ISSN 2738-7097 https://doi.org/10.11610/cybsec06

British Embassy Sofia

Cybersecurity Newsletter

IICT Institute of Information and Communication Technologies

UK – BG Partnership in Cyber Security for SME and Organizations

Newsletter March 2021 Number 6

Aims and Scope

Contents:

The current online newsletter is focused on topics related to the Higher Education in Cybersecurity. The education and training areas are specifically addressed within the cybersecurity related initiatives of the European Commission and Europe as a whole.

The education and training programmes and courses are among the main topics of the Cybersecurity Atlas project and its online platform which maps the institutions and their capabilities within the proposed European Cybersecurity Taxonomy. The Regulation on establishing the European Cybersecurity Industrial, Technology and Research Competence Centre (R630) emphasises specifically on the importance of education and training as key assets for cybersecurity policy implementation. The education, training and cybersecurity skills are also among the topical issues within the process of establishing the European Cyber Security Competence Community (CCC).

The most relevant initiative to the Higher Education in Cybersecurity is the creation of the Cybersecurity Higher Education Database (CyberHEAD) by the European Union Agency for Cybersecurity (ENISA). The Database is presented briefly at the first section of the newsletter. The data about Bachelor`s and Master`s degree programmes in cybersecurity management are presented and the need of different capabilities is identified. The CONCORDIA project online mapping tool for training courses is also presented.

The approach of the University of National and World Economy (UNWE), Sofia, Bulgaria, to deliver and integrate different capabilities into the Cybersecurity Management Master`s degree programme is introduced. The profiles of higher education institutions and how to facilitate the cooperation and integration are considered.

The edition includes a brief report on the online interactive training event dedicated on the role of Chief Information Officer (CIO) for the Bulgarian Academy of Sciences and major Bulgarian Universities led by a Professor of Systems Security at Coventry University.

The certification institutions and national educational funds in the UK and Bulgaria are presented.

As in the previous issues of the newsletter, links to online news (and their sources) and events are provided. Special attention is given to the updates of the Bulgarian National Cyber Security Strategy.

Issue Editors: **Assoc. Prof. Georgi Penchev**
Assoc. Prof. Konstantin Poudin
Chief. Asisst. Atanas Dimitrov

Issue Focus: Integrating Education Capabilities in Cybersecurity Management Programmes

Assoc. Prof. Georgi Penchev Department of National and Regional Security (DNRS), UNWE, Sofia, Issue Editor

Assoc. Prof. Konstantin Poudin, DNRS, UNWE, Sofia, Issue Editor

Chief Assist. Atanas Dimitrov, DNRS, UNWE, Sofia, Issue Editor

The main source of information for Cybersecurity Education Programmes is the online Cybersecurity Higher Education Database (CyberHEAD). The Database is established and maintained by the ENISA. This effort is not a single act of gathering and disseminating data. Several initiatives and documents related to the EU Cybersecurity Education Policy can be considered as a background for the CyberHEAD establishment (according to the ENISA website publication):

- Publication by the European Commission of the first EU Cybersecurity Strategy in 2013. The Commission invited the member states to increase their education and training efforts around network and information security (NIS) topics as well as to participate to voluntary certification programme to promote advanced skills and validate the competences of IT professionals.
- The Joint Communication 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU', issued in 2017 by the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy declared that the "effective cybersecurity relies heavily on the skills of the people concerned".
- The whitepaper on "Cybersecurity Skills Development in the EU" focuses on the state of the cybersecurity education system and difficulties in attracting more students to cybersecurity studies. It looks for ways how the number of graduates with relevant cybersecurity knowledge and skills can be increased.

The Agency also developed the report on Cybersecurity Skills Development in the EU in order to address the status of the cybersecurity education system. The report identifies gaps and shortages in educated and trained workforce. The analysis is based on the experience of four countries – Australia, France, the United Kingdom and the United States.

The CyberHEAD can also be considered as a tool supporting the development of the European Cybersecurity Skills Framework which aims to create a common understanding of the roles, competencies, skills and knowledge used in all aspects of cybersecurity – the individuals, employers, etc.

