CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Cyber workforce recruitment and retention: an awareness assessment

Erwin Orye and Gunnar Faith-Ell

NATO CCDCOE

Tallinn 2020

1. Abstract

This paper focuses on how governmental organisations manage their required level of cybersecurity and the available cybersecurity workforce. It looks at the cyber workforce from the perspective of attracting new personnel by internal and external recruitment, retaining the current cyber workforce and how to improve the retention of employees.

A survey was carried out among supporting nations of the CCDCOE[1] to evaluate and understand how critical and how complicated it is for military or related organisations to guarantee the required capacity in specific cyber competences and to distil best practice.

This paper examines how the public sector is challenged by demand that exceeds availability in the labour market. It examines if military organisations have quantitative as well as qualitative measures to attract and maintain an effective cyber workforce. It analyses if existing policies for retention exist and gives best practices to avoid a potential lack of cybersecurity workforce.

The main topics revealed in the questionnaire were perceived desirability of movement and perceived ease ofmovement. A tablet that shows the factors that influence the cybersecurity workforce have been compiled in a table that can be a useful tool for nations to indicate where an organisation could improve on cyber workforce recruitment and retention and if there is a quantitative or qualitative shortage. In the future, this table could also be used to share information among different organisations or nations about the cyber workforce.

Main takeaways are (1) we know there's a cybersecurity skills gap that is only likely to increase in future (2) that you've been able to use surveyed responses to map what job factors are considered by cybersecurity colleagues (3) this may be a useful tool for those recruiting and retaining cyber security colleagues.

[1] The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary cyber defence hub; https://ccdcoe.org

2. Introduction

Generic research on the turnover of employees has existed for some time, including literature on how to retain employees in organisations or companies and what variables play a role. However, only a few studies have dealt with the cybersecurity workforce in the public sector and even fewer with military cybersecurity workforces.

A cybersecurity workforce shortage can be a problem for national security in an increasingly digitalised society. To quantify this issue, a survey of the current cyber workforce situation was conducted. This was not an easy task since the complexity of the cyber domain makes defining the required knowledge, skills, background knowledge and being able to keep up with the latest developments a challenge [1]. The definition of a cybersecurity specialist is not just defining a list of technical skills. In cybersecurity there are different skills required [2]: providing security, operating and maintaining, overseeing and governing, protecting and defending, analysing and collecting, and investigating IT-systems [3].

There is a gap between the number of cybersecurity professionals and the number needed to keep organisations safe [4][5]. In 2019 the International Information System Security Certification Consortium, (ISC)² published *Strategies for Building and Growing Strong Cybersecurity Teams* [6] which details the number of people working in cybersecurity in the United States (US) and stating that 561,000 specialists were needed. The document extrapolates this number to other areas in the world. It estimates is that Europe in 2019 lacked 291,000 cybersecurity professionals, almost double compared to 2018. The global shortage in the cyber workforce is estimated to be 4 million people. In the same study, 65% of organisations admitted they had a shortage of cybersecurity personnel. Although there is no direct correlation between governmental cybersecurity workforce issues and global ones, those figures indicate the shortage of cybersecurity specialist but give no granularity about which specific subarea of cybersecurity is most affected.

This paper seeks to raise awareness about this problem and to inventory the current number and quality of cyber workforces in the military. The combination of high demand for IT workers, an ageing military workforce and increased job mobility could lead to significant recruitment and retention challenges. This paper will determine if there is a lack of cybersecurity workforce or not, and if nations are taking specific measures assure their cyber missions.

A questionnaire consisting of 11 questions was used (see Appendix 1). Questions Q1.1 to Q1.4 deal with the structure of the organisation and who answered the questions to put their answers in perspective. The core of the questionnaire consisted of questions about retention (Q2.1, Q2.2, Q2.3, Q2.4, and Q2.8) and recruitment (Q2.5, Q2.6, and Q2.7). The final questions are about how the organisation estimates its future cyber workforce (Q2.9, Q2.10, and Q2.11). It was sent out on 19 September 2019 and the last answers were received by mid-December 2019. The questions were sent to cyber organisations of 25 nations which were NATO members or partner nations of the CCDCOE; 11 nations provided answers to the questionnaire. The reason why not all participants answered is unknown, but it could be that some nations consider revealing their cybersecurity capability, or lack thereof, as being sensitive information. For this reason, all the information gathered from the questionnaire has been anonymised and generalised.

The answers to each question have been used as input to draw generic conclusions and extract best practice in recruiting, maintaining and optimising the cyber workforce that organisations have put in place. A summary of the answers to the questionnaire is given in Chapter 4. Chapter 5 provides a discussion and in Chapter 6 the conclusions are presented.

3. Literature review

A lot of research has been done on incentives and motivating factors in the cybersecurity workforce and retention management. To address recruiting, it is necessary to understand how the current labour market works to gain a better understanding of the Millennials and Zoomers[2] that are now entering the workforce. There is little academic literature available on how to recruit people for public careers. Most private companies and private organisations have a human resources department, which most probably use common techniques, but even in the private sector, there is little transparency on this topic. Specifically for the cyber domain, only a few sources share best practice such as 'build, rather than buy cyber talent' [4].

Mitchell et al. [7] describe job embeddedness as a broad constellation of influences on employee retention. Two factors key in retaining personnel are identified: job satisfaction and the number of alternatives. Sacrificing is the opposite focus to job satisfaction and describes what people will lose if they leave their job. Other reasons given are changes in family conditions and no promotion despite expectations.

NIST[3] describes 7 activities in cybersecurity:

- Securely Provision: Conceptualises, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of a system and/or network development.
- Operate and Maintain: Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
- Oversee and Govern: Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
- Protect and Defend: Identifies, analyses, and mitigates threats to internal information technology (IT) systems and/or networks
- Analyse (AN): Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence
- Collect and Operate: Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
- Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

They are divided into speciality areas within each category.

