International cooperation for Critical Information Infrastructure Protection: NATO-UKRAINE Trust Fund on Cyber Defence

Miruna-Maria Cocolan
Counselor
R.A. RASIROM, Romania

Abstract: *Nowadays world is marked by the rapid evolution of communication and information technologies. The 21st century can be defined by the increase in asymmetric threats to global security, in direct relationship with the technological progress and the development of virtual networks. The unprecedented level of technological evolution has led to a society change. The virtual space, among the opportunities that it provides, also generates a shift in the area of risks and vulnerabilities. The dependency on information systems increases the probability of an attack on critical infrastructures. In the borderless realm of cyberspace, the nature of the conflict has changed, so it is a certainty that cyber security cannot be achieved by each state on its own, but only by building and maintaining a strong international cooperation.*

One of the projects contributing to ensuring the security of cyber space is the NATO-UKRAINE Trust Fund on Cyber Defence, aimed at providing Ukraine with the necessary support to develop its defensive CSIRT-type technical capabilities, laboratories to investigate cyber security incidents and Incident Management Centers and also to secure one or more Critical Information Infrastructures, including a training and advisory dimension with an adaptive approach. Presenting the development of this NATO project, with Romania as lead-nation (through the Romanian Intelligence Service), RASIROM R.A. as Executing Agent (Romanian government-owned company) and other NATO-member states as contributors can help us gain a better understanding on how cooperation in the cyber realm can contribute to enhancing the security of nation-states and can lead to the implementation of more similar technical initiatives.

Establishment of NATO-Ukraine Trust Fund on Cyber Defence

NATO-Ukraine Trust Fund on Cyber Defence (NATO-UKRAINE TF CD) was agreed upon by the Alliance and Ukraine during the Wales Nato Summit in 2014 and was driven by the neeed to further develop and improve the information security of Ukraine, in the context of the crisis that emerged in the respective period of time. NATO Foreign Ministers agreed on Measures to Support Ukraine in the framework of the Distinctive Partnership in April 2014 and proposed additional measures in June the same year, that were endorsed by the NATO – Ukraine Commission Heads of State and Government in September 2014. These measures included the launching of a Trust Fund on Cyber Defence.

At the above-mentioned Summit, NATO Allies established a comprehensive and tailored package of measures so that Ukraine can better provide for its security. One of the areas the package focused on was cyber defence, with the scope of helping Ukraine develop technical capabilities to counter cyber threats. Allied and Ukrainian analyses have highlighted the weakness of Uraine's specific defence capacities in the face of cyber threats as a critical vulnerability in that period of time. In order to shape the legal basis for the process of Ukraine's national cyber defence capacity and capability building, steps have been taken towards formulating legislation on cyber defence. Effective interagency and international cooperation in the sphere of cyber defence was also needed to ensure the successful development of Ukraine's cyber security capabilities, and this required a concrete and efficient mechanism for such cooperation.

Scope of NATO-Ukraine Trust Fund on Cyber Defence

NATO-UKRAINE TF CD was intended to support Ukraine in strengthening its cyber defense capabilities, through the provision of hardware, software, technical assistance, advisory services and training. The project aimed at providing Ukraine with the necessary support to develop its strictly defensive cyber capabilities within the limits of the contributions collected from the nations.

The development of strictly defensive cyber capabilities of Ukraine was accomplished via the implementation of advanced cyber defence technical solutions and systems to Ukraine's critical infrastructure facilities, in order to ensure the proper level of cyber security, personnel training on

maintenance and management of the installed systems and setting up laboratories for computer and network forensic analysis, with their stationary and mobile components.

NATO-UKRAINE TF CD was aimed at providing Ukraine with the necessary support to develop its defensive CSIRT-type technical capabilities, laboratories to investigate cyber security incidents and Incident Management Centers and also to secure one or more Critical Information Infrastructures (CIIs). The project also included a training and advisory dimension with an adaptive approach, based on the interests of both the Allies and Ukraine and derived from the requirements of Ukraine's security and defense sector institutions.

This approach ensured concrete and relevant results in the short term, while remaining scalable according to the availability of funds and flexible to enable adaptation to relevant lessons identified in the course of the NATO-UKRAINE TF CD's implementation. In order to fulfill the project's purpose, its main characteristics were:

- Strictly defensive;
- Training&advisory dimension;
- Scalable approach, depending on the available funds.

