ISSN 2738-7097 https://doi.org/10.11610/cybsec04

British Embassy
Sofia

# Cybersecurity Newsletters

IICT
Institute of Information and Communication Technologies

## UK-BG Partnership in Cyber Security for SME and Organizations

Newsletter January 2021 Number 4

## Aims and Scope

The current online newsletter #4 is focused on digital transformation and the driving role of cyber resilience. We provide an overview of a project in Institute of ICT of the Bulgarian Academy of Sciences (IICT-BAS) in partnership with many academic institutions and State agency “e-Government” with the Institute of Public administration to define the model for digital transformation and cyber resilience in the public sector.

In defined 4 quadrants and two levels of change the focus is given here on research and education as two levels in the academic quadrant, where we believe is the key opportunity to influence the change of processes, organizations, technologies and people – the four pillars of the digital transformation, supported by the efforts in resilience of the new cyber domain. So we present our focus on change management research and education, related to digital transformation and especially cyber security.

Logical next part of the edition is to presentation of the four pilot projects under Horizon 2020 program of EU in cyber security towards the implementation of the Regulation on establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.

As in previous editions we try to provide useful news on cyber security, related to the digital transformation, research education.

Being in the period of update of the Bulgarian National Cyber Security Strategy and dedicated to support it with the National Cyber security Program we present shortly the second British National Security program of 2016 as a good practice to follow in Bulgaria.

In preparation for the implementation of the Regulation on establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres every EU Member State is to notify to the Commission in 6 months period the National Coordination center – so we shortly present here the Bulgarian CERT, performing partly such a function already with opportunity to be further extended especially in academic domain through close cooperation with IICT-BAS as a National research institution for research in cyber, HPC and AI.

**Issue Editors: Assoc. Prof. Dr. Velizar Shalamanov**

**Asst. Prof. Irena Mladenova**

# Issue Focus: Digital Transformation and Cyber Resilience

**Assoc. Prof. Velizar Shalamanov**
**IICT deputy director on**
**e-Infrastructure & secuity,**
**Issue Editor**

**Assist. Professor Irena Mladenova**
**Sofia University St. Kliment**
**Ohridski, FEBA,**
**Issue Editor**

Considering transformation as a spiral change management process in four domains – processes, technology, organization and people (Fig. 1) we definitely could add cyber resilience as a specific fifth domain, when it comes to digital transformation and changes in this area are critical for the success of the overall transformation as we create real new Global Common – Cyber space, fully designed by us human beings and we have the responsibility to secure it by design.

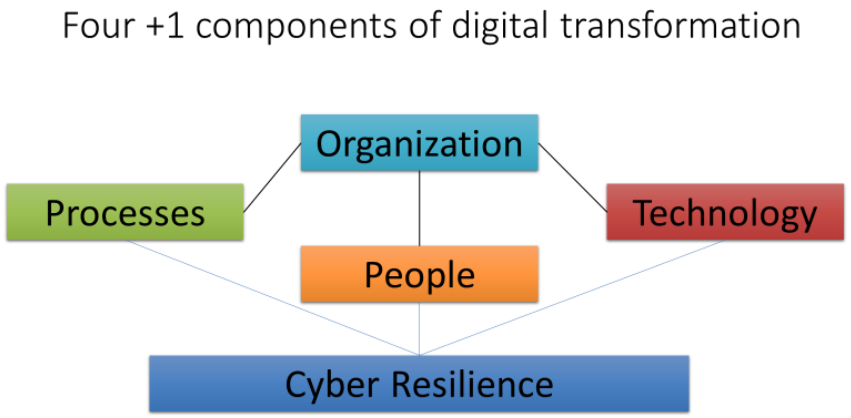

*Fig. 1. Cyber resilience as an additional component for digital transformation*

The core of digital transformation is the developed communications and information (C&I) systems to support the processes in all the areas of human activity and providing for the radically new organization of our life. It creates a lot of new dependencies and vulnerabilities, so our focus is to be on cyber resilience by design with continuous improvement, especially of the human element of this new space through education and training. So as on the Fig. 2. we could consider cyber resilience and education & training as pillars of the C&I systems, consisting, themselves, of three layers: sensors/data, communications and computer infrastructure and applications/knowledge.

