

# DUTCH INVESTMENTS IN ICT AND CYBERSECURITY

PUTTING IT IN PERSPECTIVE





HCSS helps governments, non-governmental organizations and the private sector to understand the fast-changing environment and seeks to anticipate the challenges of the future with practical policy solutions and advice.

This report is from the HCSS theme SECURITY. Our other themes are GEO-ECONOMICS and GLOBAL TRENDS.

## SECURITY

HCSS identifies and analyzes the developments that shape our security environment. We show the intricate and dynamic relations between political, military, economic, social, environmental, and technological drivers that shape policy space. Our strengths are a unique methodological base, deep domain knowledge and an extensive international network of partners.

HCSS assists in formulating and evaluating policy options on the basis of an integrated approach to security challenges and security solutions.



## DUTCH INVESTMENTS IN ICT AND CYBERSECURITY PUTTING IT IN PERSPECTIVE

*The Hague Centre for Strategic Studies*

ISBN/EAN: 978-94-92102-44-7

**AUTHORS** Michel Rademaker, Louk Faesen, Koen van Lieshout, Mercedes Abdalla

This research is directed to the National Cyber Testbed Initiative of The Hague Security Delta (December 2016).

**DISCLAIMER** This report used only publicly available sources and data, preventing it from giving absolute numbers and findings. Determining the size of channeled funds and investments of ICT and cybersecurity is challenging because: (i) of the lack of reliable and consistent reporting and data sets; (ii) the absence of a unified definition of cybersecurity, which makes it difficult to delineate which costs are specifically attributed to cybersecurity per se; (iii) cybersecurity is increasingly evolving into the integral part of business operations – rather than being a separate unit costs; (iv) collecting and mapping the data of ICT and cybersecurity investments is generally complicated as cybersecurity is mostly approached qualitatively, and not primarily from a cost perspective.

© 2016 *The Hague* Centre for Strategic Studies. All rights reserved. No part of this report may be reproduced and/or published in any form by print, photo print, microfilm or any other means without previous written permission from the HCSS. All images are subject to the licenses of their respective owners.

**Graphic Design** Studio Maartje de Sonnaville, The Hague

*The Hague Centre for Strategic Studies*

Lange Voorhout 16  
2514 EE The Hague  
The Netherlands

info@hcss.nl  
HCSS.NL

# DUTCH INVESTMENTS IN ICT AND CYBERSECURITY

PUTTING IT IN PERSPECTIVE

*The Hague* Centre for Strategic Studies

# TABLE OF CONTENTS

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>Introduction</b>  | <b>9</b>  |
| <b>2</b> | <b>The Economics Behind it</b>   | <b>13</b> |
|          | 2.1 The Dutch digital economy  | 13        |
|          | 2.2 The Dutch ICT sector   | 14        |
| <b>3</b> | <b>ICT and Cybersecurity spending</b>                                  | <b>19</b> |
|          | 3.1 ICT investments  | 19        |
|          | 3.2 ICT expenditures   | 20        |
|          | 3.3 Government spending on cybersecurity                               | 20        |
|          | 3.4 Private sector spending on cybersecurity                           | 21        |
| <b>4</b> | <b>Meta-analysis estimating the Dutch cybersecurity market</b>         | <b>25</b> |
| <b>5</b> | <b>Awareness</b>   | <b>31</b> |
| <b>6</b> | <b>Education</b>   | <b>35</b> |
| <b>7</b> | <b>Scientific Research</b>   | <b>41</b> |
| <b>8</b> | <b>Key Takeaways</b>   | <b>45</b> |
|          | <b>Annex I – overview of cybersecurity programs in the Netherlands</b> | <b>51</b> |
|          | <b>Sources</b>   | <b>55</b> |

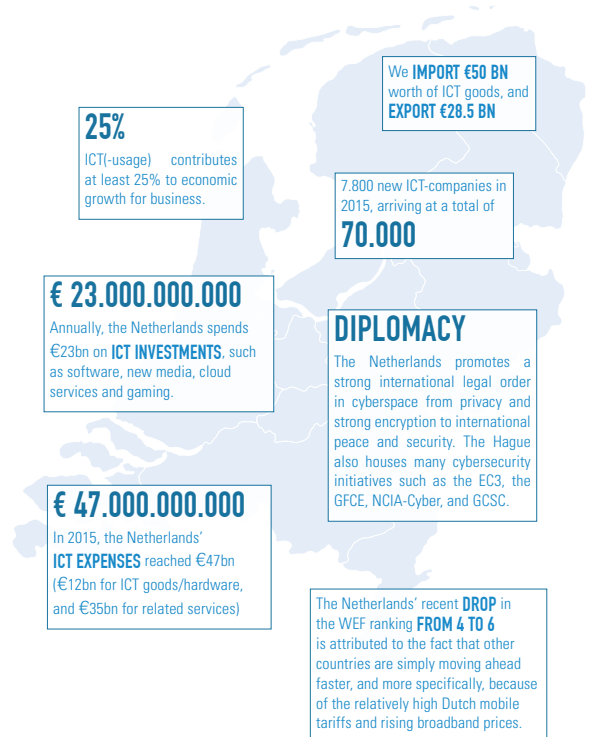
# 1 INTRODUCTION

# 1 INTRODUCTION

Digitalization has taken a predominant role in our everyday lives. The advent of networked technology has spurred innovation, cultivated knowledge, encouraged free expression, and increased our economic prosperity. The digital economy today permeates through different domains of the world economy, ranging from sectors such as banking and retail, to education and healthcare. The opportunities offered by the digital revolution and new technologies are regarded as the single most important drivers of innovation, competitiveness, and consequently, economic growth.<sup>1</sup>

The Netherlands considers itself one of the leading ICT countries, promotes itself as 'a safe place to do business' and aspires to be the digital gateway of Europe. But are we investing enough to match these ambitions and manage the risks?

In the advisory report presented to Dutch Prime Minister Rutte, Herna Verhagen, CEO of PostNL, urges the Dutch government, companies, and households to invest 10% of their annual ICT budget in cybersecurity. In her analysis, Verhagen presents a compelling overview of the current cyber threats, challenges and opportunities, and sets an ambitious goal, but does not provide any measureable benchmarks for the 10% norm, nor any insight into the current state of Dutch cybersecurity investments.



This report will first estimate the current and prospective size of the Dutch digital economy and the ICT sector, and later analyze how much the latter contributes to the national economy.

Next, we provide a holistic overview of the current level of public and private investments in cybersecurity, followed by an analysis estimating the Dutch cybersecurity market by comparing different studies.

Finally, the report gives an overview of the current state of affairs of awareness, education, and scientific research pertaining to cybersecurity in the Netherlands.

In the conclusion, we present the most important findings and assess how advanced the Netherlands is compared to the recently proposed norm that suggest governments, businesses and citizens alike should invest 10% of their ICT budget in cybersecurity.



# 2 THE ECONOMICS BEHIND IT

2.1 The Dutch digital economy

13

2.2 The Dutch ICT sector

14

# 2 THE ECONOMICS BEHIND IT

## 2.1 The Dutch digital economy

The digital economy is developing rapidly across the world. According to the analysis by Accenture Research and Oxford Economics, the digital economy accounted for 22,5% (€17.644bn) of the global economy in 2015 and is expected to rise to 25% (€22.669bn) by 2020. The share of the Dutch digital economy is similarly anticipated to increase. In 2015, its digital economy accounted for 22,9% (€158,01bn) of the total Dutch economy, and is projected to reach 25% (€190,4bn) by 2020.<sup>2</sup> According to the cross-country comparison in Figure 1 and Table 1, however, the Netherlands is still lagging behind other European countries, such as Germany, France, and the UK.

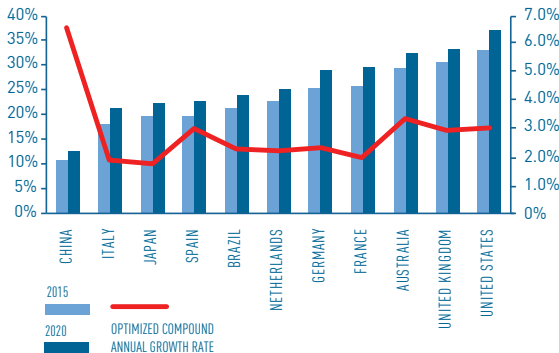


FIGURE 1 COUNTRY-BY-COUNTRY DIGITAL SHARE OF GROSS DOMESTIC PRODUCT (2015-2020) SHOWING COMPOUND ANNUAL GROWTH RATE UNDER THE OPTIMAL SCENARIO (RIGHT HAND AXIS). SOURCE: ACCENTURE STRATEGY AND OXFORD ECONOMICS.

