TALLINN UNIVERSITY OF TECHNOLOGY

Department of Computer Science

TUT Centre for Digital Forensics and Cyber Security

ITC70LT

Sophio Sakhokia 122795IVCMM

# PROPOSAL FOR A CYBER SECURITY MASTER’S PROGRAMME CURRICULUM FOR GEORGIA

Master Thesis

Tiia Sõmer
Master of Science
Early Stage Researcher

Tallinn 2017

# Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Sophio Sakhokia

18.05.2017

# Abstract

Increasing dependence on information technology in Georgia leaves businesses and the government vulnerable to cyber threats. Georgia experienced cyber attacks on its cyber space from Russia during the cyber war in 2008. Since then Georgia has carried out various works towards improving and reinforcing its cyber space, developing education is part of the overall development process. The purpose of the thesis is to build a high-level description of a curriculum based on which more specific courses can be developed. To achieve the purpose the author has studied the cyber security environment in Georgia and cyber security goals of the country based on the national guiding documents and the survey conducted among the IT professionals in Georgia. Already existing successful cyber security programmes were examined to facilitate the curriculum development process. Existing guiding principles were considered, such as National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF) and suggestions offered by Dampier, to tailor the cyber security master programme to meet the cyber security skills need in Georgia.

This thesis is written in English and is 70 pages long, including 6 chapters, 10 figures and 23 tables.

# Anotatsioon

## Ettepanek küberkaitse magistriõppe ainekavaks Georgiale

Georgia järjest kasvav sõltuvus infotehnoloogiast muudab nii era- kui avaliku sektori küberohtudele haavatavaks. Georgia küberruum sattus 2008 aastal Venemaalt pärinevate küberrünnakute sihtmärgiks. Sellejärgselt on Georgia viinud läbi mitmeid uuendusi kindlustamaks oma küberruumi, vastava hariduse arendamine on üks osa sellest protsessist. Käesoleva väitekirja eesmärk on luua üldine õppekava kirjeldus, mille põhjal saab välja töötada täpsemad kursused. Autor on oma eesmärgi saavutamiseks uurinud küberturvalisusega seotud keskkonda ja riiklikel juhisdokumentidel põhinevaid küberturvalisusega seotud eesmärke. Samuti viis autor läbi uurimuse Georgia IT-professionaalide seas. Lisaks analüüsiti juba olemasolevaidd küberturvalisuse alaseid programme. Lisaks analüüsiti juba olemasolevaid küberturvalisuse alaseid magistriõppe programme. Georgia küberturvalisuse alaste teadmiste vajadusele vastamise hindamiseks kasutati eksisteerivaid juhendprintsiipe, nagu näiteks National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF) ning Dampier'i soovituste nimekiri.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 70 leheküljel, 6 peatükki, 10 joonist, 23 tabelit.

# Table of abbreviations and terms

| | |
|---|---|
| **AAA** | Authentication, Authorization, Accounting |
| **AES** | Advanced Encryption Standard |
| **BCM** | Business Continuity Management |
| **BGP** | Border Gateway Protocol |
| **CEH** | Certified Ethical Hacker |
| **CHFI** | Computer Hacking Forensic Investigator |
| **CIA** | Confidentiality, Integrity, Availability |
| **CISO** | Chief Information Officer |
| **CISSP** | Certified Information Systems Security Professional |
| **CS** | Cyber Security |
| **DES** | Data Encryption Standard |
| **DNS** | Domain Name System |
| **GCHQ** | Government Communications Headquarters |
| **IDS** | Intrusion Detection Systems |
| **I/O** | Input/Output |
| **IoT** | Internet of Things |
| **IPS** | Intrusion Prevention Systems |
| **IS** | Information Assurance |
| **IT** | Information Technology |
| **KSAs** | Knowledge, Skills and Abilities |

| | |
|---|---|
| **MBA** | Master of Business Administration |
| **MCL** | Master of Cybersecurity and Leadership |
| **MSIT** | Master of Science in Information Technology |
| **MSU** | Mississippi State University |
| **NCII** | National Critical Information Infrastructure |
| **NCWF** | National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework |
| **NICE** | National Initiative for Cybersecurity Education |
| **NIST** | National Institute of Standards and Technology |
| **OS** | Operating System |
| **PGP** | Pretty Good Privacy |
| **PKI** | Public Key Infrastructure |
| **RSA** | Rivest-Shamir-Adleman |
| **SCADA** | Supervisory Control and Data Aquisition |
| **SDL** | Secure development Lifecycle |
| **SSL** | Secure Sockets Layers |
| **TCP/IP** | Transmission Control Protocol/Internet Protocol |
| **USC** | University of South California |
| **UTSA** | University of Texas, San Antonio |
| **VPN** | Virtual Private Network |

# Table of Contents

# List of figures

# List of tables

# Chapter 1. Introduction

Increasing dependence on information technology in Georgia leaves businesses and government vulnerable to cyber threats. In 2008 Georgia experienced cyber attacks on its cyberspace from Russia during which Georgian internet sources were blocked and cut off that made communication inside and outside the country impossible; government web sources were attacked causing damage of reputation; news and media sites, online discussion forums were shut down facilitating Russian media to spread false information; electronic banking services were not available for ten days [1]. Manipulating with information in cyber space has been useful tool for Russia and it does not seem to decrease as "the Russian view of modern warfare is based on the idea that the main battle-space is the mind and, as a result, new-generation wars are to be dominated by information and psychological warfare [2]". Furthermore, to broaden the topic of cyber attacks, it is worth mentioning that the sophistication of cyber attacks vary and a good example of a highly sophisticated malware can be Stuxnet [3]. To return to the Georgian case in 2008, the damage could be significant if Georgia had been highly dependent on cyber space. Since that there have been many initiations towards the development of business and innovation that inherently means growing dependence on information technologies. Georgia has to prepare to meet not only the upcoming business competition but also ensure the security of its cyber space as much as possible.

Today cyber security challenges set high demands to governments and industry. "Security, by its very nature, requires a deep understanding not just of the technology, but of security principles as well." [4] Governments worldwide acknowledge importance of cyber space due to the scope and the level of the damage cyber attacks can cause to a country. Many countries, Georgia among them, have included cyber security in the national interests.

The following thesis is an attempt to support Georgia on its way towards improving its cyber capabilities. The purpose of the thesis is to build a high-level description of the curriculum based on which more specific courses can be developed.

To proceed with a brief overview of the upcoming chapters: Chapter 2 covers research methodology and literature review. Chapter 3 looks at Georgia from three important perspectives:

1. Key points derived from the National Cyber security strategy of Georgia [5] such as main goals and principles; some of the taken steps; cyber threats to Georgia; scope and actions to develop the higher education in the field of cyber security in Georgia.
2. Future plans of Georgia according to the Socio-Economic Development Strategy of Georgia 2020 [6] [7] in additional to the additional supporting publicly available updated news. The “Georgia 2020” was developed by the Ministry of Economy and Sustainable Development and the Ministry of Finance of Georgia in 2014.
3. Current and expected need of cyber security skills in Georgia based on the survey conducted by the author among IT professionals involved in public and private companies and institutions (including education institutions) as well as for academic staff at private and state education institutions. Respondents represented the following sectors:
    - Education
    - Technology & software
    - Banking & Finance
    - Communications
    - Health & social services
    - Energy & utilities
    - Transportation
    - Entertainment & media
    - Human rights
    - Non-Governmental Organization

The main purpose of the survey was to receive the list of the skills expected to be important for Georgia for the upcoming two-four years. To achieve the purpose the author combined responses of academic staff and IT personnel to the following questions:

- Which cyber security skills are expected to be important for the respondents’ companies in two-four years according to the respondents?
- Which cyber security skills are expected to be important in two-four years in Georgia according to the academic staff?

- On which cyber security skills should the master programme focus according to the opinions of IT staff and the academic staff?

As the development of the successful cyber security master programme requires significant financial support it can be very beneficial for the country if government and private institutions can combine their capabilities. Because of this the author also tried to find out options for joint efforts.

The next chapter discusses and analyses Cyber security master programmes in USA, UK and Estonia. Cyber security programmes from USA were chosen based on the Research Report “2014 Best Schools for Cyber security” prepared by Ponemon, sponsored by HP Enterprise Security [8]. UK Cyber Security master programmes were selected from programmes certified by the Government Communications Headquarters (GCHQ) in cyber security and closely related fields [9]. Regarding the Cyber Security Master programme from Estonia, it is a joint programme of two biggest Estonian Universities, Tallinn University of Technology and the University of Tartu.

This section examines key points of the programmes, such as objectives, core courses, expected outcomes, admission criteria and career path details (if available). The author also outlines the specific characteristics of the programmes (if available any).

Chapter 5 is devoted to the development of the curriculum based on suggestions offered by Dampier and the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF). The research paper “Building a successful cyber-security program” by Dampier [10] lists six areas that are of crucial importance to build a successful cyber security programme: faculty, courses, equipment and laboratories, students, budget and credentials, but this chapter will focus only on one of them, developing the courses, taking into account the previous chapters’ works such as upcoming needs in Georgia, local and global cyber threats and the universities’ programmes’ experiences.

Finally, the conclusion chapter reviews the thesis and summarises key points of the work.

# Chapter 2. Methodology and Literature Review

This thesis is devoted to the development of a high-level description of a cyber security master's programme for Georgia based on which more specific courses can be developed. To achieve the goal, the author conducted a literature review of academic literature, guiding documents about developing cyber security workforce, explored different attitudes about building and designing cyber security master programmes. To gain understanding of high-level guidance on cyber security in Georgia, different national documents of Georgia were studied. A survey among IT professionals was conducted to have a glimpse at the cyber security environment and to examine the actual needs in Georgia.

### Literature review

National Cyber Security Strategy of Georgia 2017-2018 [5] was the main document based on which the cyber security goals of the country were derived. The strategy document is the only source that directs country cyber security policy and sets out plans and actions towards development of cyber security capacity and capabilities of the country. Future plans were outlined based on "Georgia 2020" – a document about the socio-economic development of Georgia [6].

The curriculum was built taking into account experiences of already existing successful cyber security master programmes [8] [9] [34], suggestions offered by Dampier David [10] in his research paper about Building a Successful Cyber-security Program; and the categories outlined in the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF) [12] by the National Institute of Standards and Technology (NIST).

The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF) [12] is a tool providing guidance to build a cyber security workforce. It portrays Knowledge Units, Skills and Abilities (KSA) crucial to address the whole cyber security spectrum. NCWF demonstrates a chain of Categories, Specialty Areas and KSAs important for achieving efficient and effective cybersecurity.

Dampier [10] in his paper discusses six areas (faculty, courses, equipment and laboratories, students, budget, and credentials) essential for building a successful cyber security programme and offers suggestions to develop each of them.

### Survey of IT professionals in Georgia

Online questionnaires were used to conduct the survey. The questionnaires were created in SurveyMonkey. The data was collected and processed by the tools offered by SurveyMonkey. Web-based questionnaire was chosen as it enables time saving compared to distributing the survey in printed form. A disadvantage of it is that it does not promise high response rate compared to interviews. The survey was conducted from April 4, 2016 till June 27, 2016. Full questionnaires (originals in Georgian and English translations) can be found in Appendix 1, Appendix 2, Appendix 3 and Appendix 4.

# Chapter 3. Exploring the environment in Georgia before developing the curriculum

The following chapter covers three major parts, the first one discusses key aspects from the National Cyber Security Strategy of Georgia 2017-2018 that is important to take into account when planning higher education programme on cyber security. The second part outlines future plans of Georgia focusing on Information Technologies and Innovations. The third part presents a report about the survey conducted by the author among IT professionals and academic staff in Georgia to gain a general understanding about the cyber security skills needed in Georgia currently and in the future.

## 3.1. Cyber security according to the National guiding documents of Georgia

The cyber war by Russia against Georgia in 2008 made it clear that “the national cyber security of Georgia cannot be achieved without ensuring security of its cyberspace [11]”, admitted the first National Cyber Security Strategy - the main document for guiding policy and plans in the field of cyber security. Since then Georgia has gone through several stages of development in the field. Georgia has ratified the second and the latest National Cyber Security Strategy (2017-2018) on January 13, 2017. The document was developed based on the Threat Assessment Document for 2015-2018 (the document defining and measuring the national security threats to Georgia) and National Security Concept of Georgia.

National cyber security strategy of Georgia emphasises importance of cyber security as dependence on information technologies is increasingly growing. Cyber security is included among the national security interests of Georgia.

### 3.1.1. Main goals and principles

According to the document, “the goal of Georgia is to create and develop cyber security system that on the one hand will protect information infrastructure against cyber threats

(Confidentiality, Integrity, Availability) and on the other hand, will be additional factor for economic and social development of the country" [5]. Georgia percives cyber security as an important means to facilitate development of the country and its information society. To meet the goals, resistance of the cyber security system of Georgia against cyber attacks should be increased; should be possible to recover quickly in the aftermath of the cyber attacks; and prventive measures should be taken, admits the document.

The document confirms that cyber security is among the national interests and its importance extends due to the increased dependence on information technologies. It is of crucial importance for the prosperity of the country.

Concerning definition of cyber security, the only document defining cybersecurity explicitly is the Action Plan 2016-2017 by the Cyber Security Bureau under the Ministry of Defence of Georgia. It is defined as follows: "Condition of the information and communication systems which gives opportunities to protect Confidentiality, Integrity, Availability, from the existing/emerging threats in cyberspace" [13].

### 3.1.2. Existing Cyber Security Environment in Georgia

After the cyber war in 2008 Georgia took several steps to develop cyber security, at initial stage institutional framework was addressed. Some key institutions were established during the last years as mentioned in the national cyber security strategy:

- Data Exchange Agency was established under the Ministry of Justice, which is assigned to issue recommendations to protect critical information infrastructure and establish information security standards;
- Computer Emergency Response Team was established under the Data Exchange Agency to deal with cyber incidents and actively cooperate with international partners;
- Cyber security Bureau was established under the Ministry of Defence to deal with cyber security in Defence field;
- Department for Fighting Cyber Crime was established under the Ministry of Internal Affairs which is responsible for cyber crime investigations;

- State Security Service was established as a separate entity (former National Security Block under the Ministry of Internal Affairs), which is dealing with cyber activities against National Security;
- National Security and Crisis Management Council was established which is responsible for developing basic framework for cyber security policy and prepares and suggests recommendations for the development of cybersecurity system to the Government;
- Government has conducted several trainings, courses and projects to develop cyber security professionals.

### 3.1.3. Cyber Threats

The list of cyber security threats starts with the threat of cyber war from Russia. Russia has been actively conducting information operations in cyber space to impede integration of Georgia into Euro-Atlantic family. The list continues with cyberterrorism, cyber espionage, Cybercrime, cyber attacks against Critical Information Infrastructure.

### 3.1.4. National Cyber Security Strategy about the Higher Education

The Cyber Security Strategy of Georgia lists five main directions to focus on:

- Research and analysis
- Development and refinement of the legal base
- Capacity building
- Raise awareness of the society and establish education programmes
- International cooperation

(Due to the interest of the thesis, the author focuses only on higher education in this section).

To start with awareness in cyber security, according to the strategy document there has been taken several initiatives to raise awareness in cyber security but the level of the awareness is still low.

The document confirms importance of continuous professional growth for cyber security personnel and admits that due to the high demand cyber security professionals are leaving not only the public sector but the country in exchange for beneficial conditions. Developing cyber security education in Georgia is mentioned as an important factor that can facilitate preparation of future professionals and smooth functioning of cyber security in Georgia.

To raise awareness of the society and establish education programmes the national document list the following measures:

- Create programmes to raise public awareness and improve education;
- Improve higher education system capabilities in cyber and information security (creation of graduate and postgraduate cybersecurity programs);
- Train personnel of Critical Information Infrastructure and other stakeholders in accordance with international information security and national standards;
- Develop specialized trainings that will help to investigate cyber incidents conducted against National Security of Georgia;
- Facilitate research projects in the field of cyber security.

Development of higher education programmes is within the action plan for 2017-2018 according to the strategy document. Responsible entities include: Ministry of Education and Science, Data Exchange Agency, Cybersecurity Bureou. Supporting entities: State Security and Crisis Management Council, State Security Service, Ministry of Internal Affairs, international support.

## 3.2. Future Plans

*The following section provides an overview on Georgia's future plans based on Socio-Economic Development Strategy – Georgia 2020 focusing on Information Technology.*

The strategy document analyses weaknesses that hinder inclusive economic growth in Georgia and provides solutions to overcome them. The document identifies three major problems: private sector's low level of competitiveness, insufficiently developed human capital and limited access to financial resources [7]. To address the problems the document suggests the following solutions:

To raise private sector competitiveness focus will be on:

- “Improving the investment and business environment
- Innovation and Technologies
- Facilitate the growth of exports
- Developing infrastructure and fully realizing the country’s transit potential” [7]

To improve human capital focus will be on:

- “Developing the country’s workforce that meets labour market requirements
- Tightening social security net
- Ensuring the accessible and quality health care“ [7]

Regarding the issues related to access to finance focus will be on the following:

- “Mobilization of investments
- Development of financial intermediation” [7]

One of the key priorities appears to be raising competitiveness of private sector. Based on the provided solution Georgia allocates and intends to allocate much effort on innovation and technologies meaning that the dependence on information technologies will be significantly increased.

## 3.3 Cyber security skills need in Georgia:

This section aims to examine the need and lack of specific cyber security skills in Georgia currently and in the future based on the survey conducted in Georgia for public and private organisations and education institutions. The beginning of the section introduces objectives of the survey which is followed by the methodology and analysis of the survey.