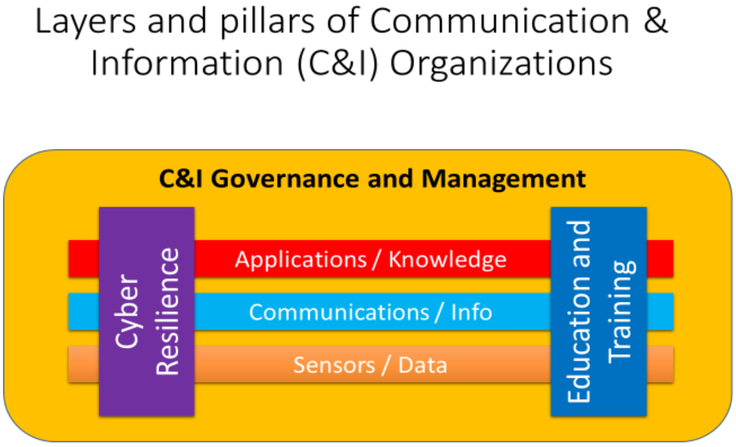
Layers and pillars of Communication & Information (C&I) Organizations
C&I Governance and Management
Applications / Knowledge
Communications / Info
Sensors / Data
Cyber Resilience
Education and Training

*Fig. 2. Layers and pillars of C&I systems*

Critical for the success in digital transformation and operation of the resulting C&I systems is the envelope of Governance and Management to guarantee the optimal decisions and their implementation in using of ICT resources for achieving the business goals.

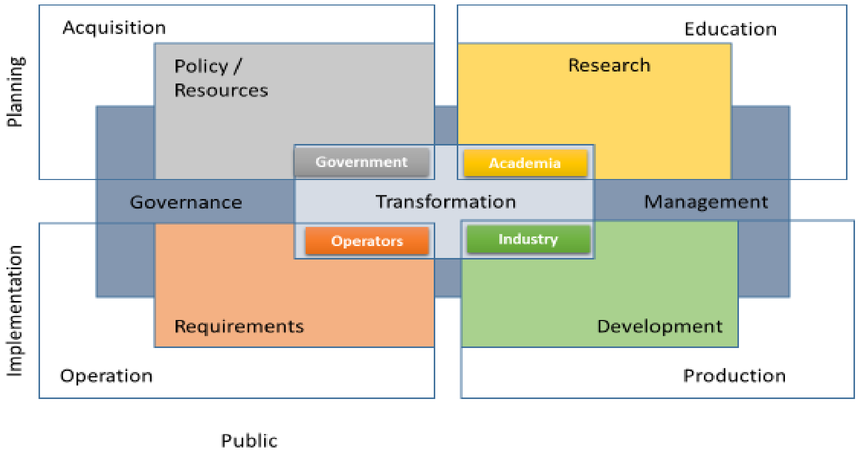

*Fig. 3 Spiral process of change in 4 quadrants*

In order to be successful, the transformation requires spiral involvement of different stakeholders as on the Fig. 3 on two spiral levels – research, policy, requirements, development and production, education, acquisition, operation. This spiral of transformation requires most effective and efficient governance and management model in a networked environment as the element of the digital ecosystem belong to the different by nature spheres – administration, academic, business, professional operators.

Since 2018 in IICT-BAS the project is started with the goal to consolidate the "islands" of competence for Digital Transformation and Cyber resilience in the academic community of Bulgaria and organize it in a collaborative network for customer funded service provision to Public Administration, SME and other potential customers for improving the innovation capacity and increase competitiveness of Bulgarian public institutions and SMEs. In addition, this consolidation goes hand in hand with the deeper integration of Bulgarian academic community in the EU research community and scientific cooperation among the NATO members.

