



Special media of strategic cyber security

# Cyberwatch Finland

MAGAZINE 2023 / 2

## THE WAR IN UKRAINE IS CHANGING THE CYBER WORLD

IMPROVING  
DIGITAL SKILLS  
FOR A BETTER  
EUROPE

CYBER WAR  
THROUGH RUSSIAN  
LENS



Cybersecurity is built by small actions and management of large concepts



# CONTENT

2023/2



## Cyberwatch Magazine

Special media of  
strategic cyber security

PUBLISHER  
Cyberwatch Finland  
Nuijamiestentie 5 C  
04400 Helsinki  
[www.cyberwatchfinland.fi](http://www.cyberwatchfinland.fi)

THE EDITORIAL TEAM  
Editor-in-Chief  
Aapo Cederberg

Subeditor  
Elina Turunen  
[elina@cyberwatchfinland.fi](mailto:elina@cyberwatchfinland.fi)

LAYOUT  
Elina Turunen  
[elina@cyberwatchfinland.fi](mailto:elina@cyberwatchfinland.fi)

ILLUSTRATIONS  
Unsplash  
Pixabay  
Shutterstock

ISSN 2490-0753 (print)  
ISSN 2490-0761 (web)

PRINT HOUSE  
Scanseri Oy, Finland

**3**

The war in Ukraine is  
changing the cyber world

**8**

The war in Ukraine will not be  
resolved in cyberbattles

**16**

Cyber Citizen Skills – What is  
their importance and how  
should they be developed in  
the EU?

**4**

Improving digital skills for a  
better Europe

**11**

Cyber war through Russian  
lens

**19**

Education of the cyber  
security professionals

**6**

The Dark Side of the Web

**14**

Old and new elements of  
cybersecurity

**25**

Quarterly review

# THE WAR IN UKRAINE IS CHANGING THE CYBER WORLD

// Aapo Cederberg

Throughout the history, wars have changed the course of history and marked the beginning of a new era. The war in Ukraine is reshaping the current European security architecture. The security environment in Finland has permanently changed, and restoring good relations with Russia are difficult and will certainly require a long time to become normal. However, NATO membership has strengthened our national security, we are not alone, but a member of the defence alliance as well as part of the alliance's cyber defence.

These political trends are visible in the cyber world, although relatively little is said about the importance of war in Ukraine in the change of the cyber world. Already at this stage, at least three significant changes can be seen:

**1** Concepts of cyber strategies are becoming more and more offensive. Active cyber operations aim to weaken the cyber power of the state actors and cyber criminals.

**2** Cybercrime is divided into activities supporting or opposing Ukraine. The combination of economic and state goals is becoming more obvious.

**3** Cyber hacktivism has grown significantly. Cyberattacks can be used to quickly respond, for example, drone attacks or political decisions.

Due to these changes, globally, the number of cyberattacks has increased significantly and more clearly the most critical functions of all societies are targeted. As a form of attack, cyber sabotage has been emphasised, for example in the form of wiper attacks. Cyber espionage is an even more integral part of state intelligence and espionage activities, and thus it is an instrument of global politics. New data leaks and cyber espionage cases are coming to light at an accelerating pace. Trust in digital systems is wavering. Data protection and classification as well as innovative protection methods are highlighted.

The US's new cyber strategy emphasises the importance of the offensive activities to weaken the both the state actors' and cyber criminals' capacity, so-called cyber power. Mere protection and passive cyber defence are no longer enough. This is also reflected in NATO's cyber strategic thinking. Member countries are required to have more active cyber doctrines. The division between military and civilian cybersecurity are more and more blurred.

The changing security environment is also an opportunity. Cyber power is relatively cheap and within the reach of smaller countries, and thus a great opportunity for cybersecurity companies. The future of cybersecurity will be based on the latest innovations and know-how – the winners are those who realize the meaning of "smart cybersecurity". In this change, the old customs and operational models alone are no longer enough.

Countries and companies who invest in new cyber capabilities to respond to the changes and challenges of the rapidly evolving cyber world will be successful. The cyber world is not going back to the way it was before the war in Ukraine and the speed of change is increasing. Global politics guides the development of the cyber world even more clearly. Strategic cyber situational understanding and risk awareness are needed at different levels of operations, especially when developing national security arrangements.



AAPO CEDERBERG

Managing Director and  
Founder,  
Cyberwatch Finland





# IMPROVING DIGITAL SKILLS FOR A BETTER EUROPE

// Henna Virkkunen

**2023** is the European Year of Skills. Digital skills are at the very core of this theme year. Basic digital skills are widely in our daily lives, in both professional and private contexts. The use of such skills for studying, working, finding information, accessing online public services and communication is often indispensable. Yet, according to the EU Digital Economy and Society Index (DESI), an annual report published by the European Commission, 4 out of 10 adults and every third person who works in Europe lack basic digital skills. In addition, there is a low representation of women, as only 1 in 6 ICT specialists is a woman. The European Commission has set a target, whereby 70 percent of European adults have basic digital skills by 2025. In a similar vein, the Digital Decade target of the EU entails that 80 percent of the EU population would be equipped with at least basic digital skills by 2030. The lack of digital skills inevitably leaves part of the population outside of the reach of digital services and can lead to exposure to new kinds of threats. Furthermore, digital skills are the key to achieving a successful green and digital transition.

Strengthening digital and cybersecurity skills is at present a prominent theme in Europe. Finland should seize this opportunity, as we offer a multitude of different educational and training possibilities for both cybersecurity and digital skills. Finland ranked first in the DESI Index in 2022. Finland is one of the leading EU Member States in the development of digitalisation. As an example, many public services are provided online. Finland leads the EU

countries on the indicators tracking human capital and has already reached the Digital Decade target of 80 percent of the population with at least basic digital skills. The divide in digital skillsets, however, remains wide. Work remains to be done, in particular with increasing the percentage of ICT specialists in employment and the share of ICT graduates.

As a response to this challenge, the European Commission introduced two Council recommendations, which are non-binding acts targeted at the EU Member States, with the aim of supporting their education sector in providing quality training for digital skills.

The Council Recommendation on the key enabling factors for successful digital education and training calls for EU Member States to guarantee universal access to high-quality digital education and training, with a view of reducing the digital divide. The recommendation creates a framework for investment, governance and teacher training, with the objective of achieving inclusive digital education and training. It promotes a whole-of-government approach to digital training and wider cooperation with stakeholders, including the private sector.

The Council Recommendation on improving the provision of digital skills in education and training addresses all levels of education and training. It underlines that EU Member States should offer training on digital skills from an early educative stage through all levels of education and training, through the establishment of cumulative objectives and targeted interventions to specific groups that are perceived as hard to reach. Member States should support the development of digital skills for adults and adopt



strategies to tackle shortages in information technology professions. In addition to improving digital skills, Europe is in great need of knowledge and expertise in the field of cybersecurity. The EU is facing a shortage of cybersecurity professionals. In 2022, the need of cybersecurity workforce in the EU was estimated at 883 000 professionals. At the same time, the shortage of cybersecurity professionals in the EU fluctuated between 260 000 and 500 000. Skilled cybersecurity experts are needed in achieving high level of cybersecurity, which is indispensable in tackling growing cyber attacks and the emerging threat landscape, building resilience and supporting Europe's growth and competitiveness.

To this end, the European Commission adopted a Communication on a Cybersecurity Skills Academy as part of the European Year of Skills. The aim of the Cybersecurity Skills Academy is to close the cybersecurity talent gap by concentrating existing initiatives on cyber skills and improving their coordination. The Skills Academy will gather education and training opportunities from public and private entities from European and national levels into one platform, in order to make access to information more straightforward.

The best way to tackle the evolving cybersecurity threat landscape and respond to emerging threats is to improve knowledge and awareness, and develop better cybersecurity skills. All of this contributes to a more resilient and competitive Europe. Reaching a higher level of cybersecurity preparedness concerns all sectors of society and involves everyone, not only specialists

working in the field. These new initiatives are much welcomed, yet long due. Their objectives are not revolutionary: Europe needs to develop a high performing digital ecosystem over long term, guarantee universal access to digital education, and develop inclusive and quality ecosystem that helps address the digital divide. Investments in digital infrastructure and digital equipment are needed.

Furthermore, the recognition of microcredentials and the validation of skills that are certified by the industry and fall outside the realm of traditional educational institutes should be improved. To this end, the upcoming European Digital Skills Certificate will be useful tool. It should be highlighted that no actor can solve the skills gap alone. Public-private partnerships should be strengthened. European industry, in particular small- and medium-sized enterprises have great potential in developing solutions to address the skills gap and the digital divide. Moreover, improving digital skillsets does not only concern the administrative sector in charge of education, but involves all sectors of the public administration due to its wide societal impact. Therefore, an aligned, whole-of-government approach is the most effective.

New technology brings countless possibilities. One cannot control the uptake of new technology, but one can develop a digital skillset to be able to understand and control technology. Cybersecurity and digital skills concern everyone. Reskilling and upskilling, as well as continuous, life-long learning should be encouraged. ■



**HENNA VIRKKUNEN**

- ' Henna Virkkunen has been a member of the European Parliament since 2014. She is a member of the Committee on Industry, Research and Energy and the Committee on Transport and Tourism.
- ' Virkkunen is a keen advocate of digitalisation. She is currently working as the EPP Shadow rapporteur on the Cyber Resilience Act. Virkkunen promotes an innovation-friendly Europe. She has served several ministerial posts in Finland as a Minister of Education and Science, Minister of Public Administration and Local Governance and Minister of Transport.





// Mira Stenhammar

People use Internet more than ever to come together and interact with others in various online environments and social media platforms. Information in social media is dynamic dialogue between and within individuals, communities, and different interest groups. Information is not permanent, but changing and relative according to the meanings people give to information in interaction. Social media and comments on online discussions and comments on comments quickly create an information space where rumours, attitudes, feelings, and facts are tangled together in such a way that fact checking is almost impossible. Disinformation and propaganda in social media have become increasingly sophisticated and harder to trace. Defamation, fear mongering and threats of violence increase communication channelling negative emotions, the result of which can be an increased feeling of insecurity in society.

The Internet offers its users a unique environment that has no equal in the offline world. Internet-mediated communication offers a fast, cheap, and anonymous mean of communication for many ideological extremist groups, and the Internet is often used to incite hatred and violence. On the Internet, an individual can represent many aspects of his/her personality or identity, depending on which online group he/she appears in at any given time.

#### INTERNET AND SOCIAL GROUPS

To understand the differences between people, it is necessary to understand the psychological mechanisms behind the behaviour of individuals, which influences their online behaviour. There are four factors distinguishing online interaction from face-to-face interaction: greater anonymity, less importance of physical features,

better control over time, and ease of finding like-minded people. Especially young people spend often a lot of time on the internet looking for like-minded friends and people. When they find such polarised groups to strengthen their own identity, it can cause social bubbles, cognitive distortion and strengthen a black-and-white worldview. More and more adolescents are exposed to harmful material such as inappropriate language, violent content, drugs, and radicalised groups.

One of the most effective ways groups can influence an individual is by reinforcing norms. Norms are common behavioural standards of group members. Once learned, they are followed to gain social approval. Belonging to groups often shapes our behaviour. Individuals relate more positively to members of the ingroup and negatively to members of the outgroup. Belonging to one's own group may be strengthened by forming negative associations with members of the outgroup. This kind of behaviour can again arouse hostility between members of different online groups and within groups.

#### FROM THE SURFACE WEB TO THE DARK WEB

Aggressive behaviour on the internet is easy in many ways. Access to the Internet and discussion forums is basically possible at any time, and no one can specifically limit it. Similarly, the content of the network is largely unregulated, and communication can be done anonymously. Anonymity refers to acting privately or without being recognised. Privacy is often justified as a fundamental human right of individuals and a need for their own personal space. People should have the freedom to interact with others without supervision. Anonymous systems make it impossible to find information about a



person without their own will. However, anonymity has two sides: on the one hand, it protects the privacy of data and their users, while on the other hand, it minimises the responsibility of one's own actions. Communicating anonymously creates a distorted image that you don't have to take responsibility for what you say. Other online chatters can bolster and encourage anonymous hateful behaviour of others. On the Internet, it is "easy" to attack other anonymous and pseudonymous people, because they are unknown and therefore more inhuman, and there is no need to fear retaliation.

The interaction of those persons and groups whose conversations and communication are marked by anger and negativity can be difficult to implement on the surface web. Those people whose opinions are moderated and censored on the surface web end up more easily on the dark web to express their opinions. Social media and especially dark web are increasingly becoming a forum for crime, abuse, and hate speech because there are no clear control mechanisms for filtering user-generated content. The dark side of social media can be thought of as a collection of negative phenomena related to the use of information technology that can harm the well-being of individuals, organisations, and societies. The dark side of social media can pose a real threat to national security as future generations are born into an environment of various polarised online information networks.

## A PLATFORM FOR THE DEVELOPMENT OF CYBERCRIME

The dark web especially, is in many ways an ideal arena for the activities for various criminal and ideological extremist groups, because it is difficult to regulate the activities happening in dark web on behalf of any individual entity or state and it offers an anonymous multimedia environment with all services. Cybercriminal groups can be examined based on their group identity and based on the motives that guides their activities. Groups can be strictly controlled or alternatively without any hierarchical structure.

Three main groups can be identified from cybercriminal groups:

- 1) traditional criminal groups
- 2) organised cybercriminal groups and
- 3) ideologically and politically motivated cybercriminal groups.

