National Cyber Security Centre
Ministry of Justice and Security

NCSC Research Agenda

2019 - 2022

Introduction

The mission of the National Cyber Security Centre (NCSC) is to *understand* the vulnerabilities and threats in the digital domain. Furthermore, we aim to *connect* parties, knowledge and information. The third part of our mission is to *prevent* societal damage and mitigate threats. The NCSC research cluster contributes to these goals by evaluating scientific innovations and by defining relevant research questions.

The 2019-2022 Research Agenda follows from our research ambitions[1]. In this Research Agenda we highlight several themes that form the foundation to engage in the cybersecurity debate in The Netherlands. We use the Research Agenda as a guide to define research questions, to decide on participation in projects, or to carry out our own research. Our team aims to balance between fundamental cybersecurity research, applied research, and research to make The Netherlands more secure.

Themes

The Research Agenda features four themes:

- Crisis management (warm phase)
- Risk management (cold phase)
- Strategic and social aspects of cybersecurity (broad view)
- Technology and cybersecurity (technological innovations)

The concepts *understand*, *connect*, and *prevent*, apply to each of the research themes. However, each theme corresponds to different areas of NCSC's mission. In this document we describe those themes and their related subthemes, and illustrate them with examples of indicative research questions.

Background

The Research Agenda was created in four steps. First, we defined the scope and carried out desk research. Following the results of the analysis we developed an initial version. Subsequently, we held a series of interviews with internal and external experts that led to the final version. The process is described in more detail in Appendix 1.

Next steps

The Research Agenda puts the 2019 Research Vision[2] into practice. It enables us to translate the Dutch Cyber Security Agenda (NCSA: *Nederlandse Cyber Security Agenda*)[3], the National Cyber Security Research Agenda (NCSRA)[4], and the findings from the annual Cyber Security Assessment Netherlands into action. The research agenda is reviewed annually in light of the insights gained in the preceding year. We may decide to stop a research direction or to enhance and broaden a topic. We decide this based on the evaluation of preceding research results and on the trends described in the annual Cyber Security Assessment Netherlands.

Once the priorities are set we work with colleagues and other stakeholders to formulate research questions. The research is done by external research institutions or by our own internal researchers. Where relevant, we will share the results with our target groups in (academic) publications or at conferences.

The NCSC research cluster has the following assignments:

- To generate relevant research questions for launching projects with research institutions such as TNO (the Netherlands Organisation for Applied Scientific Research) or the WODC (Research and Documentation Centre).
- To take part in relevant research projects with national and international academic partners.
- To map out the course for our own research activities, with the potential for related secondment and doctoral studies opportunities.
- To share knowledge through mentoring graduating students and PhD candidates and to organise lectures.
- To assess research proposals submitted following calls for projects in which the NCSC is engaged.

Structure of the 2019-2022 NCSC Research Agenda

Each chapter in this document explains the scope of a research theme. We have formulated potential research questions for illustration purposes only. They form the inspiration for further exploration of sub-themes. Despite the close connection and maybe even some overlap between the themes and research questions, we aim to approach the research topics from different perspectives.

1. Crisis management

Primarily a crisis preparedness and response organisation, crisis management is central to the NCSC's work. Supplementary to its crisis management activities at the NCTV, the NCSC examines specific cybersecurity aspects in crisis management. The ongoing survey of communication activities at Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) shows that there is potential for improvement, particularly in terms of increasing the resilience of organisations. In addition, we observe considerable development on topics such as the impact of the GDPR on CERT communication, CERT maturity models, and international collaboration.

This theme connects primarily to the mission to prevent societal damage and to improve resilience by contributing to the (organisational) progress of crisis management. Collaboration with partner organisations and with organisations in the critical infrastructure is imperative to the maturity of crisis management.

Possible research questions

- What are best practices for to CSIRT communication?
- What are the key success factors to collaboration within a sector or supply chain?
- How to narrow the gap between academic research and practical CSIRT communication?
- How can capability models such as the CTI capability model be applied at CSIRTs in the Netherlands?

