Information & Security: An International Journal

Predrag Tasevski, vol.32, 2015 http://dx.doi.org/10.11610/isij.3204

MACEDONIAN PATH TOWARDS CYBERSECURITY

Predrag TASEVSKI

Abstract: Information and communication technologies in Macedonia have experienced a phenomenal growth throughout the last decades, which has had a tremendous impact on governmental services' presence in the Internet, as well as on everyday life. Against this background, technologies-based growth introduces new risks and threats to the cyber domain in the country. To respond to those challenges the Macedonian government is pursing the establishment of a national authority to react to cyber attacks that occur, or a Computer Incident Response Team – MKD-CIRT, and the adoption of a National Cybersecurity Strategy. However, it should be taken into account that such tasks are neither easy nor simple. There are several issues that should be considered, for instance: the improvement of the measures for protection of information systems and of the critical infrastructure; the legal and policy framework; the international approach; and the formation of a cybersecurity culture, to name but a few. Simultaneously, considering that Macedonia is a candidate for accession to the EU and NATO, it has to comply with their standards when performing the reforms in the cybersecurity field. The current article briefly introduces the country's steps towards cybersecurity, provides an analysis of the legal, policy and institutional progress achieved, and suggests recommendations that should be considered to ensure safer, secure, trustworthy and resilient cyber space in the country.

Keywords: Macedonia, cyber, establishment, MKD-CIRT, strategy, security, national security

Background

The Republic of Macedonia's road to membership in the two most important Euro-Atlantic clubs has been long and, unfortunately, still unfinished. Macedonia has been a candidate for accession to the European Union (EU) since 2005,[1] but has not yet entered into negotiations. For its part, the membership in the North Atlantic Treaty Organisation (NATO) is currently pending, as it was blocked by Greece at the 2008 Bucharest Summit[2] due to a long-standing dispute on the country's official name. Still, the country joined the Partnership for Peace, and commenced its Membership Action Plan in 1999.

Despite the lack of resolution of the naming dispute, for Macedonia the integration in NATO and in the EU remains a priority, which requires political and economic stability, rule of law, as well as further internal reforms. In this context, aligning the Macedonian legislation with the EU *acquis*, the setting up of a policy framework and strategy, as well as the establishment of proper structures in the area of cybersecurity are among the main steps that the government needs to undertake in the integration processes.

Speaking of cybersecurity, we need to consider not only the obligations that derive from the further integration with the EU and NATO, but also the needs of the Macedonian society, experiencing the consequences of a phenomenal growth of the communications networks and information systems in Macedonia and worldwide in the last decades. For this reason, the society requires increased efforts to achieve safer and more reliable services when using information and communication technologies (ICT). Also, ICT have become the backbone of the economy, and of the finance, health, energy and transport sectors. As a consequence, cyber threats, the frequent occurrence of cybersecurity breaches, the losses due to those threats and breaches are increasing as well.[3] Led by this knowledge and by common sense, one can conclude that ensuring information security in this interdependent environment, called cyber space is a priority for each individual, organisation and for the society in general,[4] and is therefore an urgent national security issue.

Macedonia is among the countries where the development of the telecommunications and of the information society has been very rapid. The usage of ICT has increased significantly in recent years, and according to data provided by the State Statistical Office for 2014,[5] 68.3 % of the households have Internet access, while this figure for enterprises with 10 or more employees is 93 %. Another significant fact is that Internet connectivity via mobile broadband connection is growing, too, at a pace of 4 % as compared to 2013.

Furthermore, since late 2009 the government has pursued a national program called e-Macedonia, which was developed by the Ministry of Information Society, with priorities being: e-education, e-citizens, e-business, e-infrastructure, e-government and Information Security.[6] Such developments add value to the economic and social status of the country. At the same time, they expose both state and non-state actors to an increased cyber risk.

Previously mentioned issues leave no doubt that countries must significantly improve their cybersecurity capabilities, while government, public, academia and social sectors must work together to develop and adopt cybersecurity solutions to keep pace with the threat environment. Additionally, investing in cybersecurity can be considered from another economic aspect – by regarding cyber space as a possibility and as a resource. A protected cyber space makes it easier for businesses and individuals to plan their activities, which boosts economical endeavour and cybersecurity culture.[7]

Based on the above, this paper provides an analysis of the steps that have been undertaken by the Macedonian government, aiming to fulfill EU and NATO standards and of the requirements and the best practices in the area of cybersecurity. Then we highlight some recommendations on how the Macedonian cybersecurity area should be developed and tailored in securing the cyber space. In the end, we conclude.

