Issue 53 / 1 July - 30 September 2018

RACVIAC
SE EUROPE

CENTRE FOR SECURITY COOPERATION

NEWSLETTER

Conference on Critical Infrastructure Protection

Arms Control Symposium

10th C-WMD Network Meeting

Interview with Dr Evangelos Ouzounis

Head of Secure Infrastructure and Services Unit, ENISA

Contents:

CENTRE FOR SECURITY COOPERATION

Newsletter editorial staff:

Maj Marija Čičak, PA Officer
Ms. Sanja Romić, Language Specialist

Rakitje, Stari hrast 53
10437 Bestovje, Croatia
Tel: +385 (0)1 3330 803
Fax: +385 (0)1 3330 809
info@racviac.org
www.racviac.org

MAG POCs Meeting

held in RACVIAC

A Meeting of Points of Contact of RACVIAC - Centre for Security Cooperation Multinational Advisory Group was held on 13 September 2018 in RACVIAC.

The purpose of the Meeting was to coordinate and discuss the details related to the inputs and requests received from the Members, Associate Members and partner organizations regarding the proposed draft of Programme 2019.

RACVIAC Director, Ambassador Haydar Berk, welcomed the POCs at the opening of the Meeting noting that he greatly appreciates the inputs and support of the representatives present.

The meeting began with a presentation by RACVIAC Deputy Director Brigadier General Gordana Garašić who provided information on the draft Programme 2019 as well as some additional proposals and remarks received via the Questionnaire regarding specific requests and/or aspects of participation by RACVIAC respective Members, Associate Members and partners. In addition the Programme Managers explained some particular facets of the activities within their respective Pillars and the main focus of the projects to be conducted in 2019 and 2020.

During the discussion that followed several details were clarified resulting in a more precise and concrete draft Programme 2019 that will be presented for the approval at the upcoming MAG Meeting in October 2018. ●

Interview with Dr Evangelos Ouzounis

Head of Secure Infrastructure and Services Unit, ENISA

At the very outset could you please explain what ENISA is and what it does?

ENISA is an EU agency that was established 15 years ago. ENISA supports the EU Member States, EU Commission and private sector when it comes to understanding cyber security challenges and risks and helps them adopt the appropriate good practices. It also assists the Member States in the implementation of EU policies, for example the NIS Directive or in the past the Article 13a or even Article 19 of the eIDAS .

We are not legislators so we cannot take policy initiatives ourselves. Also, we are not an operational body. We do not send the first response in a cyber-crisis situation but we do react and communicate our position and recommendations to mitigate the incident. Our efforts focus only on the EU, i.e., we don't have an international relations component. We do our best to be as helpful to Member States and private sector as possible with our limited but very skilful resources.

The Agency works closely with the Members States and the private sector on delivering advice and solutions in several areas, including cyber security. Is there a common EU cyber security strategy or act?

Yes, there is an EU strategy adopted and published a few years ago. It is an effort aimed at bringing the Member States together to collaborate on this topic. It is an important initiative with many interesting tasks. The EU cyber security strategy recognizes the importance of the topic and its impact on the EU economy and society.

How many EU Member States have their own national Cyber Security Strategies?

Today, all EU Member States have their own cyber security strategies. It took some time for the EU countries to understand and develop their approach. We are assisting EU Member States in understanding the issues and challenges, e.g. by developing numerous good practices in this area. There are, obviously, as with many other aspects in the EU, different "maturity levels". The good thing is that all of them have really developed their strategies and are actively pursuing them. There are countries in the early stage - they have just finished their strategy a few years ago - but also there are countries that are now in a second or third stage. We are very happy to see that EU states are progressing and developing and ENISA helps them a lot when it comes to addressing their needs.

The Cyber threats environment is changing constantly and quickly. What is the most challenging thing for the EU Member States in meeting the cyber security threats? Is it response capability, public-private partnership, cooperation or something else?

