A Survey of International Cooperation in Digital Investigations

Joshua I. James[1](✉) and Pavel Gladyshev[2]

[1] Digital Forensic Investigation Research Laboratory (DFIRE),
Hallym University, Chuncheon-si, Kangwon, South Korea
joshua@cybercrimetech.com

[2] Digital Forensic Investigation Research Laboratory (DFIRE),
University College Dublin, Belfield, Dublin 4, Ireland
pavel.gladyshev@ucd.ie

Abstract. International cooperation is becoming more important in digital investigations. This work provides a comprehensive study about Mutual Legal Assistance in relation to digital evidence. A survey of available information related to making a Mutual Legal Assistance Request is given, followed by a quantitative analysis of practitioner survey results related to making and receiving Mutual Legal Assistance Requests. The given survey is a first effort to provide data behind the challenges identified by practitioners when attempting to request Mutual Legal Assistance related to digital evidence. From this data, some justification for commonly cited challenges are found, as well as the circumstances in which these challenges arise.

Keywords: Digital evidence · Digital investigation · International cooperation · Cross-border investigation · Mutual legal assistance · Jurisdiction

1 Introduction

International cooperation in digital investigations is growing more important as relevant data is increasingly stored in multiple jurisdictions [8,13]. Many prior works have discussed the growing challenges of requesting potential evidence from foreign countries [8,9,13,17]. Specifically concerning formal international requests (Mutual Legal Assistance), the Commission on Crime Prevention and Criminal Justice [16] identified challenges with formal international requests as:

- Few states reported monitoring outgoing request to ensure proportionality
- Some states prioritize incoming requests and others don't – this causes problems when one state believes the crime 'high priority' and another state believes it is 'low priority'
- Differing income levels between countries can result in a low priority for a case even if the amount is substantial in the requesting country

J.I. James and F. Breitinger (Eds.): ICDF2C 2015, LNICST 157, pp. 103–114, 2015.
DOI: 10.1007/978-3-319-25512-5_8

- Multiple follow-up inquiries also take resources away from work on more urgent cases
- Several members commented that the effort for the request may be much more than the potential punishment (in the case of extradition)
- There are several states where requests for assistance in minor cases burden the Central Authority and prosecutors to the extent that they cannot focus on more serious cases.

In the author's experience, when speaking directly with cybercrime investigators, many mention a lack of international cooperation, especially timely cooperation, with some claiming that international cooperation 'never works'. From our observations, while many investigators have some complaints, the success of international cooperation appears to differ with each requesting country, and to whom the request is being made. While other works have looked at the problem of international cybercrime, and many discuss the challenges of international cooperation [12,17], to our knowledge, none have attempted to quantify formal international cooperation related to digital investigations, and attempt to identify the causes of often-mentioned challenges.

This, however, does not mean that no work is being done to solve the problem. Kent (2014) identifies a number of challenges to requesting digital evidence, especially from foreign private companies. She also provides practical and comprehensive short, medium and long term plans to improve the situation. [blinded] looks at the capacity of national and foreign organizations to deal with incoming requests for digital evidence, and proposes a national development strategy that also considers expanding capacity and capabilities in strategically important countries. To attempt to address the challenge of communication during international requests, INTERPOL is currently working on communication channels to allow the timely sending, tracking and verification of requests. Likewise, the United Nations Office on Drugs and Crime (UNODC) continues development on a 'Mutual Legal Assistance Request Writer Tool' [6] that helps to ensure that formal international requests are complete and accurate. Of course, legislation is also needed, and a number of governments and private organizations are working towards legislation to improve international cooperation [5,7].

1.1 Contribution

This work contributes to the field of digital investigation by giving a quantitative view of challenges related to international cooperation during investigations. Specifically, this work provides raw data that allows us to assess what – and when – international cooperation is working.

2 International Cooperation

International cooperation can take many forms, however, when requesting evidence from other countries that will be used in a court of law, requests normally need to be in the form of formal Mutual Legal Assistance (MLA) requests form one Central Authority (CA) to another. This study will focus on formal MLA requests.

