

Strasbourg, le 18 février 2013

T-CY (2013)04 F

Comité de la Convention sur la cybercriminalité (T-CY)

Évaluer la mise en œuvre de la Convention de Budapest sur la cybercriminalité

Questionnaire sur la coopération internationale

(article 31 avec référence aux articles 23, 25, 26, 27, 28 et 35)

CONTEXTE

Lors de sa 8^e session plénière (5-6 décembre 2012), le Comité de la Convention sur la cybercriminalité (T-CY) a décidé d'évaluer en 2013 l'efficacité des dispositions de la Convention de Budapest sur la cybercriminalité qui portent sur la coopération internationale, en s'appuyant notamment sur l'article 31 (entraide concernant l'accès aux données stockées).

Le Bureau du T-CY a préparé le présent questionnaire à sa réunion des 4-6 février 2013. Il a chargé le Secrétariat de l'envoyer aux représentants du T-CY (Etats parties et observateurs) avec copie aux Représentations permanentes avant le 20 février 2013, la date limite pour répondre étant fixée au 10 avril 2013.

BUT DE L'ÉVALUATION

L'un des principaux obstacles aux enquêtes, aux poursuites et aux sanctions dans les affaires de cybercriminalité ou d'autres infractions qui nécessitent des preuves électroniques est l'inefficacité de la coopération internationale. Les procédures d'entraide permettant d'obtenir des données stockées dans des juridictions étrangères sont jugées trop longues et complexes.

La Convention de Budapest sur la cybercriminalité, dans son article 31, prévoit une « entraide concernant l'accès aux données stockées » selon une procédure accélérée :

Article 31 – Entraide concernant l'accès aux données stockées

- 1 Une Partie peut demander à une autre Partie de perquisitionner ou d'accéder de façon similaire, de saisir ou d'obtenir de façon similaire, de divulguer des données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, y compris les données conservées conformément à l'article 29.
- 3 La demande doit être satisfaite aussi rapidement que possible dans les cas suivants :
 - a il y a des raisons de penser que les données pertinentes sont particulièrement sensibles aux risques de perte ou de modification ; ou
 - b les instruments, arrangements et législations visés au paragraphe 2 prévoient une coopération rapide.

Le but de l'évaluation est de trouver des solutions pour « accélérer » l'entraide (article 31) et d'accroître l'efficacité de la coopération internationale en général.

Il peut être utile d'évaluer l'article 31 dans le cadre plus vaste de la coopération internationale, c'est-à-dire en lien avec les articles 23, 25, 26, 27, 28 et 35 de la Convention de Budapest.

Dans vos réponses aux questions qui suivent, veuillez vous limiter à l'entraide visant à obtenir des données qui serviront d'éléments de preuve durant la procédure pénale (plutôt que pour une coopération entre polices).

MISE EN ŒUVRE

Les représentants du T-CY sont invités à préparer/rassembler les réponses consolidées au présent questionnaire en coopération avec les autorités de leurs pays respectifs.

Les réponses devront être envoyées au plus tard le **10 avril 2013** sous forme électronique, en anglais ou en français, à :

Alexander Seger, Secrétaire du Comité de la Convention Cybercriminalité, DG 1, Conseil de l'Europe, alexander.seger@coe.int

Les membres et les Etats observateurs du T-CY recevront ensuite, d'ici au 15 mai 2013, une compilation des réponses et un projet de résumé, pour commentaires, qui feront l'objet d'une discussion lors de la 9^e session plénière du T-CY les 4 et 5 juin 2013. Les Parties à la Convention de Budapest devront être prêtes à présenter leur système pendant cette réunion.

La version finale du rapport d'évaluation doit être adoptée lors de la 10^e session plénière en décembre 2013.

1 Informations sur la fréquence de l'entraide et les types de données stockées

1.1 Types de données stockées généralement demandées par la voie de l'entraide (par exemple renseignements sur l'abonné, données relatives au trafic, données relatives au contenu)

Q 1.1.1 Sur quel type de données stockées portent généralement les demandes que vous recevez ? Selon quelle fréquence ? Veuillez donner, si possible, des statistiques sur la fréquence/quantité de demandes.

Q 1.1.2 Sur quel type de données stockées portent généralement les demandes que vous adressez à d'autres pays ? Selon quelle fréquence ? Veuillez donner, si possible, des statistiques sur la fréquence/quantité de demandes.

1.2 Types d'infractions pour lesquelles des données stockées sont généralement demandées par la voie de l'entraide (veuillez donner des statistiques si possible)

Q 1.2.1 A quel type d'infractions sont généralement liées les demandes que vous recevez concernant des données stockées ? Veuillez donner des exemples.

Q 1.2.2 Lorsque vous adressez à d'autres Parties des demandes concernant des données stockées, sur quelles infractions ces demandes portent-elles généralement ? Veuillez donner des exemples.

