Report of the Strategic Meeting on Cybercrime

19-20 November 2014

Task Force on Cybercrime

07 April 2015

FINAL

Table of Contents

1. Introduction

On 19 and 20 November 2014, the strategic meeting on cybercrime titled '*Cybercrime - rising to the challenges of the 21st century*' was held at the Eurojust premises in The Hague.

More than 40 international judicial and police experts in the field of cybercrime participated, including representatives from the Council of Europe, Interpol, Europol's European Cybercrime Centre (EC3), the FBI, CEPOL, ENISA and EEAS, as well as Eurojust College members.

Based on identified obstacles in cybercrime investigations and prosecutions, it was decided to focus the strategic meeting on three main topics: admissibility of e-evidence, trans-border access to data and data retention.

Presentations were made on, the admissibility of e-evidence under Article 19 of the Budapest Convention, the consequences of the Belgian Yahoo judgement, the Dutch Illegal Trade on Online Marketplaces (ITOM) Project, and the complementarity of the roles of Eurojust and EC3.

In order to have highly interactive exchanges on these three main topics, which would provide the participants as well as Eurojust with a better view on the obstacles and good practices encountered in cybercrime investigations, a tailor-made virtual case study was developed, which served as a basis for the discussions in the parallel workshops.

2. Presentations

2.1. Transborder access to data - Budapest Convention on Cybercrime

Mr. Alexander Seger, Executive Secretary of the Cybercrime Convention Committee (T-CY) of the Council of Europe (CoE), gave a general introduction on the Budapest Convention (hereinafter 'the Convention') and the T-CY.

The functions of the T-CY were elaborated on. One of these functions is to assess the implementation of the Convention by the Parties. Via a questionnaire and Plenary discussions, the T-CY has made an assessment of the efficiency of some of the international cooperation provisions included in the Convention (Art. 31 and related Articles). Several recommendations are proposed by the T-CY in an assessment report, which would be discussed and possibly adopted in December 2014.[1] These recommendations can be divided in three categories: 1) recommendations falling under the responsibility of domestic authorities, such as the need to make use of all available channels for international cooperation; 2) recommendations falling under the responsibility of CoE capacity building programmes, such as online resource on MLA requirements and multi-language templates for Art. 31-type MLA requests; and 3) recommendations that may require an Additional Protocol, for example on joint investigations and JITs or direct cooperation between judicial authorities.

The T-CY also drafts guidance notes on how the current articles of the Convention can be used to combat cybercrime phenomena. In this context, the question of transborder access to data and jurisdiction has been analysed by the T-CY.

Article 19 of the Convention covers the search and seizure of stored computer data within a Party's territory. Article 32 addresses the situation where a Party, without the authorization of another Party, may access stored computer data if the data is publicly available or if the person

[1] Assessment report adopted during the T-CY Plenary meeting on 2-3 December 2014

who has the lawful authority to disclose the data consents to its disclosure. Art 32 does therefor not require the sending of a mutual legal assistance request.

The T-CY Working Group has produced a draft Guidance note on Art. 32. It gives guidance on the notion of 'access without the authorization of another Party', the applicable law, the person who can provide access or disclose data, the location of this person and the domestic lawful requests versus Art. 32b.

This Guidance note would be for consideration and possible adoption in the Plenary meeting of December 2014.[2] Considering that a new Protocol on transborder access is needed but not feasible in the current context, the T-CY would consider, in the same Plenary, the setting up of a working group on criminal justice access to evidence stored in the cloud, including through mutual legal assistance (following up to the T-CY assessment of MLA provisions).[3]

2.2. Territoriality in cyberspace and digital evidence gathering

Many debates have already been held on the concept of territoriality and location in cyberspace. In this context, a presentation was given by Mr. Jan Kerkhofs, Belgian Federal Magistrate and expert in cybercrime matters, on a Belgian Court case against Yahoo!, an Internet Service Provider (ISP).

The Belgian public prosecutor (PPO) was investigating a criminal organization which was committing crimes in Belgium, using a Yahoo-account. In order to receive subscriber information from Yahoo!, a production order was sent to the ISP, based on Art. 18 of the Convention, which states that '*each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order [...] a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control [...]*'.