### 3.3.1. Introduction

Within the purpose of the master thesis it is important to be informed about the cyber security skills in demand and the overall existing situation related to education in cyber security in Georgia from the first sources. To address the issue the survey was conducted. Questionnaires were used as survey instruments. There were two questionnaires: questionnaire one was developed for information technology (IT) personnel of governmental organisations and institutions, private companies and organisations (hereinafter, questionnaire for companies); the questionnaire two – for state and private education institutions' academic staff involved in information technology (IT) field (hereinafter, questionnaire for education institutions).

The key objective of the survey was to find out which cyber security skills at present are and are expected to be in demand in future in Georgia according to the IT personnel of public and private organisations and education institutions and on which cyber security skills should the cyber security master programme focus; The complementing objective was to identify how could companies, organisations and institutions contribute to the development of the cyber security master programme in Georgia. The survey was conducted from April 4, 2016 till June 27, 2016.

### 3.3.2. Methodology

To conduct the survey a questionnaire was chosen as a survey instrument. There were developed two questionnaires which comprised of open-ended and close-ended questions i.e. the respondents were free either to choose from listed options and/or provide their own answers. The sample included professionals involved in the field of Information Technology. Respondents were chosen based on their professional experience in IT field and being employed at important companies or institutions in Georgia. The survey sample covered the following sectors:

- Banking/Finance
- Defence/Security
- Healthcare
- Technology & software
- Energy & utilities

- Transportation
- Communications
- Entertainment & media
- Industry
- Agriculture & food services
- Tourism

The survey is an attempt to receive the list of the cyber security skills that are expected to become important for Georgia in future in 2-4 years according to the IT professionals of companies and academic staff of education institutions in Georgia. The author intends to achieve the goal by combining results of the following questions:

- On which cyber security skills should the master programme focus according to the IT staff of companies and the academic staff of education institutions?
- Which cyber security skills are expected to be important for the companies according to their IT staff?
- Which cyber security skills are expected to be important according to the academic staff?

The online questionnaires were built in SurveyMonkey and the links were sent out to the sample via email. Internet survey was chosen as it is convenient and time-saving for participants and provides quick turnaround.

### 3.3.3. Design

The questionnaires were developed taking into account previous surveys conducted in the field of cyber security [14] [8] [15] and their experiences. The wording and questions were carefully developed and tailored to ensure objectivity, validity and reliability.

The questionnaires consist of four parts: Introduction, main questions, demographic questions and the closing part. The soft brief introduction welcomed the respondents and introduced the purpose of the questionnaire, as well as who were supposed to be the respondents. Additionally, a brief overview of the questionnaire design and estimate time for filling it was mentioned. This was followed by the main questions, 22 questions in case of the questionnaires for companies and 16 questions in case of the questionnaires for education institutions. The demographic part (6 fill-in fields) included screening questions, to re-check that the respondents were qualified to participate in the survey. In the closing section the author once again expressed appreciation towards the respondents and provided her e-mail address in case of questions, comments or critic.

Some questions were repeated in both questionnaires to enable the opportunity to compare the perspectives of academic staff and non-academic staff and/or combine them.

The original questionnaires for companies and education institutions can be found in Appendix 1 and Appendix 2, and the English translations can be found in appendix 3 and Appendix 4, respectively, at the end of this thesis.

**Weaknesses:** The questionnaires did not have follow-up reminders.

### 3.3.4. Analysis

The analysis subsection covers key points of the results of the survey, such as details about respondents, cyber security skills demand in Georgia, opportunities for joint efforts to support the development of the master programme, focus of the master programme and the conclusion.

#### Respondents

To start from response rate, overall, about 70 emails were sent out and 47 responses were received: 40 of respondents filled the questionnaire for companies and the rest contributed to the questionnaire for education institutions. 39 out of the 47 respondents were males and 8 females. Their ages fell within the range of 18 and 54. Majority of the respondents from companies (24 out of 40), were from large companies (250+ employees). 22 out of the 40 were from private sector and 18 respondents represented public sector. While the overall number of respondents is not very high, it is believed they reflect the situation and requirements in Georgia.

Regarding respondents' experiences in IT field, it varied from 1 year to more than 35 years. 17 participants had more than 5 years of experience in IT field, 10 of them with more than 5 years in the same company or education institution; 16 had been employed in IT field for more than 10 years, 4 of them in the same education institution and company with more than 10 years of experience (more details are available in Figure 1).

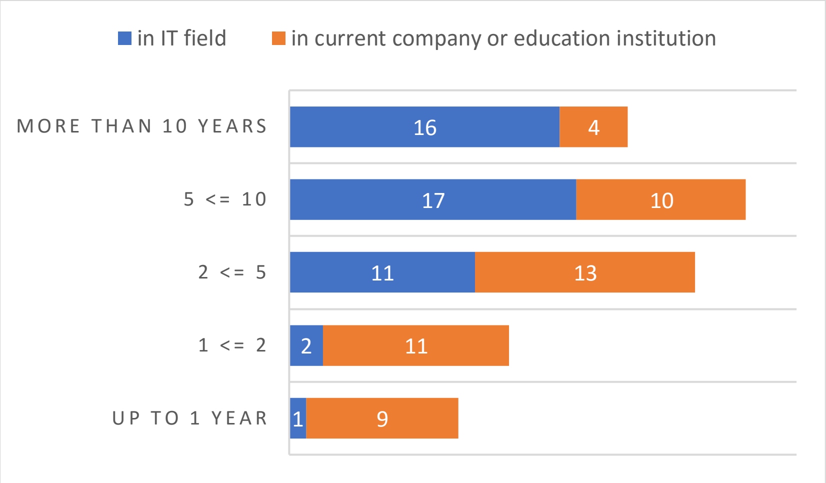


*Figure 1.Respondents' years of experiences.*

The respondents job positions included both management and non-management job titles. Detailed list is available in the Table 1. “Other” included the following job titles: program analyst, computer security specialist, IT field deputy director.

*Table 1. Respondents' job titles.*

| **Respondents positions** | **Respondents** |
|---|---|
| Executive / C-level | 2 |
| Director | 2 |
| Manager | 13 |
| System administrator | 5 |
| Network administrator | 3 |
| Technician | 3 |
| Lecturer, Researcher, Professor | 9 |
| Security analyst | 3 |
| Developer | 4 |
| Other | 3 |

Majority of the respondents represented education institutions (academic staff and non-academic staff) (see Table 2). Four of the respondents were from sectors other than listed in the questionnaire: one of them represented Human Rights, one - Non-Governmental Organization (NGO) and two were from a field of Trade.

*Table 2. Respondents according to sectors.*

| Sectors | Number of respondents |
|---|---|
| Education | 19 |
| Technology & software | 8 |
| Banking/Finance | 7 |
| Communications | 5 |
| Health & social services | 1 |
| Energy & utilities | 1 |
| Transportation | 1 |
| Entertainment & media | 1 |
| Other | 4 |
| **Total** | 47 |

### Cyber Security Skills in Demand

It has been interesting to start inquiries from the number of cyber security professionals at companies. As the results showed, majority of the companies have few or no cyber security professionals. 22 respondents out of 39 mentioned that the number of cyber security professionals at their companies varied between 0<=1%. Only one respondent admitted that the number at his company equals 90% (see Figure 2). As for the future expectations, it is worth mentioning that majority of the respondents (27 out of 40) expect to increase the number in coming 2-4 years.

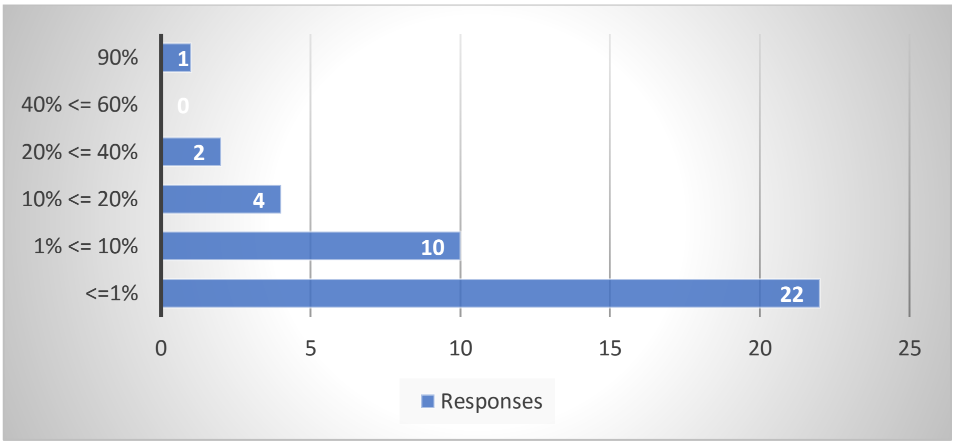


*Figure 2. Number of SC professionals at the companies.*

The respondents were asked which cyber security skills were important for their company at present and which ones they expected to be important in the future, in 2-4 years. According to the results, currently the top five, the most demanding skills are: network security, penetration testing, business continuity management, secure coding and audit. Three participants additionally admitted that there is a need for awareness trainings, insider risk reduction, risk management, incident response and handling, testing, monitoring. For future, the respondents expect significant increase of demand for secure coding and digital forensics (see Figure 3). The order of upcoming cyber security skills in demand looks as follows according to the results: network security maintains the lead position, next come Penetration testing, Business continuity management and Security coding with equal 26 votes, followed by audit, cryptography, legal aspects. Awareness training, insider risk reduction and monitoring were additionally admitted by the respondent.

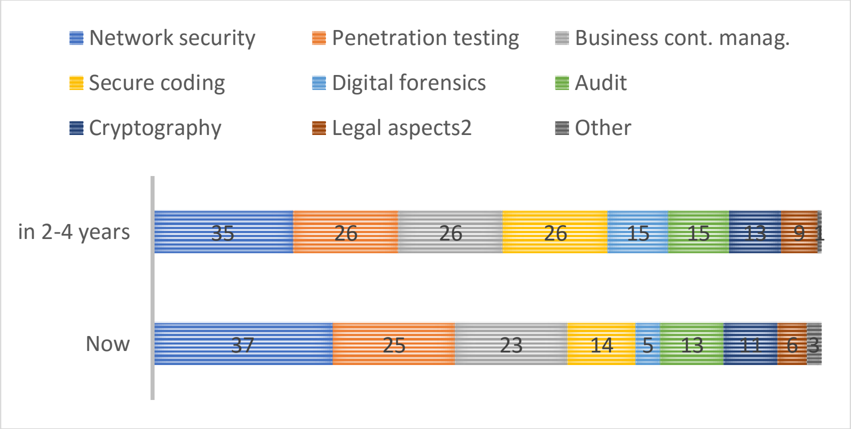


*Figure 3. CS skills in demand now and in the future according to companies.*

In comparison to the *Figure 3* above the following *Figure 4* below depicts cyber security skills demand now and in 2-4 years in Georgia, according to the academic staff (seven respondents). Network security and Penetration testing were mentioned among the most demanding skills both for current situation and future by the academic staff as well. The next order differs from the one suggested by the representatives of companies: secure coding, digital forensics, BCM, cryptography and legal aspects. None of them marked audit and there were no additional comments.

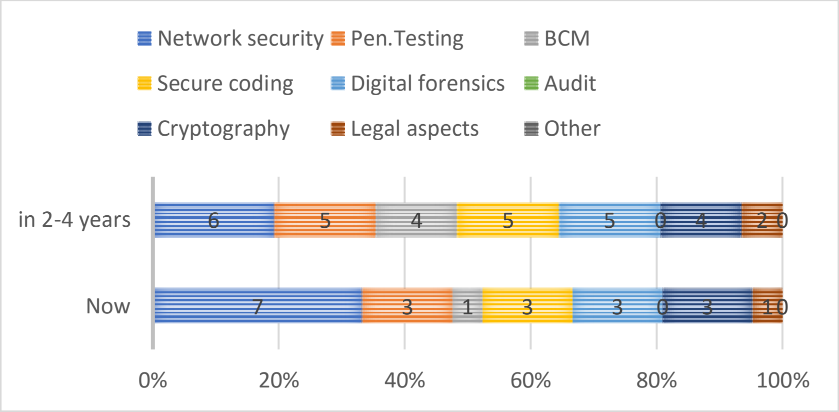


*Figure 4. Cyber security skills in demand according to academic staff.*

Both groups of respondents were asked, professionals with which cyber security skills were difficult to find in Georgia and which cyber security skills were difficult to recruit in Georgia. The combined responses show that the most difficult to find is a professional with cryptographic skills, next come digital forensics, secure coding, penetration testing, business continuity management (BCM), network security, legal aspects, audit and reverse engineering. Regarding difficulties in recruiting cyber security skills, the most scarce appears to be recruiting in digital forensics, followed by penetration testing, secure coding, cryptography and BCM, less rare - network security, legal aspects and audit. In addition to the listed skills reverse engineering was added by two respondents.

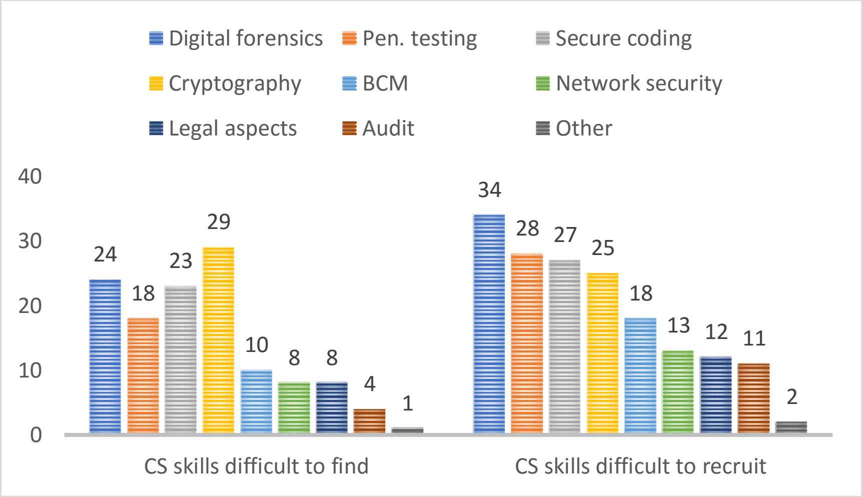


*Figure 5. Cyber security skills difficult to find and recruit in Georgia.*

To examine the demand for cyber security education from the companies now and in 2-4 years based on the respondents' answers: in response to the question which options the companies consider to improve their employees' cyber security qualification now, majority of them responded that it is not considered at all. Few are considering trainings outside their companies in Georgia, trainings abroad or internal trainings initiated by the company itself. Fewer are considering higher education. Two respondents admitted “self-education” as additional option. By 2019-2021 more respondents expect to consider higher education than at present time. They are mostly expecting to undertake external trainings and trainings abroad.

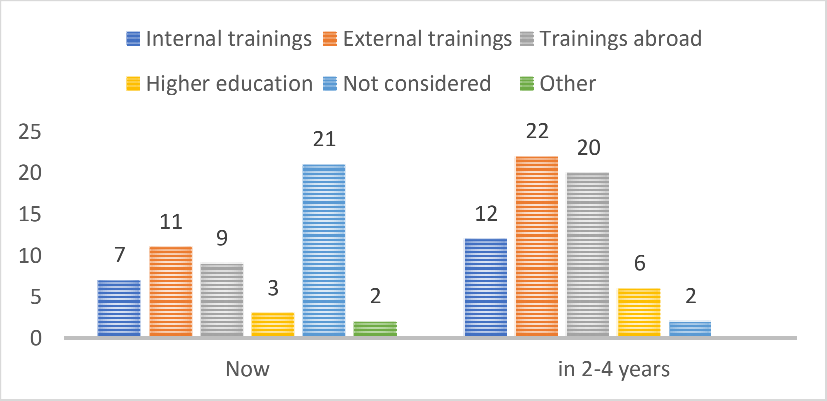


*Figure 6. Cyber security education options now and in the future.*

When companies asked if their company had addressed any of the education institutions to raise qualification of their cyber security personnel, 26 out of 40 respondents provided negative answers, 7 answered that they had addressed, and 6 added that they did not have information.

As for the education institutions, when asked if any of the companies had addressed them with a request to conduct a cyber security training to raise qualification of their personnel, 3 out of 7 provided positive response, 3 – provided negative response; 1- skipped the question. Concerning the interest in higher education in cyber security from companies, the answers were divided as follows: two from the academic staff admitted that there had been interest from companies. Four of them filled in that there had been no such case.

### Joint effort for the development of cyber security master programme in Georgia

Regarding combining efforts to support the development of the master programme, companies mentioned “developing course content” as the most possible option. The other options included providing advises, internships and sponsoring master students (Table 3). Two of the respondents provided negative answers, one of them adding that these kinds of initiatives were not possible at the present time and the second admitting that the options were not within interests of her company.

*Table 3. Joint efforts from companies' perspective.*

| **How do you think your company can support the master programme's development in Georgia?** | |
|---|---|
| Working with universities to develop course content | 17 |
| Employing students on a long-term or short-term internships | 13 |
| Providing advisory role on cyber security skills initiatives | 12 |
| Employing students on a long-term or short-term paid internships | 10 |
| Sponsoring master student(s) | 8 |
| Other | 2 |

When asked similar question to the education institutions, the most possible option coincided with the one suggested by the companies – working over the development of the course content (Table 4).

*Table 4. Joint efforts from academic staff's perspective.*

| **How do you think a company can support development of the master programme in Georgia?** | |
|---|---|
| Working with universities to develop course content | 5 |
| Sponsoring master student(s) | 4 |
| Employing students on a long-term or short-term internships | 3 |
| Employing students on a long-term or short-term paid internships | 3 |
| Providing advisory role on cyber security skills initiatives | 2 |
| Other | 0 |

### Focus of the master programme

Whether the programme should have multidisciplinary approach or focus on one field only, majority of the survey respondents support multidisciplinary approach: 27 respondents against 12 according to the company-related questionnaire results (one respondent skipped the question), 6 respondents against 1 respondent according to the academic personnel response.

