Council of the European Union

Brussels, 23 March 2016
(OR. en)

7323/16

LIMITE

JAI 230
CYBER 26
COPEN 87
DROIPEN 58
JAIEX 25



**NOTE**

| | |
|---|---|
| From: | Presidency |
| To: | Delegations |
| Subject: | Presidency Conference "Crossing borders: Jurisdiction in Cyberspace", Amsterdam, 7-8 March 2016<br>= Conference report, chair conclusions and workshop notes |

In a follow up to the discussion of the Ministers of Justice at the Council in December 2015 on criminal justice response in the digital age [1] and further to the informal meeting of the Justice Ministers on 26 January 2016 in Amsterdam, where on both occasions the need to consider pragmatic solutions enabling effective investigations in the cyberspace, including alternatives to traditional concepts were discussed, the Netherlands Presidency hosted a Conference "Crossing borders: Jurisdiction in Cyberspace" on 7 and 8 March 2016 in Amsterdam.

Delegations will find attached report from the conference, the concluding remarks of the Chair, as well as the preparatory notes for the three workshops held during the conference.

The Presidency will take these issues further to discussion at expert level and CATS with a view to preparing draft Council conclusions setting up the way forward for future follow up and action. Ministers will be invited to provide political guidance on some outstanding issues and to adopt the draft Conclusions at the Council ("Justice and Home Affairs) in June.

[1] doc. 14369/15

Furthermore it was advised by practitioners on several occasions as well by the participants of the Conference that a network for prosecutors and investigative judges on cybercrime could support the effectivity of the criminal justice response in the digital age. The Presidency therefore will submit Council conclusions on the establishment of a European Judicial Cyber Crime Network supported by Eurojust.

# Crossing Borders: Jurisdiction in cyberspace

# Amsterdam, 7-8 March 2016

# Conference report

This Report outlines the main outcomes and possible issues for future consideration deriving from the Conference "Crossing Borders: Jurisdiction in cyberspace", that took place on 7th and 8th of March in Amsterdam. Policy experts and practitioners from the Member States, together with representatives from private sector and academia had in-depth discussions on pressing issues with regard to jurisdiction in cyberspace. Three main issues were addressed at the Conference, including in dedicated workshop discussions followed by a panel discussion which are respectively referred to in this Report:

1. Cooperation between countries and the need to optimise Mutual Legal Assistance (MLA) processes for the purposes of the effective gathering of e-evidence
2. Cooperation with the private sector and the need to avoid the negative impact of conflicting regulations;
3. How to proceed in the absence of possibilities for cooperation due to unknown location of required data or of the origin of a cyber attack ("loss (of knowledge) of location").

The Conference was held under Chatham House Rule. The information in this report is not linked to names or affiliations of participants. The conference report does not represent the position of any government or organisation.

## International cooperation regime in cyberspace

Two horizontal issues related to the general principles of the international cooperation in cyberspace emerged from the Conference discussions. Notably, grounds additional to the principle of territoriality for establishing jurisdiction in cyberspace and the possibility to apply differentiated approaches to different types of data. Those two were considered relevant for the three main issues of concern addressed at the Conference.

## Grounds for jurisdiction in cyberspace

Especially, since the 1935 Harvard Research Draft Convention on Jurisdiction with Respect to Crime (Harvard Draft), the principle of territoriality has generally been regarded as the primary principle for determining jurisdiction. It follows from this principle that for any enforcement action beyond the state's own territory, the express consent of the affected states is required.
However, keeping the focus on the territoriality principle for establishing jurisdiction in cyberspace is becoming increasingly problematic due to the digitisation of criminal evidence and the volatility of data worldwide. To address this concern, two strands of work could be followed. First, by looking into possibilities to speed up the handling of formal MLA requests, as well as to explore other ways of international cooperation. Second, to address the underlying and more fundamental question about how jurisdiction in cyberspace should be established.

The need for a fundamental discussion about the connecting factors for jurisdiction in cyberspace (in addition to territoriality) was addressed by the Ministers of Justice at the Informal Justice and Home Affairs Meeting on 26 January 2016. There was a large support expressed for the consideration of alternative approaches in this regard.

During the conference, the notion was followed that the physical location of the data has become less relevant for determining jurisdiction. In addition, for cooperation with private sector, the location of the formal headquarters of the service provider was not regarded as a primary connecting factor for determining jurisdiction in cyberspace.

Various elements were put forward that could complement the principle of territoriality. They are based on legal principles that already exist, deriving from criminal international law, private international law, EU legislation on wiretapping, etc. In the absence of grounds to exercise jurisdiction, the following principles could be considered as giving rise to a justified legal claim for jurisdiction:

- A **substantial connection** between the matter and the state seeking to exercise jurisdiction
- The state seeking to exercise jurisdiction has **a legitimate interest** in the matter
- The exercise of jurisdiction is reasonable given **the balance** between the state's legitimate interest and other interests

While addressing the fundamental question on how to establish jurisdiction in cyberspace, these principles are also in line with the spirit of the Harvard Draft principles. Even in such an alternative approach territoriality would still be an important connecting factor, since it would provide a state with a substantial connection to the matter.

