Legal Cooperation to Investigate Cyber Incidents: Estonian Case Study and Lessons

Eneken Tikk and Kadri Kaska
Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia
eneken.tikk@ccdcoe.org
kadri.kaska@ccdcoe.org

Abstract: To investigate and prosecute the 2007 cyber attacks against its governmental and critical private information infrastructure, Estonia requested legal cooperation from the Russian Public Prosecutor's Office. This paper looks into the anatomy of this request and the Russian refusal to cooperate and suggests that in situations like the Estonian events in 2007, the lack of a legal mechanism or political willingness to cooperate equally result in the inability of the victim state to prosecute the cyber incidents. The paper also concludes that situations where a nation is depending on another sovereign's mercy may, in combination with the persistent trend of politically motivated cyber attacks, lead to a sense of fearlessness among patriotic hackers.

Keywords: State responsibility, criminal cooperation, cyber attacks, prosecution

1. Agreement on legal assistance between Estonia and Russia

According to article 3 of the Agreement on Mutual Legal Assistance between Estonia and Russia[1], signed in 1993, the states render each other legal assistance that includes procedural acts provided by law and conducted by the party who has received the request for mutual legal assistance. According to the abovementioned provision, the procedural activities covered by the agreement include interrogating parties, accused and accused at trial, witnesses and experts, as well as expert assessments, inspection by court, transfer of physical evidence, initiating a prosecution against the person who has committed a criminal offence, and criminal extradition, recognition and execution of court judgments in civil matters, service and transfer of documents and transfer of data on the punishment of the accused, as requested by the other party. The wording of the provision suggests that the list is non-exhaustive: this is indicated by both the phrase "such as" which introduces the list of procedural acts, and a general reference in the article to a mutual commitment to provide assistance in "procedural activities" (*protsessualnoje deistviye*).

In accordance with the aforementioned agreement, the Estonian Public Prosecutor's Office submitted a letter rogatory to the Russian Federation on 10 May 2007 in the course of investigation of the 2007 cyber attacks.[2]

The letter rogatory sought for assistance in conducting preliminary investigations in a criminal matter, more precisely, a procedural activity defined as 'identification of a person', with reference to the provisions in the Penal Code on the crimes of computer sabotage, damaging of connection to computer network, and the spread of computer viruses.[3]

The answer of the Russian Federation to the Public Prosecutor's Office on 28 June 2008 states that "the agreement stipulates that legal assistance shall be rendered in the framework of the procedural acts, according to the legal acts of the contracting party who has received a request, but it does not require cooperation in the field of operative prosecution measures (*operativno-rozysknye meropriyatiya*) in order to identify the location of a person'".

With reference to interviews with the officials of the Estonian Prosecutor General's Office, Russia's approach to this agreement is formally correct, but is not the inevitable one, especially taking into account cooperation practice with other countries with whom similarly phrased mutual assistance agreements exist.[4] Also, the interviews revealed that in practice, the Russian Federation has shown

[1] Agreement on Mutual Legal Assistance and Legal Relations in Civil, Family and Criminal Matters, signed on 26 January 1993. RT (State Gazette) II 1993, 16, 27; RT II 2002, 14, 58.

[2] Press release by the State Prosecutor's Office 2 May 2007, <www.prokuratuur.ee/28707>

[3] Articles 206, 207, 208 of the Penal Code (in the wording applicable at the time of the incident and until 24 March 2008), RT I 2001, 61, 364; 2007, 13, 69.

[4] The Estonian Central Criminal Police affirms that other countries have fulfilled requests based on similarly worded mutual legal assistance treaties.

no particular consistency in interpreting the mutual assistance agreements but has rather followed the interpretation that best corresponds to her will – or lack thereof – to cooperate in the particular matter. In its answer to the European Commission's inquiry on that subject, the Ministry of Justice pointed out the following issues with Russia regarding cooperation in criminal matters: [5]

- Revision of a letter rogatory generally takes much time and reminders are ignored;
- Assistance is refused for procedural activities regarding suspects; this is justified by referring to the fact that the notion of "suspect" does not exist in Russian legislation; also, Russia will not interrogate a person of Russian citizenship;
- A prior court ruling is required as a precondition for transferring of documents;
- Covert investigation is refused without a court order (in Estonia, the relevant authorisation is issued by the Public Prosecutor's Office);
- On occasions, Russia has insisted that a particular request be submitted through Interpol – this was also the case in relation to the letter rogatory concerning the April/May 2007 cyber attacks.

Based on the above, two legal positions with opposite effect seem possible on the applicability of the Agreement on Mutual Legal Assistance:

- A *narrow legal interpretation*, based on the view that the aim of the agreement between Estonia and Russia is to facilitate judicial proceedings; therefore, cooperation takes place mainly in pre-trial criminal procedure before judicial proceedings are initiated, presupposing that the person has already been identified. This interpretation is supported by article 60 section 1 subsection 5 of the Agreement on Mutual Legal Assistance, according to which the name of the suspect should be mentioned in the request to initiate criminal proceedings.
- A *broad legal interpretation*, based on the understanding that the objective of the Agreement on Mutual Legal Assistance between Estonia and Russia is to restrain crime in general; in that context, article 60 section 1 subsection 5 of the Agreement on Mutual Legal Assistance could be applied in the context of the circumstances related to the particular request for legal assistance, for instance, taking into account that the list in article 3 is non-exhaustive. From that point of departure, it is also possible to cooperate in activities not directly mentioned in the treaty.