2.1 Survey of Mutual Legal Assistance Contacts: Is Contact Information Available?

Documents specifying the requirements for mutual legal assistance requests are easily found[1] on public channels – in English – for over 100 countries (Fig. 1). Of the discovered documents, most countries had varying amounts of information available. At least contact information for a central authority was included, even with no further instructions. For G8/G20 countries, information also included general instructions for making an MLA request. The majority of documents did not contain dates or version numbers. Because of this, it is difficult assess whether the information collected is correct and up-to-date.

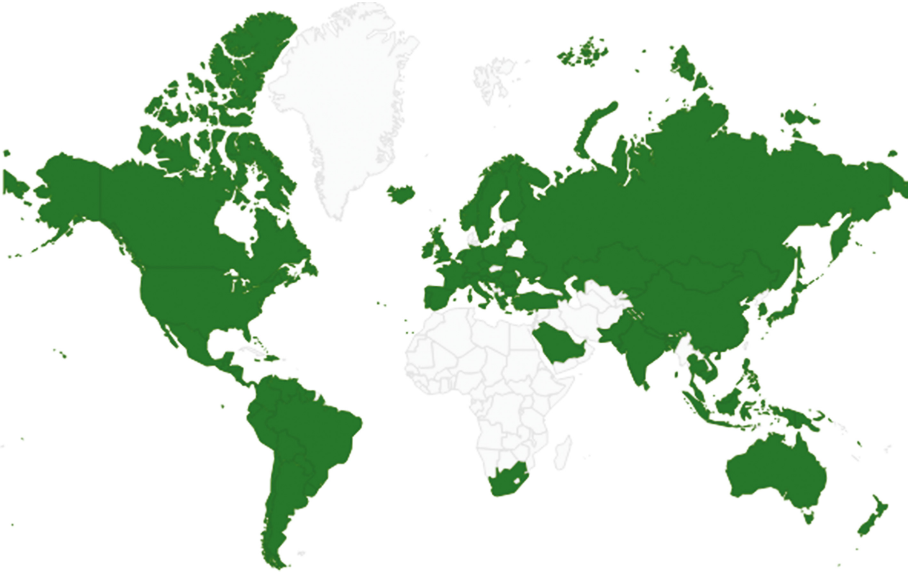

Fig. 1. A world map showing the countries where mutual legal assistance contact and basic required information can be easily found online in English.

The Council of Europe (CoE) maintains a website where associated countries should post their mutual legal assistance process information[2]. This information

[1] Easily found in this case means less than an hour searching with a public search engine using English keywords.

[2] Council of Europe. National procedures on judicial cooperation in the criminal field – Transfer of sentenced persons. http://www.coe.int/t/dghl/standardsetting/pc-oc/Country_information3_en.asp.

specifically concerns the transfer of sentenced persons, but in many cases provides general insight into the MLA process of the country.

The Organization of American States (OAS) also maintains contact information and basic MLA requirements for its members[3]. The information contained normally describes both the legal system and the mutual legal assistance process for each member country. While not exactly comprehensive in most cases, it does provide a good starting point for making contact with the country.

2.2 Mutual Legal Assistance and Digital Evidence

Almost no documents referred to computer or digital evidence directly; however, according to [10] the language of mutual legal assistance treaties are often phrased generally, and thus is able to handle new types of evidence such as those from computer hard drives, mobile phones and other digital devices.

Three examples, are Austria [1], El Salvador [14] and New Zealand[4]. In these countries there is no specific mention of digital or computer-based evidence or information. However, the language is general enough that digital evidence could be treated the same as 'traditional' evidence.

A small number of countries, however, do specifically refer to digital or computer evidence when discussing their requirements for MLA. For example, of all the G8 countries, only France referenced "material that may be held on a computer system", specifying that more specific information may be required in the case of computer evidence [15]. Similarly, in the G20 countries both France and Japan specifically mentions material that may be held on computer systems [3]. All other countries used general language, and do not specify requirements for computer-based evidence. However, although the United Kingdom did not specify computer evidence in those documents, the U.K. provides guidelines for foreign authorities that does specify material held on a computer [4].

One of the most comprehensive documents, although not country-specific, is the UNODC's manual on mutual legal assistance and extradition [2]. In it there is discussion about the production of computer records.