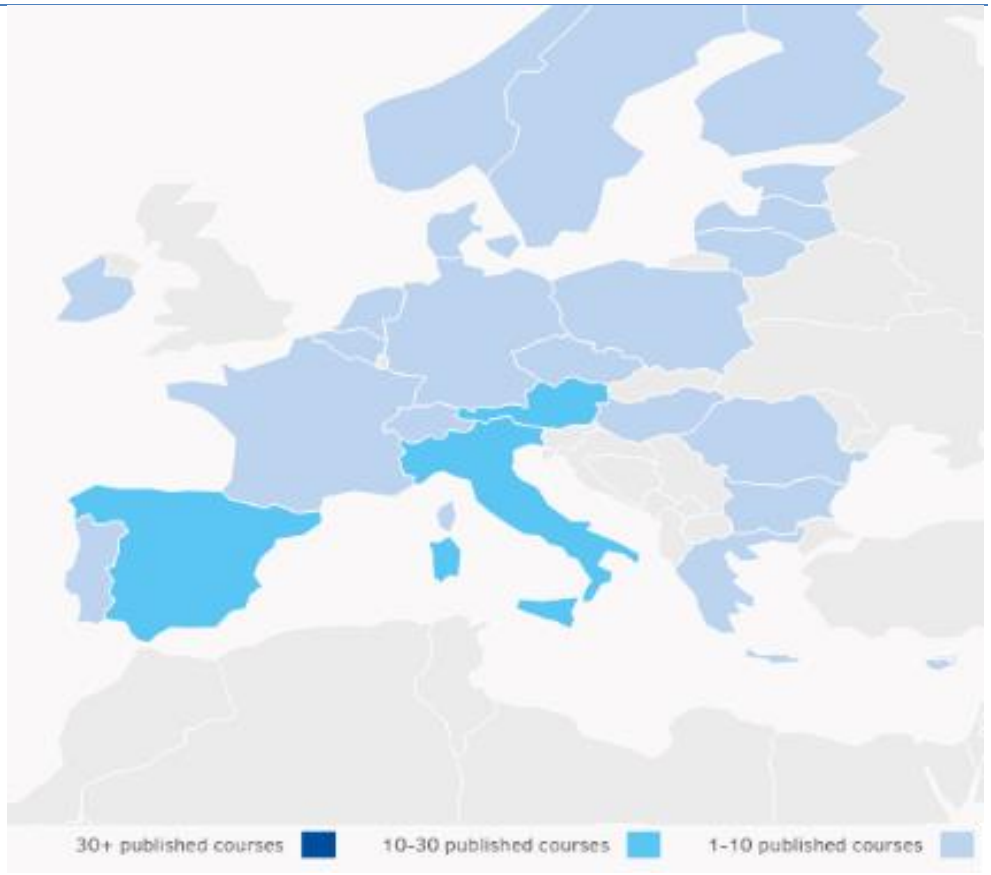
The Cybersecurity Curricula 2017 developed by the Joint Task Force on Cybersecurity Education is used as main reference for the cybersecurity education programmes in CyberHEAD database.

In general, the Cybersecurity Higher Education Database is an online platform for registering the higher education cybersecurity programmes. The registration is validated by the ENISA.

The purpose of the Database is defined as follows: 'It has been the main point of reference for all citizens looking to upskill their knowledge in the cybersecurity field. This database allows young talents to make informed decisions on the variety of possibilities offered by higher education in cybersecurity and helps universities attract high-quality students motivated in keeping Europe cyber-secure.'

Since March 2020 130 Programmes across 24 Countries are registered and the site of the platform states that this is 'the largest validated cybersecurity higher education database in the EU and EFTA countries'.

The spatial distribution of registered and validated programmes across Europe is presented on the figure below.



The distribution until the date of the current issue of the newsletter is almost equal with only three countries included into the bracket of '10-30 published courses'.

The requirements for registering, of course, are as follows:

- For **Bachelor's degree**: at least 25% of the taught modules are in cybersecurity topics
- For **Master's degree**: at least 40% of the taught modules are in cybersecurity topics
- For **postgraduate specialization programme**: at least 40% of the taught modules are on cybersecurity topics and the programme has a minimum of 60 ECTS.
- For **PhD degree**: the dissertation must be on a cybersecurity topic.

