Information & Security

B. Mednikarov et al.
vol. 53, no. 2 (2022): 205-218
https://doi.org/10.11610/isij.5314

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Cyber Hygiene Issues in the Naval Security Environment

Boyan Mednikarov, Yuliyan Tsonev, Borislav Nikolov, Andon Lazarov (✉)

Nikola Vaptsarov Naval Academy, Varna, Bulgaria
https://www.naval-acad.bg

ABSTRACT:

In the present study, the main characteristics and components of cyber hygiene as a subclass of cybersecurity are discussed. Based on institutional experience in the scope of security in the digital environment, a sequence of activities to keep resilient and reliable cyber hygiene in naval institutions is recommended. Main cyber hygiene definitions are given. Cyber hygiene software issues and institutional information security controls are analyzed. Malware infection as the main cyber hygiene concern is analyzed. Basic cyber hygiene instructions to ensure Internet users stay protected are defined.

ARTICLE INFO:

RECEIVED: 27 JUNE 2022
REVISED: 31 AUG 2020
ONLINE: 23 SEP 2020

KEYWORDS:

cybersecurity, cyberattack, cyber hygiene, main cyber hygiene rules

Introduction

Cybercrime is on the rise in the global information network. Criminal hackers through phishing emails, brute force attacks, and malware compromise millions of users' workstations. In the last two years, the number of global ransomware attacks has reached above 600 million. This requires special measures that need to be taken by organizations, network administrators, and users to counter this global threat.[1-10]

Cyber hygiene provides protection and security in the maintenance and exploitation of computer networks. Multiple points of view regarding issues

✉ Corresponding Author E-mail: a.lazarov@naval-acad.bg

that arise with different cyber attackers, cyber threats and cyber-risks from that can be referred to cyber-hygiene of individuals and institutions.[1] Effectiveness of the Cyber Essentials scheme and its security activities that mitigate the threats they were designed for, i.e., those threats exploiting vulnerabilities.[2]

Malicious network users scan network devices for vulnerable devices, investigate network security mechanisms, and detect vulnerabilities in the network to retrieve security layer (SSL) certificates or invalid URLs. During the Cyber Kill Chain recognition phase, security software is evaluated and vulnerabilities are identified.[3]

Methodology for the realization of cyber hygiene practices in Smart Grid Systems focused on smart metering systems has been proposed and tested.[4] It is proven that implementing cyber hygiene instruments can improve smart meter cybersecurity and be suitable for implementing other sensitive Smart Grid components.

Effective cyber hygiene is a challenging task for the entire institution and the responsibility of individual employees. If the role of cyber hygiene is to be summarized, it is responsible for the integrity and availability of data. Cyber hygiene includes many rules and activities to ensure cyber security.

A list of main activities in the scope of cyber security and cyber hygiene, including a set of practices for managing the most common and pervasive cybersecurity risks, faced by employees and institutions, is discussed by Ead and Abbassy.[5]

It is compulsory that users must follow strictly a high level of cyber hygiene in the financial analytical area, security and military sphere, marine and air traffic control, etc., bearing in mind that many employees keep not have good cyber hygiene. They openly exchange passwords and share private information on social networks.

Rojas and co-authors provide an analysis of end users' behaviors to promote the creation of more successful approaches in the financial analytical climate.[6] It includes recommendations that allow improving the institution's cyber hygiene in access to financial solutions in the area. Bedrich and a report by RSI Security discuss cyber hygiene checklists to prevent attacks on computer networks and rules of cyber hygiene that must follow by institutions and internet users.[7, 8]

There are different definitions of the term "cyber hygiene." There is no consensus on what constitutes cyber hygiene. Different national institutions have their own specific recommendations and rules, i.e., there is no single standard or commonly accepted mechanism for an institution to assess, evaluate or demonstrate cyber hygiene. A recent reprt by Tunggal focuses on the main characteristic of cyber hygiene, cybersecurity ratings and measures, and common cyber hygiene problems and practices.[9]

The rest of the article is organized as follows. Section II suggests cyber hygiene definitions, cyber hygiene – basic software issues, cyber hygiene - institutional information security controls. Section III discloses malware infections – cyber hygiene's main concerns.