Unfortunately, most of the surveys such as from Florentine [8] consider cybersecurity as a whole but define other skill sets that are becoming more integrated with cybersecurity such as data scientists and machine learning specialists.

3.1 Retention

Studies of employee turnover rate are not new. The term 'employee turnover rate' refers to the number of employees that have to be replaced within an organisation during a certain period. Leaving an

[2] Millennials, also known as Generation Y, are the demographic population early 1980s as starting birth years and the mid-1990s generation. Zoomers are referring to members of Generation Z, those born in the late 90s and early 2000s.

organisation includes voluntary resignation, dismissal and retirement. From the viewpoint of the organisation, this can be categorised as desirable or undesirable turnover. One of the earliest models describing turnover, already in 1958, is from J. March and H. Simon: 'Model of Motivation'[9] in Fig 1. It shows parameters that are relevant to determine the turnover ratio and highlights two major factors that influence people to move towards another position: perceived desirability of movement and, perceived ease of movement. In other words, the decision for an employee to change to a new position depends on the gain and the cost or how easy this desired change may be achieved.

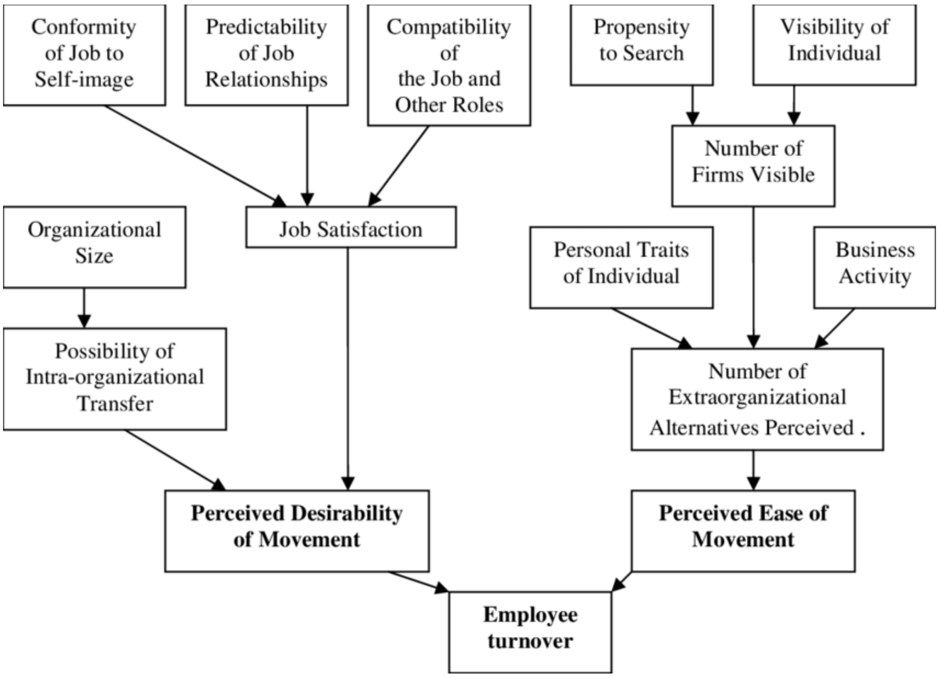
Conformity of Job to Self-image
Predictability of Job Relationships
Compatibility of the Job and Other Roles
Propensity to Search
Visibility of Individual
Number of Firms Visible
Organizational Size
Job Satisfaction
Personal Traits of Individual
Business Activity
Possibility of Intra-organizational Transfer
Number of Extraorganizational Alternatives Perceived .
Perceived Desirability of Movement
Perceived Ease of Movement
Employee turnover

Fig 1: March & Simon's model of motivation-1958 [9]

Financial compensation is often not the primary motivator for changing to a new position or remaining in the current one, at least not over a certain salary level [10]. Monetary incentives may be seen as a short-term solution and non-monetary as a long-term solution. Non-monetary incentives could be an improvement of knowledge, contribution to the organisation's success, (internal) recognition, job security, interaction with colleagues, and the work environment.

Thomas described four intrinsic rewards that drive employee engagement [11]:

- Meaningfulness: to accomplish something of real value.
- Choice: the ability to use the best judgement to accomplish the work.
- Competence: satisfaction and pride in how well the work was performed.
- Progress: encouragement in that the effort to accomplish something and move forward.

A 2009 study analysing almost 25,000 responses from the leisure and hospitality industry [12] revealed that advancement opportunities and organisational prestige were the most common reasons for high-performers to stay while extrinsic rewards were the more common reason among low performers.

Rand Corporation studies specific to cybersecurity[13][14] have indicated that financial benefit was not the only practice used to retain employees in the public sector. Being offered a median salary combined with challenging work generates a strong bond between employee, organisation and mission.

Opportunities for better pay (most relevant for wages that are under a certain threshold), poor promotion prospects and the perception of inequitable pay are the three top reasons for leaving a job [15]. Although not academically reviewed, some bloggers have come up with tips to reduce turnover [16] such as basic ideas of setting the correct expectations for the employee and showing appreciation for flexible work schemes and rewards systems.

Each loss of an employee costs a private company between 90% and 200% of their annual salary. The cost of training a new employee is estimated at 50% to 60% of a full year's wages [17]. Governmental institutions do not calculate financial gain, they focus on performance.

The company Towers Watson showed in a study that an average of 35% of the employees could be categorised as engaged and 26% disengaged [15]. The engaged group is characterised by a strong relationship between job contribution and the organisation's mission accomplishment. The disengaged group lacks pride in working for their employer, do not believe in the company and its goals, feels underequipped to effectively perform their jobs or have a work-life imbalance. Disengaged employees are more than twice as likely to leave their position as engaged ones. There is also a strong link between worker exhaustion and disengagement which in turn is connected to negative retention [18].

