CYBER SECURITY AND RESILIENCY POLICY FRAMEWORK

NATO Science for Peace and Security Series

This Series presents the results of scientific meetings supported under the NATO Programme: Science for Peace and Security (SPS).

The NATO SPS Programme supports meetings in the following Key Priority areas: (1) Defence Against Terrorism; (2) Countering other Threats to Security and (3) NATO, Partner and Mediterranean Dialogue Country Priorities. The types of meeting supported are generally "Advanced Study Institutes" and "Advanced Research Workshops". The NATO SPS Series collects together the results of these meetings. The meetings are co-organized by scientists from NATO countries and scientists from NATO's "Partner" or "Mediterranean Dialogue" countries. The observations and recommendations made at the meetings, as well as the contents of the volumes in the Series, reflect those of participants and contributors only; they should not necessarily be regarded as reflecting NATO views or policy.

Advanced Study Institutes (ASI) are high-level tutorial courses to convey the latest developments in a subject to an advanced-level audience.

Advanced Research Workshops (ARW) are expert meetings where an intense but informal exchange of views at the frontiers of a subject aims at identifying directions for future action.

Following a transformation of the programme in 2006 the Series has been re-named and re-organised. Recent volumes on topics not related to security, which result from meetings supported under the programme earlier, may be found in the NATO Science Series.

The Series is published by IOS Press, Amsterdam, and Springer Science and Business Media, Dordrecht, in conjunction with the NATO Emerging Security Challenges Division.

Sub-Series

A.	Chemistry and Biology	Springer Science and Business Media
B.	Physics and Biophysics	Springer Science and Business Media
C.	Environmental Security	Springer Science and Business Media
D.	Information and Communication Security	IOS Press
E.	Human and Societal Dynamics	IOS Press

http://www.nato.int/science
http://www.springer.com
http://www.iospress.nl

Sub-Series D: Information and Communication Security – Vol. 38
ISSN 1874-6268 (print)
ISSN 1879-8292 (online)

Cyber Security and Resiliency Policy Framework

Edited by

Ashok Vaseashta
Institute for Advanced Sciences Convergence & Int'l Clean Water Institute
Norwich University Applied Research Institutes
13873 Park Center Rd, Suite 500
Herndon, VA 20112, USA

Philip Susmann
Norwich University Applied Research Institutes
57 Old Freight Way
Northfield, VT 05663, USA

and

Eric Braman
Norwich University Applied Research Institutes
57 Old Freight Way
Northfield, VT 05663, USA

IOS
Press

Amsterdam • Berlin • Tokyo • Washington, DC
Published in cooperation with NATO Emerging Security Challenges Division

Proceedings of the NATO Advanced Research Workshop on
Best Practices and Innovative Approaches to Develop Cyber Security and
Resiliency Policy Framework
Ohrid, Former Yugoslav Republic of Macedonia
June 10-12, 2013

ISBN 978-1-61499-445-9 (print)
ISBN 978-1-61499-446-6 (online)
Library of Congress Control Number: 2014 949 223

Publisher
IOS Press BV
Nieuwe Hemweg 6B
1013 BG Amsterdam
Netherlands
fax: +31 20 687 0019
e-mail: order@iospress.nl

Distributor in the USA and Canada
IOS Press, Inc.
4502 Rachael Manor Drive
Fairfax, VA 22032
USA
fax: +1 703 323 3668
e-mail: iosbooks@iospress.com

LEGAL NOTICE
The publisher is not responsible for the use which might be made of the following information.

PRINTED IN THE NETHERLANDS

Preface

The primary objective of the NATO Advanced Research Workshop (ARW) titled "Best Practices and Innovative Approaches to Develop Cyber Security and Resiliency Policy Framework" was to gather specialists who are well versed with the technical problems, case studies, legal and policy development issues related to securing critical cyber infrastructures and enhancing resilience. All aspects of research involving hardening systems, attack prevention, response and recovery, and maximizing resources was included in the ARW. Cyberspace touches nearly every part of our daily lives. It's the broadband networks beneath us and the wireless signals around us, the local networks in our schools and hospitals and businesses, and the massive grids that power almost all nations. It is critical that we secure our cyberspace to ensure that we can continue to grow the economy and protect our way of life. Due to the significance and overarching impact of securing cyber infrastructures, a diverse range of scientific and technological disciplines must be tactically integrated to achieve effective solutions to various scientific, commercial, and operational requirements.