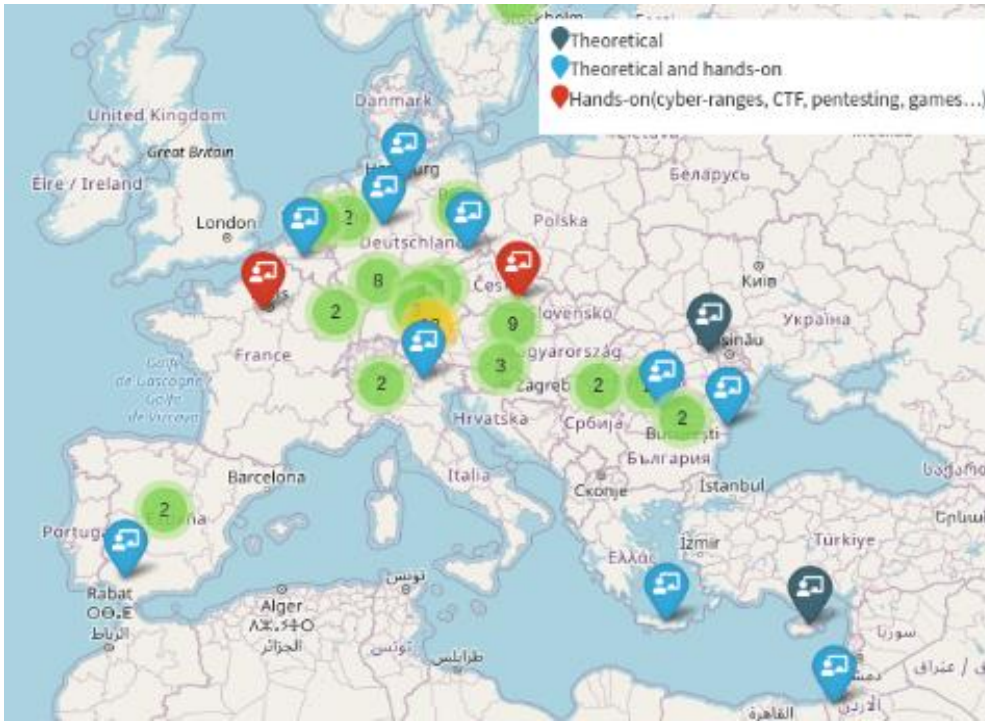
The most interesting data recorded by the Database are the Number of European Credit Transfer and Accumulation System (ECTS) as well as the ECTS dedicated to course's disciplines as percentage of total amount of course's ECTS. Having this data, we can compare the management courses and programmes and other programmes oriented more to the technical cybersecurity aspects.

The CyberHEAD do not provide options for downloading the full dataset. We experiment with keyword 'management' and the search returns 24 masters' and bachelors' programmes related in more or less to the Cybersecurity, Risk and Technology management.

The National Cybersecurity Centre (NCSC) is the certifies cybersecurity bachelors' and masters' programmes at the UK. The information about programmes is provided as a list, which can be found online here.

Courses and trainings for professionals

The four pilots project which are in the core of establishing Cybersecurity Competence Community have also strong focus on education – for example ECHO Project is focusing on Cybersecurity Skills Framework, Taxonomy, training and certification. CONCORDIA area of is closely related to education of cybersecurity professional.

	The four pilots projects are presented in previous newsletter #4  CONCORDIA also maintains a web platform for registering and mapping the courses and trainings for professionals across Europe. The figure of current registered courses of the platform is presented above. More about the CONCORDIA map of courses can be found here and here.
Organisations and Institutions Profiles	The current social environment is characterised by the dynamic processes of digital transformation in all spheres. People's daily lives are unthinkable without the use of computer technologies and communication networks. Each of us regardless of the reason – work, education, or just entertainment spends more and more time in cyberspace, especially in a pandemic. This intensive process of virtualisation of our everyday life is accompanied by different security challenges. A lot of cyber treats have arisen and exist nowadays. Affecting networks and computer systems they have the capacity to violate cyber resilience at individual, organisational or national level causing huge material and moral negative consequences. Cyberspace has become a field of warfare and different crimes. That`s why the development and maintenance of adequate counter capacity is crucial. All this determines the importance of cybersecurity education and training as one of the ways to develop such capacity. The goal of cybersecurity management education is to provide students with knowledge related to the essence and particularities of cybersecurity. The students also develop skills to analyse the internal and external environment of the entities, choose and implement approaches to avoid the cyber treats and to guarantee cyber resilience of their organisations. The education contributes to development of a relevant cybersecurity culture – a way of environmental perception, a way of thinking and acting in regard to the existing cyber threats and dangers, based on cybersecurity awareness.
Integrating Capabilities Example	The cybersecurity is a complex matter and an overlap between several spheres which could be seen, such as: management, organisational behaviour and psychology, law-enforcement, policy-making, IT, etc. That`s why the cybersecurity management education has various aspects and covers different disciplines.

