ISEC Programme 2013
Effective 24/7 PoC on Cybercrime

HOME/2013/ISEC/AG/INT/4000005180

‘Effective 24/7 Points of Contact for international cooperation on cybercrime and electronic evidence: promotion of good practice’

1st September 2014 to 31st August 2016

Project Report and Recommendations

Confidential

Partner

Associate Partners

Table of Contents

1. Introduction

The need for international cooperation in cybercrime and other criminal investigations into traditional crimes involving electronic evidence has increased at an exponential rate over past years. Traditional international cooperation treaties and practices were not created to deal with the fast response needed in order to preserve volatile data with often short lifespans, or to allow rapid cross border procedural investigative activities to take place. The capability to react rapidly to requests for assistance in these areas has been established over a number of years and separate networks have been created.

There are three acknowledged cybercrime 24/7 Point of Contact (PoC) regimes and these have all been in existence for a substantial time. The legal status of each of them is different, and they have different purposes. There have been limited attempts to evaluate the effectiveness of these networks, however, no in-depth studies, as conducted by this project have been conducted since 24/7 PoCs were introduced. There have been questionnaires, such as those informing the results of the 2009 Council of Europe study, and many "ping" tests to check if the network nodes are present to respond to requests.

This project not only investigated the efficiency and effectiveness of the 24/7 PoC regimes, but also examined their place in the overall capabilities for international cooperation and looked at identifying best practice for the future.

The results of this project will provide an informative base for all players in this field to consider as part of their future strategies and activities. This is a new approach in conducting in depth studies into the 24/7 networks and their relationships with each other as well as other component parts of the criminal justice/international cooperation system.

2. Background

The three acknowledged cybercrime 24/7 Point of Contact (PoC) regimes have all been in existence for a substantial time. Although there are three separate networks that appear on face value to be addressing the same need each has different aims, legal status and extent. The networks are managed by Interpol, the Council of Europe and the US Department of Justice (the latter on behalf of the group of eight nations (G8), now known as G7, following the suspension of Russia in 2014). A short overview of the networks follows.

Interpol

Interpol is an international organization that operates as a network of law enforcement agencies from different countries across the world. The organization, which has a global membership of 190 countries functions as an administrative liaison among the law enforcement agencies of the member countries, providing communications and database assistance. Interpol and member countries are able to communicate via an encrypted internet-based worldwide communications network known as 'I-24/7'. The network, which covers all aspects of Interpol's work and is not exclusively dedicated to

cybercrime and electronic evidence, offers constant access to Interpol's databases. The primary access to the network is through a National Central Bureau (NCB). Some countries have broadened the scope to include key areas such as airports and border access points. Member countries can also access each other's criminal databases via the I-24/7 system. At the General Assembly held in St Petersburg in October 2008, member countries approved a resolution to extend the availability of the 24/7 network to include national cybercrime units. The project was unable to identify any countries in which this expansion has occurred. 140 countries are listed in the Interpol cybercrime 24/7 Point of Contact list. Many countries have multiple contact points and many are not situated in cybercrime units. No analysis of this was conducted as part of this project, however the results of the case study exercises includes the requests made through this network.

Council of Europe

The Council of Europe Convention on Cybercrime (ETS185), also known as the Budapest Convention on Cybercrime or simply, the 'Budapest Convention', is the first international treaty seeking to address internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. There are currently 50 parties to the Convention (as of November 2016).

Article 35 of the Convention requires:

1. Each Party shall designate a point of contact available on a twenty-four hour, seven-day a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:
    a. The provision of technical advice;
    b. The preservation of data pursuant to Articles 29 and 30;
    c. The collection of evidence, the provision of legal information, and locating of suspects.

2.
    a. A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.
    b. If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis

3. Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

The CoE network is the only legally binding amongst the three examined as part of this project. Joining the network is a requirement of accession to the Budapest Convention.

“Group of Eight”

The background to the G8 network is that a meeting of the G8 Justice and Interior Ministers in December 1997 called for creation of a network as part of their action plan. Ministers called upon countries to:

- “Use our established network of knowledgeable personnel to ensure a timely, effective response to transnational high-tech cases and designate a point-of-contact who is available on a twenty four hour basis.”
- “Review our legal systems to ensure that they appropriately criminalize abuses of telecommunications and computer systems and promote the investigation of high-tech crimes.”
- “Continue to examine and develop workable solutions regarding: the preservation of evidence prior to the execution of a request for mutual assistance; transborder searches; and computer searches of data where the location of that data is unknown.”

The G8 24/7 Network was thus created as:

- A point to point network for urgent assistance in cybercrime matters
- A single point of contact (PoC)
- Available 24 hours per day, 7 days per week, with a stipulation that the PoC should be knowledgeable in cybercrime matters

The primary purpose of the Network is to preserve data for subsequent transfer through mutual legal assistance channels. This has been described in the past as a “fast freeze and a slow thaw.” The network is managed by the US Department of Justice through its Computer Crime and Intellectual Property Section (CCIPS). The network provides the following detailed description of the requirement.

In order to join the network, an applicant country must demonstrate that they have a contact point available 24/7. This means a person who can be reached 24 hours a day, 7 days a week, to receive information and/or requests for assistance from other countries within the Network. It is not necessary to establish a formal computer crime unit in order to join the network. In some jurisdictions, the contact point consists of a few investigators interested in cybercrime; in others, the contact point is part of a formal unit. In addition, some contact points are telecommunication centres that connect the caller to an appropriate official, while others are personnel with investigative and/or technical expertise. For example, one way to implement a contact point is to have four or five staff who are high-tech crime investigators on a rota system where each person is reachable outside normal working hours by a mobile phone which he or she keeps for one week out of every month.

There must be an English-speaking contact point. This is for reasons of practicality because the network is far simpler if there is a common language, and English is the most widely spoken language, particularly in relation to computing and the internet.

The person to whom calls are referred to should have a basic level of knowledge of computer crime, for example being able to understand what a "distributed denial of service" attack is, what the caller means when he or she asks for IP logs to be preserved, etc. Such knowledge can be gained in a basic computer crime course.

As a law enforcement cybercrime investigator, the person responding to the request should have an understanding of his or her authority to preserve or collect electronic evidence. In addition, he or she should know, or have the ability to quickly find out, what types of assistance to foreign countries are permitted by domestic laws.

The G8 24/7 points of contact are provided for investigations involving electronic evidence that require urgent assistance from foreign law enforcement. High-tech crimes raise new challenges for law enforcement. In investigations involving computer networks, it is often important for technically literate investigators to move at unprecedented speeds to preserve electronic data and locate suspects, often by asking Internet Service Providers to assist by preserving data. Therefore, to enhance and supplement, but not replace, traditional methods of obtaining assistance, the G8 has created the Network as a new mechanism to expedite contacts between Participating States or other autonomous law enforcement jurisdictions of a State.

To use this Network, law enforcement agents seeking assistance from a foreign Participant may contact the 24-hour point of contact in their own state or autonomous law enforcement jurisdiction, and this individual or entity will, if appropriate, contact his or her counterpart in the foreign Participant country. Participants in the Network have committed to make their best efforts to ensure that Internet Service Providers 'freeze' the information sought by a requesting Participant as quickly as possible. Participants have further committed to make their best efforts to produce information expeditiously. This is subject to the understanding that a requested Participant's legal, technical or resource considerations may affect the extent to which - and the time frame within which – the Participant may produce evidence, as well as the process of Mutual Legal Assistance, by which the requesting country seeks release of that information though the usual Mutual Legal Assistance Treaty (MLAT) agreement or Letters of Request procedure. The Network was deliberately designed with few rules and procedures to stimulate, rather than impede, cooperation.