3 Survey of Mutual Legal Assistance Requests

To identify challenges in international cooperation – and specifically MLA – the authors conducted a survey relating to respondents' experience writing and receiving MLA requests.

- n - is the number of elements in the sample
- p - refers to the proportion of sample elements that have a particular attribute.

[3] Organization of American States. Mutual Assistance in Criminal Matters and Extradition. http://www.oas.org/JURIDICO/mla/en/atg/index.html.

[4] Crown Law Office. "Making Request". http://www.crownlaw.govt.nz.

The online survey was accessed approximately 186 times resulting in 34 fully-submitted responses. Additionally, 20 hand-written surveys were submitted, making 54 submissions in total. Ideally, The survey did not collect personally identifiable information[5].

At the time of this writing, information was received from 23 countries (+2 unreported) with regional[6] distribution as follows: Africa (1), Americas (8), Asia (3), Europe (10), Oceania (1). Information was received from 4 central authorities (Ministries, etc.), 25 law enforcement personnel, 15 prosecution-related services, 5 service providers, and 5 responses claiming to not be affiliated with any of the prior groups. Survey data is made available at [blinded].

The survey was specifically targeting individuals with experience creating or receiving mutual legal assistance requests. For this reason a filter question was introduced:

> Do you have experience with either creating or responding to mutual legal assistance requests, letter rogatory or other international requests for evidence? [n = 54]
> *No (8)   *Yes (46)

Out of the sample [n = 54], only those who responded "Yes" were allowed to submit further responses. This resulted in 46 'qualified' responses. After filtering for qualified responses, the sample represents 21 countries (+1 unreported) with regional distribution as follows: Africa (0), Americas (8), Asia (3), Europe (9), Oceania (1). This distribution along with response rates is shown in Fig. 2.

Qualified responses were received from 4 central authorities (Ministries, etc.), 22 law enforcement personnel, 15 prosecution-related services, 3 service providers, and 2 responses claiming to not be affiliated with any of the prior groups. The population is summarized in Fig. 3.

85 % [n = 54] of the sample had experience with mutual legal assistance requests or international requests for evidence (any type). 72 % [n = 54] of respondents claimed to have experience specifically dealing with mutual legal assistance requests relating to cyber crime, electronic evidence or subscriber data.

3.1 Quantitative Results Overview

The first question for qualified respondents was an attempt to assess whether the sample was similar to samples from other studies. In this case, the Comprehensive Study on Cybercrime [12], question 216 was taken directly:

[5] This research was determined to be 'not human participant research', thus no IRB application was made.

[6] Regions are defined based on the United Nations regional groupings: "Composition of macro geographical (continental) regions, geographical sub-regions, and selected economic and other groupings". 31 Oct. 2013. http://unstats.un.org/unsd/methods/m49/m49regin.htm.