Several of these groups have organised activities outside the online environment. Hacktivists and politically motivated hacker groups are also one of the newest forms of cybercriminal groups. In addition to these aforementioned groups, one should not forget individuals who are increasingly using technology for illegal purposes and

inappropriate activities.

One of the most significant factors in the growth of cybercrime has been the easy availability of the necessary tools. The availability of advanced technologies and methods for committing cybercrimes has grown considerably and they are relatively easily available on the dark web. This development has enabled many less tech-savvy individuals to carry out highly sophisticated cybercrimes. Similarly, social media platforms enable bullying, harassment, and threatening of others at a low threshold. Technology also reduces the risks of an individual being caught, as detecting, and judging different types of crime is much more challenging in an online environment than in an offline environment. In cyberspace, it is also easy to maximise the proceeds of crime by targeting several victims at the same time.

Various political and social movements also use technology to spread information about their beliefs and coordinate activities both online and offline. The Internet has become a critical tool for various extremist and terrorist groups to spread ideologies and radicalise individuals to violence. Extremist groups and ideological hackers have found ways to use the Internet as a mechanism to attack governments and those in power from around the world. In this way, technology has, among other things, expanded the ability of extremist groups to influence populations better than in the physical world.

## CONCLUSION


The dark web is a kind of hidden organisation that connects traditional illegal actors and hackers through an anonymous cyber infrastructure. Over the last few years, the dark web has developed as a means of interaction, which has increased the inappropriate activity and cybercrime. The dark web is a mix of crime and idealism and everything in between. Its existence is indeed a multifaceted and problematic issue in many respects. Although the dark web is also a place of free expression for dissidents, defenders of freedom of speech and whistleblowers, it has also enabled many new forms of crime and made it easier to commit crimes. For this reason, the use of the dark web creates a kind of stigma for its users. The crime prevailing in the dark web and the challenges of tracking it are apt to increase the sense of insecurity experienced in societies. ■



**MIRA STENHAMMAR**

Chief Cyber Analyst,  
Cyberwatch Finland



A soldier in camouflage gear is shown from the chest up, holding a rifle. The soldier's face is obscured by a helmet and the text. The background is dark, and the lighting highlights the soldier's gear and the rifle. The title text is centered over the image.

# THE WAR IN UKRAINE WILL NOT BE RESOLVED IN CYBERBATTLES

// Markus Vaija

The war in Ukraine is the first conflict in the world where the cyber environment plays a significant role as one of the battlefields of war. Traditionally, these fields or domains have been thought to be land, sea, air and sometimes space. For the first time, in Ukraine the world has seen the role of the cyber domain in a large-scale war between states. However, this is not the first conflict in which the cyber environment has been extensively exploited. There have been for years, and still are ongoing cyber struggles between states in around the world. However, the war in Ukraine is (so far) the only major conflict where a cyber war is taking place at the same time as a kinetic war. It is from this perspective that it is interesting to examine it and try to understand what role the cyber operations have played in terms of the overall picture of the war.



Before the start of the war, there were ideas and theories about how cyber operations could be used to support other military activities. However, practice has shown that many of these perceptions have been wrong. When examining the situation, the aim should be to understand how cyber operations have actually been successfully utilised to advance broader strategic objectives, what their impact has been and how cyber activities have affected operations on other battlefields. However, it is extremely difficult to accurately examine a war that is still ongoing. Not only because of unreliable or non-objective information, but also because both sides actively seek to conceal information that is unfavourable to them or critical in nature. Although there are isolated cases, such as Ukraine's use of cyber intelligence to determine the location of Russian officers or bases, only the tip of the iceberg is likely to be seen. This makes it almost impossible to assess the effectiveness of operations, in particular. Keeping track of the battles in the cyber environment is made even more difficult by the fact that most operations take place outside the reach of the public eye and quietly, without massive reports. The best conclusions about the war in Ukraine and its cyber component can probably only be drawn years from now. However, it is possible to cautiously assess what can be said about cyber operations as part of a wider conflict based on publicly available information, although it is still difficult to measure their weight in terms of the war as a whole.

At the start of the war, there seemed to be two perceptions of cyber war, both of which later turned out to be wrong. Firstly, since Russia was assumed to possess massively superior cyber capabilities in comparison to Ukraine and being on the offensive, and therefore in an inherently advantageous position, it was expected that Russia would fairly quickly achieve a significant victory in the cyber world and cripple Ukraine's information systems. Secondly, there seemed to be an expectation of a significant single cyberattack or operation, the effects of which in one direction or another would have been clear and significant. Although major cyber operations have been seen on both sides, many of them cannot be said to have had extensive effects lasting several days or weeks. The battle in cyberspace has turned out to be an even-handed and slow war of attrition, with both sides likely still figuring out the best way to use it to achieve broader strategic goals.

After the first few months of the conflict, the reason for the cyberwar deviating from expectations was thought to be wrong estimates of the power balance, not a fundamental misunderstanding of the cyberbattlefield as a whole. The reasons why there was no significant victory in the cyber world were thought to be both overestimates

of Russia's performance and unforeseen Western support for Ukraine. While these factors have certainly contributed to why expectations were not met, it has gradually become more and more obvious that the potential of cyberspace in war was misunderstood in the first place. There has not, and will not be, a significant battle to resolve the cyber environment in the war, because due to the nature of the battlefield, such a battle is simply not possible, or at least not very likely.

This opinion of the new picture of cyberwar seems to have gained ground, especially in the United States. Last month, the Atlantic Council, a U.S.-based think tank, held a panel discussion on *Melding cyber and kinetic in conflict* where experts from both the military and academia sought to redefine how cyber operations should be understood in the broader context of war, based on lessons learned from the past year. According to the panel, when examining the events of the war in Ukraine, the previous understanding of the role of the cyber environment has indeed been wrong and, in order to learn useful lessons for future conflicts, the perception of the cyber world as a field of war should be changed. Michael Marten, cyber operations expert at the Atlantic Council, described that before the war, many seemed to expect a single major battle with major ramifications in the cyberspace, a kind of Pearl Harbor of the cyber world. The premise was that there would be a single battle, similar to the aforementioned turning point of the Second World War, that would shape the picture of the war as a whole. This approach, he says, is wrong. Instead of Pearl Harbor, cyber operations should be compared to the later and clearly less media-sexy Pacific submarine campaign of the same war. In this protracted operation, US submarines operated quietly and out of public view, but slowly eroded Japan's war machine, particularly by weakening its supply capability and providing significant intelligence without any major battles. ➤



**The battle in cyberspace has turned out to be an even-handed and slow war of attrition, with both sides likely still figuring out the best way to use it to achieve broader strategic goals.**

The submarine analogy is supported by the fact that it compares operations in the cyber environment with invisible operations that utilise the highest technology of the time. On the other hand, cyber weapons, unlike submarines, are not so effective when the aim is to destroy or permanently damage anything, but are more so tools of harassment, momentary interruptions or information gathering. Another possible comparison of the Second World War could be found in strategic bomber campaigns, which were also intended to weaken the opposing side's logistics or supply capabilities. Like bombings, cyberattacks have also had a significant impact on the conditions of the civilian population in the midst of war and how much war is visible and felt in their lives. Cyber operations have also had significant propaganda value, and both warring parties have used their successful strikes effectively as strategic communication tools.

The cyber environment has also enabled a completely new way of involving both our own citizens and foreign aid in the war effort. In the war in Ukraine, both sides have used crowdsourcing in their cyber operations. Crowdsourcing and its benefits have been visible in the activities of Ukraine's IT army, which recruits foreign cyber experts, in the attacks by patriotic cybercriminals used by Russia, and in the use of mobile applications aimed at Ukrainian civilians. With these applications, Ukrainian citizens have been able to report Russian aircraft or other military activities they observe quickly and directly to the armed forces. The impact of crowdsourcing has been not only concrete support for operations, but especially for the civilian population of Ukraine, it has certainly had a resilience effect. When citizens feel that they are a useful part of the conflict and that they are helping their country in the midst of war, this also has a positive impact on crisis resilience, even if the actual effects of the action would otherwise be modest.

The cyber environment as a tool for communication and information influencing has also greatly changed the traditional war environment. From the very beginning of the war, Ukraine managed to win broad international support and sympathy. A significant role in this was played by both functional telecommunications connections and the possibility to communicate directly from the conflict area. The speed of communication and the ability to follow the events of the war in near real time from anywhere in the world has had a strong impact on how much attention the conflict in Ukraine has received and, consequently, on the amount of support from abroad.

However, it should be remembered that at this stage it is simply impossible to know the truth regarding what cyber operations have managed to achieve and how effective they have been for example in supporting

intelligence gathering. When assessing the role of the cyber environment in the war, it should be kept in mind that the war in Ukraine is the first conflict in this respect, and perhaps one that serves as some kind of testing ground. It is possible that in the future, the significance and use of cyber operations as part of military operations will differ significantly from what we have seen to date. A further analogy could also be drawn from history: air warfare, which during the First World War was only emerging as a major battlefield, was only a few decades later during World War II of a completely different nature. It was significantly more advanced, resourced and played a very central role. In the First World War, air warfare was a relatively new concept, the benefits and possibilities of which were still being sought and developed. In the Second World War, on the other hand, it was already a concrete and quite essential part of the strategic struggle and the outcome of the war.

Therefore, it seems likely that the war in Ukraine will not be resolved on the battlefield of the cyber world. It is a new operating environment in the context of war, the importance of which was clearly overestimated before the start of the war. However, cyber operations have not been in vain, or the role of the cyber world has been non-existent. Their significance has only turned out to be less significant and markedly different from what was anticipated. However, this is a rapidly developing and changing field, and unlike air warfare, it is likely that there is no need to wait decades for the picture of cyberwar to change significantly again. ■



**MARKUS VAIJA**

' Cyber Analyst,  
Cyberwatch Finland







# CYBER WAR THROUGH RUSSIAN LENS

// Mikko Hynönen

The war in Ukraine has been called the world's first full-scale cyberwar<sup>1</sup>. The winner is not yet known, but there have been blows on both sides. Russia has attacked against satellites<sup>2</sup>, targeted Ukrainians with phishing messages<sup>3</sup> and carried out large-scale denial-of-service attacks on Europe<sup>4</sup>. Similarly, Russia itself has experienced setbacks on the cyber front, for example by means of cyber sabotage<sup>5</sup> and information leaks<sup>6</sup>.

This article looks at cyberwar through a broader and slightly different lens than individual operations. The article aims to describe the significance, benefits and challenges of the cyber dimension of the war from Russia's perspective. There are both things speaking in favor for Russia, but also challenging developments. For Russia, cyberattacks seem to act as a kind of unofficial extension of foreign policy, and the attempt to use the cyber front as a means to activate and involve the people and volunteers is significant. Challenges are caused by the failure of one's own cyber defence and, in particular, the shortage of experts, which can be expected to continue to grow in the future. ➤

## THE IMPORTANCE OF CYBERATTACKS FOR RUSSIA

The importance of cyberattacks in war should not be overemphasized, but neither should they be underestimated. It seems that the war will probably be resolved on the physical battlefield, by means of conventional warfare, but cyber operations will of course at least play a supporting role in physical operations. The effects of cyberattacks are manifold: they erode the morale of both adversary forces and civilian population, tie up adversary resources and support operations on the battlefield. However, expert assessments suggest that Russia has failed to combine conventional and cyber warfare, let alone achieved strategic effects through cyber operations<sup>7</sup>. This does not mean that Russia will not accumulate useful lessons for the future and succeed in developing its activities. According to some estimates, progress has been made during the war, if recent operations are compared with the attacks at the beginning of the war<sup>8</sup>.

In Russia's case, the wider significance of cyber operations does not consist solely of the destruction and harm inflicted on the adversary, as countless other benefits can also be listed. In addition to a simplified military lens, it makes sense to view cyber operations as part of Russia's foreign and domestic policy. To paraphrase Carl Von Clausewitz's classic "war is the continuation of politics by other means", Russia's cyberattacks are also a form of continuation of foreign policy by other means. This is particularly true for cyberattacks outside Ukraine. It is a recognized fact that in Russia the boundaries between criminal hacker groups and the state are blurred<sup>9</sup>. Russia has at its disposal not only criminal gangs that are separate from state actors, but most likely to some point loosely connected to them, but also APT groups under direct control of intelligence services. Thus, almost all cyber activities of Russian related groups, are likely to be motivated to some extent by the guiding hand of the state. Cyberattacks can be interpreted as sending a strategic message rather than just bullying or military objectives. For example, the message of the denial-of-service attacks against Germany in January and Finland at the beginning of May was clear. The former coincided with the decision to hand over the Leopard tanks, while the latter coincided with the confirmation of Finland's NATO membership. In the absence of, or alongside other means, cyberattacks are a way to show dissatisfaction with foreign policy decisions. Officially, of course, the Kremlin has denied that the attacks are linked to Russia, calling the allegations "absurd"<sup>10</sup>.

There are also other meanings that could be given to cyberattacks. When military operations are otherwise hampered, reports of successful cyberattacks raise the nation's morale and can serve as a propaganda weapon. Indeed, direct moral support has also been given by those

in power for the activities of non-state hackers, as evidenced by the debate held in the spring on freeing hackers acting in Russia's interests from criminal liability on February<sup>11</sup>. In this way, Russia allows ordinary citizens to participate in the war and support the motherland. Of course, crowdsourcing is not just a Russian phenomenon, as throughout the war, cyber volunteers around the world have targeted Russia. A lot has been written about this topic in Western countries, in Finland both YLE<sup>12</sup> and Helsingin Sanomat<sup>13</sup> covered the topic in the first spring of the war.