1.3 Entraide contre coopération entre polices

Q 1.3.1 Sur la base de la législation de votre pays et de votre expérience pratique, quelle différence faites-vous entre l'entraide et l'échange d'informations entre polices concernant des données informatiques stockées ?

Q 1.3.2 Quel type d'informations (y compris des données informatiques stockées) pourriez-vous transmettre dans le cadre de la coopération entre polices en l'absence ou en amont d'une demande d'entraide ? A quelles conditions serait soumise la transmission de ces informations ?

1.4 Information spontanée (article 26)

Q 1.4.1 L'article 26 porte sur l'envoi d'informations à un autre Etat en l'absence de demande d'entraide. Selon quelle fréquence envoyez-vous ou recevez-vous des informations spontanées ?

Q 1.4.2 D'après votre expérience, quelle est l'utilité de ces informations et quelles suites leur donnez-vous ? Veuillez donner des exemples pour illustrer la façon dont cette possibilité est utilisée.

2 Procédures et critères

2.1 Critères à respecter pour exécuter une demande d'entraide

Q 2.1.1 Lorsque vous recevez une demande concernant des données informatiques stockées, quels critères formels, juridiques ou autres devez-vous respecter pour pouvoir exécuter la demande ? Veuillez donner des exemples, y compris sur des demandes que vous avez dû rejeter.

Q 2.1.2 Quel est le fondement juridique qui vous permet d'exécuter ce type de demande ? Veuillez joindre en annexe le texte des dispositions légales pertinentes.

2.2 Motifs de refus de coopérer

Q 2.2.1 Les Parties qui reçoivent une demande peuvent refuser de coopérer dans certaines circonstances (voir par exemple les articles 25.4 et 27.4 de la Convention de Budapest). Veuillez énumérer les motifs de refus et donner des exemples de demandes que vous avez refusé d'exécuter.

2.3 Langue de la demande

Q 2.3.1 Lorsque vous recevez une demande, quelles sont vos exigences concernant la langue ?

Q 2.3.2 Quelle est l'ampleur du problème de la traduction depuis et vers les langues étrangères sur les plans du temps, de l'argent et de la qualité ? Quelles solutions proposeriez-vous pour y remédier ?

2.4 Procédure : procédure pas à pas pour envoyer/recevoir une demande et suites données aux demandes

Q 2.4.1 En tant qu'Etat requis : veuillez décrire pas à pas la procédure complète que vous devez suivre lorsque vous recevez une demande concernant des données informatiques stockées.

Q 2.4.2 En tant qu'Etat requérant : veuillez décrire pas à pas la procédure complète que vous devez suivre lorsque vous envoyez une demande concernant des données informatiques stockées.

2.5 Principaux problèmes en matière d'entraide concernant l'accès aux données stockées

Q 2.5.1 Quels sont les principaux problèmes auxquels vous êtes confronté en tant qu'Etat requérant ? Veuillez donner des détails et des exemples.

Q 2.5.2 Quels sont les principaux problèmes auxquels vous êtes confronté en tant qu'Etat requis ? Veuillez donner des détails et des exemples.

3 Voies et moyens de coopération

3.1 Voies, méthodes et moyens de coopération (voir aussi art. 25.3, 27.2 et 27.9)

Q 3.1.1 Veuillez confirmer que les informations relatives aux autorités compétentes figurant dans les déclarations¹ faites lors de la ratification de la Convention de Budapest ou lors de l'adhésion à la Convention sont applicables aux articles 24 (extradition), 27 (entraide) et 35 (réseau 24/7). Voir le tableau de synthèse à l'Annexe 2.

Q 3.1.2 Quels voies, procédures et moyens (fax, courrier électronique ou autre) de coopération utilisez-vous généralement pour demander par la voie de l'entraide des données informatiques stockées dans un autre Etat ?

Q 3.1.3 Quels sont les critères pour considérer une demande comme « urgente » ?

Q 3.1.4 En tant qu'Etat requérant : utilisez-vous des mécanismes, procédures ou canaux différents si vous considérez que votre demande est « urgente » ?

Q 3.1.5 En tant qu'Etat requis : utilisez-vous des mécanismes, procédures ou canaux différents pour exécuter une demande considérée comme « urgente » ?

3.2 Rôle des points de contact 24/7 en matière d'entraide (relation entre les articles 35 et 31 de la Convention de Budapest)

Q 3.2.1 Votre point de contact 24/7 est-il habilité à envoyer ou recevoir une demande d'entraide ? Si oui, veuillez expliquer quel est son rôle, y compris dans l'exécution de la demande.

