Final evaluation

Combating Cyber Crime in Kosovo (C3K)

Prepared by: Krenar Loshi

August 2021

Project and Evaluation Information

PROJECT INFORMATION

Project/outcome title: Combating Cyber Crime in Kosovo (C3K)

Atlas ID: 00112987

Corporate outcome and output:
CDP Outcome 1: Rule of law systems and institutions are accessible to all and perform in a more effective and efficient way

Strategic Plan Outcome 2: Citizen expectations for voice, development, the rule of law and accountability are met by stronger systems of democratic governance

Country: Kosovo (UNSCR 1244)

Region: Western Balkans, ECIS

Date project document signed: 7 November 2018

Project dates Start/End: 1 October 2018 – 30 July 2021

Project budget: EUR 1,024,099.00

Project expenditure at the time of evaluation: Final project charges and contractual obligations are being settled

Funding source: The Norwegian Ministry of Foreign Affairs, represented by the Royal Norwegian Embassy in Pristina

Implementing party: UNDP Kosovo

EVALUATION INFORMATION

Evaluation type (project/ outcome/thematic/country programme, etc.): Project Evaluation

Final/midterm review/ other: Final Evaluation

Period under evaluation Start End: 1 October 2018 – 30 July 2021

Evaluator/s: Krenar Loshi

Evaluator email address: krenar.loshi@gmail.com

Evaluation dates Start/Completion: 8 July 2021 – 25 August 2021

Table of Contents

Project and Evaluation Information 2

List of Acronyms and Abbreviations 4

EXECUTIVE SUMMARY 5

1. INTRODUCTION 7

1.1 Background 7

1.2 Description of the intervention 8

1.3 Evaluation scope and purpose 9

1.4 Evaluation approach and methodology 9

1.5 Theory of Change 9

1.6 Key Challenges and Limitations 10

2. DATA ANALYSIS AND FINDINGS 10

2.1 Relevance 10

2.2 Efficiency 12

2.3 Effectiveness 13

2.4 Impact 19

2.5 Sustainability 19

2.6 Transversal Themes 20

3. CONCLUSIONS AND LESSONS LEARNED 21

4. RECOMMENDATIONS 22

ANNEXES 24

List of Acronyms and Abbreviations

AIS	Agency of Information Society
C3K	Combating Cyber Crime in Kosovo project
CCIS	Cyber Crime Investigation Section
CERT	Computer Emergency Response Teams
CII	Critical Information Infrastructure
CoE	Council of Europe
CSI	Crime Scene Investigation
CVAWG	Cyber Violence Against Women and Girls
DFU	Digital Forensics Unit
DITC	Department for Information Technology and Communications
EU	European Union
ISP	Internet Service Provider
KOSSAC	Kosovo Small Arms Control Initiative
KP	Kosovo Police
KSSP	Kosovo Safety and Security Programme
MEL	Monitoring, Evaluating and Learning
MIA	Ministry of Internal Affairs
NCCS	National Council on Cyber Security
NIS	Network and Information Security
RAEPC	Regulatory Authority of Electronic and Postal Communication
ToC	Theory of Change

EXECUTIVE SUMMARY

The UNDP Kosovo has commissioned the final evaluation of the Combating Cyber Crime in Kosovo (C3K) project, to take place during 8 – 30 July 2021, in order to assess the overall achievement of the C3K project at outcome and output levels covering the period from 2018 until the end of July 2021, and to elaborate on the lessons learned and recommendations.

The evaluation is carried out according to OECD DAC criteria in terms of its relevance, efficiency, effectiveness, impact and sustainability of the project, as well as coordination and collaboration with the government and other relevant stakeholders in Kosovo.

In terms of **relevance**, the evaluation identified the following key findings:
Adequacy: Interview results show that all stakeholder representatives consider the project relevant to their needs and priorities.
Alignment: The project supports the implementation of key national strategy, the Cyber Security Strategy 2016 – 2019, as part of National Strategy and Action Plan Against Organised Crime 2018 – 2022.
Adaptability: The project successfully adapted to the constantly changing environment due to frequent government changes and the effects of the Covid19 pandemic.
Future: There's a need for continued capacity development through specialized trainings, equipment and software, with special focus on prevention measures.

Key findings regarding **efficiency:**
Value for money: Interview results confirm that the project delivered high quality services, training, and support.
Internal coordination: The institutional leadership and coordination was not fully functional at all times, which improved over time to ensure coordinated implementation efforts.
External coordination: The external coordination with the relevant projects of other organisations was mainly carried by the project on its own, and successfully.

Key findings regarding **effectiveness:**
Design: The project was structured well around three outcome areas; containing outputs, baselines, indicators, targets, activities and results. All of these components were clear and adequately linked up.
Progress: The project is well on track to achieve its targets at output and outcome levels.
Monitoring, Evaluation and Learning: The project maintained a simple M&E mechanism, with the main purpose for production of the progress reports. Beside provision of expert advice, no surveys or studies were carried out by the project.

Key findings regarding **impact:**
Personal transformation: The interviews confirmed significant impact at a personal level.
Organisational transformation: Certified trainings and specialised equipment and software has enabled better organisational response to cybercrime investigations.
Societal transformation: An increased awareness in detecting and reporting cyber-attacks by the institutions and the population alike is confirmed by the KP.

Key findings regarding **sustainability**:
Processes: The processes enhanced by the project through provision of training, equipment and software are able to continue beyond project life, while further advancement of processes is dependent on continued donor funding due to lack of own resources.

Results: Results achieved at personal and organisational level are deemed to be fully sustainable, while the results at societal level require continuous funding.
Future outlook/exit strategy: The project is foreseen to continue with the next phase, which has the full institutional support, thus no exit strategy has been developed for this phase.

Several **conclusions** can be drawn from the findings, most importantly UNDP over the years through KOSSAC and KSSP programmes, and through C3K project has established a credible profile in the field of security and enjoys full trust from all institutional CERTs, which paves the way for future engagement with MIA and respective security institutions. The project as such, is on track to achieve the targets set forth in the logframe. The overwhelming majority of interviewees was of the opinion that the project team is very committed, professional, and supportive.