From the beginning, the project was thought to be scaled depending on the contributions received from the nations and with the possibility of extension, if deemed appropriate by the Parties. The hardware, software and training needed for the NATO-UKRAINE TF CD's implementation were supported from the budget of the Fund, amount collected from Romania, as Lead-Nation, and other Contributing Nations. All hardware and software required for the implementation of the NATO-UKRAINE TF CD were purchased from the international market.

Organization of NATO-Ukraine Trust Fund on Cyber Defence

The end user of the project was Ukraine, with the Security Service of Ukraine (SBU) as national focal point. In Ukraine, the SBU is the national coordinator for the NATO-UKRAINE TF CD's implementation. SBU was also responsible for the coordination at national level with the other receipient institutions, in order to ensure the appropriate and timely implementation of all the project's stages.

Romania, acting as Lead Nation, was the coordinator of NATO-UKRAINE TF CD's implementation, through the Romanian Intelligence Service (RIS). The RIS facilitated the supplying to the receipient Ukrainian institutions, through SBU, of the equipments, software, installation services and equipment configuration services. Also, it ensured that the supplied hardware and software were working according to the technical specifications.

The Executing Agent for the project's implementation was the Romanian government-owned company RASIROM R.A., specialized in cyber and physical security and with experience in information security technologies. The company, having expertise in INFOSEC technologies and in the field of integration and engineering of complex IT&C and physical security systems, was defined authorized and responsible for the implementation of the project. The Executing Agent was defined responsible for setting up the technical components, as well as for providing related training and advisory services.

General description of the project

The implementation period of the project was 30 months. In December 2014, the NATO-UKRAINE TF CD was declared operational. First half of the 2015 was dedicated to the preparation of the implementation framework and collection of contributions. The year that followed implied the elaboration and signment of official documents, clarifying the rules and regulations under which the project operated and also the establishment of the tender procedure. After establishing the project's setup, the acquisition of the equipment followed, its delivery to Ukraine and its installation in the beneficiary institutions.

The project also included a training dimension. In May and July 2015, five training courses (amounting 100.000 EUR) were delivered by Estonia to the Ukrainian side, as an in-kind contribution. Ukrainian participants from several Ukrainian government institutions attended the courses, that were considered beneficial and helpful, indicating the interest for further courses if additional funds were to be available in the future.

The project's budget was 965.000 EUR, plus 100.000 EUR pledge, and the total cost of the project was 923.093,93 EUR. The NATO-IS Office of Financial Control acted as Treasurer for the project, a special account administered by this institution being opened with this purpose.

As regarding the contribution status, it consisted of:

- 965.000 EUR, as follows: Albania (25.000 EUR), Hungary (100.000 EUR), Italy (250.000 EUR), Portugal (30.000 EUR), Romania (500.000 EUR), Turkey (60.000 EUR);
- 100.000 EUR pledge, representing Estonia's in kind contribution (Training courses delivered by Estonia to the Ukrainian side);
- United States of America's in-kind contribution, tailored to the scope of the NATO-UKRAINE TF CD.

The technical part of the project consisted of:

- Establishing/Developing Incident Management Centers – in order to enable the collection of cyber security events (2 Ukrainian beneficiaries);
- Development of forensic laboratories (fix and mobile) – in order to support the activity following a cyber incident detection, to investigate the cyber incidents within CSIRT: Host-Based Computer Forensics, Network-Based Forensics (one Ukrainian beneficiary);
- Protection of critical information infrastructures – employ a solution based on the Romanian experience (one Ukrainian beneficiary);
- Personnel Training.

In order to succesfully complete the project, RASIROM R.A. signed a provision/supply contract with a Romanian company, by organizing a public tender procedure. The tender procedure had the subject of product acquisition for the NATO-UKRAINE TF CD, with RASIROM R.A. being the contracting authority and Ukraine being the beneficiary. The company that won the procedure had as a subcontractor an Ukrainian company.

To mark the completion of the project, between the SBU and RASIROM R.A. have been signed a TRANSFER AND ACCEPTANCE ACT OF GOODS and a DOCUMENT OF ACCEPTANCE of the hardware and software goods delivered under the NATO-UKRAINE TRUST FUND (TF) ON CYBER DEFENCE. Through this documents, SBU acknowledges the completion of the project, in accordance with the undertakings established in the Agreement on implementation of NATO-UKRAINE TF CD and in the Addendum to this Agreement.