According to studies from Thomas in 2009 [11] and Mitchell et al. in 2001 [7] a recurring theme is the hypothesis that a lack of resources in the organisation could lead to overwork which in turn could make more people leave.

3.2 Recrutement

People are getting more and more embedded in information technology. The younger people are, the more they seem to be entangled with it. They are using IT for gaming, digital media for school, and social media as an essential means of communication. This should lead to a good base to satisfy the demand for a cyber workforce in the long run, however, this does not implies that the young generations realise the security issues that come with this technology or are interested to become cybersecurity specialists.

Diversity across recruitment is a key area of focus in a wider (cyber) skills gap discourse. To give the example of gender, one current estimate states that about less than 10% of the cyber security workforce worldwide are women[21]. Literature exists about the lack of diversity across race[22] and age[23] across the cybersecurity domain. While a key area of cyber capability building, both the causes of, and potential solutions to, a lack of diversity in the workplace were considered out of scope of the questionaire. This paper therefore does not include findings on the topic of diversity and inclusion.

4. Analysis of the answers to the questionnaire

The study aimed to qualitatively measure the current status in member states and therefore this report functions as a starting point for discussion among nations about this topic.

The first four questions of the survey were intentionally put to calibrate the questionnaire and analyse if the answers were coming from cybersecurity specialists, a human resources perspective or something else. According to those self-assessment questions, all responders have a good knowledge of their cyber organisations. Most of the organisations have the task to ensure cybersecurity and cyber defence in their mission. Some of them are CERTs, defending against cyber attacks, while others also include support to operations or responding to cyber aggression. Altogether, the organisations that answered the questionnaire cover a broad span of tasks within cybersecurity including monitoring, advising, providing support, defending, forensics, reverse engineering of malware, crypto management, penetration testing, intel gathering, responsive operations, education and representation in international forums.

4.1 Recruitment of employees

For recruiting purposes, some organisations use internships or select candidates through cyber challenges. Recruiting through cyber challenges has in at least one organisation resulted in the acquisition of competencies they did not have before. The drawback of this solution is that interns require a lot of coaching. Those organisations which implemented a cyber internship have found it beneficial to recruitment. One organisation mentioned that they face legal problems because of security clearances.

Some organisations use military personnel with a basic ICT background for entry-level positions, but one organisation said that a minimum of 3 to 6 months of training is necessary.

Organisations are optimising where and how to advertise to attract new employees. One organisation reported that they only recruit internally and another organisation recruits from the technical military academy. A few answered that they have no specific initiatives. There are sometimes legal restrictions on civil personnel in military positions. Some organisations use different job descriptions for civilian and military positions to be able to hire civilian personnel.

About half the answers indicate that organisations are not working on improving the recruiting process or have not made any improvements recently. The remaining organisations are active and participate at careers days, organise cyber challenges, advertise for staff with specific skill sets, participate in conferences and use social media [19] to reach their target audience.

Two of the organisations use the principles of the National Initiative for Cybersecurity Education (NICE) framework by NIST [3] to identify the skills needed for each position.

Organisations also focus on soft skills such as the ability to work in a team. One organisation distinguishes mandatory and desirable qualifications and claims it has a positive effect on finding more candidates. Some organisations do not have entry-level requirements. Several organisations use the reserve forces to work in the cyber domain, but not all nations have a cyber reserve force.

Some have plans to train conscripts in the cyber domain, and two organisations in our pool have started with this approach already.

A very specific approach is that of Estonia that has a cyber defence league which is a reserve force and volunteers from industry, academia and the military that can give support to the nation when needed.

Consultants could be a good complement to employees, especially in areas where there is limited knowledge within the organisation or for areas under fast development. Correctly used, they could bring in new knowledge, assist where the organisation lacks resources and develop the organisation, its processes and tools. Several organisations use consultants for specific tasks such as software or technology development, but not in cybersecurity functions. Hiring consultants may or may not be an achievable option due to the available budget and the global lack of resources in this field. Security clearance and procurement procedures might take quite some time and need a lot of administration and this may be conceived as a hurdle for the potential workforce.

4.2 Retention of employees

The most cited answers to the questionnaire on motivation for staying at an organisation were (Q2.1):

1. Education and exercises: national and even abroad;
2. Serving the nation and, warrant of peace
3. Financial compensation: although not easily adapted due to state regulations, some nations manage to set a higher salary for cybersecurity personnel;
4. Job security and stability of income;
5. Career options and professional development path;
6. Prestige and recognition;
7. Job satisfaction
8. Challenging work: specific laws are applicable for military, which allow for challenging military or intelligence tasks. One nation answered that offering the possibility to do cyber operations is a motivator;
9. Room for own initiatives.
10. Flexible work-hours, the possibility for working from home and number of leave days;
11. Access to state-of-the-art equipment and software.

Education and training are used to develop employees within their area of competence and thereby assuring that an organisation can achieve its goals. Training is also used to create a common understanding of processes and it facilitates the ability to move people to new positions within the organisation. Most organisations have a roadmap for training with training objectives and an education plan including a budget to attend conferences, courses, and workshops. Some organisations confirm that they are considering improvements to their roadmap.

The NICE framework [3] was mentioned by two organisations for establishing a comprehensive training plan and setting up a specific roadmap for training.

Since knowledge gain is considered an important motivation for employees staying within a public sector organisation, and in some way as a complement the financial benefits that are, a lot of organisations invest in it.