## CYBERATTACKS AND SHORTAGE OF EXPERTS COMPLICATE RUSSIA'S POSITION

Although Russian hacker groups boast on their Telegram channels about successful cyberattacks and efforts are being made to facilitate hackers, Russia has struggled to keep its own systems protected. Russia has been hit by a massive number of cyberattacks, and there has been an increasing amount of coverage of them in the Russian media. For example, Izvestia magazine reported that DDoS attacks doubled in the first quarter of 2023 compared to a year ago<sup>14</sup>. The same newspaper has reported on the FSB's statement that the US and NATO are using Ukraine as a platform for cyberattacks directed towards Russia<sup>15</sup>. In addition, authorities announced in this March that more than 165 million personal data files concerning Russians had been leaked since the beginning of year<sup>16</sup>.

It is difficult to get a comprehensive picture of the level of cyber security in Russia. For example, in the ITU (International Telecommunication Union) Global Cybersecurity Index, Russia ranked fifth in 2020<sup>17</sup>. On the other hand, news reports of successful attacks and leaked data speak against the ranking. What is striking is that although disruptions and data leaks are reported, they have not had major or crippling effects and have not dominated the media space. It is also possible that this is a purposeful attempt to create the impression that cyberattacks are not effective. In a more cynical view, the state just doesn't care about the leaked information of its citizens. For example, opposition media Meduza has pointed out that security fines for leaks are usually only between 60,000 and 100,000 rubles (about 700–1200 €)<sup>18</sup>.

However, from the point of view of state leadership, a more worrying threat than Western hackers and leaking citizens' data is resistance from within. For example, Belarusian hackers are known to have attacked railway infrastructure, slowing down the delivery of supplies to the front<sup>5</sup>. An insider threat has also materialised when data, such as inside emails, from Vulkan, a company linked to intelligence services, was leaked by a dissatisfied employee<sup>6</sup>.

Many also vote with their feet: the departure of professionals and the resulting growing shortage of experts, which has been further exacerbated by the war, poses its own



challenge. Educational programs in computer science in Russia have traditionally been of high quality, and for many years, teams from universities in the country have achieved success in inter-university coding competitions<sup>19</sup>. As a result of the war, companies have faced challenges in retaining their employees, and up to one hundred thousand IT professionals are believed to have moved out of the country<sup>20</sup>. Efforts have been made to address this problem by improving remote work opportunities. For example, IT giant Yandex is already opening a second office in Belgrade, a popular destination for emigration<sup>21</sup>. However, the state is trying to curb emigration. Most recently, the Duma is undergoing a legislative reform aimed at raising the tax rate for workers working for Russian companies from abroad from 13 % to as much as 30 %<sup>22</sup>. There is a lot of wrangling between companies and the state, with the state using both the carrot and stick to get IT experts to Russia, as companies increase the options for working abroad. The shortage of experts can also manifest itself in a surprising way. For example, there has been discussion throughout the spring about the development of artificial intelligence with the advent of ChatGPT and its competing alternatives. The question may arise, who will develop Russian artificial intelligence or next-generation cyber weapons if experts flee the country?

## REFERENCES:

- 1 <https://www.atlanticcouncil.org/blogs/ukrainealert/vladimir-putins-ukraine-invasion-is-the-worlds-first-full-scale-cyberwar/>
- 2 <https://www.technologyreview.com/2022/05/10/1051973/russia-hack-via-sat-satellite-ukraine-invasion/>
- 3 <https://blog.google/threat-analysis-group/ukraine-remains-russias-biggest-cyber-focus-in-2023/>
- 4 <https://www.euronews.com/2023/01/26/russian-hackers-launch-cyberattack-on-germany-in-leopard-retaliation>
- 5 <https://meduza.io/en/feature/2022/07/05/the-guerrilla-war-on-belarus-s-railways>
- 6 <https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics>
- 7 <https://www.swp-berlin.org/10.18449/2023C23/>
- 8 <https://www.iiss.org/research-paper/2023/03/russias-war-in-ukraine-examining-the-success-of-ukrainian-cyber-defences>
- 9 <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a>
- 10 <https://iz.ru/1459891/2023-01-25/peskov-nazval-absurdnom-assotciatcii-liu-bykh-khakskikh-atak-s-rossiei>
- 11 <https://tass.ru/obschestvo/17021313>
- 12 <https://yle.fi/a/3-12338836>
- 13 <https://www.hs.fi/ulkomaat/art-2000008649170.html>
- 14 <https://iz.ru/1502326/mariia-frolova/poimali-volnu-cto-stoit-za-vesenni-mi-ddos-atakami-na-rossiiskie-kompanii>
- 15 <https://iz.ru/1497823/2023-04-13/fsb-soobshchilo-ob-uchastii-pentagona-v-kiberatakh-protiv-rossii>
- 16 <https://tass.ru/obschestvo/17275519>
- 17 <https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTML-E>
- 18 <https://meduza.io/feature/2022/12/22/nikogda-esche-lichnye-dannye-rossiyan-ne-utekali-v-otkrytyy-dostup-tak-chasto-i-v-takom-ob-eme-kak-v-2022-m-odna-iz-prichin-voyna>
- 19 <https://icpc.global/worldfinals/fact-sheet/ICPC-Fact-Sheet.pdf>
- 20 <https://www.themoscowtimes.com/2022/12/20/moscow-says-100k-it-specialists-have-left-russia-this-year-a79754>
- 21 <https://www.forbes.ru/svoi-biznes/486667-andeks-otkroet-vtoroj-ofis-v-belgrade>
- 22 <https://duma.gov.ru/news/56961/>

”

**When military operations are otherwise hampered, reports of successful cyberattacks raise the nation's morale and can serve as a propaganda weapon.**

## CONCLUSIONS:

For Russia, the cyber dimension of the war presents both threats and opportunities. Cyberattacks support military operations and help Russia to learn lessons for future operations. In a broader perspective, cyberattacks send a strategic message and act as an informal foreign policy messenger. At the same time, cyberattacks and encouragement for them serve as a propaganda tool and a form of crowdsourcing war.

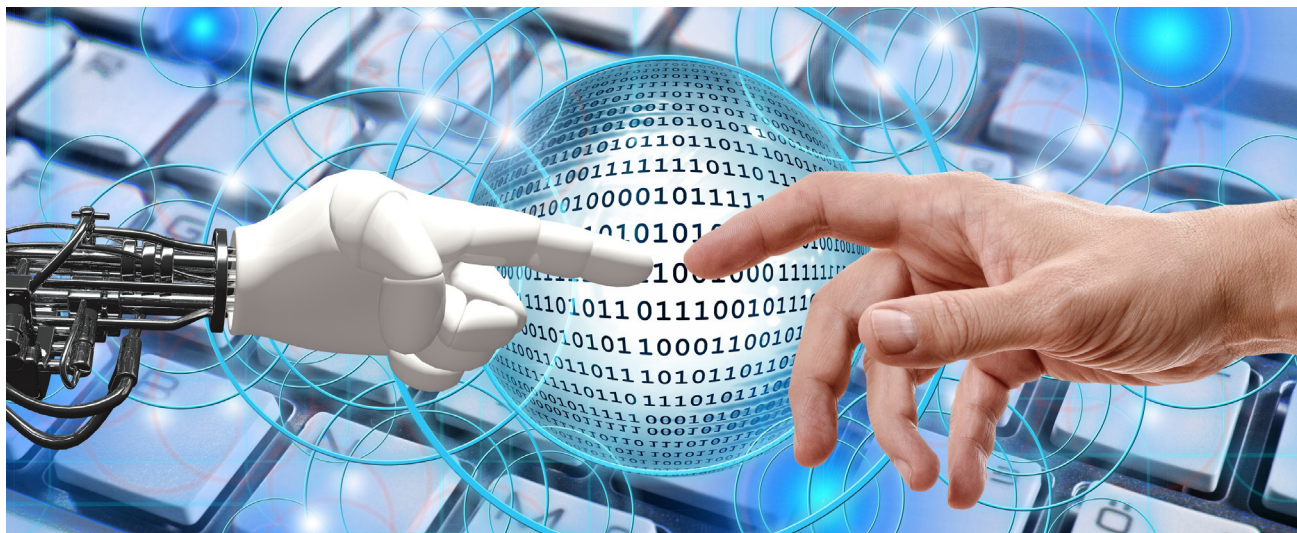
At the other end of the scale, Russia itself has fallen victim to an unprecedented cyber tsunami. Information is leaking, but the response has not been visible, at least so far. The cyber dimension is a growing threat that is accelerated by insider threats and the increasingly acute shortage of experts. ■



**MIKKO HYNÖNEN**

Cyber Analyst,  
Cyberwatch Finland





# OLD AND NEW ELEMENTS OF CYBERSECURITY

// Jukka Lång, Johanna Tuohino and Julia Vikström

The current cybersecurity landscape has forced us to learn how to cope with surrounding cyber threats. By assisting our clients and international law firms in large and complex data breach incidents, we have learned the pain points and relieving factors in the data breaches of today. Based on our experience of the busiest ever data breach year of 2022, we predict that the increase of risks and malicious cyber attacks will just continue. Our team has compiled our key takeaways into five categories of the old and new elements of cybersecurity.

## TECHNICAL CORE ELEMENTS

Cybercriminals often target the "low hanging fruits". In order to secure employees, customers, services, business partners as well as the whole business and its continuity, it is necessary to build a strong technical cyber shield in one's IT systems and environments. Therefore, organisations need to be familiar with the possible threats, available best practices and requirements of law whenever IT systems, products and services are sourced and upgraded. We need to think ahead – cybersecurity must carry on during the whole lifecycle of the system, product and service and beyond that. This entails updating, monitoring and assessing the security levels as well as applying sufficient and sustainable contractual terms in technology agreements.



## COLLABORATION

Even the best available cyber team cannot secure the whole organisation without teamwork. Large data breaches often commence with email attacks, like phishing, which are sometimes difficult to spot among the email floods. Malicious attackers often target members that are considered either the most vulnerable, such as new employees who have not yet learned the ropes, or the most influential, such as members of the management team. Collaboration and shared responsibility forms one of the key elements in protecting the organisation. This means that all members of the organisation, as well as external partners, need to collaborate in a responsible manner towards the common goal. The privacy and security functions together with all the legal counsels of the organisation have a pivotal role to play in this continuous preventive work that entail a vast field of different tasks from sourcing procedures and internal policies to third party agreements and data protection impact assessments.



## TRAINING

A certain level of training must be provided to all members of the organisation. Everyone should be familiar with the risks that are relevant in their area of responsibilities. In addition to the cyber threats, organisations need to be familiar with the relevant legal requirements stemming from data protection and cybersecurity legislation, including sector-specific legislation. Consequences and risks increase if a data breach incident reveals that mandatory legal requirements have been disregarded. In most cases, the management of organisation bears the responsibility for compliance with the applicable legal requirements.

## PLANNING

Cybersecurity entails thinking ahead, constantly. According to the leading Finnish cybersecurity experts, data breaches will occur in all organisations sooner or later. It is vital to have an extensive plan for recovery measures as well, including mapping and contacting necessary external advisors from areas of technical consultancy and legal advice. Typically, organisations face an unexpected situation when the data breach notification must be filed with the competent data protection supervisory authority or authorities within 72 hours of becoming aware of the breach. Even though the notification can be filed as preliminary and completed later, the list of requested information for the initial notification is quite extensive. Sometimes, the notification must be filed in several countries by following varying local filing procedures. Our existing international networks of law firms and other experts cover all jurisdictions globally and ensure the possibility to fulfil these obligations within the set time requirements.

## CARING

Cyber risks and their actualisation causes distress to organisations and their people and customers. A data breach, which involves personal data of individuals, may be a devastating shock to the involved data subjects. When resources are reallocated during incident management, external advisors may be helpful in reducing the distress, when some of the internal resources need to be allocated for supporting the organisation and the affected individuals. Managing cyber risks is not only protecting the business, but also taking care of the people, their security and wellbeing.

## D&I'S CYBERSECURITY CHECKLIST FOR ORGANISATIONS

- 1 Implement comprehensive technical cybersecurity measures with careful sourcing of IT systems, and keep the IT systems up to date. Consider state-of-the-art encryption and key management, especially when passwords or sensitive data are being processed. Pay attention to securing availability and integrity of data, including backups and necessary log data.
- 2 Prepare a risk management plan and a data breach policy to respond effectively to any possible security incidents. Ensure top management awareness and involvement.
- 3 Involve all members of your organisation in cybersecurity work as defined by their roles and tasks.
- 4 Map and contact your external advisors in advance in order to act rapidly in case of a data breach.
- 5 Train your organisation to protect your people, business and activities, including the methods of recognising and preventing cyber attacks, for example phishing attempts. Show that you care for both – security of people and continuation of business. ■



**JUKKA LÄNG,  
JOHANNA TUOHINO  
AND  
JULIA VIKSTRÖM**

- › Jukka Lämg  
Partner
- › Johanna Tuohino  
Senior Associate
- › Julia Vikström  
Associate

**DITTMAR & INDRENIUS**

This article has been published on 30 March 2023 in Dittmar & Indrenius Quarterly.  
Link to the original article: [www.dittmar.fi/insight/elements-of-cyber-security/](http://www.dittmar.fi/insight/elements-of-cyber-security/)



# CYBER CITIZEN SKILLS – WHAT IS THEIR IMPORTANCE AND HOW SHOULD THEY BE DEVELOPED IN THE EU?

// Marianne Lindroth

Cybersecurity skills have been the subject of much discussion in recent years, and in particular the skills profiles of cybersecurity professionals have also been defined at EU level. However, both for the collective resilience of the EU and for the resilience of individuals, the development of cyber citizen skills, is also of paramount importance. The EU-wide Cyber Citizen initiative aims to create a common model for training citizens in cybersecurity skills, taking into account the different needs of different target groups and the evolving threats in the cyber domain. The model will be used to develop a cybersecurity learning portal for all EU citizens, including a cybersecurity skills game.