Methods

Methods applied in the present study are analysis and illustration. The analysis is provided in respect of basic personal, institutional and software issues of cyber hygiene as a logical chain of definitions in respect of vulnerability to cyber-attacks, cyber threats, software instruments to ensure cyber hygiene, institutional information security controls and malware infections. Illustrations are provided with respect to a warm (virus) attack inside the attached file, phishing e-mail attacks, system software and hardware up to date.

Cyber hygiene as a part of cyber security

Cyber hygiene definitions

Cyber hygiene as a part of cyber security refers to the network users and institutions as a whole. It is a system of instructions and recommendations aimed at improving users' activity to help them gain knowledge and skills that guarantee network security, and thus ensure systems' cyber health. Cyber hygiene is a multilayer system of rules and activities users have to follow working in Internet. It is a distinctive feature. On the other hand, cyber hygiene means abilities and habits that help users and organizations mitigate the networks' potential vulnerability to cyber-attacks and enhance resilience against threats of cyber-attacks.

Cyber hygiene includes an aggregate of users' habitual skills and activities to ensure secure data exchange and resilience of networks and network devices to cyber impacts. It is like the classical medical hygiene each person has to follow. It consists of routine activities to prevent or mitigate health problems. Cyber hygiene practice includes the surveillance of all end devices connected to local networks, control of vulnerabilities, regular updates, and patching of the computers' software components.

Cyber hygiene means training to form professional habits ensuring cyber-security so that to prevent network cyber threats and internet security issues. Cyber hygiene aims to maintain hardware and software's basic health and security, ensuring they are protected from threats such as malware. Applied in everyday life, cyber hygiene helps to keep data, hardware and software safe and secure. As with any habit to be gained, cyber hygiene skills require learning and practical education to apply specific routine and repetition activities.

The routine in respect of cyber hygiene helps prevent cybercriminals from causing network intrusions, security breaches or stealing personal information. It helps keep software and operating systems up to date.

Cyber Hygiene – Basic Software Issues

Basic software issues that are in the focus of the cyber hygiene are as follows.

- Security breaches caused by threats from hackers' attacks such as phishing, malware, and viruses.
- Data loss caused by not reserved hard drives and virtual cloud storage vulnerable to unauthorized penetration and corruption.

- Vulnerability to cyber-attacks caused by out-of-date software.
- Cyber threats caused by obsolescence, i.e., not up-to-date antivirus security software that is less effective at protecting to newest software attacks.

Therefore, to ensure adequate and effective cyber hygiene, the network user must follow cyber hygiene periodicity of activities and apply the appropriate software instruments to ensure cyber hygiene.

The cyber hygiene periodicity means regular control and test routines, drawing up a schedule of different activities to be fulfilled to keep cyber hygiene on a certain level. For instance, scanning the computer for viruses using up-to-day antivirus programs, removing the old password and establishing a new one, keeping the user's applications, system software, and operating systems of all devices up to date, and cleaning the computer's hard drive. Once the user assimilates the cyber hygiene rules, it becomes part of the regular personal cybersecurity routine.[10] Appropriate software instruments to ensure cyber hygiene are as follow.

- Firewall – prevents unauthorized access from the Internet.
- Software for data-deleting prevents the risk of losing personal data while introducing new software, add on hardware, or modify system files and clears out not necessary data from the hard drive.
- A password manager maintains track of multiple passwords while using strong, complex passwords, which are changed regularly to keep internet hygiene.
- Antivirus software of high quality that schedules and performs periodic scanning to detect and remove malware and protects from multiple network threats.
- Freeing users from unusable electronic communication devices, such as laptops, smartphones, desktops, raises serious questions about cyber hygiene.
- The user must not only delete their files, but also reformat the hard drive of the devices. This also ensures the deletion of personal information stored on the disk.

The main rule of the cyber hygiene is maintaining the application and system software and hardware up to date. Web browsers, user and mobile applications, and network devices' operating systems have to be updated regularly. It eliminates software security issues. Through regular updates, new software patches are delivered to correct software failures.

For instance, the vulnerability Joomla - Core – XSS (Cross-Site Scripting) Attack Vector via SVG (Scalable Vector Graphics) (2021) (CVE (Common Vulnerabilities and Exposures)-2022-23801) is discovered in versions Joomla 4.0.0 to 4.1.0. An XSS attack via SVG (Scalable Vector Graphics) embedding in com and media files is possible. In updated version Joomla 4.1.1 the problem is fixed. Hardware updates guarantee to prevent CPU performance issues.