Q 3.2.2 Si le point de contact 24/7 n'est pas compétent en matière d'entraide, veuillez expliquer comment il agit en coordination avec les autorités compétentes dans ce domaine selon une procédure accélérée (article 35.2b). Veuillez décrire la relation entre les deux services et la manière dont la coopération pourrait être améliorée afin d'accélérer l'exécution des demandes d'entraide.

¹ <http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=185&CM=8&DF=&CL=ENG&VL=1>

3.3 Contact direct pour obtenir des données auprès de personnes morales ou physiques

Q 3.3.1 La législation de votre pays vous autorise-t-elle à contacter directement des détenteurs de données (comme des fournisseurs de services internet) dans des juridictions étrangères pour obtenir des données stockées ? Si oui :

- à quelles conditions ?
- pour quel type de détenteurs de données (fournisseurs de services internet, autres entités du secteur privé, personnes physiques) ?
- y a-t-il des différences selon le type de données demandées (abonné, trafic, contenu) ?

Q 3.3.2 La législation de votre pays autorise-t-elle les services répressifs étrangers à contacter directement des détenteurs de données dans votre Etat ? Si oui :

- à quelles conditions ?
- pour quel type de détenteurs de données (fournisseurs de services internet, autres entités du secteur privé, personnes physiques) ?
- y a-t-il des différences selon le type de données demandées (abonné, trafic, contenu) ?

Q 3.3.3 Si non, quelles sont les sanctions ?

3.4 Coordination d'affaires complexes concernant plusieurs pays

Q 3.4.1 Quels mécanismes existe-t-il dans votre pays pour coordonner les affaires complexes exigeant une action concertée (comme des perquisitions) dans plusieurs Etats ?

4 Solutions

4.1 Solutions proposées

Q 4.1.1 Que proposez-vous pour améliorer l'efficacité de l'entraide visant à obtenir des données stockées ?

Annexe 1: Extraits de la Convention de Budapest sur la Cybercriminalité

Article 31 – Entraide concernant l'accès aux données stockées

- 1 Une Partie peut demander à une autre Partie de perquisitionner ou d'accéder de façon similaire, de saisir ou d'obtenir de façon similaire, de divulguer des données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, y compris les données conservées conformément à l'article 29.
- 2 La Partie requise satisfait à la demande en appliquant les instruments internationaux, les arrangements et les législations mentionnés à l'article 23, et en se conformant aux dispositions pertinentes du présent chapitre.
- 3 La demande doit être satisfaite aussi rapidement que possible dans les cas suivants:
 - a il y a des raisons de penser que les données pertinentes sont particulièrement sensibles aux risques de perte ou de modification; ou
 - b les instruments, arrangements et législations visés au paragraphe 2 prévoient une coopération rapide.

Rapport explicatif

Entraide concernant l'accès aux données stockées (article 31)

292. Chaque partie doit avoir la capacité, au bénéfice de l'autre, de perquisitionner ou d'accéder par un moyen similaire, de saisir ou d'obtenir par un moyen similaire, et de divulguer des données stockées au moyen d'un système informatique se trouvant sur son territoire – tout comme elle doit, en vertu de l'article 19 (Perquisition et saisie de données informatique stockées), avoir la capacité de le faire à des fins nationales. Le paragraphe 1 autorise une Partie à demander ce type d'entraide et le paragraphe 2 exige de la Partie requise qu'elle se donne les moyens de la fournir. Par ailleurs, le paragraphe 2 est conforme au principe selon lequel les conditions dans lesquelles cette coopération doit être fournie sont celles qu'énoncent les traités, arrangements et législations nationales applicables concernant l'entraide judiciaire en matière pénale. En vertu du paragraphe 3, il doit être satisfait rapidement à une telle demande lorsque 1) il y a des raisons de penser que les données pertinentes sont particulièrement susceptibles de perte ou de modification, ou 2) les traités, arrangements ou législations prévoient une coopération rapide.

Article 23 – Principes généraux relatifs à la coopération internationale

Les Parties coopèrent les unes avec les autres, conformément aux dispositions du présent chapitre, en application des instruments internationaux pertinents sur la coopération internationale en matière pénale, des arrangements reposant sur des législations uniformes ou réciproques et de leur droit national, dans la mesure la plus large possible, aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et des données informatiques ou pour recueillir les preuves, sous forme électronique, d'une infraction pénale.