3. Methodology

The project methodology followed a clear path to ensure the aims and objectives were met. Project management followed Prince 2 principles, and was overseen by the project director. Potential delays or other issues were mitigated through consultation with the partners and where necessary the EC project officer. Consultation with partners, international organisations, EU member states and other interested parties occurred throughout the project; however the ability of some organisations to participate in the planned activities was not possible, primarily through operational commitments, many of which related to the terrorist activities in France and Belgium. The project meeting activities at the both ends of the project were essential activities to consult with and take soundings from a wide range of relevant organisations. Both meetings were active

meetings that took advantage of facilitated workshops. The first meeting was a mixture of presentations on the subject matter and focused workshops to elicit information to enable the work of the project to succeed. Data collected from this meeting supported the development of the scenario-based case studies. Consultation on the case studies took place with partners, associate partners and the international organisations. It was intended that the study visit team would include members from the project team, partners and subject matter experts from EU Member States. EC3 and Eurojust were asked to attend these visits as observers in order to provide an element of independent evaluation. The initial plan to hold case studies over a period of days was moderated as a result of the reduction in budget during negotiations. This meant that a shorter period was available and this was divided between establishing the situation in each country and the case study exercise. Gathering support for the study visits from subject matter experts and EU organisations, was difficult and not possible to achieve. However, subject matter expertise was available within the project team and this compensated for the shortage of physical numbers. After the study visits, the data collected was collated and presented to international organisations responsible for 24/7 networks. The opportunity was taken to discuss the findings with Eurojust. EC3 was not able to facilitate a meeting with the project team due to the operational commitments referred to above. The findings and draft report were presented at the final meeting, where workshops considered the content and made recommendations for further action. This methodology was considered the most appropriate way of approaching this subject and in this case was successful.

4. Initial Meeting

The initial ('kick-off') meeting of the project was held in Canterbury (in the UK) from 13th to 16th January 2015. The agenda for the meeting is attached as **Appendix "A"**. A total of 26 delegates from 18 countries participated in the meeting, representing project beneficiaries, associate partners, international organisations and countries. The delegate list is attached as **Appendix "B"**. They were provided with presentations explaining the project and the existing 24/7 networks. In addition, the project team learned of the EMPACT project relating to the 24/7 requirements of the EU Cybersecurity Directive and the lead country, Croatia, was invited to send a representative, which they did. The project director, outlining the scope of the project; and each of the current network representatives, namely G8, Interpol and the Council of Europe on the current international cooperation situation, gave presentations. Additionally a presentation was provided, outlining the scope and activities of the EMPACT project. The meeting agreed that it would be sensible for both projects to cooperate with each other and to share information to avoid duplication.

The main activity of the workshop was a series of facilitated workshops, where delegates were asked to consider a wide range of subject related issues. The responses to the discussions were used by the project team to inform the development of the case scenario and as supporting information during the project. The questions posed to the delegates for the discussions are attached as **Appendix "C"**.

Some of the early findings of the initial activities of the project and reinforced by the meeting were:

- Choice of network depends on previous experiences, based on what worked in the past.
- In Europe alternatives to the three systems are often employed e.g. direct contact; the Europol secure communication channels (SIENA).
- Preservation of evidence (within 24 hours) generally works well but there are difficulties in the production of evidence (often takes too long).
- One disadvantage is that the same request (or at least the same 'case') can find itself in more than one network, leading to duplication of effort and confusion.
- Recruitment, selection, organisation and training of 24/7 PoCs varies significantly between countries.
- Guidelines on the use of 24/7 PoCs would be beneficial, to assist the selection of the relevant network for each request. It was also considered that guidelines indicate a competent PoC or organisation.
- Although in general terms the responses involving EU countries are acceptable, there are difficulties with Asian and African countries. Incoming requests from these regions often lack sufficient information.
- In terms of the pros and cons of multiple networks, some of the considerations were:
    - Pros – resilience, different capabilities of the networks, wider global coverage, flexibility and availability. More channels means more potential for contact. Smaller specialised units foster personal connections.
    - Cons – possible duplication with the same request being sent through multiple channels leading to duplication of effort and confusion about which network to use, inconsistent response, some lists are not updated, some countries have duplication of PoCs with some in the police and others in prosecutors' offices. Different obligations and standards for each network may make it difficult to satisfy all requirements.

5. Case Study

The desktop exercise was developed following (and including information) from the initial meeting. The case study sought to measure if a response was received to a request and also if the information requested was provided. An important consideration for the project team was to try and identify why one 24/7 network may be chosen as opposed to one of the others. This aspect was built into the scenario methodology.

The case study was developed to allow countries to consider a case from the beginning, i.e. the complaint by the victim; through to the making of requests via 24/7 PoC networks. The exercise was designed as a paper feed with details of the complaint requiring the host country to decide, firstly if a crime had been committed, what evidence is needed, where that evidence is located and finally how they would use the 24/7 networks in furtherance of the investigation.

The case involved a cybercrime in the form of a Denial of Service Attack and an extortion demand, so included a traditional crime element.

A full set of materials were prepared for the scenario, including a series of emails to and from the criminals to a victim company, a set of documents dealing with how and when the ransom would be made.

This was deliberately made complicated to allow the case study participants to identify the crimes committed, the type and location of the evidence that existed and what enquiries they would need to make to preserve and obtain the evidence.

As this activity developed it became clear that the use of urgent requests would not be appropriate for a number of reasons, not least of which was the increase in terrorist activity in Europe during the project and the correspondingly increased workload for law enforcement. It was therefore decided to use a non-urgent request that would still achieve the aims of the project in establishing the level of response and the content of the responses. The non-urgent request sought to establish policies in countries for the retention of video and CCTV footage held by banks in each jurisdiction. Each country visited were allocated specific target countries in the scenario, to which they would make requests.

6. Country Visits

Four country visits took place to Romania, Turkey, Portugal and Croatia and meetings were held with the entities considered relevant by the host countries and in agreement with the project team. Information gathering meetings were held and the responses to a circulated questionnaire gathered. The questionnaire is included in the documents included with this report at **Appendix "K'**. There was the opportunity for the project team to gather further information through conversation with the participants. This proved to be a very effective exercise. For the most part the national delegation consisted of the 24/7 contact points from the police and prosecution service in countries where they have a responsibility. In addition, at the meeting in Croatia, there were attendees from Slovenia as they were the co-lead country for the EMPACT project. Each country visited was introduced to the case study scenario in the same way, via an introduction and a paper feed which provided participants with sufficient information to establish if crimes had been committed in their country, the extent of any evidence they required and where that evidence was held. Once the country had selected the network or networks they planned to use, they were asked to send a non-urgent message to a total of 10 countries each. The cohort of countries to be tested therefore totalled 40 and included all EU Member States (except Romania, who were project partners and were fully aware of the exercise. They did of course participate as a requesting country). Outgoing and incoming messages were collated by the host country and passed to the project team for analysis. Following the country visits and analysis of the results of the activities,

further visits were made to the international organisations (G8, Interpol and the Council of Europe) to discuss the findings and examine how to improve the current system. An additional visit was made to Eurojust but one planned to EC3 proved not possible.

a. Romania

The case study visit to Romania took place between 22nd and 25th November 2015 and the visiting team were hosted by the Directorate for Investigating Organized Crime and Terrorism (DIICOT), which is the body that functions in the Prosecutor' Office attached to the High Court of Cassation and Justice.

Romania is a member of all three PoC networks subject of this study. In addition, as a Member State of the EU, it has access to the SIENA network, as well as the Southeast European Law Enforcement Center (SELEC) network.