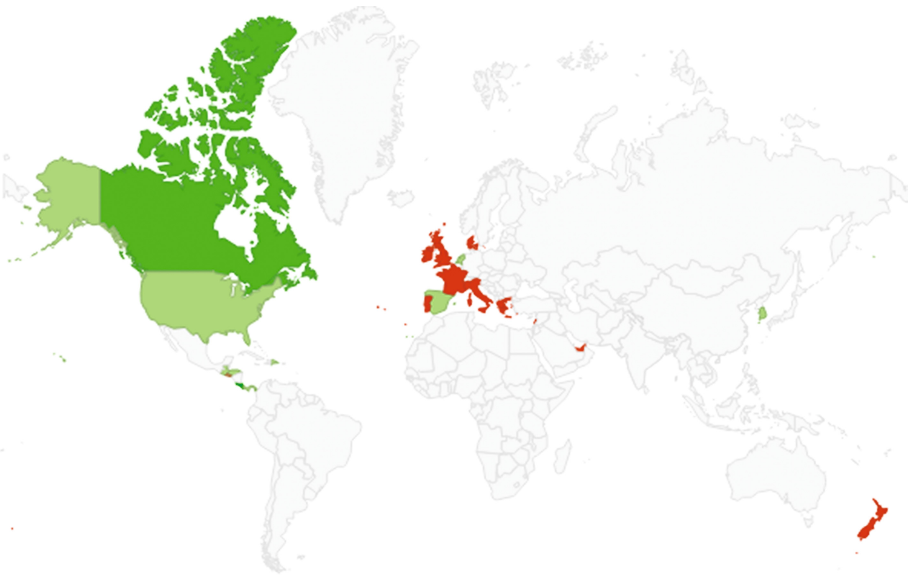

Fig. 2. World map showing countries represented in qualified responses where color denotes response rate. Red = 1 response received, and the darker the shade of green the more responses were received from the country where maximum responses <=5 (Colour figure online).

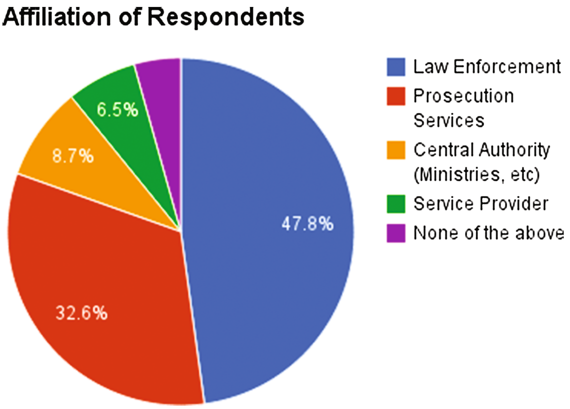

Fig. 3. The affiliation of qualified respondents by percentage of the sample [n = 46].

Does your country have legislation used as a legal basis for mutual legal assistance for cybercrime? [n = 46]
*Yes (35) *No (8) *Unsure (3)

According to the Comprehensive Study on Cybercrime, approximately 75 % of respondents reported the existence of national legislation applicable to cybercrime MLA matters. This study shows similar results, with the average respondents reporting the existence of national legislation applicable to cybercrime MLA matters being approximately 76 % [n = 46][7].

Fewer respondents (68 % [n = 46]) reported treaties, conventions and/or national legislation specifically relating to electronic evidence requests. Some groups reported that national legislation with specific provisions for electronic evidence were currently being implemented in their countries.

The most commonly referenced treaties, conventions or national legislation were the Palermo Convention (n = 31, p = 7), the Budapest Convention (n = 31, p = 7), and Penal (Criminal) Code (n = 31, p = 9).

Offered Services. The types of services being offered are relevant to the way requests for such services should be formed in terms of documents, information and wording. However, not all services were provided by all organizations. The most common service offered to other countries though MLA – in regards to electronic evidence – was reported to be **search and seizure**, with 91 % [n = 46, p = 42] of the respondents reporting that the service was available. This is followed by **preservation requests** (85 % [n = 46, p = 39]), **production of documents** (83 % [n = 46, p = 38]) and **taking of witness statements/evidence** (76 % [n = 46, p = 35]). Only 24 % [n = 46, p = 11] of respondents reported **temporary transfer of prisoners to give evidence** as a provided service. Further, 2 % [n = 46, p = 1] reported that **support teams** may be provided via MLA.

Best-Practice Request Writing Guides. Next was an attempt to determine what resources are commonly used to develop MLA requests. 52 % [n = 46] of respondents claimed that there is no step-by-step, best-practice guide available describing how to conduct each type of MLA request. Another 24 % were unsure if a guide existed, meaning that 76 % [n = 46] of respondents are unable to use a guide to help develop MLA requests[8]. 24 % of respondents, however, claimed that a step-by-step, best-practice guide does exist for their countries.

Best-Practice Requesting Digital Evidence. The respondents were asked about the level of standardization or best-practices related to requesting or obtaining digital evidence from foreign countries when requests are specifically about digital evidence. 61 % [n = 46] reported there were no national standards or best-practices specifically concerning digital evidence requests, and 21 % [n = 46]

[7] The average depends on the classification of the 'unsure' group. In this case, 'unsure' is considered a negative, or 'No' classification.

[8] Please note, in the general analysis respondent groups and countries are combined. Some respondents such as Service Providers (6 % of the population) may have no need to create mutual legal assistance request guides.

reported ‘unsure’ whether national standards or best-practices existed. Only, 17 % [n = 46] reported national standards or best practices existing.