Article 25 – Principes généraux relatifs à l’entraide

- 1 Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale.
- 2 Chaque Partie adopte également les mesures législatives et autres qui se révèlent nécessaires pour s'acquitter des obligations énoncées aux articles 27 à 35.
- 3 Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris, si nécessaire, le cryptage), avec confirmation officielle ultérieure si l'Etat requis l'exige. L'Etat requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication.
- 4 Sauf disposition contraire expressément prévue dans les articles du présent chapitre, l'entraide est soumise aux conditions fixées par le droit interne de la Partie requise ou par les traités d'entraide applicables, y compris les motifs sur la base desquels la Partie requise peut refuser la coopération. La Partie requise ne doit pas exercer son droit de refuser l'entraide concernant les infractions visées aux articles 2 à 11 au seul motif que la demande porte sur une infraction qu'elle considère comme de nature fiscale.
- 5 Lorsque, conformément aux dispositions du présent chapitre, la Partie requise est autorisée à subordonner l'entraide à l'existence d'une double incrimination, cette condition sera considérée comme satisfaite si le comportement constituant l'infraction, pour laquelle l'entraide est requise, est qualifié d'infraction pénale par son droit interne, que le droit interne classe ou non l'infraction dans la même catégorie d'infractions ou qu'il la désigne ou non par la même terminologie que le droit de la Partie requérante.

Article 26 – Information spontanée

- 1 Une Partie peut, dans les limites de son droit interne et en l'absence de demande préalable, communiquer à une autre Partie des informations obtenues dans le cadre de ses propres enquêtes lorsqu'elle estime que cela pourrait aider la Partie destinataire à engager ou à mener à bien des enquêtes ou des procédures au sujet d'infractions pénales établies conformément à la présente Convention, ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cette Partie au titre du présent chapitre.
- 2 Avant de communiquer de telles informations, la Partie qui les fournit peut demander qu'elles restent confidentielles ou qu'elles ne soient utilisées qu'à certaines conditions. Si la Partie destinataire ne peut faire droit à cette demande, elle doit en informer l'autre Partie, qui devra alors déterminer si les informations en question devraient néanmoins être fournies. Si la Partie destinataire accepte les informations aux conditions prescrites, elle sera liée par ces dernières.

Article 27 – Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

- 1 En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions des paragraphes 2 à 9 du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un

arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du reste de cet article.

- 2
 - a Chaque Partie désigne une ou plusieurs autorités centrales chargées d'envoyer les demandes d'entraide ou d'y répondre, de les exécuter ou de les transmettre aux autorités compétentes pour leur exécution;
 - b Les autorités centrales communiquent directement les unes avec les autres;
 - c Chaque Partie, au moment de la signature ou du dépôt de ses instruments de ratification, d'acceptation, d'approbation ou d'adhésion, communique au Secrétaire Général du Conseil de l'Europe les noms et adresses des autorités désignées en application du présent paragraphe;
 - d Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités centrales désignées par les Parties. Chaque Partie veille en permanence à l'exactitude des données figurant dans le registre.
- 3 Les demandes d'entraide sous le présent article sont exécutées conformément à la procédure spécifiée par la Partie requérante, sauf lorsqu'elle est incompatible avec la législation de la Partie requise.
- 4 Outre les conditions ou les motifs de refus prévus à l'article 25, paragraphe 4, l'entraide peut être refusée par la Partie requise:
 - a si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique; ou
 - b si la Partie requise estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.
- 5 La Partie requise peut surseoir à l'exécution de la demande si cela risquerait de porter préjudice à des enquêtes ou procédures conduites par ses autorités.
- 6 Avant de refuser ou de différer sa coopération, la Partie requise examine, après avoir le cas échéant consulté la Partie requérante, s'il peut être fait droit à la demande partiellement, ou sous réserve des conditions qu'elle juge nécessaires.
- 7 La Partie requise informe rapidement la Partie requérante de la suite qu'elle entend donner à la demande d'entraide. Elle doit motiver son éventuel refus d'y faire droit ou l'éventuel ajournement de la demande. La Partie requise informe également la Partie requérante de tout motif rendant l'exécution de l'entraide impossible ou étant susceptible de la retarder de manière significative.
- 8 La Partie requérante peut demander que la Partie requise garde confidentiels le fait et l'objet de toute demande formulée au titre du présent chapitre, sauf dans la mesure nécessaire à l'exécution de ladite demande. Si la Partie requise ne peut faire droit à cette demande de confidentialité, elle doit en informer rapidement la Partie requérante, qui devra alors déterminer si la demande doit néanmoins être exécutée.

- 9
- a En cas d'urgence, les autorités judiciaires de la Partie requérante peuvent adresser directement à leurs homologues de la Partie requise les demandes d'entraide ou les communications s'y rapportant. Dans un tel cas, copie est adressée simultanément aux autorités centrales de la Partie requise par le biais de l'autorité centrale de la Partie requérante.
 - b Toute demande ou communication formulée au titre du présent paragraphe peut l'être par l'intermédiaire de l'Organisation internationale de police criminelle (Interpol).
 - c Lorsqu'une demande a été formulée en application de l'alinéa a. du présent article et lorsque l'autorité n'est pas compétente pour la traiter, elle la transmet à l'autorité nationale compétente et en informe directement la Partie requérante.
 - d Les demandes ou communications effectuées en application du présent paragraphe qui ne supposent pas de mesure de coercition peuvent être directement transmises par les autorités compétentes de la Partie requérante aux autorités compétentes de la Partie requise.
 - e Chaque Partie peut informer le Secrétaire Général du Conseil de l'Europe, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, que, pour des raisons d'efficacité, les demandes faites sous ce paragraphe devront être adressées à son autorité centrale.