The UNWE, Sofia, Bulgaria has two years of experience in the field of cybersecurity education. The curriculum for the UNWE Master`s Degree Programme in Cybersecurity Management shows this diversity of courses that such a programme could include. The duration of education is two semesters. The curriculum includes:

- Fundamentals of Cybersecurity;
- Industrial Control Systems (ICS) and SCADA;
- Legal Aspects of Cybersecurity;
- Crisis Management and Cybersecurity;
- Cryptography and Cybersecurity (presented within the first semester)

and

- AI and Cybersecurity;
- Fundamentals of Cyber Intelligence;
- Good Practices in the Cybersecurity;
- Internet Security (presented within the second semester).

The complexities of cybersecurity require the involvement of lecturers with different knowledge and skills from various organisations such as: universities and research centres, business organisations, government authorities, etc.

The cybersecurity management education requires the presence of discipline(s) related to the management science in the curriculum. It is due to the fact that ensuring the cybersecurity, as all other aspects of security, requires the performance of managerial activities within the four basic management functions as follows:

- planning – setting goals related to the building up of cybersecurity and decide how to do the best for achieving them);
- organising – determining how to do the best to group the activities and resources for cybersecurity;
- leading – motivating the staff to work for the best interest of the organisation in the context of the set cyber security goals;
- controlling – monitoring and correcting ongoing activities to facilitate achievement of cyber security goals.

The participation of lecturers having knowledge and experience in the field of management is essential, e.g. university professors and government officials at political and strategic level participate in the education process.

Cybersecurity requires participation of experienced IT specialists familiar with the functioning of computer technologies and the specifics of communication networks, knowing their vulnerabilities and the ways of protection.

The cybercrimes counteractions fully engage the government attention. Part of the duties of law-enforcement bodies and specialised agencies are related to the prevention, detection and response of cyber treats and cyberattacks.

The preparation regarding the legal aspects of cybersecurity is also very important. Cybercrimes violate the rules established by the state. Each user living and working in the cyberspace is exposed of various treats violating some of his/her fundamental rights as a human being and as a citizen. The knowledge about the legal aspects is very important.

The leading department for Master`s Degree Programme in Cybersecurity Management at the UNWE is the Department of National

	and Regional Security (DNRS). The Department has more than 30 years of experience organising educational programmes in complex field of defence and security economics and management, integrating educational capabilities from different fields of knowledge. The Cybersecurity Management programme integrates efforts from more than 10 organisations – universities, research organisations, business organisations. The cooperation among organisations can be based on formal or informal agreements. After the organisation agree on cooperation the leading lecturers for the disciplines are appointed. The main focus in such integration are people – they are providers of the capabilities and have to establish well balanced and effective programme team. More about the Master`s Degree Programme in Cybersecurity Management map of courses can be found here and here (both links are in Bulgarian).
How to Facilitate Cooperation	Various forms of interaction could facilitate the cooperation between the organisations and the institutions involved in the cybersecurity education process. Most often the cooperation is based on bilateral agreements of cooperation signed with other national or foreign academic institutions, research centres, international organisations, government authorities and business entities. Facilitating the interactions between parties, the purpose of these agreements is to increase the quality and effectiveness of teaching and research activities through the exchange of academic and non-academic staff, undergraduate and postgraduate students, development of joint bachelor`s and master`s degree programmes, organisation of joint conferences and other scientific events, participation in joint research projects, exchange of experience and academic information, curricula, materials, etc. The UNWE, Sofia, Bulgaria, conducts education for Masters' degree in Cybersecurity Management and has signed agreements of cooperation with the Ministry of Interior of the Republic of Bulgaria, European Commission's Joint Research Centre (JRC) - Brussels, Centre for European University Studies (CEUS) - Vienna, International Atomic Energy Agency (IAEA) - Vienna, United Nations Industrial Development Organisation (UNIDO) - Vienna, etc. The participation in academic alliances and networks is another way to facilitate the cooperation. For example, the UNWE, Sofia, Bulgaria, is a member of ENGAGE.EU - an alliance of leading European universities in business, economic and social sciences, aiming to provide European citizens with the set of skills and competences needed to tackle major societal challenges. The alliance has to exploit the unique synergies of its members elevating existing collaborations to a new dimension under the guidance of a joint strategy and common goals. The UNWE is also a member of the Association of Economic Universities of South and Eastern Europe and the Black Sea Region, the Black Sea Universities Network, the Black Sea and Mediterranean Academic Network and others.
Online Interactive Training on the Role of CIO	On 18 January 2021, an online Interactive Training on the Role of CIO (Chief Information Officer) for the Bulgarian Academy of Sciences (BAS) and major Bulgarian Universities was held. The training was led by a Professor of Systems Security at Coventry University.