Knowledge gain has been implemented in different ways:

- Courses
- E-learning
- Conferences
- Table-top exercises
- Cyber exercises
- Training sessions
- Seminars

Almost all the organisations support on-the-job studying, even during office hours, as long as it is within the work area. A few nations have a legal framework that regulates this. Most organisations cover the cost for the studies and allow leave for preparing exams. One organisation mentioned the requirement to take courses is that the individual can show that the regular work is done. A couple of organisations have not implemented any support programme for studies.

Most of the organisations which have a programme for sponsoring studies use some kind of agreement for the employees to stay for a fixed period after the course. The agreement depends on how much time is spent and the cost of the course. Usually, an employee can buy themself out from the agreement. One organisation said that it does not have any financial compensation agreements, since this could lead to a negative attitude.

None of the organisations has chosen to locate their workplaces in places where there is more availability of a cyber workforce such as next to universities or research institutes. However, some are already located in large cities.

Some organisations allow staff to work from home under certain conditions or provide options to work in a different location to the normal place of work, but where they can guarantee the confidentiality requirements and the availability of tools.

Some organisations provide flexible working hours.

Career path planning varies between organisations: some do not have formal career paths and for others, staff have to apply for open positions. One organisation explained that they have a mandatory rotation after three to five years for military personnel. Promotion to management positions from technical seems limited. Military personnel attend more exercises than their civilian colleagues. One organisation offers a full career path, starting with an assignment at a post requiring IT and crypto knowledge before being transferred to a cybersecurity unit and finally joining a joint cyber unit. Civilian staff are mostly used for expertise. There are opportunities such as studying at graduate school or being seconded to other authorities to acquire advanced speciality.

The organisations cannot compete with private-sector wages. Mostly this is due to regulations for government employees. This has not hindered some of the organisations in experimenting with economic compensation. No answer shows discrimination between civil and military personnel but also no answer explains what the results of the economic compensation are.

Most organisations have introduced modern or even state-of-the-art hard- and software which is well received by employees. This improves work morale and productivity. Most of the organisations confirm they have modern facilities or plan to move to a modern facility within a few years.

Half of the organisations have facilities adapted for workers with physical limitations and treat their applications with no discrimination. One has used the recruitment of workers with physical limitations and one organisation is working on possible recruitment of people with Asperger's syndrome. There were no specific answers on the results of those initiatives.

The most relevant answers to the questionnaire (Q2.2) for leaving an organisation where:

1. Financial compensation (financial incentives are too low);
2. Regulations for the military with compulsory rotations during a career;
3. Not being able to improve job position;
4. Not optimised work environment (e.g. no windows in the office);
5. Afraid of outsourcing certain services to the private sector; and
6. The slow evolution of the organisation.

Turnover rate (Q2.4) is divided into voluntary and involuntary turnover. Voluntary turnover is the free will of the individual or retirement. Involuntary turnover is when the individual has no choice in the matter.

This puts military rotation in the involuntary turnover group. The optimal turnover rate is difficult to compare because of the fluctuating answers in literature and online resources.

Many of the military cybersecurity organisations are expanding. Some organisations do not have an issue with people turnover as such, but they face difficulties to recruit new staff members. Military organisations with mandatory rotations have a high turnover rate for military staff as opposed to their civilian workers. The organisations try to not affect the mission even though a high turnover introduces delays and a necessity to prioritise between a multitude of tasks.

Most of the organisations invest a considerable amount in courses and certifications to aid retention, but a problem mentioned by organisations with a high turnover rate is that the training may not give enough return on investment. A lot of the required skill in cybersecurity takes a lot of courses and a long training time on the job and courses for new staff members of often up to two years.

The answers from question Q2.4 have been recalculated to a percentage per year and are shown in Fig 2. The preferred turnover rate varies a lot amongst organisations. High rates of turnover (green lines) are due to mandatory rotation of military staff. A couple of nations have not mentioned their preferred turnover rate and are therefore presented as being zero. The red line indicates the average desirable turnover ratio for the organisations. It does not take into account those nations that have a high turnover rate due to mandatory rotations of military staff nor those that have indicated zero turnover rates.

For reference, a report from 2013 [20] states that the technology sector worldwide has employee turnover (including both voluntary and involuntary departures) was averaging 18.5% in total and 11.3% for voluntary turnover. The latter one indicated by the orange line. Note that those figures depend a lot on nation, sector and source, but the organisation's desired voluntary turnover ratio for the cyber workforce is close to the average voluntary turnover ratio in the technology sector.