### What is the digital economy?

The digital economy is the share of total economic output derived from a number of broad 'digital' inputs. This includes digital skills, digital equipment (hardware, software and communications equipment) and the intermediate digital goods and services used in production. Such broad measures reflect the foundations of the digital economy.

Despite ICTs already having a significant economic impact in The Netherlands, other countries, such as the United Kingdom, the United States, Germany and France, are investing more rapidly in their ICT infrastructure and thus, have a greater digital share.<sup>3</sup>

|                      | GLOBAL             | NETHERLANDS        | FRANCE              | GERMANY             | UNITED KINGDOM      | UNITED STATES     | CHINA             |
|----------------------|--------------------|--------------------|---------------------|---------------------|---------------------|-------------------|-------------------|
| ECONOMY 2015         | €78.418bn          | €690bn             | €2.225bn            | €3.085bn            | €2.701bn            | €16.516bn         | €9.968bn          |
| ECONOMY 2020         | €90.611bn          | €761,16bn          | €2.413bn            | €3.327bn            | €3.042bn            | €18.807bn         | €13.133bn         |
| DIGITAL ECONOMY 2015 | €17.664bn<br>22,5% | €158,01bn<br>22,9% | €582,95bn<br>26,2%  | €781,08bn<br>25,3%  | €829,207bn<br>30,7% | €5.136bn<br>33,1% | €1.047bn<br>10,5% |
| DIGITAL ECONOMY 2020 | €22.669bn<br>25%   | €190,4bn<br>25%    | €697,357bn<br>28,9% | €958,176bn<br>28,8% | €1.016bn<br>33,4%   | €6.959bn<br>37%   | €1.642bn<br>12,5% |

TABLE 1 COUNTRY-BY-COUNTRY DIGITAL ECONOMY SHARE OF TOTAL ECONOMY IN 2015 AND 2020. SOURCE: ACCENTURE STRATEGY AND OXFORD ECONOMICS.

## 2.2 The Dutch ICT sector

In 2013, ICT companies contributed to 4,4% of the total Dutch GDP according to Netherlands Statistics. At first glance, this might be in stark contrast to the digital economy's significant share of the Dutch GDP, but one has to bear in mind that the ICT sector is more narrowly defined than the digital economy, as it does not look beyond the share of the ICT sector itself.

Nearly half of the added value of the ICT sector is generated by IT service providers. This share is higher than that of other countries, with the exception of the United Kingdom and France. The higher-ranking countries, such as Japan, Ireland, and Sweden, have a stronger hardware industry and their positions reflect this.

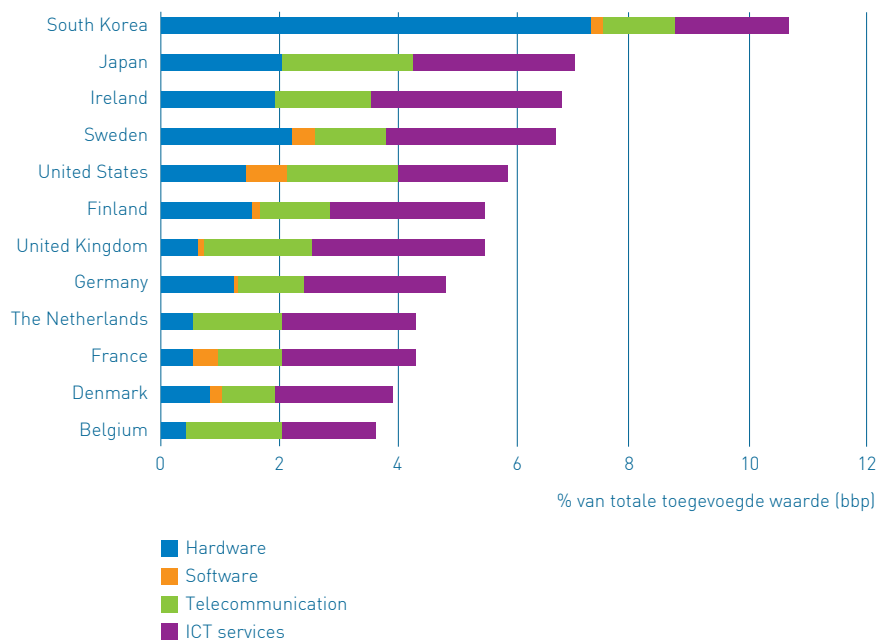


FIGURE 2 THE SHARE OF THE ICT SECTOR OF THE TOTAL ECONOMY (GDP), INTERNATIONAL, 2013. SOURCE: CENTRAAL BUREAU STATISTIEK, 'ICT, KENNIS EN ECONOMIE 2016'. IRELAND, JAPAN, UK, SWEDEN AND GERMANY 2012 INSTEAD OF 2013; CANADA: 2011 INSTEAD OF 2013.

In the context of international trade, the Netherlands imported nearly €50bn of ICT goods (88%) and services (12%) in 2014 (4,2% increase over 2013), while it exported merely €28,5bn (also a 4,2% increase over 2013), of which €18bn were goods, and €10,5bn ICT services. The annual growth of Dutch ICT export is increasing much faster than its overall export. Yet compared to other countries it still remains rather flat – especially ICT services, which makes up half of the Dutch ICT sector. Re-export, however, is not included, but constitutes over 57% of the total ICT export, or €38,4bn, in 2014.

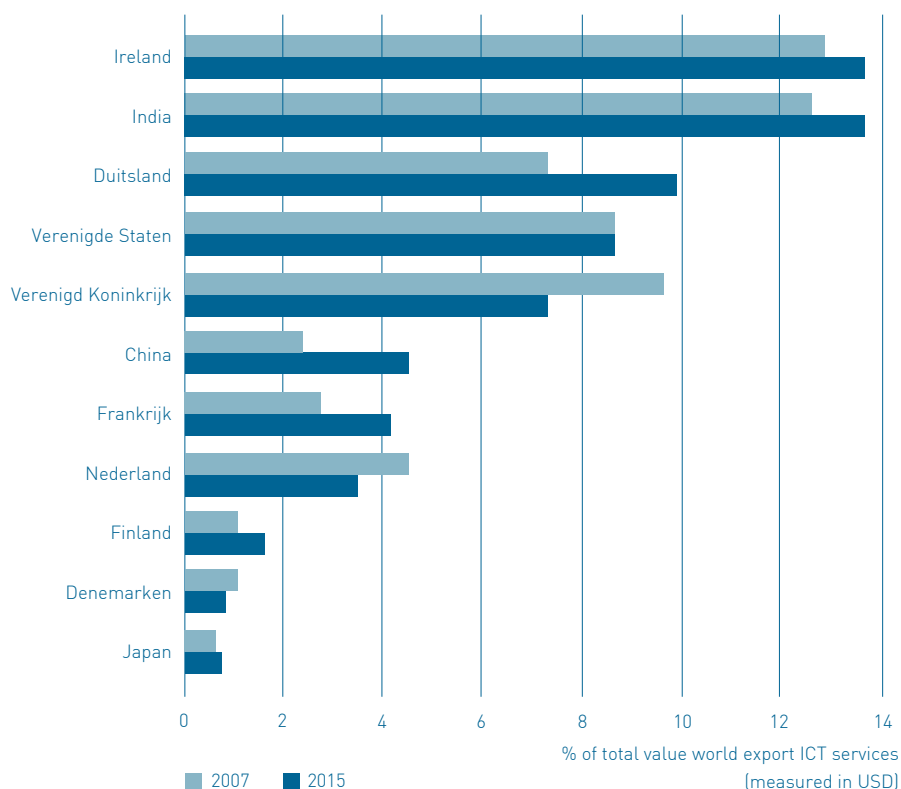


FIGURE 3 EXPORT VALUE OF ICT SERVICES, INTERNATIONAL. SOURCE: CENTRAAL BUREAU STATISTIEK, OECD (2015), DIGITAL ECONOMY OUTLOOK 2015.

With a compound annual growth rate of only 5% for the export of ICT services between 2009 and 2013, the Dutch export is not increasing as fast as in other countries, such as Germany (11%), and France (21%). As a result, the global share of export of Dutch ICT services has decreased significantly together with the UK, while Germany, France, and China have gained ground.