Cyber Hygiene – Institutional Information Security Controls

The basic controls provided by the institution are as follows [9]:

- Control usage of the hardware devices: It means to control only authorized devices to have access to the restricted area and sensitive data.
- Control usage of the system and application software: It means to control and mitigate risk by managing network software so that only certified and licensed software is installed on devices.
- Control continuous network vulnerability and risk management: It means to control regularly acquiring information in respect of new network vulnerabilities, to remove them and reduce the range of their risk impacts.
- Control usage of administrative rights: It means to control administrative rights by access control and access restriction, such as two-stage authentication or multi-stage authentication, as well as to be created approaches and instruments to track, control, prevent and correct the use, assignment, and configuration of administrative rights.
- Secure configuration of hardware and software on network devises: mobile sets as tablets, i-phones, laptops, stationary workstations and servers: It means that institutions must establish, implement and actively manage the security configuration of mobile devices as tablets, i-phones and laptops, and stationary routers, switches, servers and workstations to prevent attackers from exploiting vulnerable services and settings. This should include the use of complex passwords.
- Analyze audit documents: It means that institutions must collect, control and analyze audit logs of intrusion events to help the detection and identification of cyber-attacks.

In addition, there are the following foundational information security controls:

- Email and web browser protections: It is performed by minimizing the attack fronts and opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.
- Malware defenses: It is performed by controlling the installation, spread, and execution of malicious code and to enable rapid updating of defense, data gathering, and corrective action.
- Limitation and control of network ports, protocols, and services: It means to control and manage the ongoing functionality of ports, protocols, and services on networked devices in order to minimize vulnerabilities available to attackers and opportunities for cyber impacts.
- Data backup and recovery capabilities: It means applying server instruments and protocols to back up critical information with an effective methodology for timely recovery of it.
- Reliable and secure configuration of network devices, such as routers, switches, and firewalls: It means the institution and network administrators to establish, implement and manage the security configuration of network

infrastructure devices by configuration and processes of management, change and control to prevent cyber-attacks and exploiting vulnerabilities of services and settings.

- Boundary defense: It means boundary defense controls detection, prevention, and correction of the information flow transferring across networks of different trust levels focused on security-damaging data.
- Data protection: Sensitive data are of different types and reside in different places. It means data protection through a combination of encryption, integrity protection, and data loss prevention techniques.
- Controlled access based on the need to know: It means institutions to use instruments and processes to track, control, prevent and correct secure access to critical data according to access control rights of operators to computers, and applications based on a need or right previously classified.
- Wireless access control: It means to manage wireless access, processes and tools to track, control, prevent and correct the secure use of wireless local area networks (WLANs), access points and wireless client systems.
- Account monitoring and control: It requires controlling management across the life cycle of system and application accounts - their creation, use, dormancy, and deletion – to reduce opportunities for cyber-attacks.

There are four institution information security controls, namely:

- Establish a security awareness and training program: It means the institutions must build the specific knowledge, cyber security skills and abilities to ensure cyber defence through developing and executing a plan for identification and evaluation of problems and remediate through planning, training and awareness programs.
- Application software security: It means the institution must control the security of all acquired and used software over its life cycle.
- Incident response and control: It means institution must protect their information and reputation by developing and implementing an incident emergency response infrastructure (e.g., plans, defined roles, training, communications, and management oversight) to quickly discover attacks and then contain the damage, eradicate the attacker's access and restore the integrity of the network and systems.
- Penetration tests and red team exercises: It means institution must test their overall defense (technology, processes, and employee) by simulating the objectives and actions of an attacker. This may include on-site and off-site penetration testing, network security assessments, and testing the implementation of information security policies.

Malware Infection – Cyber Hygiene Main Concern

Definitions

The term "malware" means malicious software that contains malicious and destructive code. It is intentionally designed to damage, disrupt, and steal information, slow down and disrupt the functions of computers and servers. The malware is installed on network devices by system and internet users through downloading files or opening e-mails' attached files. Malware can damage the data and software while residing in storage and memory, but it cannot harm the hardware parts of systems or network equipment. The term "virus" is used to define entire malicious/damaging software. However, the virus is just a type of malware.