According to Article 35 of the Budapest Convention by Article 62 of the Law no.161/2003 the Service for Preventing and Combating Cyber Criminality was established as a 24/7 PoC for cybercrime issues. In 2006 the 24/7 PoC was listed as a secondary point of contact in the G8 network. The primary 24/7 PoC in the G8 network is set in the General Inspectorate of the Romanian Police, Directorate for Combating Organized Crime, Service for Combating Cybercrime. In 2004 the Service for Preventing and Combating Cybercrime was incorporated in the Directorate for Investigating Organized Crime and Terrorism. DIICOT is the specialized body that functions in the Prosecutor' Office attached to the High Court of Cassation and Justice. There are a total of seven prosecutors, including the chief prosecutor who fulfils the 24/7 role. There is no specific training for the role, as it is listed as a regular activity.

In terms of requests for assistance received on an annual basis, there are no specific statistics or information on requesting countries, however the number is estimated as "no more than twenty". The main type of requests issued are for preservation of subscriber information and traffic data (subscriber information for IP addressed used in different communication, for email boxes, logs etc.) and requests for subscriber information or traffic data (logs) addressed to worldwide service providers. Some of the worldwide service providers may reply within one month. According to the law, the results of a preservation request can be released only under a mutual legal assistance request and therefore an average time cannot be reported.

Similarly with incoming requests, there are no official statistics, however it is estimated that between two and 15 requests are received each year. Most of these are data preservation requests originating in the USA. Preservation requests are dealt with immediately by a prosecutor's ordinance. The response received from the national service providers may vary from one hour up to two days. An automatic reply is sent to the requesting PoC to serve as a receipt, and if necessary a more consistent reply is send to inform about the procedure to be subsequently followed. It is considered that the resources in Romania to deal with this function are adequate and there are no specific difficulties reported.

The case study activity was conducted with representatives from the police and prosecutors' office. A short presentation giving an outline of the case was presented, followed by a paper feed exercise. The exercise was designed to answer the following questions:

- Do these circumstances constitute crimes in your countries?
- What evidence do you need to proceed?
- How do you propose to get the evidence?

The exercise identified ten countries in which evidence was available and the country team was asked to identify what enquiries they would make and then to actually make the enquiries through the network of choice. Romania used the CoE network where countries were party to the convention, followed by the G7 contact point. It is right to say that in most cases the CoE and G7 contact points are the same, however the legally binding nature of the CoE network is a key deciding influence.
Romania issued a request to each country in the following form:

This is a non emergency request based on art.35 of the Budapest Convention.
My unit is running an investigation regarding an intrusion and data theft, that fall under art.360 and art.364 of the Romanian penal code. Some fraudulent credit cards have been used in XXXXX and from the victim's bank we received the ATMs that have been used.
In order to prepare as soon as possible a mutual legal assistance request I need some answers from your side:
1. Is it common for an ATM at a bank location to have a camera surveillance?
2. If yes, how long are these images kept and who is generally responsible for these cameras?
3. Are there any specific rules according to your legislation in order to retrieve such images?
Thank you for your cooperation
Best,
XXXXXXXXX (Redacted)
24/7 Contact Point
Service for Preventing and Combating Cyber Criminality
Directorate for Investigating Organized Crime and Terrorism Offences
Prosecutor's Office attached to the High Court of Cassation and Justice.
www.diicot.ro
XXXXX (Redacted), Bucharest, Romania

Each request was issued to the country in question. Some replies were received while the project team were present and the results of those that were not were sent to the project team at a later date. In addition to the ATM information, the Romanian team also identified further enquiries that would be made as part of the investigation. These included a forensic examination of the victim server, based in Romania, either by consent or a court order. Further enquiries with a German ISP would be made, followed by a

formal Mutual Legal Assistance Treaty (MLAT) request as Germany does not have data retention. Further enquiries would be made with Panama, Canada and the USA. Where a country is not a member of the CoE list, the Romanian authorities would use the G7 list or refer to the police for contact with Interpol as they have the direct contact. These additional enquiries were not made as they were outside of the target activities of the project, however it was interesting to observe the knowledge based decisions made by the Romanian authorities. Another aspect of the Romanian procedures is that they often will not send a 24/7 request, but will send in the first instance an MLAT request, as they are fully aware that in order to actually receive the evidence they are seeking, an MLAT is required. This is possibly because of the close proximity and relationship with the MLAT-issuing department and potentially a good example for other countries to seek to emulate.

The request and response details are included as **Appendix "D"** with this report. In terms of results, Romania received responses from eight countries. When attempting to send the request to Poland, it was discovered that there was no Point of Contact details in the CoE list and therefore the message was not sent. Additionally, when reviewing the results, it was discovered that there was no evidence that the request to Denmark was in fact issued and therefore is excluded from the analysis. Romania received seven full responses from countries and all within a six day period from the issue of the requests. One EU country did not reply or even send an acknowledgement of the request.

In order that countries were informed that the requests made were part of this project, the following information was sent to the requested countries at the conclusion of the exercise activities, in other words once no further information was expected:

Thank you for your positive reply to our request sent on 24th November, for information about the situation in your country with regard to the presence and availability of surveillance camera images at bank ATMs. The request was made, as part of an EC funded project to assess how the current cybercrime 24/7 PoC networks could be further enhanced. The project is coordinated by Canterbury Christ Church University in the UK and Turkish National Police is an associate partner, along with The Council of Europe and Interpol. The Prosecutor's Office attached to the High Court of Cessation of Romania is a full partner to the project. The network managers have expressed support for the project activities and were informed in advance of this exercise. The project coordinators would like to thank you for your co-operation as it will provide valuable information for the project and its outcomes. More information about the project may be found at http://www.canterbury.ac.uk/social-and-applied-sciences/law-criminal-justice-and-computing/research-and-knowledge-exchange/centre-for-cyberforensics/247-points-of-contact.aspx where the details of the relevant contacts are also available. The information you have provided will also be of practical value to this office as we do have many investigations of this type.

b. Turkey

The case study visit to Turkey took place from 19th to 22nd January 2015 and was hosted by the Turkish National Police Cybercrime Department.

Turkey is a member of all three 24/7 networks that are the subject of this project activity. The Turkish National Police Cybercrime Department is the contact point for the G7 - 24/7 Network for High Tech Crime and the Budapest Cybercrime Convention 24/7 Network. The Turkish National Police Interpol Department is the Interpol I-24/7 Network contact point, as they are for the Europol office. Turkey is a strategic partner of Europol.

Facebook, Google and Microsoft enquiries are made directly to the companies. There are two members of staff allocated to the G7 and CoE networks. They receive the requests and pass to the investigation division in Ankara who in turn send requests to a regional investigative office, who undertake the investigations. In addition to English, the other languages supported are Russian and French. Staff in the cybercrime department are familiar with Turkish national cybercrime legislation and the Budapest Convention. There is no specific training on 24/7 networks for staff. It is recognised that having separate departments responsible for networks may lead to duplication of requests and the effort to respond to them.

In terms of received requests for assistance the numbers are quite low. Two requests were received by the cybercrime department in 2014 and nine requests in 2015. In addition, one request from Russia was received via Interpol. The main source of requests are the USA, Germany and France. The requests are for preservation of data. The cybercrime department issued one request in 2014 and six in 2015. There are no statistics before 2014 as the responsibility lay with the anti-smuggling department. It is considered that the staffing levels are sufficient to deal with all 24/7 requests.

The length of time to receive responses to requests depends on the service provider they ask to preserve the data. The Turkish National Police are discussing sending the information directly to the service provider to save time[1]. There is a concern that there is no law to force the data holders to preserve the data even if formally requested. The government is currently focusing on terrorist matters and a data protection law was due to be passed during the first quarter of 2016[2]. There is a requirement in Turkey for providers to keep all data for between 6 months and 2 years. It takes an average of three months to provide the information for an incoming request. All requests so far are G7, although it is considered that requests through Budapest would have more influence in Turkey, as it is a ratified convention.

The main types of request issued by Turkey are preservation and access blocking requests. In relation to blocking requests, Turkey does not receive responses. The law in Turkey is strict in relation to insults and this is not the case in many countries, so there is no reciprocity. In Turkey, prosecutors issue MLATs without necessarily referring to the police.