Lastly, The Netherlands now imports most of the ICT goods from China. By the end of 2015, nearly 28% of the value of ICT goods imported by the Netherlands came from China.<sup>4</sup>

# 3 ICT AND CYBERSECURITY SPENDING

|  |    |
|--|----|
| 3.1 ICT investments                          | 19 |
| 3.2 ICT expenditures                         | 20 |
| 3.3 Government spending on cybersecurity     | 20 |
| 3.4 Private sector spending on cybersecurity | 21 |

# 3 ICT AND CYBERSECURITY SPENDING

Herna Verhagen, CEO of PostNL, recently presented the advisory report ‘Digitaal Droge Voeten’ to Prime Minister Mark Rutte at the end of the Dutch cybersecurity awareness week, AlertOnline, in which she urges the Dutch government, companies and citizens alike to invest 10% of their annual ICT budget in cybersecurity.<sup>5</sup>

The report received support from the Dutch Cyber Security Council and widespread coverage in Dutch media due to its strong and alarming message. It presents a compelling analysis of the current digital threats, challenges and opportunities for Dutch society. Unfortunately, it lacks specific sources to back the 10% norm. Either the report refers to governments with a similar norm, such as Singapore investing 8%, and Germany 10%, but lacks clear numbers, or it presents the impressive cybersecurity budgets of the US and the UK and their recent boost in funding without any reference to their ICT budget. Other countries, such as South Korea and Israel, claim to spend a respective 10% and 8% of their ICT budget in cybersecurity<sup>6</sup>, but also don’t disclose specific details.

Although the report presents a useful framework for cybersecurity spending, and sets an ambitious goal, it lacks sufficient insight into the current state of Dutch investments in either ICT or cybersecurity. The following section will attempt to provide such an overview.

## 3.1 ICT investments

Statistics Netherlands (CBS) makes a distinction between ICT investments and expenditures. Both categories constitute separate categories of expenses that do not overlap. Investments are limited to goods that are intended for production, last over one year, and have an effect on the national production capacity. In 2014, Dutch companies and governments invested €23bn in ICT capital (19% of the total national investments). Investments in ICT have been uninterruptedly increasing since 2010.

Due to the high compound growth rate, the share of ICT greatly increased vis-à-vis the total investments: in 2009 ICT investments accounted for 14% of the total, while in 2014, they accounted for 19%. As expected, Dutch companies and governments invest most in software – amounting to €17bn, or 75% of the total ICT investments. Since 2008, companies and governments have tended to invest less in hardware (with an exceptional surge in 2011).<sup>7</sup>

Of the €23bn invested in ICT, €4,7bn was invested by the Government, and over €17bn by the private sector. The remaining €1bn most likely comes from R&D.<sup>8</sup>

### **3.2 ICT expenditures**

In 2014, companies, governments and consumers spent nearly €47bn on ICT goods and services – a 3% increase from the year before. ICT expenditures are made up of government and private sector spending on ICT goods and services that are used throughout the production process but do not have the nature of investments, such as intermediary use or upkeep, and amounted to €35bn in 2014. Moreover, ICT expenditures also include consumer or household consumption of ICT – reaching €12,4bn in 2014. Dutch companies and governments spend nearly three times more on ICT than households, and the growth rate of their expenditures keeps on rising – 70% in 2008 to 74% in 2014. On the other hand, Dutch households are spending increasingly less on ICT: down €0,5bn from 2010.<sup>9</sup> This is not attributable to a decrease in overall household consumption, since the share of ICT expenditure dropped from 3,1% in 2008 to 2,6% of their total expenditures in 2014.

Unfortunately, Statistics Netherlands does not make a distinction between government and private sector expenditures in ICT.

### **3.3 Government spending on cybersecurity**

Public cybersecurity spending is not easily discernable from overall government spending. Figure 4 shows government cybersecurity spending over time as a percentage of its national GDP. This is limited to the publicly available budgets allocated to civilian and military cybersecurity. Some governments have started publicizing their budgets only recently, might disclose only parts of their budget, or may not specify exactly what it will cover. This holistic overview shows that the government of the Netherlands spends considerably less as a portion of its GDP compared to other countries.



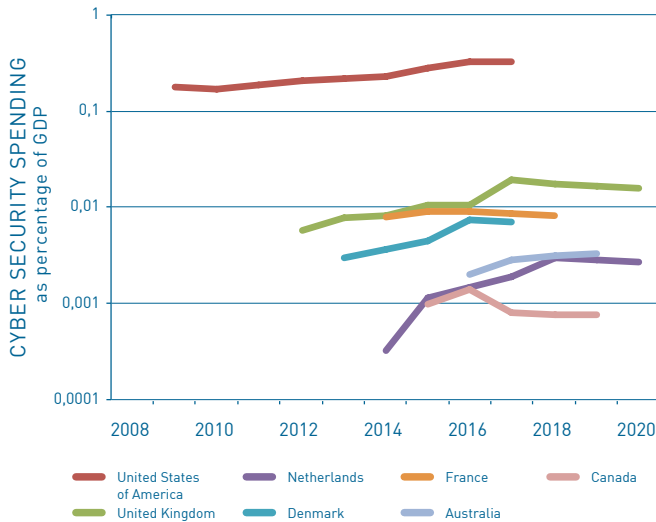


FIGURE 4 GOVERNMENT CYBERSECURITY SPENDING: A CROSS COUNTRY COMPARISON OVER TIME (2008-2020).

In 2015, the National Cyber Security Centre of the Netherlands received €2,7mn in funding<sup>10</sup>, while the Ministry of Defense spent €5mn on cybersecurity<sup>11</sup>. Besides the €7,7mn invested in civilian and military cybersecurity included in Figure 4, the Dutch government invested €13,8mn in its National Police to combat cybercrime and strengthen the security chain.<sup>12</sup> Moreover, the Dutch government made a one-off investment of €6,5mn for the Global Conference of Cyberspace in 2015 (in addition to the 2mn spent in 2014).<sup>13</sup>

Taking into account the 1.5% loss of its national GDP to cybercrime<sup>14</sup>, and the €10bn value lost by cyber risks<sup>15</sup>, there seems to be a mismatch of cybersecurity spending and the costs incurred by a lack of it. It comes as no surprise that the U.S. is the top spender, considering its authoritative role in cybersecurity as well as its unparalleled military budget.

### 3.4 Private sector spending on cybersecurity

Public cybersecurity spending is not easily discerned, but there is nevertheless sufficient data to provide a holistic overview. Unfortunately, establishing a similar overview of the private sector is more challenging, especially for the Netherlands. The sole available indication of cybersecurity spending by Dutch enterprises comes from a white paper 'Cyber Security Challenges in the Netherlands', that was published by CGI

and Pierre Audoin Consultants in 2015, in which Dutch private cybersecurity investments were compared to those of other countries in the EU, and concluded that Dutch enterprises are spending 0.08% of the total GDP or €542,3mn on cybersecurity. Furthermore, the report concludes that Dutch businesses are underspending on cybersecurity, and may therefore see it as less of a priority than its Nordic neighbors. The Netherlands would have to spend an additional 0.03% of GDP on cybersecurity to close this funding gap.

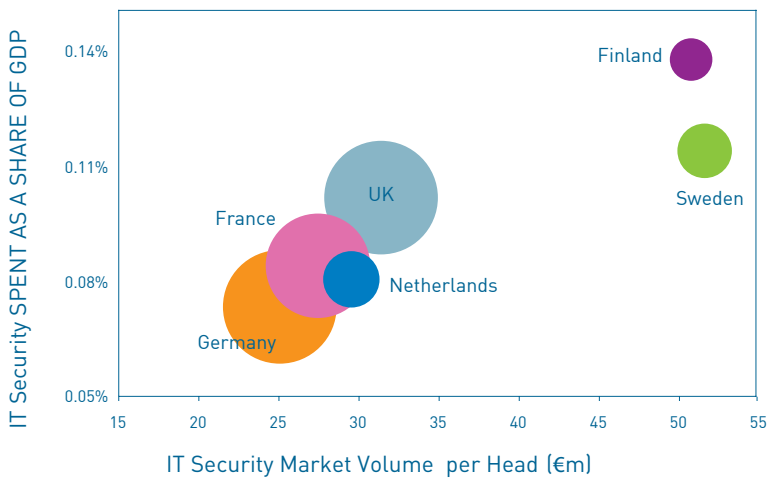


FIGURE 5 NATIONAL IT SECURITY SPENDING COMPARED TO ECONOMIC MEASURES 2015. SIZE OF BUBBLES REPRESENTS SECURITY SITS MARKET VOLUME (€M). SOURCE: PIERRE AUDOIN CONSULTANTS (PAC) AND CGI, 'CYBER SECURITY CHALLENGES IN THE NETHERLANDS', JUNE 2015. GDP AND POPULATION INFORMATION SOURCED FROM IMF.