Malware infection vectors are a multidirectional transmission of malicious codes to network platforms and devices with the aim to infiltrate, infect and spread through the system by exploiting vulnerabilities. Malware vectors capture victims who

- Trust social networking forums like Facebook, Skype, Viber, etc.
- Show inquisitiveness and curiosity about any interesting event.
- Lack of expert awareness and experience.

It is important to know that accessing an account by cracking a user's email password gives the malicious user access to the attacked user's contact list, thereby gaining access to their business contacts on social networks and allowing them to attack other users. The downloaded and embedded malware contains documents as photo, movie, music, and more, providing criminal access to the entire communication system and network of the attacked user.

Local servers or network computers can be infected with one or some malicious software as a virus, worm, adware, crypto locker, spyware, toolkits, Trojan, botnet, etc. It performs destructive activities according to their nature like stealing personal or confidential information of users or institutions, tracking and monitoring activities of the computer, installing backdoors and keystrokes loggers, making target server crash, harming the performance of online systems, usage of system resources like CPU cycles, memory and network, encrypt sensitive data. Spyware or adware can cause a sudden change in functionality. It must be aware that the infection level depends on the system defense and the residence of malware on it.

Malware authors [11, 12] use social engineering techniques to distribute and infiltrate malware, and enforce users to download, embed, and run malicious code on their systems without realizing it (Fig. 1).

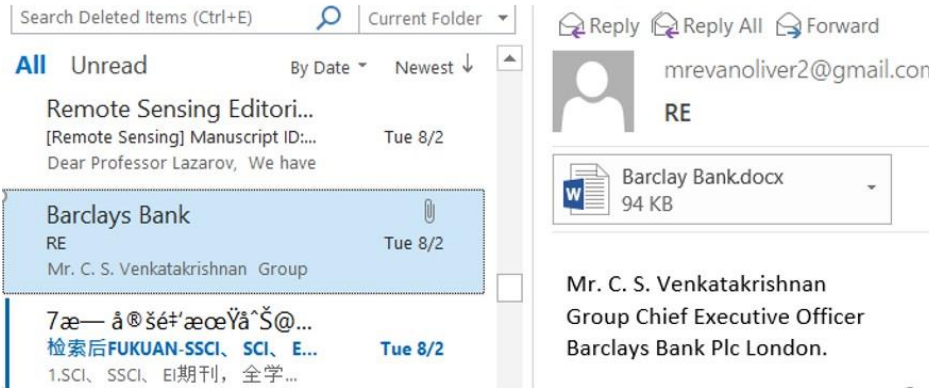

Figure 1: A worm (virus) attack inside the attached file.

Once an attacker infects a system, they can have complete control and access to that system's information and devices. Malware products exploit weak places in the cyber defense of the computer system. Malware infections find out vulnerabilities in security in previous versions of standard software applications such as picture viewers, Media Players and Windows operating systems.[11]

Malicious internet users apply social engineering tactics to find out weak security places and to transfer monovalent code in a computer in order to install their malicious code, which is able to steal confidential information. They rely on the responsiveness of people as well as their mistakes and poor cyber hygiene. Cybercriminals find vulnerabilities in a computer network to infiltrate it and gain access to personal and confidential information. This damages the security not only of an individual user, but also of the institution as a whole. All malware tools applied by cyber criminals use social engineering techniques to perform their monovalent work. Several ways are applied to spread viruses using social engineering [12]:

- Straight questioning.
- Systematic search for information.
- After gaining physical access.
- Reverse social engineering (reverse social engineering is a type of social engineering that aims to steal sensitive information and/or money through psychological manipulation and back contact with the victim).
- Online social engineering (social engineering is performed online).

Market to a device: This attack is initiated by the electronic market. The malware author uploads his malicious application to the e-marketplace site using a stolen/unauthorized identity. In the presence of malicious applications on the e-marketplace site, many users can be attacked.[12]

Web browser to device: This is a virus's distribution technique typically using downloading tactics, applied recently by network cyber-attacks.

SMS to a device: The malicious software propagates via SMS or MMS.

Network to a device: It exploits software vulnerabilities and hardware misconfigurations.

Device to device: The infection disseminates from device to device in a point-to-point manner.

USB to Device: The infection disseminates via USB devices connecting to an infected computer with new variants of a virus.