A more **subject oriented approach** was also discussed by participants. In this regard the location of habitual residence of the investigated person, and the nationality of the victim or of the suspect would follow as a logical ground for jurisdiction. With regard to cooperation with private sector, the connection of the service provider to the territory of the investigating state was put forward, referred to as a "business link". According to this approach, any service provider that provides services in the territory of a given state is considered to be bound by that state's legal framework and should therefore cooperate with law enforcement on the basis of domestic orders.

## Differentiation between types of data

International cooperation regimes in criminal matters balance the various interests involved with due respect to rights and obligations of states and individuals. This balancing results in practice in different requirements and outcomes for obtaining access to e-evidence. For example, US law does not prevent direct requests from Member States to US-based service providers if the request concerns only subscriber data. For content data MLA is required. Also, the EIO Directive provides for more grounds for refusal for interception of telecommunications involving real time monitoring, than for other investigative measures. Scattered examples of differentiation thus already exist in practice, both within and outside the EU, including in the context of the CoE Convention against Cybercrime (the Budapest Convention). However, a clear framework for obtaining data for the purposes of criminal investigations in cyberspace is lacking. In this respect, several proposals seeking to standardise the approach to different types of data were discussed at the Conference along the following lines:

***Subscriber, traffic and content data***

Different regimes can be envisaged for different types of data. This should be linked to a balance of interests test between the interests of the investigation and the privacy considerations. When the interference with the rights and freedoms of the investigated person is greater, a more stringent regime of safeguards and guarantees should be applicable.

A distinction between subscriber, traffic and content data is commonly used. Some prefer a distinction solely between content and non-content data. Both subscriber data and traffic data would then be regarded as non-content.

Subscriber data is the most often requested type of data for the purposes of criminal proceedings, followed by traffic data and finally content data. It was acknowledged by participants that the interference with the rights of the investigated person is lower in the case of subscriber data compared to traffic data and content data and therefore a lighter regime for obtaining such data could be reasonably envisaged. It was concluded that this distinction should be systematically reflected in the current legal frameworks (both national and international) and that such a solution could substantially release pressure from the existing system for international cooperation for obtaining e-evidence.

***Real time vs. stored data***

Different regimes can also be envisaged for different investigative measures. Again, for each measure a balance of interests should be struck. Some investigative measures are less intrusive than others. A privacy interference is regarded greater in the case of a real-time collection of data, in contrast with the less intrusive measure of obtaining ex-post stored data. Therefore, a lighter regime could be envisaged for a production order than, for example, search and seizure of computer systems or interception of communications.

## Cooperation between states: obtaining e-evidence via MLA

Traditional MLA proceedings are considered cumbersome or ineffective in cases were e-evidence is concerned. The obstacles that have been identified relate to the challenges to get a timely response to a request, to the formalities and paperwork involved to make and process a requests, to the limited capacity and inadequate level of knowledge in requested countries, but also to legal matters such as dual criminality, absence of arrangement for expeditious action, and lack of coordination. Practical possibilities for streamlining the existing MLA process, as well as possible solutions of a more principal nature were also discussed at the Conference.

## Practical possibilities for streamlining MLA

***Possibilities for states***

1. *Increase capacity of competent authorities*
   Training and allocating more technology literate staff is necessary for the effective handling of MLA requests, and to ensure that the requests are made in accordance with the requirements of the requested state.
2. *Optimise the use of the 24/7 contact points in MLA processes*
3. *Emergency procedures*
   Develop emergency procedures for requests related to risk of life and similar exigent circumstances.
4. *Streamline procedures*
   Standard request format ready for adoption for each requested country should be developed.
5. *MLA streamlining*
   Shorten lengthy MLA justification to the core: what crime, which specific information is needed for requested country.
6. *Parallel investigations*
   Opening of domestic investigations upon a foreign request or spontaneous information to facilitate the sharing of information or accelerate MLA should be used more often.
7. *Explore options to apply the dual criminality standard in a more flexible manner.*

***Creating an online EU portal for MLA requests***

1. *Automatic translation of forms*

   Forms for MLA requests could be only in English or with automatic translation. In some countries, in the court proceedings the forms are required in the national language.

2. *Create the possibility to track and trace MLA requests*

   Tracking could include the notice of receipt, updates, specified and previously communicated groups for refusal.

An option could be to link such a portal to the EJN and/or FIU-net.

## Options of a principal nature: Clear rules for when MLA is needed

***MLA vs. police-to-police cooperation***

The distinction between police-to-police cooperation and MLA is not always clear. For content data and traffic data, as in judicial proceedings, a formal MLA request is often required. The same applies for the admissibility as evidence in court of material received via police-to-police cooperation. The general understanding is that police cooperation is aimed at exchanging information that could lead to the opening of criminal proceedings. The purpose of MLA is to obtain evidence for use in criminal proceedings. Participants were of the opinion that when police-to-police cooperation is possible, MLA should not be used.