In terms of improvements it was reported that it would be better for incoming requests to come through Budapest Convention mechanisms. Procedures are very strict in Turkey so it is usual to receive signed and stamped documents. Currently all requests are

[1] This measure was introduced in early 2017

[2] The Data Protection law was enacted on 3 March 2016 and published in an official gazette on 7 April 2016

received by email, whereas Turkish procedure expects all requests should be by way of signed and stamped documents. It is also considered that domestic data preservation legislation would be beneficial.

For the case study exercise, the 24/7 contact points participated. The scenario used was identical to that in Romania, except for the dates and locations, and therefore to avoid duplication there is no copy of the materials used in Turkey in the project documents submitted.

Turkey identified the following crimes as having been committed:

- Article 243 – access to data processing system
- Article 136 – unlawful access to or acquisition of data
- Article 107 – blackmail

The preference for the order of enquiries is firstly to use the Budapest Convention as it is considered binding, then G7 and finally, Interpol. It is generally not possible to use Interpol in Turkey as it requires the creation of legal documents.

The message sent to each country is copied below:

Dear colleague,

This is a non-emergency request based on art.35 of the Budapest Convention/ G7 Point of Contact.

My unit is running an investigation regarding a computer intrusion and data theft, crimes that fall under art. 243, art. 136 and art 107 of the Turkish penal code.

*Some fraudulent credit cards have been used in **** and from the victim's bank we received the ATM locations that have been involved in your country.*

In order to prepare as soon as possible a mutual legal assistance request I need some answers from your side:

1. Is it common for an ATM at a bank location to have camera surveillance?
2. If yes, how long are these images kept and who is generally responsible for retaining the images from these cameras?
3. Are there any specific rules according to your legislation in order to retrieve such images?

Thank you for your cooperation

Best,
XXXXXX (Redacted)
Sergeant
National & International Relations
Turkish National Police Cybercrime Department

As with Romania, the hosts identified additional enquiries to the conducted, other than those which were the subject of the exercise, namely the requests for information about CCTV at banks in each country. The message was sent to each country at 1200hrs on 21st January. The address listed for Albania was invalid and a secondary Yahoo web mail account was listed. The request was also sent to that address. In total five requests were sent to the CoE list and the same number to the G7 list. As with Romania, some replies were received while the project team were present, and others after the event. In total Turkey received seven full replies. Three countries outside of the EU did not reply. The full list of countries and results is included in the supporting documents at **Appendix "E".**

c. Portugal

The visit to Portugal took place from 22nd to 25th February, 2015 and was hosted by the Polícia Judiciária.

Portugal is a member of each of the three networks subject of the project and in addition has nominated a point of contact in respect of the EU directive on attacks on information systems that is the subject of the EMPACT project referred to in this report.

The National 24/7 cybercrime network, created and set up in this police force (Polícia Judiciária) by legislative Act: Law 109/2009, 15SEP; is an international 24/7 PoC. During office hours it also receives national calls and is also the 24/7 for the EU directive on attacks on information systems.

In relation to Article 35 of the Budapest Convention, an article of the national law nominates the police force to be the PoC. The Portuguese cybercrime unit has a rotational system where one person is nominated as the PoC for seven days. For the 24/7 PoC of G7 there are three names listed. These are based on different expertise. They are not the same as listed for Article 35 purposes. There are a total of 24 officers who support the 24/7 facility for the CoE network and in relation to the EU directive.

The police international cooperation unit hosts the NCB for Interpol and Europol cabinet. They have their own rotation system and the general law covers their activities. The cybercrime unit has no direct access to Interpol communications. They have asked for direct access but still do not have it, although they have direct access to the child abuse database held by Interpol.

In terms of training, it is presupposed that the experience staff have with investigations is sufficient for the role, but a special course of "information security basics" is also provided. In terms of responsibility, the police are independent in safeguarding evidence. They have ten days maximum to report to the prosecutors, who 'own' the case. Preservation for the purposes of 24/7 PoC networks will be initiated by the police and then reported to the prosecutor. In relation to legislation and networks, training is given as a generic training course for inspectors on joining. Experts give input and there are refresher sessions for new legislative provisions. They are aware of the G7 courses but did not request or attend these but they do access courses developed by the European Cybercrime Training and Education Group (ECTEG).

In relation to incoming requests, for the CoE network, there are no statistics available; the 24/7 network receives as much as seven to ten contacts per year. The numbers are low because the rest of the traffic is undertaken via Europol SIENA messages; G7 requests mainly come from Asia. The process is the same and they receive three to five requests per year. Requests from EU countries, typically, come through the SIENA network. The CYBORG focal point and the TWINS focal point receive requests directly. One or two requests per day are received through SIENA for CYBORG. Portugal have requests coming via focal points and also from countries via SIENA. The major route is SIENA but there are no statistics on the number of requests received. The number of Interpol messages have decreased since the SIENA network was introduced and they can go months without any requests being received. (Indeed, there has not been a request via Interpol for last five years.) Portugal usually manages to provide an answer to incoming calls within eight hours. Requests from the US and Asian countries are considered to be the most problematic as they often lack information on the correct time and date zones of electronic communications, and also a lack of information about the reason for the need for the information and the identification of the crime under investigation.

One interesting aspect in Portugal is that although information received via 24/7 networks is for intelligence only (as in most countries) in Portugal they can use it as evidence. They still have a data retention law that requires retention for one year and it has not yet been overturned as a result of the European Court ruling on the subject.

For outgoing requests, most are issued to the US in respect of identification of user profiles of the main social networks and IP identification of Google services users. Identified issues relate to bullet proof hosting requests and corporate compliance policies that inadvertently provide information to targets that the police are asking for information about them; additionally, it is considered that US ISPs are now more difficult to deal with directly as they require court orders. The main concern for Portugal is the lack of response or the reliance on court orders by requested countries.

For the case study exercise, the head of the department for the 24/7 contact points participated. The scenario used was identical to that in Romania, except for the dates and locations, and therefore to avoid duplication there is no copy of the materials used in Portugal in the project documents submitted.

Portugal identified the following crimes as having been committed in the scenario:

- Extortion under Penal Code Article 223
- Illicit access under Penal Code Article 6
- Illicit access with access to personal data

Cybercrime is covered under the Cybercrime Law 109/2009 of 15th September 2009. Because the value of the crime is high, the potential sentence is increased. Because it is a serious crime of data theft they have to contact every customer who has had their data stolen to ask if they wish an investigation to take place.

There are three types of crime:

- Public, which the police can investigate without a complaint;
- Semi-public, which can only be investigated when there is a complaint. This can be withdrawn at any time;
- "Particular" crimes have to be reported and the victim pays a tax and has a lawyer. The victim can stop these investigations.

The crimes identified in the scenario are public crimes. There are various investigative measures that may be undertaken by the police. They can submit investigation papers to the prosecutors to invoke interception of communications and undercover operations under Articles 18 and 19 of the Cybercrime Law. In addition they can send an email and insert a mechanism to obtain the real email. For every message they receive from the offender, they are allowed to send a file with a hidden 'payload'.

The hosts noted that if this was real and in Europe they would use the SIENA communications network. In that way and if it is obtained in the requested country in a lawful manner it can be used as evidence without the need for any further procedure.

As with the previous case studies, Portugal identified other investigations they would conduct that fell outside the scope of the activity. These included making enquiries with the US Embassy legal attaché and directly to Google.