The reasoning of the PPO throughout the whole court procedure was that Yahoo!, choosing to be commercially present in Belgium, providing territorial services and being contactable in Belgium should comply with a Belgian warrant issued to obtain basic subscriber information related to Belgian territorial communication. In November 2013, the Court of Appeal ruled that Yahoo! is indeed territorially present in Belgium and that it is a provider of an electronic communications service according to the Belgian Code of Criminal Procedure. The information has to be brought by Yahoo! and if Yahoo! does not want to collaborate, it can exclude the IP range for the Belgian territory. At this stage, the case is pending before the Court of Cassation for the final ruling.

Mr. Kerkhofs continued his presentation by arguing that it is of vital importance in cybercrime investigations to handle quickly in view of the volatility of digital evidence. In this context, the annulment on 8 April 2014 by the Court of Justice of the European Union of the Directive 2006/24/EC of 15 March 2006 on data retention which prescribed data retention for a minimum period of six months and a maximum of two years, has serious consequences in the Member States: some domestic legislations have been annulled and it varies from Member State to Member State which data retention periods are respected, if any.

Mr. Kerkhofs concluded by stating that there is a need for globalization of (cyber)justice, with broad competency rules and a redefining of the concept of territoriality. There should be less but more quickly executed MLA requests and it would be good to have a European or international standard MLA request template in matters of cybercrime.

[2] Guidance note on Article 32 adopted during the T-CY Plenary meeting on 2-3 December 2014
[3] Cloud evidence Group established during the T-CY Plenary meeting on 2-3 December 2014

2.3. ITOM Project - Illegal Trade on Online Marketplaces

Beginning 2014, the Dutch authorities initiated Project ITOM on 'Illegal Trade on Online Marketplaces', which is funded by the EU and will continue until the end of 2015. Eurojust is associated to the project. Mr. Jan Dobbelaar, Project Manager, presented the aim, scope and deliverables of the project.

Project ITOM aims to implement an integrated approach to tackle EU related illegal trade on anonymous marketplaces on the internet, by initiating coordinated interventions in close cooperation with (inter)national law enforcement agencies, judicial authorities, other public organisations, and the private sector within the EU.

Within the anonymous Tor network, websites are hosted which are online marketplaces where illegal goods are traded. Due to the complete anonymity of these websites and their users, it is very difficult for law enforcement authorities to combat this kind of crime. An important issue is the uncertainty in which jurisdiction a law enforcement authority is operating, which when mistaken could easily lead to legal and diplomatic issues. Project ITOM should demonstrate that a multidisciplinary, transnational, coordinated and collaborative approach is needed and crucial to combat the illegal trade on hidden online marketplaces effectively.

The activities of the Project will include the coordination of multidisciplinary interventions, supporting the cooperation between relevant authorities at EU level and eventually evaluate the work done to identify lessons learned. One of the final objectives of the Project is to establish a European cybercrime network of prosecutors on a permanent basis which could continue to share experience, knowledge and lessons learned.

2.4. Europol-Eurojust cooperation in cybercrime cases

A joint presentation was made by Eurojust and Europol on their cooperation, key competences and the joint support they can provide in the area of cybercrime.

The complementary roles in several areas of the two agencies were highlighted: conducting analysis (intelligence vs. judicial), expertise (forensic and investigative methods vs. lawful gathering of evidence), experience (operational cooperation vs. judicial coordination) and access to counterparts (cybercrime units vs. prosecution services). Both agencies can thus support the Member States by providing assistance in abovementioned areas throughout the whole process of investigation and prosecution.

As an illustration of how Eurojust and Europol can support Member States in cybercrime cases, the BlackShades case was presented. BlackShades is a malware which enables buyers to intrude, monitor and remotely access and control a victim's computer. The use of this malware was identified by the FBI, which sent the data to the respective EU Member States for further investigation. Both Europol and Eurojust were involved in the case at the end of 2013. Several coordination meetings were held during which encountered obstacles, legal issues and a common strategy were discussed. For example, the possibility to use information provided by the United States as evidence in the participating Member States was discussed. It was agreed that a common action would be held in all involved (16) countries in May 2014. A Eurojust coordination centre was set up during the action days, which facilitated judicial support for national authorities in their own language as well as real-time information exchange between the participants on for instance posts on hacking forums of targeted persons whom tried to inform others on the ongoing house searches/arrests. EC3 provided operational support by sending around the BS interview and search guide to law enforcement officers in the field. The actions resulted in 359 house searches, 97 arrests and seizures of more than 1100 data storage

devices. The early involvement of both Eurojust and Europol/EC3 proved to be important in order to ensure smooth coordination and efficient cooperation at European level.

