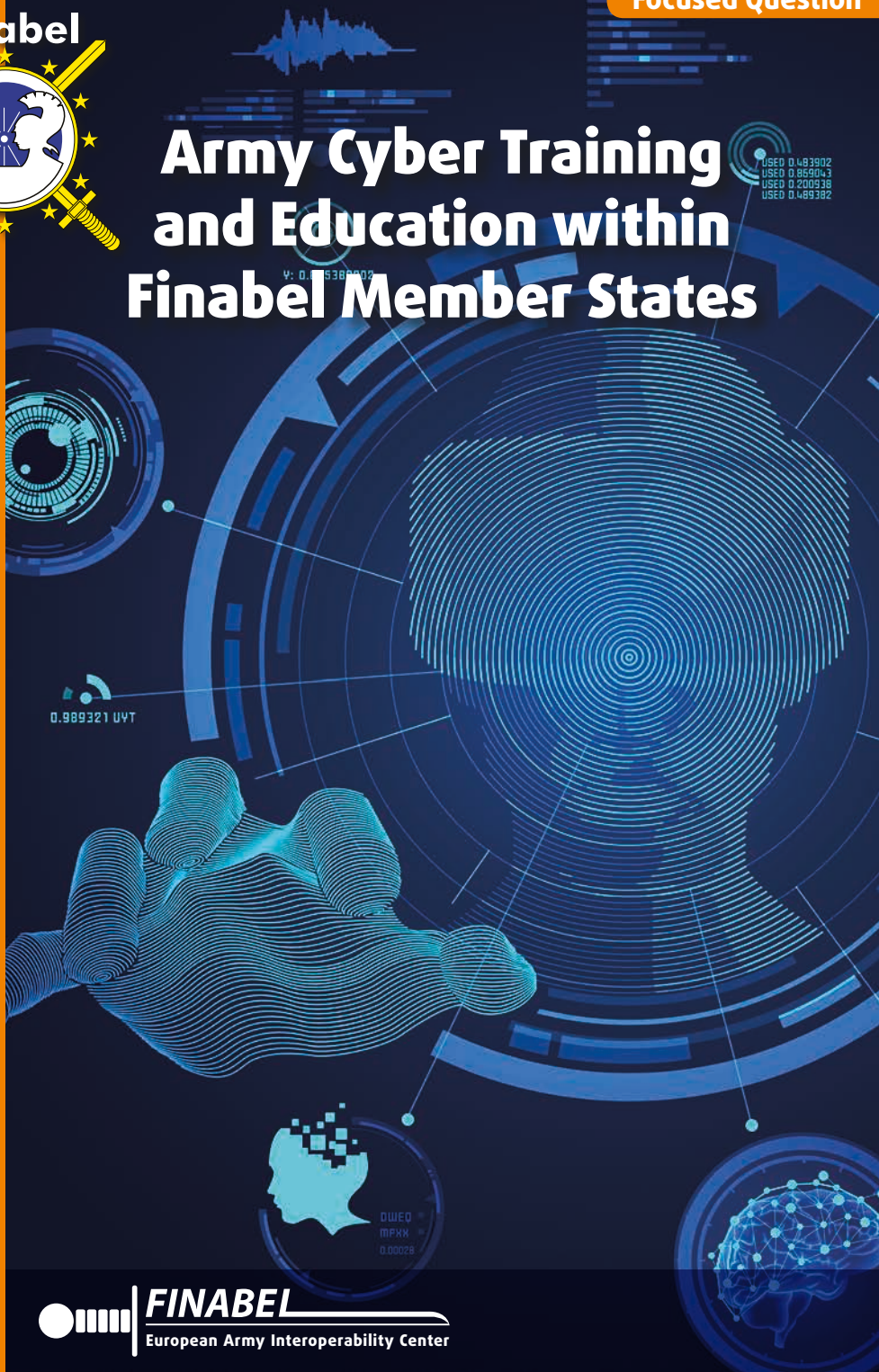
Finabel

Focused Question

Army Cyber Training and Education within Finabel Member States



AN EXPERTISE FORUM CONTRIBUTING TO EUROPEAN ARMIES INTEROPERABILITY SINCE 1953

FINABEL
European Army Interoperability Center

This focused question is a document that gives an initial reflection on the Finabel annual theme 2018-2019. The content is not reflecting the positions of the member states, but consists of elements that can initiate and feed the discussions and analyses in the domain of the theme. It was drafted by the Permanent Secretariat and is supported by the organization.