For the countries that have not developed their capabilities, skills, knowledge and expertise yet one big challenge is to develop particular capacities in this area like responding to incidents. They also need to streamline the existing policy and regulatory governance framework, to identify the agencies and the organizations which have to deal with the topic, to give them a particular mandate and recruit the appropriate people and somehow give them the opportunity to defend the country, the society and the economy. This means, for example, having a national CSIRT, running national exercises, or operating a cyber security centre.

The second challenge is to collaborate with the private sector because the assets are mainly in the hands of the

private sector. In our opinion, you cannot overregulate or order the private sector to do certain things in this area. So, you need to find the appropriate way of engaging with the private sector and follow a win-win approach.

There are also other challenges like keeping the ordinary citizens aware of the cyber security threats and risks or developing appropriate new talents with the necessary skills, e.g. at the universities. As you know, there is a shortage of skills in this sector.

Finally, it is also important to build the skills and expertise of the law enforcement agencies and give them appropriate means to run after cyber criminals.

So there are many challenges; it's a long journey actually without a final destination.

ENISA recently launched the National Cyber Security Strategies Evaluation Tool. Could you explain what its main purpose is?

The tool aims at helping the Member States to evaluate the success and impact of their strategies. This tool gives them the opportunity to assess their strategic objectives and their tasks. If the tool identifies gaps in a strategy, it offers them ideas and recommendations for improvement. So the persons dealing with the cyber security strategies can easily understand what is missing and choose one or more recommendations to implement.

We had a study on evaluating strategies in the past, about 2-3 years ago. It was a long paper. And you know, people are very busy nowadays and we saw that creating a web-based tool will be more appropriate and user-friendly. We have modernized our approach, we added some elements that will be timesaving and easy to use. We were looking forward to seeing the feedback and so far, the feedback is overwhelmingly good.

At the beginning of September 2018 the EU Commission proposed the establishment of a Network of Cyber Security Competence Centres. What could this initiative bring for EU and its Member States in the future?

As you said this is a proposal of the EU Commission suggesting the establishment of a Network of Competence Centres to be identified in Member States. The idea is to bring these national centres together to collaborate, work together and share resources on emerging cyber security topics. By doing so, we basically put together European and national resources and skills to address significant cyber security challenges in a coordinated manner. The national and European initiatives will be better synergised and the end result will be more suitable for them. It is a very interesting concept.

Who will lead this Network? ENISA or someone else?

The lead role will probably be assumed by an independent structure. I believe that the EU Commission has some ideas and they are discussing them with the Member States at the moment. Most probably, ENISA will contribute to the topics but won't have a leading role. But, it is too early to say as the debate with EU Member States, private sector and civil society is ongoing.

You have already mentioned the public-private partnership. The cooperation between the public and private sector is very important when it comes to critical infrastructure protection. What is the current status of public-private partnerships in the field of cyber security in the EU?

It is a developing topic. Ten years ago there were only a few countries actively pursuing public-private cooperation. Nowadays we estimate that approximately 15 countries have enough maturity and initiatives to cover the topic. There are many aspects that play a role. We have seen public-private partnerships emerging in countries like the UK and the Netherlands, some Scandinavian countries and later on Germany and France. There are different models we have identified, namely from the Goal Driven model to complete outsourcing or tight Control.

We have no particular opinion regarding suitability, we just analyse different models and come up with examples of good practices. Public-private cooperation has also to do with the regulatory culture of the country. Depending on how you have collaborated with the private sector over the years in other sectors you will most probably do the same with cyber security. If your approach is to have a strong control of the private sector, then you enforce particular requirements and then you audit them to see how and whether cyber security is improved. That's your cooperation model. On the contrary, if you believe that the private sector is accountable and should do its utmost to protect its assets then you follow a more participatory co-operation model.

At ENISA we are in favour of less regulation because you

cannot regulate trust, and trust is the fundamental component of such collaborations.

From ENISA's experience, what are the main challenges in establishing and developing public-private partnerships? What could be done to advance this cooperation/collaboration?

As I said the most important thing is to establish trust. You cannot command trust, you cannot regulate trust, so you have to develop it.

For that you need time to follow a very focused approach and care about the interest of all parties. As you know the private sector doesn't always trust the public sector and they will not easily reveal information about their affairs. They are afraid that it will be used against them. So you have to remove this fear of punishment and develop the relationship in such a way that there is mutual benefit. But this takes time.

