REZUME

OF SCIENTIFIC WORKS

of Colonel. Ass. Prof. Dr. Eng. NIKOLAI TODOROV STOIANOV

Scientific works are presented in three categories:

I. Monographic works and university textbooks

II. Scientific articles and reports

III. Scientific research and development

I. MONOGRAPHIC WORKS AND UNIVERSITY TEXTBOOKS

II.1.3. G. Velev, M. Bozhilova, **N. Stoianov**, **COMPUTER NETWORKS AND COMMUNICATIONS**, Publishing House "About the letters - O pismeneh", ISBN - 978-619-185-148-5, Sofia, 2014, volume: 208 p., COBISS. BG-ID – 1269811940

The monograph is devoted to computer networks, the basic principles of their operation and construction. The two most applicable network models as the basis of network communications are discussed and compared. The theoretical and physical foundations of communication environments are presented. The book is structured on the basis of the OSI model, with the focus of consideration and analysis being the protocols identified in the TCP/IP protocol stack.

II.1.4, **N. Stoianov**, **INFORMATION SECURITY**, Publishing House "About the letters - O pismeneh", ISBN - 978-619-185-130-0, Sofia, 2014, volume: 156 pages, COBISS. BG-ID – 1269970404

This book discusses issues related to the information security. The basic concepts, the different aspects in information security are presented. Attention is paid to the basic formal models, basic elements of cryptography as a science are given, various traffic security protocols, and technology solutions for security, such as virtual private networks and public key architecture, are presented.

II.1.5. Alexander Kott, **Nikolai Stoianov**, Nazife Baykal, Alfred Moller, Reginald, Sawilla, Pram Jain, Mona Lange, and Cristian Vidu, **ASSESSING MISSION IMPACT OF CYBERATTACKS**: Report of the NATO IST-128 Workshop, studios, ARL-TR-7566, DEC 2015, US Army Research Laboratory, ATTN: RDRL-CIN, 2800 Powder Mill Road, Adelphi, MD 20783-1138, 38 pp.

This report presents the results of a workshop held by the Information Systems Group (IST) of the NATO Science and Technology Organization in Istanbul, Turkey, June 2015, to explore technologies to characterize the impact of cyberattacks on different types of missions. The success of the military mission is highly dependent on the communication and information systems (CIS) that support the mission and their use in cyberspace. The inexorably growing dependence on processing computational information on weapons, intelligence, communication and logistics systems continues to increase the vulnerability of missions to various cyber threats. Attacks on CIS or other cyber incidents aggravate or interrupt the use of CIS. The frequency and complexity of these incidents is expected to increase.

II.1.6. V. Tselkov, O. Ismailov, **N. Stoianov**, **RISK MANAGEMENT, TESTING AND ASSESSMENT OF NETWORK AND INFORMATION SECURITY**, monograph, "About the letters – O pismeneh", ISBN 978-619-185-159-1, Sofia, 2016, volume: 334 pages.

Research, standards and good practices related to risk management, testing and evaluation of network and information security are discussed in this book.

The pretentious title indicates that the content covers a large area of the subject area of information security in computer systems and networks. The following directions can be clearly highlighted in the exposition:

- *Fundamentals of information technology security;*
- *Information security testing;*
- *Network and information security assessment;*
- *Development of 'good practice' standards for the protection of information in computer systems and networks.*

II.1.7. D. Polimirova, V. Shalamanov, **N. Stoianov**, T. Tagarev, Y. Yanakiev, G. Sharkov, Y. Papazov, V. Rizov, K. Ivanova, **CYBERSECURITY AND OPPORTUNITIES FOR APPLICATION OF INNOVATIVE TECHNOLOGIES IN THE WORK OF THE STATE ADMINISTRATION IN BULGARIA, CHAPTER OF** MONOGRAPH, Institute of Public Administration, Sofia, 2018, ISBN: 978-619-7262-14-8, 285 pages.

The aim of this study is to identify gaps in the regulations of cybersecurity and resilience activities in the Republic of Bulgaria, to identify good practices in the European Union and NATO and to define proposals for improving the regulatory framework, policies and strategies to ensure the secure and sustainable functioning of the state, economy and society in cyberspace.

II.1.8. V. Tselkov, **N. Stoianov**, **TOOLS FOR TESTING AND ANALYSIS OF COMMUNICATION AND INFORMATION SYSTEMS SECURITY**, PUBLISHED UNIVERSITY TEXTBOOK, "About the letters – O pismeneh", ISBN 978-619-185-466-0, Sofia, 2021 volume: 157 p., COBISS. BG-ID - 46606344

The textbook presents the educational content of the course with the same name from the program "Information Security", "National Security" and "Communications and Information" of the University of Library Studies and Information Technologies. Some of the results obtained from the studies and research carried out at the Ministry of Defence, the Commission for Personal Data Protection and the University of Library Studies and Information Technologies are also presented. The content is also based on good practices and global standards, especially the standards of the United States of America (USA). The textbook contains an introduction, four chapters, five appendices, a conclusion, literature and information about the authors.

II. SCIENTIFIC ARTICLES AND REPORTS

II.2.11. **N. Stoianov**, A. Geov, **CYBERSECURITY ARCHITECTURE – TECHNOLOGICAL ASPECTS**, Scientific and Applied Article, CIO Issue 7, Year IX, July 2013, p. 64-65, ISSN 13112-5605

The *report examines the main elements in defining cybersecurity architectures. The different features of defining technical requirements for systems and their impact on architecture (in both directions) are taken into account. Existing architectures are considered: the SANS; of Northrop Grumman Corporation (FAN); and the DNDAF.*

II.2.12. **N. Stoianov**, **Cybersecurity Metrics**, Applied Scientific Article, CIO Issue 7, Year XI, July 2015, p. 59-60, ISSN 13112-5605

The report sets out the main requirements for defining cybersecurity metrics. The SMART, PRAGMATIC and SMART-PRAGMATIC approaches are discussed.