Botnet: The term "botnet" means a robotized network. Botnets are networks of computer devices infected with a malicious backdoor program used by a malicious user to automatically carry out different cyberattacks. The attacks are data theft, server crashing, sending spam from zombie computers to attack government and military networks, DDoS (Distributed Denial of Service) attacks, anonymous Internet access; cyber criminals' access to a web server using zombie machines to commit cybercrimes such as hacking websites or transferring stolen money, selling and leasing, allows distributing malware in computer networks.

Phishing by a botnet: Botnet allows changing the addresses of phishing pages frequently using infected computers as proxy servers (Fig. 2).

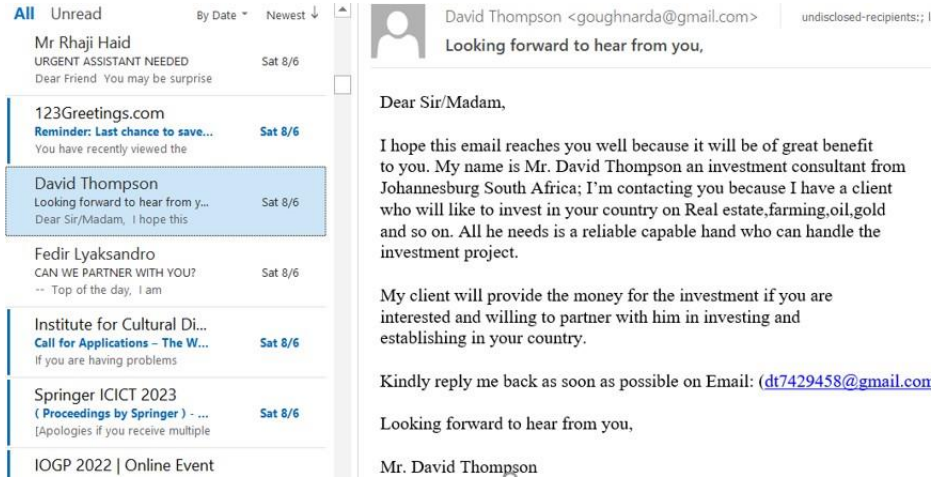

Figure 2: Phishing attack by e-mail letter (social engineering).

Virus: a type of malware attached to another software document or a legitimate program. It makes multiple replicates, infects and corrupts other files without the user's awareness.

Trojan horse: a type of malicious malware hidden or embedded in an email attachment or in a program such as a computer game, attractive to encourage a user to install it. The most insidious (and ironic) types of Trojan Horses are programs that offer to clear user's computer of viruses, but instead deliver viruses to victim's computer.

Spyware: a type of malware installed on computers or network devices without the knowledge of the user. The spyware activated on computers collects and transmits personal and institutional information such as passwords, and the numbers of credit cards.

Ransomware: a type of malware applying an encryption code to lock and/or block a user's access to a computer system or user's files until a specific amount of money is paid — usually by cryptocurrency (e.g., Bitcoin), since the transaction cannot be traced or refunded. In case the ransom is not paid, then the system and the victim's files are destroyed.

Figure 3. Worm attack by URL (web address).

Computer worm: a type of malware, a self-replicating program that copies itself from computer to computer. Rather than infect files, its main purpose is to use resources such as computer memory and network bandwidth to inflict damage.

Cyber Hygiene Instructions to Ensure Maritime Internet Users Stay Protected

The following cyber hygiene instructions Internet users are advised to apply in order to ensure they stay protected from cyber-attacks.

Create safe and secure passwords that are resistant to cracking

- For different accounts and registrations, avoid using the same password.
- The passwords need to change on a regular basis.
- Password's length has to be at least 12 characters and longer.
- The passwords have to include a mix of capital and small letters, symbols and numbers.
- The passwords must avoid sequential numbers or personal information, such as date of birth or a pet's name.
- The default passwords on IoT (Internet of Things) devices need to be changed.
- The passwords are not written down and shared them with other internet users.
- It is recommended to use a password manager to generate, store, and manage all passwords in one secure online account.
- Usage of multi-factor authentication access.

- The essential accounts – such as email, social media, or banking apps – are protected with MFA (Multi-Factor Authentication) using an app like Google Authenticator or Authy.
- MFA backup codes are saved in a password manager.