As for the question, which cyber security skills should the programme focus, companies and education institutions have provided slightly different suggestions but the top 5 suggestions remained the same for both groups: network security, penetration testing, cryptography, secure coding and digital forensics. Figure 7 portrays the whole picture.

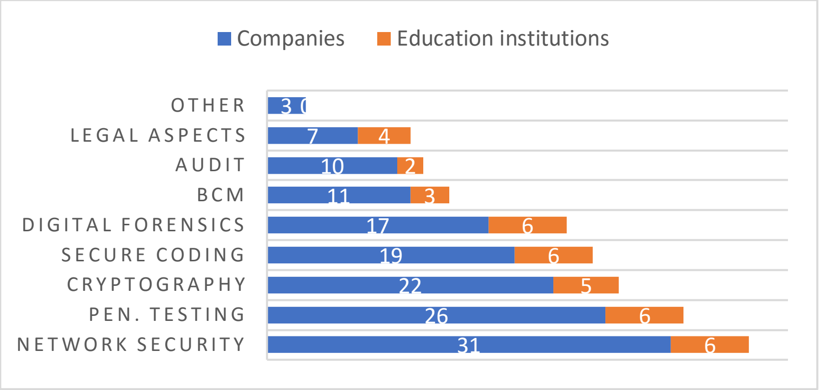


*Figure 7. The CS skills the programme should be focused according to the respondents.*

Having combined the two groups' 47 responses, we receive the following order: network security, penetrating testing, cryptography, secure coding, digital forensics, business continuity management, audit, legal aspects. Two respondents added incident handling and cyber security management.

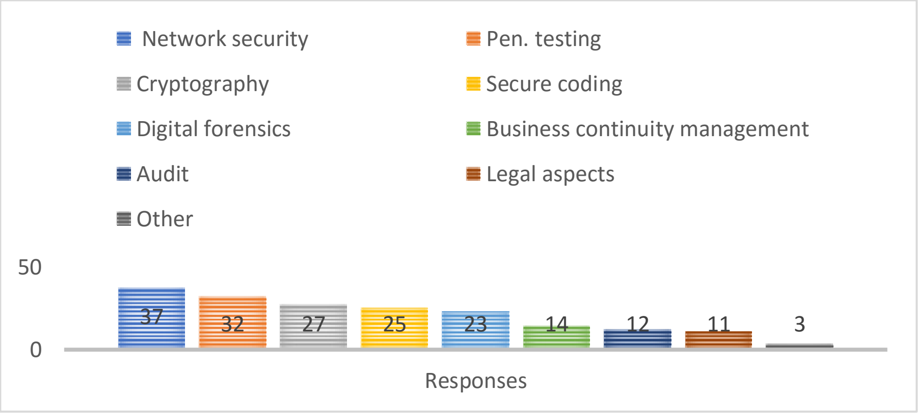


*Figure 8. Master programme focus.*

To combine the latest results with the two questions: which cyber security skills the respondents expect to be important for their companies and which CS skills are expected to be important from perspective of the academic staff we received the following list (Figure 8):

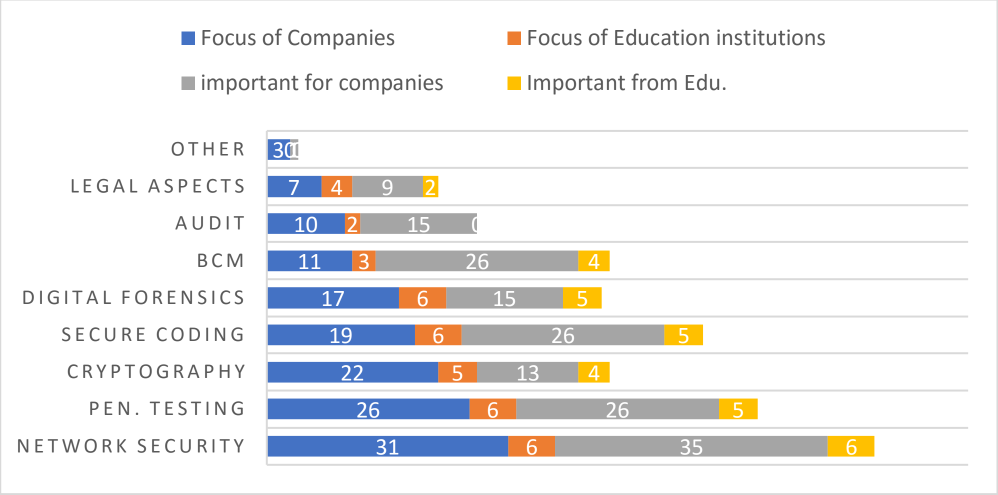


*Figure 8. Combining predicted demand of CS skills and the suggested focus for the master programme.*

1. Network Security (78 votes)
2. Pen. Testing (63 votes)
3. Secure Coding (56 votes)
4. Cryptography (44 votes)
4. BCM (44 votes)
5. Digital Forensics (43 votes)
6. Audit (27 votes)
7. Legal aspects (22 votes)
8. Other (3 votes: incident handling and cyber security management)

The overall results show that there is not sufficient or any education basis for any of the directions of cyber security in Georgia. The demand promises to increase as Georgia has been initiating several projects that will increase dependency on information technologies. To ensure long-term successful fulfilment of the projects it is of crucial importance to take measures to develop cyber security capabilities.

## Conclusion

To summarise the key points, the list of the cyber security skills in demand for future in Georgia looks as follows:

- Network security
- Penetration testing
- Cryptography
- Secure coding
- Digital Forensics
- BCM
- Audit
- Legal aspects
- Cyber security management
- Incident handling
- Insider risk reduction
- Awareness training

Furthermore, to support development of the master programme respondents are considering the following options of joint efforts (see Table 4):

- Working with universities to develop course content
- Sponsoring master student(s)
- Employing students on a long-term or short-term internships
- Employing students on a long-term or short-term paid internships
- Providing advisory role on cyber security skills initiatives.

# Chapter 4. Exploring existing leading cyber security programmes in UK, USA and Estonia

The following chapter analyses highly rated cyber security master programmes in USA, UK and Estonia. The *Introduction* explains why the author decided to focus on cyber security programmes from the three countries. *Cyber Security Master Programmes* section provides analysis of the cyber security master programmes: outlines key aspects of the programmes such as objectives, brief description, admission criteria, core courses.

## 4.1 Introduction

The cyber security master programmes were selected from USA, UK and Estonia. USA and UK universities were chosen because they have been leading the top universities [9] [8]. Estonia was chosen as a vivid example of the "e-societies" pioneering in e-services such as e-signature, e-voting and many more others. Estonia has been a good example and close partner for Georgia to defend its cyber space after the cyber war of Russia against Georgia in 2008. Estonia and Georgia has been sharing common values and interests for decades. Estonia has taken significant steps to advance its cyber security although the budget of the country is not as enormous as of UK and USA. Furthermore, USA, Estonia and UK take key positions according to the report of Global Cybersecurity Index & Cyberwellness Profiles 2015 [16] as well – 1st, 5th and 8th places, accordingly.

## 4.2 Cyber security master programmes

Cyber security programmes from USA were chosen based on the Research Report "2014 Best Schools for Cyber security" prepared by Ponemon, sponsored by HP Enterprise Security [9]. UK Cyber Security master programmes were selected from programmes certified by the Government Communications Headquarters (GCHQ) in cyber security and closely related fields [8]. Regarding the Cyber Security Master programme from Estonia, it is a joint programme of two biggest Estonian Universities, Tallinn University of Technology and the University of Tartu.

As one of the criteria when choosing the university programmes was to have "cyber security" in the title or be concentrated on cyber security to ensure that focus would be only on cyber security and not on related fields. Because of this reason the author covers only six USA universities out of twelve, overall 8 cyber security master programmes (taking into account that two of the universities have two different kind of cyber security master programmes: University of Texas, San Antonio and University of Washington). Eight more cyber security master programmes are covered (from seven universities) from the UK. Overall the author examines seventeen cyber security master programmes: the first eight represent the USA, the next eight - UK and Estonia closes the list (see Table. 5).

*Table 5. The 17 Cyber Security Programmes.*

1. Master of Business Administration (MBA) – Cyber Security concentration - **University of Texas, San Antonio (UTSA)**
2. Master of Science in Information Technology (MSIT) - Cyber Security concentration - **University of Texas, San Antonio (UTSA)**
3. Master of Science in Cyber Security and Operations - **Mississippi State University (MSU)**
4. Master of Science in Cybersecurity - **Syracuse University**
5. Master of Science in Information Technology - **Carnegie Mellon University - Africa**
6. Master of Science in Cyber Security Engineering - **University of Southern California**
7. Master of Science in Cyber Security Engineering - **University of Washington, BOTHEL**
8. Master of Cybersecurity and Leadership (MCL) - **University of Washington, TACOMA**
9. Cyber Security Master of Science - **Lancaster University**
10. Master of Science in Cyber Security - **University of York**
11. Cyber Security Master of Science - **University of Birmingham**
12. Cyber Security Master of Science - **University of Kent**
13. MSc Applied Cyber Security - **Queen University Belfast**
14. MSc Cyber Security - **University of Southampton**
15. MSc in Cyber Security Engineering - **University of Warwick**
16. Master of Science in Cyber Security and Management - **University of Warwick**
17. Master of Science in Cyber Security – **Tallinn University of Technology**

### 4.2.1 Introduction about the university programmes

The following section provides a brief overview of the University programmes such as University name, the Programme name including the web-page link, some of important achievements according to dates including the links (ex. a programme was granted a full certification by the United Kingdom Government Communications Headquarters or was accredited as a Center of Academic Excellence in Cyber Defense Research, launch of the cyber security programme, etc.), Faculty who runs the programme (see Table 6).

*Table 6. Basic information about the cyber security master programmes.*

| | **Programmes** | **Universities** | **Year** | **Faculty** |
|---|---|---|---|---|
| 1 | Master of Business Administration [17] | University of Texas, San Antonio (UTSA) | 2001[1] | College of Business, Department of Information Systems and Cyber Security |
| 2 | Master of Science in Information Technology [18] | | | |
| 3 | Master of Science in Cyber Security and Operations [19] [20] | Mississippi State University (MSU) | 2000 [10] | Department of Computer Science and Engineering, the Bagley College of Engineering |
| 4 | Master of Science in Cybersecurity [21] | Syracuse University | 2001 [21] | Department of Electrical Engineering & Computer Science |
| 5 | Master of Science in Information Technology [22] | Carnegie Mellon University - Africa | | College of Engineering |
| 6 | Master of Science in Cyber Security Engineering [23] | University of Southern California | 2013[2] | USC Viterbi School of Engineering |

[1] "The UTSA College of Business has been offering cyber security classes since 2001", University of Texas, San Antonio (UTSA). Available: http://business.utsa.edu/cybersecurity/ [Accessed: April 2017]

[2] The programme is being offered since 2013, University of South California (USC). Available: https://viterbi.usc.edu/news/news/2013/usc-viterbi-offers.htm [Accessed: April 2017]

| | | | | |
|---|---|---|---|---|
| 7 | Master of Science in Cyber Security Engineering [24] | University of Washington, BOTHEL | | School of Science, Technology, Engineering & Mathematics |
| 8 | Master of Cybersecurity and Leadership (MCL) [25] | University of Washington, TACOMA | | Institute of Technology; Milgard School of Business |
| 9 | Cyber Security Master of Science [26] | Lancaster University | 2014[3] | School of Computing &Communications |
| 10 | Master of Science in Cyber Security [27] | University of York | 2015[4] | Department of Computer Science |
| 11 | Cyber Security Master of Science [28] | University of Birmingham | 2017[5] | College of Engineering and Physical Sciences, School of Computer Science |
| 12 | Cyber Security Master of Science [29] | University of Kent | Prov.[6] | School of Computing |
| 13 | MSc Applied Cyber Security [30] | Queen University Belfast | 2011[7] | Centre for Secure Information Technologies (CSIT) |
| 14 | MSc Cyber Security [31] | The University of Southampton | | Computer Science and Software Engineering |
| 15 | MSc in Cyber Security Engineering [32] | University of Warwick | | |
| 16 | Master of Science in Cyber Security and Management [33] | University of Warwick | | |
| 17 | Master of Science in Cyber Security [34] | Tallinn University of Technology /University of Tartu | 2009 | School of Information Technologies |

[3] The Programme was granted a full certification by the United Kingdom Government Communications Headquarters (GCHQ) in 2014. Available: http://www.lancaster.ac.uk/news/articles/2014/lancaster-university-cyber-security-course-is-certified-by-uks-national-intelli/ [Accessed April 2017].

[4] The cyber security programme was granted a full certification by the UK Government Communications Headquarters (GCHQ) in 2015. Available: https://www.cs.york.ac.uk/news/ [Accessed April 2017].

[5] University of Birmingham, The University of Birmingham has been recognised for excellence in cyber security research for another five years. Available: http://www.birmingham.ac.uk/news/latest/2017/04/ACE-CSR.aspx [Accessed April 2017].

[6] The programme is GCHQ provisionally certified. Available: https://www.ncsc.gov.uk/information/gchq-certified-degrees [Accessed May 2017]

[7] The CSIT has been recognized as the Academic Centre of Excellence in Cyber Security Research (ACE-CSRs) since 2011. Available: http://www.csit.qub.ac.uk/about/WhatisanACECSR/ [Accessed April 2017].

### 4.2.2. Programme objectives and core courses

The following section provides more details about the programmes such as programme objectives, brief description or what should a student expect as an outcome; programmes concentrations/specializations (if available); core courses and their comparison; if the programme offers projects or internships; and some additional characteristics specific to the programme (see Table 7 below).

For building a successful cyber security programme it is essential to include the following courses [10]:

- Security Policy and Law
- Computer Security, including both Hardware and Software
- Network Security
- Digital Forensics
- Cyber Physical Systems Security, often referred to as SCADA Security

The table 7 below will also check if the core courses cover the five courses listed above as essential by the paper (Dampier [10]).

*Table 7. The cyber security programme's brief description (part 1).*

| | | UTSA | UTSA | MSU | Syracuse | CMU | USC |
|---|---|---|---|---|---|---|---|
| | | **1. MBA** | **2. MSc in IT** | **3. MSc in CS & Operations** | **4. MSc in CS** | **5. MSc in IT** | **6. MSc in CS Engineering** |
| **Key Points** | | Focusing on business administration while gaining cyber security knowledge and skills | Focusing on information technology while gaining cyber security knowledge and skills | Meet the increasing cyber-threats… to serve in government or industry | Identify, Prevent and Counteract cyber crime. Assured systems | Prepare for leadership positions in information security | Focuses on computer network operations |
| **Concentration and/or Specialisation** | | Cyber Security concentration | Cyber Security concentration | Two concentrations: Cyber defense and Cyber Operations | | Cyber Security concentration | |
| **Core** | **Security Policy and Law** | MBA-related courses (the list is not available) and some of the graduate cyber security courses (see table 8) | Information Technology | Cyber law and privacy | Design and Analysis of Algorithms | - | Security and Privacy in Informatics |
| | **Computer Security** | | Security risk analysis | Information and computer security | Computer security | | Computer systems assurance |
| | **Network Security** | | Introduction to voice and data security | Advanced network security | Internet security | | Security systems |
| | **Digital Forensics** | | Telecommunications Systems | Introduction to computer forensics | Principles of Operating systems | | Foundations and Policy for Information Security |
| | **SCADA Security** | | Strategic management of information technology | Cryptography and network security | Assurance foundation | | Trusted system design, analysis and development |
| **Internship/Project** | | Not mentioned | Independent study | Graduate seminar | Project | Project | Internship |
| **Students' required background** | | Academic background or work experience in information security, information systems or computer science | Prior academic achievements in information technology | Firm technical background in computer science, software, computer or electrical engineering | Firm technical background | Technical background | Degree in computer science, electrical engineering or info. security. programming skills, networking, OSs, math. foundation |
| **Other** | | Electives: voice and data security, risk management, computer forensics, incident response. | | | | Future: info. security analyst, network security engineering, security consultant, forensic analyst | Addresses the challenges of secure operating systems, secure applications, secure networking, use of cryptography and key management |

| | | UW\|BOTHEL | UW\|TACOMA | Lancaster | York | Birmingham | Kent |
|---|---|---|---|---|---|---|---|
| | | **7. MSc in CS Engineering** | **8. MCL** | **9. CS MSc** | **10. MSc in CS** | **11. CS MSc** | **12. CS MSc** |
| **Key Points** | | Protection, Detection, Correction. Protect today's and tomorrow's cyber systems with the necessary technical and leadership skills | Prepares effective interdisciplinary communicators who can integrate the technical aspects of cyber security with strategic and managerial aspects | Obtain knowledge and skills for IT security profession. Combines advanced tech. skills with economics, risk management, psychology and social science | Make technically informed principled decisions in industry or government | Covers all the layers at which security must be considered starting from operational to strategic level | Be at the fore front of the discipline equipped with a systematic and deep understanding of the subject |
| **Concentration and/or Specialisation** | | | | | | | |
| **Core** | **Security Policy and Law** | Security, policy, ethics, and legal environment | -Networking and internet security<br>-Principles of CS<br>-Business Essentials<br>-IA, Risk mngnt and secure strategies<br>-Strategic organisation change<br>-CS management<br>-Project management<br>-Leadership and Team Dynamics | Introduction to law | Focused on areas: Identity, Trust and reputation, Network security, Malware and intrusion detection, Risk management, Development of high assurance systems | Anonymity, privacy and cybercrime | The programme covers technical side of encryption, authentication, biometrics, network security, etc., also information security management and cyber security risk |
| | **Computer Security** | Vulnerability Analysis and Detection | | Info. systems security management | | Cryptography | |
| | **Network Security** | Network and internet security | | Network and systems security | | Network security | |
| | **Digital Forensics** | Incident Response and Recovery | | Information system forensic investigation | | -Secure programming<br>-Designing secure systems<br>-Secure system management | |
| | **SCADA Security** | -IS&Secure Development Lifestyle(SDL);<br>-Secure Software Development<br>-Contemporary Issues in IA<br>-Cryptography and data assurance | | -Info. Systems risk management<br>-Security and Conflict in the Digital Age<br>-Cybercrime<br>-Information system penetration and countermeasures | | | |
| **Internship/Project** | | Project | Project | Project | Project/Internship | Project | Research/project |
| **Students' required background** | | Aimed for working professionals. BA in computer science or equivalent. | For professionals and military personnel with a technical background and work experience | Honours degree in computing or a closely related field | A strong background in computer science or related | Honours degree in computer science or related | Strong programming skills |
| **Other** | | | | | | | |