II.3.69. V. Tselkov, **N. Stoianov, A QUESTIONNAIRE FOR SECURITY AUDIT OF INFORMATION SYSTEMS**, SCIENTIFIC AND APPLIED REPORT, SCIENTIFIC CONFERENCE WITH INTERNATIONAL PARTICIPATION "Military Technologies and Systems for Defence Assurance 2011 (MT&S 2011), 8-9 December 2011, Sofia, 2012, Defence Institute, ISBN 978-619-90024-1-4, p. 47-55

In this paper, the authors present a model questionnaire for security audit in information systems. The questionnaire is based on BS 7799 and ISO 27000.

II.3.70. **N. Stoianov**, **DIRECTIONS FOR DEVELOPMENT OF CRYPTOGRAPHY AFTER QUANTUM COMPUTER,** SCIENTIFIC AND APPLIED REPORT, SCIENTIFIC CONFERENCE WITH INTERNATIONAL

PARTICIPATION "Military Technologies and Systems for Defence Assurance 2011 (MT&S 2011), 8-9 December 2011, Sofia, 2012, Defence Institute, ISBN 978-619-90024-1-4, p. 56-60

Guidelines for the development of *post-quantum cryptography are presented in this paper. A brief description of the problem of quantum computing affecting cryptography is made. An explanation of the following cryptographic protocols is presented: Cryptography, lattice-based and code-based cryptography, and hash-function-based cryptography. Basic definitions and difficult to solve mathematical problems are given.*

II.3.71. D. Zheliazkov, **N. Stoianov**, **PROBLEMS IN PROTECTING INFORMATION IN CLOUD COMPUTING SOLUTIONS,** Scientific-Applied Report, Scientific Conference with International Participation "Military Technologies and Systems for Defence Assurance 2011 (MT&S 2011), 8-9 December 2011, Sofia, 2012, Defence Institute, ISBN 978-619-90024-1-4, p. 248-256

In this paper, the authors present some aspects and problems of information security in cloud computing environments. A classification of cloud computing services and information infrastructures is made in the study. An analysis of information security issues is presented. The paper presents authors‘ vision, based on their experience in implementing security solutions related to cloud computing in Bulgarian Defence Institute.

II.3.72. **N. Stoianov**, M. Bozhilova, **A STUDY OF LATTICE-BASED CRYPTOGRAPHY,** Scientific-Applied Report, 5th International Scientific Conference on Defensive Technologies, OTEH, 2012, Pages 465-469

Cryptography is one of the most important parts of information security. Most of the asymmetric cryptographic algorithms are based on hard-to-solve mathematical problems. With the increase in the speed of the computers and the huge amount of computer memory, some of these problems will be most probably solved in the near future. In addition, the study of physics, and in particular the development of a quantum computer, will dramatically change the world of cryptography. The so-called Shor and Grover quantum algorithms are facts. These algorithms will disrupt the widely used asymmetric algorithm – RSA. In addition, some groups of new algorithms have been developed and these seem more difficult to solve with quantum algorithms. This paper presents a study of one group of algorithms based on so-called "lattice problems". A basic mathematical definition is given, explanations of lattice problems (shortest-vector problem and nearest vector problem) and related cryptographic problems are shown. The most popular cryptographic schemes are explained and a small numerical example of NTRU with public parameters is given (13, 2, 31, 2).

II.3.74. **N. Stoianov**, E. Altimirski, **A STUDY OF OPEN SOURCE PKI SYSTEMS APPLICABLE INTO INDECT PROJECT**, Scientific-Applied Report, XLVIII International Scientific Conference on Information, Communication and Energy Systems and Technologies, ICEST 2013, 26-29 June 2013, Ohrid, Macedonia, Vol. 1, ISBN: 978-9989-786-90-7, pp. 191-194, http://www.icestconf.org/wp-content/uploads/2016/proceedings/icest_2013_01.pdf

This paper provides a survey of open source PKI systems applicable in the European INDECT project (FP7). The requirements for the type of certificates, the key length and the hierarchical structure are defined in the report. The architecture of the INDECT PKI with two levels of CA is explained. Based on the proposed architecture, two open source PKI systems were studied: OpenCA and EJBCA. In order to establish a testing platform, a number of tests have been performed, which are presented in the report. An EJBCA based scheme *is proposed which offers a PKI architecture and covers all the requirements (system and cryptographic) to create the final INDECT PKI system.*

II.3.75. Manuel Urueña, Petr Machník, Marcin Niemiec, **Nikolai Stoianov**, **INDECT SECURITY ARCHITECTURE**, Scientific-Applied Report, Communications in Computer and Information Science, Volume 368 CCIS, Pages 273 - 2872013 6th International Conference on Multimedia Communications, Services and Security, MCSS 2013, 6 June 2013, through 7 June 2013

To carry out their duties of serving and protecting, the police must deploy new tools and applications to keep pace with technological developments. The INDECT project is developing such new investigation tools, with the aim of supporting the European police force. However, police ICT systems have strict security requirements that may delay the implementation of these new applications. This report presents an integrated security architecture that is able to provide generic security services to both new and legacy ICT applications while fulfilling the high security requirements of the police force. By reusing the security services provided by this architecture, new systems do not have to implement customized security mechanisms themselves and can easily be integrated into the existing police ICT infrastructure. The proposed INDECT security architecture incorporates state-of-the-art technologies, such as encrypted communications at network and application levels or multi-factor authentication based on certificates stored in smart cards.

II.3.76. A. Geov, **N. Stoianov**, **MAIN COMPONENTS OF CYBERSECURITY ARCHITECTURE IN SECURE COMPUTER SYSTEMS**, Scientific-Applied Report, Scientific Session 2013, National Military University, Faculty of Artillery, Air Defence and CIS, Shumen 2013, ISSN 1313-7433

The report, entitled "Main Components of Cybersecurity Architecture in Secure Computer Systems," provides a basic cybersecurity system structure for communication and information systems. The proposed structure is divided into two main areas: technological components and functional components. The proposed components are explained and the relationship between them and domains is given. The proposed approach is the result of the authors' work in the field of cybersecurity and cyber defence.