Portugal issued a similar email to the other project case study participants to the 10 countries identified in the scenario requesting information about the CCTVs at bank ATMs. The messages were all sent on 24th February 2015. In total, seven full replies were received in the period from 24th February to 14th March. An auto-response was received from one EU country with no follow up and no responses were received from two countries within the EU. There were no CoE or G7 contact details for two EU countries. The default position for the scenario would have been to use Interpol, however the project team were informed that as the countries are in Europe, the SIENA network would be used. Full replies were received using this network and they are included in the total number received, as detailed in the summary at **Appendix "F".**

d. Croatia

The study visit took place between the 7th and 9th of March 2015 and was hosted by the high tech crime unit, which is part of the Criminal Police Directorate of the Ministry of the Interior. In addition, representatives of the Slovenian authorities engaged in the EMPACT project dealing with *EMPACT Priority G "Cybercrime Attacks", in which the Strategic goal 5 was identified "to contribute to the establishment of a coordinated multidisciplinary mechanism for response in case of a serious cyber-attack with a cross-border dimension with well-defined roles, responsibilities and procedures."*

Croatia is a member of all three networks relating to this project. The high tech crime unit, part of the Criminal Police Directorate of the Ministry of the Interior are responsible for providing the 24/7 facility. Although they have access to the Interpol i24/7 network, this is only for child abuse cases and not for cybercrime. All Interpol cybercrime requests

are routed via the National Central Bureau. The unit does receive reports from the National Centre for Missing and Exploited Children (NECMEC) via Europol, whereas they used to come directly from Interpol Washington.

Six members of staff, the head of the unit, the child abuse online investigator and four other members of the unit provide the 24/7 facilities. There is no specific training for staff in the unit with regard to the 24/7 networks and they were not aware of the availability of the G7 training courses. Awareness of the existence of the 24/7 facilities is made through publications in official journals and all e-crime investigations come to the unit.

Once again the number of requests received is very low, averaging one per year. In 2013 there was one request, in 2014, no requests, in 2015 there were two requests and one request to date in 2016. These requests have been received from Japan, Bosnia Herzegovina, France and the UK and relate to requests for information on the user of IP addresses and log files. Some challenges are created because data retention is not regulated and it is not a legal term recognized by domestic laws or bylaws.

Where providers retain data, there is no procedural mechanism for preservation, so it is easier to pass on the data upon request. All incoming requests for data are forwarded to the operative technical centre, who in turn make direct contact with the ISPs.

In terms of outgoing requests, they are as follows; in 2011 there was one request, in 2012 there were three, in 2013 there were 23, two requests were made in 2014, and seven in 2015. Until the date of the visit, no requests have been issued in 2016. SIENA is used wherever the request involves EU countries. It is reported that the State Attorney's office is not keen to send MLATs. They have to be persuaded and it is very difficult for the reason is that Croatia currently has no cybercrime prosecutors. It was reported that they send requests to the Department of Justice (DoJ) in the US, they send them as CoE requests as they are legally binding; however the USA deals with them as requests to the G7 network.

Additional information was provided by Croatia in respect of the previously mentioned EMPACT project. They sent a survey to all EU Member States via Europol and Eurojust. Europol circulated the survey but Eurojust did not, so there were 20 replies from LE organisations but none from prosecutorial authorities. The results are included in the final EMPACT report.

For the visit, their Slovenian counterparts, who were their partners in the EMPACT project, joined the Croatian team. The Croatian team identified the following crimes from the case scenario:

- Unauthorised access under Article 266 of the Criminal Code
- Extortion under Article 243 of the Criminal Code
- Misuse of Devices under Article 272 of the Criminal Code

Croatia indicated that they would try to use the same network for the requests to the ten countries. In this instance the only network that each of the countries belonged to

is the Interpol 24/7 network, in order that each recipient is aware of the activity. They would seek permission from the National Central Bureau for the activity. Their normal method would be to write the request in Croatian and send it to Interpol for translation and transmission. They also identified other enquiries that would be made that fell outside the scope of the case study.

Ten messages were sent to the selected countries. The message is almost identical to the ones sent by the previous visited countries and is therefore not included in the report. The email address for Fiji was not valid and therefore the message was not sent. Out of the remaining requests, only two full answers were received, from France and Brazil. No responses were received from seven countries (including three EU nations). The Croatian team did say that in normal circumstances they would use the SIENA communications network for European countries. The results are attached at **Appendix "G".**

7. Post Visit Analysis of the Activities

The results of visits were reviewed and informed the final report and recommendations. The analysis of each country visit is appended to the project submission and may be summarised as follows. A total of 40 outgoing messages were required as part of the case study scenario. These included all 28 EU Member States (with the exception of Romania as they were a project partner and one of the visited countries). In addition further countries were chosen on geographical criteria and their membership of one of more of the 24/7 networks. There were some technical issues that led the project team to the conclusion that a small number of requests for information may not have been delivered and in order to avoid any confusion, there were ignored for statistical purposes. It was also noted that some of the recipient email addresses were web based addresses rather than official addresses. This leads to the potential that data included in the message may be stored in a third country that may or may not have adequate data protection legislation. One explanation provided for the use of such facilities is the unreliability of official law enforcement servers in some, mainly smaller countries that may mean 24/7 requests not being delivered and acted upon. There were clear variances in the level of response received through different networks. The network with the lowest level of positive response is that operated by Interpol. It is important to mention that the cybercrime list of Interpol is not the same as the National Central Bureau used to communicate through the i24/7 Interpol network. It is however a published network.

One of the challenges to the project team was that they were not given access to the Interpol or G7 lists of contact points, the former because the project team are not law enforcement and the latter because of the rules of the network, prohibiting circulation outside of the network itself. The project team wished to analyse the contact lists in order to try to establish commonality of contact points and any reason why one network may not perform as well as others. It would require further enquiries, if the contact points that did not respond were the same across the different networks. This analysis was not achievable.

8. Network Visits

a. Interpol

Since the inception of the project, Interpol moved its cybercrime capacity from Lyon to Singapore. This created an issue in relation to the funding as travelling to Singapore is significantly more expensive than Lyon. Permission was sought and obtained from the EC for one member of the project team to visit Interpol in Singapore.

Interpol has the largest membership of countries at one hundred and ninety. Secure communications are made through the secure i24/7 network. It is important to note that this network is available for all communications and not just for cybercrime and electronic evidence cases. The staff on this network are not cybercrime specialists. There is a 24/7 national cybercrime contact point directory and this is distributed through the National Central Bureaux (NCB) of member countries. Interpol considers that legal and technical harmonisation is essential to an effective 24/7 system. At present they are working with the US authorities to validate the identity of the requestor, in cases where the request is made directly to the service provider.

The results of the case study visits to countries was discussed and the low number of responses from the Interpol network was pointed out. At present there is no mechanism to deal with countries that do not respond to urgent requests and no sanctions are imposed. The case study visit results spread sheet was provided to Interpol. Unfortunately they were not able to send a representative to the final meeting of the project and no further information has been received from Interpol on the subject.

b. US Department of Justice (G8)

The visits to the US for the G7 network took place on different dates with the activities coordinator meeting with the Department of Justice (DOJ) on 9th May 2016 and the project director visiting the chair of the G7 group on 6th June 2016. The results of the activities were discussed and in particular the low number of requests dealt with by the project visit countries. The DOJ has received some 1,500 requests in the past year. We discussed during our visits to the DOJ the issue of the gap between the efficiency and effectiveness of the 24/7 networks against the perceived ineffectiveness of the mutual legal assistance mechanisms. The DOJ has conducted “ping” tests of their 24/7 PoC network and shared with the project team initial observations on the outcome of these tests. Finally, the DOJ clarified which nation states are part of the G7 network (this information remains confidential to the DOJ).

c. Council of Europe

The Council of Europe (CoE) network exists because of the requirement under Article 35 of the Budapest cybercrime convention for each party to the convention to provide the following:

1) Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance

for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a) the provision of technical advice;

b) the preservation of data pursuant to Articles 29 and 30;

c) the collection of evidence, the provision of legal information, and locating of suspects.