***Direct access for subscriber information***

MLA should only be used when absolutely necessary, while taking into account the need to safeguard the balance of interests in the criminal proceedings. As explained above, allowing direct contacts with private sector for obtaining subscriber data was considered as an appropriate solution for relieving the heavy burdened MLA process, while drawing a balance between the interests of investigating criminal acts and those of the investigated persons.

## Cooperation with the private sector

### *Obtaining e-evidence from private sector*

Conflicting regulations hamper cooperation with the private sector. Service providers, especially those providing cloud computing services, often do not store information about clients and their activities in the countries where those clients are. Those private companies may be established in one country and provide their services in other(s). Suspects of criminal investigations can be located in one country, while the information about them in another and the service provider established in a third.

Participants observed that currently service providers are often put in a position to decide upon direct requests from competent authorities without a clear commonly applicable framework. They often feel compelled to assess the legality such requests themselves. In addition, differences in national regulations can become an obstacle for such cooperation. Complying with a request for data in one country could imply violating the law in another. The competent authorities find themselves confronted with differing service providers' policies, which make outcome of data requests unpredictable.

### *Grounds for jurisdiction*

When approaching private sector, location is a crucial factor for determining jurisdiction. However, in cyberspace the relevant location is often hard to determine. As explained above, the physical location of the data and the official headquarters of the service provider, although currently often invoked, were regarded by the participants as less relevant for determining jurisdiction. Instead, the nationality of the victim and the nationality of suspect were put forward. In addition, the location of habitual residence of the investigated subject could be a possible criterion.

Also, the relation of the service provider to a state territory was considered relevant. This was referred to as a “business link”. Applying such a connecting factor for jurisdiction can also ensure a broader impact of Article 18 of the Budapest Convention, which sets out rules enabling the competent authorities to obtain data from a person or a service provider found to be present on its territory by the services it provides on the basis of a domestic production order.A strong business link could be assumed if the service provider explicitly targets the customers in the requesting state, for example by using the domain name of the state, the local language and by showing publicity based on the location of the users. The judgement of the Belgian Supreme Court in the Yahoo!-case is a recent example in this respect.

***Establishing a common cooperation framework***

The current regime of voluntary cooperation with private parties based on direct contacts has limitations. Establishing a clear cooperation framework could benefit states, private sector and its customers as it would increase legal certainty.. The EU would be well placed to develop such a regime due to the high level of harmonisation that already exists and due to the common standards for fundamental rights and freedoms protection. A common EU regime could set a model and outreach third countries, preferably in the context of the Budapest Convention. If the EU was to develop such a regime, cooperation with the US was considered important.

It was pointed out that the obligations arising for the private sector in the requesting and in the requested state should be taken into account. Three possible situations could be considered in this regard: (1) a mandatory regime for cooperation existing in both the requesting and the requested state, (2) a mandatory regime existing in the requesting state, and a voluntary regime in the requested state or, (3) a conflict of laws arises.

***Elements of a common EU framework***

The following elements were brought forward during the discussions at the Conference as relevant in the possible development of a common EU framework for cooperation with the private sector:

1. *Contemplate modalities and conditions of requests*

Agreement in the EU on what data can be shared under which conditions would prevent the assessment of legality by the private sector themselves.

2. *Direct access for subscriber data*

Establish a lighter regime for disclosure of subscriber data. According to the US Electronic Communications Privacy Act (ECPA), subscriber data from US-based service providers can be obtained directly with the approval of the provider. MLA is not needed in these cases. For US based service providers direct access is thus already possible, but this possibility is not systematically recognised across the EU. A possible common framework should include the explicit permission for EU competent authorities to contact directly service providers abroad when subscriber data is needed. Reciprocity implications should be assessed in this respect - to whom and under which circumstances could EU service providers share subscriber information with non-EU authorities?

3. *Address conflicts between national laws*

A common EU framework could address conflicts of national laws between Member States, and anticipate the course of action for conflicts of laws with third countries. A positive obligation could be placed upon the private sector to proof a conflict of laws, instead of only presuming the existence of such conflict. This is currently worked out in the Draft Investigatory Powers Bill in the UK.

4. *Address the issue of admissibility of evidence in court*

In some states the data received directly from service providers in foreign jurisdictions is not admissible as evidence in criminal proceedings. MLA is thus required. If a lighter regime for obtaining subscriber data is envisaged, a differentiated approach in handling such data in the context of admissibility of e-evidence in national criminal proceedings should be also provided.

## Absence of possibilities for cooperation: loss (of knowledge) of location

***Sovereignty in cyberspace***

The territoriality principle is presenting a growing challenge in cyberspace. In practice, many countries already conduct cross border searches. Apart from territoriality, other principles could complement the considerations on jurisdiction. These considerations can determine which state has the greatest interest in the case.