Cyber warfare has become a major concern for international governments, military and civil agencies. Uniform enforcement within organizationally or territorially-defined jurisdictions is nearly impossible given the global architecture of networks and significant number of system administrators, as addressed in the drafting of the 2001 Council of Europe Convention on Cybercrime. A recent wave of cyber-attacks against NATO member Estonia in 2007 and Georgia in 2008 highlighted the crippling impact cyber warfare can have against a nation's critical national infrastructure. The difficulties in responding to these events for a nation state are exacerbated by ownership, operation, and associated national legal systems. Cyber critical infrastructure and its telecommunication networks are owned by the private sector. Gaining situational awareness to an emerging attack is difficult, as organizations must independently determine when to engage law enforcement or governmental agencies. The construction of these systems is dictated by competitive advantage and profit motive, not national security. All of these factors require a public-private partnership in a coordinated national policy framework.

The devastating attacks in Estonia were distributed denial of service events, primarily focused on the financial system. The trend over the last decade to network previously isolated industrial control and monitoring systems has placed national assets, including critical infrastructure, at a much higher risk. Industrial control and monitoring systems are a subset of computer systems that are subject to cyber exploitation. Furthermore, organizations increasingly share information between business systems and local and geographically remote control systems. Security breaches can cause the loss of trade secrets and/or interrupt information flow, resulting in the loss or destruction of services or products. Even more devastating consequences include potential loss of life, damage to the environment, violations of regulatory statutes, and compromises to operational safety. Effective responses to these events requires a logical escalation method through information sharing based on a decision-making model. Threats to these systems can come in many forms such as terrorist, clandestine organizations, and even trusted insiders who misuse authority. Actions in the cyber eco-system outpace the ability of human decision making. Motives and attribution in cyber-attacks are difficult to ascertain. An understanding of the impacts for diverse stakeholders is required and must be fed into the situational awareness of the cyber event which warrants engaging national security apparatus for significant events.

Cyber infrastructures are typically secured by defending the perimeter of the information system. The grand challenges of information security thus cannot be addressed by advanced science or technology alone, but needs to be layered with a national policy context and with engagement of law enforcement, judicial, legislative, and national security agencies. Design of future technologies must enhance both system security and resiliency, and allow swift restoration to full operational capacity to minimize disruption of services. This will require an organized cyber policy framework that defines situational awareness, escalation, and national or super-national decision making for continuity of critical infrastructure and government.

This workshop aimed to develop a governing policy framework to enhance the cyber security of a nation state's critical infrastructure through a process of defining the problem, followed by engaging the participants in interactive "exercises" to illustrate the issues as listed below that provided understanding of the framework.

- Establish a national cyber risk governance model that defines risks and levels of risk tolerance under varying circumstances, assigns responsibility among various stakeholders for defining and managing assigned risks, sets risk management goals and metrics, and determines the conditions for evaluating and refining the model as circumstances warrant;
- Identify and allocate resources necessary to meet risk management goals; and
- Be codified in appropriate policy-setting mechanisms, chosen from those that are constitutionally available, including national or regional legislation, executive order, and non-binding coordinating framework.

The workshop aimed to address views of the conflicting elements of a cyber policy and to initiate a dialogue across key stakeholders in the following areas, such as identifying who is responsible for actions needed to protect government, critical infrastructure, and the civilian population from the effects of a cyber-attack; engaging members of the legislature and judicial systems in developing cyber policy; and understanding what is possible and who is responsible for protecting networks and infrastructure. Furthermore the technical operators must anticipate what the next attack type may be, its severity, and what additional resources might be necessary to help defend, in addition to enhancing prevention of cyber-attacks against the government, military, critical infrastructure and the nation's civilians.