Analysis

Information security constitutes a driving force for the economic development of the countries and it must be pursued simultaneously with the improvement of the ICT infrastructure.

In a broader sense, cybersecurity also includes setting up a related legal framework, while the Critical Information Infrastructure (CII) is vital to attract economic actors for developing a favourable business environment. For this reason, cybersecurity must be clearly defined, taking into account the various actors' specific roles in the cyber domain – from individuals to organisations and states.[8]

In Macedonia, cybersecurity developments are still nascent. However, there are initiatives to elaborate and put in place parts of the required legal framework. The first step towards codifying the issue of cybersecurity was made in 2004, when the Macedonian parliament ratified the Council of Europe Convention on Cybercrime.[9] In November 2005, Macedonia also ratified an Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Thereafter, the Macedonian authorities had to urgently fulfill obligations stemming from the convention's ratification, including by means of creating and/or changing national legislation. At present, the legal framework regulating cybercrime includes:

- Criminal Code;[10]
- Law on Criminal Procedure;[11]
- Law on Electronic Communications;[12]
- Law on Communications Monitoring;[13]
- Law on e-Commerce;[14]
- Law on Electronic Management;[15]
- Code of Civil Procedure;[16]
- Law on Electronic Data Form and Electronic Signature;[17] and
- Declaration on Safer Internet.

The material provisions related to cybercrime are contained in the Criminal Code and include: endangering safety, violation of the confidentiality of correspondence and other consignments, misuse of personal data, preventing access to the public information system, copyright violation, infringement of the distribution of technical specially protected signals, audio piracy, child pornography, damage or unauthorised entry into a computer system, development and distribution of computer viruses, computer fraud, making, procuring or selling counterfeiting means, making and using fake credit cards, violation of registered or protected invention and topography of integrated circuits and spread of racist and xenophobic material through computer systems. Additionally, it defines the general terminology regarding cybercrime.

In addition to that, the Law on Criminal Procedure, which entered into force in December 2013, specifically tackles cybercrime and crimes committed with the use of computers, and the collection of digital evidence by the law enforcement authorities.

Apart from the legal framework, the technical means to protect the cyber space represent a serious challenge for the national authorities in many states, and Macedonia is no exception to that trend.[18] Accordingly, existing strategic security documents in Macedonia define the roles of various authorities, taking into account the nature of the threat. For example, as regards cybersecurity the responsible actors, linked in a crisis management system (CMS), include: the Ministry of Interior, the Ministry of Defence, the Protection and Rescue Directorate, the Crisis Management Centre, the Ministry of Transport and Communication, the Directorate for Protection of Classified Information and the Ministry of Environment and Spatial Planning. Other relevant legislation concerns the Ministry of Information Society.[19]

Moreover, the Macedonian government is pursuing the establishment of a national authority – a response team that will handle computer incidents, namely the Macedonian Computer Incident Response Team (MKD-CIRT). Last but not least, the drafting of a National Cybersecurity Strategy was initiated in the middle of 2014. Additionally, Macedonian representatives have taken part in workshops and training programs funded by the EU and NATO, such as: EU project CyberCrime@IPA,[20] and NATO SPS advanced research workshops held in Ohrid and Skopje.[21]

In the next sections, we offer analysis on MKD-CIRT and the Macedonian National Cybersecurity Strategy.

MKD-CIRT

Since 2012 there have been discussions about the establishment of a CIRT (Computer Incident Response Team) and CERT (Computer Emergency Response Team) in Macedonia[22] with technical support from the International Telecommunication Union

(ITU). However, no body has been formed to date. The progress on the issue also remains unclear.

