Summary

Reason and purpose of the study

A shortage of Cyber Security Professionals (CSPs) is a great vulnerability to the resilience of the vital sectors. In the "National Cyber Security Strategy 2 (NCSS2): From awareness to capability" (2013), it is emphasized that the Government wishes to have sufficient cyber security knowledge and skills. In this context, it is important that in the short and (medium) long term, there is a balance between demand and supply on the labor market for CSPs in private and public organizations. For this reason, the National Coordinator for Security and Counterterrorism (NCTV) wants to gain insight into the nature and scope of a (possible) shortage of these professionals (both technical and non-technical) and identify solutions in order to reduce these possible shortages in the short and (medium) long term. In this context, PLATO BV of the University of Leiden has conducted a labor market study into the demand and supply of Cyber Security Professionals in cooperation with Ockham IPS. This study is commissioned by the Research and Documentation Center (WODC).

Research questions

The following research questions are central to this study:

- To what extent can a possible qualitative and quantitative shortage of Cyber Security Professionals at higher and secondary level be expected, now and in future?
- How could these shortages in the existing and future labour market for Cyber Security Professionals be solved?

Study design and approach

In this research, the labour market for CSPs will be approached as a domain in which supply of and demand for professionals in the area of cyber security come together and (try to) find each other. In terms of gaining insight into the demand, the focus in this study is on vacancy analysis. In terms of the supply side, the study focuses on the education and training opportunities.

To gain answers to the research questions from various relevant perspectives and sources, other research methods have been used too. The study consisted of the following, partly overlapping components:

- Literature study into cyber security, the work field, characteristics and job profiles of CSPs. This included policy literature and academic literature, both Dutch and international literature.
- Analyses of the social context and developments (politically, economically, socially, technologically and legally) that influence the supply of and demand for CSPs.
- Vacancy research (with the help of vacancy spider Job feed[1] of Text kernel).
- Inventory and analyses of the education and training opportunities and inventory of the numbers of students. In this context, internet research has been conducted and 18 education providers have been consulted (by means of 18 interviews, partly face-to-face and partly by telephone).
- Preliminary and in-depth interviews (partly face-to-face and partly by telephone) with employers and employees in the private and public domain. In total, there were 34 interviews spread across 25 organizations.
- Expert meeting. This meeting was held in the final stages of the study, with the aim of discussing the discrepancies found between supply and demand as well asareas in which solutions may be found. Seven participants of these various organizations were involved in the expert meeting.

[1] http://www.jobfeed.nl/

Cyber security

Cyber security is a rather ambiguous concept. The various definitions of cyber security found in literature often emphasize information security and IT. Cyber security should not be interpreted too restrictively. The term cyber security refers to the vulnerability of companies, citizens, government and society as a whole. These vulnerabilities as well as their solutions have both technical IT aspects and interactive (human-IT) aspects. This is what makes cyber security an organizational issue in addition to a technical issue.

Conclusion 1: Cyber security is both an IT and an organizational issue.
Most of all, cyber security should be seen from a wider organizational perspective in which various roles and tasks are to be fulfilled.

The work field of Cyber Security Professionals

The work field of the Cyber Security Professional is strongly subject to change. The rapidly changing digital world with its threats and essential safety criteria sets high standards for public and private organizations being or becoming cyber secure. Both the frequency and the impact of incidents, in terms of direct and indirect damages (such as reputational damage), are increasing. Companies and public organizations are more and more aware of the fact that cyber security is not just an IT issue; it is an integral theme. Cyber security has gone from an IT issue to a 'boardroom issue,' because the survival of the company could be at stake. Growing policy attention to cyber security, the necessity to be aware of the risks (since the internet is present in all areas of daily life) and changes in legislation (with regard to privacy and data protection) have an additional driving effect on the development of demand.

Conclusion 2: Two factors keep the work field of the Cyber Security Professional rapidly changing. On the one hand, it is about societal developments (at political, economic, social, technical and judicial level). On the other hand, incidents (depending on the frequency and impact) call for adjustments in the work field.

Position groups

In the literature, three dimensions emerge on which the positions of Cyber Security Professionals can be described:

- Work activities can be classified as technically dominant or not technically dominant. Technically dominant implies that the focus is on the IT perspective. The not technically dominant positions focus more on the organizational perspective.
- The position can be specifically focused on cyber security or have cyber security as a component.
- The position can be oriented operational-tactically or tactical-strategically.

Based on these dimensions and on the analysis of vacancy descriptions, four position groups may be distinguished:

1) *Technically dominant specialist cyber-security positions*. These positions are focused very specifically on IT/information security and have a large technical component. Examples of positions are ethical hackers, penetration testers, software testers and technical security engineers.
2) *Not technically dominant specialist cyber-security positions*. These cyber security specialists look at security more from an organizational perspective. Job examples are IT security officers, IT security specialists, security officers, information security officers.

