Ministry of Internal Affairs

TRAINING OF UKRAINIAN LAW ENFORCEMENT TO EFFECTIVELY COMBAT CYBERCRIME

As all kinds of modern crimes became more and more IT-dependent, the law enforcement experts with good understanding of criminals' activity in IT sphere would be needed in any police unit, not only in the units directly responsible for combating cybercrime.

Thus, Ukraine needs the sustainable all-sufficient educational system, which would produce law enforcement officers with appropriate knowledge at all the necessary levels. In this situations mane countries start their own national programs. All this reveals the extreme necessity of creating relevant National Law Enforcement Training Strategy in order to provide all the future work of the Ministry of Internal Affairs of Ukraine. In addition to the mentioned so far Ukraine has problems with existing national legal framework related to cybercrime.

BASIC REQUIREMENTS FOR LARGE-SCALE TRAINING OF UKRAINIAN LAW ENFORCEMENT TO EFFECTIVELY COMBAT CYBERCRIME

Five training groups with numbers of relevant topics have been distinguished as a result of analyzing of the existing practices of universities in the USA and EU member states and comparing them with the respective situation in Ukraine:

1. Cybercrime investigations (with 9 training topics);
2. Computer forensic specialists (with 16 training topics);
3. Network security specialist and incident investigations (with 15 topics);
4. Economic crimes investigations (with 2 training topics);
5. Child pornography investigations (with 4 training topics).

Also the entire range of policing involved into the IT sphere has been divided into the most actual specializations as described below. And the scope of IT areas of activity required for each of them has been outlined also.

All policemen and especially first responders despite their police specialization should be able to work within up to 22 cyber-related areas of activity.

Detectives and inspectors of the Operative-Technical department and Computer Intelligence units require the knowledge of the same field, but with a greater level of detail. They should be able to:

- identify functions of nets, equipment and software required, legal issues and risks of undercover online investigations,
- describe evidential requirements and admissibility of evidence during online activity, methodology for evidence capture, communications methodologies, best practice in legend building, etc.

Training in this subject is normally broken down into the following categories:

- Theory and Good Practice – covers the basic requirements for establishing a covert online capability (13 topics);
- Communications - examines specific issues of interest to undercover intelligence (8 topics);
- File Sharing - includes application reviews, traceability, dangers and specific issues relating (8 topics)
- Internet interception and network security specialists require different skill sets depending on the type of crime being investigated (28 topics)

Digital forensic specialists are expected to have a sound technological background. They should be able to fulfill 17 specific tasks.

DIRECTIONS OF REALIZATION OF LARGE-SCALE TRAINING OF UKRAINIAN LAW ENFORCEMENT TO EFFECTIVELY COMBAT CYBERCRIME

Taking into account the significant increase in the number of sophisticated cybercrime and rapid information technologization of crime in general, as well as trying to predict the style of work of units successfully combating cybercrime, we can clearly distinguish two types of policing and, accordingly, two levels of appropriate training of police officers.

- Firstly, the majority of police officers are policemen on the street.
- The second level is the level of officers who are not obtaining evidences on the street, in offices of enterprises or whatever.

We focus on the two levels of training:

- the first of which is called the "basic" (for every single police officer),
- the second – "IT-policeman".

(*This second level is designed for police officers who have devoted all their activities combating crimes in the area of IT*.)

In Ukraine are being mainly determined by the three powerful educational centers:

- National Academy of Internal Affairs in Kyiv (the capital of the country);
- Kharkiv National University of Internal Affairs;
- Odessa State University of Internal Affairs.

The work over cybercrime issues will be considered on the example of one of these educational centres: Kharkiv National University of Internal Affairs.

While planning the development of Level I, it is necessary to bear in mind that the destination of its knowledge and skills should be a professional police officer with basic police philosophy, knowledge and skills. The officer should know, understand and feel the notions of “facts finding”, “evidence base”, etc.

Thus in the process of educating the officer to the Level I the educational system should extend his regular field of activity to broader extent. To teach him to exercise his regular job, but over the objects, which belong to the sphere of IT. This approach to new objects of IT sphere should be inculcated to both: officers with experience of many years policing without “IT-approach” and cadets of police education institutions.

The structure of educational system of the Ministry of Internal Affairs of Ukraine enables to provide this education to both: cadets and regular police officers in the field.

In order to prepare training material and provide “IT-education Level I” to cadets, it is necessary to use the fact, that the Universities of Internal Affairs of Ukraine contain a “variable part”. It means a portion of educating time, the content of which may be changed without approval of external supervisors. Now the work of creating the curriculum for “IT-education Level I” is being carried out in the Kharkiv National University of Internal Affairs within the “variable part|.

The curricula created in the Universities of Internal affairs will be also applied in training regular police officers. The studies of the officers on the basis of the created curricula will be provided via existing mandatory in-service training of Ukrainian Law Enforcement Agencies.

The implementation of the advanced level “IT policeman” would meet real difficulties on its way. A police practitioner of this level should have sufficient knowledge and skills in IT field. Of course, such serious technical background can be obtained in a technical university. But unfortunately real life evidences that graduates of such institution use to find well payed job in civilian life beyond the law enforcement sphere. On the other hand, the police practitioner of the level “IT policeman” should also have a strong police background.

The outcome of these two considerations is that the best source for “IT policemen” are the most technically educated police practitioners. It should be accepted that the vast IT knowledge and skills of the level II cannot be inculcate in process of regular in-service training. For the educational process the officer should be released from his regular duties. In order to provide the necessary education the Educational system for law-enforcement in Ukraine enables two opportunities: 1) retraining of law-enforcement (the brunch of in-service-training) through the secondment of the officer to the educational center with the duration of one to three months; 2) dispatching a law enforcement officer with an educational level of "bachelor" to magistracy by one of the specialties of anti-cybercrime.