Sadly, other countries from the region lack such teams as well.[23] Whereas other countries are progressing much more quickly and efficiently, for example Albania,[24] Bosnia and Herzegovina,[25] Bulgaria,[26] Montenegro [27] and Romania.[28]

But even though Macedonia's vision towards cybersecurity is less advanced and progressing more slowly than in some neighbouring countries, still we can say that is has future. The idea involves the creation of a team consisting of experts in information security to act as a point of coordination for monitoring, identification, warning and determining answers to computer incidents. Furthermore, it will take proactive measures in order to prevent or mitigate the consequences of possible damages, as well as undertake reactive measures for managing computer incidents. Planned proactive measures to be employed by the team include: continuous monitoring of the situation in the field of information security and at the same time issuing security alerts with prevention functions; constant monitoring of technology development for information security and dissemination of collected information; raising public awareness of the importance of information security; and conducting educational trainings for specific user target groups. Projected reactive measures at disposal of the team are: coordination in dealing with major computer incidents; preparation and distribution of security alerts, based on received information; collection, precession, preparation and distribution of security recommendations for information system vulnerabilities. The national body will also provide support for building a national culture of information security and for raising awareness among users and citizens, as pointed out by Minister Ivanovski.[29]

However, a new idea emerged in the middle of 2014, namely to form the MKD-CIRT team as part of the Agency for Electronic Communications (AEC).[30] MKD-CIRT is thus seen as an up to five-member team, providing reactive, proactive and security quality services (see table 1).

Notably, in the beginning of 2015 a public hearing was initiated by the AEC and feedback was requested from the mobile telecommunications companies about the establishment of the MKD-CIRT and the action plan of the AEC for 2015. Unfortunately, no other information is publicly available, besides that of an indicative yearly budget of 500 000 Euro.[31]

National Cybersecurity Strategy

In line with the overall efforts to make progress in the process of accession to the EU and NATO, in mid-2014 the United Nations Development Programme (UNDP) pro-

Table 1: MKD-CIRT phases.

	Phase 1	*Phase 2*	*Phase 3*
Reactive services	Incident response and handling Alert and warnings Vulnerability response	Incident response coordination Vulnerability response coordination Threat analysis	Security audits and assessments
Proactive services	Announcements and basic awareness Education and training	Vulnerability analysis Technology watch	Forensic analysis
Security quality	N/A	Advanced awareness Education and training	Management service: Risk analysis and Security consulting

posed an assessment study for the requirements for preparation of a National Cybersecurity Strategy in Macedonia.[32] The main goal was to reinforce the need for designing and adopting a National Cybersecurity Strategy for the country and to ensure compliance with the EU Cybersecurity Strategy.[33]

Therefore, a working group has been formed. It consists of eight members from different ministries, including the Ministry of Interior, the Ministry of Information Society, the Ministry of Health, the Ministry of Defence and the Ministry of Education.[34]

The necessity of a National Cybersecurity Strategy is primarily related to:[35]

- Providing an open, reliable and secure cyber space for activities and social interactions (including human rights); the economy and all national systems largely depend on the application of information and communication technologies;
- The rise in the use of the IT systems increases the risk of abuse and emergence of new, more sophisticated types of cybercrime, which makes the cybercrime one of the more serious threats to national security;
- Developing a cyber defence policy;
- Establishing an integrated, multidisciplinary approach to secure closer cooperation and coordination between the defence, institutions involved in the combat against crime, private sector, and other relevant stakeholders;
- Strengthening the operational capacity, coordination and cooperation among the relevant institutions involved in combatting cybercrime;

- Establishing common standards, training, and education of all institutions involved in the development of cybersecurity;
- Strengthening the national capacity for prevention and protection against cyber attacks, as well as implementing a campaign to raise cyber attack awareness.

The strategy will cover four segments:

- Developing and promoting the cyber defence concept;
- Measures and activities for cybercrime suppression;
- Establishing and improving a system for preventing cyber attacks;
- Managing incidents caused by cybercrime.

Despite that the proposal was made by the UNDP, it has added value to the process of drafting and developing a national cybersecurity strategy in line with the EU's Cybersecurity Strategy, ensuring a safe, secure, trustworthy and resilient digital environment for the benefit of the citizens, businesses and public administration.