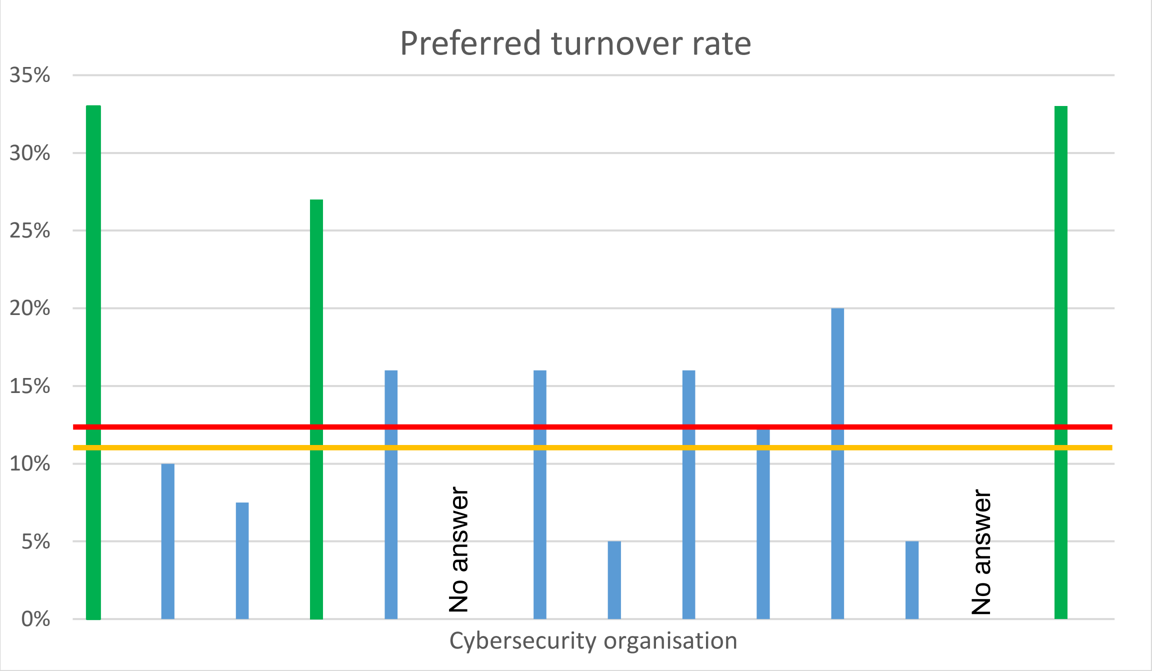

FIGURE 2: PREFERRED TURNOVER RATE IN CYBER ORGANISATIONS IN NATIONS (AVERAGE IN RED) COMPARED TO GLOBAL TECHNOLOGY VOLUNTARY TURNOVER RATE (AVERAGE IN ORANGE)

4.3 Mid-term and Long-term perspective

Opinion about the long-term trend for the recruitment of cyber specialists differs between organisations. Most have a problem in finding specialists. With more specialised education, they believe that this will improve. However, the need for cyber specialists is growing globally, which makes it harder to recruit specific profiles. Some of the organisations do not expect big changes in the mid-term, others expect that demand will grow more than availability.

Ongoing initiatives for recruiting:

1. Attending college events.
2. Organising cyber events and capture-the-flag competitions.
3. Cooperation with other governmental organisations to provide interdepartmental career solutions.
4. Investing in training opportunities.
5. Creating cyber education internally.
6. Adapting military academy courses.
7. Selecting cyber soldiers from conscripts based on tests.

The top steps to improve retention over the next five years are: improve salary, create A training programme including cyber events and conferences, and provide interesting career paths.

Suggestions from the organisations themselves:

- Separate management activities which are universal (can be done by non-specific trained staff) from expert activities.
- Become more flexible to retain cybersecurity experts by allowing remote work, flexible working hours, the possibility for talented experts to engage in exercises, and research activities.
- Engage in cooperation with partners from other departments.
- Investing in people is more important than technology.
- Limit the outsourcing of the core cyber functions to avoid becoming too dependant on industry.
- Attract more young people to cybersecurity from high schools, universities, etc.

Most needed talent:

The most wanted resources according to the questionnaire:

1. Forensics.
2. Software security.
3. Code analyst.
4. Malware analyst.
5. Operations.
6. Network security.

4.4 Additional national information

Most national surveys that are available are written in the national language. This may indicate that this topic is still considered as a national concern, although some nations have publicly available information about their cybersecurity workforce approach.

Examples of nations that have published their approach to retaining cyber personal:

The US [18]:

- Provide career progression and meaningful challenges.
- Offer training opportunities tied to retain and commitments.
- Retain qualified performers via compensation programmes.
- Identify and retain cyberspace leaders.
- Hire qualified cyber workforce personnel to make up for the lack of qualified cyber workforce personnel by US Cyber Command (authorised by Congress).
- Use bonuses for critical skills.
- Give US Cyber Command the authority to pay for moving expenses.
- Give US Cyber Command the authority to pay back student loans of newly requited civilians.
- Introduce a specific pay scale for civilians with highly sought-after skills that can boost up to an additional 40 per cent.

Estonia [24]:

- No real demand for physical ability, so disabled personnel could be hired for cyber tasks.
- Introduce a cyber track in the military service to attract young people.
- Have a cyber defence unit under the cyber defence league and as an organisation that unites elements of both a voluntary and military organisation. This means that volunteers such as employees that work in the public or private sector can temporarily take up roles in cybersecurity to support the community. The members of the cyber defence league include professors in cybersecurity and experienced people from private cybersecurity companies.

Sweden [25]:

- Convert soldiers to cyber specialists.
- The first pilot training of 30 cyber soldiers will be ready during 2020. They must fulfil all demands for conscripts but the physical demands could be adapted.

Denmark [26]:

- The report shows that demand for information security skills in the Danish labour market has tripled over the past decade.
- Demand has increased, both when measured absolutely and relatively in relation to the total labour demand.
- The rising trend is expected to continue in the coming years.
- The study of the labour market for information security skills is based on an analysis of 2.4 million job ads, a survey of 1,300 companies and 10 interviews.

5. Discussion

The main topics revealed in the questionnaire were perceived desirability of movement and perceived ease of movement [9]. The factors that influence the cybersecurity workforce have been compiled in the table below. This can be a useful tool for nations to indicate where an organisation could improve on cyber workforce recruitment and retention if there is a quantitative or qualitative shortage. In the future, this table could also be used to share information among different organisations or nations about the cyber workforce.

The absolute values in the table are not important, but the differences between different jobs or skillsets and the evolution over time of the values might be of great value to an organisation. As a disclaimer: an artificial and fictitious example is given below. The idea is that organisations modify the list, the weights of each factor and the scoring for each item. In the long term, it would be beneficial for organisations to define a set of factors, including the exact meaning of each, define the value of each parameter and compare those results.