Best-Practice Requesting Digital Evidence. Respondents who reported national standards or best practices exist in their countries, were asked to elaborate. Some respondents [n = 6, p = 1] reported that digital evidence is treated the same as physical evidence. Others [n = 6, p = 2] appear to say the same, citing the central authority as the point that decides the standard; however, no specific standard was given. Other respondents [n = 6, p = 2] also did not elaborate.

One response more thoroughly described the current situation, and is given below (redacted).

> “I would actually say ‘kind of’ not yes or no. We are supposed to make the request through the [central authority], all requests for electronic evidence go through one location... That is where the best practices ends. There is nothing else regarding formats, handling, transfer, digital verifications (hashes) etc.”

In this case, there is reference to internal standards or best-practices that are followed in terms of making or receiving requests. Internally and externally, formats, handling, transfer and verification are not defined.

Information Exchange Protocols. The above is related to the state in which information or evidence is exchanged. When asked if their country has information exchange protocols in place to transfer electronic evidence internationally, 46 % [n = 46] reported no, and 26 % [n = 46] were unsure. 28 % [n = 46] claimed their country does have information exchange protocols in place to transfer electronic evidence internationally.

Information Exchange Protocols. The respondents that reported protocols exist were asked to elaborate on their protocols. INTERPOL’s exchange protocol was the most commonly named, followed by Europol’s protocols and the Budapest Convention. Other protocols appeared to be country-specific depending on specific treaties or memorandum of understanding (MOU) that are in place.

Request Writing Experience. To attempt to capture specific information on the MLA writing process, the respondents were asked about their experience writing MLA requests for electronic evidence. 80 % [n = 46] of respondents reported having experience writing MLA requests for digital evidence, and 20 % [n = 46] reported not having experience. Respondents with no experience writing MLA requests for digital evidence were excluded from answering the following MLA request-writing-related questions.

Request Writing Challenges. When asked about the major challenges to writing MLA requests for electronic evidence, 57 % [n = 37, p = 21] of respondents identified that the acquisition of appropriate documents from the requested country was a challenge. 51 % [n = 37, p = 19] identified “appropriately describing the required scope of digital evidence" as a challenge. Both defining the required digital evidence, and the exchange protocols for digital evidence was identified by 46 % [n = 37, p = 17,17] of respondents. Protocols for the exchange of data across borders was less of a concern, with only 30 % [n = 37, p = 11] identifying it as a challenge. Other challenges given were related to the time of the request [n = 37, p = 2].

Request Success and Failure. To assess the effectiveness of requests for digital evidence through MLA, the respondents were asked how often data was received (or not). For requests made, 30 % [n = 37, p = 11] of respondents claimed that they have never received ALL data that was requested. 38 % [n = 37, p = 14] claim that only 1 % to 25 % of their requests receive ALL data requested. The percentage of requests where ALL requested evidence was returned continues to drop, until the 75 % to 99 % range, where it slightly increases again.

For requests made, 19 % [n = 37, p = 7] of respondents claimed that they have never received SOME data that was requested. 46 % [n = 37, p = 14] claim that only 1 % to 25 % of their requests receive SOME data requested. The percentage of requests where SOME requested evidence was returned continues to drop, until the 50 % to 75 % range, where it increases again.

For requests made, 14 % [n = 37, p = 5] of respondents claimed to never receive requested electronic evidence. On the other hand, 24 % [n = 37, p = 9] of respondents claimed that at least some requested information was always returned. 35 % [n = 37, p = 13] of respondents claimed that 1 % to 25 % of their requests would result in no requested information being returned.

Request Feedback. For requests made, 38 % [n = 37, p = 14] of the respondents claimed to receive no feedback for any of their requests. 27 % [n = 37, p = 10] of respondents claimed to received feedback on 1 % to 25 % of their requests.

Most Common Requests. The most commonly-requested information is IP address and subscriber information (32 % [n = 37]). This is followed by information relating to social networks, and email (contents), equally (27 % [n = 37]). The next most commonly requested information was identified as Internet access logs and forensic imaging of devices (19 % [n = 37]). It may be possible to classify some of the remaining miscellaneous requests as one of the categories already given.