Under a strict and traditional interpretation of international law, any cross border investigation without consent from the other state is not allowed due to the territoriality principle. However, over the years, states have not maintained full sovereignty in all cases. This principle is by no means absolute. For example, when satellite technology came up, sovereignty in the strict sense was not applied. Instead, a new regime was developed in which, under certain conditions, the use of this new technology was regulated. The regime comprises the right of a sensing state to collect and distribute satellite imaging without regard to the wishes of the sensed state, as well as an obligation upon sensing states to make the imaging available to the sensed state on a non-discriminatory basis and on reasonable cost terms. The legal framework applicable to satellite imaging suggest that where technology makes assertions of territorial sovereignty untenable, and where states perceive a shared interest in upholding the rule of law, there is a possibility to create an alternative regime for cooperation.

The principle of non-interference is not the only consequence of sovereignty. In addition to the rights deriving from sovereignty, states have also obligations such as the obligation to enforce the law in their territory and protect their citizens, and to prevent harm from their territory to other states. Because the capacity to act is the basis to claim sovereignty, this could be questioned when a state does not have this capacity in cyberspace. As underlined by participants at the Conference, not knowing the location of data does not mean necessarily that the data is to be found abroad, it could be located in the territory of the investigating state. Moreover, it was considered that it is a prevailing interest of the State to act in order to prevent or stop criminal effects in its territory and therefore investigative measures should be enabled.

***Differentiation between investigative measures***

In cases of a potential breach of sovereignty, or to preclude the wrongfulness of such a breach, the amount of possible harm to the interests of the implicated state was considered as a relevant factor. For certain investigative measures, the material damage to the cyber infrastructure located in another state could be only minor, e.g. for copying data, logging into the account of a suspect with legally obtained credentials, or measures that do not involve coercion. Others can be considered more harmful, e.g. deleting data or altering the functionality of a computer system. In this respect the possibility to envisage a differentiated regime, where unilateral action would be allowed in specific circumstances and under limited conditions was discussed.

***Alternative concepts***

Some alterative solutions were also touched upon. For example, according to the concept of the high seas, states have freedom of navigation, but this does not allow for a lawless space. States are allowed to act against certain criminal behaviour. Applied by analogy to cyberspace, this would require agreement on the criminal acts that states could investigate without knowing the location in advance. The flag principle could be useful in cyberspace: when the flag or origin is not known or concealed, competent authorities could be allowed to act. That would require an obligation to mark data. The international regime for satellites also provides interesting parallels. To further transparency a repository body for notifications of state activity (preferably worldwide) could be helpful, provided it allows for confidentiality on the case level. States could be held responsible for the damage they may inflict when conducting cross-border activity. The satellite regime benefits all states, which was an important factor for agreement [similarly to cyberspace which could be considered as a new common].

The application of these principles to cyberspace, perhaps in a modified form, could then possibly provide solutions for criminal investigations in cyberspace in cases of loss of (knowledge of) location, or where a state does not have the capacity to act to prevent harmful effects in another state.

A new regime enabling investigations in cyberspace when the physical location is not (yet) known could determine specific investigative measures that could be allowed, specific criminal acts and circumstances where it would apply, as well as the necessary safeguards in this respect. Transparency and notification were considered essential elements of such a solution. Developing a regime that furthers the common interest could be a condition for agreement, as in the regime for satellite imaging. In any new regime, reciprocity implications should be contemplated. Elements of Article 31 of the EIO Directive (e.g. interception of telecommunications without technical assistance) could be used. It could be instrumental to extend such a solution to similar situations in the cyberspace.

***Minimal investigative measures in case of loss of (knowledge of) location***

Another approach when the location of required data or the origin of a cyber attack are unknown(or could not be reasonably expected to be known) that was considered is to allow minimal investigative measures to determine the location. In such cases, proportionality and subsidiarity should be leading principles, with a view to containing the potential harm to the interests of the other state to the minimum. Once the other state is known, the investigating state should notify it, so that they would be in a position to determine together how to proceed. When the states do not agree, an arbitrage process could be envisaged. In exigent circumstances, pursuing a unilateral action could be allowed, subject to a later notification.

***Alternatives for location as primary nexus***

A location in cyberspace can be unknown, very hard to determine and/or rapidly changing. Location is therefore not the best way to determine jurisdiction. Moreover, location is hardly relevant in cyberspace. Data can be approached from everywhere. A customer of a service provider mostly does not know where his or her data is stored. He or she almost never chooses a service provider based on the data storage location. And often there are no other connections outside the investigating state but the location of data. The suspect, victim and crime could all fall into one state, but the e-evidence could be in another. In this respect the need to reconsider traditional concept of physical location of data was brought up also in the context of the discussions on the loss of (knowledge) of location. For example if a unilateral action would be allowed in specific circumstances and under specific conditions subject to later notification, it was considered that the state to be notified should be the state in which the data are controlled, rather then the (often unknown) state in which the data are physically located.

As said, this report will provide input for discussions on expert level and in the CATS meeting in May. In that meeting, the EU member states will discuss how they will take the outcome of this conference further, and what possible solutions they find most helpful.
The outcome of CATS will guide the preparations for the meeting of the Justice and Home Affairs Council ministerial meeting in June, where the way forward on effective criminal justice in the digital age will put on the table.