Backing up data regularly on external discs and storages

- It is recommended to keep files secure and protected against data loss by backing up essential files offline, either on an external hard drive or in a cloud.

While communicating ensure the privacy of information

- Trust social networking forums like Facebook, Skype, Viber, etc.
- It is recommended not to post private information such as a home address, private pictures, phone number, or credit card numbers publicly on social media.
- Privacy settings in the usage of social media are to be set to a high level.
- It is recommended to avoid quizzes, games, or surveys on social media that ask for sensitive personal information.
- It is recommended the user keep a computer and phone locked with a password or PIN.
- It is recommended not to disclose private information when using public Wi-Fi.
- In the case public Wi-Fi, it is recommended to maximize privacy by using a VPN (Virtual Private Network).
- Online transactions are to make via a secure website (URL starts with https://) with a padlock icon on the left of the address.
- Information about online privacy is exchanged with colleagues, friends and family members to help keep them safe as well.

Keep applications, system software, and firmware up to date

- It is recommended to update applications, web browsers, operating systems, and firmware regularly to ensure using the latest versions with possible security issues eliminated or patched.
- It to be set up a system features to ensure automatic software updates.
- It is recommended to delete applications no longer in use, but open security vulnerabilities and only download apps from reputable or official sources.

Ensure security of routers

- Default name of home Wi-Fi routers, router's username and password need to be changed.
- It is recommended to keep the router's firmware up to date.

- It is recommended to disable remote access, Universal Plug and Play, and Wi-Fi Protected Set-up.
- It is recommended to set up a separate network for guests to use.
- It is recommended to ensure that a router offers WPA2 or WPA3 encryption to protect the privacy of information sent via the network.

Protect against social engineering attacks

- It is recommended to avoid clicking on suspicious links or links, opening emails that look suspicious, downloading suspicious attachments from emails or not expected text messages, clicking on ads that promise free money, prizes, or discounts.

Using network-protected software – firewalls

- It is recommended to use a correctly configured firewall to prevent malicious software from accessing a computer or network via the internet.

Encrypting devices

- It is recommended to encrypt devices and media as laptops, tablets, smartphones, removable drives, backup tapes, and cloud storage, which contain sensitive data.

Remove all information from hard drives

- Before disposal of or selling a computer, tablet, or smartphone, make sure the hard drive is cleaned up to prevent any personal information from being accessed by others.

Ensuring high-quality antivirus protection

- It is recommended to use high-quality antivirus software that scans for and removes computer viruses and other malicious software.
- It is recommended to keep the antivirus software up to date

In conclusion, cyber hygiene means developing and following a protective routine to keep personal and financial information secure when using computers, laptops or other mobile devices. Using strong passwords and changing them regularly, keeping software and operating systems up to date, cleaning hard drives, and using a comprehensive antivirus software like Kaspersky Total Security will help users stay ahead of the latest cyber threats.

Conclusions

The main components of the cyber hygiene in the information world are defined. Cyber threats and tools used to realized them are in the focus of the present study. Based on detailed analysis, a logical sequence of rules to meet the requirements of cyber hygiene is defined. It includes cyber hygiene instructions that ensure Internet users stay protected.

References

[1] Debabrata Singh, Namrata P. Mohanty, Shrabanee Swagatika, Shrabanee Swagatika, and Santosh Kumar, "Cyber-hygiene: The key Concept for Cyber Security in Cyber-space," *Test Engineering and Management* 83 (May – June 2020): 8145 – 8152.

[2] Jose M. Such, Pierre Ciholas, Awais Rashid, John Vidler, and Timothy Seabrook, "Basic Cyber Hygiene: Does it work?" *Lancaster E-Print*s, Feature Article, 2022, https://core.ac.uk/reader/224767750.

[3] ˝An Attractive Target: Why Cyber Hygiene Matters," *FS-ISAC*, 2022, https://www.fsisac.com/hubfs/Resources/WhyCyberHygieneMatters.pdf.

[4] Matt Trevors and Charles M. Wallen, "Cyber Hygiene: A Baseline Set of Practices," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, 2017, https://resources.sei.cmu.edu/asset_files/presentation/2017_017_001_508771.pdf.