II.3.77. Z. Zdravkov, **N. Stoianov**, I. Radulov, **TECHNOLOGICAL CAPABILITIES FOR CONDUCTING CYBER OPERATIONS,** Scientific-Applied Report, Scientific Session 2013, National Military University, Faculty of Artillery, Air Defence and CIS, Shumen 2013, ISSN 1313-7433

This document presents a summary of *Cyber Operation Technologies. Technologies that are classified as cyber weapons and resources of cyber defence.*

II.3.79. I. Nenov, N. **Stoianov**, V. Tselkov, **APPROACHES TO VULNERABILITY ASSESSMENT IN COMPUTER NETWORKS AND SYSTEMS**, Scientific-Applied Report, Modern Strategies and Innovations in Knowledge Management, Proceedings, The First Scientific Conference "Modern Strategies and Innovations in Knowledge Management": ULSIT, 3-4 December 2014, Publishing House "About the Letters – O Pismeneh", Sofia, 2014, ISBN 978-619-185-140-9, p. 256-268

The approach examined in the report is based on an automated vulnerability assessment of Tenable Network Security Nessus scanners and The Open Vulnerability Assessment System (OpenVAS). A comparative analysis of the advantages and disadvantages of both products is made.

II.3.80. **N. Stoianov**, M. Urueña, M. Niemiec, P. Machník, G. Maestro, **INTEGRATED SECURITY INFRASTRUCTURES FOR LAW ENFORCEMENT AGENCIES**, Scientific-Applied Report, Multimedia Tools and Applications, Open Access, Volume 74, Issue 12, Pages 4453 - 4468, 13 June 2015

This report provides an overview of the Security Architecture of Law Enforcement Agencies (LEA) developed in the INDECT project and in particular of the security infrastructures that have been deployed so far. These security infrastructures can be organized into the following main areas: public key infrastructure (PKI) and user management, communications security and new cryptographic algorithms. The new ideas, architectures and deployed testing platforms for these areas are presented. In particular, the internal structure of INDECT PKI used for federal identity management is explained, the different technologies used in the test VPN, INDECT Block Cipher (IBC) – a new cryptographic algorithm that is integrated into the OpenSSL library and how IBC-

enabled TLS/SSL sessions and X.509 certificates are used to protect INDECT applications. All proposed mechanisms are designed to operate in an integrated way as a basis for the security of all systems developed by the INDECT project for LEA.

II.3.82. Manuel Urueña, Petr Machník, Marcin Niemiec, **Nikolai Stoianov**, **SECURITY ARCHITECTURE FOR LAW ENFORCEMENT AGENCIES**, Scientific-Applied Report, Multimedia Tools and Applications, Open Access, Volume 75, Issue 17, Pages 10709 - 107321 September 2016

To meet their duty to serve and protect, law enforcement agencies (LEAs) need to deploy new tools and applications to keep pace with evolving technologies. However, police information and communication technology (ICT) systems have stringent security requirements that may delay the deployment of these new applications because the necessary security measures must be implemented first. This paper presents an integrated security architecture for LEA that is able to provide generic security services to new and legacy ICT applications while fulfilling the high security requirements of the police force. By reusing the security services provided by this architecture, new systems do not have to implement customised security mechanisms themselves and can be easily integrated into existing police ICT infrastructures. The proposed LEA security architecture includes the most modern state-of-the-art technologies such as encrypted communications at network and application levels or multi-factor authentication based on certificates stored in smart cards.

II.3.83. D. Mahlyanov, N. Stoianov, **INTERNET OF THINGS (IOT),** Scientific-Applied Report, Eighth International Scientific Conference "HEMUS-2016", p.III-217 - III-225 (2016-)

Internet of Things (IoT) exists these days with all its benefits and risks. This article briefly describes the essence of IoT and the main security issues in IoT. Different types of IoT attacks are indicated, as well as some issues related to the implementation of IoT systems. A basic concept for creating a secure environment with IoT is presented.

II.3.84. M. Koutsakis, **N. Stoianov**, **CYBERSECURITY MODELING LANGUAGE – CYSEMOL**, Scientific-Applied Report, Eighth International Scientific Conference, Scientific Research – a Key Factor for the Acquisition of New Defence Capabilities, HEMUS-2016, 26 May 2016, Sofia, 2016 ISSN 1312–291

Over time, IT systems have grown. This has led to an increase in both the complexity and the difficulty of maintaining a complete knowledge of the system. In addition, the possibilities for attack and the number of vulnerabilities in the system are growing. This leads to problems for administrators and security officers, who often work on a tight budget and need to prioritize where to explore or improve the *system. Various tools have been proposed to assist decision makers in this kind of problem. Such a tool is CySeMoL (Cyber Security Modeling Language), which uses Bayesian networks to calculate security risks in a system model. By using CySeMoL to model known previous attacks, it is possible both to validate the model and to find areas that can be improved.*

II.3.85. **N. Stoianov**, L. Petrov, **CRITICAL INFRASTRUCTURE OVERVIEW - BASICS, DEFINITIONS, TYPES**, Scientific-Applied Report, Eighth International Scientific Conference, Scientific Research – a Key Factor for the Acquisition of New Defence Capabilities, HEMUS-2016, 26 May 2016, Sofia, 2016 ISSN 1312–291

The report presents basic concepts, definitions and types of critical infrastructures. On the basis of the presented classification, major security threats in these infrastructures have been identified. On the basis of the analysis, a model for the protection of critical infrastructure is proposed.

II.3.86. D. Atanasova, **N. Stoianov**, **CYBERSECURITY IN BULGARIA AND PAN-EUROPEAN STRUCTURES**, Scientific-Applied Report, Eighth International Scientific Conference, Scientific Research – a Key Factor for the Acquisition of New Defence Capabilities, HEMUS-2016, 26 May 2016, Sofia, 2016 ISSN 1312–291

The report reviews the main 'players' in the EU in the field of cybersecurity. Their fields of action and potential capabilities are presented. On the basis of the analysis, a model for coordination in the field of information protection and cybersecurity is proposed. The results obtained for the EU in order to build capacity in the Republic of Bulgaria are also interpreted.