# 4 META-ANALYSIS ESTIMATING THE DUTCH CYBERSECURITY MARKET

# 4 META-ANALYSIS

## ESTIMATING THE DUTCH CYBERSECURITY MARKET

The Dutch cybersecurity market is growing relatively quickly, with turnover from 2010 to 2014 increasing annually by 14.5%.<sup>16</sup> The estimated total turnover for the Dutch cybersecurity market ranges between €0,4bn and €7,5bn. In the table below, these estimates are related to the sources, their method and the economy of focus. The size of the Dutch cybersecurity market has been extrapolated from these estimates.

| SOURCE  | METHOD                    | ECONOMY                | SIZE (REVENUE) IN EURO | DERIVATIVE SIZE OF THE DUTCH MARKET |
|---|---------------------------|------------------------|------------------------|-------------------------------------|
| European Commission <sup>17</sup>                                     | unknown                   | EU (2013)              | €11.2bn                | €0.4bn                              |
| VKA/SEO (2016) <sup>18</sup>  | survey                    | The Netherlands (2014) | €7.5bn                 | €7.5bn                              |
| Pierre Audoin Consultants (2013) <sup>19</sup>                        | bottom-up                 | United Kingdom (2013)  | €3.3bn                 | €0.9bn                              |
| Pierre Audoin Consultants (2012) <sup>20</sup>                        | survey                    | France (2011)          | €5.0bn                 | €1.8bn                              |
| Bundesministerium für Wirtschaft und Technologie (2013) <sup>21</sup> | Administrative (tax) data | Germany (2012)         | €6.2bn                 | €1.4bn                              |

TABLE 2 DIVERGING ESTIMATES OF THE CYBERSECURITY MARKET SIZE<sup>22</sup>

In order to gain some understanding of why these estimates diverge so much, we take a closer look at different definitions of the scope of the market, and the effects of their respective methodologies.

Pierre Audoin Consultants investigated the cybersecurity market of the UK (2013) and France (2011) through a mixed methodology of industry surveys and a bottom-up estimation of the market by aggregating the revenues of industry firms.<sup>23</sup> Their scope

of the cybersecurity market includes security-related hardware, network equipment and management consultancy fees. Through these estimates, the markets of France (€5bn) and the UK (€3.3bn) are estimated, and then extrapolated to a Dutch estimate by applying the ratio of the Dutch GDP to that of the researched country.<sup>24</sup> The widely differing estimates stemming from these two reports (€1.8bn and €0.9bn) are likely caused by the different sizes of the French and British economies and their respective cybersecurity markets. The French cybersecurity market is larger than the British market, but the British GDP is higher than the French, leading to diverging extrapolated Dutch estimates.

The estimates of the EU market by the European Commission only concerns the cybersecurity product market, and excludes the defense, intelligence and security market (€5.8bn) and the managed security services market (€8.4bn).<sup>25</sup> If these sectors were included, however, the total amount would be around €21.8bn for the EU, which would put the estimate of the Dutch cybersecurity market around €0.9bn<sup>26</sup>. This estimate is again based on the contribution of the Dutch GDP to the total EU GDP. Yet, this adjusted estimate puts it in the same ballpark as the market approximation found in the UK report. See Figure 6 for an overview and estimation of the cybersecurity market size in Europe, the Middle East, and Africa from 2014 until 2020.

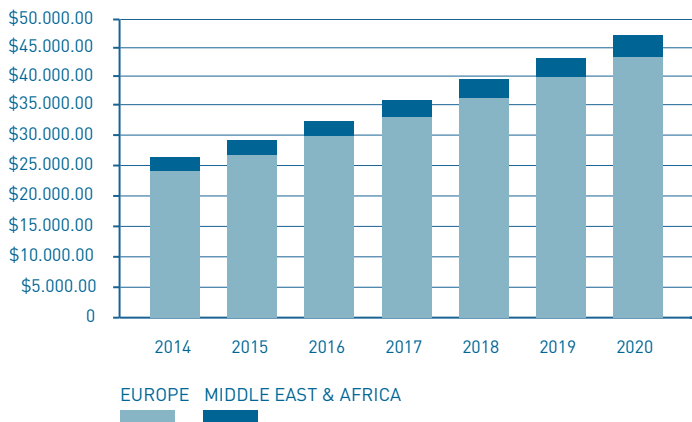


FIGURE 6 THE CYBERSECURITY MARKET SIZE OF EUROPE, AND THE MIDDLE EAST & AFRICA. SOURCE: IHS<sup>27</sup>

The VKA report shows a very high estimate (€7.5bn) for the Dutch cybersecurity market<sup>28</sup>. This study distinguishes itself from previous studies through its methodology, as it estimates the value of the cybersecurity market by approximating the extent of cybersecurity incidents and the scope of the damages<sup>29</sup>. Hence, this report aims to quantify the market through the *expected* demand for cybersecurity, rather than the current value or revenue of companies in the market. Herein this estimation is not comparable to the others, which use the method of approximation instead.

Given these abovementioned differences in methodology, it seems that the estimates for the current value of the supply in the Dutch cybersecurity market falls between €0.9bn and €1.8bn, depending on the country from which these values were extrapolated, while the estimated value reaches €7.5bn based on the extent of cybersecurity incidents and the scope of the damage.

### Putting it in global perspective

Global estimates for the growth of the cybersecurity market are promising – reaching €69bn in 2015,<sup>30</sup> and forecasted to grow to €157bn by 2020.<sup>31</sup> The private cybersecurity market is currently the fastest growing sector in ICT and is estimated to grow at a compound annual growth rate of 9.8% from 2015 to 2020, according to a report from Markets and Markets.<sup>32</sup> The promising areas for growth, according to IDC, are security analytics/SIEM (10%), threat intelligence (10%+), mobile security (18%), and cloud security (50%).<sup>33</sup>

The 2020 projections for many segments of the cybersecurity market show continued growth. The global managed security services market is expected to reach nearly €27.3bn by 2020, with a compound annual growth rate (CAGR) of 15.8% over the next 5 years.<sup>34</sup> A new cybercrime wave is driving IoT spending, and the Internet of Things (IoT) security market is predicted to grow from €6.27bn in 2015 to nearly €26.39bn by 2020 (CAGR of 33.3%) according to a report published by Markets and Markets.<sup>35</sup> Research and advisory firm Technavio predicts the global IoT security market to grow at a CAGR of nearly 55% over the period 2014-2019 – making it the fastest growing cybersecurity subsector.<sup>36</sup>

The cybersecurity insurance market is considered one of the fastest growing insurance sectors, and is estimated to reach €7bn in annual sales by 2020, up from €2.3bn this year.<sup>37</sup> This market – largely based in the US – has grown from €0.9bn to €2.3bn over the past two years, and is expected to grow dramatically both within and outside of the US over the next five years.<sup>38</sup>

| CYBERSECURITY SUBMARKETS                  | VALUE IN €BILLIONS             | COMPOUND ANNUAL GROWTH RATE |
|---|--------------------------------|-----------------------------|
| Security services <sup>39</sup>           | €13.1bn (2015) €27.3bn (2020)  | 16%                         |
| IoT security <sup>40</sup>                | €6.27bn (2015) €26.39bn (2020) | 33% (up to 55%)             |
| Cybersecurity insurance <sup>41</sup>     | €2.3bn (2015) €7bn (2020)      | 25%                         |
| Security awareness training <sup>42</sup> | €0.9bn (2015) €1.66bn (2020)   | 13%                         |

TABLE 3 OVERVIEW OF THE GROWTH RATES AND VALUES OF THE CYBERSECURITY SUBMARKETS

As the financial industry is becoming increasingly dependent on ICT, it is investing heavily in cybersecurity. Four of the largest financial institutions from the US – J.P. Morgan Chase & Co., Bank of America, Citigroup, and Wells Fargo – collectively spend €1.37bn on cybersecurity on an annual basis. JP Morgan invests €455mn, Bank of America €364mn, Citi €273mn and Wells invests €227.5mn. The budgets for those four institutions alone make up around 15% of cybersecurity spending in the global financial sector.<sup>43</sup>

The shift to the online sphere has resulted in a majority of organizations and enterprises running IT services in the cloud (63%), with a further 59% of them increasing their cybersecurity investments as a result of digitization.<sup>44</sup> Many companies (51%) are starting to use big data analytics to model for cybersecurity threats and identify incidents.<sup>45</sup>

# 5 AWARENESS



# 5 AWARENESS

Increased cyber hygiene is a necessary first step to cybersecurity. Employees and citizens that do not open suspicious emails containing malicious links or documents, install anti-virus software, and regularly update outdated software are less likely to become a victim to cybercrime and will thereby avoid the bulk of the (unsophisticated) security incidents. Awareness first needs to occur on the level of the end-user but should not stop there. The executive board and the political elite should be aware of the risks involved for their organizations as they bear a broader responsibility towards their employees and clients. In its second cybersecurity strategy, the National Cyber Security Centre (NCSC) evaluates the Netherlands as having developed sufficient cybersecurity knowledge as well as having allocated substantial investments given its pursuit for a wide educational approach, 'ranging from primary education to higher education, and from work-based training to university, and from the board room to the coalface'.<sup>46</sup> Public cybersecurity campaigns have only recently started. Examples include:

- the 'Hang op, klik weg, bel uw bank' campaign, whereby the Dutch Payments Association informs the Dutch public about the ways to protect themselves from online fraud via national radio, TV and their website;<sup>47</sup>
- the 'Alert Online' annual, two-week long public campaign in which different stakeholders join forces in order to promote cybersecurity among Dutch citizens, government and other institutions as well as the private sector by organizing workshops, meetings, presentations and other activities.<sup>48</sup> This campaign is part of the larger European Cyber Security Month that takes place every October across Europe.