[5] Waleed M. Ead and Mohamed M. Abbassy, "A General Cyber Hygiene Approach for Financial Analytical Environment," In: Derindere Köseoğlu, S. (eds) *Financial Data Analytics. Contributions to Finance and Accounting* (Springer, Cham, 2022), https://doi.org/10.1007/978-3-030-83799-0_13.

[6] Juan Carlos Olivares Rojas, Enrique Reyes Archundia, Gutiérrez Gnecchi, Arturo Mendez Patiño, Jaime Cerda Jacobo, and Ismael Molina Morenoa, "Methodology for Cyber Hygiene in Smart Grids," *DYNA* 97, no. 1 (Jan-Feb 2022): 92-97, https://doi.org/10.6036/10085.

[7] Fred Bedrich, "A cyber hygiene checklist can help prevent attacks on your business," 2022, https://www.bdc.ca/en/articles-tools/blog/cyber-hygiene-checklist-can-help-prevent-attacks-on-your-business.

[8] RSI Security, "The top 11 rules of cyber hygiene for government agencies," 2022, https://blog.rsisecurity.com/the-top-11-rules-of-cyber-hygiene-for-government-agencies/.

[9] Abi Tyas Tunggal, "What is cyber hygiene and why is it?" *UpGuard*, June 2022, https://www.upguard.com/blog/cyber-hygiene.

[10] "Top tips for cyber hygiene to keep yourself safe online," *kaspersky*, 2022, https://www.kaspersky.com/resource-center/preemptive-safety/cyber-hygiene-habits.

[11] Kaspersky Lab Global Research and Analysis Team, "Syrian Malware, the Ever-evolving Threat," Version 1.0, August 2014.

[12] Europol, "The Internet Organized Crime Threat Assessment (IOSTA)," 2015, https://doi.org/10.2813/03524.

About the Authors

Flotilla Adm. Prof. **Boyan Mednikarov**, D.Sc., graduated first in class at Nikola Vaptsarov Naval Academy in Varna in 1984. He went through the positions of Executive Officer, Commanding officer, Commander of a tactical group of ships, and Chief of staff of a squadron. He has a Doctor of Science degree in Military-Political Aspects of Security. Since 2009, Flotilla Adm. Prof. Mednikarov is a professor in the same academic field. Since May 2011, he is the Rector of Nikola Vaptsarov Naval Academy. Areas of expertise: Defence and Strategic Studies, Maritime Security and Safety, Maritime Education System, Leadership and Management in Shipping. https://orcid.org/0000-0003-4247-897X

Colonel, Assoc. Prof. **Yuliyan Tsonev**, Ph.D., graduated ex Artillery and Air-Defence Academy in Shumen in 1986, "Military Cybernetics" specialty with honor. After his graduation, he is involved in a team developing automated IT and C4I systems. He got his Ph.D. degree in 1994 in Military Scientific Research Institute, Sofia. In 2002 he is an associate professor at Nikola Vaptsarov Naval Academy, where from 2014 onward he is the head of the IT department. He is a certified Cisco Academy Instructor (CCAI 887122): ITE, CCNA, CCNP, CCNA Security, Cyber Ops and Cisco DevNet instructor. https://orcid.org/0000-0001-5602-4747

Commander **Borislav Nikolov**, Ph.D. graduated from Nikola Vaptsarov Naval Academy in Varna in 2004. He went through different positions in the IT support team of the Nikola Vaptsarov Naval Academy, including head of this team. He got his Ph.D. degree in 2021. Currently, he is an assistant professor in the IT department and the manager of the Security Operations Training Center of the academy. In the last two years, he participated in the US Fulbright-sponsored exchange program "Cybersecurity in Universities." His fields of interest include system administration (Windows Server and Linux), virtualization, and physical security systems. https://orcid.org/0000-0002-6055-8538

Prof. Dr.Sc Andon Lazarov received an M.S. degree from Saint Petersburg Electro-Technical State University (LETI), Russia, Candidate of Science degree from Minsk Air-Defence Military Academy, Belarus, and Dr. of Sc. degree from Shumen Artillery and Air Defence Academy He is a Professor at Nikola Vaptsarov Naval Academy – Varna. His field of interest includes SAR/ISAR modelling and signal processing techniques. He has authored above 100 research journals and conference papers. He is a member of the editorial and reviewer boards of many international journals in the USA, Canada, Great Britain, China, Greece, Pakistan, etc. https://orcid.org/0000-0003-2115-4415