II.3.87. Y. Kolegova-Delcheva, **N. Stoianov**, **ANALYSIS OF CYBERSECURITY IN THE ARMED FORCES**, Scientific-Applied Report, Eighth International Scientific Conference, Scientific Research – a Key Factor for the Acquisition of New Defence Capabilities, HEMUS-2016, 26 May 2016, Sofia, 2016 ISSN 1312–291

The rapid development of information systems, globalization and technological process are a prerequisite for the development of the cybercrimes. The rapidly growing number of cybercrimes, the use of the Internet by terrorists make it necessary to conduct an effective and efficient cybersecurity policy. Cybersecurity policy is present in all public and private structures, but the leading structures in maintaining peace and ensuring security are the armed forces. Therefore, they are expected to create, adopt and implement mechanisms to counteract the cyberattacks.

II.3.88. I. Ivanov, **N. Stoianov**, **ANALYSIS OF ARCHITECTURES FOR CLOUD SERVICES**, Scientific-Applied Report, Scientific Conference with

International Participation "Cloud Technologies and Information Protection", 12-13 May 2016, Shumen

The report analyzes the different types of cloud architectures – SaaS, PaaS, IaaS and the different types and ways of develop cloud systems – public, private and mixed. Based on the analysis, approaches for creating "specialized architectures for cloud services" are proposed.

II.3.89. L. Petrov, **N. Stoianov**, T. Tagarev, **CRITICAL INFORMATION INFRASTRUCTURE PROTECTION MODEL AND METHODOLOGY, BASED ON NATIONAL AND NATO STUDY,** Scientific-Applied Report, In: Zamojski, W., Mazurkiewicz, J., Sugier, J., Walkowiak, T., Kacprzyk, J. (eds) Advances in Dependability Engineering of Complex Systems. DepCoS-RELCOMEX 2017. Advances in Intelligent Systems and Computing, vol 582. Springer, Cham. https://doi.org/10.1007/978-3-319-59415-6_34

National and international security, our financial, industrial and economic prosperity, the health system and the national well-being as a whole depend on critical infrastructures that can be described as highly interdependent. Many examples are available, such as the national electricity network, oil and natural gas systems, telecommunications and information networks, transportation networks, water systems, banking and financial systems. Keeping them in a reliable and secure state and learning their dependencies is of main importance for any government or organization. There is an urgent need for their classification. Creating and developing a model and methodology that could describe their behavior will make this world safer. The model presented here and the research based on it and initial results are steps towards a reliable and secure critical information infrastructure.

II.3.90. **Nikolai T. Stoianov**, Maya G. Bozhilova, Grigor R. Velev, **TOWARDS SECURITY REQUIREMENTS OF THE SPIDER PROJECT**, Scientific-Applied Report, International Scientific Conference "Cybersecurity in the Information Society", Collection of Scientific Works, MW "V. Levski" – Faculty of Artillery, Air Defence and CIS, Shumen 2017, ISBN 978-954-9681-82-6, p.25-p.31

The need to use sensor systems and networks for intra-building situational awareness in urban military operations requires strict requirements for their security and reliability. The report defines concepts related to security in accordance with the purpose and functions of the sensor system.

II.3.91. D. Mahlyanov, N. Stoianov, **CYBERSECURITY ANALYSIS IN INTERNET OF MILITARY THINGS MODELS**, Scientific-Applied Report, International Scientific Conference "Cybersecurity in the Information Society", Collection of Scientific Works, MW "V. Levski" – Faculty of Artillery, Air Defence and CIS, Shumen 2017, ISBN 978-954-9681-82-6, p.32-p.39

IoT is expanding into different areas of our lives. IoMT is almost a brand new branch of IoT. This paper briefly describes the main IoMT implementation models based on information processing. The report carried out an analysis focusing on cybersecurity for different models.

II.3.92. L. Petrov, N. Stoyanov, **MULTI-LAYER CYBERSECURITY MODEL FOR CRITICAL INFORMATION INFRASTRUCTURE**, Scientific-Applied Report, International Scientific Conference "Cybersecurity in the Information Society", Collection of Scientific Works, MW "V. Levski" – Faculty of Artillery, Air Defence and CIS, Shumen 2017, ISBN 978-954-9681-82-6, p.124-p.129

National and international security, our national well-being depend on critical information infrastructures that can be described as highly interdependent. Keeping them in a reliable and secure state and studying their dependencies is crucial to any government or organization. The creation and development of a multi-layered cybersecurity critical information infrastructure model will make this world safer. The model described here is a step towards a reliable and secure critical information infrastructure.

II.3.93. M. Koutsakis, N. Stoyanov, **TECHNOLOGICAL MODEL FOR CYBERSECURITY IN THE STATE ADMINISTRATION**, Scientific-Applied Report, International Scientific Conference "Cybersecurity in the Information Society", Collection of Scientific Works, MW "V. Levski" – Faculty of Artillery, Air Defence and CIS, Shumen 2017, ISBN 978-954-9681-82-6, pp.140-146

The state administration is part of the mechanism of public control. The state administration provides citizens with a number of services. These services are working thanks to good planning and reliable infrastructure. The services provided by public administrations are protected and built through specific plans and steps by: "National Cybersecurity Strategy". The transfer of these services to the digital world with incorrect computer and network structure can lead to many vulnerabilities. Providing a connection and any technical means is imperative for the proper and safe functioning of the services.

II.3.94. Enev E., Velev G., **Stoianov N**., Bozhilova M., **REQUIREMENTS TO THE SENSOR PLATFORM AND NETWORK FOR INDOOR DEPLOYMENT AND EXTERIOR BASED RADIOFREQUENCY AWARENESS**, International Research Conference "105 Years Research and Knowledge for the Security and Defence, Bulgarian Military Academy "G. S. Rakovski", 6-7 April, Sofia, 2017

The main information in this report is on the results of the study of the problems required when using a sensor platform and network for internal deployment and externally based radio frequency awareness in urban operations. Basic tactical requirements and spatio-temporal parameters in which the technical means of acquiring information and data have to operate have been selected. The report serves alsoasadditional information on future trends of experiments in this project.