1.1 Communication between CERTs and CSIRTs / Maturity Models

Communication within and between CSIRTs is key for the NCSC to further improve its performance. The NCSC's target groups host multiple communication channels that are crucial for the resilience of Dutch society, with examples including EGC, MISP, o-irt-o, the ISACs and, the National Detection Network (NDN). The developments in these bodies are important. Practical experience shows a need for greater knowledge about best practices, the impact of developments such as the GDPR and how models can be applied. One example is the CTI capability model. With regard to this topic, the NCSC is uniquely equipped to organise workshops with stakeholders, to share experiences and to provide access to the NCSC network.

1.2 Resilience

In the field of cybersecurity, it is generally accepted that organisations do not work on the premise of whether you are vulnerable, but when you will be hit in an attack. It is important, therefore, not just to focus on security measures, but also to consider additional measures for an organisation's resilience and incident response mechanism. Exploratory analysis could be conducted of the factors and circumstances that play a role in the resilience of organisations following a cyber-related incident. This can also include consideration of the possible overlap or differences with traditional forms of resilience.

Possible research questions

- To what extent can resilience be measured?
- How can an organisation's resilience be increased?
- What types of measures (broadly) contribute to resilience?
- How can organisations collaborate to increase their resilience?

2. Risk management

Risk management of business processes by means of ICT security is a key factor in safeguarding the security of the Netherlands' critical infrastructure. What could be effective ways to streamline and improve ICT security? Research could help to provide insight into risks and dependencies between organisations and their ICT service providers. Furthermore, we recognise the need for research into the relationship between cyber risk management and other forms of risk management, such as financial risk management.

Risk management is related to the mission statements understand and prevent. Risk identification and mitigation prevent damage and impact. It is important that this is done as effectively as possible within the NCSC as well as within our target groups (critical providers and government bodies).

2.1 Protecting energy networks / water infrastructure management

The aim of this sub-theme is to shed light on the status of the protection of critical infrastructures and sub-topics in this sector. Internationally, energy networks already attract considerable attention, but critical water infrastructure management systems (flood defences, sluice gates, bridges, tunnels) are unique to the Netherlands. The NCSC has previously assisted and supported research into these systems. Our risk management analysis will therefore focus chiefly on these two sectors.

The Netherlands Court of Audit has concluded that the Minister of Infrastructure and Water Management still needs to make progress if she is to meet her own cybersecurity targets[4]. The NCSC requires better insight into specific vulnerabilities in ICS/SCADA systems and the security characteristics of the networks in which such systems are deployed. We also wish to know what the success factors for OT security are in relation to resilience and how organisations can improve the maintenance processes for ICS/SCADA systems. This provides insights into the level of protection, while also allowing the NCSC to enhance its knowledge of ICS/SCADA systems.

Possible research questions

- What role do human factors play in dealing with and assessing cyber risks?
- How can the complex body of information be made accessible to policymakers?
- What are the key success factors for the maturity of OT security in organisations?
- How can the division and overlap in security management processes in both critical and non-critical infrastructures be utilised more effectively, on a sector-by-sector basis?
- How can patch management be better deployed in existing systems so as to make them less vulnerable?
- How can organisations utilise the different types of 'testing' more effectively?
- How can risk management be effectively deployed in ICS/SCADA environments?
- To what extent can existing risk management models be applied to ICS/SCADA environments?

2.2 Quantification of cyber risks and damage

Within organisations, support for investment in digital security should not be taken for granted. The ability to quantify the potential risks and associated loss or damage may help to make the case for cybersecurity. Information on the quantification of cyber risks can also be a useful tool in drafting the Cyber Security Assessment Netherlands. Information about cyber risks has increased exponentially in recent years and comparative analysis of data from other countries within or outside of the EU would be interesting. This creates a need to enhance our understanding of the complexity and interconnections and apply the results in organisations. While cyber risks have the potential to impact multiple areas, all too often cybersecurity risk management is not linked in any way with risk management in other fields. At the same time, the heavy reliance on ICT products from suppliers in foreign countries is increasingly being questioned.

Possible research questions

- What does a sound and systematic quantitative risk analysis look like?
- How can cybersecurity risk management be integrated in overall risk management?
- What are the differences and similarities between Member States regarding the regulations of cyber risks and loss or damage?
- How can historical data about cyber risks be systematically analysed and quantified in a substantiated manner?
- To what extent can businesses and insurers contribute to the systematic analysis and substantiated quantification of historical data?
- To what extent has 'traditional' loss or damage shifted toward the cybersecurity domain?