3. Outcome of the virtual case

A virtual case scenario[4] was developed with a view to allowing the participants to interact and exchange views and knowledge on the subject of cybercrime, with a focus on admissibility of evidence, transborder access to data and data retention. This case scenario incorporated many elements which in cybercrime investigations often can or could cause difficulties or issues, especially given the inherent cross-border aspect and the different jurisdictions which come into play because of this. The case scenario therefore also focussed on identifying the differences in the use of investigative measures in the countries.

Admissibility of evidence: Considering that (initial) information on cybercrime related incidents often is provided by the private sector to the police at a stage where judicial authorities are in most cases not yet involved, there is a potential risk that this information, if used later on as evidence in court, may not be admissible. Moreover, evidence gathered following the use of particular investigative techniques in one country (e.g. sting operation) may not always be considered as being legally obtained and therefore admissible in court in another country.

Transborder access to data: In a virtual world it is difficult to apply the notion of 'location' in the same way as the physical notion of location as applied for other types of crime. In some cases, it is not even possible to identify the location where data is stored or from where a cyber-attack is being committed. Law enforcement and judicial authorities are therefore often confronted with unclear situations in relation to access to data. This in turn complicates MLA-procedures, which are often already considered as cumbersome and too slow, especially given the volatility of data and evidence online.

Data retention: The annulment of the Directive 2006/24/EC of 15 March 2006 on data retention which provided for some guarantees for law enforcement and judicial authorities in relation to the retention of data, has caused a void within the EU. It is currently up to the discretion and interpretation of each Member State how data retention is being dealt with, which obviously is detrimental for cybercrime investigations and can hinder European cooperation in this area as a whole.

In this chapter, a summary of the workshop discussions is presented grouped by topic.

3.1. Gathering and admissibility of evidence

Discussion revealed that there is a clear distinction between intelligence and evidence when information is obtained in the course of a sting operation. Normally, this information can always be used in the intelligence phase, in particular to start an investigation. Further information is then gathered via other means, e.g. house searches, in view of its admissibility in court. Some participants indicated that this information may also be used as evidence in their Member States provided that the court is satisfied that the information was obtained according to the law of the country where the information was gathered. In some Member States the evidence might be admitted in court but would not be relied upon for the final sentencing. Some countries indicated that it is possible to "validate" this information ex post via an official legal assistance request or a confirmation from the authorities which conducted the sting operation, that the information was obtained in accordance with their law. Furthermore, the workshop(s) revealed that there is a different understanding and confusion among

[4] See annex

practitioners of what provocation and/or entrapment means. Different approaches between civil law and continental law countries have been noted.

It was mentioned that the investigative possibilities of banks are more far reaching than those of law enforcement authorities in most countries. As a consequence, the use of this information gathered by banks differs from country to country. Some Member States cannot use the information if it is not obtained in accordance with the law, whereas others noted that the information can be used if it was obtained without the involvement or influence of law enforcement authorities. In some Member States, a complaint by a customer of the bank is needed before law enforcement authorities can initiate an investigation. Some Member States can receive the information but might not use it as evidence.

In relation to the use of gathered data as evidence in court, a distinction needs to be made between 'passive' information gathered (e.g. through observation) and information gathered actively (e.g. undercover operation); depending whether undercover operations are allowed in the concerned country, the latter type of information might or might not be admissible in court as evidence. It was also observed that some information, such as nicknames or information from anonymous sources, would not be admissible in itself in court. Other information would have to be presented along with it as evidence.

It was observed that Member States applying the opportunity principles are less inclined to start investigating mules if this is the only element operating in their country, unless it would allow getting to the criminal organisation. It was also mentioned that important information can be gathered by investigating mules. Some participants indicated that against the application of mitigating circumstances connected to their collaboration, mules tend to disclose important information on the network, procedures, links with other relevant actors, etc. It was observed that some Member States would split up the case (money laundering - cybercrime investigation), provided that in some countries a predicate offence is needed for money laundering.

3.2. Transborder access to data

Participants discussed various possibilities in connection with information to be retrieved from a Forum hosted on the web. The possibility to view and copy relevant information and seize the means from which the Forum was accessed were discussed.