So, in my opinion, it is the responsibility of the public sector to drive and demonstrate the quality of this collaboration. And this is where it becomes a little bit difficult because the public sector doesn't have the appropriate culture to approach the private sector. Also, you have to find some incentives to motivate the private sector to participate, put on the table resources and the means so that meetings and trusted information sharing takes place on a regular basis. And you have also to contribute information from the public sector to the private one. It cannot be that you are there only to listen and to get information from the private sector. It should be a win-win situation. And you have to be a bit careful about how you engage with the regulators, the police and the intelligence. So there has to be continuity so as not to upset the private sector. And above all, I think you have to show to the private sector that they are responsible for protecting their own assets and it is in their business interest to do so and if they do it properly then the state is there to help them do it better.

For years, RACVIAC has been addressing the topic of a public-private partnership especially in the area of critical infrastructure protection, as well as cyber security issues. Where do you see the possibilities for further cooperation between RACVIAC and ENISA?

We collaborate with all relevant institutions in the EU. It will be a pleasure to collaborate with RACVIAC as well.

Normally, we develop good practices on numerous topics and make them available to Member States and private sector. This is something that your Organization can benefit from. You can use all the document and tools we developed and customize them to your needs. ENISA could participate in meetings and workshops you organise with local communities and targeted stakeholders to present its work and good practices. Finally, if you are an eligible organisation our regulation allows you to ask ENISA to perform a small task or a project. This is what we call an article 14 request. ●

enisa
European Network and Information Security Agency

Dr Evangelos OUZOUNIS *is the head of ENISA's Secure Infrastructure and Services Unit. His unit facilitates Member States efforts towards a harmonised implementation of NIS Directive and Incident Reporting Scheme (article 13 a, article 4 of the Telecom Package, article 19 of the eIDAS Directive). The unit also develops good practices for National Cyber Security Strategies as well as Critical Information Infrastructures (e.g. smart grids, energy, smart cars, smart airports, eHealth and others) and IoT security.*

Prior to his position at ENISA, Dr. Ouzounis worked several years at the European Commission, DG Connect and co-founded Electronic Commerce Centre of Competence (ECCO) at Fraunhofer FOKUS (Berlin, Germany).

Dr. Ouzounis holds a Ph.D from the Technical University of Berlin and a master in computer engineering and informatics from the Technical University of Patras, Greece. He was a lecturer at Technical University of Berlin, wrote 2 books and more than 20 peer reviewed academic papers and chaired several international conferences.

Arms Control

3 - 4 July 2018, RACVIAC

The purpose of this two-day event was to discuss current and future Arms Control mechanisms and alternative national, regional and organizational programs, reforms and approaches aimed to foster a cooperative security environment and promote international security, stability and transparency.

The Arms Control Symposium 'Future Challenges and Developments in Arms Control and PSSM Domain', organized by RACVIAC - Centre for Security Cooperation with Federal Republic of Germany's support, was conducted on 03-04 July 2018 in RACVIAC.

The Symposium was a continuation of the established series of annual activities and attempts to bring together national and international experts in discussions on the future developments and possible challenges within the Arms Control domain.

The purpose of this two-day event was to build on the experience of last year's Symposium and to present the latest developments in Arms Control, with the aim to open up new perspectives on confidence-building measures in Europe. It also aimed to assemble national experts as well as expert NGOs to produce a vibrant and productive discussion on Arms Control issues, future developments, and tackle the possible challenges. An important element of its overall aims was the updating of relevant information regarding Arms Control topics and to discuss the way ahead.

The Symposium was opened with a Welcome address by RACVIAC Director Ambassador Haydar Berk who stressed the importance of a regional approach to security issues as a crucial element of peace and stability in the region and beyond. He also mentioned that this type of activity gives us an opportunity, together with the experts, to highlight the challenges and successes of the past whilst outlining the plans for the future in a very concrete way for the benefit of the SEE region.