The Vision for the project is to optimize governance and management of ICT research (science and technology) efforts in BAS as a hub for collaborative academic network of ICT competence in support of Digital Transformation and Cyber resilience of public institutions (including security sector), SME and other customers to improve innovation and competitiveness of Bulgarian digital ecosystem. Developing solid governance and management framework to provide strategic and business planning, partnership development, catalogue management, innovation management and respective infrastructure for S&T/R&D/E&T in the area of digital technologies will be the foundation of an academic part of the national (EU, NATO) digital ecosystem.

The Strategy to follow is starting with the consolidation of the competence entities in IICT-BAS and BAS in large to establish a hub for attracting and federating academic "islands" of ICT competence from universities and institutes outside BAS as well as innovative companies and start-ups. With the initial funding on this project the academic network is to achieve maturity of projectized and service oriented organization with a capacity to sustain its development under customer funding with limited (current levels of central budget funding) core funding for addressing the governance and management requirements without high overhead to the projects and services delivered.

## Research, education and training in Cyber Resilience and change management

As it was presented above in the 4 quadrants of transformation, the one we could consider as a starting point and serious driver for the spirals of change is the academic quadrant in two levels: research and education/training. In order to understand the requirements and perspective of development of this quadrant we need to put it in the context of change management and continuous improvement of the digital eco-system.

When we try to define the research agenda in digital transformation and cyber resilience, obviously we cannot stay only in the domain of C&I technologies but need to address the challenges of governance and management in this very complex process of digital transformation bringing us in the cyber space with all potential vulnerabilities, risks and real threats we to address through the cyber security/resilience program.

Managing and leading change increasingly becomes one of the crucial managerial skills to help respond to, as well as actively shape, the environment, and the challenges and opportunities it presents. There is a vast body of academic and practitioners' research which tend to agree on what are the factors that influence the success of a change initiative – and these include clarity of the vision, flexible enough structure and processes, transformational leadership, empowered change agents, coalition of supporters.

Digital transformation and cyber resilience set a bold vision with repercussions in a number of sectors, systems and institutions. The COVID-19 crisis significantly boosted the digital transformation, even in sectors which were expected to take much longer to go digital – schools, universities, governments among others. But it also highlighted how vulnerable these might be in the cyber space and made it clear that the solutions are complex.

To add to the complexity, various and numerous players are involved in setting up the overall cybersecurity and resilience agenda – on organizational, national, European level. The change needed can be viewed on at least two levels: mezo (organizations) and macro (countries, EU).

*On macro level*, charting the strategy to implement the bold vision, and then successfully implementing it is a large transformational change initiative affecting a large system. It would require developing and training the change agents and transformational leaders to move it forward. Education and training in change management, thus, is as necessary as the education and training in the cybersecurity solutions, practices and policies, to design and implement the management and governance system on national and European level.

Some research on change in large systems, virtual organizations and collaborative networks exists, though with the growth of such structures' importance this would need to be deepened. The mechanisms, pace and scope of change in such structures differs from the traditional organizations, and that calls for adjustment of the approaches.

On mezo level, similar requirements apply to organizations – managing cyber threats and vulnerabilities might require significant changes in organizational processes, systems and practices. Making sure they work depends on both the technical solutions as well as the employees actually using and abiding to them. That might require major change on individual level (learn new skills, follow new procedures), be accompanied with resistance, cynicism and ultimately failure. The change projects, thus need to raise awareness of the need to change, create the sense of urgency and desire, provide the information and tools to the people affected, remove the roadblocks and reinforce.

Technology-related change in organizations is widely researched area. Still, it is an often-cited fact that the majority of change initiatives fail to achieve their goals and targeted results. Context and organizational specifics call for tailored approaches, and advances in organizational change research are yet to provide valuable inputs.

Equipping the transformational leaders and change agents – on both mezzo and macro levels – with the necessary skills and tools to effectively and successfully lead the change, thus, should be an inseparable part of the research, and education and training agenda in support of the cyber security/resilience program.