In all, approximately 15 countries participated to experience rich technical contents at a venue with significant historical importance. The ARW site - Hotel Inex Gorica by Ohrid Lake offered an air-conditioned auditorium, sound system, internet connection, adjustable terrace seats, and space suitable for conferences, workshops and congresses. The facility supported formal and informal settings for structured and spontaneous learning and sharing of ideas. Lake Ohrid - the largest and most beautiful of Macedonia's three tectonic lakes, provided a serene mountain setting. With its unique flora and fauna characteristic of the tertiary period, Ohrid is one of Europe's great biological preserves. Most of the lake's plant and animal species are endemic and unique to Ohrid. In 1980, UNESCO proclaimed Lake Ohrid a location of world natural and cultural heritage.

The meeting lasted 3 days. The agenda was packed with sessions. The meals were arranged either in the city or at a walking distance from the hotel. This provided a much needed break from the conference room environment and most everyone stayed engaged despite the inevitable post-lunch slowdown. The unique balance of technical and social interactions materialized in alliances among participants, which have been evidenced by continued correspondence in the months following the ARW. The co-directors interpret the ongoing interaction and positive feedback from participants as an affirmation of a successful ARW. Such a constructive ARW is the outcome of efforts by participants, speakers, and co-directors in addition to a host of caring individuals who supported their work.

Much appreciation is extended to the management of staff at the Hotel Inex Gorica for their gracious hospitality to all participants. Logistics help from Dr. Anka Trajkovska and timely publication of abstract help from Dr. Anita Grozdanov is much appreciated. We offer our gratitude to Dr. Deniz Beten, the director of the NATO Emerging Security Challenges Division and Ms. Alison Trapp for their resolute encouragement and support of the ARW. The co-directors are confident that ARW participants will continue research collaborations that began in Ohrid, Republic of Macedonia to enhance safety and security for all mankind in Support of NATO mission. The ARW was supported by NATO – Emerging Security Challenges division of Science for Peace and Security program.

Organizational Support
Eric Braman, Ashok Vaseashta, Anka Trajkovska, Anita Grozdanov, Ernest Drew, Petar Dimovski, Vilma Petkovska, Aleksander Risteski and Philip Susmann

Editorial Team
Ashok Vaseashta, Philip Susmann, and Eric Braman

Meet the Authors

Sabina BARAKOVIĆ is employed as a professional associate in the Sector for Informatics and Telecommunication Systems of the Ministry of Security of Bosnia and Herzegovina, Sarajevo, Bosnia and Herzegovina since 2009. She received her Dipl.-Ing degree in electrical engineering from the University of Tuzla, Bosnia and Herzegovina in 2009. Currently she is working toward her Ph.D. at the Faculty of Electrical Engineering and Computing, University of Zagreb, Croatia. Her main research interests include Cyber security, Quality of Experience and Quality of Service management in wireless and mobile environments, with a focus on Web services and applications. She has published 20 papers in international journals and conference proceedings. She is currently involved in EU COST Action IC1003 (European Network on Quality of Experience in Multimedia Systems and Services, QUALINET) as a management committee member for Bosnia and Herzegovina and the coordinator of the Qualinet online training school.

Nazife BAYKAL completed her undergraduate studies at the Mathematics Department of the Middle East Technical University in 1987 and got an MS degree from the Computer Engineering Department at METU in 1991. She studied at the Computer Science Department at University of Maryland, College Park as a NATO science scholar between the years 1993 and 1994 for thesis research and other research projects. She received her PhD Degree from the Computer Engineering Department of the METU. After working as an academic staff at the Computer Engineering Department of METU between 1996 and 1999, she was appointed as an academic staff at the Informatics Institute at METU. In 2000, she received the title of Associate Professor of Computer Science. Between January 2002 and January 2003, Dr. Baykal studied Health Informatics at the "School of Health Information Sciences" at the University of Texas. Upon her return, Dr. Baykal contributed to the foundation of the Health Informatics Department at the Informatics Institute, METU, much earlier than most of the prominent colleges around the world did. In 2004, Dr. Baykal was appointed as the director of the Informatics Institute at METU, where she is currently working. She then opened up the Cyber Security graduate program within the same institute, together with a research center - Cyber Defense and Security Center. Her main research interests are: cyber security, cyber defense, computer networks, artificial intelligence, fuzzy logic. Furthermore, she is an active instructor of data mining, medical informatics and computer network graduate courses offered by the Informatics Institute. She provides consultancy services to many governmental and industrial organizations. She has more than 150 Refereed Publications and 7 text books.