Article 28 – Confidentialité et restriction d'utilisation

- 1 En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du présent article.
- 2 La Partie requise peut subordonner la communication d'informations ou de matériels en réponse à une demande:
- a à la condition que ceux-ci restent confidentiels lorsque la demande d'entraide ne pourrait être respectée en l'absence de cette condition; ou
 - b à la condition qu'ils ne soient pas utilisés aux fins d'enquêtes ou de procédures autres que celles indiquées dans la demande.
- 3 Si la Partie requérante ne peut satisfaire à l'une des conditions énoncées au paragraphe 2, elle en informe rapidement la Partie requise, qui détermine alors si l'information doit néanmoins être fournie. Si la Partie requérante accepte cette condition, elle sera liée par celle-ci.
- 4 Toute Partie qui fournit des informations ou du matériel soumis à l'une des conditions énoncées au paragraphe 2 peut exiger de l'autre Partie qu'elle lui communique des précisions, en relation avec cette condition, quant à l'usage fait de ces informations ou de ce matériel.

Article 35 – Réseau 24/7

- 1 Chaque Partie désigne un point de contact joignable vingt-quatre heures sur vingt-quatre, sept jours sur sept, afin d'assurer une assistance immédiate pour des investigations concernant les

infractions pénales liées à des systèmes et à des données informatiques, ou pour recueillir les preuves sous forme électronique d'une infraction pénale. Cette assistance englobera la facilitation, ou, si le droit et la pratique internes le permettent, l'application directe des mesures suivantes:

- a apport de conseils techniques;
 - b conservation des données, conformément aux articles 29 et 30;
 - c recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects.
- 2
- a Le point de contact d'une Partie aura les moyens de correspondre avec le point de contact d'une autre Partie selon une procédure accélérée.
 - b Si le point de contact désigné par une Partie ne dépend pas de l'autorité ou des autorités de cette Partie responsables de l'entraide internationale ou de l'extradition, le point de contact veillera à pouvoir agir en coordination avec cette ou ces autorités, selon une procédure accélérée.
- 3
- Chaque Partie fera en sorte de disposer d'un personnel formé et équipé en vue de faciliter le fonctionnement du réseau.
-

Annexe 2: Autorités compétentes et points de contact 24/7

Pays	Autorités d'entraide judiciaire en l'absence d'autres traités (article 27)	Autorité pour l'extradition et les arrestations provisoires en l'absence d'autres traités (article 24)	Point de contact 24/7 (article 35)
Albanie	Ministry of Justice, Bulevardi Zog. I., Tirana	Ministry of Justice, Bulevardi Zog. I., Tirana National Central Office of Interpol, Bulevardi Deshmoret e Kombit, Tirana	Sector against Computer Crime, Ministry of Interior Tirana, Albania
Allemagne	Ministry of Foreign Affairs Address: Auswärtiges Amt, Werderscher Markt 1, 10117 Berlin	Ministry of Foreign Affairs Address: Auswärtiges Amt, Werderscher Markt 1, 10117 Berlin	National High Tech Crime Unit at the Federal Criminal Police Office 65193 Wiesbaden
Arménie	Main Department on Combat Against Organized Crime of the Police of the Republic of Armenia	Main Department on Combat Against Organized Crime of the Police of the Republic of Armenia	Division on High-tech Crime, Main Department on Combat Against Organized Crime of the Police of the Republic of Armenia
Australie	International Crime Cooperation Central Authority Attorney-General's Department 3-5 National Circuit Barton ACT 2600 Australia	International Crime Cooperation Central Authority Attorney-General's Department 3-5 National Circuit Barton ACT 2600 Australia	AOCC Watchfloor Operations Australian Federal police GPO Box 401 Canberra ACT 2601 Australia
Autriche	<i>Bundesministerium für Justiz</i> (Federal Ministry of Justice) Abt. IV 4 <i>Internationale</i> <i>Strafsachen</i> (International Criminal Matters) 1070 Wien, Museumstrasse 7 Tel.: +43 1 52 1 52-0 E-Mail: team.s@bmj.gv.at	<i>Bundesministerium für Justiz</i> (Federal Ministry of Justice) Abt. IV 4 <i>Internationale</i> <i>Strafsachen</i> (International Criminal Matters) 1070 Wien, Museumstrasse 7 Tel.: +43 1 52 1 52-0 E-Mail: team.s@bmj.gv.at z	<i>Bundesministerium für</i> <i>Inneres</i> (Federal Ministry of the Interior) <i>Bundeskriminalamt</i> (Federal Criminal Police Office) Büro 5.2 Cyber-Crime- Competence-Center Josef Holaubek Platz 1 1090 Wien
Azerbaïdjan	Ministry of National Security Address: 2, Parliament Avenue, Baky, AZ 1006, Republic of Azerbaijan; e-mail: secretoffice@mns.gov.az	Ministry of Justice Address: 1, Inshaatchilar Avenue, Baky, AZ 1073, Republic of Azerbaijan; e-mail: contact@justice.gov.az	Department of Combating Crimes in Communications and IT Sphere, Ministry of National Security
Belgique	Service Public Fédéral Justice Service de la coopération	Service Public Fédéral Justice Service de la coopération	Federal Computer Crime Unit