Request Preparation. The respondents were asked approximately how long it takes to prepare a MLA request for electronic evidence. 41 % [n = 37] of respondents reported that the preparation of a request takes 0 to 2 weeks, with most reporting times in days (on written surveys). 76 % [n = 37] of respondents reported that an MLA request could be prepared in 4 weeks or less.

Request Receiving Experience. To attempt to capture specific information on MLA receiving and processing, the respondents were asked about their experience receiving and processing MLA requests for electronic evidence. 59 % [n = 46] of respondents reported having experience receiving or processing MLA requests for digital evidence, and 41 % [n = 46] reported having no experience receiving or processing MLA requests for digital evidence. Respondents with no experience receiving or processing MLA requests for digital evidence were excluded from answering the following MLA request-receiving-related questions.

Required Request Information. 37 % [n = 27] of respondents reported that 75 % to 99 % of all MLA requests received contained all information necessary to process the request. 22 % [n = 27] of respondents reported that 50 % to 75 % of MLA requests received contained all information necessary to process the request, while 26 % [n = 27] of respondents claimed only 25 % to 50 % of MLA requests received contained all information necessary to process the request.

Request Denials. 48 % [n = 27] of respondents reported that 0 % to 25 % of all MLA requests received had a scope that was "too broad" or did not appear to match the reason for the request. However, 52 % [n = 27] of respondents claimed that 25 % to 99 % of all received requests had a scope that was too broad or did not appear to match the reason for the request.

Request Denials. 48 % [n = 27] of respondents reported that 0 % of requests were denied because of a lack of dual-criminality. 30 % [n = 27] of respondents reported 1 % to 25 % of requests being denied. While 22 % [n = 27] of respondents reported 25 % to 75 % of requests being denied because of a lack of dual-criminality.

Request Denials. 56 % [n = 27] of respondents reported that 0 % of requests were denied because the request may violate local rights in the requested country. 33 % [n = 27] of respondents reported 1 % to 25 % of received requests were denied because it may violate local rights in the requested country.

Request Feedback. 37 % [n = 27] of respondents reported that feedback to received requests was being given 0 % of the time. Another 37 % [n = 27] of respondents reported that feedback to received requests was being given 1 % to 25 % of the time. 11 % [n = 27] of respondents reported that feedback to received requests was being given 100 % of the time.

Request Denial. The respondents were specifically asked what the most common reason a request for electronic evidence would be denied in their country. 33 % [n = 27] of respondents reported that most requests are denied because the data no longer exists in the requested country. 15 % [n = 27] of respondents reported that requests are not denied. Other evenly-distributed reasons include the authority conducting the investigation was not clearly identified, data protection laws, requests for data were not clear, and the requested data is not normally collected by the requesting country.

Essential Information. What asked what information is essential when requesting electronic evidence from another country, the respondents gave a list of information they considered 'essential'. IP address (or IP address history) was the most commonly mentioned piece of 'essential information' [n = 24, p = 8]. Followed by 'core information about the type of data required' [n = 24, p = 7].

Most Common Requests. When asked what the most common types of electronic evidence has been requested from them, the respondents again said that

IP addresses and related information were the most commonly received requests [n = 26, p = 8]. This is followed by acquisition of hard drive / computers, data about persons, account information / subscriber information and mobile phone information, equally [n = 26, p = 5,5,5,5].

Request Language. 41 % [nv46] of respondents reported that only nationally recognized languages are accepted for MLA requests. 39 % [nv46] of respondents reported that some other foreign languages are normally accepted for MLA requests, and 20 % [n = 46] were unsure whether foreign (not nationally recognized) languages were accepted for MLA requests.

Request Point of Contact. The respondents were asked to identify the central authority responsible for sending and receiving requests for MLA involving digital evidence. The most commonly-named central authorities are the local Public Prosecutors [n = 46, p = 17], followed by the Department or Ministries of Justice and the Ministry of Foreign Affairs [n = 46, p = 9,6].