Galit M. BEN-ISRAEL (Fixler) is the Head of the Project of Identity, Terror and CyberSpace, in the Institute of Identity Research (IDmap). Dr. Galit Ben-Israel is also a Terrorism analyst and counter-terrorism training consultant & senior lecturer of political science at the Public Administration and Policy, The Faculty of Society and Culture, Beit-Berl Academic College. She teaches courses of: World Politics and Globalization; Terror on the Digital Era and Virtual Communities and Cyber-

Terrorism. Her research field covers themes of: Hostage-Barricade Terrorism (HBT); Suicide Terrorism; Disaster Management via Social Media (Web 2.0) and Diaspora and Internet networks.

Mitko BOGDANOSKI received his B.Sc. degree from the Military Academy, Skopje, Macedonia, and M.Sc. and Ph.D. degree from the Faculty of Electrical Engineering and Information Technologies, Ss Cyril and Methodius University, Skopje, Macedonia, in 2000, 2006 and 2012 respectively. He is currently an assistant professor at the Military Academy "General Mihailo Apostolski" in Skopje. He is an author of more than 50 international/national conference/journal publications. Dr. Bogdanoski was a project leader and participant of several national international projects sponsored. He is a Senior Member of the IEEE Organization and Member of the Organization Committees of several national and international conferences. He is also a reviewer for several journals, magazines and conferences (IJCS (Wiley) (ISI), KSII-TIIS (ISI), IJNS (SCImago), Defence Science Journal (ISI), IMACST, ETAI, etc.). His research interests include cyber security, wireless and mobile networks, MANET, WSN, energy efficiency and communication theory.

Luben BOYANOV graduated from Sofia Technical University in 1985 as a computer science engineer. He defended MSc thesis (1989) and PhD thesis (1996) at the University of Manchester, UK. He became an Associate Professor at the Institute of Parallel Processing at the Bulgarian Academy of Sciences in 2006. His major is in computer science, and the topics of his research activities were LANs, computer architectures, telecommunications. His early research and interests were on LAN interfaces and transputers where he built a shared-memory model and working prototype of transputer link communications. Later work and research was on computer architectures for distributed logic simulation. During the last decade he has been teaching, consulting and working on scientific and research projects on computer networks, GRID computing, e-infrastructure, information and human behavior, smart homes and human behavior. For 8 months he was director of the first Bulgarian supercomputing center. He participated in 10 international projects, on two of which he was project manager. He is also working on two national projects, for one of which he is project manager. Since 2001 he works at the department of Computer Architectures and Networks at the Institute of Information and Communication Technologies at the Bulgarian Academy of Sciences (formerly Institute for Parallel Processing). For more than 15 year he has lectured Computing Machines, Computer Architectures and Computer Networks at Sofia Technical University, University of National and World Economy (Sofia), New Bulgarian University (Sofia), International University College (Dobrich) and European Polytechnical University (Pernik). He has more than 35 publications, including 6 books.

Eric BRAMAN is the Vice President of the NUARI and serves as the Director of the Defense Technologies Research Institute. As a former Deputy Chief of Staff for Operations in the National Guard Bureau for the Pentagon, COL. Braman's expertise lies in leadership, planning, and organization for projects involving experts from military, scientific, academic, and government domains. COL. Braman has served as the principal investigator and director for many government projects and contracts with a successful record of ensuring that all stakeholders and resources remain committed to achieving their overarching goals.

Amir HUSIĆ is employed as a head of Department for Computer Networks in the Sector for Informatics and Telecommunication Systems of the Ministry of Security of Bosnia and Herzegovina, Sarajevo, Bosnia and Herzegovina since 2009. He received his Dipl.-Ing degree in electrical engineering from the University of Tuzla, Bosnia and Herzegovina, in 2003. His main research interests include Cyber security management in public sector and VPN security.