	internationale pénale Boulevard de Waterloo 115 1000 Bruxelles Fax : +32(0)2/210.57.98	internationale pénale Boulevard de Waterloo 115 1000 Bruxelles Fax : +32(0)2/210.57.98	
Bosnie- Herzégovine	State Investigation and Protection Agency of Bosnia and Herzegovina. Director of the Sarajevo Regional Office	State Investigation and Protection Agency of Bosnia and Herzegovina. Director of the Sarajevo Regional Office	International Police Cooperation Sector, Interpol Sarajevo, Ministry of Security
Bulgarie	Ministry of Justice (trial stage), Supreme Cassation Prosecutor's Office (pre-trial stage)	Ministry of Justice (extradition), Supreme Cassation Prosecutor's Office (provisional arrests)	National Service for Combating Organized Crime under the Ministry of Interior
Chypre	Ministry of Justice and Public Order Athalassas Av. 125 1461 NICOSIA	Ministry of Justice and Public Order Athalassas Av. 125 1461 NICOSIA	Office for Combating Cybercrime and Forensic Laboratory, Cyprus Police Headquarters Ministry of Justice and Public Order Athalassas Av. 125 1461 NICOSIA
Croatie	Ministry of Justice, Dezmanova 6, 10 000 Zagreb	Ministry of Justice, Dezmanova 6, 10 000 Zagreb	Ministry of Interior, Police - Directorate for crime police, Ilica 335, 10 000 Zagreb
Danemark	Ministry of Justice, Slotsholmsgade 10, DK-1216 Copenhagen K, Denmark	Ministry of Justice, Slotsholmsgade 10, DK-1216 Copenhagen K, Denmark	Danish National Police, Police Department, Polititorvet 14, DK- 1780 Copenhagen V, Denmark
Espagne	Sub-Directorate General for International Legal Cooperation of the Ministry of Justice	Sub-Directorate General for International Legal Cooperation of the Ministry of Justice	High Technological Investigation Unit of the National Police
"Ex- république Yougoslave de Macédoine"	Ministry of Justice	Ministry of Justice	Basic Public Prosecutor's Office Skopje Alternative: Cybercrime Unit, Ministry of Interior
Estonie	Ministry of Justice	Ministry of Justice	Bureau of Criminal Intelligence, Criminal Police Department
Finlande	Ministry of Justice, Eteläesplanadi 10, FIN-00130 Helsinki	For requests for extradition, the Ministry of Justice, Eteläesplanadi 10, FIN-00130 Helsinki For requests for provisional arrest, the National Bureau of Investigation, Jokiniemenkuja 4, FIN-01370 Vantaa	National Bureau of Investigation, Criminal Intelligence Division / Communications Centre
France	From French judicial authorities directed to foreign judicial authorities transmitted through the Ministry of Justice (<i>Ministère de la Justice, 13, Place</i>	Ministry for Foreign Affairs for extradition (<i>Ministère des Affaires étrangères, 37, Quai d'Orsay, 75700 Paris 07 SP</i>); The territorially competent State	Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication"