Despite difficult situation in 2020 due to Covd19 pandemic, the institutional partners speak favourably about their collaboration with the project and are fully satisfied how the project managed to adapt the activities on-line, while maintaining a high level of quality.

In terms of **lessons learned**, of particular importance are the following two: i) ensuring continuous close communication with all stakeholders is paramount in avoiding pitfalls due to frequent changes in the government or ministerial leadership; and ii) demand driven activities and joint design of such, ensures high degree of implementation, even at challenging times, as it has been during the Covid19 pandemic.

The main **recommendation** of the evaluation is for the next phase to focus more on cybersecurity capacity development and awareness raising activities, covering prevention and advocacy aspects, and policy making and coordination processes, build around MIA, as main lead partner. The technical aspects, related to specialised equipment, software and trainings (e.g. digital forensics) required for cybercrime investigation and prosecution ought to be covered only if necessary under a separate outcome or even a separate project of more technical – procurement centred nature.

Furthermore, the project could identify suitable local partner Experts, CSOs and Think Tanks and commission analysis and research papers which are very scarce, yet necessary to feed into the policy making processes in the field of cybersecurity. This also contributes to strengthening of non-government sector capacities in the field of cybersecurity and overall sustainability of results.

With regard to project implementation, the evaluation recommends to develop a comprehensive M&E mechanism to ensure quality analysis not only on progress reporting, but also in feeding into research, policy studies, and publications. If resources allow, also engage an additional staff covering Monitoring, Evaluation and Learning aspects of the project.

In fostering greater **gender equality and human rights**, and adherence to the principle of **'leaving no one behind**', the project tackles the growing phenomenon of cyber violence, which particularly affects women and children, by supporting i) the harmonization of the Budapest Convention with the Kosovo's draft Law on Cyber Security, and ii) 'Careful in Internet' campaign to increase human vigilance regarding cyber-attacks.

1. INTRODUCTION

The UNDP Kosovo has commissioned the final evaluation of the Combating Cyber Crime in Kosovo (C3K) project, in order to assess the overall achievement of the C3K project at outcome and output levels, and to elaborate on the lessons learned and recommendations for future improvements and interventions in preventing and deterring cybercrime.

The review was conducted during 8 – 30 July 2021. This report contains the findings, conclusions, as well as recommendations of the review.

The report is structured as follows: Chapter 1 describes the background and explains the purpose and scope of the review and the methods that were used. Chapter 2 discusses the findings on relevance, efficiency, effectiveness, impact, and sustainability. Chapter 3 and 4 contain the conclusions, lessons learned and recommendations. Supplementary information and data are included in the Annexes.

1.1 Background

Kosovo has the youngest population in Europe. Half of its 1.8 mil. population is under the age of 25. According to the government data, it is estimated that more than 65 percent of the population are younger than 30.[1]

The May 2021 Public Pulse poll of UNDP Kosovo highlights three most pressing issues that impact social well-being: unemployment (34.3%), poverty (19.3%) and corruption (9.3%), whereas unemployment, poverty and urban space problems were the top three concerns in December 2020. Compared to April 2020, corruption (23.5%) has dropped by 14.2 percentage points. Kosovo Serbs consider unemployment (16.7%), public and personal security (14.8%) and urban space problems (12.9%) as three most pressing issues, whereas for other Kosovo communities the biggest problem is unemployment (51.2%), followed by poverty (18.9%) and energy supply (11.4%).[2]

The on-going rapid expansion of ICT that has significantly contributed to advancing the global economy, also carries a significant risk for criminal activity through cybercrime, which knows no borders, and threatens citizens, businesses, governments and critical infrastructure, globally. The increasing reliance and dependency on ICT makes societies vulnerable to cybercrime committed through hacking of computer data and systems. Attacks against information infrastructure and Internet services now have the potential to harm society in new and critical ways.

To this end, in 2016, the EU adopted the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems (NIS) across the EU, whereby i) Member States must develop a NIS Strategy and designate the appropriate competent authority/ies to deal with the NIS matters at national level; ii) Member States are required to exchange information on good practices and incidents via CSIRT network and the co-operation network ; and iii) Operators of essential services are required to report incidents of significant impact at their national NIS competent authority.

Prior to this, in 2001, the Council of Europe adopted the Convention on Cybercrime (No. 185), known as the Budapest Convention, which is the first international treaty on crimes committed via the Internet and

[1] https://ask.rks-gov.net/en/add-news/vler%C3%ABsimi-i-popullsis%C3%AB-2018

[2] https://www.ks.undp.org/content/kosovo/en/home/library/democratic_governance/public-pulse-xx.html

other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.

In this context, in order to address cyber related risks, the Kosovo institutions in accordance with the EU NIS and the CoE Budapest Convention provisions, have drafted and approved National Cyber Security Strategy and Action Plan 2016 – 2019, which also constitutes the main pillar of the UNDP's Combating Cyber Crime in Kosovo (C3K) project in support to implementation of the strategy and enhancing the combat against cybercrime.

1.2 Description of the intervention

The Combating Cyber Crime in Kosovo (C3K) project, funded by the MFA of Norway for the period of 2018 – 2021 with a total budget of EUR 1,024,099.00, aims to support the government institutions in implementation of Cyber Security Strategy and enhance the combat against cybercrime through:

i) implementation of an outreach campaign aimed at the general population and at legal entities owning and managing critical infrastructure;

ii) provision of software and relevant professional training to the Computer Emergency Response Teams (CERT) in the Kosovo Police and Ministry of Internal Affairs (MoIA); and

iii) provision of capacity development in internet and darknet investigations.

The C3K project is designed around 3 main outcomes and outputs:

Outcome 1. Institutions and Critical Information Infrastructure (CII) have skills to successfully implement cybersecurity measures and immediately respond to potential threats.

> *Output 1.* Capacities of the institutions and legal entities involved in the management of selected Critical Information Infrastructure (CII) are developed.

Outcome 2. Kosovo Police, crime scene investigators, prosecutors and judges have the skills and resources to prevent, deter and convict cybercrime.

> *Output 2.* Initiate and implement training programmes for police officers, prosecutors and judges in the field of cybercrime prevention and investigation.