Jasmina Baraković HUSIĆ is employed by BH Telecom, Joint Stock Company, Sarajevo since 2005. She has been working as a professional associate in the Directorate BH Mobile. She graduated from the University of Tuzla, Faculty of Electrical Engineering in 2004. She spent six months at the Munich University of Technology as a scientific researcher during the same year. She has defended doctoral thesis in the field of signaling information transmission at the University of Zagreb, Faculty of Electrical Engineering and Computing in 2009. She joined the University of Sarajevo, Faculty of Electrical Engineering in 2011, where she works as Assistant Professor at the Department for Telecommunications. She also teaches at the Department of Communications of the Faculty of Traffic and Communication. Her research concerns a variety of topics in quality of service and signaling in next generation networks. She has published more than 30 science and professional papers based on her research interests. She is member of IEEE Communication Society and Bosnian-Herzegovinian Society for Telecommunications–BHTEL.

Adnan KULOVAC is employed as head of the CIS Security Department in the Sector for Protection of Classified Information of the Ministry of Security of Bosnia and Herzegovina, Sarajevo, Bosnia and Herzegovina since 2008, after working as a head of IT department in Coal mines “Kreka” and Central Election Commission. He received his Dipl.-Ing and M. Sc. degree in electrical engineering from the University of Tuzla, Bosnia and Herzegovina, in 2002 and 2008, respectively. His main research interests include security management of Web applications and Web services.

Miroslav JOVANOVIC is an expert in the sphere of information technologies with an engineer’s degree in computer science and IT. In the course of his engagement at various managerial positions both in Macedonia and in Serbia, he was dedicated to the IT management and implementation of large ICT systems in the public sector, while in the position of IT Director at the Ministry of Finance he was meritorious for the successful implementation of several projects, including the e-budget project. Prior to his appointment as the Chief Technical Director of Makedonski Telekom in 2009, Mr. Jovanovic worked as a Key Long-Term Expert - Financial Management Information Systems in Serbia. He was appointed to the position of Chief IT Officer of T-Mobile Macedonia on 15 March 2010 and as of 15th October 2011 he assumed the position of Chief IT Officer of Makedonski Telekom.

Gevorg MARGAROV is the head of Information Security and Software Development Department at the State Engineering University of Armenia (Polytechnic), Yerevan, Armenia. The scope of his current scientific interests includes Architecture of Computer Systems and Complexes, Organization and Management of Information Security Systems, Digital Steganography, Applied Cryptography, E-learning and Knowledge Assessment Tools. Gevorg has over 180 scientific publications. He has supervised 10 theses for Candidate of Sciences (PhD) degrees in Armenia and a thesis for the degree of Doctor of Philosophy (PhD) in computer science in France. Gevorg is a member of the Governing Board of National Centre for Professional Education Quality Assurance Foundation (ANQA, Yerevan, Armenia), a professional member of the Association for Computing Machinery (ACM, New York, USA) and a member of the Computer Science Teachers Association (CSTA, New York, USA).

Zlatogor MINCHEV is an 'Associate Professor' on 'Automation and Control' at the Institute of Information and Communication Technologies (IICT), Bulgarian Academy of Sciences (BAS), IT for Security Department (2010); collaborator of the 'Cognitive Psychophysiology' department, Institute of Neurobiology, BAS (since 2003); part-time Associate Professor at the Institute of Mathematics and Informatics – BAS, Operations Research, Probability & Statistics department (2010); B.Sc. degree on 'Informatics & Mathematics' from 'St. St. Cyril and Methodius', University of Veliko Tarnovo (2001); PhD on 'Cybernetics & Robotics' (2006) from Center for Biomedical Engineering 'Prof. Ivan Daskalov', BAS. Since 2001 he is working in the areas of: Computer Science, Robotics and Psychophysiology and since 2005, he is with the applied Operations Research, Planning, Modelling & Simulation for Crisis Management. In 2007 he was appointed as a Director of Joint Training Simulation & Analysis Center, IICT-BAS. During his ten years scientific career he took part in more than 25 scientific projects funded by: Bulgarian government, EU, NATO, USA and the non-governmental sector. Since 2006 Dr. Minchev works with young Bulgarian talents in the fields of mathematics and informatics in cooperation with the non-governmental sector. Since 2010 he participated in a European Network of Excellence in the field of cybersecurity – SysSec where his achievements are marked by UN, EU and NATO. He is also participating in a number of national and international project and initiative in the cyber security area. He has authored and co-authored more than 60 scientific publications, including: nine books and two patents.