	<p><i>Vendôme, 75042 Paris Cedex 01)</i></p> <p>From foreign judicial authorities directed to French judicial authorities are transmitted through diplomatic channels (<i>Ministère des Affaires étrangères, 37, Quai d'Orsay, 75700 Paris 07 SP</i>)</p>	Prosecutor for requests for provisional arrest	(11, Rue des Saussaies, 75800 Paris)
Géorgie	<p>Ministry of Justice of Georgia 24a Gorgasali str. Tbilisi 0114 - Georgia Tel: +995322405143 - Fax: +995322405142 E-mail: international.psq@justice.gov.ge</p>	<p>Ministry of Justice of Georgia 24a Gorgasali str. Tbilisi 0114 - Georgia Tel: +995322405143 Fax: +995322405142 E-mail: international.psq@justice.gov.ge</p>	<p>Cybercrime Unit Ministry of Internal Affairs of Georgia Criminal Police Department 10 G. Gulua str. Tbilisi 0114 - Georgia</p>
Hongrie	<p>Before starting the criminal procedure: the Hungarian National Police International Implementing Co-operation Centre Budapest, Teve u. 4-6 1139 - Hungary After starting the criminal procedure: the General Prosecutor's Office of the Republic of Hungary Budapest, Markó u. 4-6 1055 - Hungary</p>	<p>Ministry of Justice for extradition or provisional arrest.</p> <p>The National Central Bureau of Interpol for provisional arrest.</p>	<p>International Law Enforcement Cooperation Centre, Police</p> <p>Alternative:</p> <p>High Tech Crime Unit, National Bureau of Investigations</p>
Islande	<p>Ministry of Justice, Skuggasundi, 150 Reykjavík, Iceland</p>	<p>Ministry of Justice, Skuggasundi, 150 Reykjavík, Iceland</p>	<p>National Commissioner of the Icelandic Police (Ríkislögreglustjórnin), Skúlagata 21, 101 Reykjavík, Iceland</p>
Italie	<p>Ministry of Justice Department for Affairs of Justice Directorate General of Criminal Justice Office II (International Judicial Cooperation) Viale Arenula 70 I - 00186 ROMA</p>	<p>Ministry of Justice Department for Affairs of Justice Directorate General of Criminal Justice Office II (International Judicial Cooperation) Viale Arenula 70 I - 00186 ROMA</p>	<p>Servizio Polizia Postale e delle Comunicazioni Ministry of the Interior</p> <p>Alternative: Office of District Attorney of Rome -Cybercrime Section</p>
Japon	<p>The Minister of Justice or the person designated by the Minister (Director of International Affairs Division) and The National Public Safety Commission or the person designated by the Commission (Director of International Investigative Operations Division) Organized Crime Department National Police Agency 2-1-2, Kasumigaseki Chiyoda-ku Tokyo 100-8974</p>	<p>The Minister for Foreign Affairs 2-2-1, Kasumigaseki Chiyoda-ku Tokyo 100-8919</p>	<p>International Investigative Operations Division Organized Crime Department National Police Agency 2-1-2, Kasumigaseki Chiyoda-ku Tokyo 100-8974</p>

Lettonie	Ministry of Justice Brivibas Blvd. 36, Riga LV-1536, Latvia	Prosecutor General Office Kalpaka Blvd. 6, Riga LV-1801, Latvia	International Cooperation Department of Central Criminal Police Department of State Police Brivibas Str. 61, Riga LV-1010, Latvia
Lituanie	Ministry of Justice and the General Prosecutor's Office of the Republic of Lithuania	Ministry of Justice and the General Prosecutor's Office of the Republic of Lithuania	Police Department under the Ministry of the Interior of the Republic of Lithuania
Malte	The Office of the Attorney General The Palace Valletta Malta Email: ag.mla@gov.mt	The Ministry for Justice Office of the Prime Minister Auberge de Castille Valletta VLT 2000 Malta	Cybercrime Unit Malta Police Police General Headquarters Floriana Malta
Moldavie	Office of the Prosecutor General in the phase of penal prosecution: 26, Banulescu - Bodoni str., MD-2012 Chisinau, Republic of Moldova. Ministry of Justice in the judiciary phase or the execution of punishment: 82, 31 August 1989 str., MD-2012 Chisinau, Republic of Moldova.	Office of the Prosecutor General in the phase of penal prosecution: 26, Banulescu - Bodoni str., MD-2012 Chisinau, Republic of Moldova. Ministry of Justice in the judiciary phase or the execution of punishment: 82, 31 August 1989 str., MD-2012 Chisinau, Republic of Moldova.	Direction of Prevention and Combating of Cybernetic, Information and Transnational Offences of the Ministry of Internal Affairs: 14, Bucuriei str., MD-2004 Chisinau, Republic of Moldova.
Monténégro	Ministry of Justice of Montenegro, address: Vuka Karadžica 3, 81 000 Podgorica	Ministry of Justice of Montenegro, address: Vuka Karadžica 3, 81 000 Podgorica For provisional arrest in the absence of an agreement: NCB Interpol in Podgorica, address: Bulevar Svetog Petra Cetinjskog 22, 81 000	Inspector for fighting cybercrime Police Directorate of Montenegro
Norvège	The National Criminal Investigation Service (KRIPOS)	Royal Ministry of Justice and the Police, P.O. Box 8005, N-0030 OSLO	High Tech Crime Division National Criminal Investigation Service (KRIPOS)
Pays-Bas	Landelijk Parket van het openbaar ministerie (National office of the public prosecution service) Postbus 395 3000 AJ ROTTERDAM	The Ministry of Justice Office of International Legal Assistance in Criminal Matters PO BOX 20301 2500 EH THE HAGUE	Landelijk Parket van het openbaar ministerie (National office of the public prosecution service) Postbus 395 3000 AJ ROTTERDAM
Portugal	Procuradoria-Geral da República (Rua da Escola Politécnica, 140 – 1269-269 Lisboa, Portugal)	Procuradoria-Geral da República (Rua da Escola Politécnica, 140 – 1269-269 Lisboa, Portugal)	Judiciary Police (Policia Judiciária) Rua Gomes Freire, 174 1169-007 Lisboa Portugal
République dominicaine	Procuradoria General de la Republica	Procuradoria General de la Republica	High Tech Crimes Investigation