INTRODUCTION

The cyber sector has become increasingly important for military planning over the past decade. Cyber warfare is a rising trend at the international level, and the threat of potential attacks on military and governmental networks, as well as business infrastructures, is more pressing than ever. With the rapid evolution of the cyber field, relevant training and awareness of armed forces needs to be increased at the national and European level. Yet, there is still plenty of initiatives to be taken on both levels. As European Parliament's rapporteur Urmas Paet stated in June 2018, "*cyber defense remains a core competence of the member states, but due to the borderless nature of cyberspace, it is impossible for one state to tackle the threats and challenges alone.*"

According to the European Defence Agency (EDA), "*cyberspace is understood as the fifth domain of warfare equally critical to military operations as land, sea, air, and space*". European armies are now increasingly reliant on cyberspace, for achieving their military defence and security missions.

In February 2013, the European Union tackled this issue with the release of the *Cyber Security Strategy for the European Union*, endorsed by the Council in June 2013. EU cyber defence future projects and formations have to address all aspects of capability development including leadership, organisation, personnel, doctrine, training, technology, infrastructure, logistic and interoperability.

In terms of common European training in the field of cyber defence, the EDA and the European Security and Defence College (ESDC) have launched various training projects, to meet the needs of the European Member States. The EDA focused on a platform for Cyber Defence Training and Exercise, which included a computer simulation for cyber security. Furthermore, the Agency will develop a new platform which shall facilitate all cyber trainings and exercises jointly undertaken by the Member States: the Cyber Defence Training & Exercises Coordination Platform (CD TEXP). The ESDC, the only European training provider for Common Security and Defence Policy (CSDP) operations, is increasing its role in pooling European training capacities in the cyber sector. Thanks to an evolving understanding of cyber threats, and subsequent training adapting to these, European countries are aiming to be at the forefront of cyber defence.

The NATO Cooperative Cyber Defence Centre of Excellence is a great success. The CoE is often solicited to provide training in the cyber domain. Due to the rather limited capacity of this CoE and the high demand for their expertise, they can only provide a small part of the necessary training.

The following paper highlights the current capabilities of European Armies for cyber defence training, in order to have a clear overview of training and education in a sector that has already proven to be pivotal.

All data and information were provided by Finabel's Member States at their discretion.

OVERVIEW OF THE VARIABLES AND ACRONYMS

This section of the research paper is intended to address the variables used in the explanatory table, which will determine the trainings and courses of Armed Forces employees regarding the cyber domain.

The independent variables represent Finabel's Member States.

The dependent variables show the different trainings provided by Finabel's Member States, and are explained as followed:

- Basic training: Basic Cyber Training/ Courses given during initial education after incorporation into the Army;
- Advanced training/course: Advanced cyber training course for the officer/ warrant officer (WO) or soldier during his career;
- Pre-mission cyber awareness training: Cyber training/course given to Land Forces personnel before deployment;
- Cyber expert level course: Course provided for those specializing in the cyber domain within the Land Forces;
- Extra-mouros training: Cyber training and courses provided by private stakeholders, joint services, or international organisations to Land Force personnel.