Mladen MRKAJA is employed as an assistant minister of security in the Sector for Informatics and Telecommunication Systems of the Ministry of Security of Bosnia and Herzegovina, Sarajevo, Bosnia and Herzegovina since 2010. He received his Dipl.-Ing degree in electrical engineering from the University of East Sarajevo, Bosnia and Herzegovina, in 2003. Currently he is working toward his M.Sc. at the Faculty of Electrical Engineering, University of East Sarajevo, Bosnia and Herzegovina. His main research interests include spectral efficiency of mobile WiMAX, and he is an author of two papers in conference proceedings.

Constantine PAPATHEODOROU is Assistant Professor in the Geomatics & Surveying Department of the Technological Educational Institute of Serres, Greece. He obtained PhD in Engineering Geology from the Civil Engineering Department of the University of Thessaloniki, Greece. He has over 17 years teaching experience in subjects including "Engineering Geologic applications in Civil Engineering", "Chartographic applications in Geology", "Remote Sensing Applications", "Geomatics & Data analysis" (post graduate course in Natural Hazard Prevention & Management), "Geographical Information Systems applications in Natural Hazard Prevention and Management" (post graduate course in Natural Hazard Prevention & Management), "Geographic Information Systems" Post- graduate course "The environment & New Technologies"). His research interests include natural Hazard prevention and management, Geographic Information Systems applications (especially in Natural Hazard Mitigation and in Environmental Protection), Groundwater protection and management, Remote Sensing applications in Geology and the Environment, Applied geophysical research using Ground Penetrating Radar and Seismic Refraction. He is editorial board member of many professional magazines including Geoinformatics.

Predrag PALE was the first one to chase hackers in Croatia as early as 1994 and ever since is present in the information security (IS). He is leading the Information security group within the Laboratory for systems and signals at Faculty of Electrical Engineering at University of Zagreb. The group is intensely involved in technical aspects of information security, is assisting their clients in detecting vulnerability of their systems and designing their protection. He is also active in theoretical research in subfields of IS attack taxonomies, knowledge based authentication, untamperable monitoring of operating systems, and anonymity in electronic voting systems. He established Croatian national CERT and was a member of governmental task force designing National program for information security, the predecessor of the Law on information security. Ever since 1993 he is frequent invited speaker on topic of information security and information warfare at worldwide conferences, NATO & RACVIAC workshops and NATO open road conference. He regularly speaks, teaches and leads workshops for managers, IT specialists, parents, teachers and general public. He is the founder and head of the Center for information security at the Faculty of Electrical Engineering and Computing of Zagreb University aimed at raising awareness about information security in general public and especially to work with youth attracted to the field of information security.

Aleksandar RISTESKI received his B.Sc., M.Sc. and Ph.D. degrees in telecommunications at the University Sts. Cyril and Methodius, Skopje, Macedonia in 1996, 2000 and 2004, respectively. He is currently a professor and a vice-dean for research and international cooperation at the same university, in the Faculty of Electrical Engineering and Information Technologies. In 2001, 2003 and 2004, he had several internships at IBM T. J. Watson Research Center, Yorktown Heights, NY, USA, where he worked towards his Ph.D. degree. His research interests are in the field of secure communications, optical communications, and coding theory. He is an author of more than 70 journal and conference papers He is a mentor of 40 M.Sc. and 6 Ph.D. candidates. Dr. Risteski was a project leader of two national research projects and also a participant in several national and international projects sponsored by European

Commission and IBM. He has also leaded and participated in a number of industry-related consultancy projects. He is a member of the National Board for Accreditation and Evaluation of Higher Education in the Republic of Macedonia. He is president of the Society for Electronics, Telecommunications, Automatics and Informatics (ETAI) of Republic of Macedonia, co-chairman of Conferences ETAI 2009, ETAI 2011, ETAI 2013, and a co-director of NATO Advanced Research Workshop. From 2005 to 2007, he was an independent member of the Board of Directors of Makedonski telekom AD Skopje. He is also a member of the IEEE.

