Opportunities and obstacles for the Dutch cybersecurity sector in southern Germany

Objective
The Netherlands and Germany both have clear cybersecurity ambitions. Due to the digital transformation in service provision, there is an increasing demand for secure digital production processes and data-sharing within both government and industry. The German cybersecurity market is highly competitive and German customers often prefer to use local parties. Despite this, customers in Germany still look to the international market for specific knowledge and expertise, for instance in the areas of defence, information security management systems (ISMS) and interaction between people, organisations and technology (source: Die Lage der IT-Sicherheit in Deutschland 2019 (The State of IT Security in Germany 2019)). The Dutch cybersecurity ecosystem has the expertise to provide this knowledge and know-how, while also requiring knowledge and know-how from Germany. Discussions with businesses during company visits or trade fairs, for instance, have shown that there is a need for more information on the cybersecurity opportunities in southern Germany and for additional support in establishing contacts there.

Market study
In order to gain a clear insight into the opportunities for Dutch cybersecurity parties in southern Germany (Bavaria and Baden-Württemberg), the consulate-general in Munich, together with the Netherlands Enterprise Agency (RVO.nl) wishes to commission a market study that aligns with the relevant economic work plan and the strategic internationalisation agenda for ICT in Germany. This market study should list the possibilities for knowledge-intensive cooperation as well as market opportunities. This study will allow the needs of Dutch cybersecurity parties in southern Germany to be identified, as well as providing insight into possibilities for knowledge-intensive cooperation, market opportunities, limitations and challenges and suggestions as to how Dutch cybersecurity SMEs can best be promoted in southern Germany.

Research question
How can economic cooperation between southern Germany and innovative Dutch companies and knowledge institutions in the area of cybersecurity be strengthened?

Anticipated outcomes
In seeking to respond to the question above, the market study must also answer the following questions:

- Where do opportunities exist for Dutch cybersecurity companies and knowledge institutions in southern German industry? Which sectors and sub-sectors are relevant for the various Dutch cybersecurity solutions?
- What are the needs of Dutch cybersecurity businesses and knowledge institutions when entering the southern German market?
- What issues and obstacles exist for Dutch cybersecurity SMEs within southern German industry?
- What issues and obstacles exist for Dutch cybersecurity knowledge institutions in terms of establishing contact with their southern German counterparts?
- What legislation, guidelines and standards are important within this market?
- Which cybersecurity research and business clusters in southern Germany can Dutch parties work with/join?
- How can we best promote the Dutch cybersecurity sector/Dutch cybersecurity solutions in southern Germany?
- Who are the main cybersecurity players in southern Germany and what are the potential investments?

End product
The market study must provide Dutch cybersecurity companies with a clear insight into the characteristics of and opportunities for the Dutch cybersecurity sector in southern Germany. The resulting report will be made available to interested Dutch companies (SMEs), local, regional and provincial authorities, clusters, Regional Development Agencies (ROMs) and knowledge institutions, so that they can explore opportunities in this market and develop follow-up activities.

The results will be presented in the first quarter of 2020. In the Netherlands, this will be done by way of an opportunity seminar, while in Germany it will possibly be done during the King's Day celebration in Munich. If there is sufficient interest from the Dutch side, trade and innovation missions can be organised from Germany to the Netherlands and vice versa. The primary goal over

several years is to offer guidance to individual companies and use available Netherlands Enterprise Agency (RVO.nl) instruments (including the Partners for International Business (PIB) programme) to create clusters of businesses and knowledge institutions.

The report must be written in easily understood English; this being the responsibility of the party conducting the study.

Schedule and reporting
Once the contract has been awarded, desk research and interviews with major stakeholders in the Netherlands and southern Germany should be conducted over a period of six weeks. Two weeks before the deadline the contractor should submit a draft report to the consulate-general in Munich. The contractor will then have one week to incorporate the consulate-general's feedback into the final report.

Delivery
The final report should be delivered electronically to RVO.nl. RVO.nl and the consulate-general in Munich will hold exclusive copyright on the research and are the only organisations that may copy the report and disseminate the results.

Budget
A maximum of €20,000, including VAT.

Contact
Marlou Peters, Economic officer, Consulate General in Munich (marlou.peters@minbuza.nl or +49 892 0602 6728)

Annexe
- Background information

Introduction and background

Cybersecurity is a top priority, both for the private sector and for government, in southern Germany and the Netherlands. This is why in the coalition agreement the Dutch government set out a structural investment of €95 million in cybersecurity. The establishment of the Cyber Security Council, the Digital Trust Center, The Hague Security Delta, the National Cybersecurity Agenda (NCSA) and other, regional initiatives also show how high a priority cybersecurity is for the Netherlands.