## EU four pilot projects in Cyber Security and European Competence Centre on Cyber Security (ECC)

### R&D and Innovation effort of EU in Cyber security

Four pilot projects – ECHO, CS4E, CONCORDIA and SPARTA were funded under the Horizon 2020 Program with the aim to connect and enhance knowledge sharing and building across various domains and member states. The four pilot projects collectively are expected to help shape the cybersecurity and resilience capabilities in Europe and develop a common cybersecurity strategy and ecosystem. The projects share the same vision but differ in the aspects and fields covered.

The European Competence Centre (ECC) will be an important part of the Cybersecurity Competence Network aimed to help Europe retain and develop the capacities necessary to secure the Digital Single market.

All of the above are presented shortly below:

**ECHO** – The ***E***uropean network of ***C***ybersecurity centres and competence ***H***ub for innovation and ***O***perations (ECHO) consortium consists of 30 partners from different fields and sectors including health, transport, manufacturing, ICT, education, research, telecom, energy, space, healthcare, defence & civil protection.

The *main objective* of ECHO is to strengthen the proactive cyber defence of the European Union, enhancing Europe's technological sovereignty through effective and efficient multi-sector and multi-domain collaboration. The project will develop a European Cybersecurity ecosystem, to support secure cooperation and development of the European market, as well as to protect the citizens of the European Union against cyber threats and incidents.

Main ECHO concepts are:

- **ECHO Governance Model**: Management of direction and engagement of partners (current and future)
- **ECHO Multi-Sector Assessment Framework**: Transverse and inter-sector needs assessment and technology R&D roadmaps
- **ECHO Cyber Skills Framework and Training Curriculum**: Cyber skills reference model and associated curriculum

- **ECHO Security Certification Scheme**: Development of sector specific security certification needs within EU Cybersecurity Certification Framework from ENISA
- **ECHO Federated Cyber Range**: Advanced cyber simulation environment supporting training, R&D and certification
- **ECHO Early Warning System**: Secured collaborative information sharing of cyber-relevant information

**CS4E** – The ***C***yber***S***ec***4E***urope (CS4E) consortium consists of 43 partners and covers a wide spectrum of cybersecurity issues: 14 key cybersecurity domain areas, 11 technology/applications elements and nine crucial vertical sectors.

CyberSec4Europe's *main objective* is to pilot the consolidation and future projection of the cybersecurity capabilities required to secure and maintain European democracy and the integrity of the Digital Single Market. CyberSec4Europe has translated this broad objective into measurable, concrete steps: three policy objectives, three technical objectives and two innovation objectives.

As a research project, CyberSec4Europe is working towards harmonising the journey from the development of software components that fit the requirements identified by a set of short- and long-term roadmaps, leading to a series of consequent recommendations. These are tied to the project's real-world demonstration use cases that address cybersecurity challenges within the vertical sectors of digital infrastructure, finance, government and smart cities, healthcare and transportation.

**CONCORDIA** – ***C***yber security c***O***mpete***NC***e f***O***r ***R***esearch an***D*** ***I***nnov***A***tion (CONCORDIA) consortium consists of 46 partners representing leading universities, industries, public bodies and organizations.

CONCORDIA's *main goal* is to lead the integration of Europe's excellent cybersecurity competencies into the network of expertise to build the European secure, resilient and trusted ecosystem.

The consortium has 12 objectives in the areas of building cybersecurity ecosystem with open and adaptive governance model, develop cybersecurity roadmap and solutions, scale up research and innovation and identify marketable solutions, work with multiple communities, support entrepreneurs and establish an education ecosystem.

**SPARTA** consortium consists of 44 partners from various fields and sectors.

SPARTA's *mission* is to re-imagine the way cybersecurity research, innovation, and training are performed in Europe across domains and expertise, from foundations to applications, in academia and industry.

SPARTA runs 4 core programs:

- **T-SHARK** – explores innovative work in full- spectrum situational awareness, with the goal of enabling the supervision of complex systems over heterogeneous time scales.
- **CAPE** – investigates new avenues for continuous assessment and new evaluation tools and techniques for handling tomorrow's dynamic and elastic digital systems.
- **HAII-T** – develops a foundation for secure-by-design intelligent infrastructure built on strong formal approaches, addressing multiple cybersecurity facet.