Providing a platform that enables Members to update the SEE region on the relevant information on changes and plans regarding Arms Control topics in the participants' respective countries this RACVIAC Symposium on the first day focused on the current Arms Control challenges in Europe and world in general, the recent developments and new technologies in weapon systems as well as new threats regarding armaments and the current situation related to CSBMs in Europe. The recent developments in the Physical Security and Stockpile Management as well as Small Arms and Light Weapons area (training, deficiencies, solutions, support mechanisms, etc.) were a part of the Symposium's Agenda on the second day.

The Symposium gathered 29 participants and lecturers, representatives of ministries of foreign affairs, defence, security and interior and national authorities responsible for the implementation of Arms Control treaties or Arms Control experts in the field of SALW and/or PSSM from all over Europe as well as UNDP SEESAC, and OSCE Mission to BA.

After the Opening remarks the first to take the floor was Ms Isa Ghivarelli, Counsellor, Deputy Head of Delegation for the Politico-Military Dimension during the 2018 Italian OSCE Chairmanship, giving an overview of the 2018 Annual Security Review Conference organized by the Italian Chairmanship under the motto 'dialogue, ownership and responsibility to foster security in the OSCE area'.

Mr Zoltan Bacs from the Budapest Public University addressed the audience on the topic of current Arms Control Challenges in Europe and beyond touching upon both the social and scientific challenges from an academic standpoint.

Symposium

Later on Mr Richard Moyes, Managing Director of Article 36, a nongovernmental organization based in the UK, talked about the future challenges in Recent Developments, New Technologies in Weapon Systems and New Threats reg. Armament, and drew attention to the reasons behind the new weapon system's popularity and the concerns about their use expressed during the New Conventional Weapon Law discussions on a UN platform.

The last presenter of the day was Mr Andrew Dolan, Expert on Non-Proliferation of WMDs, who talked about global challenges in this domain.

The intention behind all of the abovementioned lectures was to stress the importance of looking forward to the upcoming challenges in the Arms Control domain. The focus was put on the European, but also the global challenges in the control of conventional but also non-conventional weapons. This allows us to look at a bigger and comprehensive picture, and opens up more space for discussion, new ideas and new perspectives.

The second day started with a presentation by Mr Dragan Bozanić from UNDP SEESAC, who gave an overview of the Western Balkan's SALW Roadmap as well as the issue of mainstreaming gender in SALW control. He shared the draft results of the survey conducted by SEESAC stressing its importance in highlighting the gender aspect of SALW and in helping to endorse the gender-blinded approach.

The second presenter of the day, LtCol Jens Kermes from BWVC, provided an insight into the BWVC's engagement in international SALW/CA Training as well as into PSSM projects while talking about the challenges they encountered, the methodological approach they used and the success they achieved during their work.

Mr Blaž Mihelic, an Advisor in the MoD of SI, took the floor after LtCol Kermes and introduced the International Ammunition Technical Guidlines.

The last presenter of the day and the Symposium, Mr Denis Selimović, Senior Expert at the Ministry of Defence of Bosnia and Herzegovina, gave an overview of the work of the BA Coordination Board for SALW and discussed the status of the implementation of BA SALW Control Strategy 2016-2020.

Thanks to excellent speakers and the participants' level of motivation the Symposium was a very successful event. Taking into consideration this year's results and proposals made by the participants RACVIAC will strive to build on this year's experience and organize another successful event next year.

The 10th Meeting of the C-WMD Network

17-19 September, RACVIAC

Back in 2015 RACVIAC with its partners recognized the urgent need to embark on the process of developing sound counter proliferation strategies that would leverage our strengths across the region. Today, three years into the project, most of the participating nations are nearing the completion of the drafting process and planning the testing and validation phase of their strategies.

The September 2018 Meeting was an opportunity to further discuss future sustainable cooperation within the RACVIAC C-WMD Network.

The 10th Meeting of the C-WMD Network national working/drafting groups took place in RACVIAC - Centre for Security Cooperation on 17-19 September 2018.

The Meeting was organized with the continued support of US European Command, US Defence Threat Reduction Agency, International Counter proliferation Programme, Proliferation Security Initiative and the Republic of Croatia.

