and Value are fundamental success factors for the Cybercrime Information Exchange. Valuable information can only be shared in a trusted environment. For this purpose a 'traffic-light protocol' is used, where 'red' information must not be disseminated outside the exchange, 'amber' information may be shared within the organization on a need-to-know basis, and 'green' information may be circulated more widely within a particular community. This sharing of information is beneficial for both industry and government. By learning from each other, every participant can improve their level of assurance.

The Information Exchange is pictured as a 'flower model'. The heart of the flower is made up of government bodies, like the police, intelligence services, GOVCERT.NL and the NICC. They meet with participants from the critical industry sectors every two months. Meeting face-to-face, a trusted community is built. Five sectors (financial institutions, drinking water, gas/electricity, Amsterdam airport and multinationals) are currently working together in the Information Exchange. Several others are either being established or at the preparation stage, such as the railway and telecommunications sectors and the Port of Rotterdam.

In addition, there is a thematic 'petal' on process control security, represented by SCADA (Supervisory Control And Data Acquisition) systems and EuroSCSIE, the European SCADA and Control Systems Information Exchange. Confidential and mutually beneficial information about electronic security threats, vulnerabilities, incidents and solutions in the process control environment is shared in these meetings. This theme extends across all industries.



Address

Wilhelmina van Pruysenweg 104 / 2595 AN The Hague
P.O. Box 84011 / 2508 AA The Hague
The Netherlands
www.samentagencycybercrime.nl

Research, trials and pilot studies

The National Infrastructure grows through research, trials and evaluation projects. Such projects focus on a specific problem area in the public or private sector, while at the same time generating knowledge about cybercrime and providing a greater understanding of the 'blind spots' on the overall map of the National Infrastructure. This enhanced knowledge in turn leads to the generation of further creative projects.

The NICC has conducted research amongst small and medium-sized enterprises (SMEs) and trials and evaluation projects at schools and with municipal authorities. It is also in the process of aligning Notice and Takedown procedures.

International partnerships

Cybercrime is an international phenomenon, and knows no borders. Cybercriminals typically operate in countries where they are least likely to be thwarted by legislation and enforcement. International exchange and cooperation is the only way to fight cybercrime effectively, via national organizations or programmes like the National Infrastructure against Cybercrime.

The NICC therefore actively engages in international partnerships in order to be connected as closely as possible to organizations and programmes in other countries. These include the pan-European programmes launched by Franco Frattini, the EU Commissioner responsible for Justice, Freedom and Security, the European SCADA Platform and the London Action Plan (LAP).

The NICC programme is temporary and will be operational until mid-2009. The National Infrastructure against Cybercrime itself, however, will remain.