From 2018 to 2022 Bavaria is investing a total of €3 billion in its digital future. The BAYERN DIGITAL II master plan sets out cybersecurity as one of the main pillars of digitalisation. Through the establishment of the Landesamt für Sicherheit in der Informationstechnik (State Office for Security in Information Technology) in Nuremberg, the Bundeswehr University Munich CODE research institute and the expansion of the Cyber-Allianz-Zentrum Bayern (Bavarian Cyber Alliance Centre) and Zentralstelle Cybercrime Bayern, Bavaria aims to become a leader in cybersecurity. Baden-Württemberg is also making significant investments in cybersecurity. Between 2016 and 2020 a total of €1 billion is being invested in digitalisation to enable the state to achieve its aim of becoming the lead region in digitalisation. In 2017 Baden-Württemberg developed the *digital@bw* digitalisation strategy, which contained a significant number of tangible, innovative projects and measures, including in the area of cybersecurity. Examples include the Zentrale Ansprechstellen Cybercrime and the Cyberwehr.

Recent research

Research carried out by Technopolis in 2019 on innovation and trade opportunities for the Dutch ICT sector in Germany included a quick scan of German and Dutch strengths, weaknesses and opportunities (including for export) in the area of cybersecurity. This quick scan showed that the Netherlands and Germany both have clear ambitions when it comes to cybersecurity and that both sides are interested in working together. Dutch SMEs already offer specialised products and services in Germany, in areas such as personal data protection and dark web analysis. Products or services that protect companies from cyberattacks are still needed on the German market, however. At present, there are a limited number of comprehensive yet cost-effective solutions. In addition, southern German SMEs are still considerably less advanced in terms of security for their systems, including production systems (source: Germany Trade & Invest (GTAI), German Software and Cybersecurity Landscape 2019).

Dutch offering and interests

The Netherlands is one of the most digitally advanced countries in the world. This places us in an excellent position to be an international trailblazer, as well as to roll out and use new technologies quickly, freely and securely. In economic terms, at least 30% of growth in the Netherlands (and in other developed countries) is due to IT and its use. The Netherlands invests around €14 billion annually in IT services and products. In the EU, the added value of IT is €600 billion and companies invest a quarter of their research and innovation budget in IT; a total of €29 billion (source: Knowledge and Innovation Agenda 2018-2021).

A high level of digitalisation and excellent internet connections means that the Netherlands has built a very strong cybersecurity sector. At international level too, the Netherlands has made a name for itself as a renowned and recognised partner and authority in the area of cybersecurity. The Netherlands can benefit from this position in Germany, which is less digitally advanced.

The field comprises a relatively small group of 'real' cybersecurity companies. Often, these are SMEs with a strong reputation in specialised solutions. It is unclear exactly how big the market is for cybersecurity service providers but it is estimated that there are around 250 companies offering such services in the Netherlands. This includes companies that focus solely on cybersecurity, as well as companies that offer cybersecurity products and services as part of a wider portfolio. However, it excludes the large number of self-employed persons offering such products and services. According to the cybersecurity industry association Cyberveilig Nederland, cybersecurity is a growth sector dominated by SMEs. Research by Technopolis shows that the Dutch cybersecurity sector particularly excels in the area of smart grids and security relating to vital infrastructure, attacks, defence and security by design.

In the Netherlands, public-private partnerships help raise awareness and promote the development of new technologies. Examples include The Hague Security Delta, InnovationQuarter (the regional economic development agency for the greater Rotterdam-The Hague area), the Cyber Resilience Centre in Eindhoven and The Garden – the Smart Industry Field Lab in Hengelo.

One of the key themes of the National Cybersecurity Agenda is that the Netherlands wants to lead the way in the development of cybersecurity knowledge. Dutch cybersecurity research is both international and high quality in nature. Experiments and innovations are taking place in a range of labs in areas such as attacks, defence and design.

In 2019 Technopolis carried out a SWOT analysis of the Dutch cybersecurity sector.