## AN INITIATIVE FOR ALL EUROPEANS

The cyber citizen skills initiative Cyber Citizen responds to the practical need for creating security culture in the human-centred digital environment. The initiative aims to develop a common, shared model for learning cyber citizen skills across the European Union for all Europeans. The initiative is funded by the EU Recovery Instrument, commissioned by the Finnish Ministry of Transport and Communications and implemented by Aalto University.

Overall, the Cyber Citizen initiative will produce a European model for cybersecurity learning which in turn will strengthen European cybersecurity and produce common practices. Based on the model, a digital learning portal will be built. This portal will make use of a wide range of e-learning methods. An integral part of the portal is a cybersecurity game that provides information and

understanding in an entertaining way.

In the first phase of the initiative, the current teaching methods, views, and materials of cyber citizen skills education and training in all the European Union member states were studied. This included national characteristics and requirements of the member states. Official EU policies were also reviewed. Additionally, a game analysis, an assessment of cybersecurity indices, and a scoping literature review were part of the research. The data used was gathered from a wide range of resources. The results of this qualitative research can be found as an extensive research report.



## TOWARDS A UNIFIED, PEOPLE-CENTRED APPROACH

The report shows that there is a high degree of disparity in cyber skills development across the EU and that citizens in all Member States would benefit from a more unified, people-centred approach to cybersecurity.

Cybersecurity threats are increasing in all countries of the European Union. To counter this growing threat, national governments across the EU have invested in programmes to improve the cyber skills of their citizens. However, there are significant differences in cybersecurity awareness, education and training. Despite cybersecurity being a transnational threat, there is currently no common model for cybersecurity learning or practice.

'Cyber citizen skills' have traditionally focused largely on technology, and based on the research, our understanding of cyber skills should be updated to be more people-centred.

Jarno Limnell, Professor of Cybersecurity at Aalto University and Director of the Cyber Citizen initiative, compares the people-centred approach to understanding the rules of the road when driving a car:

"A citizen's cybersecurity consists of their knowledge, skills, and attitudes. Simply mastering technology is not enough to be cybersecure. Similarly, driving a car is not enough to be safe; you also need to know the rules and different situations, and be aware of other road users. Cyber citizen skills are not only necessary for a smooth and safe daily life, they are also essential for the security and economic success of the EU as a whole".

Cybersecurity culture in the EU Member States is currently being built. Creating and strengthening culture takes time, which is why it is essential to work with determination. For this reason, we urgently need actions such as the Cyber Citizen initiative.

In time, we can elevate a shared understanding and extensive competence into common culture, which has great significance to the future of the whole of society and its citizens.

## HIGHLIGHTS OF THE STUDY

The study showed that there is a clear willingness in EU member states to develop civic competences in cybersecurity and to support lifelong learning. A common model would help to achieve this.

Education policy guidelines on cybersecurity in EU countries are relatively new, making it difficult to assess their impact at this stage. However, there is clear progress and recognition of the importance of the issue. Cybersecurity is no longer seen as the sole responsibility of

professionals. Instead, it is an integral part of all social activity.

Cyberspace has become more diverse and versatile – something that is now better understood in the European Union. The current situation highlights more than ever the importance of continuous learning and the extensiveness of required skills and knowledge. Cyber citizen skills are to be understood as dynamic skills that change with the context and environment, and in addition to vigilance, the need for lifelong learning cannot be stressed enough.

Everyone should have basic cybersecurity skills. The development of security culture that is based on human competence and civilization should be strengthened with determination. All age groups have different levels of competence, from digital novices to digital gurus. The question is how to take different target groups into account. The basic know-how and general level of cybersecurity knowledge vary a lot in the European Union member states. This is indicated by the great variance in indices that measure the level of cybersecurity and views on how to improve cybersecurity competence and culture.

People are different, learn differently and may have different constraints, for example, and therefore in cybersecurity training, one-size-fits-all solutions will not work. Currently, the differences between the different target groups are not yet sufficiently taken into account in different EU member states.

The offering of cybersecurity educational and training materials varies both in terms of quality and content, and the responsibility for arranging education and training has been shared in different ways. This directly impacts how widely and in what ways education and training is available and how likely citizens are to enrol in it. High-quality education and training in cybersecurity and related cooperations should be increased and overlapping work reduced. One of the goals of Cyber Citizen initiative is to promote the harmonization and the rationalisation of education and training.

In many EU countries, training in digital skills, including cybersecurity skills, is based on the European Digital Competence Framework for Citizens (DigComp). It is good that a common framework already exists in the background, as this will facilitate the development of a common training model. Of course, cybersecurity skills are only one aspect of DigComp and therefore need to be deepened and refined.

The cybersecurity labour shortage also affects the training of citizens, as professionals are needed to educate citizens and design the content of training. Of course, this problem has been recognised more widely and various measures are being taken to address it. However, it is important to stress the urgency. ➡

Games have established themselves as a form of social behaviour and are increasingly becoming a key learning tool. This finding supports the Cyber Citizen initiative's idea of game development and the use of gamification for learning also in the learning portal.

## CYBER CITIZEN SKILLS

As part of the research, cyber citizen skills were defined. A cyber citizen is a person who lives permanently or temporarily in an EU member state and uses digital services or benefits from the production of these services. A cyber citizen skillset is comprised of knowledge, skills, and capabilities required in cyberspace. It is made of components that help people develop and maintain their knowledge and skills in a way that gives them the required ability and motivation to act sensibly in different situations in life. Having cyber citizen skills means taking personal and social responsibility and understanding the meaning of this responsibility in cyberspace.

In the European Union, we need a common definition for cyber citizen skills and ways to measure skill levels. Cyber citizen skills are understood differently across the EU, and only some member states have defined them in the first place. Definitions can be almost identical, but due to national and cultural differences, they are interpreted in various ways. The European Digital Competence Framework for Citizens (DigComp) has a significant influence in most of the member states. For this reason, the Cyber Citizen research team identified concrete cyber citizen skills which will support the adoption of the DigComp framework in the EU. Cybersecurity skills can be found in all of the DigComp competence areas which are information and data literacy, communication and collaboration, digital content creation, safety, and problem solving.

## TOWARDS A SAFER AND MORE SECURE EUROPE

When citizens have a good attitude and a sense of security based on know-how, they are more willing to use digital services. This way, the European Union will become more sustainable, competitive, and independent. Civic learning opportunities create an understanding of the environment, actors and processes that affect everyone's digital life. Through the improvement of our personal skills, our personal and collective abilities improve our sense of confidence. In the second phase of the initiative, a learning concept for cyber citizen skills is created from the

basis of the research report and especially the cyber citizen skills framework. In the third phase, a learning portal in line with the learning concept is designed.

The learning portal will have content for all citizens, and this content, such as a cyber citizen skills learning game, will take into account different target groups. Citizens' abilities to act in a safe and secure manner in the digital world are improved with educational and communicative elements in the learning portal. Citizens will be asked to take part in planning the educational content. The availability and accessibility of education and training is important when a shared cybersecurity culture based on improving competence is created in the European Union.

## COLLABORATIVE NETWORK OF CYBER CITIZEN SKILLS

The diversity of projects and practices across the EU means that there is something to learn from every corner of Europe. The Cyber Citizen initiative is currently creating a European-wide network of cooperation, welcoming all those interested in developing cyber citizenship skills.

Views on cyber citizen skills and how to develop them through the learning model and portal will be discussed with all EU countries and experts will be invited, for example, to workshops to discuss the best solutions, as well as to offer their expertise. In the future, citizens will also be involved in the design of the content. The aim is to create something new and interesting for all EU citizens and also to raise interest in cybersecurity.

In summary, the project aims to create a learning model, publish a learning portal including a game, build a Europe-wide network of cyber citizen skills stakeholders and raise awareness of cyber citizen skills and their importance among citizens and policy-makers alike. The researchers are therefore asking anyone involved in cybersecurity, research or education, or who believes they have something to contribute, to join the Cyber Citizen initiative network. ■

 **MARIANNE LINDROTH**

- › Project lead, Cybersecurity Awareness, Education and Training
- › Cyber Citizen Initiative
- › Aalto University, Cybersecurity

**A!**  
Aalto University





A photograph of a person's legs and feet sitting on a tall stack of books. The person is wearing blue jeans with the cuffs rolled up. They are barefoot, and their feet are resting on the spines of the books. A laptop is open on their lap. The background is a plain, light-colored surface.

# EDUCATION OF THE CYBER SECURITY PROFESSIONALS

// Martti Lehto

The field of cybersecurity suffers from a massive skills shortage in Finland. The results of the research clearly show that the current number of cyber professionals will not be sufficient to cover all recruitment needs in cybersecurity. In cyber security training is needed cooperation between higher education institutions, support from the third sector and investments of public body. ➡



## INTRODUCTION

Finland is a world leader in using digitalization in higher education and in continuous learning. Digitalization aims to make educational content as widely available as possible. In view of the growing needs for skills renewal, continuous learning should be given greater priority in the higher education sector.

The shortage of skilled cybersecurity experts is globally recognized. Regarding this skills shortage, it is important to consider the different competences needed in different jobs. The range of knowledge, skills, and competences in cybersecurity is wide, and cyber professionals need to specialize in a specific area. This must be considered in education, that is, educators will need to be mindful of the jobs in which graduating students are expected to be employed. Of course, it must be kept in mind that education provides certain basic competences, which may be developed later into deeper expertise through work assignments, specialization, and possible specialist training.

## CYBERSECURITY EDUCATION IN THE UNIVERSITIES OF APPLIED SCIENCES

The cybersecurity education provided by universities of applied sciences (UAS bachelor's and UAS master's degrees as well as specialist education, continuing education, and conversion training) is comprehensive in content and can adapt to the needs of the industry due to its modular structure.

Information and Communication Technologies and in Business Information Technology degree programs offer cyber security training.

The curriculum structures have different categories in terms of whether cybersecurity had been placed in compulsory, specialization (or professional studies), or elective studies. The most important ones are the degree programmes aiming at cybersecurity or the degree programmes offer specialization studies oriented towards cybersecurity.

Based on this categorization, four-degree programmes in UAS master's level are in three universities of applied sciences:

- JAMK, Master's Degree in Information Technology, Cyber Security, Engineer
- TurkuAMK, Software Engineering and ICT Engineer
- Business Administration
- XAMK, Cyber Security, Engineer

The UAS bachelor's degree programmes comprised complex curriculum structures. At some UAS the curricula

have been compiled in order to present lot of courses to students. Alternatively, the specialisations were built into a single curriculum, from which students could make modular choices. Four UAS offer bachelor's level cybersecurity degree programme:

- JAMK, ICT, Engineer
- Laurea, Computer Science, Cyber Security, Business Administration
- TurkuAMK
- ICT, Engineer
- Data Processing, Business Administration
- XAMK, Cyber Security, Engineer

The current intake in cybersecurity studies at universities of applied sciences in Finland is about 555 (degree programme students 165 and 390 minor students). More cyber security experts are needed to meet the demands of continuously expanding digitalization. As a result, cybersecurity expertise is increasingly needed in various digitalizing industries.

When considering the resources for training, it should also be remembered that universities of applied sciences generally provide technical cybersecurity training, which aims for technical competence. Such engineering instruction requires extensive and complex learning environments, which are expensive to acquire and maintain. To guarantee sufficient technical expertise, the acquisition, development, and maintenance costs of the necessary learning and training environments must be considered in resource allocation.