Outcome 3. General population and institutions are more resilient against cybercrime.

> *Output 3*. Increase the understanding and reporting of cyber incidents at both institutional and individual levels.

The expected overall results will contribute to:

1. Safe and secure network in the Kosovo Police (KP) and in the Ministry of Internal Affairs (MIA);
2. Capacity in the field of cybercrime investigations strengthened;
3. Awareness among the general population and legal entities increased and incidents faster reported;
4. Full implementation of the Convention on Cybercrime of the Council of Europe (CETS No.185), (known as the Budapest Convention) made possible.

1.3 Evaluation scope and purpose

The main purpose of this evaluation is to assess the overall achievement of the C3K project at outcome and output levels and elaborate on the lessons learned and recommendations for future improvements and interventions in preventing and deterring cybercrime. The evaluation is carried out according to OECD DAC criteria in terms of its relevance, efficiency, effectiveness, impact and sustainability of the project, as well as coordination and collaboration with the government and other relevant stakeholders in Kosovo.

Institutional scope: The evaluation focuses on the progress made with the key project stakeholders and beneficiaries in Kosovo, namely: Ministry of Internal Affairs (ICT Department), Kosovo Police (Cyber Crime Investigation Section, Digital Forensics Unit & ICT Directorate), Regulatory Authority of Electronic and Postal Communication, Agency of Information Society, Prosecutor's Office, Academy of Justice, representatives of civil society organizations, and implementing partners.

Geographical scope: Kosovo wide.

Time scope: The evaluation covers the project implementation period from 2018 until the end of July 2021.

1.4 Evaluation approach and methodology

The approach and methods for data collection and analysis were outlined in the Inception report, which was approved by UNDP on 21 July 2021. The evaluation was overall implemented as planned. The methods are briefly described in the following:

Document review: C3K documents and reports (Annex 3), including Project Document and progress reports and other documents, including strategic and policy documents, were reviewed for answers to the evaluation questions but also to contextualise the findings, conclusions, and recommendations.

Inception report: An Inception report was drafted based on the preliminary briefing conclusions and desk review findings, containing appropriate methodology to be applied during the final evaluation, as well as the work plan and technical instruments to be used during the course of the assignment.

Interviews: 15 qualitative, semi-structured interviews with the project and institutional stakeholders were carried out, including with civil society initiative bugHunters from Mitrovica (Annex 2).

Validation: Two debriefings on preliminary findings were carried out with the project team and the UNDP senior management respectively – as well as the review of the draft evaluation report provided opportunities for feedback through a dedicated feedback form, containing both comments and evaluation responses.

Reporting: The evaluation report follows the structure outlined in the evaluation ToR and reflects the feedback from the debriefing on preliminary results and from report draft versions.

1.5 Theory of Change

The evaluation will aim to reconstruct the logic of the C3K project interventions and trace its evolution and practical implementation on the ground. The reconstructed intervention logic of the project will allow contrasting of the observed results against the original plans and identify possible shortcomings and gaps at each level of the intervention, revealing possible flaws or shortcomings in achieving desired results. Furthermore, the evaluation will aim to collect evidence of what has changed (outcomes) and then, working backwards, determine whether and how an intervention has contributed to these changes.

1.6 Key Challenges and Limitations

The project maintained a very simplistic M&E framework and results reporting (Annex 4c), mainly desribing the activities implemented and number of participants where applicable, In addittion, at the time of the evaluation, the project had yet not drafted the 2020-21 progress report, which posed another challenge in this regard in terms of collecting activity and results inforation. Furthermore, the evaluation was not able to either access further internal data on cybercrime from the Kosovo Police due to secrecy of the data, but had no negative impact on the evaluation. As such no credible M&E data was available to allow for more comprehensive quantitative analysis, thus analysis are more of a qualitative nature, based on interviews with the main stakeholders.

Nevertheless, the evaluation managed to develop a template (Annex 4b) for essential data gathering and was able to collect all the basic/necessary data needed from the project team to allow for successful completion of the evaluation.

2. DATA ANALYSIS AND FINDINGS

This chapter provides the findings to the evaluation questions (EQ) as presented in the Evaluation Matrix (Annex 1), which was developed during the inception phase based on the evaluation questions that the UNDP formulated in the ToR for the evaluation, pertaining: Relevance, Efficiency, Effectiveness, Impact and Sustainability of the project.

2.1 Relevance

The relevance chapter assesses to what extent the project aligns with the needs and priorities of the target groups as well as the extent to which the project's theory of change is realistic and reasonable. The chapter responds to EQ 1.1 – 1.4.

Key finding EQ 1.1 (Adequacy): Interview results show that all stakeholder representatives consider the project relevant to their needs and priorities.

Key finding EQ 1.2 (Alignment): The project supports the implementation of key national strategy on cybersecurity, the Cyber Security Strategy 2016 – 2019, as part of National Strategy and Action Plan Against Organised Crime 2018 – 2022.

Key finding EQ 1.3 (Adaptability): The project successfully adapted to the constantly changing environment due to frequent government changes and the effects of the Covid19 pandemic.

Key finding EQ 1.4 (Future): There's a need for continued capacity development through specialized trainings, equipment and software, with special focus on prevention measures.

The project's objective to support the government institutions in implementation of Kosovo Cyber Security Strategy 2016 – 2019 and enhance the combat against cybercrime, continues to be relevant for the citizens and institutions alike. The interviews with stakeholders confirmed that the project was highly relevant to the situational context and addressed the immediate challenges and demands of the targeted beneficiaries.

The project outputs were developed as a bottom up approach whereby all relevant institutions were involved in designing their outputs, which were combined into outcomes and results of the project. MIA as a lead entity insisted on additional activities, which were added at a later stage in full agreement with Norway, the donor.

The selection of the targeted beneficiaries was also adequate and encompassed all the key cybersecurity institutions, namely MIA DICT, KP's DICT, CCIS and DFU, REAPC and AIS. The project also engaged with the Prosecutor's Office, Academy of Justice and relevant CSOs.

The project is aligned well with Kosovo's national strategies, UNDP's strategy, SDG goals and EU strategies, as illustrated in the table 1 below.

