Summary

Technological progress has enabled the world around us to become more and more digital. Just like the industrial revolution, digitization has brought us into a new digital age and has an impact on many aspects of our lives. Some examples of this are international interconnectivity, acceleration of innovation, online opportunities, but also competitiveness on a global scale. Besides the benefits of digitization, it is also important to consider the risks brought about by a digital economy. The world around us is becoming more and more dependent on IT and the impact of system failures or malicious breaches is becoming ever greater. As a result, securing the cyberspace, also known as cybersecurity, has become increasingly important.

In the past decade, both public and private interest in cybersecurity has risen. In addition, awareness of cybersecurity has increased due to an ever-growing list of cyber threats. Especially since 2015, consumer markets have experienced the rise of cyber threats such as hacking, malware and data leaks.

Cybersecurity comprises all aspects of security that have an impact on the cyberspace. It covers the technical aspects such as cryptography and access control that are used to protect data, but also the operational and management mechanisms used to operate and maintain digital systems. The main infringements that are a result of shortcomings in cybersecurity include phishing, malware, human error, theft and loss of data.

The goal of this study is threefold, namely:

- to map the current developments in Flanders in the field of cybersecurity;
- to compare the position of Flanders with a number of countries, both within and outside Europe;
- to formulate recommendations as a basis for the elaboration of policy initiatives and government interventions to further support developments in the field of cybersecurity in Flanders.

We have examined various indicators based on desk research and discussions with subject-matter experts. As a result, we can state that the current Flemish cybersecurity ecosystem has its strengths, but that its position could be strengthened even more on the following dimensions:

1. Education
2. Research
3. Businesses
4. Policy initiatives
5. Security awareness

Education

An important stimulus for increasing the Flemish cybersecurity talent pool is providing an appropriate educational offer. Today, cybersecurity is already present in the Flemish educational offer in the form of programs that are entirely dedicated to ICT security, specializations within an existing master's or bachelor's program or as a supplementary course.

Also in foreign countries, various programs on cybersecurity are offered. Some countries such as France go even further and certify master's and bachelor's programs in order to guarantee the quality level for both students and employers.

In other countries, such as the Netherlands, universities are joining forces to jointly offer a master's degree in cybersecurity. This is the case, for example, at the Cyber Security Academy, which was established by the University of Leiden, the Delft University of Technology and The Hague University of Applied Sciences.

Despite the presence of cybersecurity in the higher education of Flanders, only a limited number of students graduate each year. In this study, various recommendations are formulated to improve cybersecurity education and to increase the number of graduates from a few dozen to a hundred students per year.

We recommend improving the cooperation between Flemish universities, following the example of Brussels and Wallonia or the Netherlands, and jointly offering a Master in Cybersecurity. It seems appropriate to us that such a cooperation should be realized between equal partners, each of whom contributes their relevant expertise. Certifying cybersecurity programs can also help guarantee their general quality level.

Providing information on cybersecurity early on can also help to raise awareness in our future talent pool and to stimulate more young people in choosing a professional career in cybersecurity.

Research

Flanders has various research centers for cybersecurity. Those research centers that are part of Flemish universities such as ESAT-COSIC (KU Leuven) are the front-runners here. Attention is also paid to cybersecurity within Flanders Make and imec. Furthermore, there are organizations such as the Flemish Agency for Innovation and Entrepreneurship, the Research Foundation of Flanders and the Institute for Innovation by Science and Technology, that also support pioneering scientific research through scholarships and project funding.

In the benchmark countries, research centers are also present that are engaged in cybersecurity research, such as the Cyber Security Lab in the Netherlands. In Germany, the Ministry of Education and Research supports several competence centers for IT security.

Flemish universities are known for the progress of their research in cybersecurity and cryptography where publications are concerned.

Even though the number of cybersecurity related patents has doubled in Belgium over the last decade (a total of 48 in 2018), we score the worst when we compare this number with the benchmark countries. For comparison, the United States and China each registered 10.000 and 1.244 patents, respectively.

For that reason, it seems favourable to strengthen the leading academic position by providing additional support to specialized researchers. The commercial value of research and prototypes can additionally be encouraged by granting stimulants for research. This might have a positive influence on patent applications and spin-offs in the long term of Flemish universities.

Businesses

If we inspect the labor market, we clearly notice a gap between the supply and demand of cybersecurity related jobs. An important reason for this talent shortage is the fact that every year only a handful of cybersecurity professionals graduate.

Flanders has around 2.000 cybercrime specialists, as compared with 46.000 in the Netherlands. Search results from LinkedIn profiles also show that there are significantly fewer cybersecurity professionals in Flanders than in the benchmark countries. This translates into a higher number of outstanding cybersecurity related vacancies.

It is therefore important that the educational offer is tailored towards the needs of the private sector and that high-quality cybersecurity related trainings are provided. In addition, partnerships between universities and the private sector could also be encouraged, such as guest lecturers and internships. In the meantime, it is important to assist companies in providing continuous development of their human capital through on-the-job training and certification programs on cybersecurity.

None of the cybersecurity companies based in Flanders are in the Cybersecurity 500 List. The majority of these companies (72%) are located in the United States.

A number of spin-offs and start-ups have also emerged from various Flemish universities. Some examples are n-Auth (ESAT-COSIC – KU Leuven), Custodix (UGhent), and HI10 (UAntwerp). At the global level, the main spin-offs are located in the United Kingdom and the United States. In the list of the most famous spin-offs from VentureRadar, we note that HI10 is just outside of the top 10.

Existing, but also new spin-offs can be assisted in their further development through better financing and with the help of business, marketing and legal support. In addition, the cooperation between spin-offs and industrial actors can also be encouraged.

Flanders Investment & Trade is currently working on guiding foreign investors in setting up their activities in Flanders via the ICT Welcome Team. In order to ensure that more companies become interested in establishing themselves in Flanders, more investments must be made in human capital through education and continuous development of existing professionals, as previously mentioned. In addition, it is important to promote the cooperation between the various actors in the cybersecurity ecosystem (enterprises, education and government).

Policy initiatives

In the context of policy initiatives, the Center for Cyber Security occupies the most important role. They operate on a national scale and are mainly involved in sensitizing, advising and helping government bodies and public institutions to implement security standards and guidelines. In addition, they also work together with the government in the event of cyber incidents. In 2015, they drew up a national Cyber Emergency Response Plan for handling cyber incidents on a national scale.

The other countries in this study have similar policy initiatives. For example, the French ANSSI is, among other things, responsible for the accreditation of cybersecurity trainings and actively contributes to the education policy. It is important to see this in the right perspective. The Belgian CCB currently employs about fifteen people and plans to grow to around thirty. In France and Germany, the ANSSI and BSI each have more than six hundred employees.

Neither Belgium nor Flanders currently have a laboratory for the technical certification of security products. Setting up such a lab, or expanding and supporting the functioning of an existing lab, would have a positive effect on governments, companies and researchers.

Security awareness

Cybersecurity also includes securing the human aspect of organizations. Raising awareness among employees can be done by explaining to which safety risks they are exposed, by showing that they too can be the target of a cyber attack, regardless of their position within the company.

It is important to keep creating awareness. Because even today, in a world where both the public and private sectors are already taking initiatives to raise awareness, 20% of the breaches in organizations are still due to human error.

That is why it remains important to encourage organizations to develop safety awareness programs or to continually improve existing programs. Such a program should be in accordance with the size of the respective organization. For an SME of 50 people this is a part-time effort of one person; according to SANS, however, this can amount to at least 2,6 FTE for a mature awareness program within an international company. The appointment of safety awareness ambassadors is a step in the right direction.