Furthermore, the following list of acronyms shall be used in this paper:

- CCDCOE: Cooperative Cyber Defence Centre of Excellence, is based in Tallinn, Estonia, which provides a hub of cyber defence expertise.
- CSDP: Common Security and Defence Policy
- EDA: European Defence Agency
- ESDC: European Security and Defence College
- MISP: Malware Information Sharing Platform
- NCO: Non-commissioned officers
- SI-CERT: Slovenian Computer Emergency Response Team, is the national cyber security response team based in Ljubljana, Slovenia.
- SME: Special Military Expert
- WO: Warrant officer

* *FI-Finland and RO-Romania are providing cyber trainings and courses to the Military Corps in Joint Command. Their national Army currently does not provide any type of cyber education on its own.*

** *CY-Cyprus and MT-Malta do not have any cyber capabilities on their own, however depending on the needs of the Land Forces, personnel can be sent abroad (to other EU countries) to complete a specific module on cyber training.*

EXPLANATORY TABLE

	BE	CY**	CZ	DE	EL	ES	FI*	FR	HR
Basic training	✓	✗	✗	✓	✗	✓	✗	✗	✗
Advanced training/course	✓	✗	✗	✗	✓	✓	✗	✓	✓
Pre-mission cyber awareness training	✓	✗	✓	✓	✓	✓	✗	✗	✗
Cyber expert level course	✓	✗	✗	✓	✓	✓	✗	✓	✓
Extra-mouros training	✓	✗	✓	✓	✓	✓	✗	✓	✓

HU	IT	LU	LV	MT**	NL	PL	PT	RO*	SE	SK	SI	UK
✗	✓	✓	✓	✗	✓	✓	✗	✗	✓	✗	✓	N/A
✗	✓	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	N/A
✓	✓	✓	✗	✗	✓	✗	✗	✗	✓	✓	✗	N/A
✗	✓	✓	✗	✗	✓	✓	✓	✗	✓	✗	✗	N/A
✗	✓	✓	✗	✗	✓	✗	✗	✗	✓	✗	✓	N/A

OVERVIEW OF CYBER TRAINING AND EDUCATION PER MEMBER STATES

BE-Belgium

The Belgian Army basic training is part of the Joint Individual Common Core Skills and provides an Awareness Training based on the CCDCOE's Course. It lasts for 1 to 3 hours and is available to all Land Forces personnel.

Their advanced cyber training course and their Expert level course are provided by the private sector, CCDCOE and other stakeholders and aims to deliver specific education in forensic, cyber intelligence, and operations to cyber experts, either to NCOs or Officers. This course tends to last between 5 to 15 days.

Before deployment, the Belgian Army personnel is required to attend a session of 1 to 2 days, where they are briefed again on the Basic Training, and updated on the specific threats coming from the environment of the deployment destination country.

Last but not least, Belgian Land Forces personnel can follow cyber courses outside the military sphere depending on their needs. Often in universities or international organisations (EDA, CCDCOE, etc.), modules can be undertaken by Senior NCOs and Officers.

CZ-Czech Republic

The Czech Land Forces proposes a short program on cyber hygiene, for soon to be deployed personnel. This one hour briefing states basic elements of the cyber domain. It is mandatory for all and provided by the Military Academy.

WO and Officers specializing in cyber can attend courses in outside organisations such as NATO schools or the CCDCOE.

A basic training on cyber during initial education will be established in 2019.

DE-Germany

Every year, army personnel in Germany need to complete a 2 hour basic cyber awareness e-training provided by the unit to all. Therefore, as this is a continuous process, its reach extends to an advanced level throughout the military career of Land Forces personnel.

The German military school provides a pre-mission cyber awareness regular course only for cyber security personnel (soldiers and officers). Similarly, Expert Level Courses and extra murros education is only available for cyber security personnel (soldiers and officers) in other European military schools or in civilian universities.

FR-France

Although there is no proper basic training in cyber defence, Army personnel receive information about cyber threats during their initial training provided by the Military Academy and school.

Before deployment, the French soldiers and officers are made aware of possible threats on social media by their Unit Commander.

The French Land Forces offer different advanced cyber courses during the WO's and officers' career given by the Military School or civilian universities. The course length differs from one day to a few weeks.

Cyber Experts and specialists can acquire a masters degree in the field, as well as extra-murros training provided by the civilian university.

HR-Croatia

Croatia, Finabel's latest Member State, is offering an advanced cyber training course to its Army soldiers and officers specialized in cyber. The course is provided by the J6 directorate every year and lasts one week. During this time, the course participants are being trained to detect cyber threats by using system handling and system securing.