*Table 8. The cyber security programme's brief description (part 2).*

|  |  | QUB | Southampton | Warwick | Warwick | TUT |
|---|---|---|---|---|---|---|
|  |  | **13. MSc Applied Cyber Security** | **14. MSc in CS** | **15. MSc in CS Engineering** | **16. MSc in CS and Management** | **17. MSc in CS** |
| **Key Points** |  | Prepares next generation industry leaders | Combines technical subjects with criminology, risk management, law and social sciences | Prepare professionals who can function at various strata within an organization – server room, operations room, board room | Develop strategic thinkers who understand the cyber threat to an organization and its resources, and are able to build and manage secure systems that support the strategic growth of a business | Develop skills in all aspects of the security of information system |
| **Concentration and/or Specialisation** |  |  |  |  |  |  |
| **Core** | **Security Policy and Law** | Ethical&legal issues in cyber security | Foundations of cyber security | Information risk management and governance | Information risk management and governance | Network Technology |
|  | **Computer Security** | Software assurance | Software engineering and cyber security | Cryptosystems and data protection | Cryptosystems and data protection | Strategic and operational aspects of cyber security |
|  | **Network Security** | Network security&monitoring | Implementing cyber security | Security architectures and network defence | Security architectures and network defence | Foundations and management of cyber security |
|  | **Digital Forensics** | -Computer forensics<br>-Malware | Cyber crime, insecurity and the dark web | -Digital forensics<br>-Cyber intelligence and operations | Digital forensics | Malware |
|  | **SCADA Security** | Applied Cryptography | Project preparation | -Enterprise cyber security<br>-Cyber-physical systems<br>-Industrial Espionage and counterfeiting | Industrial espionage and counterfeiting |  |
| **Internship/Project** |  | Research Project/Internship | Project |  |  |  |
| **Students' required background** |  | Recent math or engineering graduate with strong programming skills and technical software development experience | Honours degree in IT, engineering or computer science |  |  | Degree in IT or related discipline |
| **Other** |  |  |  |  |  | May lead to job positions: security analyst, architect or research engineer; project/team leader, technology officer |

*Table 9. The cyber security programme's brief description (part 3).*

### 4.2.3. More details:

**(1) The University of Texas, San Antonio (UTSA)** offers two cyber master programmes with concentration on cyber security: Master of Business Administration (M.B.A.) and Master of Information Technology. The College of business at UTSA has been offering cyber security classes since 2001 [35]. The university leads the list of best cyber security schools in the research report by Ponemone – “2014 Best Schools for Cyber Security”. The outline the main characteristic of the MBA programme with concentration on cyber security: the programme is focused on business courses while efficiently integrating technical cyber security courses such as voice and data security, risk assessment, computer forensics, incident response in its curriculum. Students can choose rest of the core courses from the list below (see Table 10):

*Table 10. Overview of the UTSA M.B.A. courses [17]*

| | Courses | Covers |
|---|---|---|
| **1** | Information Technology | Computer architecture and operating systems, information retrieval techniques, graphical user interfaces, networks, groupware, computer performance evaluation, efficiency of algorithms, cryptography. Hands-on exposure to Internet services, SQL database language, PowerBuilder graphical interface language, and object-oriented programming language |
| **2** | Software Engineering Management | Focuses on managing and improving the delivery of software in organizations, especially projects that include the development of large, multidiscipline systems |
| **3** | Telecommunication Systems | current, future, and basic technical concepts and related telecommunications operations; explores critical issues of communications and connectivity among information systems from strategic, organizational, and technical perspectives. An in-depth examination of basic telecommunication terminology and concepts. |
| **4** | Introduction to Voice and Data Security | A study of security in both the voice and data networks and an examination of the security issues associated with the movement toward a convergence of the two infrastructures. Topics to be covered include voice and data network connectivity, modem security, VOIP security, wireless security, cryptography, intrusion detection systems, voice and data firewalls, malicious software, information operations and warfare, and denial of service attacks. |
| **5** | Security Risk Analysis | tools, techniques, and methodologies in performing computer system and network security risk analyses. Computer system and network vulnerabilities will be examined as well as tools designed to discover or exploit them. Security Best Practices and audit requirements for specific environments will be studied. Topics to be covered include internal and external penetration tests, wardialing, wireless security technology, risk analysis methodology, and security audits |

| | | |
|---|---|---|
| **6** | Secure Network Designs | Network design, firewalls, security, fault management, and performance management. Current network management software, network security evaluation, and the role of the network architecture and protocols will also be discussed. The course is intended to provide the background on issues related to secure network design and management |
| **7** | Security Incident Response | The detection and response portion of the security operational model. Takes an in-depth look at intrusion detection methodologies and tools and the approaches to handling intrusions when they occur. Examines the laws that address cybercrime and intellectual property issues. Includes a study of proper computer and network forensics procedures to aid in the identification and tracking of intruders and in the potential prosecution of criminal activity |
| **8** | Computer Forensics | The role of computer forensics in the security process. Technical issues concerning how to conduct a forensic examination as well as the legal issues associated with the process will be studied. Current forensics software will be used to illustrate the process |
| **9** | Cyber Law | Legal issues associated with cybercrimes will be studied. Laws associated with cybercrime, and rules of evidence will be the main issues discussed in this class. Intellectual property and privacy will also be included |
| **10** | Policy Assurance for Infrastructure Assurance | The policies associated with infrastructure assurance. This will include the laws and regulations from a governmental body as well as policies generated by a business organization. The emphasis will be to examine the effect that policies and policy decisions have on the security function. Current case studies will be included |
| **11** | Secure Software Design | Ways of designing and implementing secure software. Techniques for developing interconnected software that is secure from outside attack will be explored. Modifying legacy code will also be discussed. Case studies and class projects will be used to illustrate the design principles discussed in class |
| **12** | Supervisory Control and Data Acquisition | Supervisory control and data acquisition systems are used to control many utility networks, chemical plants, pipelines and many other types of industries. This course will examine the vulnerabilities associated with these systems and discuss how they can be made secure from outside attack. Fundamentals of software-controlled processes will also be discussed |
| **13** | Introduction to Data Mining | This course introduces the fundamental data mining concepts and techniques that are applicable to business research. The course covers basic skills required to assemble analyses for both pattern discovery and predictive modeling. It provides extensive hands-on instruction using data mining software. This course is open to all graduate students |

**(2)** In case of **Master of Science in Information Technology (M.S.I.T.)** – Cyber Security Concentration covers compulsory courses: Information Technology, Telecommunication Systems, Introduction to Voice and Data Security, Security Risk Analysis and Strategic Management of Information Technology. The latter course “develops a conceptual framework for strategy, its definition, elements, and relationships to the basic business functions of management of information technology. Considers the impact of technology and environmental forces on strategic management of organizations. Examines the role of information technology in business process re-engineering, product life cycles, and new business models [18]”. The first four courses have the same description as the ones mentioned for M.B.A. programme above (Table 8).

**(3) Mississippi State University (MSU)** was one of the first institutions recognized as a Center of Academic Excellence in information Assurance/Cyber Defense Research for research universities in 2008 [10]. MSU is launching a new Master of Science in Cyber Security and Operations from Autumn 2017. The programme is for students willing to “meet challenges posed by increasing cyber threats” [19]. … It will equip students with “a focused education within a broad analytical framework for evaluating, understanding, and solving cyber security problems” [19]. The programme will have two concentrations Cyber Defense and Cyber Operations. “The Cyber Defense concentration will focus on those aspects of cyber security needed to prepare an enterprise level system to protect itself’- according to the University Committee report [19]. The second concentration “will prepare students for advanced operations in the cyber domain such as penetration testing, after action analysis, and malware analysis” – the report concludes.

*Table 11. Cyber Defense and Operations MSc programme brief curriculum description [19].*

| **Core courses** | **Cyber Defence Concentration** | **Cyber Operations Concentration** |
|---|---|---|
| Information and Computer Security | Security Management | Reverse Engineering |
| Introduction to Computer Forensics | Two additional advanced cyber security electives | Wireless Networks |
| Cryptography and Network Security | | Advanced Cyber Operations |
| Cyber Law and Policy | | |
| Advanced Network Security | | |
| Graduate Seminar | | |

**(4) Syracuse University** - Master of Science in Cybersecurity. The programme admits that it is not enough for systems only to be “merely secure” and to provide Confidentiality, Integrity and Availability, it also needs to be assured, meaning its properties need to be “verified or proven”. It aims to teach students to design new systems that will be inherently secure; protect web, mobile and critical infrastructure; provide systems assurance though application of mathematical logic; analyse and detect malware or suspicious behavior [21].

*Table 12. Syracuse University MSc in Cybersecurity core courses [21].*

| **Core Courses** | **Areas of Study** |
|---|---|
| Computer security | Operating system security; Unix security; trusted computing base; authentication; access control; security models; capability; sandboxing; software vulnerabilities; worms; viruses; secure engineering principles; secure programming; auditing; and forensics. |
| Internet Security | Internet architecture; security and attacks on TCP/IP, DNS, and BGP protocols; Internet protocol security; firewalls; intrusion detection; network traceback; web security; encryption; Public Key infrastructure; one-way harsh function; digital signature; and security protocols. |
| Assurance Foundations | Functional programming; theorem proving; and logic for reasoning about access control, security, and trust. |
| Design and Analysis of Algorithms | Asymptotic analysis and recurrences; classical numeric algorithms; advanced data structures; graph algorithms; divide-and-conquer, greedy choice, dynamic programming, and other computational strategies; and NP-completeness. |
| Principles of Operating Systems | Design and implementation of operating systems; process and memory management; resource scheduling; file system management; I/O and kernel services; and structuring. |

**(5) Carnegie Mellon University (CMU) –** Master of Science in Information Technology – Cyber security Concentration. Students will be prepared to meet the job requirements for Information Security Analysts, Network Security Engineers, Security consultants and Forensic Analysts. The programme prepares future leaders in the field of information security [22]. The programmes does not explicitly list core courses but it presents recommended courses (see Table 13).

*Table 13. Description of some of the courses of MSc in Information Technology, CMU [22].*

| | **Recommended courses** | **Description** |
|---|---|---|
| 1 | Introduction to Info Security | The main objective of the course is to enable students to reason about information systems from a security engineering perspective, taking into account technical, economic, and policy factors. Some of the topics covered in the course include elementary cryptography; access control; common software vulnerabilities; common network vulnerabilities; policy and export control laws in the U.S., Japan, and elsewhere; privacy; management and assurance; economics of security; and special topics in information security |
| 2 | Wireless Network Security | N/A |
| 3 | Privacy in Digital Age | The main objective of this course is to provide an informed and critical view of the role and value of privacy in the digital age. Because privacy is a complex and multi-faceted concept, the course aims to present and combine technical, economic, legal, and policy perspectives |
| 4 | Internet Security | N/A |
| 5 | Information Security Risk Analysis | N/A |
| 6 | Information Security Risk Policy & Management | The course is to complement students' technical understanding with some key economics, policy and managerial frameworks that explain key challenges in security and privacy for individuals, firms and the nation |
| 7 | Cyber Security for Critical Infrastructure | N/A |
| 8 | Network Security Analysis | N/A |

**(6) University of Southern California**, Cyber Security Engineering M.S. The programme equips students with the knowledge and skills required for dealing with computer security. Students will be focused on the fundamentals of developing, engineering and operating secure information systems. They will also be introduced to policy-related issues such as how to develop a security policy and how policy drives technology decisions. The programme addresses challenges and problems related to secure operating systems, secure applications, secure networking, database security and privacy, use of cryptography and key management [23].

*Table 14. Core courses of MS Cyber Security Engineering, USC [23].*

| Core | Covers: |
|---|---|
| Security Systems | Protecting computer networks and systems using cryptography, authentication, authorization, intrusion detection and response. Includes lab to provide practical experience working with such systems. |
| Foundations and Policy for Information Security | Threats to information systems; technical and procedural approaches to threat mitigation; policy specification and foundations of policy for secure systems; mechanisms for building secure security services; risk management. |
| Computer Systems Assurance | Assurance that an information system will behave as expected; assurance approaches for fielding secure information systems;<br>case studies. |
| Trusted System Design, Analysis and Development | Analysis of computer security and why systems are not secure. Concepts and techniques applicable to the design of hardware and software for Trusted Systems. |
| Security and Privacy in Informatics | Societal implications of information privacy and how to design systems to best preserve privacy. |

**(7) University of Washington, BOTHEL:** Master of Science in Cyber Security Engineering. According to the programme web-page, students are prepared with the necessary technical and leadership skills to secure today's and tomorrow's cyber systems, they learn to make cost-benefit analysis to support sound decision-making. It is built based on the three basic principles: protection, detection and correction. Students will have the opportunity to have hands-on experience in penetration testing, emerging technologies, vulnerability analysis, network security, human-computer interaction, wireless security, and cryptography [24]. The programme core knowledge covers wide range of fields (see Table 15).

*Table 15. Core courses of MSc in Cyber Security Engineering, UW:BOTHEL [24]*

| Core | Description |
|---|---|
| Security, Policy, Ethics, and the Legal Environment | Addresses ethical, legal, and policy frameworks within which information assurance and secure development lifecycle professionals must practice. |
| Contemporary Issues in Information Assurance | Addresses current developments in information assurance and cyber security, such as the changing threat spectrum, legal developments, international relationships, and intellectual property protection with an emphasis on the ethical and moral perspectives. Covers communities and resources important to becoming a responsible professional in the security field |
| Information Assurance and Secure Development Lifecycle | Covers the foundations of Information Assurance (IA) and the Secure Development Lifecycle (SDL) needed to understand and apply best practices for development and on-going support of secure software systems in organizations. Uses workshops and applied project to practice methods and create artifacts important to IA principles |
| Incident Response Recovery | Explores management of response to security incidents including identification, examination, and integration of diverse crisis and emergency management, disaster recovery, and organizational continuity management issues. Also covers incident tracking, patch management, and corrective responses to internal and external stakeholders |
| Cryptography and Data Assurance | Explores symmetric and asymmetric cryptography, key management, and encryption algorithms such as DES, AES, RSA, and PGP. Discusses PKI, SSL, and VPN including how to use protocols, hashing, digital signatures, and certificates and certificate authorities. Covers policies, procedures, and methods for the proper use of cyptography in secure systems |
| Network and Internet Security | Examines the theory and practice of network security, the role of cryptography, and the current state of the art in building secure networked systems. Covers topics such as access control, authentication, perimeter security defense, firewalls, virtual private networks, intrusion detection systems, and wireless security and network security auditing tools |
| Secure Software Development | Examines secure design and secure coding principles, practices, and methods including least privilege, threat modeling, and static analysis. Covers common vulnerabilities such as buffer overruns, integer overflows, injection attacks, cross-site scripting, and weak error handling in detail |
| Vulnerability Analysis and Detection | Explores vulnerability analysis and exploitation, penetration testing tools, and defense techniques. Covers topics such as OS fingerprinting, remote network mapping, software and operational vulnerabilities, attack surface analysis, fuzz testing, patch management, and security auditing |

The program pays attention to writing skills as well to enable students develop technical and scientific skills, make assessments. The programme is concluded with a project or a master thesis.

**(8) The University of Washington** offers a second master programme – Cyber Security & Leadership. “The programme develops leaders who can effectively identify and promote solutions that protect an organization’s cyber systems” [25]. The programme covers the following courses:

- Principles of Cybersecurity
- Business Essentials
- Leadership and Team Dynamics
- Networking and Internet Security
- Information Assurance, Risk Management and Security Strategies
- Strategic Organization Change
- Cybersecurity Management
- Project Management

Students are expected to gain significant risk management skills.

**(9) Lancaster University - Cyber Security Master of Science.** The programme combines advanced technical skills with disciplines such as Economics, Risk Management, Psychology and Social Science [26]. Fosters broadening awareness to make sound decisions. The programmes is concluded with a dissertation in communication and information systems.

Additional value of the course is that it equips students with the knowledge and skills required to obtain certificates such as CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker) and CHFI (Computer Hacking Forensic Investigator).