However, we can observe that there is still room for improvement. Such improvement could help increase the capabilities of the defence sector, e.g. by integrating some valuable pieces of advice as highlighted in the CCD COE National Cyber Security Framework Manual[36] and the Tallinn Manual.[37]

Likewise, we can underline that the initiative for drafting the strategy in Macedonia is based on a multidisciplinary (technology, law, economics) and multi-stakeholder (government, civil society, business) approach; rather than on a multi-level (local-national-regional-global) approach. Another relevant point concerns the fact that the EU strategy has a specific research and development, and investments and innovation spin, while the Macedonian draft strategy does not foresee any provisions in this regard.

For this reason, in the next section we discuss suggestions and structures for promoting safer and trustworthy cyber space in the country.

Recommendations

Indeed, reforms in the cybersecurity domain are not easy to make. Such are the establishment of a strategic and legal framework, and of a national CIRT authority. Yet, we have to bear in mind that cybersecurity is everyone's responsibility. Thereby we offer some recommendations on how the Macedonian cybersecurity path should be further charted. These recommendations focus mainly on legislative and institutional aspects and build on the requirements for EU and NATO membership.

Despite slowly progressing relations with the EU and NATO, it is crucial that the Macedonian authorities move speedily in taking action in regard to cybersecurity. For instance, the authorities should form a multi-stakeholder and multi-level expert group, consisting of representatives of the government, the civil society and the private sector, and of course of local, regional and global networks to help respond to any possible cyber threat and/or attack.

We might conclude that the draft policy documents on cybersecurity are broadly in line with the EU strategy for cybersecurity, and in compliance with the Convention on Cybercrime. What Macedonia's draft strategy lacks, are measures for fostering research and development, and investments and innovation, as put in the EU cyber strategy (for example, Romania is launching a Cybersecurity Innovation Centre).[38] Furthermore, the draft Macedonian strategy lacks capacity building measures for the defence sector, as recommended by the Tallinn Manual, particularly definitions on: cyber espionage, cyber-enabled terrorism, cyber-warfare, hybrid war, etc.

Additionally, EU's strategy emphasises definitions such as: cybercrime, cyber defence, cybersecurity and cyber resilience. However, the Macedonian policy documents are missing a definition of cyber resilience. Therefore, adding such will bring benefit to the building of military and non-military capabilities, and will increase interoperability in technical, legal, policy and decision-making terms.

Talking about resilience logically leads us to the MKD-CIRT. We should note that the conceptualisation and the establishment of such a national body should be more transparent and protect not only national/state interests but also the interests of the private sector and of the citizens. Unfortunately, with the reforms progressing only very slowly, the capabilities of the Macedonian authorities to tackle cybersecurity issues remain unclear. Hence, this is an issue to be properly addressed in the very near future. Moreover, a well-functioning institutional and legal framework is to be urgently established, considering national specifics and international experience.

Another crucial element is awareness, which is present in the draft strategy. However, it is important to emphasise that awareness must reflect the vision, the culture and the history of a nation, and the global dimension, and to educate the weakest link in cybersecurity, which is the end-users. This could be achieved by introducing and developing a cybersecurity culture, followed by awareness and education campaigns, etc.

Last but not least, it should be noted that the Balkan region seems to be vulnerable to cyber attacks, especially when it comes to large-scale cyber attacks. Still, there are countries that are quickly progressing, while others are slowly moving forward. Therefore, we have to think towards securing and protecting the cyber space at a regional scale and assess the need for the establishment of a Balkan Defence League Cyber Unit, e.g. following the example of the Estonian Defence League's Cyber

Unit.[39] The main goal would be a voluntary collaboration among all national, regional and, most importantly, international actors to protect Balkan cyber space. Furthermore, a strong partnership among all actors is needed in order to meet the challenges that the country is facing in the field of cybersecurity. Needless to say, as a candidate country for EU and NATO, Macedonia has to actively participate in cybersecurity initiatives and programs worldwide.

Conclusion

In this paper we aimed to give an overview of the path towards cybersecurity in Macedonia and analyse the activities taken by the government. The establishment of policy, legal and institutional national framework has been initiated, but has been slow, non-transparent and without significant results so far. We hope that in the near future this process will be fast-forwarded. In line with requirements to accede to the EU and NATO, which are indeed the main foreign policy objectives of the country, important reforms have been initiated. Those reforms, such as the adaptation of the legal and policy framework for cybersecurity, the establishment of a national corresponding body to work as an incident response team and the development of a National Cybersecurity Strategy, are on the go. Our study analysed those reforms and provided suggestions for furtherer charting the path towards cybersecurity in Macedonia.