HU-Hungary

Hungarian Land Forces require its troops to undertake a pre-deployment training before going on a mission. This training aims to increase cyber awareness, especially in relation to online identity of the deployed personnel. This briefing lasts one hour and is given by the system security officer.

IT-Italy

The Italian Land Forces, every six months offers a security awareness course provided by the barracks. This half-day training is mandatory for all as it explains the relevant threats in the cyber domain.

Before deployment, all Army personnel needs to follow a basic roots training on cyber (3-5 days) provided by the barracks. This training incorporates a security awareness course, for those who will serve on missions.

The Advanced Cyber Training Course and the Expert Level Course are both given by the Military Academy. The seminars can last from between one week to one year depending on the needs of the cyber officer/WO.

LU-Luxembourg

Starting next year, Luxembourg's Army plans to give a general introduction course to establish basic cyber hygiene to all its personnel for the duration of 3 hours. This class will be taught by the Public/Private Cyber Competence Centre.

Before deployment, all personnel deployed need to follow a reminder course provided by the cyber unit on cyber hygiene as well as a specific awareness training depending on the mission's environment.

The Expert Level courses provided by different EU Military Academies (most likely the French or the Dutch) are designed for Officers and can last between 1 week to 6 weeks. The subject may vary depending on the officer's specialisation (cyber operations, cyber defence, etc.).

According to the specific needs, Luxembourg's Land Forces can send its personnel to outside courses on risk management trainings and MISP.

LV-Latvia

Latvian Land Forces provide a basic training to all its personnel during initial incorporation.

NL-Netherlands

During the pre-military training, the Dutch Army personnel receive a basic awareness training on cyber security. This class is followed by an e-training.

Before deployment, all personnel is asked to complete the specific mission training during which a panel will be reserved for cyber awareness.

The Dutch Land Forces has one Expert Level Course on Cyber called "Cyber Opleiding Programma" which touches upon offensive,

defensive, and forensic topics. This course is designed for WO and Officers.

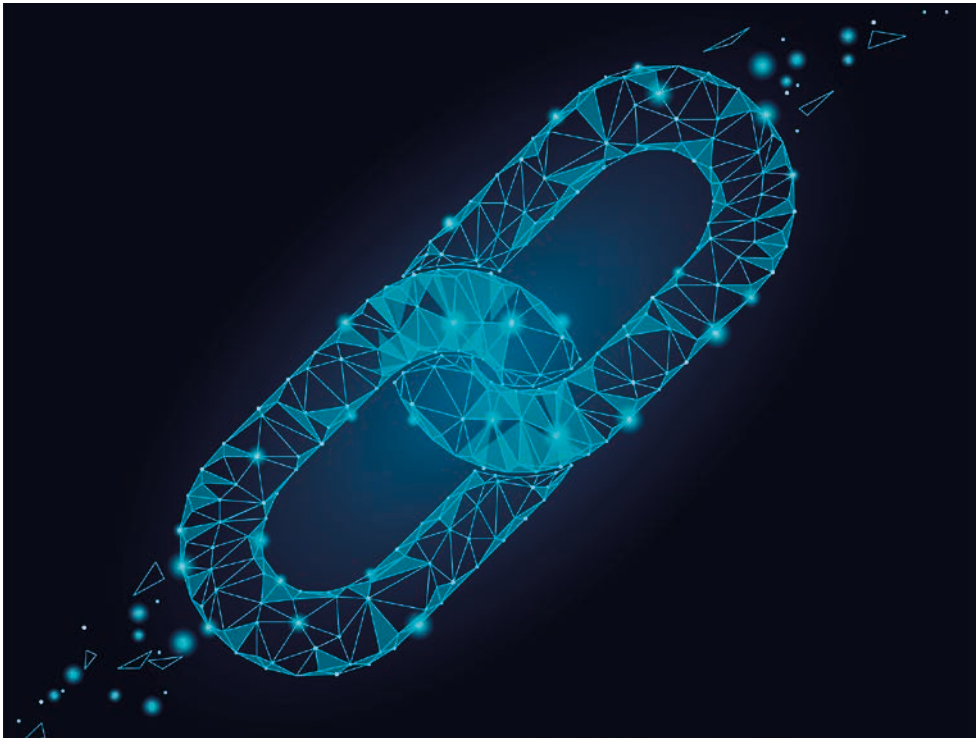
For additional training, the Dutch Army hires private companies (SANS, Deloitte, etc.) to enrich the knowledge of their personnel. These courses can either be seminars or e-trainings.