The CIO has the ultimate beneficial ownership of information and digital operations. It is also the one that would deliver the digital transformation to the Academy and Universities.

The training was organised as a follow-up of an earlier high-level consultation meeting on the digital transformation and digitalisation strategy development of BAS and Universities.

The Deputy Vice Chancellor and Chief Operations Officer at Coventry University was the consultant at this meeting (SIN project, Dec 2019).

During the CIO training, through an interactive tutorial, the UK Professor held a general session on Coventry University's view about the CIO critical role and function in modern organisations. The following interactive 'Scenario-Based Cyber Exercises' session provided an opportunity for the Bulgarian participants to practise an effective response to potential cyberattacks.

The exercises based on real incidents were designed to build awareness and capacity towards an increased understanding of cyber risks and potential effective mitigation strategies, to build up key skills and agreed responsibilities. The training finished with a feedback on results and conclusion discussion.

The knowledge obtained during the event will be used by Bulgarian participants to develop programmes for training CIO`s at various institutions in the country.

The exercises were part of a research project implemented by the Coventry University, exploring factors that shape cybersecurity decision-making by seeking to understand how people respond to cyber incidents and to provide actionable guidance. The participant responses to hypothetical cyber incidents were scored to give insights into decision-making and response tendencies.

There were Bulgarian participants from a wide range of institutions: Institute of ICT – BAS; Laboratory of Telematics – BAS; Institute of Organic Chemistry - BAS; Technical University of Sofia; Naval Academy Varna; University of National and World Economy; University of Library Studies and Information Technologies; Institute of Public Administration; National Institute of Defence; State e-Government Agency; Ministry of Defence; Ministry of Interior.

This event was a continuation of a great collaboration between SIN Bulgaria and Coventry University and Bulgarian cyber security stakeholders in Academia and University sectors.

Cyber Institutions & Initiatives in UK & Bulgaria

UK National Cyber Security Centre (NCSC)

Launched in October 2016, the NCSC has headquarters in London and brought together expertise from CESG (the information assurance arm of GCHQ), the Centre for Cyber Assessment, CERT-UK, and the Centre for Protection of National Infrastructure.

The NCSC provides a single point of contact for SMEs, larger organisations, government agencies, the general public and departments. We also work collaboratively with other law enforcement, defence, the UK's intelligence and security agencies and international partners.

The activities of The NCSC are defined as follows:

- understands cyber security, and distils this knowledge into practical guidance that we make available to all;
- responds to cyber security incidents to reduce the harm they cause to organisations and the wider UK;

	• uses industry and academic expertise to nurture the UK's cyber security capability; • reduces risks to the UK by securing public and private sector networks. NCSC-certified degrees With so many UK universities offering degrees containing cyber security content, it can be difficult for students and employers alike to assess the quality on offer and to identify the degree that best suits someone's preferred career path. NCSC-certified degrees help: • universities to attract high quality students from around the world • employers to recruit skilled staff and develop the cyber skills of existing employees; • prospective students to make better informed choices when looking for a highly valued qualification.
The National Evaluation and Accreditation Agency (NEAA)	The National Evaluation and Accreditation Agency is a statutory body for evaluation, accreditation and monitoring of the quality in higher education institutions and scientific organizations aiming at the enhancement of their teaching and research, as well as of their development as scientific, cultural, and innovative organizations. The Agency monitors the ability of institutions, their main units and branches to provide good quality of education and scientific research through an internal quality assurance system. The mission of the NEAA is to encourage higher education institutions in assuring and enhancing the quality of education they offer by sustaining high academic standards and good education traditions in Bulgaria. Accredited Higher Education Institutions Accredited Doctoral Programmes on Cybersecurity