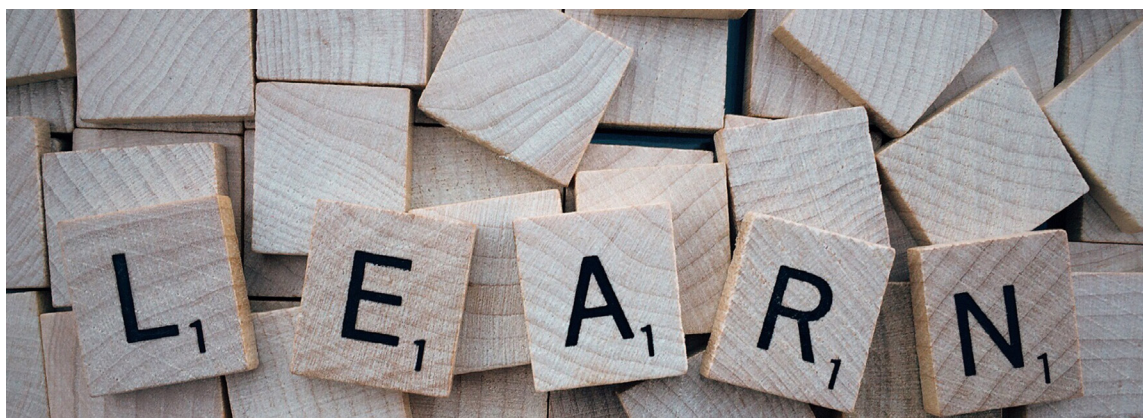
## CYBERSECURITY EDUCATION IN THE UNIVERSITIES

The number of degree programmes dedicated to cybersecurity is small, and teaching is concentrated in the master's level. Universities produce relatively few cybersecurity experts in relation to the identified skills shortage. A great number of degree programmes have integrated cybersecurity into the degree structure as elective or compulsory studies worth 1 to 15 ECTS credits. Universities provide further education in the cyber field to a small extent. The following table illustrates the degree programmes which include cyber security education (major and minor):

| University                           | Degree Programmes/Key course modules   | Intake 2022 |
|--------------------------------------|--|-------------|
| <b>Aalto University</b>              | Security and Cloud Computing (Security)  | 11          |
| <b>Aalto University</b>              | Security and Cloud Computing (SECCLO)  | 76          |
| <b>University of Helsinki</b>        | Master's Programme in Computing Sciences   | 45          |
| <b>Tampere University</b>            | Specialisation: Advanced Studies in Information Security                                   | 1-30        |
| <b>Tampere University</b>            | Master's Programme in Security and Safety<br>Management: Safety Management and Engineering | 8           |
| <b>Tampere University</b>            | Master's Programme in Security and Safety<br>Management: Security Governance               | 8           |
| <b>University of Jyväskylä</b>       | Master's Programme in Cybersecurity  | 45          |
| <b>University of Jyväskylä</b>       | Master's Programme in Security and Strategic Analysis                                      | 25          |
| <b>University of Turku</b>           | Cyber Security major + EIT Digital Master School<br>Dual Degree Programme                  | 35          |
| <b>University of Turku</b>           | Cryptography major   | 5           |
| <b>University of Turku</b>           | Communication and cybersecurity technology major   | 6-8         |
| <b>University of Oulu</b>            | Information technology   | 100         |
| <b>Åbo Akademi University</b>        | Thematic module: Safety-Critical and Autonomous Systems                                    | n/a         |
| <b>University of Eastern Finland</b> | Computer science BSc + MA  | 68          |
| <b>University of Vaasa</b>           | Automation and information technology BSc (Tech) + MSc (Tech)                              | 52          |
| <b>LUT University</b>                | Information technology BSc (Tech) + MSc (Tech)   | 82          |

The list shows that there are relatively few degree programmes dedicated to cybersecurity. Universities' cybersecurity degree programmes or those closely related to the field vary in content. In other words, universities have different specialisations in cybersecurity. It is also noteworthy that the teaching is concentrated in the master's level. Individual cybersecurity studies are generally available in a number of degree programmes as compulsory or elective studies.

Cybersecurity and security degree programmes have an estimated total intake of roughly 250 (110 in major, 140 in minor) in 2023. The above-mentioned figure only includes the initial intake of cybersecurity and security degree programmes and therefore excludes degrees in related fields, such as computer science. Overall, the number of experts produced by universities is relatively small when considering the identified skills shortage. ➡



## CYBERSECURITY TRAINING BY OTHER EDUCATIONAL PROVIDERS

Non-degree studies in cybersecurity are available in Finland, but currently those most in need of education will not find it, nor will they seek it. For example, there is very little training aimed at older people. There are quite a few providers of training to companies and other organizations in Finland.

In the third sector, the most extensive training related to cybersecurity is organised by the National Defence Training Association of Finland (MPK). In addition, some adult education centres provide training related to cybersecurity.

Children and young people currently receive training in cybersecurity as part of their educational pathways, in both primary and lower secondary education as well as in later studies. However, those who completed their studies at a time when cybersecurity was not part of basic education or further studies may currently be completely excluded from cybersecurity training if they do not receive it at their workplace.

There are quite a lot providers of training to companies and other organisations in Finland. Employees in large companies and public organisations generally receive training in connection with their work, but employees in SMEs and the self-employed may not. Another problem may be that the management of SMEs or entrepreneurs do not recognise the need for training.

## QUANTITATIVE NEED OF THE CYBER-SECURITY EXPERTS

The business sector, public administration, and the third sector all need new cyber professionals. In the survey on cyber competence needs by the Ministry of Transport and Communications, 73% of respondents identified a significant shortage of experts in their organization. Almost all respondents would recruit new professionals if they were available. The survey indicates that the needs vary widely. A small group (16%) of respondents considered the skills gap to compromise the safety or profitability of their operations. The question is no longer about decreased growth, but viability.

There is also a strong demand within the cybersecurity industry. According to a survey by the Finnish Information Security Cluster (FISC), 87% of companies in the sector intended to hire cybersecurity personnel. The FISC survey reveals that around 35% of respondents reported that skill shortages are the most important factor constraining the growth of the sector.

The skills shortage is a reality, although it is difficult to predict its level accurately. Based on existing data, it is estimated that Finland will need between 5,000 and 8,000 cybersecurity professionals in the coming years. In

addition, between 1,000 and 5,000 new professionals will work with cybersecurity alongside other work. All these people need to be trained accordingly.

Companies have a wide range of skills needs. The cyber competence profile can be defined based on the commonly used NCWF classification. The American framework has been extensively used in describing the main categories of expertise related to cybersecurity, as well as the specific areas of expertise under them. According to the study, the quantitative needs of companies vary in different areas of expertise. The greatest number of new experts is needed in secure production. This need for 6,000–13,000 new cyber professionals is distributed by main field of study as follows:

1. Secure production 1,100–2,400 persons
2. Operation and maintenance 900–1,900 persons
3. Oversight and governance 1,000–2,200 persons
4. Protection and defence 1,000–2,300 persons
5. Analysis 800–1,700 persons
6. Collection of data and operation 600–1,300 persons
7. Investigation 600–1,300 persons

The research indicates that particular needs were in (a) oversight and governance (with specialist areas such as systems architecture, cybersecurity management, strategies, and cybersecurity or information security managers working with strategies) and (b) more operative competence with an emphasis on systems protection and related analysis. The public sector is relatively more looking for broad expertise leadership and risk management experts, while the business world is looking for more management and architecture experts.

The competence need is fairly evenly distributed across all cybersecurity competence areas. This means the need for comprehensive education and training. The degree studies of higher education institutions and conversion and continuing education must cover all these areas in order to meet the skills needs.



**The business sector, public administration, and the third sector all need new cyber professionals. In the survey on cyber competence needs by the Ministry of Transport and Communications, 73% of respondents identified a significant shortage of experts in their organization. Almost all respondents would recruit new professionals if they were available.**

”

**There is a global recognition of a shortage of skilled cybersecurity experts. This same shortage applies to both Europe and Finland. Globally, the need of skilled workforce is in the millions; for Finland, it is safe to say that it is several thousands.**

## CONCLUSION

In cybersecurity, one of the most important and valuable assets to protect is skilled personnel. No matter the technical solutions and processes in an organization, it does not have cyber resilience without skilled personnel. This is true for all employee roles because incompetence or lack of knowledge among the staff may subject the organization to vulnerability in cyberspace.

There is a global recognition of a shortage of skilled cybersecurity experts. This same shortage applies to both Europe and Finland. Globally, the need of skilled workforce is in the millions; for Finland, it is safe to say that it is several thousands.

Regarding this skills shortage, it is important to take into account the different skills needed in different jobs. The identification and incident management of cyberattacks requires different cybersecurity expertise than cybersecurity management or the acquisition of new systems. This must be taken into account in the training, that is, in which jobs graduating students are expected to be employed. Of course, it must be kept in mind that training provides certain basic competences which may be developed later into deeper expertise through work assignments, specialization, and possible specialist training in the area.

Cybersecurity education should also be targeted at different areas of working life. In this way, the necessary skills would be available to society in general. Continuing education that updates degrees also requires teaching resources. Education must produce enough experts so that society is prepared to respond to the challenges of today's world.

The article is based on a report produced for the National Cyber Security Director Rauli Paananen in 2022: Development Needs in Cybersecurity Education, JYU research paper 93/2022

The number of cybersecurity experts in society can be increased by influencing several factors. One way is to increase the number and initial intake of degree programmes in the field. This requires an increase in human resources. In addition, the number of cybersecurity experts can be increased by developing continuing education. Furthermore, improving educational cooperation between higher education organizations would enable students to acquire more versatile specializations in different areas of cybersecurity.

Increasing the intake of cybersecurity education requires resources for both education and research. The challenge is to recruit researchers and teachers to higher education institutions within a short timeframe.

Effective cooperation networks have been established in other EU countries, connecting companies, government bodies coordinating cybersecurity training, and the third sector. Finland would also benefit from a cooperation network for developing citizens' cybersecurity skills, under the leadership of the body responsible for citizens' training and coordinating training cooperation. The network could also be used in the design of the website that gathers all cyber training and in the further development of the concept of cybersecurity for citizens.

A step in the right direction has been taken when the Ministry of Education and Culture has funded the programme starting in 2022 to develop and increase the availability of cyber security education. It is an extensive cooperation project coordinated by the University of Jyväskylä and the JAMK University of Applied Sciences. The project will assemble a network to develop, coordinate and provide higher education in cyber security. 9 universities and 11 universities of applied sciences and Network University FiTECH participate in it. ■



**MARTTI LEHTO**

- ' Professor of Practice, PhD (Military Sciences)
- ' University of Jyväskylä





*"If you know how to use a smartphone, you also know how to use the app."*

– Teemu Pesonen, Komatsu Forest



## Every second matters

**Helps to secure day-to-day operations, manage crises and save lives.**

**Better safety for employees who are working in the field or alone  
– also alerts for help unless you can't.**

**Alerting, coordination, quick situational awareness and mobile reporting within reach.**

**Do you want to know more?**

[sales@secapp.fi](mailto:sales@secapp.fi)  
[secapp.fi](https://secapp.fi)





# QUARTERLY REVIEW

## Q1 / 2023

// Timo Rinne

### CONTENT:

1. NIS2 and CER – towards greater cybersecurity and resilience
2. Country analysis: Ireland
3. Offensive cyberdefence
4. International competition for artificial intelligence technology

### INTRODUCTION

The NIS2 and CER directives accelerate EU countries' discussions of cybersecurity. In particular, actions related to the NIS2 directive will be seen in the near future, as it imposes the same level of financial sanctions on organisations as the data protection directive GDPR. The first part of the review examines the nature and impact of these directives on the Finnish cybersecurity field.

In this millennium, the largest concentration of data centers in Europe has been centralised in Ireland. In particular, American IT giants have been building data centers in Ireland mainly for fiscal reasons. For example, personal data collected by various social media services are stored in these centers. The data center's security is ultimately the responsibility of its owner, but the environment also has an impact on security. Ireland is not at the top of the EU in terms of cybersecurity but nevertheless offers a reasonably low-risk cyber environment for data centers.

The offence is the best defence even in cyber warfare. Led by the United States, several countries are changing the doctrine of cyber warfare in an even more offensive direction. The third part of the review sheds light on the guidelines of the new cyber security strategy of the United States and NATO's plans in this area.

Artificial intelligence has been considered one of the decisive technologies in the political, economic, and military competition between great superpowers. The United States leads the global competition, with China following. Artificial intelligence is reaching a maturity level where practical services can be developed and offered to the public. At the same time, the special status of AI technology is gradually merging with other technologies. However, the world is still waiting for new, revolutionary innovations, which this technology platform makes possible. ➡





## NIS2 AND CER – TOWARDS GREATER CYBERSECURITY AND RESILIENCE

// Timo Rinne

1. The NIS2 and CER directives are once again activating EU countries' cybersecurity efforts. NIS2 has a GDPR-level sanctions system built into it, which is an important factor in accelerating concrete improvements.
2. The NIS2 and CER directives extend the concept of critical infrastructure to a number of new industries. In addition, NIS2 is a much more comprehensive set of requirements than its predecessor and will affect a significant proportion of medium-sized enterprises, i.e., companies employing more than 250 people.
3. New directives can easily confuse an already complex field of cybersecurity requirements. There is a danger that the requirements will be read too theoretically, the essentials will be lost and the sense of proportion will disappear. Although there are many standards and directives, they all contain the same things from different points of view. It is good to understand the relationships between standards and directives, which at best can promote the objectives of several cybersecurity requirement specifications with the same effort.

The EU's Cybersecurity Directive, or NIS2 directive (Network Information Security 2), was published at the end of last year. The new directive replaces the first version of the previous NIS directive, which has been in force for about five years. Like other directives, the obligations of NIS2 are transposed into national law. At the beginning of this year, the Ministry of Transport and Communications launched an implementation project to create national legislation. This work is expected to be completed at the end of 2024.

The purpose of NIS2 is to update the cybersecurity requirements and address the inefficiencies of the original directive. This inefficiency has manifested itself, in particular, in the fact that the obligations of the directive have been implemented and enforced in a very diverse way in various European countries. The situation is typical of EU directives. Some countries comply with the requirements to exact and others make their own prioritizations. The result is a very diverse level of cybersecurity across countries, which does not contribute to the EU's collective effort to achieve a better level of cybersecurity and resilience in countries.