PL-Poland

The Polish Land Forces offers 3 different pre-entry basic cyber courses. The first one is available to all, and focuses on the security network environment. It is a regular course taking place over 12 days. The second regular course is designed for Cadet Officers, who are expected to become Officers. The classes can last to up to 88 hours/20 days. The third course is designed for soon to be NCOs and can last to up to 169 hours/ 40 days. These classes are provided by the Signal and Informatic Training Centre.

Furthermore, throughout the military career of personnel, the Polish Army provides 4 different types of advanced cyber training:

- A course on network environment security for professional soldiers, dedicated to communication, and information technology personnel corps. This regular course lasts for 7 days (10 hours lecture and 20 hours of laboratory) and it is provided by the Informatics Inspectorate – National Centre of Cryptology;



- A course on the administration of ITC networks and management of databases for professional soldiers of the personnel corps. This course lasts for 30 days (42 hours of lectures and 78 hours of laboratory) and it is provided by the Informatics Inspectorate - National Centre of Cryptology;
- A course on the use of information and communication systems and administration of networks. This course lasts for 30 days (54 hours of lectures and 66 hours of laboratory) and is provided by the National Centre of Cryptology, C2 Systems Inspectorate, the General Staff and the Informatics inspectorate;
- A course on the management of computer networks environment. This course lasts for 29 days (40 hours of lectures and 80 hours of laboratory) and is provided by the National Centre of Cryptology.

Regarding the Cyber Expert Level Course, the Polish Army offers two different versions. Both of them are designed for Cadet Officers and are provided by the National Centre of Cryptology. The first module consists of a Bachelor of Sciences (7 semesters) in Cryptology or Cybersecurity, with a specialization on cyber defence information or cryptographic systems. The second module consists of a Masters of Science (3 semesters) with a specialization in cybersecurity information or cryptographic systems.

PT-Portugal

The Portuguese Land Forces provide a regular Advanced Cyber Training course, for the duration of 2 weeks to security analyst officers, that takes place within the unit. They also provide a Cyber Expert Level course that takes place regularly for the duration of one month to security analyst officers, taking place at the training centre.

SE-Sweden

The Swedish Armed Forces and Unit offer an online basic cyber training course to its newly incorporated members as part of their initial education process. This training is aimed at all categories of the Army, and lasts up to one day to one week, depending on the module courses selected.

Advanced cyber training courses, and cyber awareness pre-mission training are also provided by training centres, the cyber sector, as well as public, and private universities, in a blended learning training type. These are open to all categories of the Land Forces personnel, the duration is dependant on their designated role, and to the specific tasks or missions they are/will be assigned to.

SME's can also benefit from Cyber Expert Level courses and extra muros training in civilian environments; provided by training centres, public, and private actors. This type of training is based on blended learning, with the duration depending on the relevant task.

SK-Slovakia

The Slovak Armed Forces currently provide cyber awareness training for 2 hours pre-mission TESSOC briefing for all its personnel, which takes place in the training centre.

SI-Slovenia

The Slovenian Army requires its personnel to follow an anual mandatory cyber awareness e-training. Furthermore, the Slovenian Armed Forces sends its personnel to different cyber courses through their career.

Officers can attend a course on cyber security studies at the European Centre for Security Studies – Marshall Centre.

NCO and Officers can attend trainings provided by the NATO school in Latina on cyber defence crypto custodian and computer science. These courses last for 3 weeks.

The National Guard of Colorado provides classes to NCO and Officers four times a year.

WO, NCO and officers can attend special courses focused on network security, cyber incident handling, and disaster response course organised by NATO school in Oberamergau.