2) a) A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b) If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3) Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

The CoE network is the only one in which parties have a legal obligation to provide a 24/7 cybercrime and electronic evidence capability.

The CoE has been very proactive in its attempts to improve the efficiency of the network and conducts "ping" tests twice a year. There are currently fifty[3] countries that have acceded to the Budapest Convention, with invitations to accede issued to a number of countries. The CoE have also conducted a number of studies and research activities into international cooperation mechanisms of the Convention, including Article 35.

Currently, the 49 Parties to the Budapest Convention nominated 61 contact points with 12 Parties having established two contact points.

The T-CY Secretariat developed a Directory with the details of contact points for all the Parties to the Budapest Convention, and disseminated it to all the Parties, in order to be used for the purpose of article 35.

In order to contain accurate information, the Directory is up-dated on a regular basis by the T-CY Secretariat. Also, twice a year, the Secretariat is organising Ping tests as to verify if the contact points are functional and if the details contained in the directory are still valid.

Between 20 September 2016 and 23 September 2016, the T-CY Secretariat organised a ping test.

[3] Andorra became the 50th country to accede to the convention in November 2016 and therefore did not participate in the ping test conducted in September 2016.

Results:

- 59 contact points (97%) replied to the Ping test by email or phone;
- 16 contact points replied in less than 1 hour;
- 2 contact points did not reply;
- 8 contact points updated the information for their point of contact;
- Currently, the data in the Directory is updated for 60 points of contact.

In addition to the ping tests, the CoE has conducted studies of the efficiency of the networks and made recommendations in the broader context of the international cooperation mechanisms. Among the publications are:

1) A discussion paper on the effectiveness of international cooperation against cybercrime – examples of good practice, published on 12th March 2008
2) A discussion paper on the functioning of the 24/7 points of contact for cybercrime, published on 2nd April 2009
3) The European Committee on Crime Problems (CDPC) report on the summary of the replies to the questionnaire on Mutual Legal Assistance in Computer-Related Cases
4) The T-CY assessment report: the mutual legal assistance provisions of the Budapest Convention on Cybercrime published in December 2014
5) Rules on obtaining subscriber information, a report adopted by the T-CY at its 12th Plenary (2nd to 3rd December 2014)

a. Eurojust

The project team were accompanied by a representative of the project partner and met with two representatives from Eurojust. The organisation visited was provided with an explanation of the project and the purpose of the visit. Observations were made that where there is an MLAT in place, and Eurojust know the contact in country, the process is streamlined and works well. They gave the example of Switzerland, where the police the prosecutors are co-located, which enables close cooperation and a more speedy response. In cases where they are separate, close contact between police, prosecutors and investigative judges is needed. There are only five common law countries in Europe, so in most cases, prosecutors and judges are involved in the investigation process. It is acknowledged that the 24/7 process is often rapid and there is a need for a swift MLAT process in many countries. Eurojust considers it would be advantageous for there to be a clear definition of the role of the 24/7 contact points, and that a guidance note on Article 35 of the Budapest Convention may assist.

In ideal circumstances it is considered that a function for coordination at Eurojust would include Mutual Legal Assistance (MLA) requests within the EU. There is already an 'on call' phone network for prosecutors/judges, which would assist this process.

Among current initiatives is the creation of a network of prosecutors during the Netherlands EU presidency. This network is designed to exchange information concerning legislation, case law and available tools. There is also a plan to create a

cybercrime judicial network. Discussions have begun and there is movement towards something more formal; however this will not be an operational network.

b. Europol

This activity was included in the project plan and the team requested a meeting with EC3, in order to discuss the project, learn more about how the SIENA network is used in project relevant activities and to seek their views on the existing networks and improvements that could be made. EC3 was unable to accommodate the project team, primarily because of their commitments in relation to the on-going terrorist activities in Europe.

9. Closing Meeting

The final meeting of the project was held in Canterbury from 11th to 14th July 2016. Participants represented the coordinator, co-beneficiary, the associate partners, with the exception of Interpol, who were unable to send a delegate. In addition there was representation from Eurojust as well as EU Member States, many of whom had attended the initial meeting. Three academic members of staff from the School of Law, Criminal Justice and Computing at Canterbury Christ Church University acted as facilitators for the 'break out' discussion groups, at no additional financial cost to the project or Commission. The agenda of the meeting is attached at **Appendix "H".**

The delegates were provided with an update that outlined the following:

"The project has sought to analyse existing international cooperation mechanisms and initiatives, such as the G7 countries' 24/7 network, Interpol's I-24/7 system and the requirements of the Budapest Convention on Cybercrime, and seeks to identify the advantages and disadvantages of these and other initiatives. In addition the project has been working with those responsible for the implementation of the project resulting from the Operational Action Plan (OAP) of the EMPACT Priority G "Cybercrime Attacks", in which the Strategic goal 5 was identified "to contribute to the establishment of a coordinated multidisciplinary mechanism for response in case of a serious cyber-attack with a cross-border dimension with well-defined roles, responsibilities and procedures."

Amongst other activities, the project has undertaken study visits to four countries belonging to at least one of the current 24/7 networks to examine the systems and analyse the role and functioning of 24/7 Points of Contact (PoC) for criminal justice and international cooperation systems. The countries visited were Romania, Turkey, Portugal and Croatia, the latter being the leaders on the EMPACT project. The visits included a pre-vist questionnaire and meetings with those responsible for the 24/7 mechanisms in each country. The main acitivity of the visits was to use a case study to conduct a "soft test" of the networks based on the decisions of the host countries, as to which network they would use to make a non urgent request for information.

The primary project output will be a report on the role of 24/7 PoC (including relevance, efficiency and effectiveness) within the institutional framework for international cooperation on cybercrime and electronic evidence. It will include recommendations for

further improvements to criminal justice systems for international cybercrime investigations".

Presentations were given by the project director, the representative of the Council of Europe, the G7 network manager and the lead representative of the EMPACT project. The major activity was to discuss the project with the particpants and focussed workshops were held to achieve this.

The workshops considered the interim findings of the project and were asked to revisit the issues that were discussed at the initial meeting and provide any further information they consider relevant. The list of particpants is included at **Appendix "I".**

The workshops considered the advantages and disadvantages of the various networks and there now follows an analysis of some of the matters raised. It is imprtant to mention that advantages on the part of one view, may be seen as disadvantages on another view:

Interpol

Advantages

The Interpol network provides a secure and reliable communications platform with a link to 180 countries

Disadvantages

The staff in the i24/7 units are not knowledgable about cybercrime and electronic evidence and this is coupled with the suggestion that the 24/7 cybercrime list operated by Interpol (formerly known as the NCRP list), lacks credibility. Using the i24/7 network, while the communicaiton is immediate, the time taken to receive a response to the specific request may be too long.

G7

It is first noted that this network is specifically for data preservation requests.

Advantages

Speed of communications; the quality and credibility of contacts; the availability of the contact list.

Disadvantages

It is not legally binding and often needs an informal check before instituting a request, particularly in terms of ensuring the compatibility of crimes in the requesting and requested country.

Council of Europe

Advantages

It is a network of trusted countries that meet rule of law, democracy and human rights and is legally binding on the parties to the Budapest Convention. The directory of contacts is regularly checked and updated. It may be used for crimes that may not be cybercrimes but involve electronic evidence. Another advantage is that the procedural and international cooperation articles of the convention enable cooperation at an early stage in the investigation. The list of countries having a 24/7 PoC under the Budapest Convention is public.

Disadvantages

The network does not have a specific secure communications network.

SIENA

Advantages

A secure and stable network for EU Member States that my be used for intelligence in relation to cyber threats and data exchange.

Disadvantages

Access to the network is limited to nominated staff and it is not user friendly to those unfamiliar with its functioning.

It was also noted that there are other methods by which communication with international colleagues is undertaken. These include personal contacts, legal attaches at embassies and legal bilateral mechanisms.