II.3.95. T. Tagarev, G. Sharkov, **N. Stoianov**, **CYBER SECURITY AND RESILIENCE OF MODERN SOCIETIES: A RESEARCH MANAGEMENT ARCHITECTURE,** Scientific-Applied Report, 16 Information & Security: An International Journal, Volume 38, p.93-108 (2017), http://dx.doi.org/10.11610/isij.3807

Advanced Information and Communication Technologies (ICT) facilitate the increased effectiveness and efficiency of defence and security organizations, government services, the economy, and quality of life, while at the same time providing opportunities for malicious actors to cause significant damage. Security and resilience policies of modern societies to cyber threats and risks take into account the envisaged cyber threats, their immediate impact on ICT infrastructure, the subsequent effects on critical services, as well as the cascading effects in systems and infrastructures. This report presents the architecture used for planning and, therefore, managing cybersecurity research in Bulgaria. It covers five application areas (information management systems; industrial control systems; unmanned and remotely piloted vehicles; biointegrated systems, and cognitive processes and decision-making), systems of systems research, and support for the formulation and implementation of cybersecurity policy.

II.3.96. Lytvynov, V., **Stoianov, N**., Skiter, I., Trunova, H., & Hrebennyk, A, **ЗАХИСТ КОРПОРАТИВНИХ МЕРЕЖ ВІД АТАК З ВИКОРИСТАННЯМ КОНТЕНТ-АНАЛІЗУ ГЛОБАЛЬНОГО ІНФОРМАЦІЙНОГО ПРОСТОРУ**, Scientific-Applied Report, Technічні Sciences ta Technologї, (1(11), 115–130. Viluceno I http://tst.stu.cn.ua/article/view/135504

The aim of the article is to organize collective protection of corporate networks by introducing threat monitoring systems, active intelligence activities in the global information area in order to search, collect and analyze data on attacks, unusual behavior and content of Internet resources.

II.3.98. V. Litvinov, N. **Stoyanov**, I. Skiter, O. Trunova, A. Grebennik, **АНАЛІЗ СИСТЕМ ТА МЕТОДІВ ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНИХ ВТОРГНЕНЬ У КОМП'ЮТЕРНІ МЕРЕЖІ, Научно-приложен доклад, Інформаційні і телекомунікаційні технології, УДК 004.056.5, ISSN 1028-9763.**

The report presents a mathematical approach to form an approach of normal functioning of systems and define a generalized assessment of the state of the system to be protected. The main disadvantages and guidelines for further development of intrusion detection systems are described.

II.3.99. Tagarev, Todor & **Stoianov, Nikolai** & Sharkov, George, **INTEGRATIVE APPROACH TO UNDERSTAND VULNERABILITIES AND ENHANCE THE SECURITY OF CYBER-BIO-COGNITIVE-PHYSICAL SYSTEMS**, Scientific-Applied Report, (2019) Conference: 18th European Conference on Cyber Warfare and Security ECCWS 2019At: University of Coimbra, Portugal, 2019 pp. 492-500

This paper outlines the problem of vulnerability of each of the five domains to influences from cyberspace. It presents some achievements in cross-domain understanding of vulnerabilities, supported by examples of cybersecurity studies and provides the outlines of a relevant interdisciplinary research program developed around the concept of systems from systems. The authors conclude by predicting that the field of cybersecurity will be subject to significant growth in the coming years, requiring multi- and interdisciplinary competencies and scientific support.

II.3.100 A. Ivanov, **N. Stoianov**, **NEW APPROACH OF SOLVING CONGRUENCE EQUATION SYSTEM**, Scientific-Applied Report, Communications in Computer and Information Science, Volume 1284 CCIS, Pages 16 - 24, 2020 10th International Conference on Multimedia Communications, Services and Security, MCSS 2020, Kraków, 8 October 2020through 9 October 2020

Currently, some special basic algorithms are used in public-key cryptography. The advanced Euclidean algorithm and the Chinese remainder theorem are the most common basic algorithms. In recent years, mathematicians have done much to improve the speed of execution of these algorithms. This paper presents a new approach to solving a system of congruence equations.

II.3.101 M. Pappalardo, M. Niemiec, M Bozhilova, **N. Stoianov**, A. Dziech, B. Stiller, **MULTI-SECTOR ASSESSMENT FRAMEWORK – A NEW APPROACH TO ANALYSE CYBERSECURITY CHALLENGES AND OPPORTUNITIES,** Scientific-Applied Report, Communications in Computer and Information Science, Volume 1284 CCIS, Pages 1 – 15, 2020 10th International Conference on Multimedia Communications, Services and Security, MCSS 2020, Kraków8 October 2020, through 9 October 2020

In this report, a new approach to analyzing cybersecurity challenges and opportunities, focused on developing a new framework for risk assessment and management, is presented. Such a multi-sectoral assessment framework should be able to assess and prioritize cybersecurity risks in an inter-agency and cross-sectoral *context. This leads to a proper allocation of resources and mitigation actions after an attack.*

II.3.102 I. Burmaka, **N. Stoianov**, V. Lytvynov, M. Dorosh, S. Lytvyn, **PROOF OF STAKE FOR BLOCKCHAIN BASED DISTRIBUTED INTRUSION DETECTING SYSTEM,** Scientific-Applied Report, Advances in Intelligent Systems and Computing, Volume 1265 AISC, Pages 237 – 247, 2021 15th International Scientific-Practical Conference on Mathematical Modeling and Simulation of Systems, MODS 2020, Chernihiv29 June 2020through 1 July 2020

One of the most important components of any corporate network is the intrusion detection system. At the same time, however, it is difficult to find a mechanism for establishing trust between nodes in a large distributed system. Blockchain can be used as such a mechanism, but most working blockchains use cases related to cryptocurrencies. In this report, the authors propose several modifications to the proof-of-partition consensus protocol to be adopted for use with blockchain-based IDS. Also, an agent-based model has been created to simulate a staking process for our modified consensus protocol. The modelling result will help to evaluate the performance of blockchain-based IDS in normal state and in some critical situations and to find the most appropriate consensus protocol parameters depending on the network size.

