Centre for Security Cooperation

Military Academy "General Mihailo Apostolski"-Skopje

Ministry of Defence Bosnia and Herzegovina

Ministry of Foreign Affairs Bosnia and Herzegovina

Ministry of Security Bosnia and Herzegovina

American University in Bosnia and Herzegovina

Conference on
"Ensuring personal data protection while securing cyber space
(Challenges and perspectives for the South East European countries)"
(IRC-08-P)

29-30 October 2014, Sarajevo, Bosnia and Herzegovina

Activity Background

Technological development of social networks, smart cards, cloud computing and location based services has brought forth new challenges in view of personal data protection.
Disclosing personal data is increasingly becoming a part of modern life and people feel that they give away too much data and that they are not in control of their data.

The aims of this event included exchange of information, transfer of knowledge, views and ideas as well as dissemination of international standards regarding data protection. Another aim of this event was to identify the key actors and their priorities regarding who, when and where in SEE countries is responsible for the actions needed to organize and conduct effective personal data protection while building a secure cyberspace.

Activity Venue, Duration and Participation

The Conference took place in Sarajevo, Bosnia and Herzegovina, from 29–30 October 2014 on the premises of the Bosnia and Herzegovina Parliamentary Assembly.
It comprised three sessions which were designed to include presentations and discussions.
The participants and lecturers included representatives from Albania, Bosnia and Herzegovina, Croatia, Serbia, the Former Yugoslav Republic of Macedonia[1], Montenegro, Romania, Slovenia, Turkey, the USA, the EU Institutions, NATO, RACVIAC and other institutions and organizations deployed in Bosnia and Herzegovina, with around 150 participants in total.

Conference Opening

The opening speeches were given by Ambassador Branimir Mandić, Director of RACVIAC, Dr Danilo Türk, former President of the Republic of Slovenia, Mr Igor Rajić, Director of SEECSC, Mr Esmir Ganić, President of AUBiH and Mr Tomislav Limov from the Ministry of Security of Bosnia and Herzegovina.

Ambassador Branimir Mandić expressed gratitude to the respective ministries in Bosnia and Herzegovina- the Ministry of Foreign Affairs, Ministry of Security and Ministry of Defence- for extending their support in making this event a reality. Also he expressed thankfulness to the American University in Bosnia and Herzegovina for its generous support as a co-organizer of this event, and appreciation to the Military Academy "General Mihailo Apostolski" from Skopje which also decided to support the event.

"…due to certain challenges or barriers which are mainly political, financial, organizational and legal in nature, the level of cyber security is at a different level in different countries."

HE Amb. Branimir Mandic, Director of RACVIAC

Ambassador Mandić went on to say: "As soon as RACVIAC - Centre for Security Cooperation adopted the new strategy and broadened its scope of activities and area of interest to new issues, cyber security was recognized as one of the subjects that should be a part of the RACVIAC curriculum due to the fact that the volume of cybercrime is significantly increasing, while cyber security is at different levels in different countries in the South East European Region."

[1] *Turkey recognizes the Republic of Macedonia with its constitutional name*

From 2007 to the present day RACVIAC has organized six events that have covered different topics related to cybercrime and cyber security threats, vulnerabilities in cyberspace, discussions on Cyber Defence Strategies and Policies, Impact of Cybercrime in Economy Environment, etc. The last one was organized in May 2014 when cyber security experts, members of Computer Emergency Response Teams from SEE countries got together and discussed at length relevant topics in the field. The aim of that event was to enable participants to exchange knowledge and experience as well as to facilitate networking among them, and once again to raise awareness of the importance of cooperation in response to cyber threats on the national and regional level.
As a kind of conclusion to all of these events, it was recognized that due to certain challenges or barriers which are mainly political, financial, organizational and legal in nature, the level of cyber security is at a different level in different countries.
Ambassador Mandić also pointed out: "New technologies bring new challenges – new technologies also imply uncontrolled sharing of information – that is to say, sharing of information in the wrong way and with or among wrong people, whereby the largest proportion of information shared is personal (private) data."
Information technology development and use of cyberspace is progressing much faster than legislative development in this field and privacy or personal data protection is (or should be) based on legislation or regulations and there is that gap between technological development and the legal framework that needs to be narrowed down. Precisely for that reason it is very important to confront different perspectives, public policy makers, industry representatives and technical experts in order to hear things from different perspectives (in other words, possible agreements and disagreements, all points of view)."