3) *Technically dominant positions of which cyber security is a component*. These professions are technical in nature but not specialized in cyber security. This is a large group of professions that require or preferably require a cyber-security related certificate. Job examples are system operators, software developers and architects.
4) *Not technically dominant positions of which cyber security is a component*. This is the least defined position group. It contains numerous positions, such as policy advisors, lawyer, directors and auditors. With these positions, cyber security can be subject of the core activity (for example, a lawyer specialized in privacy issues or a policy advisor in the field of cyber security). Furthermore, it concerns positions that view cyber security as part another domain rather than as core of the work (for example, part of policy making, jurisdiction).

The distinction operational-tactical and tactical-strategic is reflected in all four position groups.

Conclusion 3: Based on the literary and analysis of vacancy descriptions, four position groups are distinguished for the Cyber Security Professional that may be used in relation to labour market research:
- *Technically dominant specialist cyber-security positions.*
- *Not technically dominant specialist cyber-security positions.*
- *Technically dominant positions of which cyber security is a component.*
- *Not technically dominant positions of which cyber security is a component.*

The demand for Cyber Security Professionals and the total CSP employment

In the first three quarters of 2014, a total of 916 vacancies have been published related to the security domain. On an annual basis (during the last quarter of 2013 and the first three quarters of 2014) there were 1,158 published vacancies in the field of cyber security. The total demand will be higher, because informal recruitment channels and challenges[2] aimed at recruitment do not count as vacancies in the vacancy analysis.
To get an impression of total employment (the total number of jobs) in the security domain, we draw a comparison with the number of published vacancies and employment in the broader IT sector. In the broad IT sector, one vacancy equals six jobs.[3] If we apply the same relationship between vacancies and jobs in the security domain, the total employment in the security domain is estimated at 7,000 jobs based on this.

Based on the environmental analyses (the societal interest and the role of incidents increase, see conclusion 2), it is expected that the demand for Cyber Security Professionals will increase. On the one hand, the urgency to apply knowledge and skills in this field increases. On the other hand, the cyber-security domain is increasingly seen as an organizational and as a multidisciplinary matter.
The expected rise in demand applies to all four position groups as well as to adjacent positions. The cyber domain is an important part of life, which is why various adjacent positions in which knowledge of cyber security is indispensable, are necessary.
A distinction must be made between the demand in positions at the level of Upper Secondary Vocational Education, Higher Vocational Education and University. Because of digitization and automation, the demand for professionals with Uppper secondary Vocational Education is decreasing, whereas the demand for higher educated professionals is increasing.

[2] A 'challenge' in this study is referring to a recruitment activity with a *gaming* character during which issues related to cyber security must be solved.

[3] In 2013, total employment in the IT/automation sector was approximately 300,000 (Panteia based on P-Direkt and Dutch Labour Force Survey, Statistics Netherlands). The total number of vacancies on an annual basis is approximately 50,000 (Panteia/PLATO based on vacancy analysis Job Feed). The ratio between the number of vacancies and total employment is therefore 1 : 6.

Conclusion 4: Even though the number of visible vacancies is still modest, there are indications (increase in urgency and a broader interpretation of the cyber-security domain) that the demand for CSPs (in its totality) will increase in the future. The increase will mainly apply to higher educated professionals and less to professionals with Upper Secondary Vocational Education.

The nature of the demand for the four position groups as identified in this study may best be defined as follows:

1) *Technically dominant specialist cyber-security positions*. Aside from big employers (banks, police and defence), the labour market for this profile is dominated by consultancy companies. These specialists (hackers, penetration testers) share the role of front-runner in the development of cyber security with cyber criminals. In order to keep up with the technological developments of cybercrime, the demand for these specialists will rise steadily.
2) *Not technically dominant specialist cyber-security positions*. The labour market for this position profile has a more diverse range of demanding organizations. Hiring this type of CSP is the first step for many organizations to straightening out cyber security. In many cases, one CSP is sufficient for organizing the security. Specialist tasks are performed by hiring a third party. After strong growth in the first five years, the demand for not technically dominant specialist cyber-security positions will decline lightly, because organizations have embedded cyber security in their organizations. At that point, however, the replacement demand will also start to play a role in the development of demand. Vacancies in relation to this position group often ask for experienced people.
3) *Technically dominant positions of which cyber security is a component*. In the labour market for this position group, the highest increase in demand is expected. This market is dominated by software developers. In recent years, these companies have been committed to improved security of their software (secure by design) and they demand IT people with experience in the domain of security, security certificates or security affinity. Since a growing number of organizations can be seen as software companies (IT is the core of many companies), the demand for these technicians increases in future. The demand for safer systems resonates in the system development and system management.
4) *Not technically dominant positions of which cyber security is a component*. The labour market for this position profile has a multitude of different positions, and some professionals might not even realize that they deal with cyber security. In future, competences regarding cyber security-related tasks will be asked more often and more explicitly.