Earlier in 2016, Gartner Inc. stated that the security awareness training market exceeds €0.9bn in global annual revenue, and is growing by approximately 13% on a yearly basis.<sup>49</sup> Furthermore, Chief Information Security Officers (CISOs) are increasingly

turning to educational security awareness solutions to help improve organizational compliance, expand security knowledge and change poor security behaviors. This all contributes to the rapidly increasing importance of the cybersecurity market on a global scale.

# 6 EDUCATION

## 6 EDUCATION

Apart from publicized campaigns, cybersecurity issues have been promoted through educational programs both in the private and the public sectors, in which the NCSC asserts a leading role. The Centre publishes knowledge documents, such as its annual 'Cyber Security Assessment' and the 'Trend Report on Cybercrime and Digital Security', which are aimed at informing senior executives in the public and the private domain.<sup>50</sup> Moreover, in order to enlarge the pool of cybersecurity experts, funds were granted to three leading Dutch universities, resulting in the launch of several programs on cybersecurity studies in the past years.<sup>51</sup> See Annex I for an overview of the cybersecurity programs offered in the Netherlands.

In a working paper, Claire Vishik (Intel) and Maritta Heisel (University Duisburg-Essen), gathered data from 19 countries on cybersecurity education for ENISA. Although the data is not comprehensive, they give us a preliminary view of the available curriculum. Unfortunately, at this time the database is still too underdeveloped to allow us to compare approaches of different member states. Figure 7 shows the number of graduate and undergraduate cybersecurity programs per country. As expected, undergraduate programs are very scarce. Cybersecurity is mostly instructed at a graduate level, and is led by the UK and Germany. As shown in Figure 8, most courses are offered in the discipline of computer science.<sup>52</sup> This is unsurprising, considering the predominantly technical nature of cybersecurity, and the fact that most of the studies submitted so far came from computer science, computer engineering, information systems, or information management departments. This can give a shortsighted overview. Nonetheless, one thing is undeniable: cybersecurity is drastically underrepresented in other non-technical educational programs. This is of particular relevance since many governments and companies are increasingly calling for an interdisciplinary approach to cybersecurity as it no longer is a purely technical matter, but transcends into other domains, such as law, economics, politics and defense. As a starting point, cybersecurity should thus be instructed in other academic domains alongside the largely technical discourse.

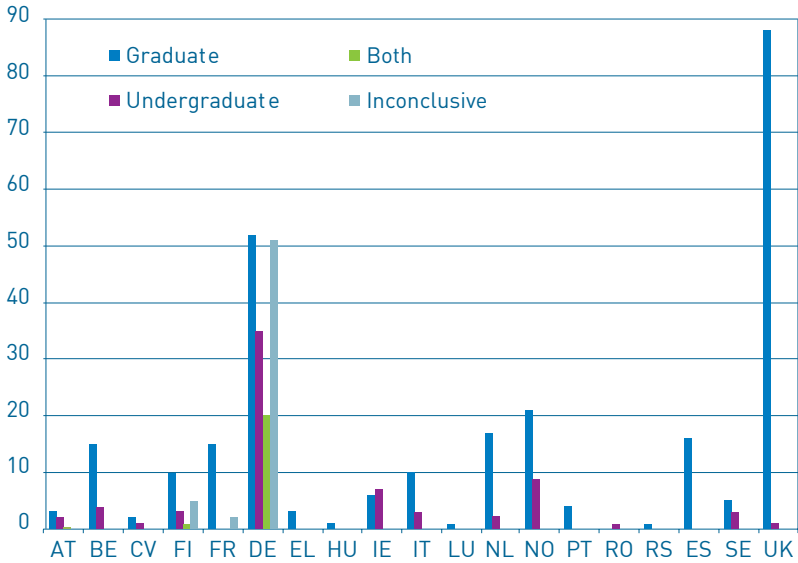


FIGURE 7 NUMBERS OF GRADUATE AND UNDERGRADUATE CYBERSECURITY COURSES PER COUNTRY SNAPSHOT TAKEN IN AUGUST 2015

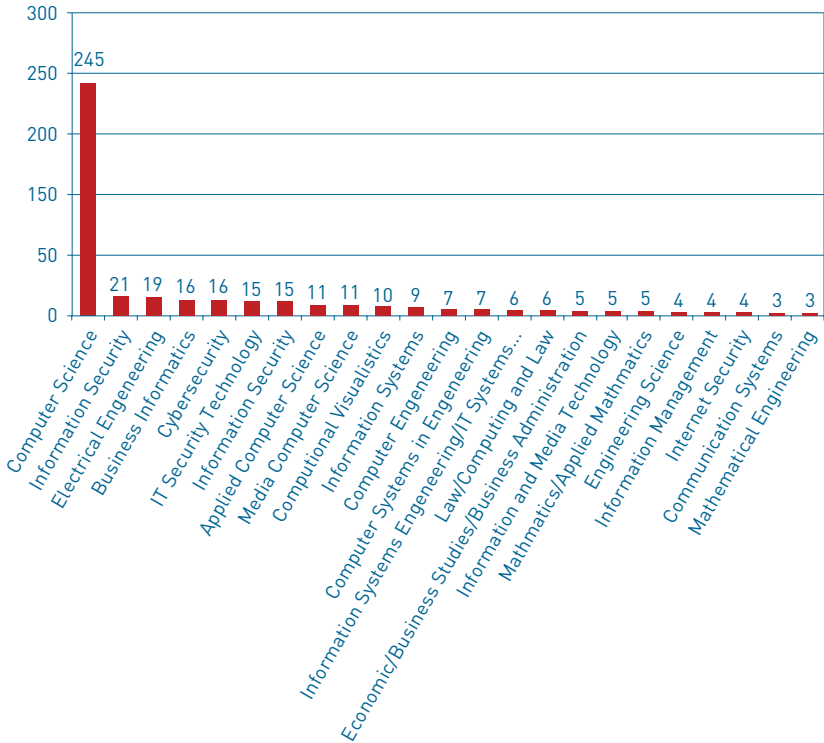


FIGURE 8 NUMBER OF DISCIPLINES IN WHICH MOST COURSES ARE OFFERED (SNAPSHOT TAKEN IN AUGUST 2015)

An important threat to the cybersecurity market is the ICT labor epidemic, with more than 11,000 ICT jobs left unfilled in the Netherlands.<sup>53</sup> According to research of a leading job website that analyzed its Dutch and Irish job market, the amount of unfilled cybersecurity jobs increased with 53% from 2014 to 2015, while the year before it only increased with 5%. The company therefore put cybersecurity experts as the leading potential job for the future, followed by IoT developer, which, from 2014 to 2015, increased with a staggering 377%.<sup>54</sup>

The ongoing talent squeeze is likely to drive more organizations to turn to third parties to help run some or all of their security programs.<sup>55</sup> In the Netherlands, a shortage of trained cybersecurity specialists is imminent and is expected to grow further due to the insufficient number of students graduating from ICT programs, especially those tailored to cybersecurity.<sup>56</sup> Furthermore, concerns have been raised about the connection of the education to the expectations of the private sector, as important skills expected by the companies are not taught in these programs.<sup>57</sup>

# 7 SCIENTIFIC RESEARCH

## 7 SCIENTIFIC RESEARCH

In developing response options to cyber attacks, the Netherlands has taken a comprehensive approach in which one of its primary objectives is to 'strengthen research and analysis capabilities to gain more insights into threats and risks in the digital domain'.<sup>58</sup> Together with the National Cyber Security Research Agenda II, the National Cyber Security Strategy highlights the importance of a multi-stakeholder approach, facilitating innovation to a further extent. The Agenda, in fact, provides the framework, setting up two research trajectories (short-term and long-term), highlights the economic benefits, and stresses the importance of taking a broad scope for the needed research.<sup>59</sup>

Since 2012, the vast majority of research programs have been primarily funded by several Dutch ministries – such as Defense, Economic Affairs, Security and Justice, and Infrastructure and Environment. Other bodies that contribute include the Dutch research council NWO,<sup>60</sup> the Cyber Security Council through its research in the scope of the Security Research Agenda<sup>61</sup>, and dcypher, which is responsible for the scheduling and the coordination of cybersecurity research after consulting with businesses, and government and knowledge institutions in the field.<sup>62</sup>

In 2013, which marked the second round for cybersecurity research funding, a sum of 6.4 million euros was made available by the government and NWO.<sup>63</sup> This research portfolio tends to be rather technically orientated, leaving out alpha studies that address the political, social and legal implications.<sup>64</sup> This could be improved by nurturing a more multi-disciplinary approach towards cybersecurity.