Finally, we believe that if applied, the recommendations will introduce a new chapter in the Macedonian path towards cybersecurity, and may also provide a positive example for other Balkan countries, thus contributing to the security and stability in the region and promoting economic growth.

Notes:

[1] European Commission, Bilateral relations: The former Yugoslav Republic of Macedonia, accessed on 16 April 2012, ec.europa.eu/competition/international/bilateral/fyrom.html.

[2] Materials from NATO Summit Bucharest 2008, accessed on 04 February 2008, http://www.summitbucharest.ro/ro/1.html.

[3] Xingan Li, "Cybersecurity as a Relative Concept", *Information & Security An International Journal* 18 (2006): 11-24, http://dx.doi.org/10.11610/isij.1801.

[4] Sabina Baraković, Mladen Mrkaja, Amir Husić, Adnan Kulovac, and Jasmina Baraković Husić, "Overview of the Current Situation in Bosnia and Herzegovina with Focus on Cyber Security and Fighting Cyber-Crime by Establishment of BIH CERT Body," in Ashok Vaseashta, Philip Susmann, and Eric Braman, eds., Cyber Security and Resiliency Policy Framework (IOS Press, October 2014), 65-81, http://dx.doi.org/10.3233/978-1-61499-446-6-65.

[5] State Statistical Office, Information Society, accessed on 20 April 2015, http://www.stat.gov.mk/OblastOpsto_en.aspx?id=27.

[6] Ministry of Information Society of Macedonia, "Developed Information Society," accessed on 15 March 2010, www.mioa.gov.mk/files/pdf/Broshura_MIO_design_FINALNO.pdf.

[7] Stein Schjolberg and Solange Ghernaouti-Helie, "A Global Protocol on Cybersecurity and Cybercrime," *Cybercrimedata* (Oslo: E-dit, 2009), available at www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf.

[8] Schjolberg and Ghernaouti-Helie, "A Global Protocol on Cybersecurity and Cybercrime."

[9] Council of Europe, Convention on Cybercrime, available at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=20/02/2015&CL=ENG, Status as of 20 February 2015.

[10] The Official Gazette of R.M no. 37/1996, 80/1999, 4/2002, 43/2003, 19/2004, 81/2005, 50/2006, 60/2006, 73/2006, 87/2007, 7/2008, 139/2008, 114/2009, 51/2011, 51/2011, 135/2011, 185/2011, 142/2012, 143/2012, 166/2012, 55/2013, 82/2013.

[11] The Official Gazette of R.M no. 150/2010, 100/2012.

[12] The Official Gazette of R.M no. 13/2005, 14/2007, 55/2007, 98/2008, 83/2010, 13/2012, 59/2012, 123/2012, 23/2013.

[13] The Official Gazette of R.M no. 121/2006, 110/2008, 4/2009, 116/2012.

[14] The Official Gazette of R.M no. 133/2007, 17/2011, 188/2014.

[15] The Official Gazette of R.M no. 105/2009, 47/2011.

[16] The Official Gazette of R.M no. 79/2005, 110/2008, 83/2009, 116/2010.

[17] The Official Gazette of R.M no. 34/2001, 98/2008.

[18] Weber H. Rolf, "Internet of Things New Security and Privacy challenges," *Computer Law & Security review* 26, no. 1 (January 2010): 23-30, http://dx.doi.org/10.1016/j.clsr.2009.11.008.

[19] Metodi Hadji-Janev, "Toward Effective National Cyber Security Strategy: The Path That Macedonia Must Consider," in Ashok Vaseashta, Philip Susmann, and Eric Braman, eds., *Cyber Security and Resiliency Policy Framework* (IOS Press, October 2014), 57-64. http://dx.doi.org/10.3233/978-1-61499-446-6-57.

[20] Council of Europe, CyberCrime@IPA, Assessment Report, 18 June 2013, available at http://www.coe.int/t/DGHL/cooperation/economiccrime/Cybercrime/cy%20project%20balkan/2467_Assess_Rep%20v51_public.pdf.