Factor	Perceived desirability of movement	Weight	Perceived ease of movement	Weight
Interesting and challenging work	8/10	8	10/10	4
Career path	5/10	7	8/10	6
Prestige	7/10	6	3/10	5
Meaningfulness – to accomplish something of a real value	5/10	8	4/10	8
Ability to use the best judgement to accomplish the work	4/10	4	8/10	5
Satisfaction and pride in how well the work was performed	8/10	7	8/10	8
Progress – encouragement in that the effort to accomplish something and move forward[11]	3/10	5	3/10	4
The risk to get overloaded and/or exhausted	2/10	3	7/10	9
Monetary and other compensations	5/10	7	10/10	9
Working conditions (work from home, flex hours, …)	4/10	8	8/10	5
Workplace attractions and design (equipment available, ergonomics, …)	4/10	9	4/10	4

Non-financial benefits (number of days of leave, pension age, …)	7/10	8	8/10	6
Rotation terms	5/10	3	5/10	7
Non-cybersecurity related duties to perform (e.g. military training)	8/10	3	4/10	4

5.1 Recruitment

A topic emphasised strongly within the answers is recruiting. Recruiting is an area where organisations could learn from each other by, for example, using a common framework for cybersecurity workforce. Not all of them have a recruitment policy or plan. Some use social media, directed advertising, cyber challenges, attending fairs, cyber events, cyber competitions, collaborations with universities, selecting candidates from soldiers for basic tasks, using conscripts with an IT background or selecting people from the reserve forces. The organisations that state that they have a long-term recruitment planning are clearly saying that this gives advantages.

Specific military demands such as physical demands could also be lowered if they are not necessary for the job. This has been announced to acquire specific hard-to-find skillsets.

Trainees or on the job training is another option used by a few organisations where the best candidates may be recruited. This is a good complement to traditional recruitment, but it also takes a lot of resources from the organisation and it can take 3 to 6 months until the person can execute their tasks. The organisations that did this were positive about this approach.

In certain cases, the idea of having consultants to fill in specific gaps might look attractive, but it can be hard to find the right resources that are mostly globally scarce. Consults must also have some time to settle in the organisation before they can become productive and there might be issues with security clearances, so organisation are not looking at consultants for pure cybersecurity jobs.

5.2 Retention

Interesting and challenging work is a motivator provided that the salary is above a certain threshold. There are studies which measure the happiness of people related to their income, but actual values differ depending on where you live [27]. Career opportunities are another important factor. According to the answers to the questionnaire, organisations focus on keeping the work interesting and challenging.

The organisations' prestige is one common reason for high-performers to stay. This reportedly gives pride, makes the job meaningful and encourages working towards accomplishing something, which reduces turnover. However, lack of resources raises a risk that employees become overloaded and exhausted. This could lead to disengagement which is closely connected to retention.

Only a few of the organisations have a clear career path. This may be because moving towards a management position for an expert takes him away from the technical path, so it is not always desirable for the organisation to lose an expert and the specialist might not be interested in a management role. Introducing a technical career path is an option to reduce turnover.

Financial compensation is one of several incentives that could be used for attracting and keeping employees, but it is not always mentioned as the primary incentive. According to the answers on the questionnaire, the salaries in the cyber organisations for some organisations are higher than average state salaries but still lower than comparable positions in the private sector. None of the answers mentioned how big the difference is but some organisations see this as a hurdle. This mismatch is hard to reduce since most organisations must comply with state regulations on salaries. Changing legislation may not be an option since it can have unintended consequences for other parts of the state labour market and the internal structure of the organisation.

Most of the organisations use training as an alternative to monetary compensation to improve the skills of the employees and as a motivator to keep employees in the organisation. The budget for training and education is usually separated from the budget for salaries. One of the consequences is that well-educated and -trained personnel become more sought after by other organisations and the private sector. Some organisations try to bind attendees on expensive courses by an agreement to stay for a certain time after the education. One organisation explicitly said that it does not apply this procedure because it could lead to creating a negative attitude.

Workplace attraction could affect turnover, but most organisation state that they have decent facilities or are planning to have them shortly. A general rule is that organisations provide modern, sometimes state-of-the-art, equipment and software. Other incentives are patriotism and the stability of a governmental job. Some organisations mention flexible work hours and the possibility to work from home. Some of the military organisations claim that a rotation scheme is a motivation factor for the employee.

Scrutinizing turnover in a more structured way, an IT-organisation has an average voluntary turnover of 11.3% [20] due to people retiring, family reasons, or moving to another company or organisation. This is in line with the desired turnover rate of the organisations that have answered the questionnaire, not taking into account the compulsory turnovers that apply to most military personnel. Potentially, a specific cyber career path for military staff in cybersecurity could be considered. However, some turnover is natural for an organisation and also desirable since newcomers bring in new knowledge and revitalise the organisation[28]. Combining this with a swift handover of specific knowledge between leaving and arriving employees could raise the total level of competence in the organisation and increase its liveliness.

While a high turnover rate might be considered undesirable in cybersecurity as compared to less specialised job profiles, a certain turnover ratio is unavoidable. It appears that organisations that have a goal on the desired turnover ratio are better at optimising capacity planning in the cybersecurity workforce.

6. Conclusions

It is a difficult task to draw generic conclusions that encompass all the organisations that answered the questionnaire, but all are indicating that good cybersecurity workforce recruitment, maintenance and retention needs special attention. In some cases, specific incentives are needed or are expected to be needed in a near future to have the desired level of the cyber workforce. The number of answers to the questionnaire and the additional related documents indicates that the cybersecurity workforce is still considered as a national topic and, depending on the organisation, if this information can be shared or not.

The rather generic questions did not intend to solve all the potential issues correlated with the cybersecurity workforce, but it revealed that, by sharing more information, looking for synergies among organisations, sharing of best practices, finding a common terminology about specific cybersecurity skillsets and defining learning objectives the effect on cybersecurity personnel is positive. This would improve the current cybersecurity workforce situation and nations would be better prepared to cope with a potential future cybersecurity workforce gap. This sharing of information among allies, bilaterally or in a larger context such as NATO, will probably grow in importance since cyber is now the fifth domain for NATO.