A distinction can be made between countries where police would be able at the time of a house search, to view and copy information displayed on a Forum and seize the device(s), even without a prior warrant or approval from a judge or prosecutor. In these cases, an approval or warrant from a judge or prosecutor ex post would suffice. In other countries however, police would need a prior search warrant from a judge, which depending on the country may be formulated in a general way or needs to be very specific and detailed.

If relevant data is found to be stored on a server located in another country, some participants indicated that they would still access and copy the data, provided they get a warrant or court order from a judge. In some countries however, from the moment it becomes clear that the server is located in another country, article 32b of the Budapest Convention is applied, thus prior authorisation of the concerned country is needed and/or an MLA request would have to be sent. If prior authorisation is not possible, the authorisation is requested as soon as possible. If the location of the server is unknown and the data needs to be preserved urgently, some participants pointed out that national authorities investigating could in good faith proceed with the gathering of this information.

A distinction between stored static versus active data was made. It appears that the regime for active data, such as ongoing chat sessions, is quite similar to that of interception of telecommunications. For many, a court order is needed to gather this data.

3.3. Data retention

Participants are concerned about the impact of the European Court of Justice's annulment of the Directive on data retention, and on the negative impact on investigations and prosecutions especially when cross border elements are present. All participants stressed the importance of data retention.

In general, data retention periods vary considerably from 12 to 6 or 1 month, or even no retention period at all.

In some Member States the annulment has led to the suspension or abolishment of the national laws or provisions on data retention related to criminal investigations. As a consequence, there is no data retention obligation anymore and what is more, some ISPs and private sector companies refuse to release data, although it is available for commercial purposes and even if there is a court order, as they claim that they cannot be forced to cooperate. This might also affect other countries who ask for this data on the basis of an MLA request.

Other Member States are not (yet) affected by the invalidity of the data retention Directive because the national law has not been challenged, new legislation is already being prepared, the current criminal law provisions still allow obtaining the data available or the Directive was simply not implemented.

The need to strike a balance between data retention and fundamental rights (in particular the right to privacy) was highlighted.

Reference was made to a judgement of the ECHR (KU v. Finland) where the Court ruled that countries have the obligation to their citizens to do proper electronic investigations.

In the US, use is being made of data preservation instead of data retention. This was brought forward as a useful way to safeguard the data needed.

As the data retention periods vary greatly, it was suggested by several participants that Eurojust could make an overview of the data retention periods in the Member States. This information would be very useful in cybercrime cases.

3.4. Use of investigative methods

Next to the three main topics of the workshops, participants also discussed the use of different investigative methods and opportunities. From these discussions, it became very clear that the legal possibilities and restrictions in investigating and prosecuting cybercrime cases differ considerably within the EU.

The legislation in several Member States date back to a pre-computer time period and as such does not foresee and adequately address issues faced by judicial and law enforcement authorities in cybercrime cases.

Regarding access and search for information in e-mail accounts where credentials are known, some participants would proceed as it was a regular search, others would see it as interception of telecommunications and therefore would require a warrant from a judge (no need for consent by the person himself). One participant mentioned that it is not allowed in his country to log into the account if the credentials are known but the person does not consent to it; it is nonetheless allowed to break the encryption and access the computer. In one country, people can be required to provide passwords and logins, as they can receive a penalty if they do not comply. If credentials are not known (and if the server is located in a Member State), some said that in good faith and if there is a high risk that data is lost, a search could take place anyway. Other participants indicated that this would not be possible as e-mail accounts would be treated as private correspondence. A participant noted that in urgent cases, the prosecutor can issue a search order on the spot which then must be validated by a judge ex post.

In most countries, it is not allowed to use civilians (*in casu* the suspect) as undercover agent. Few countries do allow this, but under strict procedural requirements, only for a limited scope of serious offences and/or under certain conditions. In several countries it is however permitted to use a civilian as an informant, for instance to get a police officer introduced on a Forum. Some participants mentioned that it is allowed in their Member State to inject malware in the computer in order to get the full picture of the criminal activities. In this context, some concerns were raised though regarding the potential committing of offences by undercover agents/civilians in other jurisdictions.

Some participants confirmed that the police would take down the Forum or make it inaccessible, if possible. It was observed that in these cases, it would be advisable to inform other involved countries of the takedown. It was mentioned that the US government would not ask an Internet Service Provider (ISP) to take down a website as this is considered to go against the freedom of speech. This means that it is best for foreign authorities to ask ISPs directly to take down a website instead of requesting the assistance of the US government with this.