Former president of the Republic of Slovenia **Dr Danilo Türk** emphasized the importance of the fact that Bosnia and Herzegovina is taking an initiative in the area of cyber security which is of great importance for this part of Europe.

"...the purpose of new technologies has always been to secure better life for the people, however, we have to be aware of the potential risks..."

Dr Danilo Türk, former President of the Republic of Slovenia

Dr Turk continued "I believe that all countries of South East Europe are interested in this subject and they all know how important it is to protect their citizens from cyber-attacks. We are talking here about a very important subject for our future. Slovenia is dealing with this issue in the framework of the European Union and NATO, but it is very important to establish a connection among the experts from the region."

Mr Tomislav Limov, head of the Office of the Deputy Minister of Security of Bosnia and Herzegovina, who in his speech among other things emphasized that this conference is a good opportunity to see what we did and what we need to do in order to be more effective in terms of personal data protection in cyber space.

"…computerization brings many advantages but at the same time possibilities for different types of criminal activities... Those problems are transnational and, thus, the response to them must be transnational..."

Mr Tomislav Limov, head of the Office of the Deputy Minister of Security of Bosnia and Herzegovina

The conference propounded activities of the AUBiH's newly established Southeast Europe Cyber Security Center (SEECSC) which will contribute to the protection and data security development of institutions in Bosnia and Herzegovina and the region.

The Director of the Center **Mr Igor Rajić** welcomed all participants and said that "The cyber-attacks on the web pages and information systems, fraud, identity theft and child pornography are just a small piece of the globally expanding phenomenon of mushrooming cybercrime. With that in mind, ***the use of advanced technology and education is a critical factor in overcoming cyber security challenges and creating a more secure environment.***"

Human rights and privacy in the digital age in the context of "Security vs. Privacy"

During the first session **Dr Metodi Hadji-Janev**,**(Col)**, from the Military Academy "General Mihailo Apostolski" - Skopje elaborated on the topic "Human rights and privacy in the digital age in the context of 'Security vs. privacy debate ' ".

At the start of his presentation Dr Hadji-Janev talked about the geopolitical environment, security trends and human rights in the context of the process of power redistribution and redefinition of power after the end of the Cold War. Globalization and technological development enabled many non-state actors (groups and individuals), but also some states to gain strategic power. New technologies also create new

challenges and threats that only a few security concepts could partially be applied to in order to counter them.

By asking the question ***"National security vs. human rights - where is the right balance?"*** Dr Hadji-Janev explained that actually there are some challenges in finding the right balance between national security and human rights because we (people of different countries) have different cultural perspectives, threat perceptions and different approaches when we talk about criminalization and punishment of cyber offence. Dr Hadji-Janev also talked about data protection and data retention, giving the example where the European Court for Human Rights found "that the indefinite retention of biodata such as fingerprints, cell samples and DNA profiles from persons suspected of, but not convicted of, crimes was an intrusion into privacy that was disproportionate to the public interest which was sought to be protected." [2]

NATO policy on personal data protection while securing cyber space

LTC Brian Bengs, Legal Advisor from the NATO School talked about the NATO perspective regarding Personal Data protection and offered an explanation concerning the NATO Cyber Defence Procedure.

Answering the question in regards to the NATO Policy on Personal Data Protection, LtC Bengs said: "NATO does not have a single, comprehensive policy on Personal Data Protection, but multiple sources address different topics".

It is the national responsibility to develop and maintain capabilities for personal data protection in cyber space, in other words - Cyber defense & personal data protection are the primary responsibilities of NATO member nations, not NATO.

Talking about NATO Biometrics Information Policy it was emphasised that it allows each NATO nation to choose its level of participation in NATO biometric operations & maintain control of the biometric data produced by its national forces as required by national legislation.

Referring to the NATO Summit 2014: Wales Summit Declaration, LtC Bengs emphasized the part of the Declaration that is related to cyber threats: ***"Cyber threats and attacks will continue to become more common, sophisticated, and potentially damaging. To face this evolving challenge, we have endorsed an Enhanced Cyber Defence Policy, contributing to the fulfillment of the Alliance's core tasks…*** *Our policy also recognizes that international law, including international humanitarian law and the UN Charter, applies in cyberspace. Cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security and*

[2] *S. and Marper v. the UK [2008] ECtHR App Nos. 30562/04; 30566/04, [200*

stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm, therefore, that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis."