	and High Tech Crimes Investigation Department (DICAT), National Police	and High Tech Crimes Investigation Department (DICAT), National Police	Department (DICAT), National Police, Santo Domingo, Dominican Republic
République slovaque	Ministry of Justice of the Slovak Republic (Zupné námestie 13, 81311 Bratislava) and the General Prosecutor's Office (Stúrova 2, 81285 Bratislava)	Ministry of Justice of the Slovak Republic (Zupné námestie 13, 81311 Bratislava) for extradition Competent prosecutor of the Regional Prosecutor's Office and the Ministry of Justice for receiving requests for provisional arrests Ministry of Justice of the Slovak Republic and the court competent for issuing an international arrest warrant	National Central Bureau Interpol Vajnorská 25812 72 BratislavaSlovakia
Roumanie	The Prosecutor's Office to the High Court of Cassation and Justice for pre-trial investigations (address: Blvd. Libertatii nr. 12-14, sector 5, Bucuresti) The Ministry of Justice for the requests during the trial or execution of punishment	Ministry of Justice (address: Str. Apollodor nr. 17, sector 5, Bucuresti)	Service of Combating Cybercrime within the Section for Combating Organised Crime and Drugs Trafficking to the High Court of Cassation and Justice (address: Blvd. Libertatii nr. 12-14, sector 5, Bucuresti).
Royaume- Uni	For matters related to England, Wales, and Northern Ireland: UK Central Authority Home Office 5th Floor Peel building 2 Marsham Street London SW1P 4DF For matters related to Scotland: International Co-operation Unit Argyle House C Floor 3 Lady Lawson Street Edinburgh EH3 9DR For matters related to indirect taxation: Law Enforcement & International Advisory Division HM Revenue and Customs – Solicitor's Office Room 2/74 100 Parliament Street London SW1A 2BQ	Home Office Judicial Co-operation Unit 5th Floor, Fry building 2 Marsham Street London SW1P 4DF Scottish Government (when the person is believed to be in Scotland) Criminal Procedure Division St. Andrew's House Regent Road Edinburgh EH1 3DG	Cyber Duty Officer SOCA Cyber
Serbie	District Attorney for High-Tech Crime of the Republic of Serbia Savska 17A 11000 Beograd	District Attorney for High-Tech Crime of the Republic of Serbia Savska 17A 11000 Beograd	District Attorney for High-Tech Crime of the Republic of Serbia Savska 17A 11000 Beograd

	Ministry of Interior of the Republic of Serbia Directorate of Crime Police Department for the fight against organized crime Bulevar Mihajla Pupina 2 11070 Novi Beograd	Ministry of Interior of the Republic of Serbia Directorate of Crime Police Department for the fight against organized crime Bulevar Mihajla Pupina 2 11070 Novi Beograd	T Ministry of Interior of the Republic of Serbia Directorate of Crime Police Department for the fight against organized crime Bulevar Mihajla Pupina 2 11070 Novi Beograd
Slovénie	Ministry of Justice Zupanciceva 3 SI - 1000 Ljubljana	Ministry of Foreign Affairs for extradition: Presernova 25 SI - 1000 Ljubljana Ministry of the Interior, Criminal Investigation Police Directorate, International Police Cooperation Section for requests for provisional arrests: Ministry of the Interior Criminal Investigation Police Directorate International Police Cooperation Section	Cyber Investigation Unit Criminal Police Directorate
Suisse	Federal Office of Justice, the Federal Department of Justice and Police, 3003 Berne	Federal Office of Justice, the Federal Department of Justice and Police, 3003 Berne	Operations Centre FEDPO Federal Office of Justice
Ukraine	Ministry of Justice of Ukraine (concerning courts' commission) and the General Prosecutor's Office of Ukraine (concerning commissions of bodies of prejudicial inquiry)	Ministry of Justice of Ukraine (concerning court's inquiries) and the General Prosecutor's Office of Ukraine (concerning inquiries of bodies of prejudicial inquiry)	Division for Combating Cybercrime, Ministry of Internal Affairs