News on Cybersecurity

The National Cybersecurity Strategy "Cyber Resilient Bulgaria 2023" was adopted (link)	The National Strategy for Cybersecurity "Cyber Resilient Bulgaria 2023" (updated Cybersecurity Strategy) was adopted by the Council of Ministers on 31 March 2021. The strategy was developed by an interdepartmental expert group and coordinated with the Security Council to the Council of Ministers of the Republic of Bulgaria. The draft Strategy was publicly announced for consultation between 11 and 24 February 2021. The Roadmap for the Cybersecurity Strategy implementation is expected within six months from the adoption of the Strategy and will involve all related stakeholders. The complete text of the Strategy could be found here (At this stage: available in Bulgarian language only).
Position of National Cyber Director in the White House (link)	The National Defense Authorization Act (NDAA) for fiscal 2021 created the Office of the National Cyber Director within the Executive Office of the President. The office will be headed by the United States' first national cyber director (NCD) and is intended to lead the implementation of national cyber policy and strategy, with a focus on making rapid progress on domestic cybersecurity. The director will serve as the president's senior adviser for cyber issues. The creation of the Office of the National Cyber Director comes at a pivotal time in the development of the nation's cybersecurity and on the heels of one of the most widespread cyber incidents ever inflicted on the

	country. The nation's lead cyber agency, the Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security, continues to slowly mature into its crucial role. Still in the midst of the presidential transition, President Biden has begun to organize his staff at the White House, including with the creation of a deputy national security adviser for cyber and emerging technologies. While Biden has made it clear that cybersecurity will be a top priority for his administration—and the creation of the new deputy national security adviser is certainly indicative of this—many questions remain. The confluence of these developments and the creation of the Office of the National Cyber Director has led some observers in the administration, the private sector, and the media to pose questions about the nature and role of the new office. The NDAA provides clear descriptions of the office's several mandates. But questions remain about the motivation for the creation of the office, its authorities and how it relates to other cyber-relevant roles within the White House.
Support for UK education sector after growth in cyber attacks **(link)**	The National Cyber Security Centre (NCSC), which is a part of GCHQ, has today (Tuesday) published an alert to education establishments warning of an increase in ransomware attacks and setting out steps they can take to keep criminals out of their networks. While operational details cannot be disclosed, the NCSC has dealt with a significant increase in the number of attacks since late February, when establishments were preparing to welcome students back to the classroom. There is no reason to suspect the same criminal actor has been behind each attack, which have caused varying levels of disruption, including targeting school financial records.
78% of top security leaders say their organizations are unprepared for a cyberattack **(link)**	Seventy-eight percent of senior IT and security leaders believe their organizations lack sufficient protection against cyberattacks, according to research conducted by IDG Research Services on behalf of Insight. The high level of concern expressed by these leaders resulted in 91% of organizations increasing their cybersecurity budgets in 2021 — a figure that nearly matches the 96% that boosted IT security spending in 2020.
Microsoft hack: Biden launches emergency taskforce to address cyber-attack **(link)**	The Biden administration is launching an emergency taskforce to address an aggressive cyber-attack that has affected hundreds of thousands of Microsoft customers around the world – the second major hacking campaign to hit the US since the election. The attack, first reported by security researcher Brian Krebs on 5 March, allowed hackers to access the email accounts of at least 30,000 organizations in the US. These back channels for remote access can affect credit unions, town governments and small business, and have left US officials scrambling to reach victims, with the FBI on Sunday urging them to contact the law enforcement agency.
North Korea accused of hacking Pfizer for Covid-19 vaccine data **(link)**	North Korea attempted to steal Covid-19 vaccine technology from US pharmaceutical company Pfizer, according to South Korean intelligence officials. It is currently unclear as to what, if any, data was stolen. South Korea's National Intelligence Agency privately briefed lawmakers about the alleged attack, reported local news agency Yonhap. The BBC has asked Pfizer for a comment but it has yet to respond .

Feedback

For questions & recommendations

E-mail: acerta@bas.bg

Editorial Board

Academic CERT association under an agreement signed from a group of academic bodies (IICT, DI, ESI as a first step) to strengthen cooperation in cyber-security related research

The publication of the newsletter is supported by the British Embassy in Sofia.

The opinions in the newsletter reflect the authors' point of view.

British Embassy Sofia

IICT Institute of Information and Communication Technologies

Bulgarian Defense Institute

ESI European Software Institute Center Eastern Europe

СЪЮЗ ЗА СТОПАНСКА ИНИЦИАТИВА
UNION FOR PRIVATE ECONOMIC ENTERPRISE