A 6 month training, at a Civilian Cyber Expert Level is provided by SI-CERT. In addition, training for civilians, WO, NCO and officers is conducted in-house in a private training centre and provides special courses.

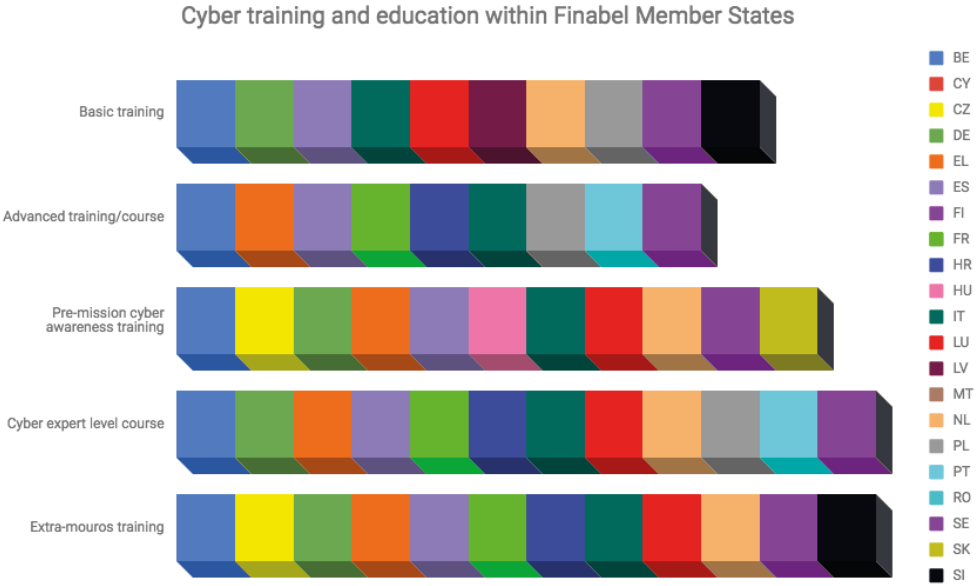
ANALYSIS OF DATA

The previous table provided an overview of the situation regarding cyber training and education within Finabel's Member States.

In this section, the data collected will be analysed to understand the advances of European Armies in this domain. Therefore, European Armies can position themselves and identify their strengths and weaknesses regarding the cyber domain. The following graph offers a detailed synopsis of the current situation:

Overall, the trend shows that Cyber Expert Level Courses as well Extra-mouros trainings in civilian universities or private companies are better implemented than any other type of cyber training.

Providing basic cyber training to entry personnel seems to have become a pressing concern for Member States which recognise the



increasing threat of cyber in the everyday life of Army personnel. Therefore, 10 countries (47,60%) have already established a training providing a Basic Cyber Course to all its personnel, increasing awareness in this domain.

Furthermore, the general trend shows that the least developed course in cyber for all Finabel Member States is the "Advanced training course during military career". Only 42,85% of the respondent countries have made this type of training available.

Pre-mission cyber awareness training must be developed further as deployed personnel should be aware of the cyber threats of the new environment as well as other permanent threats such as social media exposure. However only 52,38% of surveyed countries have established this type of training. Cyber awareness pre-deployment training shall be generalized within member states to reach a high security level of all deployed personnel.

The percentages used in the analysis above has been gathered from Finabel Member States and shows the balanced participation of Member States in each cyber training:

Countries delivering Basic training	47,60%
Countries delivering Advanced training/course	42,85%
Countries delivering Pre-mission cyber awareness training	52,38%
Countries delivering Cyber expert level course	57,14%
Countries delivering Extra-mouros training	57,14%

As in the previous analysis, the percentages used below has been gathered from Finabel's Member States and shows the repartition of the number of trainings delivered:

Countries delivering all the trainings	19%
Countries delivering four trainings	19%
Countries delivering three trainings	14,28%
Countries delivering two trainings	14,28%
Countries delivering one training	14,28%
Countries delivering none of the trainings	19%

As shown by the percentages, cyber trainings are fully delivered by only 19% of the Member States. Belgium, Spain, Italy and Sweden have already incorporated all types of training in their staff education. On the contrary, 19% of Finabel's Member States delegate their cyber training and education issues completely to independent structures from their Land Forces (Joint Commands, other Bodies of their Forces, other organisations or other countries).