The list of questions considered by the workshops is attached as **Appendix "J".**

Many comments were made about the continued practice of some countries using web based email accounts rather than official accounts to communicate, together with the associated concern that communications through such media is insecure and there is the potential for sensitive information to be passed to inappropriate persons.

One of the major concerns expressed is the lack of a timescale given for requests to be activated and responded to. Some countries simply do not reply. Even a reply that the request was not going to be acted upon would be beneficial. The total silence is not helpful and leaves countries hoping there will be a response in the future. Other countries acknowledge the request but give no idea of the timescale for the full response to be completed. Some automated responses leave the requesting country with information that there will be a response but no idea of timescale. There were some observations that a request template may be useful, with a suggestion that something similar the Council of Europe template for MLAT requests would help. Further suggestions include the potential for information about data retention periods for each country to be included in the contact lists. There was agreement on the importance of regular checks of the network, such as the ping tests conducted on the G7 and Council of Europe networks. The preferred method of communication is email as there is an audit trail and less opportunity for misunderstanding as compared to phone communication.

There was general agreement that it would be preferable for there to be one contact point irrespective of the network and an understanding that countries may choose different contacts. There was a general view that better training is needed for contact points, and that they should have a responsibility nationally to ensure that their availability is well known to investigators.

Following on from the discussions, the workshop participants agreed on the following recommendations from the meeting:

- Countries should always acknowledge a request and state what the action taken is/is going to be (even if this is going to be no further action (NFA). Also provide updates on the progress of the request.
- 24/7 networks should use a simple template to avoid mistakes and improve accuracy.
- Avoid duplication of channels for same request; make sure to use:
    - Interpol 24/7 or G7 lists for outside EU countries or countries not signatories to the Budapest Countries
    - CoE 24/7 lists for 'Budapest Convention' countries
- Professional experience cannot be sufficient for the 24/7 contact person: consider training on appropriate channels to use in each circumstance.
- Train personnel in cybercrime investigation basics and domestic/international law.
- Make sure the request is technically accurate and state where the situation is really urgent (triage criteria should be clear).
- Promote the networks domestically (within own country).

10. Project Conclusions

The conclusions of the project are detailed below:

- The CoE network should be used where possible as it is legally binding.
- Many PoCs are the same irrespective of the network.[4]
- Succession planning for PoCs is limited, with no documented strategy for succession.
- Induction training for new PoCs is almost non existent and relies on 'word of mouth'.[5]
- There appears to be a lack of clarity about the functions and potential support of each network.
- There is a lack of clarity about the use of the Interpol 24/7 cybercrime network as opposed to the i24/7 facility that supports secure communications.
- Networks are used much used less than expected, with most countries incoming and outgoing requests being in single figures nationally. The US DOJ received some 1500 requests alone in 2015, so it is apparent that the lack of clear statistics may be distorting the understanding of the actual use of the networks.
- There are too many occasions when requests are unanswered. This causes difficulties for the management of investigations. Countires are left in an uncertain position when no response is received, as they are unsure whether this is because of a technical problem with the receipt of the request, or because the request is still being considered by the national body concerned, or for other reasons (e.g. unwillingness to cooperate).
- There is too much "distance" between 24/7 and MLAT processes. In other words the 24/7 process is fairly efficient in preserving data, while the follow up MLAT process can take many months if not years to be concluded (usually by other government departments). In some instances it was established that MLATs are often not even issued.[6] The slowness of the MLAT process is one of the main obstacles to successfully obtaining evidence from abroad and requires immediate attention. The final meeting noted however, that the Council of Europe has been conducting activity regarding this aspect.

[4] The project was not given access to the G7 or Interpol lists, so does not know which countries are members. The CoE country list is public.

[5] The G7 network developed three training courses for PoCs. These could be useful for cross network training.

[6] Good practice in Romania often allows MLAT and 24/7 to be simultaneous processes.

11. Recommendations

Recommendations from the project include:

- Countries should recognise the importance of the 24/7 processes and to properly resource their facility and ensure that succession planning and induction training are introduced.

- The network operators should consider developing a joint induction manual to take account of expectations and functionality of each network and information about the appropriate network to be used in given circumstances. This should include the requirements of the EU directive.

- Countries, with the support of the network operators should utilise the G7 training courses, already developed, to improve the ability of PoCs to undertake routine uncomplicated investigations prior to allocation to other units.

- Network managers should consider introducing a requirement for countries to respond to requests within eight hours in order to enable requesting countries to manage their investigations. Responses should be made even if the request will be refused.

12. Appendices

Appendix "A"

Agenda for initial project meeting

Tuesday 13th January 2015		
Time	**Location**	**Session Title**
Various Times	TBA Hotel	Arrival of delegates, welcome, registrations and distribution of meeting documentation
Wednesday 14th January 2014		
Time	**Location**	**Session Title**
0900 - 0930	Auditorium	Welcome and Introduction to the project – Professor Robin Bryant
0930 - 1030	Auditorium	Overview of proposed project activities and objectives of the meeting Professor Robin Bryant
1030 - 1100	Cafeteria	Break
1100 - 1200	Auditorium	Presentation Interpol i24/7 Network - Redacted
1200 - 1300	Auditorium	Presentation CoE 24/7 Network - Redacted
1300 - 1400	Cafeteria	Lunch
1400 - 1500	Auditorium	Presentation G8 countries 24/7 network - Redacted
1500 - 1530	Cafeteria	Break
1530 - 1630	Auditorium	Delegate comments on presentations and experience of 24/7 networks
1630 - 1700	Auditorium	Introduction to and allocation of Delegates to workshops
1700		Meeting Closes

Thursday 15th January 2015		
Time	**Location**	**Session Title**
0900 - 1100	Breakout room	Breakout Group 1 to discuss the project and prepare feedback on specific questions and project objectives and activities
0900 - 1100	Breakout room	Breakout Group 2 to discuss the project and prepare feedback on specific questions and project objectives and activities
0900 - 1100	Breakout room	Breakout Group 3 to discuss the project and prepare feedback on specific questions and project objectives and activities
1100 - 1130	Cafeteria	Break
1130 - 1300	3 Breakout rooms	Continue breakout groups
1300 - 1400	Cafeteria	Lunch
1400 - 1500	3 Breakout rooms	Break out groups to finalise conclusions
1500 - 1530	Cafeteria	Coffee Break
1530 - 1700	Auditorium	Presentations by breakout group moderators to plenary
1700		Meeting Closes
1900	TBA Restaurant	End of Meeting dinner location in Canterbury
Friday 16th January 2015		
Time	**Location**	**Session Title**
0900 onwards	Auditorium	Conclusions, recommendations and presentation of the outcomes of the meeting and proposals to meet the project objectives. Feedback from delegates – Professor Robin Bryant
Various times during the day		Closure of meeting and departure of delegates

Appendix “B” (Redacted)

Initial Meeting Delegate List

Appendix "C"

Breakout Group Discussion

Primary Questions

1. What are the advantages/disadvantages of having multiple, cybercrime and electronic evidence, 24/7 PoCs

2. How should the current networks be utilised? e.g. should there be guidelines on which network is best suited to which request?

3. Why are alternatives to the 24/7 system (e.g. Europol, EC3, personal contacts, etc) sometimes used? What are their advantages/disadvantages?

4. Would clearer guidelines concerning direct requests made to companies and other non-law enforcement organisations e.g. Facebook, Google, Microsoft, etc., be useful?

5. Is training and equipping of 24/7 PoCs to the required level and standard? Is deep knowledge and skills in cybercrime investigation and national/international legislated required?

6. Are there any countries that consistently do not meet the expectations of other network members?

2nd Tier questions

1. How can duplication of the same request made to/by different PoC Networks be avoided?

2. How could the role of the Interpol Cyber Fusion Centre be further developed? For example, the dedicated portal? Is there a need for more than one portal?