- **SAFAIR** – devises approaches to make systems using AI more reliable and resilient through enhanced explainability and better threat understanding.

All four pilot projects are actively working with the communities and welcome new participants.

**European Cybersecurity Competence Centre.** On 11 December 2020, the EU institutions reached a political agreement on the Cybersecurity Competence Centre and Network of National Coordination Centres (NCC) – an initiative focused on improving and strengthening technology and industrial cybersecurity capacities of the EU and help create a safe online environment.

The Cybersecurity Competence Centre will be located in Bucharest to facilitate and coordinate the work of the Network and foster the Cybersecurity Competence Community.

To do so, the Centre and the Network will pool resources from the EU, its Member States and the industry to improve and strengthen technology and industrial cybersecurity capacities, enhancing the EU's open strategic autonomy. The tasks of the Center are to:

- Set up and help coordinate National Coordination Centres (NCC) Network and Cybersecurity Competence Community
- Implement cybersecurity-related financial support from Horizon Europe and Digital Europe Programmes

The Cybersecurity Competence Centre and Network will help the Union and Member States to take a proactive, longer-term and strategic perspective to cybersecurity research, development, and industrial policy. This approach should help not only to come up with breakthrough solutions to the cybersecurity challenges which the private and public sectors are facing, but also support effective deployment of these solutions. The Centre and the Network together will enhance our technological sovereignty through large-scale Cybersecurity projects in areas such as Cyber Threat Intelligence, Cyber secured hardware and operating systems, and security certification.

## Cyber Resilience News

### COVID-19 impact on SecOps: Increased threats, greater investments in automation

(www.helpnetsecurity.com)

Siemplify released a research that studies how the sudden shift to remote work during the COVID-19 pandemic has affected SecOps analysts' ability to perform their jobs and the impact on overall security postures. The overall cybersecurity posture has remained strong due to greater investments in security automation technologies and reliance on managed security service providers (MSSPs), potentially paving the way for many security operations centers (SOCs) to become permanently remote, a Siemplify survey reveals. SecOps is a highly collaborative function, with security analysts working closely in physical SOCs to address tens of thousands of alerts and security incidents daily, hunt for threats and problem-solve responses.

### Qatari research center chooses Leonardo for cyber range

(www.defensenews.com)

A Qatari cyber research center has selected Leonardo to provide a cyber range and training system to support security operations, the Italian firm announced Feb. 3. The Qatar Computing Research Institute, or QCRI, was established by the Qatar Foundation for Education, Science and Community Development. The training platform ordered by the QCRI is capable of simulating cyberattacks so users can assess the resilience of digital infrastructure.

### Vulnerabilities in NextGEN Gallery Plugin Exposed Many WordPress Sites to Takeover

(www.securityweek.com)

Two severe vulnerabilities in the NextGEN Gallery WordPress plugin could have exposed more than 800,000 websites to complete takeover, WordPress security company Defiant reported on Monday. Available for more than a decade, the plugin provides users with a broad range of gallery management capabilities, such as batch upload of photos, metadata import, thumbnail editing, photo and gallery management, and more. In December 2020, security researchers with Defiant's Wordfence team discovered two cross-site request forgery (CSRF) vulnerabilities in the popular plugin, the most severe of which could lead to remote code execution (RCE) and stored cross-site scripting (XSS).

### U.S. Agencies Publish Ransomware Factsheet

(www.securityweek.com)

The National Cyber Investigative Joint Task Force (NCIJTF) on Friday released a joint-sealed ransomware factsheet detailing common attack techniques and means to ensure prevention and mitigation. The factsheet has been developed by an interagency group of experts in ransomware, from more than 15 government agencies, and is meant to help increase awareness on the threat that ransomware poses to critical infrastructure. The two-page document explains that, in addition to encrypting the data on victim systems to make it unusable, ransomware operators might also pressure victims into paying the ransom by threatening to destroy the data or release it to the public. Ransomware attacks affect all sectors, including state, local, tribal, and territorial governments, but also impact hospitals, police, fire departments, municipalities, and other critical infrastructure.