2.3 Supply chain risk

ICT services are becoming increasingly important and are provided in a network of organisations. Exactly which organisations and processes rely on one another? Organisations purchase ICT as a service or depend on others for the provision of these critical services on their behalf. Organisations increasingly depend on a network of providers for their continuity and security (and may or may not have a contract with those providers). The management, and risk management in particular, of all these dependencies throughout the chain is becoming more and more important.

Analysis of dependencies within chains has previously been conducted in specific environments, including the Port of Rotterdam and Amsterdam Airport Schiphol. Experiences from these processes can help to formulate considerations at a more general level or to yield new research questions, potentially enabling us to produce generic advice or recommendations for our target group. Other developments, such as the Software Bill of Materials (SBOM), help us identify these dependencies more effectively.

Possible research questions

- What methods are available for identifying supply chain risks with devices, applications, platforms, networks, or services in the critical infrastructure and what results do these methods deliver?
- How can SBOM be used to reveal vulnerabilities in the critical infrastructure?
- How can cyber risks associated with reliance on service providers be identified and understood?

3. Strategic and social aspects of cybersecurity

Cybersecurity is a complex field, and efforts to increase the resilience of the Netherlands depend on a variety of social, economic, political and administrative processes. By analysing the cybersecurity aspects in these processes, the NCSC will be able to enhance its role as a crisis and response organisation and improve its position within the network. There has been a growing awareness in recent years that cybersecurity is a multi-disciplinary field that covers more than just technical solutions. Increasing resilience, for instance, depends on improved organisational processes and international collaboration. The sub-themes below deal with governance issues, secure actions by end users, capacity building for the NCSC and the role of ethics within cybersecurity.

By *connecting* in the right way, the NCSC is able to contribute effectively to digital security. At the same time it is important to *understand* how social processes contribute to threats and vulnerabilities. Simultaneously, social processes can also be a means to control threats and to *prevent* damage.

3.1 Cybersecurity governance

Cybersecurity governance concerns the administration and management of cybersecurity at state level and organisation level. However, it also encompasses national and international cybersecurity networks, partnerships and alliances. Domestic and international laws and regulations are an important aspect of this. There is a growing need among different parts of the NCSC for a greater understanding of the processes that influence its work. Effective collaboration within (transnational) multilateral organisations such as ICANN, RIPE and IETF is essential. Topics that contribute to this are analysis of national and international collaboration between CERTs, the legal restrictions on collecting and sharing incident data, and the role of economic security in the cybersecurity arena.

Possible research questions

- How can international collaboration between CERTs be further improved?
- What role do non-technical influences such as economic security play in the cyber domain?
- How can trust between national and international actors in the cyber domain be further improved?
- What are the legal restrictions and possibilities for sharing data to enable the implementation of an effective cybersecurity policy?
- Which roles within an organisation are relevant for ensuring cybersecurity is effectively structured and implemented, and what are the difficulties in fulfilling these roles?

3.2 Enabling end users to act more securely

Awareness training has been a priority for years. However, we now know from practical experience that while raising awareness may help, it does not completely solve the problem. This sub-theme examines additional solutions, such as analysis of alternative incentives or improved user interface design.

Possible research questions

- Which organisational and/or economic incentives are available to organisations for increasing security?
- Which resources present the greatest threat for end users (smartphone, email, apps), and how can they be made more resilient?
- How can cybersecurity risks be effectively communicated by the systems and devices themselves?
- Where does information tend to be misunderstood, and how can communication about cyber risks be adapted to the user's level of knowledge?
- What measures can be taken to combat disinformation about ICT security at end users?

3.3 Capacity building

The shortage of cybersecurity experts, by no means recent phenomenon, is also noticeable within the NCSC. Multidisciplinary exploratory analysis can focus on the opportunities for increasing the number of cybersecurity experts in the Netherlands, for example by examining success factors and potential training and retraining programmes such as Life-Long Learning. Other possible topics include comparative research of data from other countries (within and outside of the EU) with regard to capacity building, and an inventory of the competences that will be needed in the cybersecurity field in 2025.