## Crossing Borders: Jurisdiction in cyberspace
## Chair conclusions[2]

This conference was dedicated to the issue of jurisdiction in cyberspace in view of enhancing the effectiveness of investigation of cybercrimes and the gathering of e-evidence, following the discussion of the Justice and Home Affairs Council ministerial meeting in January.
Law enforcement practitioners, policy makers, private enterprises and academics convened here to have in depth discussions on possible solutions to identified obstacles for law enforcement. Also, many papers were provided as contributions to this conference.

The discussions focused on improving the efficiency and effectiveness of mutual legal assistance, on conflicting regulations for private parties on direct exchange of data and on investigations of crime from unknown locations or criminal safe havens.

The conference underlined both the need for solutions for effective law enforcement investigations, and the importance of clear frameworks, including proper conditions and safeguards for cross border investigations.

Participants agreed that where electronic evidence is stored in foreign jurisdictions mutual legal assistance in criminal matters is the primary means to obtain data. However, in view of the evolved use of internet and communication technologies, current MLA procedures need to be updated and improved.

Regarding the improvements of mutual legal assistance procedures, several proposals were discussed to limit the duration and bureaucracy. These proposals included an online portal, trusted single points of contact, automatic translations, emergency procedures and limiting requests to the information that is strictly necessary. Adequate staffing and sufficient training were also mentioned. The discussion provided options for practical measures to be implemented, hopefully in a relatively short term.

[2] The chair is independent. These conclusions do not represent the position of any government or other organisation.

Subscriber information is the most often requested type of data, the obtaining thereof being a lesser interference to the rights of individuals than obtaining traffic information and content information. A simplified regime for MLA requests for subscriber information was contemplated. A subject oriented approach for traffic and content data could be elaborated in the medium or longer term. Distinctions between stored and flowing data, and powers used could be relevant. And perhaps MLA processes should not be used when it is not necessary.

On the issue of conflicting regulations on direct exchange of data, it was noted that private parties are often brought into a position to decide upon requests from law enforcement authorities without a clear – regional or universal - legal framework.

Next to this the possibility of issuing production orders based on article 18 of the Cybercrime Convention, to companies offering a service in the territory of a state, was brought up.
Service providers often feel compelled to assess the legality of law enforcement requests themselves.

While the amount of direct requests to providers is on the rise, law enforcement agencies find themselves confronted with differing company policies, which make disclosure of data unpredictable.

Clearer frameworks would benefit both law enforcement and private parties.. Again a lighter and more adequately devised regime for disclosure of subscriber information by private companies was discussed. The frameworks are to be designed to ensure that legal safeguards and the protection of rights of individuals are protected.

When approaching private companies, location is a crucial factor for determining the jurisdiction to enforce. However, in cyberspace the relevant location is often hard to determine. Various factors including the nationality of the victim and the suspect, and the relation of the service provider to the territory were considered relevant.

Solutions for these issues might be agreed upon easier for the less invasive use of investigative powers. For this purpose, distinctions could be made between types of data, like the distinction between content, traffic and subscriber data.

On the issue of crime from unknown locations, the issue of sovereignty, and the rights and obligations connected to it, were discussed. The duty of states to act against criminal activity originating from their territory and the obligations of states to protect the rule of law were an important part of the discussion

In order to find solutions, several creative ideas for alternative legal concepts were put forward and applied to cyberspace. Examples are the concept of the high seas and the concept of open skies.
As a more practical way forward, several circumstances and conditions were put forward to determine whether unilateral action could be justified. Proportional action to determine the location, notification of the other state as soon as it is identified, and transparency were part of the discussion. A way forward could be to determine under what conditions unilateral actions could be accepted. Proportionality and subsidiarity are important in a cyberspace environment.
The Netherlands presidency will provide a comprehensive report on the discussions we have had here in the past two days. Your contributions in the discussions will be kept anonymous, as the Chatham house rule requires.

The report will provide input for discussions on expert level and in the CATS meeting in May. In that meeting, the EU member states will discuss how they will take the outcome of this conference further, and what possible solutions they find most helpful.
The outcome of CATS will guide the preparations for the meeting of the Justice and Home Affairs Council ministerial meeting in June. Together with the incoming Slovak presidency and EU institutions, the presidency will discuss the way forward after the summer.

# Preparatory note Workshop A

# Creating effective MLA processes for e-evidence

7 March 2016

**Subject of this workshop**

This workshop focusses on possible innovations in the Mutual Legal Assistance (MLA) processes in order to accommodate specific needs in gathering electronic data. The aim is to provide for the optimum use of MLA instruments in cyberspace.

This workshop addresses both existing MLA treaties used within the EU and in the relations of EU (member states) with third countries. It also will deal with more recent instruments of mutual recognition, including the European Investigation Order, of which the implementation date expires in one year.

This workshop does not discuss direct contact with internet service providers established in another territory than the requesting state. The parallel workshop, Workshop B, is dedicated to this issue. Furthermore, in this workshop the requesting and requested states are assumed to be known. Situations where a so called "loss of location" is recognized are dealt with in Workshop C.