*Table 16. Lancaster University Cyber Security MSc core courses [26].*

| **Core** | Brief Description |
|---|---|
| Information Systems Security Management | Students will gain a solid understanding of the current information security technologies and practices, and will develop a wide appreciation of IT security by exploring |

| | |
|---|---|
| | access control systems, business continuity and disaster recovery, all within the context of legal and ethical frameworks |
| Information Systems Penetration and Countermeasures | Develops skills and understanding required to test IT infrastructure for vulnerabilities to malicious attack |
| Information Systems Forensic Investigation | Covers skills and technologies required to gather information and draw inferences from that data regarding the attack as it occurred or as it unfolds |
| Information System Risk Management | This module will identify key frameworks, international standards and best practices involved in Risk Assessment, Business Impact Analysis, Asset Identification and Risk Management |
| Network and Systems Security | This module provides an introduction to the process of networked system security, reviewing network and system security issues and threats, and presents a broad view of network and system security services and mechanisms, whose understanding is essential in the design and implementation of security strategies for a networked environment |
| Security and Conflict in the Digital Age | N/A |
| Cybercrime | This module helps to acquire a more critical understanding of deviance online, “cybercrime”, and “cybersecurity”. It encourages students to reflect on the various historical, cultural, socio-economic, socio-political and socio-technical contexts that may contribute to the emergence of criminal activity and deviance online |
| Introduction to Law | N/A |

**(10) University of York** – Cyber Security Master of Science. This course provides a “broad education in cyber security” and “allows make technically informed principled decisions”. It is aimed for students with strong technical background (computing and networks) willing to pursue a career in industry or government [27].

The programme will address the following areas:

- Identity

- Trust and reputation
- Cryptography
- Network Security
- Malware and Intrusion detection
- Risk Management
- Development of high assurance systems

**(11) University of Birmingham** – Cyber Security Masters. The programme is aimed for graduates in a computing-related discipline. It equips students with the knowledge and skills necessary to design cyberattacks-resistant systems. The programme covers cryptography, network security and secure programming, also offers optional courses in hardware and embedded system security, operating systems and incident management and forensics [28].

*Table 17. MSc Master's programme core courses at the University of Birmingham [28].*

| Compulsory | Description |
|---|---|
| Anonymity, privacy and cybercrime | Covers most common cyber-crimes; how cyber crime can be stopped and how can people protect themselves; privacy protection and anonymity system |
| Cryptography | Covers the fundamentals of cryptography, as well as its applications and issues of how cryptography is used in practice |
| Designing secure systems | This module will introduce the fundamental concepts involved in designing systems that are secure, with examples and counter-examples |
| Network security (Extended) | The module introduces the threats and attacks which may be perpetrated on computer networks, and some of the mechanisms designed to address them. Some technology case studies are presented and evaluated. Pre-requisite: Networks, OSs, Computer systems & architecture, C/C++ |
| Secure programming | The module covers the basics of software security. Classic design principles for the protection of information in computer systems are introduced. Some of the most important vulnerabilities in current software systems and the corresponding attacks are reviewed. It is then shown how to defend code against these attacks, both by means of careful programming technique and automated machine support |
| Secure system management | The course will cover fundamental security concepts currently covered in the withdrawn Computer Security (assets, threats, risk analysis and adversarial thinking), security management systems such as ISO 27001 and security professionalism |

| | |
|---|---|
| Project | This module enables the student to demonstrate professional competence in a substantial software-related task and to apply material learned in other components of the degree programme. Projects are chosen from staff suggestions or are developed from the student's original idea. The project may be completed in industry in the form of a work placement |

**(12) University of Kent** – Cyber Security MSc. This is a cyber security programme for students with firm programming skills and "will teach the essential skills to support cyber security within commercial and government organisations. This includes the technical side of encryption, authentication, biometrics, network security, etc as well as information security management and cyber security risk" [29]. The programme lists eight possible modules that could be covered during the whole education process: network-related courses such as network and network security, advanced network security seem to take important part in the process, covering network protocols, layers and their security, firewalls, routing, IDS, IPS, weaknesses of networks and countermeasures among many others. The programme might also encompass computer security (topics related to cryptography, OSs security, malwares among the listed ones), system security (including secure software development) and biometric technologies. The crowning part of the programme is Project and Dissertation (or a project as an alternative) during which student's research abilities, understanding and practical skills are examined.

**(13) Queen University Belfast** – MSc Applied Cyber Security. "You'll be analytical, quizzical, technical. A modern-day codebreaker"- the programme has quite tantalising address text. The programme prepares students to be involved in threat intelligence, network security, information assurance, security operations centers; for a position of Chief Information Officer (CISO) [30].

*Table 18. MSc Applied Cyber Security core courses at Queen University Belfast [30].*

| **Modules** | |
|---|---|
| Network Security & Monitoring | Network Traffic Manipulation, Detection Tools, Secure Design Principles |
| Ethical & Legal Issues in Cyber Security | N/A |
| Software Assurance | Security in Software Development |
| Computer Forensics | Digital Media Analysis, Data Extraction, Preserving Digital Information |

| | |
|---|---|
| Malware | Understand Malware Behaviour, Obfuscation Techniques, Malware Analysis |
| Applied Cryptography | Number Theory, Security Architectures, Side-channel Cryptanalysis, Secure Algorithms |

**(14) The University of Southampton** – **MSc Cyber Security**. This is a one-year multi-disciplinary programme that addresses criminology, risk management, law and social science alongside the technical subjects enabling students broadening their understanding in the field of cyber security [31].

*Table 19. MSc Cyber Security Programme core courses, University of Southampton [31]*

| **Compulsory** | **Brief Description** |
|---|---|
| Foundations of Cyber Security | Introduces cyber security landscape considering not only technical measures and defences but also legal, management, crime, risk, social and human factors |
| Implementing Cyber Security | Involves practices to implement cyber security |
| Software Engineering and Cyber Security | This module focuses on both theoretical and practical perspectives in the development of software systems, exploring secure software design and development methods, and software analysis and reverse engineering. It therefore explores aspects of software engineering that are directly applicable to cyber security |
| Cyber Crime, Insecurity and the Dark Web | To critically evaluate cutting edge research in the area of Cyber Crime and Cyber Security; To introduce the history of research into Cyber Crime; To understand the organisations and key stake holders in the business of preventing, controlling and policing Cyber Crime; To critically evaluate the theoretical foundation of research into Cyber Crime; To develop an approach to Cyber Crime and Cyber Security that recognises the interdisciplinary nature of the area |
| Project Preparation | Preparation for the master project |

**(15) MSc in Cyber Security Engineering** at the **University of Warwick** provides broad understanding of cyber security covering aspects of technology, people and organisations [32].

*Table 20. MSc in Cyber Security Engineering core courses, University of Warwick [32].*

| **Core Modules** | **Brief Description** |
|---|---|
| Security Architecture and Network Defence | Covers the domain and fundamental concepts of cyber security such as security infrastructure and protocols; furthermore, |

| | |
|---|---|
| | malware and attacks, the threat ecosystem, phishing, pharming and data theft, the AAA of security, firewalls and defence, intrusion detection systems |
| Cyber Intelligence and Operations | This module gives students a framework to reason about cyber security in order both to anticipate incidents, and to deal with their occurrences |
| Cyber-Physical Systems | The overall aim of this module is to enable the cyber security specialist to have a meaningful conversation with practicing engineers concerning the security of cyber-physical systems |
| Enterprise Cyber Security | The course addresses key strategic cyber security issues from the perspective of an organisation's Chief Information Security Officer |
| Information Risk Management and Governance | Teaches how to establish and maintain an information risk management framework in order to guarantee that security and assurance strategies are aligned with business objectives and are consistent with legal and regulatory obligations |
| Cryptosystems and Data Protection | This module focuses on the use of encryption technology to provide authorization and access control systems, and in particular the numerous cryptosystems and protocols that allow us to keep communications private |
| Industrial Espionage and Counterfeiting | Examines motivations for industrial espionage and the various methods of attack on the physical security of an organisation, its electronic infrastructures and its staff and suppliers. Learning to analyse and mitigate potential attacks through industrial espionage, and understanding counterfeiting attacks, during this module you will design countermeasures and will carry out risk management processes in both industrial espionage and counterfeiting |
| Digital Forensics | This module investigates the core techniques currently used for the purpose of data retrieval, evidence preparation, crime scene management and intelligence extraction. Students will get an overview of international digital forensic investigation infrastructures and put legal procedures into context |

**(16) The University of Warwick** also offers **MSc in Cyber Security and Management** which prepares strategic thinkers for a leading technical or managerial positions. Core modules include (the core module description can be found in the Table 20 above) [33]:

- Security Architecture and Network Defence
- Information Risk Management and Governance
- Cryptosystems and Data Protection
- Industrial Espionage and Counterfeiting

- Digital Forensics

**(17) Tallinn University of Technology & University of Tartu – Cyber Security MSc.** The programme equips students with skills in all aspects of information systems. The programme offers students to focus either on organizational (Law, organization, psychology, standards) or technical aspects (networking, attack/defence technology) [34].

*Table 21. Cyber Security Master Programme core courses, Tallinn University of Technology [34]*

| **Core Courses** | **Brief Description** |
|---|---|
| Strategic and Operational Aspects of Cyber Security | Provides and overview of cybersecurity issues at the strategic level, also scenario training exercise |
| Malware | Covers malware types, methods, technics to analyse and remedy them with hands-on exercises |
| Network Technology I | Introduces fundamentals of networking |
| Foundations and Management of Cyber Security | Covers an overview of the area of cybersecurity, cyber introduce the core concepts and technologies and cyber security management |

**Observation 1:** In most of the cases core courses include networking, cryptography, operating systems, programming, law courses or some combination of them (ex. Combination of Networking and cryptography). All of the university programmes explicitly address network security except the Master of Science in Cyber Security by the University of Southampton.

**Observation 2:** In case of UK Universities' programmes, there are few courses that the programmes have in common and there are little options for elective courses. This can be caused by the fact that UK universities offer one-year master programme and they are limited in time, thus, focusing on more specific and more important courses for the programme to meet its objectives.

**Observation 3:** Universities are constantly reviewing and studying emerging threats, keeping close cooperation with leading industry companies and governments, based on that modifications are made in the education programmes to meet the industry and government need and demand.

# Chapter 5. The curriculum

The following chapter consists of four parts: the first part covers a brief review of the analysis made by the author in chapter three about Georgia, the next section identifies which university programme is most close to the cyber security objectives of Georgia, which is afterwards modified according to the Dampier and NICE Cybersecurity Workforce Framework (NCWF) and the cyber security skills need in Georgia. Next comes the high-level description of the curriculum, courses with brief descriptions, based on which more specific courses can be developed. Finally, the curricular is validated/verified by mapping the courses to the essential five fields suggested by Dampier and the NCWF categories.

## 5.1. What Do we have so far?

The goal of Georgia is to develop a resistant cyber security system, decrease possible damage level, recover quickly and take preventive measures. Accordingly, the programme has to meet the following criteria:

- Ensure cyber security system Confidentiality, Integrity, Availability (CIA)
- Mitigate negative results
- Ensure quick recovery
- Make corrections and take preventive measures

Existing and emerging threats facing Georgian and global cyberspace are other important aspects that should be considered when developing the programme. The National cyber security strategy document lists the following threats: cyberterrorism, cyber espionage, Cybercrime, cyber attacks against Critical Information Infrastructure. Reports by security companies [36] and some countries (UK [37], Estonia [38]) name the following wide-spread threats' list: IoT botnets, ransomware, targeted cyberespionage attacks, financial theft, hacktivism, mobile threat, carelessness and apathy in the performance of elementary procedures.

Considering the future plans, Georgia intends to put more emphasis on innovation and technology that points to the need of more information infrastructures to be secured.

The author has also conducted a survey (see chapter three) mainly to find out about the upcoming need of cyber security skills in Georgia as well as the respondents' opinion on what the cyber security master programme should be focused. The results showed (more details are available in the analysis part of the survey):

1. Network Security (78 votes)
2. Pen. Testing (63 votes)
3. Secure Coding (56 votes)
4. Cryptography (44 votes)
5. BCM (44 votes)
6. Digital Forensics (43 votes)
7. Audit (27 votes)
8. Legal aspects (22 votes)
9. Other (3 votes: incident handling and cyber security management).

## 5.2. Developing the curriculum

Having considered the requirements of Georgia in chapter three and having reviewed the university programmes in chapter four, the Cyber Security Master Programme by University of Washington [39] appears to be very close to the cyber security objectives of Georgia: the cyber security system should be robust enough to resist cyber attacks; since there is no 100 % security, Georgia should be ready for attacks and be able to recover quickly from consequences, furthermore, taking preventive measures. The Washington university programme is based on the three pillars that coincides with the cyber security goals of Georgia:

- "Protection – hardening our information infrastructures to make them more resistant to attack;
- Detection – since no amount of protection can provide 100% security, detection of intrusions by outsiders or abuses of privilege by insiders becomes critical;
- Correction – how to respond to attacks to minimize losses and facilitate re-engineering our information infrastructures to eliminate vulnerabilities being exploited and resume operations at a higher level of assurance" [39].

Another important aspect of the programme is that “students learn how to make decisions regarding investments of scarce resources in information assurance, using cost-benefit analyses to support management decisions” [39].

The cyber security master programme in Georgia could cover similar courses but with some modifications. While developing the programme the author has taken into account some key aspects suggested by Dampier [10] and NICE Framework [12].

The research paper by Dampier about building a successful cyber-security program lists courses necessary for building a cyber security programme. The list encompasses:

1. Security policy and law
2. Computer security, including both hardware and software
3. Network security
4. Digital Forensics
5. Cyber Physical Systems Security, often referred to as SCADA Security

Dampier also considers incorporating the suggestions outlined in the NICE Framework. The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF) by the National Institute of Standards and Technology (NIST) (Draft NIST special publication 800-181) is “the product of many years of collaboration regarding workforce training and education. NCWF provides as fundamental reference resource for describing and sharing information about cybersecurity work roles, the discrete tasks performed by staff within, and the knowledge, skills, and abilities (KSAs) needed to complete the tasks successfully” [12]. The framework takes proactive risk management approach and helps to provide continues monitoring of skills, knowledge and abilities needed in cyber security, the same document concludes.

National Initiative for Cybersecurity Education (NICE) Framework suggests seven categories within which cyber security work should fall:

*Table 22. NICE Framework Workforce Categories [12].*

| **NICE Framework Workforce Categories** | **Description** |
|---|---|
| Securely Provision | Conceptualizes, designs, and builds secure information technology (IT) systems, with responsibility for aspects of systems and/or networks development |
| Operate and Maintain | Provides the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security |
| Oversee and Govern<br>Protect and defend | Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work |
| Protect and Defend | Identifies, analyzes, and mitigates threats to internal IT systems and/or networks |
| Analyze | Performs highly specialized review and evaluation of incoming cybersecurity information to determine usefulness for intelligence |
| Collect and Operate | Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence |
| Investigate | Investigates events or crimes related to information technology (IT) systems, networks and digital evidence |

## 5.3. The Curriculum

The cyber security master programme will be based on three principles: Protect, Detect and Correct. It should encompass three specializations at initial stage: Network security, Risk management and digital forensics. The programme will be aimed only for students with academic and professional background in computer science or related field.

**Mission:** The mission of the programme is to provide students with a broad understanding of the cyber security alongside equipping them with technical skills, to enable them “think globally and act locally”. To prepare students meet the upcoming challenges.

**Career goals:** Students will be prepared to fulfill the roles in the field of cyber security.

**Competences:** Students will be able to build resistant cyber security systems, make assessments of the cyber security systems, identify threats and make corrections is necessary. In case of cyber attacks they will be able to recover, make assessments and take preventive measures.

The courses that should be offered by the programme:

### 1. Security, Policy, Ethics, and the Legal Aspects:

Covers nationally and internationally accepted legal, policy and ethical frameworks within which information cyber security professionals must practise.

**Outcome 1:** students will understand fundamentals of Georgian and international ethical, legal and policy frameworks, their responsibilities and rights.

**Observation 1:** Few courses had not included similar course in their curriculum. Most of the programmes had been focused on multidisciplinary technical courses. Besides, it is worth mentioning that some of the programmes do not provide full list of the courses offered, accordingly, it is difficult to proffer more precise information.

### 2. Designing Secure Systems

Explores fundamental concepts, principles and technologies for designing secure systems. The course will have prerequisites: cryptography and secure system management.

**Outcome 2:** Students will be able to make assessments, identify weak and strong design decisions and suggest corrections if necessary.

### 3. Incident Management and Forensics

The course focuses on the managerial side of cyber security incident response and handling such as identification, examination and integration of appropriate processes; Organisational continuity management issues; Techniques and tools required to gather information and draw inferences. This course will require technical knowledge and skills as a prerequisite.

**Outcome 3:** students will be introduced to the steps involved in incident response and recovery, reinforced by the practical part.

**Observation 3:** the requirement for such skills were derived from responses in the survey (see survey analysis of chapter 3).  Some of the universities who prepare students for government sector require security clearance before taking similar courses.

### 4. Cryptography

Explores fundamentals of cryptography, how it is applied and used in practise. Its integration in data assurance and network security.

**Outcome 4:** students will gain understanding of fundamentals of cryptography such as encryption, digital signatures, secure hashes. Select appropriate techniques and apply them to specific cases. Design and evaluate security protocols.

**Observation 4:** cryptographic skills are very important as the cases of ransomware has significantly increased during the previous years. McAfee named 2016 as the year of ransomware in its report [40], recent cases of WannaCry ransomware emphasize its importance [42].

### 5. Network and Internet Security

The course is a combination of theory and practice during which student will explore network security and the role of cryptography.

**Outcome 5:** students gain knowledge and skills for building and supporting secure networks. Furthermore, they will also address common vulnerabilities exploited for accomplishing successful cyber attacks and countermeasures.

**Observation 5:** Respondents mentioned network security as top one in demand now and in coming two-four years in Georgia.

### 6. Secure Software Development

Explores principles and techniques of secure coding for developing or modifying computer applications or software taking into account software assurance best practices. The course is a combination of theory and practice.

**Outcome 6:** students will explore and apply theoretical and practical part of secure coding.

**Observation 6:** Secure coding was mentioned by the respondents in top 3 cyber security skills.

### 7. Vulnerability Analysis and Detection

Addresses vulnerability analysis and exploitation, penetration testing tools, and defense techniques. Senses potential threats. Covers topics such as OS fingerprinting, remote network mapping, software and operational vulnerabilities, attack surface analysis, fuzz testing, patch management, and security auditing.