Table 1: C3K alignment to stakeholder goals and strategies

National Strategies	UNDP Kosovo Strategy	SDG/EU
Cyber Security Strategy 2016 – 2019 National Strategy and Action Plan Against Organised Crime 2018 – 2022	Contributing Outcome (UNDAF/CPD, RPD or GPD): Outcome 1.1: Rule of law systems and institutions are accessible to all and perform in a more effective and efficient way Strategic Plan Output Linkage: 2.2. Citizen expectations for voice, development, the rule of law and accountability are met by stronger systems of democratic governance	Goal 16: Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels Target 16.4: By 2030, significantly reduce illicit financial and arms flows, strengthen the recovery and return of stolen assets and combat all forms of organized crime EU NIS Convention CoE Budapest Convention on Cyber Crime

The project successfully adapted the training activities to be carried out online during the Covid19 pandemic, and in addition managed to increase the number of participants as a result of savings by not needing to cover accommodation and travel related costs.

Furthermore, the project successfully navigated through the frequent government changes (3 different changes of the government occurred during the project lifetime), which had affected the functionality of the National Council on Cyber Security, which is traditionally chaired by the MIA Deputy Minister. It did so, by maintaining effective communication and following up on the needs and concerns of each stakeholder separately, at times when the Council was not fully functional.

There's clear understanding and commitment by the institutional stakeholders on the need for continued capacity development through specialized trainings, equipment and software, which are in line with the project purpose. Nevertheless, MIA as lead partner, expresses that that there's a need for more focus on cybersecurity preparedness rather than on consequences i.e. cybercrime investigations. In this regard it highlights aspects of policy and strategy making, institutional coordination and citizen awareness as key focus areas and priorities.

2.2 Efficiency

In this chapter, the evaluation assesses the extent to which the project made good use of its human and financial resources as well as the adequacy of the Project Team structure and internal/external coordination mechanisms. The chapter responds to EQ 2.1 – 2.3.

Key finding EQ 2.1 (Value for money): Interview results confirm that the project delivered high quality services, training, and support.

Key finding EQ 2.2 (Internal coordination): The institutional leadership and coordination was not fully functional at all times due to frequent government changes, which improved over time as a result of project's coherent communication and information sharing.

Key finding EQ 2.3 (External coordination): The external coordination with the relevant projects of other organisations was mainly carried by the project on its own, and successfully.

The project is on track to utilise the entire budget. The project was delivered by a minimal team of three professional staff, consisting of a Project Manager, a Project Officer, and a Project Associate, all apportioned with other projects under KSSP umbrella. External expertise was engaged on needs basis in assessing and developing complex procurement ToRs. Interview results confirm that the project delivered high quality services, training, and support.

The fact that the project team was based in the MIA premises was instrumental in its successful implementation. This meant, for example, that project staff were able to rigorously monitor activities and work side by side with authorities and staff, which greatly increased the quality of the outputs and the local ownership.

Another important aspect that facilitated the smooth implementation of the project was that the project team had already worked with the relevant institutions as part of the UNDP's KSSP programme and as such had an established credibility amongst the stakeholders, ensuring effective communication and information sharing between the project stakeholders, resulting in high quality services, training, and support.

UNDP added value

The investment of the C3K project would not have gone so far without the experience, reputation, and trust of UNDP in Kosovo in the project area.

UNDP Kosovo has vast experience in the security area through KOSSAC and KSSP programmes, which allowed C3K project to work with a solid network based on trust acquired after years of work with MIA and Kosovo Police, in particular.

The institutional leadership and coordination was not fully functional at all times due to frequent government changes, which improved over time as a result of project's coherent communication and information sharing. The project had adopted the existing coordination mechanism for the implementation of the UNDP's Kosovo Safety and Security Programme (KSSP) under the leadership of MIA, which was implemented through the National Council on Cyber Security (NCCS) chaired by the MIA Deputy Minister, but due to frequent changes of governments (3 different government coalitions during the project lifetime) coordination proved to be challenging at the beginning, but was significantly improved over time through meetings of the UNDP senior management with MIA leadership, and the follow-up by the new project manager.

The project largely made own efforts in coordinating with other organizations, through meetings and sharing of information to avoid any duplication with activities of the relevant projects implemented by the U.S. Embassy/ICITAP programme, EU in Kosovo and OSCE Mission in Kosovo/Community Safety programme. The KP organised a coordination meeting with all relevant donor projects, to share information on planned activities. In some instances, where there was a need for equipment, which could not be provided by the project, other projects/donors were invited to step in, allowing to complete the infrastructure needed. Norway also financed an OSCE project in KP and ensured it was implemented in coordination with UNDP.

2.3 Effectiveness

This chapter assesses the effectiveness, the project progress reports were used, supplemented with findings from the interviews and further document review. The chapter responds to EQ 3.1 – 3.3.

Key finding EQ 3.1 (Design): The project was structured well around three outcome areas, containing outputs, baselines, indicators, targets, activities and results. All of these components were clear and adequately linked up.