Future Threats in Cyber Security

Dr Brian Woerner, Professor & Dept. Chair of the Lane Department of Computer Science & Electrical Engineering at West Virginia University started his presentation with the following words: ***"Just as gunpowder made obsolete the use of castles as defensive measures in modern warfare, disruptive technologies threaten to render traditional Cyber Security measures inadequate to protect information assets."***

"…it is a user responsibility to update/secure the operating system and security software on individual machines..."

Dr Brian Woerner, Professor & Dept. Chair, Lane Department of Computer Science & Electrical Engineering, West Virginia University

Dr Woerner continued his presentation by explaining some future challenges for cyber security and data privacy and talked about Wireless and mobile systems, Cloud assets, Social media and data aggregation, Biometrics and Blurring of jurisdictional boundaries.

Technical aspects of protecting privacy in cyberspace

SEECSC SOUTHEAST EUROPE CYBERSECURITY CENTER

During the conference the participants had the opportunity to see some practical samples of cyber-attacks (Cyber Warfare using Mobile Device as a Weapon), the ways of prevention and cybercrime investigation and use of data by the legislative authorities. This was presented by the team members and experts from SEECSC.

National experience, challenges and perspectives to ensure personal data protection while building a secure cyberspace

The last session was dedicated to the national presentations, during which the country representatives had an opportunity to present their own experiences, the current status, challenges and perspectives regarding personal data protection.

During this session it was recognized that all participating countries have the legislation and institutions (agencies) in place that deal with personal data protection. These legislative documents are mainly in line with the EU Directives and regulations dealing with cyber security.
As was mentioned by almost all of the speakers during this conference, it is impossible for one nation to protect itself against cyber-attack and, thus, cooperation on a regional and global scale is a must.
The participants acknowledged that the information provided during the conference and issues discussed were of great benefit to them.
One of the main conclusions was that there is still room for improvement concerning personal data protection and ensuring cyber security and that we should continue with our activities to fulfill the joint needs of the countries of the SEE Region.

CONFERENCE CONCLUSIONS – It is necessary to take in consideration the following:

1. Creation of a sustainable system on a continuous basis, intermediate and advanced education of the pupils and teachers/professors regarding the principles of personal data protection in primary and secondary education.
2. Strengthening of the public-private partnership and international cooperation in dealing with cyber security issues.
3. State institutions and organizations should comply with the principles of data processing and should not obtain personal data excessively.
4. Involvement of the civil sector, educational authorities and media in the process of raising of public awareness (advancing the cyber security culture).
5. Keeping up to date with the latest technologies used in processing of personal data.
6. Continuing the harmonization of the national legislation in separate areas with the documents of the Council of Europe, European Commission and use of good practices of the EU member states. Consumers should give their personal data consciously to related parties in the context of buying a product or subscribing to a service.
7. It is essential that personal data must be processed:
   - fairly and lawfully;
   - upon consent of the data subject;
   - adequately, relevantly and not excessively in relation to the purposes for which they are collected;
   - accurately, and, where necessary, up to date;
   - kept in a form which permits identification of data subjects for no longer than necessary.
8. Continuous adjustment of the legislation with the problems faced in practice.
9. Detecting and mitigating digital intrusions means that visibility and response is an absolute must.
10. The Information technologies such as mobile devices are useful and they are here to stay but we have to be aware that they could be used as a weapon against users and their organizations.

11. It is the responsibility of assigned organizational management to take reasonable and appropriate measures to safeguard sensitive information in line with regulatory demands and consumer expectations.
12. Ensuring that the law of personal data protection is respected in all areas where personal data is processed, particularly in cyberspace.
13. Identification of problems and violations regarding the applicability of the legislation related to the protection of personal data.
14. Improvement of efficiency of inspection.
15. Unification of implementation of the legislation for personal data protection.
16. Introduction of online inspection where possible.

Compiled by: LtC Josip Mlakic, Conference Coordinator, RACVIAC – Centre for Security Cooperation