Lastly, the private sector is a major contributor to research and development. According to the Statistics Netherlands, 3.335 ICT companies were involved in R&D in 2014.<sup>65</sup> These were predominantly service providers (96%), which counters the general understanding that the industry invests more in R&D than the service sector. Of all companies involved in R&D in 2014, 18% were ICT companies.



# 8 KEY TAKEAWAYS

## 8 KEY TAKEAWAYS

In this report, we set out to collect and present the publicly available and relevant data that allows us to assess the current state of Dutch cybersecurity, especially in relation to the recently proposed norm that suggests governments, businesses and citizens alike should invest 10% of their ICT budget in cybersecurity.

We can conclude that the volume of cybersecurity investments is steadily increasing as a result of the growing number of incidents. However, one should bear in mind the challenges of determining the size of channeled funds: (i) the lack of reliable and consistent reporting and data sets; (ii) the absence of a unified definition of cybersecurity, which makes it difficult to delineate which costs are specifically attributed to cybersecurity per se; (iii) cybersecurity is increasingly evolving into the integral part of business operations – rather than being a separate unit costs; (iv) collecting and mapping the data of ICT and cybersecurity investments is generally complicated as cybersecurity is mostly approached qualitatively, and not primarily from a cost perspective.

That being said, the economic value of digitization and ICTs has been significant for the Netherlands, and will continue to grow. If we take a snapshot of the Dutch ICT sector in 2013, we see that it contributed to 4,4% of the total GDP. Nearly half of this added value is generated by ICT service providers. Compared to other European countries, the Netherlands is on equal footing with France, but lags behind Germany and the UK. In 2015, the Dutch digital economy accounted for €158bn or 22,9% of the total Dutch economy, and is projected to reach €190,4bn, or 25% of the expected total economy by 2020. Although this share appears impressive, the Netherlands still lags behind other European countries such as Germany, France, and the UK in this regard, and the realization of the expected growth will depend on the spread of Dutch investments in the development of digital skills and novel technologies and their security, such as IoT.

|                    | RESILIENCE RANKING (2016) | INTERNET PENETRATION (2016) | ICT CONTRIBUTION TO GDP GROWTH (2000-2009 AV.) | PRIVATE INVESTMENT AS % GDP (2016) | GOVERNMENT SPENDING AS % OF GDP (2016) | TOTAL NATIONAL INVESTMENT AS % GDP | CYBERCRIME COST AS % OF GDP (2014) |
|--------------------|---------------------------|-----------------------------|--|------------------------------------|--|------------------------------------|------------------------------------|
| U.S.               | 1                         | 87%                         | 29,8%  | n/a                                | 0,3209%                                | 0,321%                             | 0,64%                              |
| U.K.               | 2                         | 92%                         | 20,2%  | 0,10%                              | 0,0107%                                | 0,111%                             | 0,16%                              |
| <b>Netherlands</b> | <b>3</b>                  | <b>93%</b>                  | <b>22,1%</b>                                   | <b>0,08%</b>                       | <b>0,0015%</b>                         | <b>0,082%</b>                      | <b>1,50%</b>                       |
| Australia          | 4 =                       | 85%                         | 16,2%  | n/a                                | 0,0020%                                | 0,002%                             | 0,08%                              |
| Canada             | 4 =                       | 87%                         | 23,4%  | n/a                                | 0,0014%                                | 0,002%                             | 0,17%                              |
| Germany            | 4 =                       | 86%                         | 35,2%  | 0,08%                              | n/a                                    | 0,075%                             | 1,60%                              |
| Finland            | 7                         | 92%                         | 14,6%  | 0,14%                              | n/a                                    | 0,135%                             | n/a                                |
| France             | 8                         | 84%                         | 28,1%  | 0,09%                              | 0,0090%                                | 0,094%                             | 0,11%                              |
| Denmark            | 9                         | 96%                         | 39,0%  | n/a                                | 0,0073%                                | 0,007%                             | n/a                                |

TABLE 4 CYBERSECURITY CROSS-COUNTRY OVERVIEW INCLUDING (FROM LEFT TO RIGHT) THE POSITION IN THE HCSS RESILIENCE RANKING, INTERNET PENETRATION, PRIVATE INVESTMENTS IN CYBERSECURITY AS A SHARE OF THE GDP, GOVERNMENT CYBERSECURITY BUDGET AS SHARE OF THE GDP, THE TOTAL PUBLIC AND PRIVATE INVESTMENTS, AND THE COSTS OF CYBERCRIME AS A PERCENTAGE OF THE GDP.

The assessment of the Dutch investments in cybersecurity as a share of ICT investments is less promising:

- Dutch companies and governments are increasingly investing in ICT, accumulating to €23bn in 2014. Nearly 75% (€17bn) was dedicated to software, which, for the most part, was imported from other countries.
- In that same year Dutch companies and governments spent €35bn and households over €12bn on ICT goods and services – a 3% increase from the year before. While governments and companies are spending more, Dutch households are spending increasingly less on ICT.
- In total, the Dutch government and private sector spent €58bn in total on ICT investments and expenditures.
- In 2015, the Dutch private sector invested €542,3mn in cybersecurity while the public sector €7,7mn, bringing the total to €550mn and just under 1% of the respective ICT budget of the Netherlands.
- In addition, however, the government invested nearly €14mn in the National Police – recurring over the following four years. While the UK and Australia allocate around 15% of their cybersecurity budget to the National Police to combat cybercrime, the Netherlands invests nearly 65%.
- Regardless of the remaining undisclosed cybersecurity budgets, this much is undeniable: The Netherlands is underspending on cybersecurity and still is a long way from the 10% benchmark compared to its European counterparts.

Nonetheless, the Verhagen norm offers governments, companies and households a helpful framework that allows for a more integrated approach in dealing with cybersecurity in relation to new ICT goods and technology.

Taking into account the 1,5% loss of its national GDP to cybercrime, which correlates well to the €10bn value loss through cyber risk in the Netherlands, the Dutch private sector, and especially the government, can invest more in cybersecurity to reduce the impact and damage of cyber of cybercrime and –risks. In addition, there is a drastic increase in demand anticipated for cybersecurity experts and IoT developers. There is a pressing urgency for The Netherlands to address the labor deficit and match Dutch capabilities with those of its European peers.

The Dutch cybersecurity sector's value is estimated to be between €0,9 and €1,8bn. However based on the extent of security breaches and scope of the damage caused, its estimated value could reach as high as €7.5bn. As a final observation, this estimation of the Dutch cybersecurity market could function as the optimal cybersecurity budget to counter the risks and threats, albeit one that is higher than the 10% norm.

# ANNEX I – OVERVIEW OF CYBERSECURITY PROGRAMS IN THE NETHERLANDS

# ANNEX I – OVERVIEW OF CYBERSECURITY PROGRAMS IN THE NETHERLANDS

Currently, there are several bachelor and master programs in the Netherlands that offer specialization in cybersecurity:

- Master’s Degree Program in Network and System Engineering: Security at the University of Amsterdam;
- Master’s Degree at the Cyber Security Academy, a joint initiative by Leiden University, Delft University and The Hague University of Applied Sciences<sup>66</sup> (Technical and governance policy);
- Master’s Degree in Cyber Security at the Webster University, Leiden;<sup>67</sup>
- TU4 Cyber Security Master’s Degree, offered jointly by the Delft University of Technology and the University of Twente;<sup>68</sup>
- TRU/e Master’s Degree in Cyber Security, a joint program by Radboud University and the Eindhoven University of Technology;<sup>69</sup>
- Similarly, Radboud University offers a Bachelor’s Degree in Informatics and Cyber Security;<sup>70</sup>
- EIT Digital Security & Privacy programme, also offered at the University of Twente;<sup>71</sup>
- Master’s Degree in Law and Technology at the University of Tilburg;<sup>72</sup>
- MBA-module ‘Business and Cyber Robustness’ at the Nyenrode Business University;<sup>73</sup>
- Specialization ‘IT Forensics’ of the Bachelor Programme Informatics at the University of Applied Sciences Leiden;<sup>74</sup>
- Technical Informatics Curriculum comprising cybersecurity courses at the University of Applied Sciences, Rotterdam;<sup>75</sup>
- Bachelor HBO-ICT, IT Services, IT Development and Business Intelligence, Minor in Cybersecurity /Information security, and a in Minor Automated Digital Forensics Research at the Zuyd University of Applied Sciences;<sup>76</sup>
- The Security Academy offers programs in IT-Security & BCM.<sup>77</sup>