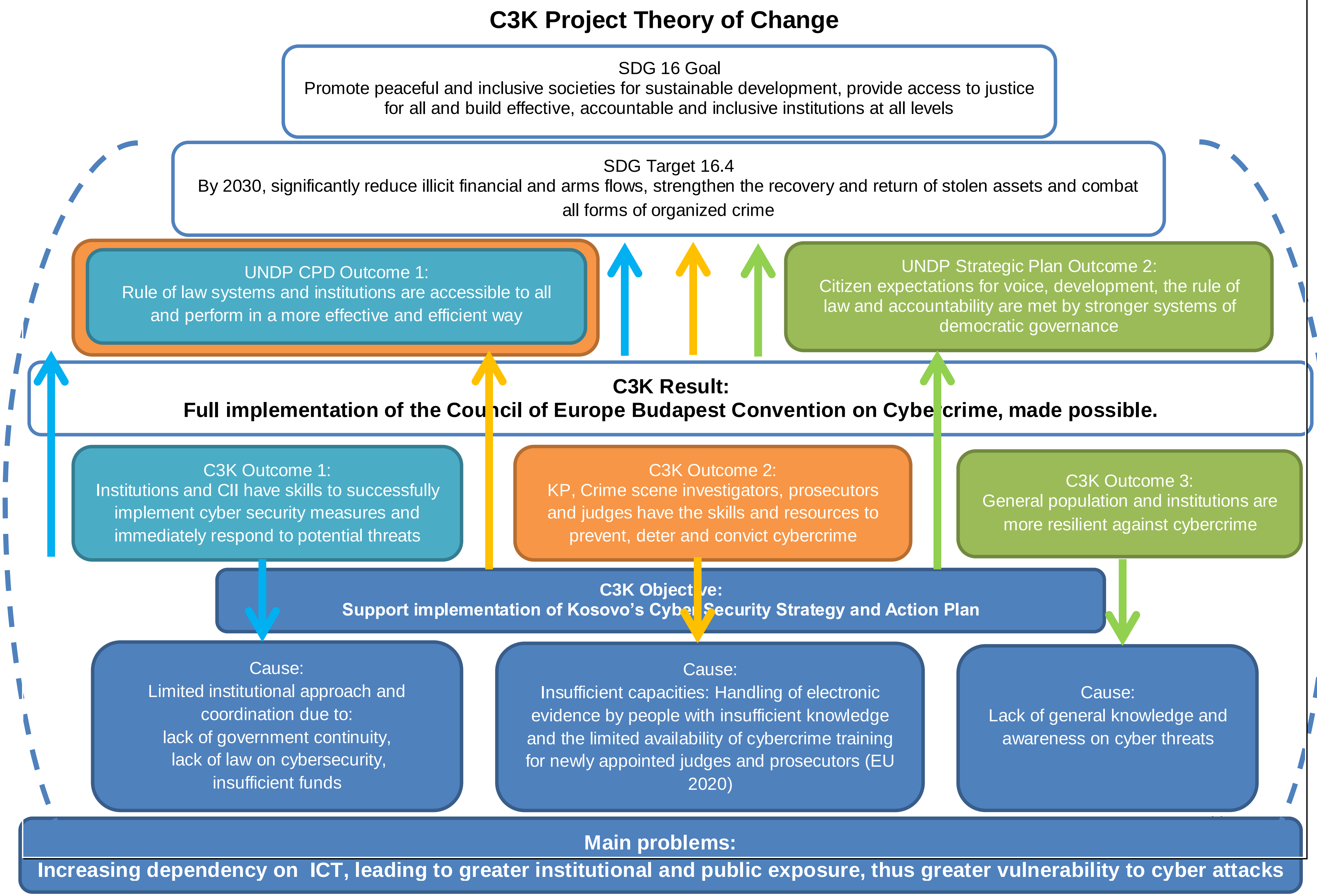
Key finding EQ 3.2 (Progress): The project is well on track to achieve its targets at output and outcome levels.

Key finding EQ 3.3 (MEL): The project maintained a simple M&E mechanism, with the main purpose for production of the progress reports. Beside provision of expert advice, no surveys or studies were carried out by the project.

The C3K project has its own defined ToC and related results, outcomes and outputs, which are well interlinked and realistic. The project outputs were developed based on a demand driven approach, whereby all relevant institutions were involved in designing their outputs, which were then combined into outcomes and results.

The project has a coherent Logical Framework and Theory of Change assumptions that explain the sequence of the change being pursued. The evaluation has reconstructed the Theory of Change to reflect the underlying problems and causes, and how the project is addressing them in the context of UNDP strategic outcomes and SDGs. The reconstructed ToC is presented in the chart 1 below.

Chart 1: C3K project reconstructed Theory of Change



C3K Project Theory of Change

SDG 16 Goal
Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels

SDG Target 16.4
By 2030, significantly reduce illicit financial and arms flows, strengthen the recovery and return of stolen assets and combat all forms of organized crime

UNDP CPD Outcome 1:
Rule of law systems and institutions are accessible to all and perform in a more effective and efficient way

UNDP Strategic Plan Outcome 2:
Citizen expectations for voice, development, the rule of law and accountability are met by stronger systems of democratic governance

C3K Result:
Full implementation of the Council of Europe Budapest Convention on Cybercrime, made possible.

C3K Outcome 1:
Institutions and CII have skills to successfully implement cyber security measures and immediately respond to potential threats

C3K Outcome 2:
KP, Crime scene investigators, prosecutors and judges have the skills and resources to prevent, deter and convict cybercrime

C3K Outcome 3:
General population and institutions are more resilient against cybercrime

C3K Objective:
Support implementation of Kosovo's Cyber Security Strategy and Action Plan

Cause:
Limited institutional approach and coordination due to:
lack of government continuity,
lack of law on cybersecurity,
insufficient funds

Cause:
Insufficient capacities: Handling of electronic evidence by people with insufficient knowledge and the limited availability of cybercrime training for newly appointed judges and prosecutors (EU 2020)

Cause:
Lack of general knowledge and awareness on cyber threats

Main problems:
Increasing dependency on ICT, leading to greater institutional and public exposure, thus greater vulnerability to cyber attacks

The reconstructed ToC implies that the increasing dependency on ICT, leads to greater institutional and public exposure and vulnerability to cyber-attacks (main problem), caused by i) lack of general knowledge and awareness on cyber threats; ii) limited institutional approach, policies and coordination on cybersecurity and iii) insufficient capacities in handling of electronic evidence, limited availability of cybercrime training for newly appointed judges and prosecutors (EU 2020).

In addressing the problem and its causes, the project intends to Support implementation of Kosovo's Cyber Security Strategy and Action Plan (objective), through ensuring that Institutions and CII have skills to successfully implement cyber security measures and immediately respond to potential threats (outcome 1); that KP, Crime scene investigators, prosecutors and judges have the skills and resources to prevent, deter and convict cybercrime (outcome 2); and that General population and institutions are more resilient against cybercrime (outcome 3). In doing so, the project aims that full implementation of the Budapest Convention on Cybercrime of the Council of Europe (CETS No.185), is made possible (result).