**Outcome 7:** students will be introduced to and practise principles and techniques to detect system vulnerabilities, identify potential threat.

**Observation 7:** Penetration testing was ranked as the number two among the skills in demand in Georgia by the respondents (see survey analysis part of the chapter 3).

### 8. Malware Reverse Engineering

Explores techniques, methods and principles for analyzing malwares. The course will have a glimpse at some influential malwares throughout the history.

**Outcome 8:** students will be equipped with the knowledge and skills necessary for conducting malware reverse engineering.

**Observation 8:** some programmes include similar course.

### 9. Secure System Management:

Addresses fundamental security concepts (assets, threats, risk analysis, adversarial thinking), security management systems.

**Outcome 9:** Students will be able to conduct risk assessments and develop risk treatment plans.

Additionally, other courses due to changing requirements could be considered: Principles of Operating Systems, Biometrics (face, fingerprint, image recognition), Embedded systems.

To continue with the admission requirements in Georgia, generally unified post-graduate exam [41] should be passed to be eligible for joining a master-level university programme; student should hold at least a bachelor's degree and should have earned minimum credits in some field(s) (ex. a student may be accepted to a Master programme in Information Systems only if he/she had earned minimum 10 ECTS credits in mathematics and minimum 10 ECTS credits in programming); the student has to pass a programme admission exam (ex. a student has to pass an exam in informatics to be allowed to join the Master programme in Information Systems). For admitting students to the Cyber Security master programme, at least the following criteria should be met:

- A bachelors' degree in computer science or closely related field (information systems, information technology or electrical engineering)
- Programming capabilities
- Understanding of computer networking and Operating Systems

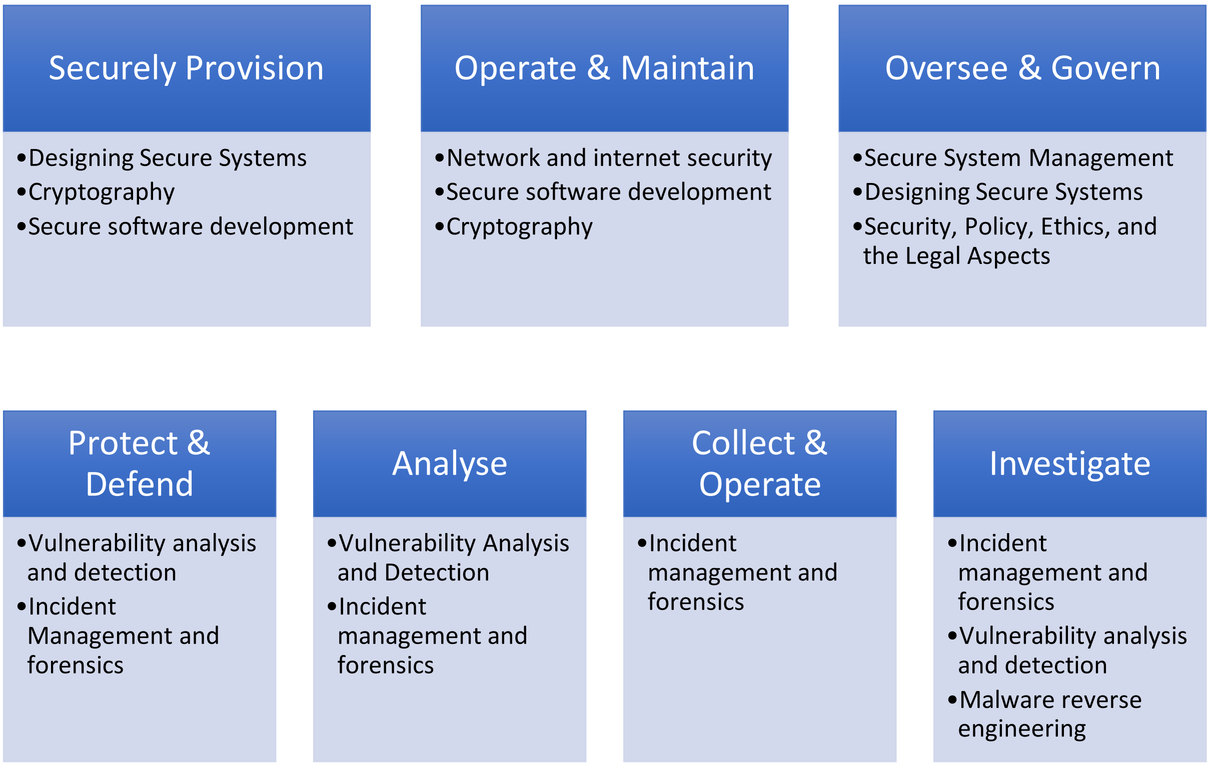
## 5.4. Validation

The final version of the curricular meets the criteria suggested both by Dampier and the NCWF:

*Table 23. Mapping courses with the five essential fields suggested by Dampier.*

| N | Essentials | Corresponding courses in the curriculum |
|---|---|---|
| 1 | Security Policy and law | Security, Policy, Ethics, and the Legal Aspects |
| 2 | Computer security | - Designing Secure Systems<br>- Secure Software Development<br>- Vulnerability Analysis and Detection<br>- Malware Reverse Engineering |

| | | |
|---|---|---|
| 3 | Network security | - Cryptography<br>- Network and Internet Security<br>- Designing secure systems |
| 4 | Digital forensics | - Incident Management and Forensics<br>- Malware reverse engineering |
| 5 | Cyber Physical systems security | - Designing Secure Systems<br>- Secure system management |



Securely Provision

- Designing Secure Systems
- Cryptography
- Secure software development

Operate & Maintain

- Network and internet security
- Secure software development
- Cryptography

Oversee & Govern

- Secure System Management
- Designing Secure Systems
- Security, Policy, Ethics, and the Legal Aspects

Protect & Defend

- Vulnerability analysis and detection
- Incident Management and forensics

Analyse

- Vulnerability Analysis and Detection
- Incident management and forensics

Collect & Operate

- Incident management and forensics

Investigate

- Incident management and forensics
- Vulnerability analysis and detection
- Malware reverse engineering

*Table 24. Mapping courses and NICE Framework categories.*

**Securely Provision** category will be addressed by three courses: Designing Secure Systems, Cryptography, Secure Software Development.

Three courses Cryptography, Network and Internet Security and Secure Software Development will focus on the second category - **Operate and Maintain**.

Category **Oversee and Govern** will be covered in three courses: Secure Systems Management, Designing Secure Systems, and Security, Policy, Ethics and Legal Aspects.

The three course can develop skills and knowledges to oversee if the developments are compatible with legal and policy frameworks and meet the cyber security criteria.

Category **Protect and Defend** will be covered in Vulnerability Analysis and Detection and Incident Management and Forensics which will be focused on detecting weaknesses to facilitate the process of making corrections where necessary.

Courses Vulnerability Analysis and Detection, and Incident Management and Forensics will also address the category **Analyze**.

Course Incident Management and Forensics falls within the category **Collect and Operate** as it focuses on collecting and managing data important for making investigations.

Category **Investigate** will be covered in courses Incident Management and Forensics, Vulnerability Analysis and Detection and Malware Reverse Engineering.

# Chapter 6. Conclusion

The purpose of the thesis has been to build a high-level description of the curriculum based on which more specific courses can be developed.

To achieve the purpose the author has studied the cyber security environment in Georgia and cyber security goals of the country based on the national guiding documents and the survey conducted among the IT professionals in Georgia. Already existing successful cyber security programmes were examined to facilitate the curriculum development process. Existing guiding principles were considered, such as National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF) and suggestions offered by Dampier, to tailor the cyber security master programme to meet the local and global cyber security skills need in Georgia.

Conducted analysis implied to the main principles on which the curriculum should have focused – Protect, Detect and Correct. Protect – to ensure cyber security systems are built (and modified if necessary) taking into account security concepts and techniques to reinforce Confidentiality, Integrity and Availability of cyber security systems. Detect – since there is no fully guaranteed cyber security, there should be appropriate means available to identify and detect threats; and in case of cyber attacks to take urgent measures to redress from adverse impacts caused by the cyberattacks - addressed by the third principle - Correct. The latter also encompasses further corrections and preventive measures to reinforce the cyber security system. Therefore, the author demonstrated the programmes at initial stage should offer three specialisations in Network Security, Risk Management and Digital Forensics.

The curriculum described above lists major courses that should be covered by the cyber security master programme in Georgia. Additionally, the analysis provided can be helpful for education institutions willing to initiate the cyber security programme or make improvements in the existing one. The curriculum does not portray deep description of the courses and accreditation has been beyond the scope of this master thesis. Further developments of the curricular are in the hands of the educations institutions willing to take advantage of the work done.

# Bibliography

[1] E. Tikk, et al. (November 2008). “Cyber Attacks Against Georgia: Legal Lessons Identified”. Tallinn, Estonia: CCDCOE.

[2] J. Berzins (April 2014). “Russia’s New Generation Warfare in Ukraine: Implications for Latvian Defense Policy”. National Defence Academy of Latvia, Center for Security and Strategic Research.

[3] N. Falliere, L. O Murchu, and E. Chien (February 2011). “W32.Stuxnet Dossier”. Symantec.

[4] W.A Conklin, R.E. Cline, T. Roosa, “Re-engineering cybersecurity education in the US: an analysis of the critical factors”, Proceedings of the Annual Hawaii International Conference on System Sciences, pp. 2006-2014, 2014.

[5] საქართველოს მთავრობა, საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნული სტრატეგია (2017). Available: http://gov.ge/files/469_59439_212523_14.pdf [Accessed: April 2017].

[6] Government of Georgia, Ordinance of the Government of Georgia on Approval of Socio-Economic Development Strategy of Georgia – “Georgia 2020” and Associated Activities (June 2014). Available: https://matsne.gov.ge/en/document/view/2373855 [Accessed: April 2017].

[7] Government of Georgia, Socio-Economic Development Strategy of Georgia – “Georgia 2020” (2014). Available: https://www.adb.org/sites/default/files/linked-documents/cps-geo-2014-2018-sd-01.pdf [Accessed: April 2017].

[8] Ponemon Institute (February 2014). “2014 Best Schools for Cybersecurity”. Available: https://www.ponemon.org/local/upload/file/2014%20Best%20Schools%20Report%20FINAL%202.pdf [Accessed: April 2017].

[9] National Cyber Security Centre (May 2016). “GCHQ-certified Degrees”. [Online]. Available: https://www.ncsc.gov.uk/information/gchq-certified-degrees [Accessed: April 2017].

[10] D. Dampier (2010). “Building a Successful Cyber-security Program”. Distributed Analytical and Security Institute, Mississippi State University. Available: http://www.dasi.msstate.edu/publications/docs/2015/06/13502Cyber_Security_Workshop_paper_-_Final.pdf [Accessed: April 2017].

[11] Government of Georgia, “National Cyber security strategy of Georgia 2012-2015,” dea.gov.ge. Available: http://www.dea.gov.ge/uploads/National%20Cyber%20Security%20Strategy%20of%20Georgia_ENG.pdf [Accessed: April 2017].

[12] B. Newhouse, S. Keith, B. Scribner and G. Witte (November 2016), “NICE Cybersecurity Workforce Framework (NCWF)”. Draft NIST Special Publication 800-181, National Institute of Standards and Technology (NIST), U.S. Department of Commerce.

[13] Cyber Security Bureau, “Action Plan 2016-2017”. Ministry of Defence of Georgia, Tbilisi, Georgia. Available: http://csbd.gov.ge/doc/Cyber-Security-Development-Action-Plan-GEO-ENG.pdf [Accessed: April 2017].

[14] Cabinet Office and Government Communications Headquarters, “Cyber security skills: business perspectives and government’s next steps”. Department for Business, Innovation & Skills, UK, March 2014. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/289806/bis-14-647-cyber-security-skills-business-perspectives-and-governments-next-steps.pdf [Accessed: May 2017].

[15] SANS Institute. “Cybersecurity Professional Trends”. A SANS Survey. May 2014. Available: https://www.sans.org/reading-room/whitepapers/analyst/cybersecurity-professional-trends-survey-34615 [Accessed: May 2017].

[16] Global Cybersecurity Index and Cyberwellness Profiles (April 2015), International Telecommunications Union (ITU). Geneva, Switzerland, 2015.

[17] University of Texas, San Antonio (UTSA), “Master of Business Administration – Cyber Security Concentration”. utsa.edu [Online]. Available: http://catalog.utsa.edu/graduate/business/informationsystemscybersecurity/#degreestext [Accessed: May 2017].

[18] University of Texas, San Antonio (UTSA), “Master of Science in Information Technology – Cyber Security Concentration”. utsa.edu [Online]. Available: http://catalog.utsa.edu/graduate/business/informationsystemscybersecurity/#degreestext [Accessed: May 2017].

[19] Mississippi State University (September 8, 2016), “New Graduate Degree Outline Form”. University Committee on Courses and Curricular. Mississippi State, USA.

[20] Mississippi State University, “MSU adds master’s program in cyber security and operations”. Mssstate.edu. [Online]. Available: http://www.msstate.edu/newsroom/article/2017/04/msu-adds-master’s-program-cyber-security-and-operations/ [Accessed: May 2017].

[21] Syracuse University, “Master of Science in Cybersecurity”, engineeringonline.syr.edu. [Online]. Available: https://engineeringonline.syr.edu/graduate-programs/cybersecurity/ [Accessed: May 2017].

[22] Carnegie Mellon University (CMU) - Africa, Master of Science in Information Technology (MSIT) – Cyber Security Concentration. Cmu.edu. [Online]. Available: http://www.cmu.edu/africa/degree-program/concentrations/cyber-security.html [Accessed: May 2017].

[23] University of South California, Master of Science in Cyber Security Engineering. Usc.edu. [Online]. Available: https://gapp.usc.edu/cyber [Accessed: May 2017].

[24] University of Washington, BOTHEL, Master of Science in Cyber Security Engineering. Uwb.edu. [Online]. Available: https://www.uwb.edu/cybersecurity [Accessed: May 2017].

[25] University of Washington, TACOMA, Master of Cybersecurity and Leadership (MCL). Tacoma.uw.edu. [Online]. Available: http://www.tacoma.uw.edu/institute-technology/cybersecurity-leadership [Accessed: May 2017].

[26] Lancaster University, Cyber Security Master of Science. Lancaster.ac.uk [Online]. Available: http://www.lancaster.ac.uk/scc/postgraduate/taught-masters/courses/cyber-security-msc/ [Accessed: May 2017].

[27] University of York, Master of Science in Cyber Security. Cs.york.ac.uk. [Online]. Available: https://www.cs.york.ac.uk/postgraduate/taught-courses/msc-cybersecurity/ [Accessed: May 2017].

[28] University of Birmingham, Cyber Security Master of Science. Birmingham.ac.uk. [Online]. Available: http://www.birmingham.ac.uk/postgraduate/courses/taught/computer-science/cyber-security.aspx#CourseOverviewTab [Accessed: May 2017].

[29] University of Kent. "Cyber Security – MSc". Kent.ac.uk. [Online]. Available: https://www.kent.ac.uk/courses/postgraduate/1225/cyber-security [Accessed: May 2017].

[30] Queen University Belfast, "MSc Applied Cyber Security". Csit.qub.ac.uk. [Online]. Available: http://www.csit.qub.ac.uk/EducationatCSIT/MSc-Applied-Cyber-Security/ [Accessed: May 2017].

[31] The University of Southampton, "MSc Cyber Security". Ecs.soton.ac.uk. [Online]. Available: http://www.ecs.soton.ac.uk/programmes/msc-cyber-security#_ga=1.62635756.1333079416.1492779158 [Accessed: May 2017].

[32] University of Warwick, "MSc in Cyber Security Engineering". www2.warwick.ac.uk. [Online]. Available: http://www2.warwick.ac.uk/fac/sci/wmg/education/prof-ed/postgraduate/post_grad/cyber_engineering [Accessed: May 2017].

[33] University of Warwick, "Master of Science in Cyber Security and Management". www2.warwick.ac.uk. [Online]. Available: http://www2.warwick.ac.uk/fac/sci/wmg/education/prof-ed/postgraduate/post_grad/cyber/ [Accessed: May 2017].

[34] Tallinn University of Technology, "Cyber Security". Ttu.ee. [Online]. Available: https://www.ttu.ee/studying/masters/masters_programmes/cyber-security/cyber-security-4/ [Accessed: May 2017].

[35] University of Texas, San Antonino. "Cyber security". Business.utsa.edu. [Online]. Available: http://business.utsa.edu/cybersecurity/ [Accessed: May 2017].

[36] Kaspersky. "2016 results, 2017 predictions". AO Kaspersky Lab. [Online]. Available: https://blog.kaspersky.com/kaspersky-predictions-2017/13776/ [Accessed: May 2017].

[37] National Cyber Security Centre. "Cyber threat to UK business". 2016-2017 Report. National Crime Agency (NCA). Available: https://www.ncsc.gov.uk/content/files/protected_files/news_files/The%20Cyber%20Threat%20to%20UK%20Business%20%28b%29.pdf [Accessed: May 2017].

[38] Information System Authority (2016). "2015 Annual Report of the Estonian Information System Authority's Cyber Security Branch". Available: https://www.ria.ee/public/Kuberturvalisus/2015-RIA-Annual-cyber-report.pdf [Accessed: May 2017].

[39] University of Washington, BOTHEL. "Curriculum". Uwb.edu. [Online]. Available: https://www.uwb.edu/cybersecurity/curriculum [Accessed: May 2017].