II.3.103 Bozhilova, M., Yanakiev Y., **Stoianov N.**, & Stoianov D., **AN APPROACH FOR PRIORITISATION**, Scientific-Applied Report, Journal of Defence & Security Technologies 3, no. 1 (2020): 55-83

This article aims to propose a methodology for prioritizing national interests. It begins by researching and defining the key term – national interest. The focus of the definition is on the long-term and relatively stable goals that nations strive to achieve. The paper then presents an overview of existing methods for assessing national interests. The main part of the article is focused on the proposed approach for prioritizing the national interests of the EU member states, based on expert assessment methods and more precisely the evaluation is done by applying an Analytical Hierarchical Process. Finally, an illustrative example of verification and validation of the proposed methodology is described.

II.3.104 Y. Yanakiev, **N. Stoianov**, D. Kirkov, G. Velev, **DEFENCE STRATEGY AND NEW DISRUPTIVE TECHNOLOGIES NEXUS: IMPLICATIONS FOR THE MILITARY ORGANISATIONS,** Scientific-Applied Report, Journal of Defence & Security Technologies, Volume 3, Issue 1, Number 2, p.7-41 (2020)

This paper aims to explore the role of strategy in the field of defence, with a special focus on how technological innovation can influence strategy *development. The key question is how and in what ways technological progress can affect the development of defence strategy. It begins with the evolution of the concept of defence strategy in recent years, as well as its possible future transformation, in parallel with the trends of new and emerging defence technologies. Then, different conceptual models of defence strategy are analyzed based on case studies of national defence strategy documents presented in the EU Predictive methodologY for Technology Intelligence Analysis (PYTHIA) project consortium, as well as EU and NATO documents. Finally, the paper summarizes some conclusions regarding the dynamic nature of the interrelationship between defence strategy development and technological innovation. In addition, some ideas are presented regarding how defence research can meet operational needs by supporting with new knowledge the production and supply of the most needed weapon systems.*

II.3.105 **Nikolai Stoianov**, Andrey Ivanov, **PUBLIC KEY GENERATION PRINCIPLES IMPACT CYBERSECURITY,** Scientific-Applied Report, Information & Security: An International Journal, Volume 47, Issue 2, p.249-260 (2020)

Public key cryptographic algorithms are based on the laws and principles of number theory. For any cryptographic system, one of the most important issues is the user's key that he/she uses to encrypt the messages. This is the reason why the process of key generation is always fundamental to data protection, and because cryptography takes up more space in our daily lives, the principles of public key generation are so important. In this paper, the authors discuss the Miller-Rabin primality test in its relation to the key generation process.

II.3.106 **Nikolai Stoianov**, Maya Bozhilova, A **MODEL OF A CYBER DEFENCE AWARENESS SYSTEM OF CAMPAIGNS WITH MALICIOUS INFORMATION**, Scientific-Applied Report, Information & Security: An International Journal, Volume 46, Issue 2, p.182-197 (2020)

Many organizations are subjected to cyberattacks to spread malicious information. Situational awareness is a tool to counter campaigns of malicious information and reduce its spread. This paper proposes a conceptual model for a cyber-defence awareness system that aims to assist human operators to avoid this type of threat. The system will identify (classify) three types of campaigns for malicious information operations – malicious injection of information into web content, injection of malicious information into fake social network accounts, and dissemination of malicious information through email messages. A model for identifying the type of campaign of malicious information operations based on Dempster-Shafer theory of evidence is proposed. The work presented here is part of the project Cyber Rapid Analysis for Defence Awareness of Real-time Situation - CyRADARS.

II.3.107 Todor Tagarev; Salvatore Marco Pappalardo; **Nikolai Stoianov**, **A LOGICAL MODEL FOR MULTI-SECTOR CYBER RISK MANAGEMENT**, Scientific-Applied Report, Information & Security: An International Journal, Volume 47, Issue 1, p.13-26 (2020)

The increasing use of digital infrastructures makes entire sectors of the economy and public services vulnerable to cyber-attacks. Some progress has been made in understanding vulnerabilities and ways to reduce cyber risk at the subsector level. While the sectoral level remains a significant challenge, this study goes beyond, addressing also the cyber risk arising from cross-sectoral and multi-sectoral interdependencies in a consistent logical model. The paper presents the scope of this logical model, outlines the problem of risk assessment structured around the triplet "Threats – Vulnerabilities – Impact" and the structuring of risk mitigation around the types of risk reduction measures, the purpose of risk decision making and modes of application. Examples are provided of the application of the logical model underlying the ECHO multisectoral evaluation framework and concludes by highlighting the advantages that the logical model and framework provide.

II.3.108 Velizar Shalamanov, **Nikolai Stoianov**, Yantsislav Yanakiev, **ICT GOVERNANCE, HUMAN FACTORS AND CYBER SITUATIONAL AWARENESS,** Scientific-Applied Report, Information & Security: An International Journal, Volume 46, Issue 1, p.7-10 (2020)

The article summarizes the results of the four sessions during the Second International Scientific Conference Digital Transformation, Cybersecurity and Resilience DIGILIENCE 2020. These are developing and managing ICT for digital transformation, Cyber Situational Awareness and Information Exchange, Approach to Integrating Human Systems to Cybersecurity and Education and Training for Cyber Resilience.

II.3.109 **Nikolai Stoianov**, Maya Bozhilova, **EXPERT'S STUDY ON SITUATIONAL AWARENESS OF OPERATIONS DIRECTED AT THE WIDE DISSEMINATION OF MALICIOUS INFORMATION**, Scientific-Applied Report, Conference Proceedings, MODS2020, Chernihiv, Ukraine (2020)

The report presents the results of an expert study in the context of the CyRADARS project for the needs of the so-called. end users in the development of the system for monitoring malicious activities in cyberspace. On the basis of the research, the directions for the development of the system are defined.