The C3K project contributes to achievement of UNDP's CPD Outcome 1: Rule of law systems and institutions are accessible to all and perform in a more effective and efficient way and Strategic Plan Outcome 2: Citizen expectations for voice, development, the rule of law and accountability are met by stronger systems of democratic governance, contributing further to the achievement of the SDG Goal 16/Target 16.4: By 2030, significantly reduce illicit financial and arms flows, strengthen the recovery and return of stolen assets and combat all forms of organized crime.

Progress made

Overall, the interviews reiterated the quality of the projects services and associate several results directly with the project. Interviews indicate that there have been improvements with regard to preparedness, skills and know-how in preventing cyber-attacks across CERT's (in MIA, KP, RAEPC, AIS), through professional trainings, equipment and software, and increased general public awareness on the safer use of internet and reporting. The project provided a range of policy related outputs, including contributions to draft law on cybersecurity, which is considered an absolute necessity and has the potential to have positive effects in addressing the leadership and inter-institutional coordination in the field of cybersecurity.

In tracking the progress made, the project maintained a simple M&E mechanism, with the main purpose for production of the progress reports. Beside provision of expert advice, no surveys or studies were carried out by the project.

In this section the evaluation analyses the progress the project has made compared to what was planned under each outcome.

Outcome 1 expected result: Institutions and Critical Information Infrastructure (CII) have skills to successfully implement cyber security measures and immediately respond to potential threats		
Output 1.1 expected result: Capacities of the institutions and legal entities involved in the management of identified Critical Information Infrastructure (CII) are developed		
Output Indicator	**Output Target**	**Evaluation assessment**
1. Number of officials of reached and informed about	1.1. Officials of at least 10 institutions informed about cyber security related issues	**Achieved:** The project was implemented in close cooperation and coordination with the Ministry of Internal Affairs (DICT), Kosovo Police (DICT, CIIS and DFU), REAPC, AIS, Prosecutor's Office and Academy of Justice. The officials

cyber security related issues.		interviewed overall state that they have gained substantial knowledge through the trainings provided.
	1.2. Systematic reporting of security breaches and audits implemented in 10 institutions	**Partially achieved:** Regarding the implementation of Information security audits in selected institutions, the project is currently finalizing procurement of software and two licenses to monitor and audit critical infrastructure and active directory of the Agency for Information Society (AIS). AIS is responsible to maintain a safe government network that supports 800 government buildings and 15,000 number of users. This procurement will enable AIS to audit and monitor all systems, equipment, traffic and applications in its ICT infrastructure, thus enable the project to fully complete the activities planned under outcome 1.

Outcome 2 expected result: Kosovo Police, Crime scene investigators and investigators, prosecutors and judges have the skills and resources to prevent, deter and convict cybercrime		
Output 2.1 expected result: Initiate and implement training programmes for police officers, prosecutors and judges in the field of cybercrime prevention and investigation		
Output Indicator	**Output Target**	**Evaluation assessment**
1. Increased capacity of CSI in KP	1.1. 2 representatives trained and certified in CSI	**Over achieved:** The project provided the planned certified trainings for the 2 representatives within the KP's CCIS and 2 officers in the KP's DFU on the use of the digital forensics toolkit, and as such increased the potential for professional support to investigators and prosecutors on cyber related crime. In addition, a total of KP 11 personnel were trained in Crime Scene Investigations (CSI). All 4 KP CCIS and DFU representatives interviewed unanimously stated that the advanced high quality of trainings provided has enabled them to increase the personal and organisational effectiveness in crime scene investigations.
2. Toolkit on digital forensic delivered	2.1. Toolkit on digital forensic delivered	**Achieved:** The toolkit on digital forensics was delivered as planned to KP DFU and certified trainings on the use of the equipment provided to 2 KP DFU officers. The 2 DFU officers interviewed both stated that the toolkit provided enables them to access more advanced digital devices confiscated, which previously was not possible.
3. Capacity increased in internet investigations in KP	3.1. Representatives of 7 police regions and HQ trained in internet investigations	**Over achieved:** The project provided specialised certified trainings to 118 KP personnel at the HQ level and across regions in the field of Internet Investigations including Darknet. The 2 KP CCIS representatives interviewed confirmed that they already receive better quality reports on internet investigations

4. Capacity increased in darknet investigations in KP	4.1. Representatives of 7 police regions and HQ trained in darknet investigations	from the field, but also state that this type of training should expand in the future, covering more officers and more advanced modules. Furthermore, the project procured and delivered the SPLUNK software, in accordance with the KP specifications. which enables the Kosovo Police to monitor, search, analyze, visualize and interact with large amounts of data and ability to monitor all information systems in real-time and in integrated approach, a function which Kosovo Police did not previously possess. This has increased the detection capabilities and optimized security operations through faster responses, leading to increased security of law enforcement apparatus in Kosovo. A total of 15 Kosovo Police personnel responsible to cybernetic security in the KP DITC benefitted from a specialized training on the use of Splunk.
N/A Output indicator missing	N/A Output target missing	**Not evaluable against the logframe due to lack of the indicator and target. Achieved as per plan of activities (section IV of prodoc):** Concerning capacity development activities for prosecutors and judges in the field of internet crime, the project delivered trainings to 120 judges and prosecutors in gaining the necessary knowledge to better recognize cyber incidents and build skills that will lead to more evidence collection, intelligence gathering and investigative leads. Nevertheless, the judiciary still operates with no specific law on cybersecurity, having to draw judgements from the Penal Code and other existing laws, which often fall short due to lack of specific legal provisions needed. This area is expected to improve significantly once the draft Law on Cyber Security is adopted.