Participants highlighted the crucial importance of seeking direct contacts with competent national authorities in other involved States, in particular third countries. Direct contacts are crucial to "alert" the requested State about an incoming request for legal assistance so as to speed up its execution.

Regarding cooperation with companies (e.g. ISP) located in third States, it was highlighted that in general cooperation when a request for traffic data is made works well; some participants indicated that for this type of data a single entry point for EU Member States could be useful, and also that in some instances a letter from US authorities authorising cooperation with foreign authorities has been beneficial. No MLA request is required for this type of data. On the contrary, it was noted that when content data is at stake, cooperation becomes more difficult. In this case, it was pointed out that it can be useful to be very precise when requesting content data, and provide as much detail as possible, to use every channel available (e.g. Liaison Magistrates, Facebook law enforcement portal, etc.). On a general note it was mentioned that some Providers notify their customers when they are asked by the authorities to provide information. It would therefore be useful to ask Providers on beforehand if they notify their customers of such requests or not.

3.5. Role of EU and other bodies

When links to other Member States would appear, participants mentioned they would ask the police to set out the information to other law enforcement authorities in those Member States (police-to-police information). In parallel, the involvement of Eurojust would be beneficial, as the agency can assist and facilitate cooperation by advising on a number of issues such as the initiation of parallel investigations, transfer of proceedings, identifying which Member State is in the best position to prosecute or the avoidance of *ne bis in idem* problems at a later stage. In general, Eurojust's involvement at an early stage gives the best chance for a smooth cooperation and coordination of cybercrime investigations, which on the one hand may minimize the risk of encountering legal obstacles and on the other hand guarantees the resolution of such obstacles, if they occur.

Reference was made to Operation Onymous as a good example of the support Eurojust can provide to national authorities, particularly in cases of parallel investigations running in different Member States.

JITs were referred to as a very useful tool in cybercrime cases, especially if set up also at an early stage. JITs were considered useful when deciding on whether taking down a Forum, as authorities in other involved Member States might still need to gather evidence from the said Forum and the taking down would severely frustrate their investigations and/or prosecutions.

Europol and Interpol are particularly useful in assisting national authorities to build up the "intelligence picture". The role of FIUs and AROs should not be underestimated, in particular in connection with investigations and prosecutions of mules which could lead to asset recovery.

4. Conclusions

The strategic meeting was considered a big success. The informative presentations, the highly interactive workshops as well as the possibility participants had to liaise with experts from other countries were considered very useful. The following conclusions were presented at the end of the meeting:

- A clear distinction needs to be made between intelligence and evidence. In view of the admissibility of evidence in court, it is important to keep a trail of the evidence gathered. Especially when information comes from the private sector, it is essential to know how the data was gathered. Standards for collection of e-evidence, which is easy to modify and destroy, should be established.

- Participants of the meeting came to the conclusion that Member States' legislation is not adapted or adequate enough to investigate and tackle the cyber threats which we are faced with today. There is a need to redefine the concept of territoriality in cyberspace. The particular issues of loss of location and constantly new emerging modus operandi of cyber criminals are proof of the need to have adequate legislative frameworks in which law enforcement and judicial authorities can keep pace with this rapidly evolving crime type. New legal tools should be explored to fight cybercrime more effectively.

- The use of investigative methods in cybercrime cases differs considerably in the Member States. In multilateral cases, this can cause obstacles in the cooperation between countries and potentially lead to issues with the admissibility of evidence in court. What is more, it appeared from the workshops that in circumstances where authorities might access data stored in another country, the applicability of Article 32 of the Budapest Convention is not always straightforward. Indeed, often police and judicial authorities find themselves in a situation where on-the-spot they have to strike a balance between the preservation of important data or the consideration of the territoriality and jurisdictional rules. Also in relation to data retention rules and periods, there is a lot of disparity among the Member States. All of these differences may substantially hinder cross-border investigations and prosecutions.