**MLA and the challenge of digitalisation**

International cooperation in criminal investigations and judicial proceedings has so far been undertaken within different frameworks, corresponding to different courses of action. In short, we can distinguish the following instruments:

1. MLA, usually based on a mutual legal assistance treaty (MLAT),
2. mutual supranational data sharing, often in an institutionalised setting, including multilateral databases (SIS), matching of national databases (Prüm), and bodies to facilitate information exchange between countries, such as Interpol, Europol, and Eurojust
3. extraterritorial investigation, in which officials from state A perform or assist in investigative activities in state B, such as (short term) cross border hot pursuit, or police and judicial liaison officers;
4. joint supranational investigations, such as EU Joint Investigation Teams.

The dominant interpretation of international law implies that accessing data that are, or later turn out to be, stored on a server located in the territory of another state without the prior consent of that state constitutes a breach of the territorial sovereignty of that state and thus a wrongful act.
Therefore, states resort to traditional procedures for MLA in cases where evidence-gathering powers extend beyond national borders. In the context of rapid digitalisation, these traditional procedures for gathering digital evidence turn out to be increasingly problematic in practice.
Obstacles identified relate to the inability to get a timely response to a request, to the formalities and paperwork involved, to the limited capacity and inadequate level of knowledge in requested countries, legal obstacles such as dual criminality, the absence of arrangements for expeditious action, and lack of coordination. Despite efforts to streamline and facilitate MLA in cyber-investigation, the procedures remain inadequate in situations in which there is a need for expeditious data gathering, or where (cyber)criminals move data around with high frequency.
Due to the difficulties of MLA procedures, practitioners sometimes resort to investigative (e.g. internet or interception) activities on foreign territory without formal authorisation, although they often consult with local investigation officers in the foreign state.

**Location of data and consequences for international cooperation**

A discussion on the use of MLA procedures not only has practical aspects. It also requires a critical assessment of how MLA procedures should be applied in cyberspace.
In which circumstances MLA is needed traditionally depends on the location where the evidence is to be found, and the jurisdiction to enforce of the investigating authorities. Depending on whether this location is within or outside of the territory of the investigating authorities international cooperation will be required. This question has become more complex and a variety of answers is possible for digital evidence.
For digital evidence various approaches exist in addition to the traditional object-oriented approach for defining jurisdiction to enforce.

Options include:

- The country where the data is physically stored (this could raise issues when data packets are automatically stored in different countries),
- The country where the private party resides,
- The country where the investigated person uses the services of the private party,
- Location of habitual residence of the investigated person
- The country where the production order is to be executed (i.e. where an employee is physically present and will retrieve the data).

The issue of location can become very frustrating for law enforcement officials when the suspect, the victim and the crime committed are all in his own country, but the evidence is in another. Other factors than the location of the storage of data could be more relevant.

**Developments in the EU**

Within the EU over the last decades a transition can be identified from traditional MLA mechanisms, where the requested State has a wide discretion to comply with the request of another State, to the acceptance of the principles of mutual recognition and mutual trust where each State in principle recognises and executes a request coming from another Member State.

Also the EU has shown flexibility with regard to the object oriented approach to procedural jurisdiction. For example, with regard to wiretap competences the EU has put forward the location of the person whose communication is intercepted as a localisation criterion.

As noted in the Luxembourg paper and discussed in the informal meeting of EU ministers of Justice in Amsterdam on January 26, the borderless nature of cyberspace poses special challenges for law enforcement and judicial authorities, often leading to impunity. The ministers find this unacceptable. They call for urgent improvement of law enforcement and judicial action in cyberspace. They have asked for analysis and recommendations to improve the effectiveness of existing instruments. Options to assure the timely and effective access to data stored by internet service providers in other countries are to be examined. Clear, unambiguous procedures and regulations are needed. The cooperation with third states, especially the US, should have close attention.

**Proposals MLA improvements within the EU**

1. Create the possibility for tracking MLA requests (notice of receipt, updates, specified and previously communicated grounds for refusal)
2. Digitalize MLA processes (possibility of developing a common EU portal for MLA requests)
3. Increase capacity law enforcement (training and allocating more technology-literate staff)
4. Streamline procedures (include legal justification, uniform request format, automatic translation or in English language)
5. MLA cleaning: shorten lengthy MLA information to the core (what crime, which specific information is needed, etc).
6. Increase the effective implementation of the 24/7 contact points
7. Clear rules for when MLA is used (and when not: police-to-police or direct access). A distinctions could be made between types of data (between content, traffic and subscriber data, between real time and ex post data) and distinctions between powers used (production orders/search and seizure for example).
8. Develop emergency procedures for requests related to risk of life and similar exigent circumstances
9. Opening of domestic investigations upon a foreign request or spontaneous information to facilitate the sharing of information or accelerate MLA (TCY)
10. Apply dual criminality standard in a flexible manner (TCY)

**Way forward**

What factors besides territoriality could be helpful to determine the relevant investigative powers?

Would a distinction between types of data and between powers used be helpful?