Outcome 3 expected result: General population and institutions are more resilient against cybercrime		
Output 3.1 expected result: Increase the understanding and reporting of cyber incidents at both institutional and individual levels		
Output Indicator	**Output Target**	**Evaluation assessment**
1. Human vigilance of general population increased and reporting increased with 25%	1.1. Knowledge about internet safety increased with 30%	**Not evaluable against the logframe due to lack of data. Achieved as per plan of activities (section IV of prodoc):** Regarding the awareness raising activities in support of the Ministry of Internal Affairs to increase human vigilance regarding cyber-attacks, the project supported a series of outreach campaign activities, including documentaries, debates, videos and promotion materials, which according to campaign implementer’s report (koperativa, 28 June 2021) was ‘quite successful’. MIA DICT representative interviewed also confirmed the usefulness and the positive impact of the campaign on citizens, which needs to be intensified further in the future, to also include real time cyber-attack stimulations and scenarios, thus providing more practical insights into

		cybercrime prevention needs for the non-governmental organisations, businesses and citizens alike. Furthermore, as part of the awareness raising activities, the project organised the Kosovo Cyber Challenge in the frame of the *Careful on the Internet* campaign, which aims to increase knowledge of cyber threats and empowering Kosovo's general public to navigate safer online. The challenge was won by the bugHunters – group of students from Mitrovica. The 2 bugHunters representatives also confirmed the need for much more competitions of this type and opportunity to participate in real time cyber-attack stimulations as it is the norm in developed countries, which contributes to greater motivation of young ICT students to specialise in the field of cybersecurity. Lastly, the project organised a virtual conference on Combating Cybercrime: Risks, Challenges and Legal Response, held on 21st October 2020, where experts and law enforcement officials were able to share insights on cybercrime investigation and emergency response. The cybersecurity conference was organised in support to Kosovo's upcoming strategic orientation to enhancing cybersecurity and ensuring the security of society. The MIA representative interviewed praised the quality of experts involved and discussions, but it failed to generate wider interest of the public who participated in very low numbers, stating that in the future conferences of this kind should be left to institutions to organise.
2. Online reporting platform developed	2.1. Online platform on the RAEPC website and linked to KP and CERT in RAEPC and KP and MIA are adequately responding to this reporting.	**Achieved:** The project supported the development of the Incident Response and Threat Intelligence Platform as planned, which enabled the RAEPC/KOS-CERTs to carry out operational duties in dealing with security incidents that need to be detected, collected, analysed and flagged for further investigation to the Kosovo Police, ISPs and MIA. The RAEPC officer interviewed confirmed the project's immense contribution, as the best support so far in enabling the full functionalization of the National KOS-CERT through provision of the platform software and training, stating that KOS-CERT is now one step ahead in detecting cybercrime before it happens, thus ensuring greater safety of critical infrastructure.

In addition to the planned activities, at the request of the NCCS, the project in close cooperation with MIA organised a study visit to the National Centre for Cyber Security in Norway, where the NACCS members had the opportunity to gain insights about the mandate and functioning of the cybersecurity institutions in Norway. The visit contributed to discussions in shaping further the ideas on the envisaged Cyber Security Authority, expected to be established through the forthcoming Law on Cyber Security.

In response to the emerging challenges posed by the pandemic, although not part of the originally planned activities, the project also managed to contribute to improvement of the KP's conference capabilities at HQ level, through digitalisation of the conferencing platform and purchase of Zoom licences, which enabled the KP HQ to communicate and coordinate more effectively.

2.4 Impact

This chapter assesses the extent to which the project has (or has potential to) achieved impact at personal, organisational and societal levels. The chapter responds to EQ 4.1 – 4.3.

Key finding EQ 4.1 (Personal transformation): The interviews confirmed significant impact at a personal level.

Key finding EQ 4.2 (Organisational transformation): Certified trainings and specialised equipment and software has enabled better organisational response to cybercrime investigations.

Key finding EQ 4.3 (Societal transformation): An increased awareness in detecting and reporting cyber-attacks by the institutions and the population alike is confirmed by the KP.

The interviews confirmed significant impact at a personal level achieved through the highly specialised and certified trainings provided, enabling immediate use of knowledge and skills gained in performing daily tasks in an improved and advanced manner. This regards especially the KP's CCIS and DFU.

In addition to training, the supply of relevant specialised equipment and software has enabled better organisational response to cybercrime investigations by the KP's CCIS and DFU, and prevention preparedness by the AIS and RAEPC. The trained staffs, in most cases, as highlighted in the Effectiveness section, were able to make immediate use of the new knowledge and skills gains, which positively impacted the overall organisational performance.

At the societal level, an increased awareness in detecting and reporting cyber-attacks is confirmed by the KP. Although most of the reported cases relate to acquiring of personal data through manipulation, which is not considered a cybercrime by the KP, this is still a sign of increased population awareness on the dangers of personal data sharing over the internet. Besides the public, also institutions benefited from awareness and advocacy activities, which prompted greater initiative amongst staff of MIA in safeguarding passwords by making them more complex and not sharing with others – as confirmed by the KP DICT.

2.5 Sustainability

The sustainability chapter is based on the findings from the interviews and the document review, and it focuses on: continuity of institutional processes and results, and projects future outlook and exit strategy. The chapter responds to EQ 5.1 – 5.3.

Key finding EQ 5.1 (Processes): The processes enhanced by the project through provision of training, equipment and software are able to continue beyond project life, while further advancement of processes is dependent on continued donor funding due to lack of own resources.

Key finding EQ 5.2 (Results): Results achieved at personal and organisational level are deemed to be fully sustainable, while the results at societal level require continuous funding.

Key finding EQ 5.3 (Future outlook/exit strategy): The project is foreseen to continue with the next phase, which has the full institutional support, thus no exit strategy has been developed for this phase.

All institutional stakeholders stated that they're fully equipped to apply in practice the knowledge and skills gained through the project, and ensuring continuity of institutional processes installed regardless of the project life, while further advancement of processes is dependent on continued donor funding due to budget limitations for specialised trainings such as the ones provided by the project.

Whereas the results achieved at the personal and organisational level are deemed to be fully sustainable, results at the societal level require continuous funding as local CSO's and Think Tanks still lack specialisation and funding for large scale advocacy activities in the field of cybersecurity. Businesses alike are still at preliminary stages of understanding and preparedness on cybersecurity. Institutions, such as KP are able to provide in kind advocacy support through lectures and participating in CSO led campaigns, but not at sufficient level due to lack of staff and budget to support CSO campaigns.

The project during this phase functioned more as a pilot, in i) building the necessary knowledge of the needs and priorities of institutions in the area of cybersecurity; ii) establishing the credibility and trust amongst stakeholders through provision of demand based high quality products, and iii) forging partnerships with key institutions in preparation for future phase. As such there hasn't been an explicit exit strategy developed for this phase, as the project is foreseen to continue with the next phase, which now has the full institutional support.