[40] McAfee Labs. "Threats Report December 2016". Mcafee.com. [Online]. Available: https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-dec-2016.pdf [Accessed: May 2017].

[41] National Assessment and Examination Center. “Unified Post-graduate Exam”. www1.naec.ge. [Online]. Available: http://www1.naec.ge/component/content/article/172-all-category/1171-unified-post-graduate-exam.html?lang=en-GB [Accessed: May 2017].

[42] The Guardian. “Ransomeware attack “like having a Tomahawk missile stolen”, says Microsoft boss”. The guardian News. [Online]. Available: https://www.theguardian.com/technology/2017/may/15/ransomware-attack-like-having-a-tomahawk-missile-stolen-says-microsoft-boss [Accessed: May 2017].

# Appendix 1 – Questionnaire for public and private companies

(the original questionnaire in Georgian)

## 1. შესავალი

მოგესალმებით და წინასწარ მადლობას გიხდით მონაწილეობისათვის!

კითხვარი ნაწილია სამაგისტრო ნაშრომისა, რომელიც მიზნად ისახავს საქართველოსთვის კიბერუსაფრთხოების სამაგისტრო პროგრამის შემუშავებას.

კითხვარი გამიზნულია კერძო და სახელმწიფო სტრუქტურებში, დაწესებულებებში, ორგანიზაციებსა თუ კომპანიებში ინფორმაციული ტექნოლოგიების სფეროში დასაქმებული პირებისათვის.

კითხვარი მოიცავს 28 კითხვას : 22 კითხვა - თემატური ნაწილი, 6 კითხვა - დემოგრაფიული ნაწილი. პასუხ(ებ)ი შეგიძლიათ აირჩიოთ ჩამონათვალიდან ან მიუთითონ საკუთარი ვარიანტი. კითხვარის შესავსებად დაგჭირდებათ დახლოებით 10 წუთი. კითხვარის ფორმატი უზრუნველყოფს კონფიდენციალურობას.

კითხვებთან კომენტარებით შეგიძლიათ მიმართოთ სოფიო სახოკიას:

Sophio.Sakhokia@mail.ttu.ee

## 2. კითხვარი

გთხოვთ, შეავსოთ ქვემოთ მოცემული ველები.

1. მიუთითეთ თქვენი კომპანიის სიდიდე:

1. მიკრო (0-9 თანამშრომელი)
2. მცირე (10-49 თანამშრომელი)
3. საშუალო (50-249 თანამშრომელი)
4. მსხვილი (250+ თანამშრომელი)

2. ჩამოთვლილთაგან რომელ სექტორს მიეკუთვნება თქვენი კომპანია?

1. სახელმწიფო
2. კერძო

3. ჩამოთვლილთაგან რომელ სფეროს მიეკუთვნება თქვენი კომპანია?

1. საბანკო/საფინანსო
2. თავდაცვა/უსაფრთხოება
3. ჯანმრთელობა და სოც. მომსახურება
4. ტექნოლოგიები/პროგრამული უზრუნველყოფა
5. ენერგეტიკა და სხვა კომუნალური მომსახურებები
6. ტრანსპორტი
7. კომუნიკაციები
8. გართობა და მედია
9. მრეწველობა
10. სოფლის მეურნეობა და კვება
11. ტურიზმი
12. სხვა:

4. ამჟამად თქვენი კომპანიის IT განყოფილებაში რამდენ პროცენტს შეადგენენ კიბერუსაფრთხოების სპეციალისტები?

1. 0 <= 1%
2. 1% <= 10%
3. 10% <= 20%
4. 20% <= 40%
5. 40% <= 60%
6. სხვა:

5. თქვენი აზრით, გაიზრდება თუ არა კიბერუსაფრთხოების სპეციალისტების რაოდენობა თქვენს კომპანიაში 3-5 წელიწადში?

1. დიახ
2. არა

6. კიბერუსაფრთხოების რომელი უნარ-ჩვევებია ამჟამად ყველაზე მნიშვნელოვანი თქვენი კომპანიისთვის?

1. ქსელის უსაფრთხოება
2. კრიპტოგრაფია
3. უსაფრთხო კოდირება (Secure coding)
4. შეღწევადობის ტესტირება (Pen testing)
5. ციფრული კრიმინალისტიკა (Digital forensics)
6. ბიზნესუწყვეტობის მართვა (Business continuity management)
7. აუდიტი
8. სამართალი
9. სხვა:

7. თქვენი აზრით, კიბერუსაფრთხოების რომელი უნარ-ჩვევები შეიძლება იყოს ყველაზე მნიშვნელოვანი თქვენი კომპანიისთვის 3-5 წელიწადში?

   1. ქსელის უსაფრთხოება
   2. კრიპტოგრაფია
   3. უსაფრთხო კოდირება (Secure coding)
   4. შეღწევადობის ტესტირება (Pen testing)
   5. ციფრული კრიმინალისტიკა (Digital forensics)
   6. ბიზნესუწყვეტობის მართვა (Business continuity management)
   7. აუდიტი
   8. სამართალი
   9. სხვა:

8. თქვენი აზრით, კიბერუსაფრთხოების რომელი მიმართულების სპეციალისტის პოვნაა ყველაზე რთული ამჟამად საქართველოში?

   1. ქსელის უსაფრთხოება
   2. კრიპტოგრაფია
   3. უსაფრთხო კოდირება (Secure coding)
   4. შეღწევადობის ტესტირება (Pen testing)
   5. ციფრული კრიმინალისტიკა (Digital forensics)
   6. ბიზნესუწყვეტობის მართვა (Business continuity management)
   7. აუდიტი
   8. სამართალი
   9. სხვა:

9. ყველაზე მეტად რომელი მიმართულებით ვერ ხერხდება ამჟამად საქართველოში განათლების მიღება?

   1. ქსელის უსაფრთხოება
   2. კრიპტოგრაფია
   3. უსაფრთხო კოდირება (Secure coding)
   4. შეღწევადობის ტესტირება (Pen testing)
   5. ციფრული კრიმინალისტიკა (Digital forensics)
   6. ბიზნესუწყვეტობის მართვა (Business continuity management)
   7. აუდიტი
   8. სამართალი

9. სხვა:

10. რა საშუალებებს მიმართავს თქვენი კომპანია კიბერუსაფრთხოების სფეროს თანამშრომლების კვალიფიკაციის ასამაღლებლად?

1. კომპანიის შიდა ტრენინგები
2. ტრენინგები საქართველოში, კომპანიის გარეთ
3. ტრენინგები საზღვარგარეთ
4. უმაღლესი საგანმანათლებლო პროგრამები
5. არ განიხილება
6. სხვა:

11. თქვენი აზრით, რა საშუალებებს მიმართავს თქვენი კომპანია კიბერუსაფრთხოების სფეროს თანამშრომლების კვალიფიკაციის ასამაღლებლად 3-5 წელიწადში?

1. კომპანიის შიდა ტრენინგები
2. ტრენინგები საქართველოში, კომპანიის გარეთ
3. ტრენინგები საზღვარგარეთ
4. უმაღლესი საგანმანათლებლო პროგრამები
5. არ განიხილება
6. სხვა:

12. მიუმართავს თუ არა თქვენს კომპანიას რომელიმე სასწავლო დაწესებულებისთვის კიბერუსაფრთხოების სფეროს თანამშრობლების კვალიფიკაციის ასამაღლებლად?

1. არა
2. დიახ
3. არ ვიცი

13. თქვენს კომპანიაში კიბერუსაფრთხოებაზე ზრუნვა ეკისრება:

1. თანამშრომელს, რომელსაც ინფორმაციული

ტექნოლოგიების სხვა სფეროც ევალება

2. თანამშრომელს, რომელსაც მანამდე ინფორმაციული ტექნოლოგიების სხვა სფერო ევალებოდა
3. კიბერუსაფრთხოების მაგისტრატურის კურსდამთავრებულს
4. ინფორმაციული ტექნოლოგიების ბაკალავრიატის კურსდამთავრებულს
5. კიბერუსაფრთხოების გამოცდილი წარმატებულ პროფესიონალს
6. სხვა:

14. თქვენი აზრით, როგორ შეუძლია თქვენს კომპანიას ხელი შეუწყოს საქართველოში კიბერუსაფრთხოების სამაგისტრო პროგრამის განვითარებას?

1. შესაძლებელია წინადადებების შეთავაზება კიბერუსაფრთხოების უნარ-ჩვევებთან დაკავშირებით
2. შესაძლებელია უნივერსიტეტთან თანამშრომლობა საკითხების შემუშავებისას
3. შესაძლებელია სტუდენტებისთვის გრძელვადიანი ან მოკლევადიანი სტაჟირებების შეთავაზება
4. შესაძლებელია სტუდენტებისთვის გრძელვადიანი ან მოკლევადიანი ხელფასიანი სტაჟირებების შეთავაზება
5. შესაძლებელია მაგისტრანტ(ებ)ის დაფინანსება
6. სხვა:

15. თქვენი აზრით, სამაგისტრო პროგრამას უნდა ჰქონდეს ერთი ძირითადი მიმართულება თუ რამდენიმე?

1. ერთი
2. რამდენიმე

16. თქვენი აზრით, ძირითადად რომელ მიმართულება(ებ)ზე უნდა იყოს ორიენტირებული კიბერუსაფრთხოების

სამაგისტრო პროგრამა? (მე-15 კითხვის პასუხის გათვალისწინებით, მიუთითეთ ერთი ან რამდენიმე მიმართულება)

1. ქსელის უსაფრთხოება
2. კრიპტოგრაფია
3. უსაფრთხო კოდირება (Secure coding)
4. შეღწევადობის ტესტირება (Pen testing)
5. ციფრული კრიმინალისტიკა (Digital forensics)
6. ბიზნესუწყვეტობის მართვა (Business continuity management)
7. აუდიტი
8. სამართალი
9. სხვა:

17. თქვენი აზრით, სად უნდა შეიქმნას კიბერუსაფრთხოების სამაგისტრო პროგრამა:

1. სახელმწიფო უმაღლესი სასწავლებლის ბაზაზე
2. კერძო უმაღლესი სასწავლებლის ბაზაზე
3. სამხედრო უმაღლესი სასწავლებლის ბაზაზე

18.თქვენი აზრით როგორი უნდა იყოს აკადემიური პერსონალი:

1. გამოცდილი პროფესიონალი, რომელიც ამჟამად მუშაობს კიბერუსაფრთხოების სფეროში
2. გამოცდილი პროფესიონალი, რომელსაც აქვს უმაღლესი განათლება ინფორმატიული ტექნოლოგიების სფეროში და მუშაობს კიბერუსაფრთხოების სფეროში
3. სხვა:

19.თქვენი აზრით, უნდა სთავაზობდეს თუ არა სამაგისტრო პროგრამა კურსდამთავრებულს დასაქმების შესაძლებლობას?

1. დიახ

2. არა

20.თქვენი აზრით, სასწავლო პროგრამაში გათვალისწინებული უნდა იყოს სტაჟირებები?

1. დიახ
2. არა

21.თქვენი აზრით, პროგრამაში გათვალისწინებული უნდა იყოს თუ არა აქტივობები სასწავლო კურიკულუმს გარეთ (მაგ. კომპანიების მონახულება, პრობლემების გადაჭრის პროცესზე დაკვირვება და/ან მათში მონაწილეობა)?

1. დიახ
2. არა

22. თქვენი აზრით, საერთო სამაგისტრო გამოცდების შედეგების გარდა, კიდევ რა კრიტერიუმები უნდა იყოს გათვალისწინებული კიბერუსაფრთხოების სამაგისტრო პროგრამაზე ჩარიცხვისას?

1. აუცილებელია უმაღლესი განათლება ინფორმაციული ტექნოლოგიების სფეროში; ასევე, აუცილებელია მინიმუმ ორწლიანი სამუშაო გამოცდილება ინფორმაციული ტექნოლოგიების სფეროში
2. აუცილებელია უმაღლესი განათლება ინფორმაციული ტექნოლოგიების სფეროში; სამუშაო გამოცდილება აუცილებელი არ არის
3. დასაშვებია უმაღლესი განათლება არატექნიკური მიმართულებით; აუცილებელია მინიმუმ ორწლიანი სამუშაო გამოცდილება ინფორმაციული ტექნოლოგიების სფეროში
4. სხვა:

## 3.დემოგრაფიული მონაცემები

გთხოვთ, შეავსოთ ქვემოთ მოცემული ველები:

1. ასაკი:

1. 18 – 24
2. 25 – 34
3. 35 – 44
4. 45 – 54
5. 55 – 64
6. 64+

2. სქესი:

1. მამრობითი
2. მდედრობითი

3. რამდენი ხანია რაც მუშაობთ ინფორმაციული ტექნოლოგიების სფეროში?

1. <= 1 წელი
2. 1წელი <= 2წელი
3. 2 წელი <= 5 წელი
4. 5 წელი <= 10 წელი
5. სხვა:

4. რამდენი ხანია რაც მუშაობთ თქვენი კომპანიის ინფორმაციული ტექნოლოგიების სფეროში?

1. <= 1 წელი
2. 1წელი <= 2წელი
3. 2 წელი <= 5 წელი
4. 5 წელი <= 10 წელი
5. სხვა:

5. დაკავებული თანამდებობა:

1. აღმასრულებელი თანამდებობის პირი
2. დირექტორი
3. მენეჯერი
4. სისტემის ადმინისტრატორი
5. ქსელის ადმინისტრატორი
6. ტექნიკოსი
7. სხვა:

6. საკონტაქტო ინფორმაცია (შევსება სავალდებულო არ არის):

## 4. კითხვარის შევსება დასრულებულია.

კითხვები, კომენტარები ან შენიშვნები შეგიძლიათ მიუთითოთ ქვემოთ მოცემულ ველში ან მიმართოთ სოფიო სახოკიას: Sophio.Sakhokia@mail.ttu.ee

მადლობა მონაწილეობისათვის!

# Appendix 2 – Questionnaire for public and private education institutions

(the original questionnaire in Georgian)

## 2. შესავალი

მოგესალმებით და წინასწარ მადლობას გიხდით მონაწილეობისათვის!

კითხვარი ნაწილია სამაგისტრო ნაშრომისა, რომელიც მიზნად ისახავს საქართველოსთვის კიბერუსაფრთხოების სამაგისტრო პროგრამის შემუშავებას.

კითხვარი გამიზნულია სახელმწიფო და კერძო უმაღლესი საგანმანათლებლო დაწესებულებების ინფორმაციული სფეროს აკადემიური პერსონალისათვის საქართველოში.

კითხვარი მოიცავს 22 კითხვას : 16 კითხვა - თემატური ნაწილი, 6 კითხვა - დემოგრაფიული ნაწილი. პასუხ(ებ)ი შეგიძლიათ აირჩიოთ ჩამონათვალიდან ან მიუთითოთ საკუთარი ვარიანტი. კითხვარის შესავსებად დაგჭირდებათ დაახლოებით 10 წუთი. კითხვარის ფორმატი უზრუნველყოფს კონფიდენციალურობას.

კითხვებითან კომენტარებით შეგიძლიათ მიმართოთ სოფიო სახოკიას:

Sophio.Sakhokia@mail.ttu.ee

## 2. კითხვარი

გთხოვთ, შეავსოთ ქვემოთ მოცემული ველები.

1. თქვენი აზრით, კიბერუსაფრთხოების რომელ უნარ-ჩვევებზეა ყველაზე მეტი მოთხოვნა ამჟამად საქართველოში?

    1. ქსელის უსაფრთხოება
    2. კრიპტოგრაფია
    3. უსაფრთხო კოდირება (Secure coding)
    4. შეღწევადობის ტესტირება (Pen testing)
    5. ციფრული კრიმინალისტიკა (Digital forensics)
    6. ბიზნესუწყვეტობის მართვა (Business continuity management)
    7. აუდიტი
    8. სამართალი
    9. სხვა:

2. თქვენი აზრით, კიბერუსაფრთხოების რომელ უნარ-ჩვევებზე შეიძლება იყოს ყველაზე მეტი მოთხოვნა საქართველოში 3-5 წელიწადში?

    1. ქსელის უსაფრთხოება
    2. კრიპტოგრაფია
    3. უსაფრთხო კოდირება (Secure coding)
    4. შეღწევადობის ტესტირება (Pen testing)
    5. ციფრული კრიმინალისტიკა (Digital forensics)
    6. ბიზნესუწყვეტობის მართვა (Business continuity management)
    7. აუდიტი
    8. სამართალი
    9. სხვა:

3. თქვენი აზრით, კიბერუსაფრთხოების რომელი

მიმართულების სპეციალისტის პოვნაა ყველაზე რთული ამჟამად საქართველოში?

1. ქსელის უსაფრთხოება
2. კრიპტოგრაფია
3. უსაფრთხო კოდირება (Secure coding)
4. შეღწევადობის ტესტირება (Pen testing)
5. ციფრული კრიმინალისტიკა (Digital forensics)
6. ბიზნესუწყვეტობის მართვა (Business continuity management)
7. აუდიტი
8. სამართალი
9. სხვა:

4. ყველაზე მეტად რომელი მიმართულებით ვერ ხერხდება ამჟამად საქართველოში განათლების მიღება?

1. ქსელის უსაფრთხოება
2. კრიპტოგრაფია
3. უსაფრთხო კოდირება (Secure coding)
4. შეღწევადობის ტესტირება (Pen testing)
5. ციფრული კრიმინალისტიკა (Digital forensics)
6. ბიზნესუწყვეტობის მართვა (Business continuity management)
7. აუდიტი
8. სამართალი
9. სხვა:

5. გთხოვთ, მიუთითოთ თუ ისწავლება რომელიმე მიმართლება თქვენს სასწავლებელში:

1. ქსელის უსაფრთხოება
2. კრიპტოგრაფია
3. უსაფრთხო კოდირება (Secure coding)
4. შეღწევადობის ტესტირება (Pen testing)
5. ციფრული კრიმინალისტიკა (Digital forensics)
6. ბიზნესუწყვეტობის მართვა (Business continuity management)

7. აუდიტი
8. სამართალი
9. სხვა:

6.თუ დაინტერესებული რომელიმე კომპანია, თქვენს სასწავლო დაწესებულებას ჩაეტარებინა ტრენინგები კიბერუსაფრთხოების სფეროში?