Regarding these figures, we can deduce that 81% of these Armies (coming from 17 countries) are providing at least one of the trainings described above. Even if we need to keep in mind the differences within Land Force Organisations, cyber authorities and the different Chain of Command, this data highlights the balanced situation of the cyber trainings within Finabel's MS Armies.

If a real awareness about cyber issues has been implemented within most of the European Land Forces, in terms of international threats, the development of security skills among European Armies officers should be improved. More than a specialized required skill, cyber will obviously be a key aspect of tomorrows conflicts, at all levels. For this reason, stressing the incorporation of cyber security trainings as part of "Basic Trainings" must be one of the top priorities.

CONCLUSIONS AND RECOMMENDATIONS

The broad implication of the present research and results is the increasing importance of Army personnel education in different areas of cybersecurity. The results of this study provide a basis for understanding this field for both military personnel, and the layperson. This issue is critical for each sector of state security, and above all, it is clear that adequate training, and preparation, are the keys to success. One of the responses to this new threat is the national governments offering different types of trainings in their own or in other partner states, supported by the data provided from Finabel's Member States.

Another way in which states are trying to face this complex problem, is through national conferences in which they try to raise awareness for citizens and organisations. For example, the European Union started a campaign in October – CyberSecMonth with this exact goal in mind.

The cyber threats that we face today are constantly evolving, yet so are the measures against these threats, albeit at times seemingly too slow. The collected data of this report suggest that there is still a long way to go for many states and it shows visible inequalities of the cyber training level. The following recommendations would aid in this goal, being the first among many steps that will be needed.

Cybersecurity Awareness and Education

2018 has been a big year for cyber security. At the civilian level the Cybersecurity Act, which is in its final stages, will lead to regular EU-level cybersecurity exercises, support, and promote EU policy on cybersecurity certification. In general, emphasis has already been placed on creating visibility on cybersecurity issues and encouraging discussions across the EU on this vital topic. There is a need to spread awareness, and knowledge of European cybersecurity, among the EU Armed Forces, adopting a proactive approach for cybersecurity education and training for the forces.

Invest in Basic Training in Predeployment for Every Level

This would be a part of an overall proposal for an increase in budget for cybersecurity across the Armed Forces. There should be a common standard, reaching all areas of the forces, to avoid sectors being left behind and consequently resulting in weak links. Awareness should be raised for basic "cyber hygiene" at each level of the Armed Forces. This needs to become "business as usual". Emphasis must be placed on raising awareness at every level of the forces for basic security measures. This should be seen in the same manner road users are made aware of basic road safety rules (wearing your seatbelt etc.). Automatic reflexes must be encouraged and emphasised, such as protecting all devices physically (patches on webcam, regular upgrades…) and virtually

(firewall, encrypted data…), and these reflexes should come from education and information, at all levels, at every stage of the armed forces.

Encouraging Cooperation for Military Cybersecurity Training Forces

Emphasis should be placed on creating a shared cybersecurity standard and framework. A possible NATO and EU framework could be created and implemented for this purpose, which would concentrate on implementing shared standards. There should be a move from a reactive to a proactive stance. At the civilian level, one of PESCO's (Permanent Structured Cooperation) 17 projects is the EU Cyber Rapid Response Force. A similar initiative needs to be introduced for the armed forces in Europe, concentrating on cooperation, and allowing the ability to share "best practices" and "lessons learned".

Fostering Transparency

Concentration should be placed on defining and clarifying a shared language and categorisation framework. Emphasis could be placed on including language training during basic cybersecurity training for the forces so as to improve transparency and understanding within the forces. This can be achieved through shared definitions, and metrics.