[21] System/Network Administrators from the Former Yugoslav Republic of Macedonia Train in Cyber Defence, *NATO A-Z*, 8 April 2014, http://www.nato.int/cps/en/natolive/news_99718.htm?selectedLocale=en.

[22] Ministry of Information Society and Administration of Macedonia, "Establishment of a National Body for Dealing with Computer Incidents (National CIRT)," 8 August 2012, http://www.mioa.gov.mk/?q=node/3198.

[23] ENISA, CERTs by Country, Interactive Map, accessed on 21 April 2015, http://www.enisa.europa.eu/activities/cert/background/inv/certs-by-country-interactive-map.

[24] Eranda Begaj, "Albania's Vision towards Cyber Security," Paper from DCAF Young Faces 2014 - Cybersecurity Winter School for the Western Balkans (Geneva: DCAF, 2014), http://www.dcaf.ch/content/download/234387/3678194/version/1/file/YF14PolicyBrief-BEGAJ.pdf.

[25] Sabina Baraković, "Establishment of a CERT body in Bosnia and Herzegovina," Paper from DCAF Young Faces 2014 – Cybersecurity Winter School for the Western Balkans (Geneva: DCAF, 2014), www.dcaf.ch/content/download/234384/3678160/version/1/file/YF14PolicyBrief-BARAKOVIC.pdf.

[26] CERTBG, accessed on 7 June 2015, https://govcert.bg/.

[27] CIRT.ME, accessed on 21 April 2015, http://cirt.me/.

[28] CERT-RO, accessed on 7 June 2015, http://www.cert-ro.eu/.

[29] Ministry of Information Society and Administration of Macedonia, "Establishment of a National Body for Dealing with Computer Incidents (National CIRT)."

[30] Agency for Electronic Communications, accessed on 21 April 2015, http://www.aek.mk/en/.

[31] Agency for Electronic Communications, Public Hearing of the Annual Work Program of the Agency for Electronic Communications 2015, 24 October 2014, www.aek.mk/en/dokumenti/javni-raspravi/item/download/648_7406ed771ecd3545913 ae5573bb84b97.

[32] UNDP, International Expert for Preparation of an Assessment Study for the Requirements for Preparation of a National Cyber Security Strategy, 5 March 2014, http://jobs.undp.org/cj_view_job.cfm?cur_job_id=43974.

[33] EU, EU Cyber Security Strategy – Open, Safe and Secure, 7 February 2013, http://eeas.europa.eu/top_stories/2013/070213_cybersecurity_en.htm.

[34] Besnik Limaj, "Enhancing Cyber Security: the Challenges in FYROM, Kosovo and Moldova," 5 January 2015, http://www.observatoire-fic.com/contribution-enhancing-cyber-security-the-challenges-in-fyrom-kosovo-and-moldova/.

[35] UNDP, International Expert for Preparation of an Assessment Study for the Requirements for Preparation of a National Cyber Security Strategy.

[36] Alexander Klimburg, *National Cyber Security Framework Manual* (Tallinn: NATO CCD COE, 2012), available at https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf.

[37] Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Tallinn: NATO CCD COE, 2009), available at https://ccdcoe.org/research.html.

[38] Anna Humphrey, "USTDA Helps Launch Cybersecurity Innovation Center in Romania," 14 May 2015, www.ustda.gov/news/pressreleases/2015/MENAEE/Romania/PR-Cybersecurity-Innovation-Center-in-Romania_051415/Press-Release-USTDA-Helps-Launch-Cybersecurity-Innovation-Center-in-Romania_051415.asp.

[39] Estonian Defence League's Cyber Unit, http://www.kaitseliit.ee/en/cyber-unit.

Predrag TASEVSKI holds a MSc degree in Engineering in the field of cybersecurity and is doing a Post-Master in Communication and Security in France. His research interests are in the field of cybersecurity, cyber defence, security awareness, risk assessment, identity/risk management, cyber risk, cyber insurance, cybersecurity awareness, socio-technical aspects, data science and hacktivism. Predrag is the author of two paperback books: *Messenger-Pigeon* and *Interactive Cyber Security Awareness Program*, and has published in the PenTest, Hackin9 and Nova Makedonija magazines. He is also a Microsoft Certified Trainer and a Lead/External Auditor for ISMS. At present, he is an independent researcher.