Conclusion 5: An increase in the demand applies to all position groups, but the largest growth is expected in the technically dominant positions of which cyber security is a component.

Supply of Cyber Security Professionals from education and training

In this research, over eighty different types of supply have been inventoried. If the number of supply locations is incorporated, it involves many hundreds of training programs and other forms of supply. The training supply related to cyber security is extremely varied and extensive. Many forms of education co-exist, such as graduate and post-graduate programs, short courses, master classes, workshops, seminars, learning through practice, distance learning and in-company training.
The trainings are offered on numerous locations. There are graduate and post-graduate programs from Upper Secondary Vocational Education to University. In the private sector, the supply is huge as well. The focus here is on keeping the knowledge and skills

of working professionals up-to-date. With regard to the content and depth, the supply is varied as well. This includes educational programs with clear technical and IT contents as well as programs with clear security, legal or forensic contents. There are also programs that train participants indirectly but in-depth in courses and competences relevant to cyber security. This category includes educational programs that have a strong IT component, but that focus on areas other than technology or security, such as artificial intelligence, methods and technologies studies, medical information technology, logistics, measuring and regulations technology, etc. In conclusion, there is a much wider range of educational programs that contribute to students' knowledge and skills other than the programs directly aimed at IT, or internet and cyber security.

The multitude of courses, educational programs and other forms of supply, however, also lead to lack of transparency of the supply. Information about educational programs and processes are retrievable, but no clear overview of the educational possibilities in relation to the competences in which participants want to and/or have to be educated exists.

Conclusion 6: The educational supply regarding cyber security is varied and extensive. Educational programs are often offered on various locations and there is much variation in types of education or training. At the same time, the supply is not transparent.

Regarding the supply of professionals from education and training, a sufficient number of participants seem to be in a relevant training program in 2014:

- An inflow of 6,880 students at Upper secondary Vocational Education level 4;
- An inflow of 73 students at Higher Vocational Education associated degree level;
- An inflow of 4,053 students at Higher Vocational Education level;
- An inflow of 292 students at Master level;
- An inflow of at least 200 participants in post academic and post-executive Masters (as appears from the interviews).

Therefore, there is a great potential of people who appear to be employable in principle. Even if we take into account a dropout rate of 50%, the numbers remain high compared to the available vacancies. At the same time, these numbers only lead to an inflow into cyber security related positions to a very limited extent. Upper secondary Vocational Education students often continue their studies in Higher Vocational Education. Many broader Higher Vocational Education and University programs have included cyber security in their programs to a limited extent only, and there are only few specialist cyber-security programs. This means that students do not, or only relatively late, include cyber security as an option in their studies or career.

Conclusion 7: The education potential is, in principle, sufficient to meet the demand for CSPs. The question is whether participants in cyber security related programs view cyber security as a possible career option.

Found discrepancies between supply and demand

Found discrepancies at research question 1: To what extent can a possible qualitative and quantitative shortage of Cyber Security Professionals at higher and secondary level be expected, now and in future?

In the relation between the supply of and demand for CSPs, lack of transparency and qualitative discrepancies can be ascertained rather than quantitative discrepancies. The challenge lies not in educating more people, but in sparking people's interests in cyber security and jobs in said area during their education. The problems in connectivity

(discrepancies between supply and demand) that organizations experience are of a qualitative nature rather than of a quantitative nature, or they are a result of a lack of transparency of the labour market. In short, the following discrepancies arise:

- While students are trained in areas relevant to cyber security, they miss a specific focus on cyber security.
- Many organizations have insufficient knowledge about what they need, who they look for and where to find them.
- There is sufficient supply; however, the professionals do not have the desired level of expertise yet. They lack (depending on the position and tasks) either the technical knowledge or the organizational knowledge.
- Professionals have gotten cyber security as an additional subtask, but they are not specifically trained in that area. Since they have many other tasks, rapid development of competences in the field of cyber security is not easily done.

Conclusion 8: Quantitatively, there is no shortage in the supply. The match between the demand for CSPs and the supply of these professionals is obstructed by qualitative discrepancies and a lack of transparency.

Solution areas to found discrepancies

This concerns answering the second research question: How could these shortages in the existing and future labour market for Cyber Security Professionals be solved? In other words, how can the match between supply and demand be improved? In the study, the following (also emphasized by experts in the field of cyber security) directions in which solutions may be found emerge:

1. *Use the possibilities of education in solving discrepancies.*

Education can play a major role in solving discrepancies. This includes raising awareness amongst pupils and students in general, motivating some of these students to make a study selection relevant to cyber security, and providing an even more select group of students with appropriate and expert training. Learning and specializing in a rapidly developing field as cyber security requires a lifelong-learning approach. In the context of lifelong learning, it is important to look for efficient and effective ways to develop and share knowledge in work situations, and to translate that into improvements and innovations. The work environment goes beyond the borders of one's own organization.