### Microsoft Fixes Windows Zero-Day in Patch Rollout

(www.darkreading.com)

Microsoft's monthly security fixes addressed a Win32k zero-day, six publicly known flaws, and three bugs in the Windows TCP/IP stack. Microsoft today patched a Windows zero-day vulnerability as a part of its monthly Patch Tuesday rollout, which fixed a relatively low number of Common Vulnerabilities and Exposures (CVEs) but a high number of publicly known bugs. The 56 vulnerabilities patched today exist in Microsoft Windows, .NET framework, Windows Defender, Azure IoT, Azure Kubernetes Service, Exchange Server, Skype for Business and Lync, Office and Office Services and Web Apps, and Microsoft Edge for Android. Eleven of these flaws are classified as critical in severity, 43 are important, and two are moderate.

### SOC teams spend nearly a quarter of their day handling suspicious emails

(www.scmagazine.com)

Security professionals know that responding to relentless, incoming streams of suspicious emails can be a labor-intensive task, but a new study shared exclusively with SC Media in advance indicates just how time-consuming it actually is. Researchers at email security firm Avanan claim to have authored the "first comprehensive research study" that quantifies the amount of time security operations center (SOC) employees spend preventing, responding to, and investigating emails that successfully bypassed default security and are flagged by end users or other reporting mechanisms.

### Securing Classified Telework: 3 Principles for Protecting Sensitive Data

(www.tenable.com)

As pandemic restrictions linger, federal agencies are preparing for a rise in classified telework. Here's why a continued focus on cybersecurity fundamentals is imperative.

The COVID-19 pandemic accelerated the move to remote work beyond all prior expectations. While there were many exceptions to the rule in the early days of the pandemic response, we are seeing those exceptions decrease as the remote work environment matures. The sudden need for secure remote work drove innovation and flexibility as necessary attributes of a successful transition. Leaders at the Defense Information Systems Agency (DISA), for example, commented that this demand, and the resultant security upgrades, were a sort of "silver lining" within the pandemic "cloud."

### AI needed to vet 100 billion cyber threat items per day

(www.jpost.com)

Artificial intelligence is an absolute imperative to vet obscene amounts of data and cyber-threat intelligence, up to 100 billion items per day, according to an AI expert at a conference analyzing how the issue impacts national security.

Derek Manky, chief of security insights for global threat alliances at Fortinet, made his remarks at a virtual conference co-sponsored by the Institute for the Research of the Methodology of Intelligence and Israel Defense.

### US, Estonia Partnered to Search Out Cyber Threat From Russia

(www.securityweek.com)

In the modern twist on old-fashioned war games, the U.S. military dispatched cyber fighters to Estonia this fall to help the small Baltic nation search out and block potential cyber threats from Russia. The goal was not only to help a NATO partner long targeted by its powerful neighbor but also to gain insight on Russian tactics that could be used against the U.S. and its elections.

The U.S. Cyber Command operation occurred in Estonia from late September to early November, officials from both countries disclosed this week, just as the U.S. was working to safeguard its election systems from foreign interference and to keep coronavirus research from the prying reach of hackers in countries including Russia and China.

### The challenges of keeping a strong cloud security posture

(www.helpnetsecurity.com)

In this interview, Badri Raghunathan, Director of Product Management for Container and Serverless Security at Qualys, talks about cloud security, and their approach for enabling global CISOs to focus on what's most important.

The usage of public cloud infrastructure is mainstream, and enterprises often have a multi-cloud footprint. However, even after 10+ years of the public cloud, enterprises still struggle with the security principle of shared responsibility. This has to do with putting in place a security architecture (or a set of principles) that meets the organization's needs and works in the public cloud world.