The purpose of this three-day Meeting was to continue facilitating the development of national C-WMD strategies and action plans as well as to continue enhancing regional cooperation in counter proliferation.

Opening the Meeting RACVIAC Director, Ambassador Haydar Berk, extended a warm welcome to DTRA's Deputy Director Mr David Musgrave and thanked all experts for the indispensable support in this project since its very beginning. The Ambassador continued by saying that it was remarkable to see how many people have participated in and influenced this project since its beginnings when the C-WMD Network project idea was developed as one of the results of the Regional PSI exercise held in Zagreb, Republic of Croatia in November 2013. The concept was adopted in 2014 with a view to supporting countries in the SEE region to develop or refine their national strategies and action plans against the proliferation of WMDs. Further on Ambassador Berk invited everyone not to forget Croatia's invaluable support since it shared its own experience in developing its national strategy with all

participating countries and seconded personnel dedicated exclusively to this project.

In his Opening remarks Mr David Musgrave, DTRA's Vice Director for Plans and Programs, said that more secure cooperative regional efforts and deeper cooperation are needed in order to counter proliferation and weapons of mass destruction. He also mentioned that it is important to shift beyond national strategies and examine implementing cooperative means and counterproliferation networks across the South East European region. He concluded by saying: *"in order to counter a network you have to have a network and this group is a network to counter the WMD network."*

This Meeting was a watershed in the development of the CWMD Network. It signified a recognition that the formal element of strategy development technical advice has, for the most part, come to an end. It was also a recognition that most of the participating countries are well into the drafting and validation phase of strategy development, including the refinement of Strategy Action Plans.

The September 2018 RACVIAC Meeting was an opportunity to peer review the progress in the development of national C-WMD strategies and discuss various approaches for further regional cooperation.

This Meeting was also a watershed in the development of the CWMD Network. It signified a recognition that the formal element of strategy development technical advice has, for the most part, come to an end. It was also a recognition that most of the participating countries are well into the drafting and validation phase of strategy development, including the refinement of Strategy Action Plans. However, the September workshop was also a watershed moment as it initiated the 'end state' phase of the Network - the development and sustainability of CWMD regional cooperation efforts - which in itself was an exceedingly important process.

Additionally, the September 2018 event was an opportunity to launch the final phase of the project through the identification, refinement, and selection of activities that might be suitable as regional collaborative efforts. Since RACVIAC C-WMD Network was recognized as the right forum for cooperation in counter proliferation issues, during the Meeting participating nations submitted their suggestions for improving cooperation both at the national and regional level and proposals for continuation of the project in the future.

A part of the Meeting Agenda was dedicated to a Tabletop Exercise (TTX). The aim of this simulation TTX was to examine the role and importance of combating proliferation from a regional cooperative perspective. The exercise was set in the future 2019 but sought to reflect many of the current considerations relevant to proliferation. Although the exercise was fictitious, it was nevertheless based on a number of real events.

The Meeting gathered more than 50 participants, representatives of C-WMD Network participating nations and lecturers from DTRA, USEUCOM, Hungarian National Security Institute - National University of Public Service and Polish Ministry of Foreign Affairs. ●

The C-WMD Network project would have never seen the light of day without invaluable and constant support from US EUCOM, the International Cooperation Program and the Proliferation Security Initiative from DTRA and the Republic of Croatia.

27 - 28 September, Zagreb, HR

Conference on Critical Infrastructure Protection

The importance of critical infrastructure (CI) increases the more industrially developed a country is and the more dependent it is on the undisturbed functioning of CI both on its own and on the territory of other countries. The modern world has become highly dependent on certain sectors of CI such as the energy sector, communications, road and transport systems, finance, the internet and public services and every disruption in functioning leads to serious standstills and difficulties for individuals, the society and business entities as well as the functioning of the State. The modern trends in the development of the critical infrastructure protection field have various forms, from protecting the physical infrastructure to cyber protection and development of models in those specific fields.