Concentrating on Key Security Issues and Fields

Protecting infrastructure, especially the energy infrastructure, and the defence supply chain for example, needs to be prioritised. Capabilities need to be improved sector by sector. This should be achieved by providing training for personnel in each sector. For example, some systems in the manufacturing sector are running on outdated systems, that

are left vulnerable, as they cannot be adequately protected. Systems need to be updated and then protected. The recent hacking allegations related to the U.S. elections can be seen as a clear example of how Europe needs to improve its efforts for cybersecurity in the Armed Forces.

Military – Civilian cooperation in cyber awareness training programs

Since the capacities of the cyber training teams in the land forces are far too limited, the solution must be sought in a Mil-Civ cooperation. In the domain of cyber training, land forces need to look for close partnerships with civilian companies that can provide training for the military. This is a crucial part of building the necessary basic knowledge to create a cyber safe working environment.

E-learning integration at all levels

Awareness training is a continuous process and requires many resources. One way to reach the military relatively easily is to offer an E-learning module about cyber awareness. There is a need to further develop this path in a multinational environment. Countries need to collaborate more to exchange their E-learning modules and to permanently improve the quality of these training courses.

Creation of the Cyber field manual for the European Soldier

At the request of the land force commanders, Finabel is currently working on the realization of a cyber field manual for the European soldier. This manual will give an insight into threats that the cyber world entails in a very understandable and punctual way.

BIBLIOGRAPHY

- (2018), European Parliament News, "Cyber defence: MEPs call for better European cooperation".
  Accessed on the 25th of October 2018, available at:
  http://www.europarl.europa.eu/news/en/press-room/20180516IPR03618/cyber-defence-meps-call-for-better-european-cooperation
- (2017), European Defence Agency, "Cyber Defence".
  Accessed on the 25th of October 2018, available at:
  https://www.eda.europa.eu/what-we-do/activities/activities-search/cyber-defence
- (2018), European Cyber Security Month.
  Accessed on the 25th of October 2018, available at:
  https://cybersecuritymonth.eu/
- (2013), Li, J. J. & Daugherty, L. "Training Cyber Warriors" RAND Corporation, Santa Monica, Calif. ISBN-10 0-8330-8728-2
- (2013), European Commission, "Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions".
  Accessed on the 25th of October 2018, available at:
  http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

Created in 1953, the Finabel committee is the oldest military organisation for cooperation between European Armies: it was conceived as a forum for reflections, exchange studies, and proposals on common interest topics for the future of its members. Finabel, the only organisation at this level, strives at:

- Promoting interoperability and cooperation of armies, while seeking to bring together concepts, doctrines and procedures;
- Contributing to a common European understanding of land defence issues. Finabel focuses on doctrines, trainings, and the joint environment.

Finabel aims to be a multinational-, independent-, and apolitical actor for the European Armies of the EU Member States. The Finabel informal forum is based on consensus and equality of member states. Finabel favours fruitful contact among member states' officers and Chiefs of Staff in a spirit of open and mutual understanding via annual meetings.

Finabel contributes to reinforce interoperability among its member states in the framework of the North Atlantic Treaty Organisation (NATO), the EU, and *ad hoc* coalition; Finabel neither competes nor duplicates NATO or EU military structures but contributes to these organisations in its unique way. Initially focused on cooperation in armament's programmes, Finabel quickly shifted to the harmonisation of land doctrines. Consequently, before hoping to reach a shared capability approach and common equipment, a shared vision of force-engagement on the terrain should be obtained.

In the current setting, Finabel allows its member states to form Expert Task Groups for situations that require short-term solutions. In addition, Finabel is also a think tank that elaborates on current events concerning the operations of the land forces and provides comments by creating "Food for Thought papers" to address the topics. Finabel studies and Food for Thoughts are recommendations freely applied by its member, whose aim is to facilitate interoperability and improve the daily tasks of preparation, training, exercises, and engagement.

Quartier Reine Elisabeth
Rue d'Evere 1
B-1140 BRUSSELS

Tel: +32 (0)2 441 79 38
GSM: +32 (0)483 712 193
E-mail: info@finabel.org

You will find our studies at
www.finabel.org

Responsible publisher: Mario BLOKKEN - Finabel Permanent Secretariat - QRE - Rue d'Evere,1 - B-1140 Brussels - +32 (0)2 441 79 38