The global lack of cybersecurity workforce will at some point affect the recruitment and retention problems in public organisations, if it has not been the case yet. In private companies, increased demand for this specific skill set will result in higher salaries and higher rates of voluntary turnover. In public organisations where wages are mostly defined by law and therefore not easily adapted, the most common ways to compensate for financial benefits are offering education or allowing a reduction in the quality of applicants on terms of, for example, cybersecurity knowledge level or physical fitness.

Practical measures that were revealed in the answers to the questionnaire are that some organisations are experimenting with using conscripts or reserve forces to strengthen their cyber workforce, support educational programmes by giving time off to their employees for study, and potentially paying for specific courses.

Accelerated promotions were not mentioned in the answers although it is known that in the military, as in other governmental institutions and the private sector, managers earn more than specialists. Due to obfuscation about wages in the private sector, it is not clear if some specific hard-to-find skillsets are paid more than management-level wages. However, there are exceptions in military organisations like physicians, professors, special forces and aircrew that have different pay rates, bonuses or promotion prospects. These practices were not mentioned for cybersecurity personnel among the answers. The long process of recruiting and the validation of security clearances might also influence the recruitment of the cybersecurity workforce.

The answers to the questionnaire indicated that organisations are working with the following parameters:

- An increase of knowledge for the individual;
- Possibility to acquire certifications;
- Job security;
- Work-family balance;
- Flexible working hours and home working;
- Comfortable working space;
- Promotion perspectives;
- Providing a challenging and rapidly changing work environment;
- Access to state-of-the-art hardware and software; and
- Providing work experiences that are only possible in a military context (specific laws applicable, access to specific information, exercises).

This research also revealed that cybersecurity workforce human resource management is still very much considered a national responsibility. By presenting this work, the authors are taking the first step to start nations discussing this topic at an international level. By doing so, they will better understand the current international situation and learn more from the best practices already put in place in some organisations.

References

[1] J. Dawson and R. Thomson, “The future cybersecurity workforce: Going beyond technical skills for successful cyber performance,” *Front. Psychol.*, vol. 9, no. JUN, p. Article 744, pg 1–12, 2018.

[2] W. Crumpler and J. A. Lewis, “The Cybersecurity Workforce Gap,” *Cent. Strateg. Int. Stud.*, no. July 2016, pp. 1–10, 2019.

[3] W. Newhouse, S. Keith, B. Scribner, and G. Witte, “National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework,” 2017.

[4] W. Markow, S. Bittle, and L. Pang-Cheng, “Recruiting Watchers for the Virtual Walls - The State of Cybersecurity Hiring,” *Burn. Glas. Technol.*, no. June, p. 26, 2019.

[5] A. Baldwin, H. J. Bax, and A. Cendrello, “Building a better working Europe,” 2018.

[6] (ISC)2, “Strategies for Building and Growing Strong Cybersecurity Teams,” 2019.

[7] T. R. Mitchell *et al.*, “Why People Stay : Using Job Embeddedness to Predict Voluntary Turnover Miriam Erez Published by : Academy of Management Stable URL : http://www.jstor.org/stable/3069391 REFERENCES Linked references are available on JSTOR for this article : You may need to,” *Acad. Manag. J.*, vol. 44, no. 6, pp. 1102–1121, 2001.

[8] F. Sharon, “12 most difficult IT roles to fill The importance of flexibility and employee experience,” *CIO*, 2020. [Online]. Available: https://www.cio.com/article/3279767/10-most-difficult-it-jobs-for-employers-to-fill.html#tk.cio_rs. [Accessed: 16-May-2020].

[9] J. G. March and H. A. Simon, “The Future of Humand Resource Management,” 1958.

[10] L. F. Hernandez and D. K. Johnson, “Designing Incentives for Marine Corps Cyber Workforce Retention,” 2014.

[11] K. Thomas, “The Four Intrinsic Rewards that Drive Employee Engagement,” 2009. [Online]. Available: https://iveybusinessjournal.com/publication/the-four-intrinsic-rewards-that-drive-employee-engagement/. [Accessed: 19-Feb-2020].

[12] J. P. Hausknecht, J. Rodda, and M. J. Howard, “Targeted employee retention: Performance-based and job-related differences in reported reasons for staying,” *Hum. Resour. Manage.*, vol. 48, no. 2, pp. 269–288, Mar. 2009.

[13] L. Schmidt *et al.*, *Cyber Practices: What can the U.S. Air Force learn from the commercial sector?* 2015.

[14] M. Libicki, D. Senty, and J. Pollak, *Hackers Wanted: An Examination of the Cybersecurity Labor Market*. 2018.

[15] Towers Watson, “Global Workforce Study,” 2012.

[16] M. E. Vidal, “How to Minimize Employee Turnover,” *Training Magazine Network*, 2019. [Online]. Available: https://trainingmag.com/how-minimize-employee-turnover/. [Accessed: 03-Jul-2020].

[17] C. Likavec, M. Olaya, and D. Wang, “Increased Turnover Risk & Other Trends in Workplace Engagement,” *TINYpulse*, 2016.

[18] W. E. Parker, “Cyber Workforce Retention,” 2016.

[19] K. K.-Y. Tan and A. Pang, “Assessing the Use of Social Media for Employee Engagement in the Singapore Military,” pp. 11–36, 2018.

[20] Radford EMEA, “Europe Leads All Regions for Workforce Stability,” 2014.

[21] W. R. Poster, “Cybersecurity needs women,” *Nature*, vol. 555, no. 7698, pp. 577–580, 2018.