What existing proposals for MLA improvement are most relevant or helpful and should be implemented urgently within the EU?

Would a distinction between types of data and between powers used be helpful?

What elements should a uniform request format contain?

Would the development of a common EU portal for MLA request be a constructive option?

## Preparatory note Workshop B

## Conflicting regulations hamper cooperation with private parties

7 March 2016

**Subject of this workshop**

Conflicting regulations hamper cooperation with private parties. Internet service providers, especially those providing cloud computing services, often do not store information about clients and their activities in the countries where those clients are. Those private companies may be established in one country and provide their services in others. Suspects of criminal investigations can be located in one country while information about them is in another, and the service provider is established in a third country. It can be necessary for law enforcement and judicial authorities to request information physically stored in other countries. For law enforcement organisations MLA procedures can be too cumbersome and time consuming to be effective, leaving crime unpunished too often. For internet service providers, differences in regulations between those countries can become an obstacle for cooperation. Complying with a request for data in one country could imply breaking the law in the other.

This preparatory note aims to support the discussions in the expert workshop. It draws on papers submitted for the jurisdiction conference and previous work, mostly from the Cybercrime Convention Committee and its working groups at the Council of Europe. It presumes basic concepts to be well known to the participants. Its content does not describe the views of its authors or any government position.

**Developments**

In the absence of a clear framework for obtaining evidence across borders, two developments are especially relevant:

- Law enforcement authorities use national law and national courts to assure compliance by private parties. National law may then require using investigative powers that collect evidence present in another country. In the case of Yahoo!, the Belgian Supreme Court ruled that, since Yahoo! aimed its activities at Belgium and was active there, it should comply to Belgian law, regardless of the formal residence of Yahoo! or the location where it stores its data. In the case of Microsoft, courts in the US have decided that Microsoft should comply with orders from the US authorities, regardless of where the data is stored.
- Law enforcement authorities approach private parties for voluntary cooperation. Although in many cases this helps to obtain evidence, there are serious disadvantages to this approach. First, it forces private parties in a position to decide whether to cooperate. They are currently forced to use their own criteria for these decisions, leading to different outcomes in different cases, without proper democratic or judicial oversight. Second, without a legally binding duty to comply, private parties can be vulnerable to legal action from customers whose data is made available to foreign authorities. Voluntary cooperation is therefore not a satisfactory solution.

**Location: what is where?**

The borderless nature of the internet does not correspond well to the concept of territorial jurisdiction. This becomes especially apparent when trying to determine where an investigative power will be used. A private party can be active in many countries, and in many different ways. If for example a production order, or search and seizure is to be issued, where will that power be used? And the authority in which country should order it? Different options are possible, for example:

- The country where the data is physically stored (this could raise issues when data packets are automatically stored in different countries),
- The country where the private party resides,
- The country where the investigated subject uses the services of the private party,
- Location of habitual residence of the investigated person
- The country where the production order is to be executed (i.e. where an employee is physically present and will retrieve the data).

The issue of location can become very frustrating for law enforcement officials when the suspect, the victim and the crime committed are all in his own country, but the evidence is in another. Other factors than the location of the storage of data could be more relevant. Moreover, it could be questioned what data protection laws are applicable. In the case of Yahoo! the Belgian court considered the retrieval of data stored in the US, executed in Belgium, not a material act in the US.

**Safeguards and conditions, types of data**

Legal systems differ in the applicable conditions and safeguards for obtaining data for law enforcement purposes. These conditions and safeguards reflect the outcome of democratic decision making, and they should make sure fundamental human rights and the protection of data is taken into account appropriately. Usually, the greater the infringement on the privacy of the subject, the stricter the conditions and safeguards will be. The infringement on privacy is different for different types of data, e.g. subscriber data, traffic data and content data. The difference between ex post and real time data can also be relevant. A comprehensive regime for obtaining e-evidence across borders could reflect these differences. For different types of data, conditions and safeguards could be determined separately. In their paper Daskal and Woods mentioned that the following factors should be taken into account: authorization, cause, particularity, legality, severity, notice, speech, minimization, emergency, transparency, audits and sanctions.[3]

**Way forward**

What factors besides territoriality could be helpful to determine the location relevant for investigative powers?

What elements should a regime for obtaining e-evidence across borders contain?

How can proper safeguards and conditions be put in place without resorting to MLA procedures?

How could a differentiation between types of data be envisaged in practice?

What are the most important differences in regulations between EU-countries?

Can the European Investigation Order be used as an inspiration for discussions with countries outside the EU?

[3] Daskal, J., and A.K. Woods (2015), "Cross-Border Data Requests: A Proposed Framework", *Lawfare*, November 2015.

## Preparatory note Workshop C

## Crime from nowhere: Legal challenges from unknown locations

7 March 2016

**Subject of this workshop**

This workshop discusses jurisdiction in situations in which MLA is not possible. These situations can arise when it is not, or not reasonably, possible to determine the location of data or the origin of a cyber attack. Criminals can use technical means to hide themselves, their data and their infrastructure. It could also be possible that the location or origin is known, but in a country that does not respond properly to MLA requests, for example because of lack of capabilities or because the government chooses not to respond. Such a country can effectively become a safe haven for cyber criminals. These issues can lead to impunity and governments being unable to protect their businesses and citizens from crime.