Marjan STOILKOVSKI graduated in 2000 from the Military Academy in Skopje. From 2009 to 2011 he was working on his Mater degree on Cybercrime investigation and digital forensics with the Faculty for Information technology on the University College Dublin in Dublin, Republic of Ireland. Currently, he is working toward his PhD on Computer incidents and digital forensics with the Faculty for Information technologies on the European University in Skopje. From 2008 he was appointed as a Head of the Cybercrime Unit in Ministry of Interior and from 2013 as a Head of the Cybercrime and digital forensics department in Ministry of interior. Beside the professional experience in investigating cybercrime cases he was appointed in the working group for developing the National CERT in Republic of Macedonia and also he is leading the working group for developing a Cyber security strategy in Republic of Macedonia.

Philip SUSMANN obtained a BS from Norwich University and an MBA from Clarkson College of Technology, NY. Currently, he is the VP of Strategic Partnerships at Norwich University responsible for new business initiatives at Norwich University. Mr. Susmann has been at Norwich University for the past 27 years as a faculty member, Chief Information Officer, and recently responsible for creating a research and development activity – Norwich University Applied Research Institutes (NUARI) credited with the development of a Distributed Environment for Critical Infrastructure Exercises (DECIDE) - a platform used to deliver two large scale financial sector exercise Quantum Dawn 1 & 2. In addition, NUARI has developed, in partnership with USU Space Dynamics Lab, Cyber SMART - a cyber exercise scenario development tool.

Ashok VASEASHTA received a PhD from the Virginia Polytechnic Institute and State University, Blacksburg, VA in 1990. Before joining as the Director of Research at the Institute for Convergence of Information, Science, Technology, and Knowledge (formerly Institute for Advanced Sciences Convergence) and International Clean Water Institute, he served as a Professor of Physics and Physical Sciences and Director of Research at the Nanomaterials Processing and Characterization Laboratories, Graduate Program in Physical Sciences at Marshall University. Concurrently, he holds a visiting professorship at the 3 Nano-SAE Research Centre, University of Bucharest, Romania; and a chaired professorship at the Academy of Sciences of Moldova, Chisinau, Moldova.He served as a visiting scientist at the Helen & Martin Kimmel Center of Nanoscale Science at the Weizmann Institute of Science, Israel. In 2007-08, he was detailed as a William C. Foster fellow to the Bureau of ISN at the U.S. Department of

State working with the Office of WMDT and FCM programs. He served as a Franklin Fellow and S&T advisor to the office of VTT/AVC in the Bureau of Arms Control Verification and Compliance at the U.S. Department of State. He is a fellow of the American Physical Society, Institute of Nanotechnology, and New York Academy of Sciences. He was awarded a Gold medal by the State Engineering University of Armenia for his contribution to Nanotechnology. In addition, he has earned several other fellowships and awards for his meritorious service including the Marshall University 2004/2005 Distinguished Artist and Scholar award. His research interests include counter-terrorism; advanced and nano materials for development of chemical-bio sensors/detectors; water safety and security; environmental pollution monitoring, detecting and remediation; and green nanotechnology. He authored over 230 research publications, edited/authored five books on nanotechnology, presented many keynote and invited lectures worldwide, served as the NATO Project Director of five NATO ASI/ARW, multi-year SPS program, and co-chair of an ISNEPP conferences. He led the U.S. position on Nanotechnology in High Technology Coordination Group to joint U.S. and India delegation. In addition, he served as a member of the U.S. Department of Commerce, NIST, and ANSI delegation to the U.K. representing the U.S. position on Standards in Nanotechnologies at the inaugural meeting of the ISO/TAG to TC-229. He is a member of NATO-SET-040, an exploratory team panel investigating security and surveillance applications of nanotechnology. He serves as an expert counsel to the UNESCO, ObservatoryNANO, and COSENT – south-east consortium on Nanotechnologies on NANO-Science and Technologies. He is an active member of several national and international professional organizations.

NATO – Advanced Research Workshop Best Practices and Innovative Approaches to Develop Cyber Security and Resiliency Policy Framework June 10-12, 2013, Ohrid, Republic of Macedonia

Selected Photographs

Questions?

INEX
HOTEL GORICA

A long-term strategy
for cyber secu

УНИВЕРЗИТЕТ
ЗА ИНФОРМАТИЧКИ НАУКИ И ТЕХНОЛОГИИ
СВЕТИ АПОСТОЛ ПАВЛЕ - ОХРИД
University
for Information Science and Technology
„St. Paul the Apostle" - Ohrid

This page intentionally left blank

Contents