As it was mentioned, in both cases the “cybercrime IT education” is based on the knowledge and skills of a law-enforcement professional. Regarding the levels of readiness of the educational system of the Ministry of Internal Affairs of Ukraine to implement the mentioned training system, it is necessary to pay attention to the two main aspects: 1) availability of necessary equipment; 2) availability of trainers; 3) level of their proficiency.

Concerning the Level I (basic IT level), the educational framework in the Ministry of Internal Affairs of Ukraine is sufficient. The classes can be delivered by Ukrainian trainers. However they need to enhance their knowledge and skills.

Of course, we are eagerly inviting experts from the countries known for their successes in the areas of police activity related to combating cybercrime. The main goal of the visits of experts to the University is to organize Train the Trainers Program in order to make the system of dissemination of acquired knowledge and skills self-sufficient through Cascading Programs.

Definitely, implementing of the Level II (“IT-Policeman”) would need even more trainings for our teaching staff in the countries with vast positive experience of combating cybercrime. It is obvious because of strong reasons: 1) more sophisticated knowledge and skills, 2) sophisticated equipment, 3) this equipment is not available at training centres in Ukraine.

In 2012 in response to the Order of the Minister of Internal Affairs of Ukraine (MIA) “On the organizing of activity of the Office of cybercrime of MIA and regional cybercrime units of MIA they were establishment.

However, large-scale training of law enforcement agencies in this fight, as well as international cooperation, are not included in the list of the tasks of these units. Although this interaction is necessary and directly in daily practice of combating cyber-crime, and in the course of permanent enhancement of tools and methods of this activity. Therefore, the theoretical part of this work to be accomplished, should be entrusted to law enforcement educational centres.

First cyber-police officers graduate in Ukraine (2016)

84 cyber-police officers, trained by the Office for Security and Cooperation in Europe (OSCE) started work in Ukraine on the grounds of Kharkiv National University of Internal Affairs.

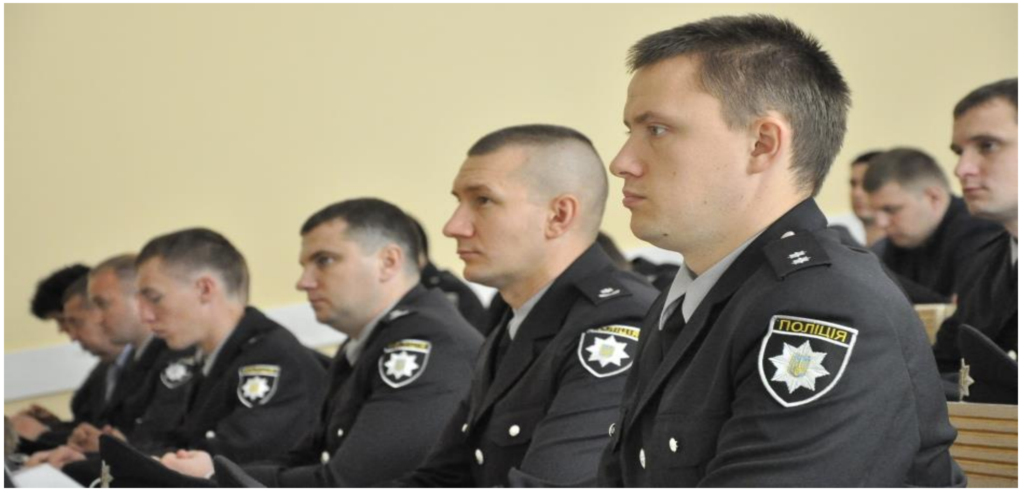
The initial 20 special agents and 64 inspectors make up one-third of the personnel of the new Cyber Police Department, which was created within the National Police of Ukraine as part of the wider law enforcement reforms in the country.

To start a full and good training of cyber policemen helped the Government of Canada and the OSCE. Unique courses on digital forensics and computer security were developed.

The education of inspectors and special agents designed for 400 hours.

Every year starting in 2016 an OSCE-supported re-training programme for cyber police officers in Ukraine. 100-hour training course, developed and implemented by the OSCE Project Co-ordinator in Ukraine, is an opportunity to enhance skills and knowledge of 100 officers who have already passed the attestation process.

International experts presented officers of the Ministry's specialized units from the central office and six regional centers with skills and details of handling cases related to malware distribution, network infrastructure attacks as well as the storage and distribution of child pornography. Among other topics were techniques for identifying and establishing the location of a suspect, uncovering and gathering evidence of cybercrimes, including how to counter attempts to hide and encrypt data.



Training center:

The OSCE Project Co-ordinator has been building the capacity of Ukrainian law enforcers in their responses to cybercrime since 2011. The Project Co-ordinator has helped to equip a training room with modern equipment in two police education establishments and headquarters, and trained police staff with the support of international practitioners.
From 2012 twenty Ukrainian police officers and experts improved their knowledge and skills in investigating cyber-related crimes at a six-day intensive training course, organized in Kyiv by the OSCE Project Co-ordinator in Ukraine

Forensic lab

Created with support of US Embassy in Ukraine.

The main aims are:

- forensic examination of seized evidence;
- supporting agents in the investigations;
- collecting evidences;

Thank You!

Anna TYTKO

Senior Researcher of National Academy of Internal Affairs

PhD, Associate Professor