1. დიახ
2. არა

7.თუ დაინტერესებული რომელიმე კომპანია, თქვენს სასწავლო დაწესებულებას ჰქონოდა უმაღლესი საგანმანათლებლო პროგრამა კიბერუსაფრთხოების სფეროში?

1. დიახ
2. არა

8.თქვენი აზრით, როგორ შეუძლიათ კომპანიებს ხელი შეუწყონ საქართველოში კიბერუსაფრთხოების სამაგისტრო პროგრამის განვითარებას?

1. შესაძლებელია წინადადებების შეთავაზება კიბერუსაფრთხოების უნარ-ჩვევებთან დაკავშირებით
2. შესაძლებელია უნივერსიტეტთან თანამშრომლობა საკითხების შემუშავებისას
3. შესაძლებელია სტუდენტებისთვის გრძელვადიანი ან მოკლევადიანი სტაჟირებების შეთავაზება
4. შესაძლებელია სტუდენტებისთვის გრძელვადიანი ან მოკლევადიანი ხელფასიანი სტაჟირებების შეთავაზება
5. შესაძლებელია მაგისტრანტ(ებ)ის დაფინანსება
6. სხვა:

9. თქვენი აზრით, სამაგისტრო პროგრამას უნდა ჰქონდეს

ერთი ძირითადი მიმართულება თუ რამდენიმე?

1. ერთი
2. რამდენიმე

10. თქვენი აზრით, ძირითადად რომელ მიმართულება(ებ)ზე უნდა იყოს ორიენტირებული კიბერუსაფრთხოების სამაგისტრო პროგრამა? (მე-9 კითხვის პასუხის გათვალისწინებით, მიუთითეთ ერთი ან რამდენიმე მიმართულება)

1. ქსელის უსაფრთხოება
2. კრიპტოგრაფია
3. უსაფრთხო კოდირება (Secure coding)
4. შეღწევადობის ტესტირება (Pen testing)
5. ციფრული კრიმინალისტიკა (Digital forensics)
6. ბიზნესუწყვეტობის მართვა (Business continuity management)
7. აუდიტი
8. სამართალი
9. სხვა:

11. თქვენი აზრით, სად უნდა შეიქმნას კიბერუსაფრთხოების სამაგისტრო პროგრამა?

1. სახელმწიფო უმაღლესი სასწავლებლის ბაზაზე
2. კერძო უმაღლესი სასწავლებლის ბაზაზე
3. სამხედრო უმაღლესი სასწავლებლის ბაზაზე

12.თქვენი აზრით როგორი უნდა იყოს აკადემიური პერსონალი?

1. გამოცდილი პროფესიონალი, რომელიც ამჟამად მუშაობს კიბერუსაფრთხოების სფეროში
2. გამოცდილი პროფესიონალი, რომელსაც აქვს უმაღლესი განათლება ინფორმაციული ტექნოლოგიების სფეროში და მუშაობს კიბერუსაფრთხოების სფეროში

3. სხვა:

13.თქვენი აზრით, უნდა სთავაზობდეს თუ არა სამაგისტრო პროგრამა კურსდამთავრებულს დასაქმების შესაძლებლობას?

1. დიახ
2. არა

14.თქვენი აზრით, სასწავლო პროგრამაში გათვალისწინებული უნდა იყოს სტაჟირებები?

1. დიახ
2. არა

15.თქვენი აზრით, პროგრამაში გათვალისწინებული უნდა იყოს თუ არა აქტივობები სასწავლო კურიკულუმს გარეთ (მაგ. კომპანიების მონახულება, პრობლემების გადაჭრის პროცესზე დაკვირვება და/ან მათში მონაწილეობა)?

1. დიახ
2. არა

16. თქვენი აზრით, საერთო სამაგისტრო გამოცდების შედეგების გარდა, კიდევ რა კრიტერიუმები უნდა იყოს გათვალისწინებული კიბერუსაფრთხოების სამაგისტრო პროგრამაზე ჩარიცხვისას?

1. აუცილებელია უმაღლესი განათლება ინფორმაციული ტექნოლოგიების სფეროში; ასევე, აუცილებელია მინუმუმ ორწლიანი სამუშაო გამოცდილება ინფორმაციული ტექნოლოგიების სფეროში
2. აუცილებელია უმაღლესი განათლება ინფორმაციული ტექნოლოგიების სფეროში; სამუშაო გამოცდილება აუცილებელი არ არის
3. დასაშვებია უმაღლესი განათლება არატექნიკური მიმართულებით; აუცილებელია მინიმუმ ორწლიანი

სამუშაო გამოცდილება ინფორმაციული ტექნოლოგიების სფეროში

4. სხვა:

## 3.დემოგრაფიული მონაცემები

გთხოვთ, შეავსოთ ქვემოთ მოცემული ველები:

1. ასაკი:

1. 18 – 24
2. 25 – 34
3. 35 – 44
4. 45 – 54
5. 55 – 64
6. 64+

2. სქესი:

1. მამრობითი
2. მდედრობითი

3. რამდენი ხანია რაც მუშაობთ ინფორმაციული ტექნოლოგიების სფეროში?

1. <= 1 წელი
2. 1წელი <= 2წელი
3. 2 წელი <= 5 წელი
4. 5 წელი <= 10 წელი
5. სხვა:

4. რამდენი ხანია რაც მუშაობთ თქვენი კომპანიის

ინფორმაციული ტექნოლოგიების სფეროში?

1. <= 1 წელი
2. 1წელი <= 2წელი
3. 2 წელი <= 5 წელი
4. 5 წელი <= 10 წელი
5. სხვა:

5. დაკავებული თანამდებობა:

1. აღმასრულებელი თანამდებობის პირი
2. დირექტორი
3. მენეჯერი
4. სისტემის ადმინისტრატორი
5. ქსელის ადმინისტრატორი
6. ტექნიკოსი
7. სხვა:

6. საკონტაქტო ინფორმაცია (შევსება სავალდებულო არ არის):

## 4. კითხვარის შევსება დასრულებულია.

კითხვები, კომენტარები ან შენიშვნები შეგიძლიათ მიუთითოთ ქვემოთ მოცემულ ველში ან მიმართოთ სოფიო სახოკიას: Sophio.Sakhokia@mail.ttu.ee

მადლობა მონაწილეობისათვის!

# Appendix 3 - Questionnaire for the public and private companies

## 1. Introduction:

Hello and thank you for your participation in the survey in advance!

The following questionnaire is a part of the master thesis aimed to develop a cyber security master programme for Georgia.

The questionnaire is targeted for public and private companies, institutions and organizations. The focus is on personnel involved in the field of Information Technology.

The questionnaire consists of 28 questions: 22 of them are related to the development of cyber security master programme in Georgia, 6 questions cover a demographic part. You can either choose answer(s) from suggested options and/or provide your own suggestion. The overall process will take around 10 minutes. The format of the questionnaire ensures confidentiality.

In case of questions or comments please contact Sophio Sakhokia: sophio.sakhokia@ttu.ee

## 2. Questionnaire

Please fill the fields below.

1. Please indicate the size of your company:
   a) Micro (0-9 employees)
   b) Small (10-49 employees)
   c) Medium (50-249 employees)
   d) Large (250+ employees)

2. Please indicate if your company is public or private:
   a) Public
   b) Private

3. Which of the sectors does your company represent?
   a) Banking/Finance
   b) Defence/Security
   c) Health & social services
   d) Technology & software
   e) Energy & utilities
   f) Transportation
   g) Communications
   h) Entertainment & media
   i) Industry
   j) Agriculture & food services
   k) Tourism
   l) Other:

4. Please indicate percentage of cyber security professionals at IT department of your company:
   a) 0% <= 1%
   b) 1% <= 10%
   c) 10% <= 20%
   d) 20% <= 40%
   e) 40% <= 60%
   f) Other:

5. Do you think the number of cyber security professionals in your company will increase in 3-5 years?
   a) Yes
   b) No

6. Which of the cyber security skills are more important for your organization at present?
   a) Network security

b) Cryptography
c) Secure coding
d) Penetration testing
e) Digital forensics
f) Business continuity management
g) Audit
h) Legal aspects
i) Other:

7. Which of the cyber security skills do you expect will be more important for your organization in 3-5 years?
   a) Network security
   b) Cryptography
   c) Secure coding
   d) Penetration testing
   e) Digital forensics
   f) Business continuity management
   g) Audit
   h) Legal issues
   i) Other:

8. Cyber security professionals with which CS skills do you consider to be difficult to find in Georgia at the present time?
   a) Network security
   b) Cryptography
   c) Secure coding
   d) Penetration testing
   e) Digital forensics
   f) Business continuity management
   g) Audit
   h) Legal issues
   i) Other:

9. Which cyber security skills are not available for training/education in Georgia at the present time?

a) Network security
b) Cryptology
c) Secure coding
d) Penetration testing
e) Digital forensics
f) Business continuity management
g) Audit
h) Legal aspects
i) Other:

10. Which option(s) are considered to raise employees' cyber security proficiency at your company?
    a) Internal trainings (trainings within our company)
    b) External trainings within Georgia
    c) External trainings abroad
    d) Higher education programme
    e) Not considered at all
    f) Other:

11. Which option(s) would most likely be considered to raise employees' cyber security proficiency at your company in 3-5 years?
    g) Internal trainings (trainings within our company)
    a) External trainings within Georgia
    b) External trainings abroad
    c) Higher education programme
    d) Other:

12. Has your company addressed any of the education institutions to raise qualification of its cyber security personnel?
    a) No
    b) Yes
    c) Do not know

13. Which option(s) are considered to fill a cyber security professional need at your company?

a) IT field employee is assigned to ensure cyber security as well

b) Train/educate current IT professionals

c) Accepting a new employee with Cyber Security Master degree

d) Accepting IT-field graduate

e) Hunting for experienced CS professional

f) Other:

14. How do you think your company can support the master programme's development in Georgia?

    a) Providing advisory role on cyber security skills initiatives

    b) Working with universities to develop/deliver course content

    c) Employing students on a long-term or short-term internships

    d) Employing students on a long-term or short-term paid internships

    e) Sponsoring master student(s)

    f) Other:

15. Should the Cyber security master programme have multidisciplinary approach or should focus on one field?

    a) Focus on one field

    b) Take multidisciplinary approach

16. On which of the directions should the programme focus (choose one or more from the list taking into account your answer to the previous question)?

    a) Network security

    b) Cryptography

    c) Secure coding

    d) Penetration testing

    e) Digital forensics

    f) Business continuity management

    g) Audit

    h) Legal aspects

    i) Other:

17. How do you think where should the CS programme be established?

    a) State education institution

b) Private education institution

c) Military education institution

18. Please select the criteria the academic staff should meet:

a) Experienced IT professional being employed in cyber security field

b) Experienced IT professional with higher education in IT field and being employed in cyber security field

c) Other:

19. Should the programme offer employment opportunities to graduate students?

a) Yes

b) No

20. Should the programme provide internships?

a) Yes

b) No

21. Should the programme include extracurricular activities (ex. visiting companies on site and observing and/or participating in the actual task accomplishment processes)?

a) Yes

b) No

22. Choose one or more criteria you think is important for accepting a student at the CS programme (in addition to the results of the unified national exams)?

a) Higher education in IT field; at least two years of experience in IT field

b) Higher education in IT field; experience is not required

c) Higher education in non-IT field is acceptable; at least two years of experience in IT field

d) Other:

**3. Demographic information:**

1. Please indicate your age from the drop-down list:
    a) 18 – 24
    b) 25 – 34
    c) 35 – 44
    d) 45 – 54
    e) 55 – 64
    f) 64 +

2. Please indicate your gender from the drop-down list:
    a) male
    b) female

3. Please indicate how long have you been employed in IT field:
    a) <= 1 year
    b) 1 year <= 2 years
    c) 2 years <= 5 years
    d) 5 years <=10 years
    e) other:

4. Please indicate how long have you been employed within your company IT filed:
    a) <= 1 year
    b) 1year <= 2 years
    c) 2 years <= 5 years
    d) 5 years <=10 years
    e) other:

5. Please indicate your current position:
    a) Executive / C-level
    b) Director
    c) Manager
    d) System Administrator
    e) Network Administrator
    f) Technician
    g) Other:

6. Contact information (not compulsory):

**4. Closing section:**

You can add questions, comments or remarks in the field below or address Sophio Sakhokia to the following email: sophio.sakhokia@ttu.ee

Thank you for your participation!

# Appendix 4 - Questionnaire for public and private education institutions

## 2. Introduction:

Hello and thank you for your participation in the survey in advance!

The following questionnaire is a part of the master thesis aimed to develop a cyber security master programme for Georgia.

The questionnaire is targeted for Information Technology field academic staff at public and private education institutions.

The questionnaire consists of 22 questions: 16 of them are related to the development of cyber security master programme in Georgia, 6 questions cover a demographic part. You can either choose answer(s) from suggested options and/or provide your own suggestion. The overall process will take around 10 minutes. The format of the questionnaire ensures confidentiality.

In case of questions or comments please contact Sophio Sakhokia: sophio.sakhokia@ttu.ee

## 2. Questionnaire

Please fill the fields below.

1. Which of the cyber security skills do you think are in high demand in Georgia at present?
   a) Network security
   b) Cryptography
   c) Secure coding

d) Penetration testing

e) Digital forensics

f) Business continuity management

g) Audit

h) Legal aspects

i) Other:

2. Which of the cyber security skills do you think will be in high demand in Georgia in 3-5 years?

   a) Network security

   b) Cryptography

   c) Secure coding

   d) Penetration testing

   e) Digital forensics

   f) Business continuity management

   g) Audit

   h) Legal aspects

   i) Other:

3. Cyber security professionals with which cyber security skills do you consider to be difficult to find in Georgia at the present time?

   a) Network security

   b) Cryptography

   c) Secure coding

   d) Penetration testing

   e) Digital forensics

   f) Business continuity management

   g) Audit

   h) Legal aspects

   i) Other:

4. Which cyber security skills are not available for training/education in Georgia at the present time?

   a) Network security

   b) Cryptography

c) Secure coding

d) Penetration testing

e) Digital forensics

f) Business continuity management

g) Audit

h) Legal aspects

i) Other:

5. Please indicate if any of the directions are taught at your education institution:

   a) Network security

   b) Cryptography

   c) Secure coding

   d) Penetration testing

   e) Digital forensics

   f) Business continuity management

   g) Audit

   h) Legal aspects

   i) Other:

6. Has a company requested from your institution to conduct a cyber security training to raise its employees' cyber security qualification?

   a) Yes

   b) No

7. Has a company expressed interest in higher education programme in cyber security at your education institution?

   c) Yes

   d) No

8. How do you think a company can support development of the master programme in Georgia?

   a) Providing advisory role on cyber security skills initiatives

   b) Working with universities to develop/deliver course content

   c) Employing students on a long-term or short-term internships

   d) Employing students on a long-term or short-term paid internships

e) Sponsoring master student(s)

f) Other:

9. Should the Cyber security master programme have multidisciplinary approach or should focus on one field?

   a) Focus on one field

   b) Take multidisciplinary approach

10. On which of the directions should the programme focus (choose one or more from the list taking into account your answer to the previous question)?

   a) Network security

   b) Cryptography

   c) Secure coding

   d) Penetration testing

   e) Digital forensics

   f) Business continuity management

   g) Audit

   h) Legal aspects

   i) Other:

11. How do you think where should the CS programme be established?

   a) State education institution

   b) Private education institution

   c) Military education institution

12. Please select the criteria the academic staff should meet:

   a) Experienced IT professional being employed in cyber security field

   b) Experienced IT professional with higher education in IT field and being employed in cyber security field

   c) Other:

13. Should the programme offer employment opportunities to graduate students?

   a) Yes

   b) No

14. Should the programme provide internships?

a) Yes

b) No

15. Should the programme include extracurricular activities (ex. visiting companies on site and observing and/or participating in the actual task accomplishment processes)?

a) Yes

b) No

16. Choose one or more criteria you think is important for accepting a student at the CS programme (in addition to the results of the unified national exams)?

a) Higher education in IT field; at least two years of experience in IT field

b) Higher education in IT field; experience is not required

c) Higher education in non-IT field is acceptable; at least two years of experience in IT field

d) Other:

**3. Demographic information:**

1. Please indicate your age from the drop-down list:

a) 18 – 24

b) 25 – 34

c) 35 – 44

d) 45 – 54

e) 55 – 64

f) 64 +

2. Please indicate your gender from the drop-down list:

a) male

b) female

3. Please indicate how long have you been employed in IT field:

a) <= 1 year

b) 1 year <= 2 years

c) 2 years <= 5 years

d) 5 years <=10 years

e) other:

4. Please indicate how long have you been employed within your company IT filed:

a) <= 1 year

b) 1year <= 2 years

c) 2 years <= 5 years

d) 5 years <=10 years

e) other:

5. Please indicate your current position:

a) Executive / C-level

b) Director

c) Manager

d) System Administrator

e) Network Administrator

f) Technician

g) Other:

6. Contact information (not compulsory):

**4. Closing section:**

You can add questions, comments or remarks in the field below or address Sophio Sakhokia to the following email: Sophio.sakhokia@ttu.ee

Thank you for your participation!