The new directive introduces a number of new

obligations to improve cybersecurity. The NIS2 directive is much more comprehensive than the previous directive and covers more sectors of activity and the organisations and companies covered by them. The new directive broadens the range of critical sectors of society and imposes new cybersecurity obligations on them. New sectors covered by the directive include, for example, wastewater management and the space industry. NIS2 automatically applies to all medium-sized enterprises, i.e., enterprises employing more than 250 people operating in critical industries.

The NIS2 directive divides companies and organisations operating in critical sectors into key and important actors who are subject to various control measures. Key actors are monitored by means of preparedness inspections or audits carried out before the start of operations. Important actors are monitored through ex-post audits.

Obligations can be roughly divided into management measures and reporting obligations. Management measures focus on risk management but include practically all the basic requirements for cybersecurity management and administration. As in the GDPR, the

reporting obligation includes time limits for reporting deviations to the authorities. An advance warning of deviations must be given within 24 hours and the information must be specified within 72 hours of the detection of the deviation.

Failure to comply with cybersecurity management measures or reporting obligations is subject to GDPR-level sanctions. This means a fine of up to EUR 10 million or 2% of turnover imposed on key players. For important operators, the corresponding figures are EUR 7 million and 1.4% of net sales.

There has not been much news coverage of the actual GDPR fines, nor have they been imposed much in number. By the end of February 2023, the Data Protection Ombudsman has imposed 17 administrative sanctions. In December, the largest sanction to date was imposed on the Finnish branch of the Swedish debt collection group Alektum. It amounted to EUR 750,000 and was due to the company's indifference to requests for information from private individuals. The second largest fine has been received by Vastaamo (608,000 EUR) and the third on the list is Viking Line (230,000 EUR).

In the case of the GDPR, the deterrent of high administrative sanctions has worked as intended. Organisations and companies increased their security budgets to improve the level of data protection, and most organisations launched some kind of data protection project. The pressure on data protection generated new business related to data protection, for example, in the areas of consulting services and software development. As a result, both European companies and companies offering their services to Europe genuinely improved the quality and security of the processing of personal data.

The same trick is now attempted made to correct the inefficiencies experienced by the first NIS Directive in the area of cybersecurity. All European countries must be involved in cybersecurity efforts. This is an important issue due to the security policy situation in Europe, so all countries need to bring their cybersecurity status to a good level.

NIS2's sanctions deterrent has a twofold effect. On the other hand, it forces corporate management to take cybersecurity seriously and ensure that the necessary resources are set aside for the development of cybersecurity. The other side is the GDPR's familiar loss of sense of proportion, especially if the NIS2 requirements are interpreted too theoretically with the aim to completely eliminate all risks. Implementing NIS2 into practice requires experience in correctly dimensioning safety controls and the ability to prioritise future development targets. Otherwise, there is a risk of

"shooting a fly with a cannon" and driving the cybersecurity team to death for fixing things that are of no practical importance.

Another EU directive on cybersecurity and security of supply, which is nearing the end of its deliberations, is called CER (Critical Entities Resilience). The purpose of the CER Directive is to harmonise and strengthen the resilience and preparedness practices of critical entities in EU countries. Critical infrastructure in the EU has been identified as largely vulnerable and the CER Directive, together with the NIS2 Directive, aims to improve the resilience of society.

Critical infrastructure has been a traditional target for cybercriminals and state cyber actors. Several areas of critical infrastructure are vulnerable from a cybersecurity perspective, each in its own way. For example, energy production and water supply use a lot of old industrial systems that were originally built closed but have now been opened up to public networks with remote management requirements. In this way, initially, poorly protected systems have openly entered the playing field of cybercriminals. The IT infrastructure of the banking and financial markets has been built on more modern technology, but these have also been successfully damaged.

Both NIS2 and CER are again putting pressure on organisations to improve cybersecurity. The GDPR and, most recently, the Data Management Act, which targets public administrations, have increased cybersecurity budgets, and extended the working day of cybersecurity professionals. In addition to NIS2 and CER, there are several other cybersecurity-related requirements in the discussions, increasing the risk of drowning in a jungle of different requirements.

While there are a number of different cybersecurity requirements in the discussions, they are not entirely different from each other, but all aim to improve cybersecurity from different perspectives. It is good to understand the relationships between standards and directives, which at best can promote the objectives of several cybersecurity requirement specifications with the same effort. However, understanding the big picture requires monitoring the work of several ministries, as the preparatory work for the different requirement specifications for cybersecurity is each divided into a different ministry. NIS2 belongs to the Ministry of Transport and Communications, CER to the Ministry of the Interior, and the Information Management Act to the Ministry of Finance. The whole thing is manageable, although centralised management and coordination of cybersecurity improvement projects could make it easier. ■

References  
on page  
32





## COUNTRY ANALYSIS: IRELAND

// Timo Rinne

1. American IT giants such as Google, Microsoft, Amazon, and Apple have created the largest concentration of data centers in Europe in Ireland. These data centers also hold huge amounts of personal data. Data center owners have billions in annual budgets to ensure cybersecurity.
2. Ireland's level of cybersecurity is below average on a European scale. Ireland is ranked 28th on the European list of the ITU Global Cybersecurity Index. The biggest shortcomings are in cybersecurity cooperation between different organisations and companies. In 2021, Ireland has established a national cybersecurity development centre to improve cooperation.
3. Ireland's cybersecurity is managed by the National Cybersecurity Centre. Cyber warfare forces are stationed in the Communications and Information Services Corps of Irish armed forces. Cooperation with NATO provides a good basis for the development of cyber warfare also in the future.
4. Ireland is slightly below the European average when it comes to cybercrime. In 2021, one in three SMEs reported having been the victim of some kind of cyberattack or crime, or such an attempt. However, the security of data centers is not particularly threatened by it.

In this millennium, Ireland has seen the emergence of the largest concentration of data centres in Europe. American IT giants, in particular, have been racing to build data centers in Ireland. The reasons for Ireland's popularity have been explained as a skilled IT workforce, a cool climate and wind power that saves energy costs, geographical proximity to the American continent, and, above all, fiscal and economic reasons. Ireland's corporate taxation has been among the lowest in the EU in recent years. The basic rate for corporate taxation in Ireland is 12.5 %, on top of which a premium of a few percent is added for foreign companies, depending on the scale and nature of the business. However, the overall percentage is well below twenty.

American IT giants' interest in moving their data center operations to Europe accelerated with the GDPR

directive in the late 2010s. The GDPR significantly hampered the operations of non-European service providers by requiring that personal data must be stored on EU soil. The storage and processing of personal data outside the EU is possible, but only through special agreements and arrangements. This is how virtually all American data giants such as Microsoft, Google, Meta/Facebook, Amazon, and Apple set up their data centers in Ireland. Today, data center operations are so extensive that their electricity consumption and, with it, their environmental impact have become a cause for concern.

If Ireland has the largest repositories of personal data in Europe, should we be concerned about the cybersecurity of the repositories? The cybersecurity of data centers is primarily the responsibility and control of their owners. As a rule, all large IT companies have implemented the

cybersecurity of their services with high quality. This is made possible by unprecedented cybersecurity budgets. Amazon, Apple, Google, Microsoft, and IBM said last year that they would spend a total of about \$30 billion over the next five years to maintain and develop cybersecurity. On average, this means an annual budget of just over a billion dollars per company.

While the implementation of cybersecurity in data centers is largely in the hands of its owners, the environment also has an impact. Cybercrime is usually rampant where it is easiest to operate and where the overall level of cybersecurity is not high. Ireland ranks only 46th in the ITU International Cybersecurity Index and 28th in Europe.

What is the basis for Ireland's modest performance in cybersecurity? The Cyber Security Index measures a country's maturity in terms of legislation, organisation, cooperation, skills, and technical capabilities. Ireland receives almost full marks in terms of legislation and technical cybersecurity. Ireland's cyber legislation is based on EU directives, which Ireland has transposed into national law effectively and without delay. The technical cybersecurity area targets the activities of the National Cyber Security Centre, and in this area, too, Ireland performs flawlessly in addition to many other EU countries.

At the heart of the organisational area are the national cybersecurity strategy and the management of cybersecurity. Ireland still receives good marks in this area by European standards. In terms of cybersecurity expertise, Ireland is at most within the EU average. Competence measures a country's activity through cybersecurity education and awareness-raising campaigns aimed at different population groups. There is room for improvement in Ireland in the areas of national cybersecurity awareness and cyber hygiene.

Ireland receives the worst rating in the area of cybersecurity cooperation. This section examines public-private cooperation projects, cooperation between different public administration organisations, and international cooperation and information exchange agreements. Indeed, in 2021, Ireland established a national cybersecurity development centre to improve its performance in this area.

Irish cyber activities are led and coordinated by the National Cyber Security Centre. The Centre operates under the Ministry for the Environment, Climate and Communications. The centre's main responsibilities are to secure public administration information networks, to provide cyber training and advice to the private sector and citizens, to maintain and monitor the cyber situational picture, and to solve incidents, i.e. the so-called Computer Security Incident Response Team (CSIRT).



**American IT giants such as Google, Microsoft, Amazon, and Apple have created the largest concentration of data centers in Europe in Ireland. Data center owners have billions in annual budgets to ensure cybersecurity.**

The Irish National Cyber Security Centre works closely with the Irish Defence Forces and, in particular, with the Communications and Information Services Corps (CIS), where the cyber warfare forces and know-how are concentrated. In addition to cyber forces, CIS is responsible for military communications and technical military intelligence.

CIS cyber soldiers receive their training at the army's own training institutes and at Irish engineering universities. Special lines of study focusing on cybersecurity and military technology have been established at the Carlow University of Technology. The Centre for Cybersecurity and Cybercrime Investigation operates at the University of Dublin, working closely with the CIS forces, the Irish Police and the Cybersecurity Centre in training and research.

Ireland is slightly below the European average when it comes to cybercrime. In 2021, one in three SMEs reported having been the victim of some kind of cyberattack or crime, or such an attempt. The European average is 28%. About 12% of the SMEs affected by ransomware had paid a ransom. This figure is double the European average.

The most famous case in Ireland's cybercrime history is the May 2021 attack on the country's healthcare information systems by ransomware. Irish healthcare information systems immediately fell into chaos and paper-based fallback methods were introduced. In addition to disrupting information systems, patient data was stolen and published online. The Irish army's CIS forces were also involved in the investigation of the case and the recovery of the information systems, and it also called in a number of reservists to resolve the situation.

The future development of cybersecurity in Ireland will be underpinned by the support and resources of the EU and NATO. EU legislation is one of the most advanced in the world and the requirements of directives are quickly instilled in national legislation. The Irish armed forces work closely with NATO, participate in NATO cyber warfare exercises, and keep up with developments through NATO cooperation. There is serious cybercrime in Ireland, but the security of data centres is not particularly threatened. ■

**References  
on page  
32**





## OFFENSIVE CYBERDEFENCE

// Timo Rinne

1. Cyberspace is one of the domains of warfare in addition to land, sea, air, and space. Weapons developed for cyberwarfare are mainly custom-built targeted malware.
2. Cyberweapons and ordinary weapons differ in many regards from one another. Cyberweapons are kept hidden before their usage, in order to not reveal their properties and function. Ordinary weapons of war are developed and brought to use in public in order to create deterrence and possibly avoid conflict.
3. Assessing the capabilities of opponents in cyberwar is difficult. Cyber intelligence has to happen within the target's operation environment, in order to gain intel about attack preparations and the development of new weapons. The United States has developed the concept of Hunt Forward operations for carrying out cyber intelligence, and these operations have uncovered for example properties of Chinese and Russian cyberweapons.
4. Cybercriminals and -terrorists utilize second-hand cyberweapons. Once used and therefore revealed cyberweapon is less effective than a previously unknown one.

President Biden's administration released a new U.S. cybersecurity strategy in early March. In the American style, the strategy is built on a few "pillars" that define the high-level goals and principles of the strategy. The cybersecurity strategy has five pillars, one of which will accelerate the development of American cyber defense in a more offensive direction.

In its new strategy, the United States names its worst cyber enemies, which are China, Russia, Iran and North Korea. In addition to designated states, cybercriminals are commonly cited as the enemy of the United States. According to the strategy, China's activities are mainly cyber espionage in order to increase its own scientific, economic, and ideological influence globally. Russia's goal is to disrupt the critical infrastructure of Western powers, use the Internet to spread disinformation, and support its current military activities against Ukraine with cyberattacks. Iran has a geographical focus, in its operations to disrupt the United States and its partners through cyberspace it mainly focuses on the Middle East region. North Korea's main purpose is to raise funds for the country, and in particular for its nuclear weapons projects, through cybercrime.

According to the second pillar of the cyber strategy, the United States fights its cyber enemies by offensive means. According to the "Disrupt and Dismantle Threat Actors" pillar, the United States is actively seeking to undermine the cyber capabilities of its enemies. In addition to actual cyberattacks, the measures may include diplomatic and economic actions, information influencing, and military force. Thus, according to the strategy, it is possible that the United States may even physically destroy elements related to the adversary's cyber activities.

Offensive cyber warfare is not new to US doctrine. The development began as early as the early 2010s when President Obama's administration defined a then-still complex process that could result in cyberattacks targeting other states or cybercriminals. The threshold for cyberattacks has been lowering year after year and it became significantly easier to launch an attack in 2018 after President Trump's administration defined an even faster process to launch the attack.