II.3.110 T. Tagarev, **N. Stoianov**, **SCOPING THE SCENARIO SPACE FOR MULTI-SECTOR CYBERSECURITY ANALYSIS**, Scientific-Applied Report, "Studies in Big Data", Volume 84, Pages 203 - 217, 2021

The report presents the results of the Horizon 2020 ECHO project, supporting the identification and development of cyber-attack scenarios. It explores scenario space in four dimensions: (1) critical infrastructures and basic services critically dependent on ICT infrastructure; (2) types of malicious actors and their capabilities; (3) exploited vulnerabilities; and (4) short versus longer term horizon. The study serves to comprehensively cover the space of scenarios. The authors present a partial list of selected scenarios, storylines and use cases that are used in follow-up research to identify key components of capability requirements: technology roadmaps, cyber skills framework, information exchange and certification requirements.

II.3.111 P. Vasilev, **N. Stoyanov**, Ts. Tsonev, **APPROACH IN THE PREPARATION OF INNOVATIVE CYBERSECURITY TRAINING PROGRAMS**, Scientific-Applied Report, Proceedings of the International Scientific Conference Advanced Research and Technologies for Defence, ARTDef – 2021, 29 – 30 June 2021, Nikola Yonkov Vaptsarov Naval Academy – Varna, ISSN 2815-2581, 2021, II-186

This report presents an approach to creating innovative cybersecurity training programs in the field of aviation, energy networks and naval forces selected in the European Commission's FORESIGHT project and considers the advantages of this approach.

III. SCIENTIFIC RESEARCH AND DEVELOPMENT

II.4.22. Methodology for anticipating trends in the development of military technologies and their impact on the construction of the defence capabilities of the Republic of Bulgaria, Ministry of Defence - Program 7.1, National Science Project, IE, 2019

The main objective of the project is to develop and experiment methodology and to offer views and recommendations for permanent monitoring to identify emerging technologies and their impact on the development of defence capabilities in long term.

II.4.23. Acquisition of sensor information from land, water and unmanned aerial vehicles and visualization in a decision room, Ministry of Defence - Program 7.1, Program 7.2, Program 1.7.7, National Science Project, IE, 2018

The aim of the project is to explore and provide the opportunity to obtain, send and visualize real-time information from an area of operational (crisis) information by using mobile land, water and unmanned aerial vehicles (off-road *vehicles, radio-controlled boats, drones, etc.) and subsequent computer processing of the received information from sensors and visualization in a decision-making center.*

II.4.24. Building a prototype of a highly reliable cloud (Cloud) architecture, providing a platform for information services and secure information exchange in a data center system, Ministry of Defence‒Program 7.1, Program 7.2 and Program 1.7.7, 2016 - 2019, National Science Project, IE, 2016

The main objective of the project is to develop a prototype of a high-availability cloud architecture to provide an information service platform and secure exchange (replication) of information in a system of data centers for the needs of the Ministry of Defence and the Bulgarian Academy of Sciences by using modern visualization technologies.

II.4.25. Malicious Network Activities Monitoring and Data Analysis (MAMA), Ministry of Defence - Program 7.1 "Research Activities and Projects", 2019 - 2022. National Science Project, IE, 2019

The project aims to create approaches to intercept and analyze cyberattacks in order to explore potential cyber threats in three Internet-connected departmental networks – the Defence Institute "Prof. Tsvetan Lazarov", the Ministry of Defence and the National Laboratory of Computer Virology – BAS. The idea is to install the same type of Honeypot in the three networks. This Honeypot will configure itself to monitor threats from the Internet. The data collected by Honeypot will be mapped against system log records, thus obtaining a picture of the malicious attacks on the networks of the three organizations.

Based on a statistical analysis of the collected information, situational awareness of threats in the national cyberspace will be improved, sources of threats, as well as the most common types of attacks will be identified. The results of the analysis will allow help for the development of theoretical foundations, methods and recommendations for cyber protection of computer networks in MoD and Bulgarian Army.

In the context of the increasing by amount, intensity and damages caused by cyberattacks, the results of the project are extremely important for the acquisition of the cyber defence capability.

II.4.26. Homemade Explosives and Recipes characterizations (HOMER) EU project, FP7-SECURITY, Grant agreement ID: 312883, EC-2012.1.3.2, Coordinated by Police Service of Northern Ireland United Kingdom, 2013-2016, International Science Project (FP7), Defence Institute, 2016.

The aim of the HOMER project is to implement a comprehensive, coherent European survey of home-produced explosives, including the identification, detection *of explosives, the prevention of threats from home-produced explosives and the easy identification of bomb factories.*

II.4.27. GAP - Gaming for Peace, H2020, Grant agreement ID: 700670, H2020-BES-2014-2015, DOI https://doi.org/10.3030/700670, International Science Project (H2020), Defence Institute, 2018.

The GAP project proposes an iterative process of developing and refining a curriculum for military, police and civilian personnel who evaluate the game and the built-in basic/baseline curriculum by playing the game and thus bringing their own experience to the game. In this way, they further develop the CPPB curriculum and relevant soft skills. The game can be accessed anywhere over the Internet and there is no limit of the number of staff that can be trained. The game can be customized at a low cost by various stakeholders. The GAP consortium is multidisciplinary with expertise in social sciences, computer science, end-users (including army and police) and SMEs specializing in game design, curriculum development and skills standardization and harmonization.

II.4.28. SOLOMON - Strategy oriented analysis of the market forces in EU defence "H2020, Grant agreement ID: GA 831379 – SOLOMON, PADR-STF-02-2018" International Science Project (PADR), Bulgarian Defence Institute, 2021

The SOLOMON project intends to bring together the two complementary visions of grand strategy (as derived from the geo/political/economic positions of the EU) and business strategy (as derived from Michael Porter's value chain theory) to outline the possible roadmaps for dealing with the supplies risk for EU armed systems in a world of changing strategies, emerging technologies and changing government constraints.