## Cyber Institutions & Initiatives in UK & Bulgaria

### UK National Cyber Security Programme

**2016 National Cyber Security Programme.**

Chancellor sets out vision to protect Britain against cyber threat in Government Communications Headquarters (**GCHQ**) speech, GOV.UK 2015-11-17 with **£1.9 billion** in spending 2016-2021 (the same period for the Bulgarian National Cyber Security Strategy "Cyber Resilient Bulgaria 2020")

National Cyber Security Centre is the home to the UK's "cyber force", but there are £40m for an MoD Cyber Security Operations Centre. In addition, £22 million are marked "to stand up new Army cyber operations centres across the UK."

Important role is given to the "Institute for Coding: Centre for Digital Skills and Computer Science" and the "Cyber Streetwise"/"Cyber Aware" (cyberaware.gov.uk) campaign for 2015/16 with total cost £4 million (ex-VAT) and £3.3 million in 2017/18.

The program includes £265m investment in Cyber Vulnerability Investigations (CVI) programme for MoD.

A six-month "cybersecurity incubator" funded via **Department for Digital, Culture, Media and Sport** (**DCMS)** – HutZero initiative.

About £10m are used to establish a 'Cyber Innovation Fund'. In addition £14m ("up to") investment in a London cyber security innovation centre (This is the DCMS-funded LORCA (London Office for Rapid Cybersecurity Advancement))

There are £50m ("up to") for the Protecting of the Government. Important for the partners is the International Cyber Security Capacity Building Programme.

There are £13.5 million for the cyber innovation centre.

Cyber Security Skills Immediate Impact Fund (CSIIF) is established Feb 2018 with focus "as of end of October 2018, approximately 170 individuals were either participating or had been identified to take part in the seven initiatives supported through the Cyber Skills Immediate Impact Fund (CSIIF) pilot."

Because of National security restrictions it is a principle of funding through the National Cyber Security Programme that the Government is unable to detail individual NCSP funding by department or initiative.

Important for this issue of the Newsletter is the fact that up to £800,000 are planned to support UK academic institutions in commercialising cyber security innovation.

### CERT-BG

**CERT Bulgaria** is the National Reaction Center for Incidents in Connection with Information Security. The mission of the Center is to support its service users in proactive activities to reduce the risks of information security incidents and to assist in resolving such incidents in the event that they have already occurred.

The Center provides a centralized database of information related to providing a secure and secure information environment.

The goals to be achieved include:

- protection of information and technological assets;
- limiting the direct impact of security incidents on the information society;
- help in recovering from incidents;
- assessing the impact of security incidents;
- collecting and disseminating technical information related to information security incidents, as well as vulnerabilities in the security of the systems and ways to prevent them;
- conducting research related to new technologies in network and information security;
- conducting training related to information security and incident management.

## Links to Cyber Related Institutions

### Links to Bulgarian, UK & International bodies

The NCSC and the Engineering and Physical Sciences Research Council (EPSRC) jointly recognise Academic Centres of Excellence in Cyber Security Research (ACE-CSR).

Following the most recent assessment panel, 19 universities have been recognised as ACE-CSR. These universities have met tough minimum standards and proven they have:

- commitment from the university's leadership team to support and invest in the university's cyber security research capacity and capability
- a critical mass of academic staff engaged in leading-edge cyber security research
- a proven track record of publishing high impact cyber security research in leading journals and conferences
- sustained funding from a variety of sources to ensure the continuing financial viability of the research team's activities

**Doctoral studentships:** In order to further stimulate cyber security research in the UK, the NCSC supports Doctoral students across the ACEs-CSR. In addition, there are three Centres for Doctoral Training (CDT) in cyber security, under the banner 'Trust, Identity, Privacy and Security'. The CDTs are at:

- The University of Bristol with the University of Bath
- Royal Holloway, University of London
- University College London

**The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary cyber defence hub**

Nikola Vaptsarov Naval Academy is the oldest technical educational institution in the Republic of Bulgaria. Its history, past and present achievements establish the institution as the most prestigious centre for training of maritime specialists in the country. Recently the Academy opened Cyber Operations center and started a bachelor program on Cyber Security.

## 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

DIGILIENCE Conference Series
https://digilience.org