- Eurojust should be involved at an early stage in cross-border cybercrime cases in order to facilitate cooperation and coordination of investigations. Early involvement would first of all build in a safeguard for the admissibility of the gathered evidence in court at a later stage. Furthermore, Eurojust can provide expertise and its involvement allows to avoid and overcome legal and judicial obstacles and to discuss a common strategy among countries, so as to decide commonly on a number of points: who will investigate which offences, which country is in the best position to prosecute, timing for the investigations/common action day, etc.
- The participants were of the opinion that it should be considered to set up a network for cybercrime prosecutors and judges, which would enable these experts to share expertise and knowledge, as well as exchange best practices through case examples of court decisions. Such a network would facilitate to overcome legal differences and issues. In this context, participants also expressed the wish to have this type of meeting on a regular (yearly) basis, so as to exchange views and experiences and maintain close contact with the practitioners in the Member States.

ANNEX: VIRTUAL CASE SCENARIO

PART 1

In the frame of an investigation related to large scale hacking activities towards banks, the FBI is monitoring a hacking forum by using undercover agents. Someone is selling data of hacked European and US bank accounts for further exploitation. The FBI did a sting operation and succeeded in buying data (account numbers with PIN and access codes) from different sellers.

Through the analysis of the data, the FBI identified two sellers: Tom Jones, who is already selling data for several years on the forum and Tina Smith, who is a new member on the forum. Both persons appear to be living in your country (A).

The FBI sent information to your police authorities on the affected bank account numbers in your country and the two sellers for further identification. Information was also sent to four other affected Member States (B, C, D, E), one of which (country B) has already started investigations.

Questions part 1:

- Can you accept and start an investigation on the basis of police information received?
- Is the information coming from the FBI admissible as evidence?
- If yes, for which offences could you start up an investigation and which inquiries would you undertake?
- As regards the sting operation, , would you be able to use the information obtained through the operation

PART 2

At the same time, one of the biggest banks in your country passes information on to the police that several of its customers have been the victim of hacking and that money has been transferred from their accounts to money mules in your country and other EU countries. The information was gathered actively by the bank's IT department, investigating the money transfers (IP addresses, bank account details etc.). One money mule in your country has been identified as Jean Do. Many of the bank account numbers provided by the bank are matching the ones sent by the FBI.

Questions part 2:

- Do you start an investigation against Jean Do?
- Is the bank a legitimate aggrieved party?
- Can you use the information of the bank if they have been proactive in investigating the money transfers?
- What do you do if you find links to other MS when investigating Jean Do?

PART 3

Following information coming from MS (B), you have started an investigation.

During the house search of Tom Jones, Tom was found behind his computer but was able to escape. Later on, country B issues an EAW for Tom.

The hacking forum website was displayed on the computer as well as chat sessions with different persons and with a possible hacker, who was offering newly hacked data. Tom has a Gmail account, which was not open on the computer at the time of the house search. A paper document next to the computer displays a list of logins and passwords for several Gmail accounts, PayPal accounts, websites and servers and some bank accounts in your country.

Questions part 3:

- Would you view/copy and seize the hacking forum website displayed on the computer of Tom? If yes, under which legal conditions? If no, why not?
- If yes, what would you do if you knew that the servers of the hacker and hacking forum are:
  - located in an EU MS?
  - located in a third state?
  - not clear where the servers are located?
- Would you view/copy and seize the chats displayed on the computer of Tom? If yes, under which legal conditions? If no, why not?
- May you access the Gmail accounts using the logins and passwords, without having the prior consent of Tom?
- Would there be any restrictions to use all the information gathered above as evidence in Court?
- What do you do with the information about the Paypal account?
- What do you do with the bank accounts
  - In your country?
  - In other EU/non-EU countries?

PART 4

During a check at the airport of country C, Tom Jones is arrested. Country C intends to prosecute Tom. Besides country B, you had issued an EAW against Tom Jones and the FBI is also interested in having him extradited to the US.

Questions part 4:

- How do you deal with this situation?

PART 5

Tom Jones admits that he is an administrator to one of the hacking forums.

Questions part 5:

- Would/could you consider using Tom in his administrator function in order to continue the investigation?
- Would you take down the hacking forum?

PART 6

The information obtained in the different Gmail accounts provides a complete overview of the recruitment of money mules.

Questions part 6:

- What information would you request from Google?
- May you request information from Google, as the service provider involved, (identification, connection data with respect to mailbox):
  - if Google only has a sales branch in your country?
  - if Google has no physical representative whatsoever in your country?
- What are the possible data retention issues you might be confronted with? Which is the current situation in your country as regards data retention?