Malware is one of the basic tools of cyber warfare. While the enemies of the United States use cybercriminals, namely APT groups, to make weapons, the NSA and now also the Cybercommand unit of the US Army operate

as US cyberweapons factories. Malware made for cyber warfare is almost invariably based on zero-day vulnerabilities, so they require a lot of time and resources to manufacture.

The offensive cyber strategy of the United States has also given rise to a conflict prevention strategy called "Defend Forward". The concept was first introduced in the writings of US Cybercommand, the U.S. Center for Cyber Warfare, back in 2018. Defend Forward means fighting a cyber enemy and cyberattacks even before they materialise, and not only after the attack has been detected in its target. The concept has radically changed cyber defence from reactive to proactive.

The aim of the defend forward concept is to change the behaviour and intentions of the attacker in such a way that it potentially abandons the cyberattack already at the planning stage. In practice, this goal can be achieved through various proactive countermeasures, all of which require effective cyber intelligence and clarification of the attacker's intentions.

Once an observation has been made of a possible cyberattack planned by the enemy and its target has been understood, the protection of the target can be strengthened, and the risk of the attacker being caught can be significantly increased. When the operation is successful, the attacker no longer sees the target as an easy goal but understands that more time and resources are needed to carry out the operation, causing the attacker to retreat or at least have to change his plans.

Another possibility is to undermine the benefit of a cyberattack. The U.S. cybersecurity strategy specifically mentions measures to combat financial crime to make the use of cryptocurrencies more difficult. Cryptocurrencies like Bitcoin are practically the only chance for cybercriminals to turn the outcome of, say, a ransomware attack into a financial return. Making it more difficult to use cyber currencies aims to prevent ransomware attacks and increase the risk of criminals being caught.

NATO, too, is increasingly changing its cyber defences in an offensive direction. Cyber warfare itself is still in the development phase of NATO's operations. In 2008, NATO established a NATO Cyber Defence Centre of Excellence in Tallinn and has been studying cyber warfare for a long time. It wasn't until its 2016 General Assembly that NATO recognised cyberspace as one of the operating environments for warfare, in addition to land, air, and sea. Soon after, NATO established the Cyber Operations Center (CyOC) to coordinate its cyber defence.

In defensive cyber warfare, NATO countries cooperate closely, share threat intelligence in order to improve situational awareness and participate in cyber defence through NATO's Cyber Operations Centre. When it comes to carrying out cyberattacks, cooperation or

coordination is not so close. The capabilities of NATO countries to manufacture cyber weapons and carry out attacks vary greatly. In the early 2020s, only half of the thirty NATO countries reported having or developing offensive cyber capabilities (OCO, Offensive Cyberspace Operations). For cyberattacks, NATO has developed a strategy for independent action by member states, known as SCEPVA (Sovereign Cyber Effects Provided Voluntarily by Allies).

The SCEPVA strategy allows member states to independently develop and use offensive cyberweapons, such as malware. The strategy gives a NATO country three options for action to carry out a cyberattack; 1) share information about the malware and its impact among NATO countries prior to the attack, 2) notify NATO in advance of the cyberattack without revealing the details of the cyber weapon, or 3) carry out the cyberattack completely independently and without prior information to NATO.

The SCEPVA strategy is based on a number of specific features related to cyber warfare. Cyber weapons are disposable, meaning that a cyber weapon based on the same vulnerability cannot be used a second time, as the target's security programs are updated quickly once the vulnerability is discovered. In most cases, a member state that has developed a cyber weapon wants to choose its use independently and does not hand over the cyber weapon or precise information about its operating principles to be coordinated by NATO.

The development of malware and its features must be kept strictly secret before an attack is carried out. In the worst case, the exposed malware code can be used against its author, as has often happened sooner or later after the malware has been exposed. The third peculiarity relates to the differences in capabilities between NATO countries in the development of cyber weapons. About half of the NATO countries are capable of developing cyber weapons, and even within these there is a wide range of know-how, and there is not necessarily a desire to actively share this know-how with other member states.

Cyber defence is undergoing a drastic shift in the offensive direction. The United States and its key adversaries have been developing and using cyber weapons for years, but their use is now increasingly being included in cybersecurity strategies. In addition to aggressive attack action, preventive strategies such as Defend Forward have been developed, which have also been applied to the business world. As the cyber capabilities of NATO countries level out, the alliance's offensive cyber activities can also be coordinated more effectively. ■





## INTERNATIONAL COMPETITION FOR ARTIFICIAL INTELLIGENCE TECHNOLOGY

// Timo Rinne

1. Artificial intelligence applications enhance the services of consumers, businesses, and public administrations in many different situations. Self-learning algorithms bring many efficiency benefits and automatic decision-making can also be used in military applications.
2. Artificial intelligence can be used for both cyberattacks and cyber defence. In cyber defence, the greatest benefit is currently achieved in the automatic processing of alerts generated by surveillance systems.
3. The United States and China are the world's leading countries in the development and utilisation of artificial intelligence. In the international comparison, Finland ranks 13th best among the Nordic countries. Russia is only ranked 32nd in international statistics, but the statistics do not necessarily give a completely correct picture of Russia's abilities. In addition, Russia relies on China for all its high-tech needs, including artificial intelligence.
4. Artificial intelligence remains an important aspect of the competition between states for economic, political, and military leadership. However, artificial intelligence has become commonplace in recent years and no longer has the same special status as it did a few years ago

In recent months, artificial intelligence applications have reached consumers. ChatGPT has delighted its experimenters by solving even complex tasks and by writing poems on a desired topic or compiling a convincing resume for a job search. ChatGPT is one of the first artificial intelligence services implemented for consumer use and with an easy user interface.

However, AI has been working with consumers in the background for years. Manufacturers of mobile devices and services have used AI-based algorithms for functions that improve their performance without the consumer being aware of it. Pattern recognition and automatic focus and exposure of phone cameras work with the help of artificial intelligence. The user unconsciously teaches the AI applications by using social media services, in which case they produce, for example, better-targeted content for the user.

Many public administration services and businesses also benefit from the use of artificial intelligence. X-ray camera software learns to recognise cancerous tissues automatically, agricultural production can be enhanced by predicting the effects of weather phenomena, and the efficiency of transport services can be improved by optimising routes according to traffic volumes and weather conditions.

Automatic decision-making can be delegated to artificial intelligence in many different situations. If a high-quality AI application indicates that the result is almost certain, it is not necessarily worth wasting human judgment time on a low-risk decision, because the application can make the decision directly. Artificial intelligence can also be applied to military applications to speed up situational decision-making.

AI technology is an important enabler of the future also in cybersecurity from the point of view of both cyberattacks and cyber defence. AI can be used for cyberattacks mainly in three ways. The first is the use of artificial intelligence in the reconnaissance phase of the target. The AI-based OSINT application quickly learns the target's cyber security practices. For example, how often and with what delay the systems are updated, the utilisation rate of the target system and its fluctuations, and the timing of changes in access rights are important information in timing a cyberattack and finding the weakest target.

Another way is to equip the malware itself with an AI algorithm so that after entering the target system, it can learn the things described above and carry out the attack at the most opportune moment. The third way is to manipulate the AI systems in the target system during their AI training phase. The functionality of artificial intelligence is currently based on teaching the system using a defined data set. If the attacker can manipulate the

data used to teach the system, it can make the target's artificial intelligence system work the way the attacker wants.

In cyber defence, AI is of course used in the opposite way, i.e., to identify and anticipate the special features of the attacker's activities. In addition, artificial intelligence can significantly improve the reliability of cybersecurity alerts. Static rules often produce a significant number of false positives. AI can be used to learn the characteristics of false alarms and highlight only the most important observations. The natural language processing system, NLP, is a part of artificial intelligence that can be used to predict cyberattacks by analysing the text and the pre-attack phenomena or, for example, emotional states.

In 2022, around \$430 billion was spent globally on the development and implementation of AI technologies and services. The actual AI market, i.e., customer investments and spending on artificial intelligence implementations, is smaller than this, just over one hundred billion dollars. The size of the market is about half compared to the global cybersecurity market. The industry is still very much in the product development phase, but already in 2025, the revenue of the AI market alone is estimated to be one hundred billion.

Various indexes have been developed to compare the AI capabilities of states. Generally, the measures of such indices are related to legislation, infrastructure readiness, public and private sector investments, technology usage in applications, the number of research and product development projects, etc. Several actors, from IBM to Stanford University, have developed their own indices for assessing the AI capabilities of countries.

One of the most respected indexes is the Global AI Index of the British Tortoise Community think tank. According to it, the overwhelming number one is the United States, an equally clear second place is China, and the third place, very close to each other, are Great Britain, Canada, Israel, Singapore, and South Korea. Finland is in 13th place in the overall statistics, followed immediately by Denmark, and among the other Nordic countries, Sweden is in 19th place, Norway 25th, and Iceland 37th.

The American position is easy to understand. The success of the IT giants operating in the country has created for the United States an undisputed position in all developments related to IT technology. The United States currently has an overwhelming leadership position in research and product development and in the commercialisation of AI. Also, most of the world's AI experts currently work in the United States. The United States clearly lags behind the rest of the world in the readiness of regulations governing artificial intelligence, public administration strategies, and the nation's readiness to put the technology to good use. ➡



China's second place is equally clear in almost all areas. It even surpasses the United States in infrastructure readiness for AI use. This means, for example, the development of telecommunications infrastructure and especially 5G networks, as well as the spread of computing capacity needed by AI in the form of supercomputers and these networks. In the field of AI expertise, China somewhat surprisingly lags many other countries. Instead, India ranks second in this area, right after the United States.

But where is Russia? It is found only in the 32nd place in the overall statistics. Its ranking in all sub-areas is in line with the overall ranking, but Russia ranks in the top six in state administration strategies and development programs. So, Russia invests in research, product development, and commercialisation of AI, but the results, at least so far, have clearly lagged other major powers in the world if Russia can be considered as such.

Russia's weak result in the international comparison does not say all when it comes to cybersecurity. Russia's AI investments are most obviously focused especially on state administration projects and military technology, in which case their readiness may be significantly higher than what public statistics show. In this area, Russia also relies on China, which has supported it in many high-tech areas, for example in the introduction of 5G technology.

Assessing the technological capabilities of authoritarian states is generally challenging. Public funding is not open, the state regulates scientific publishing, and the

country's top expertise is not brought to commercial applications, but the resources are concentrated for the state administration's own purposes. Thus, in China and Russia, for example, the development may be further along than what public sources suggest.

However, the biggest challenge of authoritarian states in the development of AI is the lack of top experts. Both China and Russia produce their own experts, but the societal order and conditions of these countries do not attract top foreign experts to the country other than perhaps for ideological reasons. A Western society that emphasizes individual freedom and the opportunity to commercialise innovations is more attractive than closed societal models in academic circles. For these reasons, the United States has succeeded in creating centers of excellence like Silicon Valley.

AI is seen as one important area in the struggle between countries for economic, political, and even military influence. Artificial intelligence will play an increasingly important role in all information technology applications. States compete for leadership positions in the development of AI and invest in research and utilization of the technology. At the same time, the role of artificial intelligence is becoming commonplace and has become a part of everyday life. AI no longer has the special position it had a few years ago among other technologies. In cybersecurity, the use of AI is still in its growth phase, and therefore its management is important for cyber market operators and in cyber defence. ■

## REFERENCES

### NIS2 AND CER – TOWARDS GREATER CYBERSECURITY AND RESILIENCE

<https://www.nis-2-directive.com/>  
[https://www.europarl.europa.eu/thinktank/en/document/EPRS\\_BRI\(2021\)689333](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333)  
<https://www.enforcementtracker.com/>  
<https://valtioneuvosto.fi/hanke?tunnus=SM047:00/2022>

### COUNTRY ANALYSIS – IRELAND

<https://www.ncsc.gov.ie/>  
<https://www2.hse.ie/services/cyber-attack/>  
<https://www.military.ie/en/who-we-are/army/army-corps/cis-corps/>  
<https://www.gov.ie/en/consultation/a2020-national-cyber-security-strategy-2019-2024-mid-term-review-consultation/>  
<https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>  
<https://edition.cnn.com/2022/01/23/tech/ireland-data-centers-climate-intl-cmd/index.html>

### OFFENSIVE CYBERDEFENCE

<https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>  
[https://www.hoover.org/sites/default/files/research/docs/deeks\\_webreadypdf\\_0.pdf](https://www.hoover.org/sites/default/files/research/docs/deeks_webreadypdf_0.pdf)  
 Jensen, M. (2022). Five good reasons for NATO's pragmatic approach to offensive cyberspace operations. *Defence Studies*, Vol 22 n:o 3, pp. 464-488.  
[https://www.nato.int/cps/en/natohq/topics\\_78170.htm](https://www.nato.int/cps/en/natohq/topics_78170.htm)  
 Goldsmith, J (ed). (2022). *The United States' Defend Forward Cyber Strategy: A Comprehensive Legal Assessment*. Oxford University Press.