Besides the aforementioned degree programs, there are also summer schools dedicated to cybersecurity, like the International Cyber Security Summer School, involving The Hague Security Delta, *The Hague* Centre for Strategic Studies, The Dutch Cyber Security Platform for Higher Education and various intergovernmental organizations, such as EUROPOL and NATO Communications and Information Agency.<sup>78</sup>

# SOURCES



# SOURCES

- 1 Digital Economy, *European Commission*, October 17, 2016. Available at: <http://ec.europa.eu/growth/sectors/digital-economy/>.
- 2 Digital Disruption: The Growth Multiplier, *Accenture Strategy*, 2016. Available at: <https://www.accenture.com/us-en/insight-digital-disruption-growth-multiplier>.
- 3 *The Global Information Technology Report 2016*, *World Economic Forum*, 2016, (see *The Networked Readiness Index*). Available at: [http://www3.weforum.org/docs/GITR2016/GITR\\_2016\\_full%20report\\_final.pdf](http://www3.weforum.org/docs/GITR2016/GITR_2016_full%20report_final.pdf)
- 4 *ICT, Kennis en Economie*, Centraal Bureau Statistiek, 2016, p.59-60. Available at: <https://www.cbs.nl/nl-nl/publicatie/2016/26/ict-kennis-en-economie-2016>.
- 5 *De economische en maatschappelijke noodzaak van meer cybersecurity – Nederland digitaal droge voeten*, Herna Verhagen, September 2016. Available at: [https://www.thehaguesecuritydelta.com/media/com\\_hsd/report/104/document/Rapport-NCSR-Nederland-digitaal-droge-voeten-061016.pdf](https://www.thehaguesecuritydelta.com/media/com_hsd/report/104/document/Rapport-NCSR-Nederland-digitaal-droge-voeten-061016.pdf)
- 6 Ting, Lisabel. *S'pore to spend 10% of IT budget on cyber security*. The Straits Times, October 7, 2015. Available at: <http://www.straitstimes.com/singapore/spore-to-spend-10-of-it-budget-on-cyber-security>
- 7 *ICT, Kennis en Economie*, Centraal Bureau Statistiek, 2016, p.50.
- 8 For a detailed overview of the Dutch investments (including in ICT) over the past 5 years, see: <http://statline.cbs.nl/Statweb/publication/?DM=SLNL&PA=82600ned&D1=0-91&D2=a&D3=15-20&VW=T>.
- 9 *ICT, Kennis en Economie*, Centraal Bureau Statistiek, 2016, p.52.
- 10 *VI Veiligheid en Justitie Rijksbegroting 2016*. Tweede Kamer, vergaderjaar 2015–2016, 34 300 VI, nr. 2, p. 70. Available at: <https://www.rijksoverheid.nl/documenten/begrotingen/2015/09/15/vi-veiligheid-en-justitie-rijksbegroting-2016>.
- 11 *Rijksbegroting 2015 x Defensie*. Tweede Kamer, vergaderjaar 2014–2015, 34 000 X, nr. 1, p.96. Available at: <https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/begrotingen/2014/09/16/x-defensie-rijksbegroting-2015/x-defensie.pdf>.
- 12 *Begroting 2015-2019 Nationale Politie*. Nationale Politie, p.41. Available at : <http://www.rijksbegroting.nl/binaries/pdfs/begroting-np-2015.pdf>
- 13 *Rijksbegroting 2015 v Buitenlandse Zaken*. Tweede Kamer, vergaderjaar 2014–2015, 34 000 V, nr. 2, p.28. Available at: <https://www.rijksoverheid.nl/documenten/begrotingen/2014/09/16/v-buitenlandse-zaken-rijksbegroting-2015>

- 14 *Net losses: Estimating the Global Costs of Cybercrime*. June, 2014, CSIS and Intel Security.
- 15 *Cyber Value at Risk in the Netherlands*. April 2016, Deloitte.
- 16 André Hendriks, Dick Brandt, Kim Turk (VKA) & Viktoria Kocsis, Daan in 't Veld, Tom Smits (SEO Economisch Onderzoek), 17 Mei 2016. *Economische Kansen Nederlandse Cybersecurity-Sector: Een verkenning*. Available at: [https://www.thehaguesecuritydelta.com/media/com\\_hsd/report/101/document/economische-kansen-nederlandse-cybersecurity-sector.pdf](https://www.thehaguesecuritydelta.com/media/com_hsd/report/101/document/economische-kansen-nederlandse-cybersecurity-sector.pdf) (last accessed 20-10-2016).
- 17 European Commission (Digital Economy & Society), *Cybersecurity Industry Market Survey*, 12 January 2016. Available at: <https://ec.europa.eu/digital-single-market/en/news/cybersecurity-industry-market-survey> (last accessed 20-10-2016).
- 18 André Hendriks, Dick Brandt, Kim Turk (VKA) & Viktoria Kocsis, Daan in 't Veld, Tom Smits (SEO Economisch Onderzoek), 17 Mei 2016. *Economische Kansen Nederlandse Cybersecurity-Sector: Een verkenning*. Available at: [https://www.thehaguesecuritydelta.com/media/com\\_hsd/report/101/document/economische-kansen-nederlandse-cybersecurity-sector.pdf](https://www.thehaguesecuritydelta.com/media/com_hsd/report/101/document/economische-kansen-nederlandse-cybersecurity-sector.pdf) (last accessed 20-10-2016).
- 19 Pierre Audoin Consultants, July 29th 2013. *Competitive analysis of the UK cyber security sector*. Available at: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/259500/bis-13-1231-competitive-analysis-of-the-uk-cyber-security-sector.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/259500/bis-13-1231-competitive-analysis-of-the-uk-cyber-security-sector.pdf) (last accessed on 20-10-2016).
- 20 Franck Nassah (Pierre Audoin Consultants), 21 March 2013. *L'Observatoire de la filière de la confiance numérique en France*. Available at : <https://www.pac-online.com/lobservatoire-de-la-fili%C3%A8re-de-la-confiance-num%C3%A9rique-en-france> (last accessed on 20-10-2016).
- 21 Bundesministerium für Wirtschaft und Technologie, August 2013. *Der IT-Sicherheitsmarkt in Deutschland: Grundstein für eine makroökonomische Erfassung der Branche*. Available at: <http://www.bmwi.de/BMWi/Redaktion/PDF/Publicationen/Studien/it-sicherheitsmarkt-in-deutschland> (last accessed on 20-10-2016).
- 22 Centraal Planbureau, 6 July 2016. *Risicorapportage Cyberveiligheid Economie*. Available at: <https://www.cpb.nl/sites/default/files/omnidownload/CPB-Notitie-6juli2016-Risicorapportage-cyberveiligheid-economie.pdf>.
- 23 Pierre Audoin Consultants, July 2013 and March 2013.
- 24 *Ibid.*
- 25 IHS, 11 May 2016. *New Regulations Impact EMEA Cybersecurity Market in 2016, IHS Says*. Available at: <http://press.ihs.com/press-release/technology/new-regulations-impact-emea-cybersecurity-market-2016-ihs-says>.
- 26 *Ibid.*
- 27 *Ibid.*
- 28 André Hendriks, Dick Brandt, Kim Turk (VKA) & Viktoria Kocsis, Daan in 't Veld, Tom Smits (SEO Economisch Onderzoek), 17 Mei 2016. *Economische Kansen Nederlandse Cybersecurity-Sector: Een verkenning*. Available at: [https://www.thehaguesecuritydelta.com/media/com\\_hsd/report/101/document/economische-kansen-nederlandse-cybersecurity-sector.pdf](https://www.thehaguesecuritydelta.com/media/com_hsd/report/101/document/economische-kansen-nederlandse-cybersecurity-sector.pdf).
- 29 *Ibid*, p.4.
- 30 Susan, Moore. *Gartner Says Worldwide Information Security Spending Will Grow Almost 4.7 Percent to Reach \$75.4 Billion in 2015*. Available at : <http://www.gartner.com/newsroom/id/3135617>