The two-day International Conference *"Public and Private Security Companies in Critical Infrastructure Protection"* was conducted in "The Westin Zagreb" Hotel on 27-28 September 2018. The Conference was the 6th event in a RACVIAC mid-term project focusing on the changes in public and private partnerships and the effects of privatisation. It was organized by RACVIAC - Centre for Security Cooperation and the Croatian Institute for Urban Security and magazine "Zaštita".

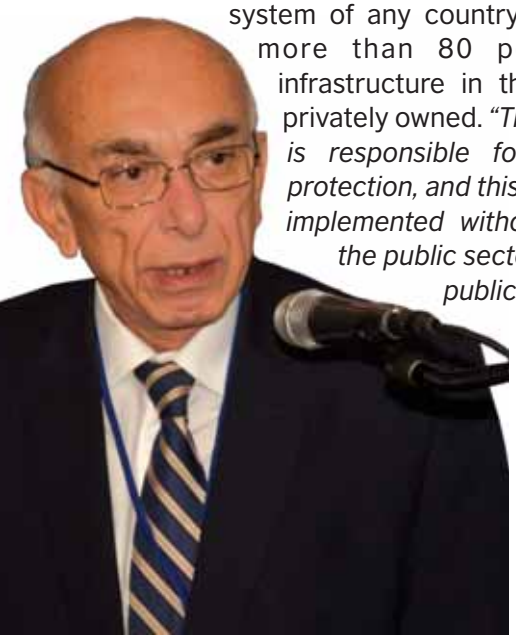
The aim of the Conference was to provide an interdisciplinary approach to the representation and application of modern methods in the protection of National and European critical infrastructure through the display of normative regulation, key activities of the protection stakeholders and development of the model of education and exercises.

The Conference was opened by Deputy Prime Minister and Minister of Defence of the Republic of Croatia H.E. Damir Krstičević who presented the Croatian Homeland Security System. Talking about the security system and critical infrastructure (CI) protection the Minister stressed that the key elements in protecting CI are procedures of security risks and crisis situation management and that this is a complex process. Later on the Minister spoke about the importance of effective security risk management in relation to CI since serious discrediting of CI always influences people and broader social community in some way.

"The importance of effective security risks management in relation to critical infrastructure results from the fact that serious discrediting of critical infrastructure always influences people and the broader social community in some way. That is why elements of the Homeland Security System on the state level should support owners/managers of critical infrastructure. This is especially true for providing support in the assessment of those security risks which only government bodies have the necessary and relevant capabilities for ",

said Minister Krstičević.

Director of RACVIAC - Centre for Security Cooperation, Ambassador Haydar Berk, in his Welcome address spoke about CI as an integral part of the national security system of any country. He underlined that more than 80 percent of critical infrastructure in the western states is privately owned. *"Thus, the private owner is responsible for management and protection, and this cannot be effectively implemented without cooperation with the public sector. The priority for the public sector is that critical infrastructure works without standstill and facilitates the delivery of products and services. In this context the concept of a public-private partnership in the protection of critical infrastructures presents the best platform for societal development and enables the proper functioning of states, organizations and individuals*", concluded Ambassador Berk.



"The concept of a public-private partnership in the protection of critical infrastructures presents the best platform for societal development and enables the proper functioning of states, organizations and individuals",

said Ambassador Berk.

This two-day Conference consisted of two panels: "Cyber Dimensions of Critical Infrastructure Protection" and "International Cooperation in Critical Infrastructure Protection".

Both of the panels were moderated by Mr Robert Mikac, PhD (Faculty of Political Science of the University of Zagreb).

The first panel focused on the cyber domain in critical infrastructure protection. Several international and national norms, standards, methods and good practices were presented.

The session emphasized the importance of continuous cooperation and coordination between the public and private sector in protecting critical services from cyber attacks, as well as in managing cyber incidents. In addition to continuous coordination, training, and building of trust, "proactive resilience" was highlighted as substantial in reducing the risks and responding to incidents.