Request Creation. 54 % [n = 46, p = 25] of respondents reported that they used their own organization's internal document template to create MLA requests. 52 % [n = 46, p = 24] of respondents also reported that departments or investigators create their own MLA request documents. This is followed by 15 % [n = 46, p = 7] of respondents claiming to use request forms from INTERPOL.

Request Forms for Digital Evidence. 41 % [n = 46] of respondents reported that MLA request documents do not contain specific fields for requesting electronic evidence. 35 % [n = 46] of respondents claimed MLA request documents do contain fields specifically concerning digital evidence. 24 % [n = 46] of respondents were unsure.

Request Channels. When asked about the most commonly used channels for MLA requests, 63 % [n = 46, p = 29] of respondents reported using their national central authority. 52 % [n = 46, p = 24] of respondents reported working directly with the central authority in the requested country. 41 % [n = 46, p = 19] of respondents made requests directly with Law Enforcement organizations in the requested country, and 33 % [n = 46, p = 15] of respondents reported working directly with investigators in the requested country. This was followed by the use of the INTERPOL I24/7 network (30 % [n = 46, p = 14]).

4 Conclusions

The described survey is a first effort to provide data behind the challenges identified by practitioners when attempting to request Mutual Legal Assistance related to digital evidence. From this data, a number of weaknesses in communication and information sharing may be seen that contribute to lower quality, or even incomplete requests being made. Further, there appears to be a disconnect between the communication about the status of requests, and the status updates that are received by the requesting country. Further, more in-depth, analysis, however, is left to future work. By making this data available, this work helps to improve awareness about weaknesses of international cooperation relating to cybercrime investigations, and help describe why those weaknesses may exist.

4.1 Future Work

Future work will include a through analysis of the data beyond a superficial quantitative analysis. Further, there is much that can be said about the survey results, including which countries are 'more successful' in MLA requests, and why. We hope to use this study to develop real-world solutions that help international cooperation relating to digital evidence.

References

1. Austria national procedures for mutual legal assistance in criminal matters. Technical report
2. Manual on Mutual Legal Assistance and Extradition: Technical report. United Nations Office on Drugs and Crime, Vienna (2012)
3. Requesting Mutual Legal Assistance in Criminal Matters from G20 Countries: A step-by-step guide. Technical report, G20 (2012)
4. Requests for Mutual Legal Assistance in Criminal Matters: Guidelines for authorities outside of the United Kingdom. Technical report, Home Office (2012)
5. Internet and Jurisdiction (2015)
6. Mutual Legal Assistance Request Writer Tool (2015)
7. Mutual Legal Assistance Treaties (2015)
8. Broadhurst, R.: Developments in the global law enforcement of cyber-crime. Polic.: Int. J. Police Strat. Manage. **29**(3), 408–433 (2006)
9. Cerezo, A.I., Lopez, J., Patel, A.: International cooperation to fight transnational cybercrime. In: Proceedings of the 2nd International Annual Workshop on Digital Forensics and Incident Analysis, WDFIA 2007, pp. 13–27 (2007)
10. Chêne, M.: Mutual legal assistance treaties and money laundering. Technical report, Anti-Corruption Resource Centre (2009)
11. Gail, K.: Sharing Investigation-Specific Data With Law Enforcement - An International Approach (2014)
12. Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S., Ignatuschtschenko, E.: Comprehensive study on cybercrime. Technical report February, United Nations Office on Drugs and Crime (UNODC) (2014)
13. Martini, B., Choo, K.K.R.: Cloud storage forensics: OwnCloud as a case study. Digit. Inv. **10**(4), 287–299 (2013)
14. Ramirez, J.: The mutual legal assistance process in El Salvador. Technical report (2009)
15. ROMA-LYON GROUP: Requesting mutual legal assistance in criminal matters from G8 countries: A step-by-step guide. Technical report, Commission on Crime Prevention and Criminal Justice, Vienna (2011)
16. ROMA-LYON GROUP: Addressing Requests for Mutual Legal Assistance in De Minimis Cases. Technical report, G8 (2013)
17. Westmoreland, K., Gail, K.: Foreign Law Enforcement Access to User Data: A Survival Guide and Call for Action (2015)