Researchers state that a diverse workforce contributes to more effective collaboration in teams and organisations. The diversity within the cybersecurity workforce is lagging behind and even dimishing. What is the effect on the digital security of the Netherlands, within the NCSC, and within our target groups?

Possible research questions

- What role do organisations similar to the NCSC in other countries and Member States play in relation to capacity building?
- Which roles and tasks in the cyber domain will, or might, disappear in the future due to innovations such as artificial intelligence?
- How do other countries in the EU and elsewhere organise capacity building and what valuable lessons can be drawn by the NCSC and/or the Netherlands?
- Which best practices can the NCSC learn from other organisations, and how should those practices be adapted for the NCSC?
- To what extent do roles and functions of the NCSC match those of other cyber-related government departments?
- How can the NCSC contribute to an inclusive and more diverse community of cybersecurity specialists?
- How to retain people and how to deploy them more effectively?
- What barriers to joining the profession exist in the Netherlands? And how can they be removed?
- Which competences are currently being instilled in education and which competences will cybersecurity experts need by 2025?

3.4 Ethics within cyber security

There is a growing awareness within the NCSC of potential conflicts of interest between ethics and incident response capability. The public debate is increasingly focused on ethical aspects of artificial intelligence, social media and other ICT applications. How can organisations deal with dilemmas in this field, and how do science and academia study them?

Possible research questions

- What are the ethical dilemmas facing the NCSC, now and in the future?
- What solutions can be proposed for dealing with ethical dilemmas?
- What ethical guidelines are available for security screening and controls, for example as applied within ethical committees? To what extent can they be adopted by the NCSC?
- What are the ethical limits of vulnerability disclosure?
- How does vulnerability disclosure change in the case of multi-vendor coordination processes?

4. Technology and cybersecurity

The pace of technological development in the cybersecurity field is rapid. Both the academic world and the business community are seeing major investments in research and development of artificial intelligence (AI) and the security of the Internet of Things (IoT). At the same time, strengthening resilience calls for a review of product development processes to ensure that security considerations are firmly embedded within them. While these developments can improve the operations of the NCSC, they also present threats and opportunities to our target groups.

Keeping track of technological innovations is essential to understand digital vulnerabilities. Technology is means to effectively connect organisations, knowledge, and information. Developments in technology also provide for new measure to prevent damage.

4.1 Privacy by Design

The NCSC also focuses on preventive measures, from the privacy perspective of 'You can't lose what you don't have'. An emerging topic in this field is privacy-by-design, and in this context our main focus is on big data analysis, machine learning and AI applications with significant demand for data. We are also examining the privacy aspects of sharing data, by the NCSC or others, with the primary focus on technical measures, although organisational measures are also considered.

Possible research questions

- How can big data analysis and privacy-by-design be reconciled?
- Which privacy models and methods are available for sharing incident data and information within the National Detection Network (NDN)?
- What are the features of the market development of privacy-friendly products? Do those products have a competitive advantage?
- Which developments in Privacy-Enhancing Technologies (PETs) increase the security of data sharing?
- What will the business model of software (as a service) look like in the future, and what impact will this have on data control?
- Which standard protocols or middleware exist or can be developed to achieve privacy-by-design for today's legacy systems, such as email, diaries/calendars, etc.? (It is a technical challenge to obtain IMAP, CALDAV, CARDDAV, etc. with client-side encryption, for instance.)

4.2 Internet of Things

The focus with regard to the Internet of Things (IoT) is on standardisation and certification, and the analysis of its status in the Netherlands. The NCSC has an interest in IoT-security in relation to the country's resilience. While studies have been carried out into IoT-related security risks for the critical infrastructure, there is a need for more and broader analysis to make those risks visible and measurable.

Possible research questions

- How can IoT-related cyber risks be made visible and measurable?
- What promising forms of certification and standards (e.g. SBOM and MUD) exist, and how can they be utilised for the country's critical infrastructure?
- Do we need certain levels of certification of critical and non-critical infrastructure? What is the financial impact?
- What are the IoT-related cybersecurity risks for the critical infrastructure?

4.3 Foundations of the Internet

The Internet is a clear example of a domain where security-by-design has not been applied. One result of this is that DDoS attacks pose a major threat to Dutch infrastructure, and one that is unlikely to disappear any time soon. Are there measures that can be taken to mitigate the impact of these types of attack, or is it possible to embrace a different design?