This workshop aims to identify possible solutions to these issues by reviewing the application of the concepts of territoriality and sovereignty in cyberspace from a law enforcement perspective. This preparatory note aims to support the discussions in the expert workshop. It draws mostly on papers submitted for the jurisdiction conference and it presumes basic concepts to be well known to the participants. Its content does not describe the views of its authors or any government position.

**Rights and obligations of states**

In international law sovereignty creates various rights, for example the right of non-intervention. These rights limit the jurisdiction to enforce of other states. However, sovereignty also creates obligations. One example is the obligation to protect society and individuals against crime, while respecting the rule of law and human rights standards. For this obligation, securing evidence on computer systems has become essential. Another example is the obligation to prevent harm to other states from activities originating from its territory.

While jurisdiction is linked to territoriality, it is not exclusively tied to it. In some cases, states would be entitled to exercise jurisdiction over a conduct that does not take place within its territory, but produces harmful effects there. In cybercrime cases, criminals and victims are often not in the same country, which raises the question how the rights and obligations of sovereign states should be interpreted in cyberspace.

**Location and views on LEA activity in cyberspace**

If a police officer logs into a computer system in another country, where is he doing that? Is he searching for data abroad, or at his own police station? The way we describe what actually happens often determines our view of the legal reality. In most discussions, terms like “entering computer systems” or “breaking into” them are used. However, there is no-one physically entering the system or breaking into it. It could be helpful to describe what happens more precisely. For example, if a computer system is being approached, what really happens is that a person sends a coded message (from his own computer) to that system and receives a response (from that system). The messages can be meant to make the system response like it is intended to do, or they can be meant to “fool” the system. Taking into account the technicalities of LEA action acknowledges the specific characteristics of investigation in cyberspace. It enables a more accurate discussion on the admissibility of the search in international law.

**A breach of sovereignty**

In cyber investigations it is sometimes hard to determine what constitutes a breach of sovereignty. Several views are possible. First, any act that involves the territory of another state could be viewed as a breach. In this view, all investigative measures that involve data present on computer systems in other countries are illegal. A second view holds that there must be some form of material damage done in the other country to constitute a breach of sovereignty. In this view, there is no breach as long as there is no, or hardly any, negative impact on, or interference with, the computer system in the other country. A third view holds that a breach of sovereignty requires a severe amount of damage in the other country. In this view, most law enforcement powers can be used unilaterally. In the absence of a common understanding, states increasingly resort to their own interpretations on the jurisdiction to enforce in cyberspace.

**Alternative legal concepts**

Some authors have mentioned other cases in which territoriality was supplemented by other legal concepts to provide a new framework. One example is the concept of the high seas and free passage. It is noted that free passage is not an absolute right, and law enforcement activity is possible on the high seas for certain crimes, like piracy and slave trade, regardless of the flag of the suspected ship. Moreover, limited law enforcement powers were granted to maintain a minimum rule of law at sea, and the concept of hot pursuit was developed. A second example is the open skies / outer space framework, in which the disclosure of acquired images and data ensured the framework was mutually beneficial. When implemented thoughtfully, these views could enhance law enforcement investigations and increase the protection of personal data and fundamental rights. It could provide more clarity for people and organizations what legal framework is applicable on their data.

**Circumstances and conditions**

Regardless of views on location, sovereignty and what constitutes a breach, impunity is not acceptable. Therefore, common conditions and circumstances could be developed to determine in which cases cross border law enforcement activity is justified without prior consent of the other state. In literature, many are mentioned, for example:

- There is a clear connection between the matter and the investigating state
- The investigating state has a legitimate interest in the matter
- The interest of the state should be balanced against other interests
- The location of the data / origin of the attack is unknown and cannot reasonably be determined
- The location of the data / origin of the attack is (willfully) concealed by technical means
- The location of the data / origin of attack is effectively a safe haven
- The LEA activity limits itself to certain forms of data, e.g. subscriber data and metadata vs. content data, ex post vs. real time data

- The LEA activity has no material consequences / effect / damage in the other country
- The LEA activity will always respect the integrity of computer systems in another state, and do no damage to its functionality
- Other methods of acquiring the data would be disproportionate
- The nature and seriousness of the offence would justify the LEA activity
- Data would be used only for taking of measures destined to preserve the status quo, that is, so that the data could not be tampered with
- There is strong presumption that the time needed for resorting to a traditional procedure of letters rogatory would compromise the search
- The investigative authorities would inform the authorities of the other state
- Data would not be used unless the involved state would grant its consent
- All acquired data will be disclosed to the other state

**Way forward**

What parts of the discussions are most relevant or helpful?

What concepts would be most helpful to develop further?

What basic principles should be fundamental in further discussions?

Is it possible to determine what circumstances and conditions are most applicable?

Given the reciprocity of cross border activity, what would be acceptable from other states?