Challenges encountered in the implementation of NATO-UKRAINE TF CD

The main challenge encountered in the implementation of NATO-UKRAINE TF CD did not consist in setting-up the technical side of the project, which was handled without any obstacles, but in the alignment of the legal provision of all Parties involved. The legislation of Romania is not very simmilar with the one of Ukraine's, so all the efforts had to be made in order to align them and to find the best possible options so the project could be succesfully implemented. In addition to that, the compliance with NATO and EU regulations also had to be taken into consideration. The area where the project was considered to be the most challenging was the assurance of a smooth transfer of the equipment from Romania to Ukraine, as follows:

- The export procedures

After the acquisition of the equipment has been completed and the packages were labeled and prepared for delivery, the Executing Agent submitted to the Department for Export Controls of Romania (ANCEX) the documents required by law for classifying the products as dual/non-dual. After analyzing the documents, ANCEX stated the need for an export license for the dual-use equipment. Therefore, activities and procedures in order to obtain the export licenses mandatory for the export process were conducted, their duration causing a delay in the project's implementation.

The equipment delivered to Ukraine was both dual-use and non dual-use. Dual-use products are those products and technologies that usually have civilian use but, due to their characterstics, they can have military applicability. The classification of the products in dual-use and non-dual use is made by ANCEX, the national authority in the field of export controls, import and other military operations, following the consultancy requests made by the exporter of the products. Based on the operation type and the final destination, ANCEX states the need for obtaining an export-license for the dual-use products.

ANCEX also controls the way Romania fulfills the obligations and commitments assumed by the international treaties, agreements and arrangements in the above-mentioned domain and in accordance with the European Union legislation and treaties. It grants licenses for export, import, international transit, transshipment, brokering and technical assistance operations for military and dual-use items, as well as for operations performed without touching the physical territory of Romania.

Taking into consideration the above-mentioned statements, in order to grant the export licences, ANCEX *required end-user certificates for the dual-use equipments.* This document guarantees the fact that the delivery of the dual-use equipments is done only with the established purpose of the delivery, thus the equimpents will not be used with a military purpose.

- The alignment with EU Regulations

The Department for Export Controls of Romania also required that the Ukrainian part certifies the fact that the products delievered under the NATO-UKRAINE TF CD will not be re-exported to Crimeea and Sevastopol, according to the *Council Regulation (EU) No 692/2014 of 23 June 2014 concerning restrictions on the import into the Union of goods originating in Crimea or Sevastopol, in response to the illegal annexation of Crimea and Sevastopol.*

Conclusions

The first phase of NATO-UKRAINE TF CD put the basis for a solid Ukrainian National Cybersecurity System that can be further developed and extended according to the Ukrainian necessities and to the available funds. Starting from its concrete results, the Parties involved agreed to continue the enhancement of the Ukrainian strictly defensive cyber defence capabilities, focusing on securing more CIIs identified by Ukraine as priorities.

The technical project implemented in the first phase of NATO-UKRAINE TF CD has contributed in organizing Ukraine's cyber security field at a national level, being the basis for Ukraine's nationally integrated informational architecture, thus producing concrete results. In 2016 and in 2017 were adopted the Cyber Security Strategy of Ukraine and the Cyber Security Law of Ukraine. It also produced long term effects for the defence and cyber security of the Allies.

As an outcome, the first phase of NATO-UKRAINE TF CD provided a strong ground for the enhanced Ukrainian National Cybersecurity System mentioned above, as follows:

1. Provided an integrated system for cyber security and cyber defence (Incident Management Centers and Forensic Labs);

2. Provided cyber defence training and exercises;

3. Provided the framework to further develop Ukraine's cyber defence through national effort.

Cyber defence remains a critical area of focus in the modernization of Ukraine's security and defence sector. Significant progress has been made in this field. The lessons learned from the first phase of the NATO-UKRAINE TF CD will facilitate the processes of the second phase.

Way forward:

The threats comming from the cyber space are to be countered not only by enhancing cyber capabilities at national level, but also through international cooperation. The second phase of NATO-UKRAINE TF CD aims at further strenghtening Ukraine's stricly defensive cyber technical capabilities based on the scalable technical project proposed by Romania in 2014, when NATO launched the Trust Funds for Ukraine and which delivered concrete results providing Ukraine a strong ground for an enhanced National Cybersecurity System.

For the second phase of the project, we aim to:

- Keep the organizational format of NATO-UKRAINE TF CD: Romania (Lead-Nation)& RASIROM R.A. (Executing Agent);
- Raise new contributions to further develop the Ukraine's cyber security and defence strictly defensive capacities:

- Secure more CIIs according to the Ukrainian needs; the cost estimation for the second technical project depends on the number and architecture of the CIIs to be secured;
- Deliver training courses to the Ukrainian beneficiaries, according to the needs identified after handling the integrated system for cyber security and defence implemented in the first phase of NATO-UKRAINE TF CD.