Possible research questions

- What effective and feasible measures are available in the foundations of the Internet itself for combating DDoS attacks?
- What other types of threat ensue from the present standards in the Internet?
- How can the Internet of the future contribute to enhancing Dutch digital security?
- How can parties be encouraged to strengthen the foundations of the Internet in terms of ICT security (open source community, Internet providers, Internet exchanges, public authorities, multilateral organisations)?

4.4 Artificial Intelligence for cybersecurity

Substantial investments are being made in AI, including, for instance, research into smart cars, image recognition and automated problem analysis. The potential of AI for cybersecurity is currently the subject of considerable debate. Nationally and internationally there is also growing attention for the implications of AI for the labour market, and for the role of ethics in AI. What is AI's added value for cybersecurity? Does it offer potential for use by NCSC, too? Given the many unknowns that still exist, there is a need for detailed analysis and exploratory study of the opportunities and threats of artificial intelligence.

Possible research questions

- How can we use AI, and what forms of AI should we use, to improve the current attack and defence techniques?
- What new modes of attack are enabled by AI?
- What are the vulnerabilities of AI?
- Which factors can help boost trust in the use of AI?
- What level of algorithmic accountability is required to enable responsible use of AI by non-technical persons?
- What measures are needed to develop inclusive and non-discriminatory AI and to prevent bias?

4.5 Forecasting

Forecasting is the ability of organisations to effectively anticipate the future. By comparing past experience with what we know today, it is possible to identify breaks with past trends in a timely manner and to alter course. The NCSC and its target groups have access to many subject-matter experts. However, effective forecasting also relies to a considerable extent on maintaining a broad outlook and by combining knowledge from different disciplines. How can we provide specialists and experts with the tools to develop this broad outlook?

Forecasting increases organisations' responsiveness and resilience and helps drive down costs. The NCSC already makes tools that enable analysis of future expectations. One example is the Cyber Security Radar, which was recently renamed the 'Cyber Compass'. The NCSC also participates in the current Cyber Forecasting Tournament, where forecasters learn to actively anticipate future developments. Research allows trend analyses to be improved and practical forecasting techniques to be selected. Trend analyses can also be enhanced by social science research into the human factors of cyber attacks, for instance by drawing up criminological profiles of perpetrators and their organisations.

Possible research questions

- How can a forecasting methodology be developed based on insights gained from tools such as the Cyber Radar/Cyber Compass and the Cyber Forecasting Tournament?
- Which forecasting techniques and tools are important for the NCSC and how can we further develop these?
- How can these forecasting techniques and tools be improved with knowledge about criminal activities?
- What are the anticipated trends for human factors that may play a role in future cyber attacks?
- How can historical/forensic data contribute to trend analysis?

References

1. National Cyber Security Centre (2018) Onderzoeksvisie 2019 [Research Vision 2019] [internal document]. The Hague.
2. National Coordinator for Security and Counterterrorism. Nederlandse Cybersecurity Agenda [Dutch National Cybersecurity Agenda]. The Hague. Consulted on 27 November 2018: https://www.nctv.nl/binaries/CSAgenda_def_web_tcm31-322330.pdf.
3. Dcypher (2018) National Cyber Security Research Agenda III. The Hague. Consulted on 6 May 2019: https://www.dcypher.nl/sites/default/files/uploads/documents/NCSRA-III_0.pdf.
4. National Coordinator for Security and Counterterrorism. Cyber Security Assessment Netherlands 2018. Available from: https://english.nctv.nl/topics/cyber-security-assessment-netherlands/documents/publications/2018/08/07/cyber-security-assessment-netherlands-2018.
5. Netherlands Court of Audit (2019) Digitale dijkverzwaring: cybersecurity en vitale waterwerken. [Digital dyke strengthening: cyber security and critical water defence works]. The Hague. Consulted on 2 May 2019: https://www.rekenkamer.nl/publicaties/rapporten/2019/03/28/digitale-dijkverzwaring-cybersecurity-en-vitale-waterwerken.