Strengths	**Weaknesses**
Public-private partnerships Smart grids Vital infrastructure Attacks Defence and design Research	Lack of talent Knowledge valorisation Small domestic market
Opportunities	**Threats**
Specialist/niche solutions	International acquisitions

German offering and interests

The demand for technologies and solutions to improve IT security in Germany is bigger than ever: in 2019 German companies are expected to spend €4.6 billion on hardware, software and services within the cybersecurity sector. This is a record high and 10% more than in 2018, which was already a record-breaking year (source: Bitkom). In 2018 turnover growth in cybersecurity solutions was around 9%, which was five times stronger than the German economy's growth as a whole. In 2018 Germany made around €4.2 billion in the cybersecurity sector. This makes Germany Europe's second biggest cybersecurity market after the United Kingdom (source: Bitkom Research, Studienbericht 2018). In 2020 further growth of 7.5% is expected on the 2019 figure, taking total turnover to €4.9 billion. The German cybersecurity market has an extremely strong predicted average growth rate of 9.2% for the period 2016 to 2021. This is the highest in Europe (source: Bitkom).

Spending on cybersecurity services in Germany for 2019 is expected to total €2.4 billion (53% of the total cybersecurity market), an increase of 10.2%. In addition, companies in Germany are expected to spend €1.4 billion on cybersecurity software, 9.9% more than in the previous year. Spending on equipment and hardware is expected to total €780 million, a 9.6% increase (source: Bitkom). The highest growth is expected in the care and financial sectors, where large amounts of personal data are processed. The German market is a mature one with lots of competition from a large number of cybersecurity companies.

The same report by Technopolis also contained a SWOT analysis for the German cybersecurity sector.

Strengths	**Weaknesses**
Large number of investment companies Large internal market Growth market Critical infrastructure Cryptography Embedded systems Internet of Things (IoT) Research	Lack of talent Knowledge valorisation
Opportunities	**Threats**
Care and financial sectors Industry 4.0	Preference for local parties

Research in innovation
To stimulate innovation and offer access to financing, €15 billion in research funding has been made available for specific areas of cybersecurity. A range of research institutions and public stakeholders are carrying out cybersecurity research. Three centres of expertise for IT security research have been set up by the Federal Ministry of Education and Research: the National Research Center for Applied Cybersecurity (ATHENE) in Darmstadt, the Helmholtz Center for Information Security (CISPA) in Saarbrücken and the Competence Center for Applied Security Technology (KASTEL) in Karlsruhe. CISPA already has a partnership with the Dutch organisation dcypher, with both organisations signing a declaration of intent during the royal visit to Saarland in 2018.

Cybersecurity clusters with various specialisations are spread throughout the country. Examples include the Bavarian IT Security Cluster, Security Network Munich, IoT Security Cluster for North Rhine-Westphalia and the Fraunhofer Urban Security Cluster. There is expertise in the areas of cryptography, embedded systems and IoT. German expertise in protecting critical infrastructure has been stimulated through the introduction of the IT Security Act (IT-Sicherheitsgesetz) in 2015, which is comparable to the EU NIS Directive 2016. In addition, the TeleTrusT partnership is active at national level, looking for new links in international markets, including in the Netherlands.

The costs of attacks
Attacks on companies are responsible for record financial losses in Germany. Sabotage, data theft and espionage cost the Germany economy €102.9 billion annually. This includes both digital and analogue attacks. This figure is almost twice as high as two years ago, in 2016/2017, when the annual total was €55 billion. Three quarters of companies have been affected by an attack in the past two years. Of the remainder, 13% suspect they have been affected. In 2016/2017, only one in two (53%) businesses fell victim (source: Bitkom).

Demand for cybersecurity solutions
Domestic demand for cybersecurity solutions continues to rise. Changing legislation, growing awareness of cyberthreats and an increase in digital business strategies mean that companies are continuing to spend more and more on cybersecurity solutions.

Many German businesses, especially SMEs, are only just starting the digital transformation process, which means that the demand for cybersecurity solutions will continue to increase with time. Significant cybersecurity opportunities exist in the manufacturing sector, given that industrial production is enthusiastically adopting digitalisation. The digital transformation of German industry, smart and autonomous driving concepts and the secure management of data that are needed for online transactions are indeed the driving force behind the demand for cybersecurity in Germany (source: GTAI, German Software and Cybersecurity Landscape 2019).

Southern Germany
Southern Germany is responsible for more than 40% of Germany's total Gross Domestic Product (GDP), and the industrial sector (i.e. the main user of cybersecurity applications) is located primarily in the states of Bavaria and Baden-Württemberg. The region is home to the highest levels of economic growth and the lowest levels of unemployment. In addition, the investment ratio is higher than average and twice as many patents are applied for than the German average. Furthermore, the four themes for public-private partnerships, as designated by the International Enterprise Department (DIO) (smart industry, mobility, health and energy) are concentrated primarily in this region. Finally, the Netherlands is missing out on a lot of opportunities in southern Germany, with a market share of only 7%, compared to a 9% market share in the German market as a whole.