[22] J. Reed and J. Acosta-Rubio, “Innovation through inclusion: The multicultural cybersecurity workforce An 2017 Global Information Security Workforce Study,” 2017.

[23] A. D. Rayome, “The world needs more cybersecurity pros, but millennials aren’t interested in the field,” *TechRepublic*, 2017. [Online]. Available: https://www.techrepublic.com/article/the-world-needs-more-cybersecurity-pros-but-millennials-arent-interested-in-the-field/.

[24] K. Kaska, A. Osula, and L. T. C. J. Stinissen, “The Cyber Defence Unit of the Estonian Defence

League Legal , Policy and Organisational Analysis," 2013.

[25] Swedish Defence Forces, "Försvarsmakten utbildar cybersoldater," 2019. [Online]. Available: https://www.forsvarsmakten.se/sv/aktuellt/2019/02/forsvarsmakten-utbildar-cybersoldater/. [Accessed: 19-Feb-2020].

[26] Danish Business and Industry Agency, National Agency for Digitization, Security Center for Cyber Security, and Ministry of Education and Research, "Arbejdsmarkedet for informationssikkerhedskompetencer i Danmark," 2019. [Online]. Available: https://erhvervsstyrelsen.dk/sites/default/files/2019-12/Arbejdsmarkedet for informationssikkerhedskompetencer i Danmark - Rapport.pdf.

[27] D. Kahneman and A. Deaton, "High income improves evaluation of life but not emotional well-being," *Proc. Natl. Acad. Sci. U. S. A.*, vol. 107, no. 38, pp. 16489–16493, 2010.

[28] J. A. Ashlock, "Why Turnover is a Good Thing for Your Company," *The Frontier Project*, 2015. [Online]. Available: https://www.inc.com/frontier-project/why-turnover-is-a-good-thing-for-your-company.html.

Appendix 1

Questionnaire about recruitment and retention of cyber workforce.

Questions about the organisation:

Q1.1: What is the mission and vision of your cyber organisation?

Q1.2: Give a short overview of your cyber organisation, their tasks and goals.

Q1.3: What is your task/position in the organisation?

Q1.4: Are you working full time in cybersecurity? If not, please specify.

Questionnaire:

Q2.1: What do you do to retain your cyber workforce in your organisation?

Q2.2: Why are your cyber experts leaving or staying in your organisation?

Q2.3: Explain how the current turnover rate in your cyber organisation affects your mission or future goals?

Q2.4: What is for your organisation the desirable turnover ratio?

Q2.5: Are there some areas where it is extra difficult to find the right competence (as well for junior level, senior level as for independent of the level)?

Technical

Q2.5.1 Network security

Q2.5.2 (Private- or pubic) cloud computing

Q2.5.3 Operating system security

Q2.5.4 Data storage security

Q2.5.5 Software security / code annalist

Q2.5.6 Software security developer

Q2.5.7 Forensics

Q2.5.8 Malware annalist

Q2.5.9 Cryptography

Q2.5.10 Operations

Q2.5.11 Monitoring

Operations

Q2.5.12 Legal advisor

Q2.5.13 User interface

Q2.5.14 Support

Management

Q2.5.15 Information technology manager

Q2.5.16 Information security manager

Q2.5.17 Security architect

Q2.6: There is a lot of research on how to recruit and maintain human resources. Some of the research has produced best practises. Which best practices have you been able to implement in your organisation?

Q2.7: How have you improved recruitment of new or education of existing personnel to supply the organisation with cyber expertise (e.g. training, courses, advertising, …)?

Q2.7.2: What are the results of those improvements?

Q2.8: In order to keep a healthy cyber organisation over time, have you implemented the following and what is the result?

Q2.8.1 Education for existing staff.

Q2.8.2 Locate or have satellite workplaces for your cyber organisation to locations where cyber workforce is more abundant? (e.g. close to universities, …).

Q2.8.3 Introduce a cyber specific career path for junior personnel (military as well as civilian). What is the difference between this path and the path for non-cyber specialists?

Q2.8.4 Introduce a specific cyber expertise career path for military and civilian specialists. What is the difference between this path and the path for non-cyber specialists?

Q2.8.5 Experiment with different compensations (financial, certifications, promotion, …). How does this compare to compensations for non-cyber specialists?

Q2.8.6 Improve work place attraction (e.g.: modern office, work equipment, …)?

Q2.8.7 Recruit workers with physical limitations (e.g.: modify physical requirements that are traditionally in place for military workforce, modify workspace, …)?

Q2.8.8 Lowered experience/education requirements from what the position demands?

Q2.8.9 Use civilians in military positions and/or vice versa?

Q2.8.10 Do you have a program to support employees with personal studies (study time during working hours, financial benefits, promotion, …)? If so, please explain those programs.

Q2.8.11 Have agreements with employees to stay during a specified period in exchange for education? If so, please specify what the agreement is.

Q2.8.12 Recruit from conscripts, soldiers, reserve force, … and train on the job?

Q2.8.13 Replace hard-to-find cyber expertise with outsourcing or consultants?

Q2.8.14 Outsource cyber responsibilities (e.g. monitoring, intrusion detection, …)? Having cybersecurity as a service? If so, please explain which areas.

Q2.8.15 Introduce a trainee program for students/conscripts/soldiers to become cybersecurity specialists? If so, please describe the program.

Q2.9: What do you expect to be the long-term trend for the recruitment of cyber specialists (for instance: will it be easier or harder to recruit them, is this the same for all types of cyber specialists)?

Q2.10: What is your organisation’s ambition to improve recruitment and retention of hard to find experts for the next five years (training programs, organisational changes, …)?

Q2.11: What would you propose to other nations to improve recruitment and retention of hard to find cyber experts?