Annex 1: Method

The 2019-2022 NCSC Research Agenda was created by following four steps:

1. **Define scope and desk research**: The first step was to define the scope of the research agenda. In principle, that scope was determined by the NCSC Research Agenda, the Cyber Security Radar, the Cyber Security Assessment Netherlands, as well as by the legal remit of the NCSC. In a parallel exercise, desk research was carried out to compare the scope with that of similar agenda's in other EU Member States (UK, DE, DK, BE), the United States, and international organisations (EU, ENISA, NATO, OSCE, Interpol, OECD, UN). The documents used in this desk research are listed below.
2. **Analysis and development of initial version**: The results of the desk research were compared with the NCSC's mission. The qualitative analysis looked at similarities and differences in focus areas, objectives and priorities. The scope of the research agenda was extended to reflect the national priorities and focus of the NCSC. Based on the above analysis, the initial draft was written.
3. **Collecting input from internal and external experts**: Interviews were held with internal and external cybersecurity experts in order to triangulate and validate earlier findings within the NCSC network. The interviews contributed to the evaluation of the research themes.
4. **Fine-tuning and development of final version**: The final version of the research agenda was drawn up based on all the findings from the desk research and the interviews.

Desk research references

Danish Ministry of Finance (2018) 'Danish Cyber and Information Security Strategy'. The Danish Government, Ministry of Finance. Copenhagen.

Danish Agency for Science and Higher Education (2018) 'Research 2025'. *Danish Government, Ministry of Education and Science*. Accessed 9 April 2019 from https://ufm.dk/en/publications/2018/research2025-catalogue.

Dcypher (2018) 'National Cyber Security Research Agenda'. Herbert Bos, Michel van Eeten, Sandro Etalle, Frank Fransen, Jaap Henk Hoepman, Erik Poll, Jan Piet Barthel (eds). The Hague.

Di Franco, F (2018) 'Analysis of the European R&D priorities in cybersecurity: Strategic priorities in cybersecurity for a safer Europe'. *European Union Agency for Network and Information Security (ENISA)*, doi:10.2824/14357. Athens.

German Federal Ministry of Education and Research (2015) 'Self-determined and secure in the digital world 2015-2020: The German government's research framework programme on IT security'. Federal Ministry of Education and Research (BMBF) Division Communication Systems, IT Security. Bonn.

Kenneally, E Randazzese, L and Balenson, D (2018) 'Cyber Risk Economics Capability Gaps Research Strategy'. *United States Department of Homeland Security, Science and Technology Directorate*, doi: 10.23721/1460960.

National Coordinator for Security and Counterterrorism (2018) The Netherlands Cyber Security Policy 2018. *Ministry of Justice and Security – National Coordinator for Security and Counterterrorism (NCTV)*, June, The Hague.

National Cyber Security Centre of the Netherlands (2018) *Cyber Security Radar.* Report of the National Cyber Security Centre, July, The Hague.

National Cyber Security Centre United Kingdom (2018) NCSC Annual Review. Accessed 9 April 2019 from https://www.ncsc.gov.uk/annual-review-2018.

North Atlantic Treaty Organization (2019) NATO Cyber Defence factsheet. Accessed 11 April 2019 from: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf.

Organisation for Economic Cooperation and Development (2015), Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264245471-en

Organisation for Economic Cooperation and Development (2019) 'Policies for the Protection of Critical Information Infrastructure: Ten Years Later'. *OECD Digital Economy Papers*.

Organisation for Economic Cooperation and Development (2019) 'Draft OECD Recommendation on Digital Security of Critical Activities' OECD Directorate for Science, Technology and Innovation / Division for Digital Economy Policy. Accessed 11 April 2019 http://www.oecd.org/sti/ieconomy/digital-security-of-critical-activities.htm.

Organization for Security and Co-operation in Europe (2016) 'OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies', PC. DEC/1202, 10.

Rothenpieler, S (2017) 'National Cyber Security Strategy 2016'. *Federal Office for Information Security (BSI)* [presentation]. ENISA April 26, 2017, Athens.

United States Department of Homeland Security (2018) 'Cybersecurity Strategy'. United States Department of Homeland Security. NATO Public Diplomacy Division.

Publication
National Cyber
Security Centre (NCSC)
P.O. Box 117, 2501 CC The Hague
Turfmarkt 147, 2511 DP The Hague
+31 (0)70 751 5555

More information
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

January 2020