Aside from professionalization in the sense of personal development in the profession, there is also the necessity of development in the field. Cyber security is a domain in which much work is done in numerous public and private (small and bigger) organizations and industries at various levels. The educational world also contributes to the developments in the cyber security domain. Collaboration between all parties involved is of vital importance in keeping the cyber security sector and those who work in it up to date. This is demonstrated by the active involvement of IT companies in academic programs, in participation of practitioners as teachers in higher education programs, and in the participation of scientists in solving practical problems.

2. *Change the work processes in organizations and collaboration between organizations in order to upgrade the level of cyber security and maintain it.*

In the study as a whole, the following possibilities have emerged in this regard:

- Create opportunities in and between organizations to share knowledge and to learn from each other;
- Improve secondary employment conditions/benefits, which can make the work more attractive to more groups, such as women;
- More efficient and specific recruitment (also within one's own organization, by pointing out the possibilities of growth in a cyber-security related position to prominent employees);

- Deployment of a pool of professionals from various organizations, outsourcing and hiring external specialists;
- Make visible the work of the CSP within the organization and its use;
- Establish and make use of a less hierarchical organizational structure (applies to larger organizations).

3. Clarification of education and training paths.

The relation between training paths, the competences to be acquired, positions to be fulfilled, and positions to be achieved in the labour market is diffuse. The paths that support career developments in cyber security are too. Making choices in the galore of possibilities is not always easy. Both the people concerned and the organizations experience the disadvantages of that. It means that too often, the right man or woman ends up in the wrong place. It leads to inefficient and ineffective training and career paths. Clarification of the education and training paths will have a positive effect on the quality of the supply and the guidance of outflowing participants and students to positions in the field of cyber security. This solution also points towards lifelong learning. The work field of cyber security asks for continuous updating of knowledge and skills. In this regard, the necessity to create and establish a system of maintenance, update and development of knowledge grows.

4. Monitor developments in society, education and courses, and the labor market. The resulting data can positively influence the match between supply and demand in the short and (medium) long term.

In line with solution three, data acquisition and registration on study programs and the demand on the labor market can be a usable resource for quality improvement. The study into the labor market for Cyber Security Professionals, as described in this report, provides a state of affairs. Society as a whole and the work field of CSPs are changing rapidly. A form of monitoring of developments in society, the labour market and the education market can contttribute to the match between the demand for and supply of CSPs in the shorter and longer term.

5. Creating a stronger and more challenging image of the cyber-security work field and positions.

Cyber security positions are often associated with a specific type of ethical hackers who get lost in their jobs completely (black t-shirts, ponytails etc.). On the other hand, cyber security positions are associated with 'troublemakers in the organization:' because of their focus on everything that could go wrong, they are a bit difficult in the eyes of others. The challenging, progressive and complex aspects of the work may be placed to the forefront. A different issue is that the sector predominantly consists of men. In the domain of cyber security, various positions requiring different types of competences can be fulfilled. This makes the work field interesting for both men and women. A positive image of the possibilities and challenges creates a larger pool. Instructions, courses and public actions (in the form of challenges) could also contribute to change.

6. Take on cyber security as a common responsibility of citizens, government, organizations and education: aimed at raising awareness.

All organizations and experts consulted agree: cyber security is a matter that influences the life of almost every citizen. Therefore, it is important to work on raising awareness of society as a whole. The purpose of this is to make everyone aware of the risks and to defend themselves against and of the means to do so. This has resulted in a desire to train and use experts who can reach this broader range of citizens with the message that cyber security calls for alertness, precautions and audits in the field of information security.

This also implies that cyber security should be seen as something that plays a role anywhere anytime people work and interact with IT systems. It is also a task for basic

education (primary and secondary education). How this should be shaped will have to be researched in future studies.

Conclusion 9: Solutions for discrepancies in the labor market for CSPs cover:

1. *Use the possibilities of education in the field of, inter alia, raising awareness, study selections, clarification of study paths and opportunities for lifelong learning in the area of cyber security.*
2. *Strengthen and improve work processes in organizations and stimulate collaboration between organizations.*
3. *Clarify study and training paths.*
4. *Monitor developments related to the labor market of CSPs.*
5. *Improve and strengthen the image of the cyber-security work field and the CSP.*
6. *Continue on the chosen path to approach cyber security as a common responsibility of citizens, government, organizations and education: aimed at raising awareness.*