- 31 Steve Morgan, *Cybersecurity Market Reaches \$75 billion in 2015; Expected to Reach \$170 Billion by 2020*, Forbes, 20 December 2015. Available at: <http://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/>'\ '5adf4b002191.
- 32 Markets and Markets, 2015. *Cyber Security Market worth 202.36 Billion USD by 2021*. <http://www.marketsandmarkets.com/PressReleases/cyber-security.asp> (last accessed 21-10-2016).
- 33 Steve Morgan, *Cybersecurity Market Reaches \$75 billion in 2015; Expected to Reach \$170 Billion by 2020*, Forbes, 20 December 2015. Available at: <http://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/#5adf4b002191>.
- 34 *Ibid.*
- 35 Markets and Markets, 2015. *Cyber Security Market worth 202.36 Billion USD by 2021*. <http://www.marketsandmarkets.com/PressReleases/cyber-security.asp> (last accessed 21-10-2016).
- 36 Steve Morgan (CSO), 15 September 2015. *New cybercrime wave drives IoT security spending*. <http://www.csoonline.com/article/2984193/cyber-attacks-espionage/new-cybercrime-wave-drives-iot-security-spending.html> (last accessed 21-10-2016).
- 37 PricewaterhouseCoopers, 16 September 2015. *Cyber insurance market set to reach \$7.5 billion by 2020*. <http://press.pwc.com/News-releases/cyber-insurance-market-set-to-reach--7.5-billion-by-2020/s/5CC3FA21-221C-43DF-A133-05435E365342> (last accessed 21-10-2016).
- 38 *Ibid.*
- 39 Bhawna Kohli (Allied Market Research), 2015. *Managed Security Services Market Is Expected to Reach \$40.97 Billion, globally by 2022*. Available at: <https://www.alliedmarketresearch.com/press-release/managed-security-services-market.html>.
- 40 Steve Morgan (CSO), 15 September 2015. *New cybercrime wave drives IoT security spending*. Available at: <http://www.csoonline.com/article/2984193/cyber-attacks-espionage/new-cybercrime-wave-drives-iot-security-spending.html>.
- 41 Price Water House Coopers, 16 September 2015. *Cyber insurance market set to reach \$7.5 billion by 2020*. Available at: <http://press.pwc.com/News-releases/cyber-insurance-market-set-to-reach--7.5-billion-by-2020/s/5CC3FA21-221C-43DF-A133-05435E365342>.
- 42 Steve Morgan (CSO), 26 March 2015. *CISOs turn to security awareness solutions to change poor employee behaviors*. Available at: <http://www.csoonline.com/article/2926173/security-awareness/cisos-turn-to-security-awareness-solutions-to-change-poor-employee-behaviors.html>.
- 43 *Ibid.*
- 44 *Ibid.*
- 45 Price Water House Coopers, 2016. *Turnaround and transformation in cybersecurity, The Global State of Information Security Survey 2016*. Available at: <http://www.pwc.ru/riskassurance/publications/assets/gsis2016-report.pdf>

- 46 Nationaal Cyber Security Centre, *National Cyber Security Strategy 2*. October 29, 2013. Available at: (<https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf>).
- 47 Nationaal Cyber Security Centre, '*Cyber Security Assessment the Netherlands CSAN2015*', December 2015. Available at: <https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2015.html>.
- 48 Alert Online (en), 'Alert Online 2016,' text/html, *Alert Online (En)*, (October 19, 2016), <https://www.alertonline.nl/en/home>.
- 49 Steve Morgan (CSO), 26 March 2015. *CISOs turn to security awareness solutions to change poor employee behaviors*. <http://www.csoonline.com/article/2926173/security-awareness/cisos-turn-to-security-awareness-solutions-to-change-poor-employee-behaviors.html> (last accessed 21-10-2016).
- 50 'Expertise & Advice,' *National Cyber Security Centre*, accessed October 19, 2016, <https://www.ncsc.nl/english/services/expertise-advice>.
- 51 'Cyber Security Assessment the Netherlands CSAN2015.'
- 52 Claire Vishik (Intel), Maritta Heisel (University Duisburg-Essen). *Cybersecurity Education snapshot for workforce development in the EU*. September, 2015.
- 53 Centraal Bureau voor de Statistiek, *ICT, Kennis en Economie, Centraal Bureau Statistiek*, 2016, p.7. Available at: <https://www.cbs.nl/nl-nl/publicatie/2016/26/ict-kennis-en-economie-2016>.
- 54 Mamertino, Mariano. *Dit zijn de 10 banen van de toekomst*. MT, 9 March 2016. Available at: <http://www.mt.nl/management/dit-zijn-de-10-banen-van-de-toekomst/89160>.
- 55 Price Water House Coopers, 2016. *Turnaround and transformation in cybersecurity, The Global State of Information Security Survey 2016*. Available at: <http://www.pwc.ru/ru/riskassurance/publications/assets/gsis2016-report.pdf>
- 56 André Hendriks, Dick Brandt, Kim Turk (VKA) & Viktoria Kocsis, Daan in 't Veld, Tom Smits (SEO Economisch Onderzoek). 17 Mei 2016. Economische Kansen Nederlandse Cybersecurity-Sector: Een verkenning. [https://www.thehaguesecuritydelta.com/media/com\\_hsd/report/101/document/economische-kansen-nederlandse-cybersecurity-sector.pdf](https://www.thehaguesecuritydelta.com/media/com_hsd/report/101/document/economische-kansen-nederlandse-cybersecurity-sector.pdf) (last accessed 20-10-2016).
- 57 *Ibid.*
- 58 Nationaal Cyber Security Centre, *National Cyber Security Strategy 2*. October 29, 2013. Available at: (<https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf>).
- 59 The Hague Centre for Strategic Studies, 'NWO Funded Cyber Security Research: A Bird's Eye View of the Current Research Portfolio', 2015.
- 60 'Nieuwe Impuls Voor Cyber Security Onderzoek,' June 28, 2012, <http://www.nwo.nl/en/news-and-events/news/2012/new-boost-for-cyber-security-research.html>.
- 61 'Dutch Cyber Security Council,' Cyber Security Raad, (August 20, 2016), <https://www.cybersecurityraad.nl/index-english.aspx>.
- 62 'About Us,' dcypher, available at: <https://www.dcypher.nl/en/content/about-us>.

- 63 'Government and NWO Invest More than 6 Million Euros in Cyber Security Research,' accessed October 19, 2016, <http://www.nwo.nl/en/news-and-events/news/2013/ew%5B2%5D/government-and-nwo-invest-more-than-6-million-euros-in-cyber-security-research.html>.
- 64 'NWO Funded Cyber Security Research: A Bird's Eye View of the Current Research Portfolio.'
- 65 Centraal Bureau voor de Statistiek, *ICT, Kennis en Economie, Centraal Bureau Statistiek*, 2016, p.201.
- 66 'Cyber Security Academy,' *Cyber Security Academy*, accessed October 20, 2016, <https://www.csacademy.nl/en/>.
- 67 'MS Cybersecurity,' *Webster University the Netherlands*, accessed October 20, 2016, <http://www.webster.nl/graduates/master-cybersecurity/>.
- 68 'Cyber Security,' *4TU.Federation*, accessed October 20, 2016, <https://www.4tu.nl/cybsec/en/>.
- 69 'Master's Specialization in Cyber Security,' *Radboud University*, accessed October 20, 2016, <http://www.ru.nl/english/education/masters/cyber-security/>.
- 70 'Bachelor Informatica en Cyber Security,' *Radboud Universiteit*, accessed October 20, 2016, <http://www.ru.nl/opleidingen/bachelor/informatica/>.
- 71 'Security and Privacy,' *EIT Digital Master School*, accessed October 20, 2016, <http://www.masterschool.eitdigital.eu/programmes/sap/>.
- 72 'LLM Law and Technology,' *Tilburg University*, accessed October 20, 2016, <https%3A%2F%2Fwww.tilburguniversity.edu%2Feducation%2Fmasters-programmes%2Flaw-and-technology%2F>.
- 73 'Nyenrode Business University | Dcypher,' accessed October 20, 2016, <https://www.dcypher.nl/nl/content/nyenrode-business-university>.
- 74 'University of Applied Sciences Leiden | Dcypher,' accessed October 20, 2016, <https://www.dcypher.nl/en/content/university-applied-sciences-leiden>.
- 75 'University of Applied Sciences Rotterdam | Dcypher,' accessed October 20, 2016, <https://www.dcypher.nl/en/content/university-applied-sciences-rotterdam>.
- 76 'Zuyd University of Applied Science | Dcypher,' accessed October 20, 2016, <https://www.dcypher.nl/en/content/zuyd-university-applied-science>.
- 77 'IT-Security & BCM Opleidingen | Security Academy Nederland,' accessed October 20, 2016, <https://www.securityacademy.nl/opleidingen>.
- 78 'National Cyber Security Summer School 2016,' *HSD The Hague Security Delta*, accessed October 20, 2016, <https://www.thehaguesecuritydelta.com/events/event/1095-national-cyber-security-summer-school-2016-2016-08-22>; 'International Cyber Security Summer School,' *INTERNATIONAL CYBER SECURITY SUMMER SCHOOL*, accessed October 20, 2016, <http://summerschoolcybersecurity.weebly.com/>.



*The Hague* Centre for Strategic Studies

Lange Voorhout 16  
2514 EE The Hague  
The Netherlands

info@hcass.nl  
HCSS.NL