II.4.29. PYTHIA - Predictive methodology for technology intelligence analysis, H2020, Grant agreement ID: GA 800893 – PYTHIA, PADR-STF-01-2017, International Science Project (PADR), Defence Institute, 2019

The PYTHIA project aims to produce an innovative methodology for strategic technology foresight, capable of providing frequent 'forecasts' on technology-related issues, including the discovery of major trends in a selected area.

II.4.30. ROBORDER - Autonomous swarm of heterogeneous robots for border surveillance "H2020, Grant agreement ID: 740593, H2020-SEC-2016-2017, DOI https://doi.org/10.3030/740593, International Science Project (H2020), Bulgarian Defence Institute, 2022.

The ROBORDER project aims to develop and demonstrate a fully functional autonomous border surveillance system with unmanned mobile robots, including air, surface, underwater and ground vehicles, capable of functioning both *independently and in swarms, which will incorporate multimodal sensors as part of an interoperable network. The system is equipped with adaptive sensor and robotic technologies that can operate in a wide range of operational and environmental settings. To provide a complete and detailed picture of situational awareness, the network of sensors includes static network sensors such as border surveillance radars, as well as mobile sensors customized and installed aboard unmanned vehicles.*

II.4.31. National Scientific Program "Security and Defence", Ministry of Education and Science, National Scientific Program, Council of Ministers, 2022

Providing a secure and favorable environment for the development of society and the state by conducting coordinated and targeted fundamental and applied research in the field of security and defence and creating a sustainable partnership between the included scientific and educational organizations in the program for joint participation in national and European international research networks, programs and projects.

II.4.32. CyRADARS - Cyber Rapid Analysis for Defence Awareness of Real-Time Situation, Science for Peace and Security, NATO, 2017-2021, International Science Project (NATO SPS), Bulgarian Defence Institute, 2021

The project has developed new theoretical formulations, methods and research prototypes of software tools for creating situational awareness for large cyber campaigns: operations aimed at the wide dissemination of malicious information.

II.4.33. ODYSSEUS - Preventing, countering, and investigating terrorist attacks through prognostic, detection, and forensic mechanisms for explosive precursors, H2020, European Commission International Science Project (H2020), Bulgarian Defence Institute, CORDIS, 2021

The fight against terrorism requires an arsenal of tools. One of them is knowledge of explosive precursors – chemicals that can be used for legitimate purposes, but can also be used for the illegal manufacture of homemade explosives. In this context, the EU-funded ODYSSEUS project will develop effective and efficient forecasting, detection and investigation tools to improve the prevention, counteraction and investigation of terrorist incidents involving home-made explosives. The knowledge will help in the development of tools for monitoring the chemical supply chain and reporting explosive precursors (almost) in real time. The tools will be tested on site in three operational use cases.

II.4.34. CUIIS - Comprehensive Underwater Intervention Information System, EDIDP, European Commission, International Science Project (EDIDP), Bulgarian Defence Institute, 2021

The scope of the CUIIS project focuses on an innovative complete system solution in the field of underwater technologies for physical maintenance and restoration of divers, construction of C4I systems for underwater management, underwater monitoring, situational awareness, positioning, navigation and pooling between diver and unmanned platforms.

II.4.35. ECHO (European network of Cybersecurity center and competence Hub for innovation and Operations, 2019, H2020, European Commission, International Science Project (H2020), Bulgarian Defence Institute, 2019.

Cyber protection is vital to prosperity and security. The ECHO project aims to provide an organsed and coordinated approach to improving the European Union's proactive cyber defence, allowing the union to act in anticipation, defending itself against an attack on computers and networks. ECHO is developing a network through which EU cybersecurity centres and competences can be best coordinated and optimised. This will contribute to the durable and sustainable development of cybersecurity skills, including enhanced research and experimentation on certified security products such as early warning systems and cross-sectoral technology roadmaps.

II.4.36. CyNet - CyNET: Boosting the scientific excellence and innovation capacity in Cyber security of the Bulgarian Defence Institute

The aim of the project is to increase the quality and scale of cybersecurity research at the Bulgarian Defence Institute, as well as to strengthen the connections between research institutions specializing in this field.

II.4.37. CyberTwin, European Scientific Networks Program, Ministry of Education and Science, Coordinator‒University of Library Studies and Information Technologies, 2020-2022, International Science Project, Bulgarian Defence Institute, 2020.

The CyberTwin project aims to increase the research and innovation capacity of University of Library Studies and Information Technologies *and its Bulgarian partners Sofia University and Bulgarian Defence Institute in the field of cybersecurity and its applications (focus on digital information protection) through networking and "twinning" with two international leading research institutions in the field. The project stimulates technology transfer and open innovation activities with other partners in order to build an appropriate innovation ecosystem in the field of cybersecurity. The basic principle for capacity building is "training through research". Special workshops will be organised to prepare proposals and implement projects.*

II.4.38. Web Intelligence 2019 Workshop - Security Analytics and Threat Detection on the Web, International Conference, Member of the Organizing Team, https://mklab.iti.gr/sacti2019/

This workshop is focused on an interdisciplinary research area including web intelligence, security informatics, big data analysis, "deep" learning/machine learning, and cybersecurity, and aims to investigate the deliberate misuse of technical infrastructure for subversive purposes, including (but not limited to): the spread of extremist propaganda, antagonistic or hateful comments; the proliferation of malware; online fraud and identity theft; denial-of-service attacks; etc. A better understanding of such phenomena on the web (including social media) allows their early detection and is at the heart of the development of effective cybersecurity threat forecasting models.

II.4.39. Advanced European platform and network of Cybersecurity training and exercises centres - ACTING, International Science Project (EDF 2021), Bulgarian Defence Institute, 2022

The ACTING project proposes an organized and coordinated approach to proactively improve the effectiveness of cyber defence training and exercises in the European Union through effective and efficient multi-sectoral cooperation. The 28 partners from 13 Member States, supported by 6 Ministries of Defence. The ACTING project integrates research, design, prototyping and testing activities in the field of cybersecurity. In order to achieve good synchronization between the ACTING project and the requirements of the Ministries of Defence, 3 validation seminars will be organized.