### INTERNATIONAL COMPETITION FOR ARTIFICIAL INTELLIGENCE TECHNOLOGY

[https://www.business-standard.com/article/technology/global-artificial-intelligence-spending-to-reach-434-bn-in-2022-report-122022000195\\_1.html](https://www.business-standard.com/article/technology/global-artificial-intelligence-spending-to-reach-434-bn-in-2022-report-122022000195_1.html)  
<https://www.tortoisemedia.com/intelligence/global-ai/>  
<https://aiindex.stanford.edu/report/>  
<https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges>  
[https://www.researchgate.net/publication/343328470\\_Artificial\\_Intelligence\\_for\\_Cybersecurity\\_A\\_Systematic\\_Mapping\\_of\\_Literature](https://www.researchgate.net/publication/343328470_Artificial_Intelligence_for_Cybersecurity_A_Systematic_Mapping_of_Literature)



**TIMO RINNE**

- ' Cybersecurity Expert
- ' Doctor of Science in Economics
- ' CISSP (Certified International Information Security Professional)
- ' CISA (Certified Information Systems Auditor)





A PASSION  
FOR A SAFE  
CYBER WORLD



Cyberwatch Finland is a strategic cybersecurity consultancy house that provides professional services for companies and other organisations by strengthening and developing their capabilities to protect and defend their most significant assets.





## Our Mission: Make Cybersecurity a Business Opportunity

Cyberwatch Finland serves companies and other organisations by strengthening and developing their cybersecurity culture.

Increasing regulation improves cybersecurity in all organisations, but compliance with the minimum requirements is not enough in the ever-tightening competition. A high-class cybersecurity culture is a competitive advantage and creates new business opportunities.



Our strength is a unique combination of profound know-how and extensive experience.

Our team of experts consists of versatile competence in strategic cybersecurity, complemented by extensive experience in management, comprehensive security and operations in an international business environment.

Our experts know how to interpret and present complex phenomena and trends in the cyber world in an easy-to-understand format. Our work is supported by advanced technology platforms as well as modern analysis tools.



“We help our clients stay up-to-date and consistently develop a cybersecurity culture. At the same time, we are building a more sustainable and safer world together”

Aapo Cederberg, CEO and Founder, Cyberwatch Finland



## OUR SERVICES



### Management Advisory Services

We are experienced and trusted experts and management advisors. We give support in comprehensive security, cybersecurity, internal security, and third party risk management. Our working methods include, for example, theme presentations, background memorandums, workshops, and scenario work.

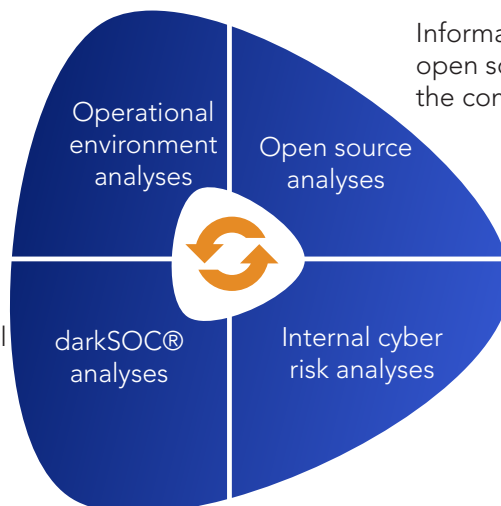


### A Comprehensive Situational Picture

A comprehensive situational picture of cybersecurity is created with the help of the modular service developed by Cyberwatch Finland, for which the necessary data is collected using numerous different methods.

By analysing the operational environment from different perspectives, an overall insight is formed about the events, phenomena, and trends affecting the organisation.

The dark and deep web data is collected non-stop at 9 Gb per second, from servers located all around the world.



Information collected from open sources complements the comprehensive picture.

With the help of internal cyber risk analysis, a comprehensive picture of the organisation's insider threats, and other risk factors are formed.



# OUR SERVICES

## Reviews

Cyberwatch's analysis team constantly monitors the cybersecurity operational environment by collecting and analyzing information about events, phenomena and changes in the cyber world. The situational picture is produced by regular situational reviews.



### Weekly Review

Weekly reviews introduce the current events of the cyber world and are declarative in nature. The focus of the weekly review is identifying phenomena and trends and placing them in a relevant framework.

The weekly reviews serve as the basis for the monthly and quarterly reviews and the annual forecasts that are based on this data.

With the help of the weekly reviews, it is possible to get an up-to-date understanding of the significant events in the cyber world to support decision-making. The weekly reviews are published 52 times a year in Finnish and English.

### Monthly Review

The monthly review sums up, expands, and puts into context the themes and phenomena discussed in the weekly reviews.

The monthly review describes of the development of phenomena, focusing on different perspectives of hybrid influencing.

With the help of the monthly review, it is possible to get a deeper insight into how the events of the cyber world affect society and the operational environment.

The monthly reviews are published 12 times a year in Finnish and English.

### Quarterly Review

The quarterly review focuses on the most significant events in the cyber world during the review period. It monitors the effects and developments of the phenomena in the longer term. The quarterly review evaluates future scenarios and development trends and is predictive in nature.

The quarterly review includes a country analysis, which examines the assets, threats, and cybersecurity solutions related to the cyber activities of an individual state.

The quarterly reviews are published 4 times a year in Finnish and English.



### Cyberwatch Magazine

Cyberwatch magazine is a digital and printed publication, in which experts from both inside our organisation and from our professional network explain about the current events of the cyber world, the development of technology and legislation, and their impacts on society, organisations and individuals.

### Special reports

We produce reports and overviews on customised themes, for example from a specific industry or target market: assessments of the current state, threat assessments, analyses of the operational environments, and forecasts.

## OUR SERVICES

### darkSOC® – the Dark and Deep Web Analysis

With darkSOC® -analysis, we examine and report your organisation's profile and level of exposure in the dark and deep web. Data is collected non-stop at 9 Gb per second, from servers located all around the world. The analysis reveals organisation's cybersecurity deficiencies, data breaches, and other potential vulnerabilities. With the help of analysis, you get an overview of what the organisation looks like from the cybercriminal's perspective.

We prepare a written report from the analysis, in which we highlight key findings to support management's decision-making. The report also includes a more detailed presentation of the findings. We also give recommendations on immediate corrective actions and strategic-level development targets.



### The Benefits of darkSOC®



Increases cyber intelligence capabilities



Anticipates constantly changing cyberworld



Complements company's cybermaturity



Serves as a forensic investigation tool



Supports organisational strategic decision-making



Complements strategic cyber situational picture



Discovers vulnerabilities and weaknesses



Facilitates cyber strategy process



## OUR SERVICES

### Analysis



#### The Surface Web Analysis

We form an external view of your level of cybersecurity in the surface network and compare your position with other organisations in the same industry. Our analysis is based on the platform of our global partner SecurityScorecard, whose data is based on a trusted, transparent classification method and data collected from millions of organisations. Based on our analysis, we make recommendations on corrective measures and draft a road map for their practical implementation in your organisation.

Powered by



#### The Open Source Analysis

We produce analyzes based on open sources on the topics you choose. We use advanced digital tools with which we search for information from public free and commercial sources as well as from various media and social media platforms. We refine the data into a form relevant to the goals of the analysis.



#### Internal Cyber Risk Analysis

With the help of an internal cyber risk analysis, it is possible to form an overall picture of insider threats and other risk factors related to your organisation's cybersecurity.

We analyse the up-to-dateness and comprehensiveness of your organisation's cybersecurity policies, guidelines, instructions and other documentation. In addition, we interview the selected management members and other key personnel.

As a result of the analysis, you will have an image of the balance between your organisation's operation and the internal guidelines and external regulations that guide it, as well as a road map for developing the operation.



## OUR SERVICES

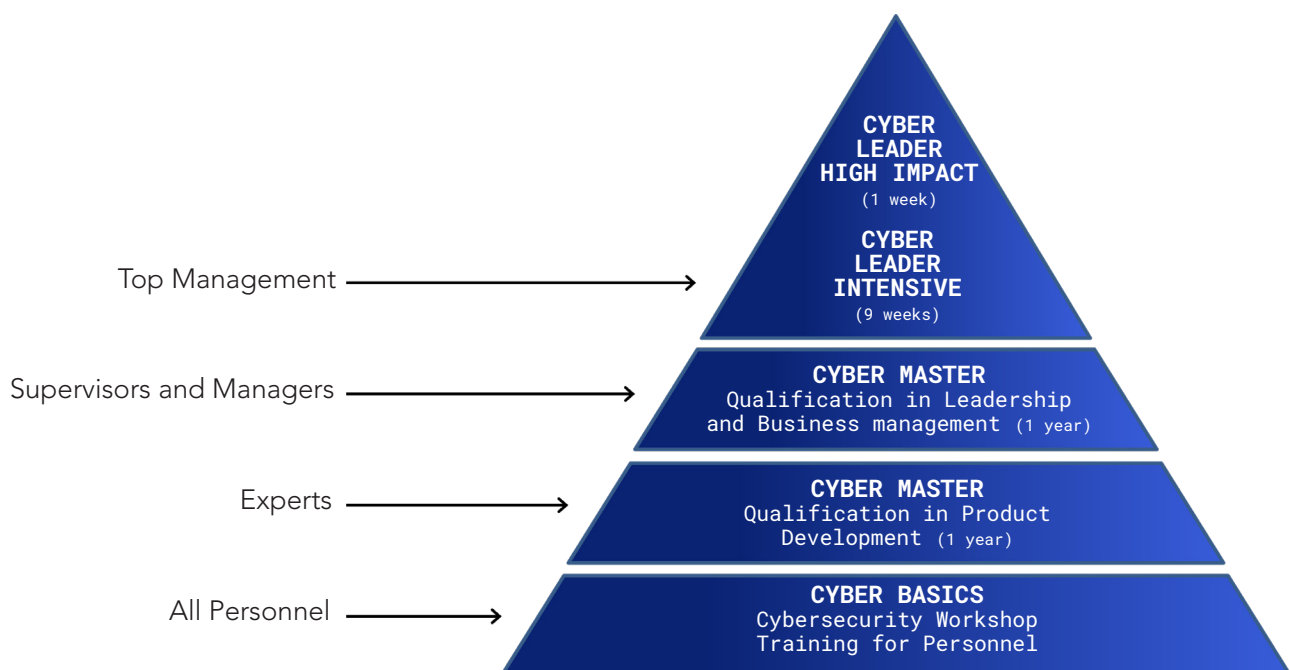
### Training and Competency Development

We produce training for the Cyber Master specialist vocational qualification in co-operation with the Management Institute of Finland MIF Oy.

Currently, in the programs, it is possible to complete the Cyber Master qualification in leadership and business management as well as in product development.

We also provide tailored training for your organisation, which helps to strengthen your organisation's cybersecurity skills and helps you to be better prepared for the challenges of the digital operating environment.

Our all training offering consists of modules, from which student or organisation can choose the options according to their needs.





## OUR SERVICES

### Forensic services

#### Investigations and Special audits

We support organisations in all cases of misconduct related to their activities in investigating suspicions and violations. We have extensive experience in corporate investigations and special audits.

Our expert experience consists of, among other things, numerous frauds and corruption schemes as well as different types of violations of the code of conduct.

#### Background checks

We review the reputation, integrity and operating history of companies and related individuals by collecting and analysing information to support our client's decision-making in various situations, such as M&A situations or dealing with third parties such as contractors and service providers.

#### Risk Management Services

We help your organisation to identify, assess and manage risks that may affect your operations.

In addition to our experienced subject matter experts we utilize modern risk management technologies.

#### Anti-Money Laundering (AML)

We support your organisation in fulfilling the obligations of the Anti-Money Laundering Regulation.

Know Your Customer (KYC)  
Customer Due Diligence (CDD)

Supporting in prevention of money laundering and terrorist financing:  
policies, programs, risk assessments.



### Cyberwatch eWHISTLE Channel

Cyberwatch eWHISTLE whistleblowing channel is a responsible, secure, and privacy-secured whistleblowing channel with a clear environment for processing, investigating, and making decisions. The legislation compliant eWHISTLE offers ready-to-go packages, or a service tailored to your needs

We plan and implement the whistleblowing channel from the beginning to the very end. Our experts help you create a compliant report management and investigation process and the required documentation related to the whistleblowing channel. After the implementation of the service, we receive reports, assess them, and propose further actions to you. If requested, we support you in investigating the incident.

The technical platform of the eWHISTLE is produced Easywhistle Oy. The system is easy to access, data secure and user friendly. The service is available in all needed languages. The channel fulfils the GDPR-requirements, and the servers are located in the EU.



# FOR A BETTER DIGITAL FUTURE

Technology and digitalisation are changing people's behaviour, business practices, and market dynamics. Cyber Security Nordic will explore cybersecurity from the perspectives of both businesses and public administration. The speeches will cover topics such as the impact of digitalisation on democracy and technology regulations, the increasing diversity of cyber-attacks, and approaches to risk management for critical functions of companies and societies.

**Read more and register at [cybersecuritynordic.com](https://cybersecuritynordic.com)**



**7-8 November 2023**

Helsinki Expo and Convention Centre

## KEYNOTE SPEAKERS

**Max Schrems**

Lawyer, author, privacy activist  
NOYB – European Center  
for Digital Rights



**Valentino De Sousa**

Principal Director,  
Europe Cyber Threat Intelligence Lead  
Accenture Security



**Colm Murphy**

Senior Cyber Security & Privacy Advisor  
Global Cyber Security & Privacy Office,  
Huawei



**Henna Virkkunen**

Member of European Parliament  
(EPP)







# A PASSION FOR A SAFE CYBER WORLD



## Contact

Cyberwatch Oy  
Nuijamiestentie 5C  
00400 Helsinki Finland

[aapo@cyberwatchfinland.fi](mailto:aapo@cyberwatchfinland.fi)  
[ake@cyberwatchfinland.fi](mailto:ake@cyberwatchfinland.fi)