The speakers were: Ms Anna Sarri of the European Union Agency for Network and Information Security (ENISA), Ms Franziska Klopfer from the Geneva Centre for the Democratic Control of Armed Forces (DCAF), Mr Robert Žunac, Director of the Information Systems Security Bureau (Croatia), Mr Peter Yapp, Deputy Director of the National Cyber Security Centre (UK), Ms Katri Liekkilä of the National Emergency Supply Agency (Finland), Mr Mate Botica, Director of the Digital Signals and Networks (OIV) (Croatia) and Mr Nino Talian, Information Security Section Head at King ICT Company (Croatia).

The second session, "International Co-operation in Critical Infrastructure Protection and Way forward" highlighted the advantages of international cooperation. The panel speakers presented some national and international normative regulations, and key activities of the CI protection stakeholders.

The relevant examples and cooperation experiences of public and/or private sector representatives were presented by Ms Isabella Palla of the Federal Ministry of the Interior, Department of Security Policy (Austria), Mr Richard J. Larkin, Expert for Critical Infrastructure

Protection (Minnesota, USA), Ms Ivana Cesarec, Senior Advisor at the National Protection and Rescue Directorate (Croatia), MAJ György Kelemen of the National Directorate General for Disaster Management, Department for Critical Infrastructure Coordination (Hungary), Mr Edin Garaplija, General Director of INZA Group (Bosnia and Herzegovina) and Mr Darko Barbalić, Senior Engineer at Hrvatske vode (Croatia).

At the end of the Conference it was concluded that both the public and private sector have the same importance in strengthening resilience and CI protection and that effective cooperation and innovative partnerships between national authorities, international organisations, civil society, and the private sector are crucial.

The Conference gathered more than 90 participants, governmental representatives, critical infrastructure expert staff, practitioners, creators of public opinion, owners or managers of CI, representatives of private security companies, and researchers from United States and all corners of Europe with special emphasis on the area of South East Europe. ●

LtC Kristina Pecirep ended her three-year tour of duty at RACVIAC - Centre for Security Cooperation on 31st August 2018. Filling the position of Operations Manager she will be remembered for her dedication and remarkable contribution to the Organisation and smooth running of RACVIAC activities. She was not only a good staff member but also a very helpful and courteous colleague to us all. Thanking her for her professional commitment and friendship we wish her all the best in her future career and private life.

After three years of service as the Leader of C-WMD Network **Ms Ivana Barabara Blažević** ended her tour of duty at the end of September 2018. We would like to thank her for all the efforts she put in order to support all RACVIAC C-WMD activities and ensure proper functioning of the Network. As a very good and efficient organizer Ms Blažević successfully managed all organizational, planning, and administrative work, facilitating the development of national WMD counter-proliferation strategies and management of response plans. She efficiently cooperated not only with all RACVIAC staff but with host nation institutions and partner organizations as well. Ms Blažević was an excellent team player and a good colleague, able to carry out her duties for the benefit of our Organization and its Members. We wish her all the best in her future career at the Croatian Ministry of Defence and in her private life.

C-WMD Network

No.	Topic / Title	Host / Venue	Date
1.	Nuclear Security Detection Architecture Awareness "Planning, Implementing, and Evaluating Detection Operations"	RACVIAC	09-12 October

Security Sector Reform

No.	Topic / Title	Host / Venue	Date
1.	6th Annual Conference on Security Challenges for Europe	Zagreb, HR	22-23 November
2.	Advanced SSR Series / Defence Resources Management: "Human Resources Management Challenges in the Security Sector"	RACVIAC	03-07 December

International and Regional Cooperation with focus on Euro Atlantic Integrations

No.	Topic / Title	Host / Venue	Date
1.	Workshop on Floods Protection and Prevention Project	RACVIAC	22-24 October
2.	Workshop on Developing Strategies on Rehabilitation and Reintegration of Foreign Terrorist Fighters (FTF)	Tirana, AL	12 - 14 November

MAG

No.	Topic / Title	Host / Venue	Date
1.	40th MAG Meeting	RACVIAC	18 October

CENTRE FOR SECURITY COOPERATION

„....fostering dialogue and cooperation on security matters in South East Europe...“

Follow us at:

www.racviac.org
twitter: @RACVIAC
facebook.com/RACVIAC