3. How those countries with more than one national police force/organisation with cybercrime responsibilities, be supported, more effectively, by 24/7 networks?

4. How can the PoCs impact on the need for rapid MLA response in cybercrime and electronic evidence cases?

5. How widely should the identities of the PoCs be disseminated throughout a country?

Project level questions

1. Information is time critical. How can we reflect this truism in our 24/7 PoC capabilities?

2. How useful are the CoE guidelines and the annual, capability assessments of the Budapest Convention?

3. Would collection and sharing of statistics on the use of 24/7 networks lead to improvement in their capability?

4. Is it appropriate for any PoC networks to insist on a single language for communication between PoCs?

5. How can others have a voice in the development of 24/7 (e.g. in terms of privacy, human rights, authorisation levels etc.)

6. How far should the informal nature of some of the networks be maintained?

7. Can/should the requirements on membership of networks be enforced e.g. preservation of evidence?

8. Would it be helpful to agree a common set of guidelines for making requests across networks and keeping PoC lists up to date?

9. Is the overlap of personnel between networks an issue?

10. Should dual criminality be a requirement for all requests to PoCs?

11. What are the benefits of maintaining and expanding informal networks that are effective?

Appendix “D” (Redacted)

Case study Results from Romania

Appendix “E” (Redacted)

Case study Results from Turkey

Appendix “F” (Redacted)

Case study Results from Portugal

Appendix “G” (Redacted)

Case study Results from Croatia

Appendix "H"

Agenda for final project meeting

Monday 11th July 2016		
Time	**Location**	**Session Title**
Various Times		Arrival of delegates, registration and distribution of meeting documentation
????		Canterbury Cathedral
Tuesday 12th July 2016		
Time	**Location**	**Session Title**
0900 - 0930		Welcome and Introduction to the project – Professor Robin Bryant
0930 - 1100		Overview of project activities conducted and findings - Professor Robin Bryant
1100 - 1130	Cafeteria	Break
1130 – 1300		Update – Results of EMPACT project on improving operational national contact points (NCP) for exchange of information in accordance with Art. 13 of the Directive 2013/40/EU – Redacted - Croatia
1300 - 1415	Cafeteria	Lunch
1415 - 1500		Presentation on results of ping test of G7 Network – Redacted
1500 - 1545		Update Presentation Interpol i24/7 Network - Redacted
1545 - 1615	Cafeteria	Break
1615 - 1700		Update Presentation CoE 24/7 Network – Redacted
1700		End of meeting

Wednesday 13th July 2016		
Time	**Location**	**Session Title**
1000 - 1130		Breakout Group 1 to discuss the project and prepare feedback on specific questions and project activities and outputs
1000 - 1130		Breakout Group 2 to discuss the project and prepare feedback on specific questions and project activities and outputs
1130 - 1200	Cafeteria	Break
1200 - 1330		Continue breakout groups
1330 - 1430	Cafeteria	Lunch
1430 - 1530		Break out groups to finalise conclusions
1530 - 1600	Cafeteria	Coffee Break
1600 - 1700		Presentations by breakout group moderators to plenary
1700		Meeting Closes
1900	TBA	End of Meeting – Optional Social Event
Thursday 14th July 2016		
Time	**Location**	**Session Title**
0900 - 1100		Final Conclusions, recommendations and presentation of the outcomes of the meeting and plans for final report Feedback from delegates – Professor Robin Bryant
Various times during the day		Departure of delegates

Appendix “I” (Redacted)

Final Meeting Delegate list

Appendix "J"

Break-out group questions and tasks

*Please do not feel restricted by these questions. Remember the point of the exercise is to generate ideas and recommendations that will improve the functioning of the **"Cybercrime"** 24/7 PoC systems. Please also remember that the project relates to the 24/7 networks dealing with cybercrime and electronic evidence, not general crimes.*

1. Outline your experience of the 24/7 systems to other members of the break-out group.

   In terms of your own 24/7 PoC how does this operate? For example, is there a single PoC for all networks? Why is a particular network chosen? How many requests go through 'alternative' channels e.g. direct one-to-one requests? Why is this so?

2. Give some examples of good practice using 24/7 PoC networks.
3. Give some examples of problems encountered.
4. Are the criteria and mechanisms for joining a particular network clear?
5. Do we need to regularly test network integrity? What should happen in the event of failure?
6. Some countries lack the basic infrastructure for collecting and retaining electronic evidence. How can they be assisted?
7. The channel for making and receiving requests now seems predominantly by email rather than phone. Are then any problems envisaged with this?
8. Why do some countries appear to not respond to requests? Are all truly 24/7?
9. How can duplication of the same request made to/by different PoC networks be avoided?
10. How long should a record of a request be retained in the system?
11. Could/should requests be structured in a way that improves likelihood of prompt and comprehensive responses? E.g. inclusion of 'grounds for refusal'? Marking of requests as 'urgent', 'non-urgent' etc?
12. Should there be a requirement on countries PoCs in terms of time of response? E.g. 8 hours? In terms of confirmation that requests have been received? How to respond to clarifications requested? Should there be a requirement to maintain a log of requests?
13. How do you view the current forms of testing of a system? E.g. sending of test messages? Should there be penalties for failure to respond?
14. Are some methods better than others in keeping membership and contact details of 24/7 PoC networks up-to-date? What are they?

15. How well do the current methods for direct requests to ISPs and other private providers (such as Facebook) function? Would clearer guidelines concerning direct requests made to companies and other non-law enforcement organisations e.g. Facebook, Google, Microsoft, etc., be useful?
16. It seems to be generally agreed that user guidelines and greater clarity for which networks to utilise would be helpful. What should be the criteria for a) using a 24/7 PoC; b) for using a particular network? For example, in terms of a) should the criteria include urgency, seriousness (measured for example, in monetary value in the case of cyberfraud), requirement for 'dual criminality' etc? (Can you add to this list?)
17. Do your 24/7 PoCs receive any induction training to familiarise them with the various networks and their functions?
18. Is training and equipping of 24/7 PoCs to the required level and standard? Is deep knowledge and skills in cybercrime investigation and national/international legislated required?
19. Should training of 24/7 PoCs be the responsibility of the country or the network operators?
20. Does the likelihood of a successful MLAT, influence decisions to make 24/7 requests?
21. How well do the 24/7 PoC networks 'mesh' with the need in some cases for MLATs and Letters Rogatory?
22. How do we get prosecutors 'on board' at an early stage? And more generally, greater involvement from non-LEA interested parties?
23. Does Eurojust have a role in 24/7 requests to improve efficiency and effectiveness? If so, how would that work?
24. Would a closer relationship between Europol and Eurojust assist investigations?
25. Would integration of the various PoC networks into a single manageable list be an improvement on the current situation?

Overall:

If there was one improvement you were able to make to each of the 24/7 PoC networks what would it be?

Appendix “K”

Country Questionnaire
Which 24/7 cybercrime networks do you belong to?
Which organisation in your country is the 24/7 POC for the networks?
How many member of the 24/7 facility are there?
What training do staff receive for the role?
How many requests for assistance do you receive each year? (Are statistics available for the past 5 years)?
How many requests for assistance do you issue each year? (Are statistics available for the past 5 years)?
Which countries do you receive most requests from?
What types of requests do you receive?
Are there any received requests that cause particular difficulties?
Do you have sufficient resources to deal with the level of incoming requests?
What is the average “turn around” time for incoming requests?
Do requests from any particular countries cause more difficulties than others?
If, so please detail the issues
Which country do you issue most requests to?
What types of request do you issue?
Are your requests usually successful?
What is the average “turn around” time for outgoing requests?
What types of requests do you issue?
Are there any issued requests that cause particular difficulties?
Are there any countries that do not respond In the manner you would expect?
If so, please identify the issues

Any other comments