2.6 Transversal Themes

The Council of Europe Budapest Convention on Cybercrime is the first international treaty on crimes committed via the internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It defines a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware).[3]

According to CoE, cyber-harassment is perhaps the broadest form of cyber violence and involves a persistent and repeated course of conduct targeted at a specific person that is designed to and that causes severe emotional distress and often the fear of physical harm. It is often targeted at women and girls and termed "cyber violence against women and girls" (CVAWG or Cyber VAWG), which among others involves: unwanted sexually explicit emails or other messages; offensive advances in social media and other platforms; threat of physical or sexual violence; hate speech - language that denigrates, insults, threatens or targets an individual based on her identity (gender) and/or other traits (such as sexual orientation or disability). Children on the other hand, seem to represent a primary group of victims of cyber violence, in particular with respect to online sexual violence.[4]

In fostering greater gender equality and human rights, and adherence to the principle of 'leaving no one behind'[5], the project tackles the growing phenomenon of cyber violence, which particularly affects women

[3] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[4] https://www.coe.int/en/web/cyberviolence/types-of-cyberviolence#Cyberharassment

[5] With the adoption of the 2030 Agenda for Sustainable Development, 193 United Nations Member States pledged to ensure "no one will be left behind" and to "endeavour to reach the furthest behind first."1 In practice, this means taking explicit action to end extreme poverty, curb inequalities, confront discrimination and fast-track progress for the furthest behind.

and children, as increased availability of internet access and the expansion of social media exposes them the most to cyber harassment.

In this regard, UNDP through the C3K project has lobbied in harmonization of the Budapest Convention with the Kosovo's draft Law on Cyber Security, which through the procedural powers and the provisions on international cooperation of the Convention on Cybercrime will help investigate cyber violence and secure electronic evidence. UNDP has lobbied that policy response should be formulated in recognition of the fact that gendered based violence in cyberspace is a form of VAWG and needs to be addressed as any other form of sexual or gender based violence. Furthermore, as part of the 'Careful in Internet' campaign in support of the Ministry of Internal Affairs to increase human vigilance regarding cyber-attacks, the project supported a series of outreach campaign activities, including documentaries, debates, videos and promotion materials, aiming to reach to teenagers in particular, through a variety of social media platforms.

3. CONCLUSIONS AND LESSONS LEARNED

Several conclusions can be drawn from the findings, of which these are deemed particularly important:

- UNDP over the years through KOSSAC and KSSP programmes, and through C3K project has established a credible profile in the field of security and enjoys full trust from all institutional CERTs, which paves the way for future engagement with MIA and respective security institutions.
- The project, specifically through the trainings, has contributed to improved performance of institutional CERTs, especially KP's CCIS and Digital DFU, and the RAEPC.
- The project is on track to achieve the targets set forth in the logframe. The overwhelming majority of interviewees was of the opinion that the project team is very committed, professional, and supportive.
- Generally, and despite a difficult situation in 2020 due to Covd19 pandemic, the institutional partners speak favourably about their collaboration with the project and are fully satisfied how the project managed to adapt the activities on-line, while maintaining a high level of quality.
- The forthcoming Law on Cyber Security is expected to add to the quality of the interventions and improve the institutional capacities for leadership and coordination.

In terms of lessons learned, of particular importance are the following two:

- Ensuring continuous close communication with all stakeholders is paramount in avoiding pitfalls due to frequent changes in the government or ministerial leadership.
- Demand driven activities and joint design of such, ensures high degree of implementation, even at challenging times, as it has been during the Covid19 pandemic.

4. RECOMMENDATIONS

Overall:

- Focus more on cybersecurity capacity development and awareness raising activities, covering prevention and advocacy aspects, and policy making and coordination processes, build around MIA, as main lead partner, in cooperation with KP, RAEPC and AIS.

- The technical aspects, related to specialised equipment, software and trainings (e.g. digital forensics) required for cybercrime investigation and prosecution, besides requiring significant resources, they are largely covered by other donors such as the U.S. and the EU programmes respectively, thus ought to be covered only if necessary under a separate outcome or even a separate project of more technical – procurement centred nature.

Strategic/Policy level:

- Focus on providing policy support to completion of the legal infrastructure and development of the new Strategy Cyber Security, through sponsoring relevant local surveys, analysis and research papers in the domain of cybersecurity.

- Identify suitable local partner Experts, CSOs and Think Tanks and commission analysis and research papers which are very scarce, yet necessary to feed into the policy making processes in the field of cybersecurity.This also contributes to strengthening of non-government sector capacities in the field of cybersecurity and overall sustainability of results.

Operational/Institutional level:

- The anticipated establishment of the Cyber Security Authority by the government, most probably under the MIA, is expected to lead and coordinate all cybersecurity efforts, and should be the centre of focus in terms of capacities to gather, analyse and disseminate information amongst relevant stakeholders.

- Further strengthen capacities of KP first responders in regional and local KP stations, in preliminary investigation techniques related to reported cybercrime, as this stage determines the effectiveness of later more advanced investigation stages.

- Ensure continuity of provision of specialised professional trainings and certification to CERTs in demand driven basis.

Societal/Advocacy level:

- Advocacy and awareness should be further enhanced, both in terms of protection from potential cyber threats, as well working with various local IT labs, to target more women to specialise on cybersecurity.

- Engage with MEST to strengthen awareness and advocacy actions targeting schools, pupils and students.

- Engage with institutions and businesses to open up and encourage ethical hacking activities in testing their cybercrime prevention capacities. Offer awards to successful hacks.

- Identify Champions of Change and support their engagement in TV debates, presentations, lectures, etc.

Project/Implementation level:

- Maintain demand driven approach to development of trainings, and where possible spread out trainings over time to provide more space for stakeholders to participate while being able to carry out their daily duties uninterrupted.

- Develop a comprehensive M&E mechanism to ensure quality analysis not only on progress reporting, but also in feeding into research, policy studies, papers and publications. If resources allow, engage an additional staff covering Monitoring, Evaluation and Learning aspects of the project.

ANNEXES

(Attached separately)