In the latter case, one has to consider the possible counterarguments: the principle of legal clarity, and international obligations of the countries. Regarding the former, according to article 2 of the Estonian Code of Criminal Procedure[6] the sources of criminal procedural law are the Constitution of the Republic of Estonia; the generally recognised principles and provisions of international law, and international agreements binding on Estonia; the Code of Criminal Procedure and other legislation which provides for criminal procedure; and decisions of the Supreme Court in issues which are not regulated by other sources of criminal procedural law but which arise in the application of law. Therefore, any person subject to proceedings has to take into account the legal effects of the Estonian law as well as the treaties concluded with other countries to the extent that is predictable according to the relevant agreements.

In conclusion, it must be held that both interpretations can be supported and the first interpretation (the narrow one) is not by nature prevalent above the second (the broad). Therefore, it can be derived that the problematic interpretation of the Agreement on Mutual Legal Assistance between the Republic of Estonia and the Russian Federation is not determined by the ambiguity of the norms but is rather dependent on Russia's pragmatic will to (not) cooperate.

Cooperation in criminal matters is also possible on basis of other international legal instruments. Likewise, in the aforementioned context, there are sufficient arguments to support the second approach discussed above.

2. Other possibilities for international cooperation in criminal matters

In addition to bilateral legal agreements, there are multilateral treaties of various scopes of application, and other legal instruments dealing with cross-border investigation of cybercrimes. Professor R. Broadhurst holds the Council of Europe Convention on Cybercrime[7] and United Nations

[5] Ministry of Justice, 8 April 2008, letter No. 12-6/4620 *Re: judicial cooperation between Estonia and Russian Federation*.
[6] RT I 2003, 27, 166; RT I 2010, 8, 35
[7] *European Convention on Cyber Crime*, ratified on 12 December 2003, published in RT II 2003, 9, 32.

General Assembly Resolution on the protection of critical information infrastructure[8] to be the primary instruments among them.[9] Both are also discussed below.

2.1 The Council of Europe Convention on Cybercrime

The Council of Europe Convention on Cybercrime[10] is so far the only internationally binding instrument of international law specifically aimed against cybercrime. The convention lays down a foundation for developing a criminal policy on cybercrime that is consistent at the international level; it also defines prerequisites for international cooperation.

The convention is open for signature to all member states of the Council of Europe, as well as non-members. The total number of signatures as of May 2010 was 46, followed by 28 ratifications. Four non-member states of the Council of Europe (Canada, Japan, the Republic of South Africa, and the United States of America) have signed the treaty; the USA has also ratified it.

Russia has not ratified the convention; in fact, in 2008 President Putin withdrew the earlier order of 2005 regarding signature of the convention. The signature was related to the condition of Russia's success to obtain an amendment of article 32 section b,[11] which for Russia allegedly represented a potential danger to the sovereignty and security of the contracting states as well as to the rights of their citizens.[12]

The convention has been criticised because of its alleged imbalance, especially the fact that it does not sufficiently consider the need to protect personal privacy.[13] Although the convention refers to multiple international legal instruments and to those of the Council of Europe, for instance the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (1950), the United Nations International Covenant on Civil and Political Rights (1966) and the Council of Europe Convention for the Protection of Individuals with Regards to Automatic Processing of Personal Data (1981), it might be reasonable to analyse whether the rules aimed at the protection of privacy are enough considering the level of development of current electronic communications technology as well as the possibilities and risks related to service provision. If necessary, proposals should be considered to ascertain this balance by supplementing national law as well as international treaties.

2.2 Other / general conventions of the Council of Europe on criminal procedure

There are several conventions of the Council of Europe addressing the issue of cross-border legal/judicial cooperation in criminal matters[14]. The most relevant in the context of pre-trial investigation of cybercrime is the European Convention on Mutual Assistance in Criminal Matters with its additional protocols.[15] For Estonia, the convention entered into force in 1997[16] and for Russia, in

---

[8] UNGA Resolution 58/199. Creation of a global culture of cybersecurity and the protection of critical information infrastructures, 30 January 2004.

[9] Roderic Broadhurst, Queensland University of Technology: At the international level two new treaty instruments provide a sound basis for the essential cross-border law enforcement cooperation required to combat cyber crime. The first of these instruments, the Council of Europe's Cyber-crime Convention, is purpose built and although designed as a regional mechanism, has global significance. The second is the United Nations Convention against Transnational Organised Crime, which is global in scope but indirectly deals with cyber-crime when carried out by criminal networks in relation to serious crime.

[10] Council of Europe Internet Portal. Cybercrime. Standards: The Convention and its Protocol. <www.coe.int/t/DG1/LEGALCOOPERATION/ECONOMICCRIME/cybercrime/default_en.asp> 11.4.2008

[11] Putin defies Convention on Cybercrime. *Computer Crime Research Center*, March 28, 2008. <www.crime-research.org/news/28.03.2008/3277/>

[12] *Id.*[13] See for instance the common position of *Electronic Frontiers Australia and US Center for Democracy and Technology*: "The treaty is fundamentally imbalanced: it includes very detailed and sweeping powers of computer search and seizure and government surveillance of voice, email and data communications, but no correspondingly detailed standards to protect privacy and limit government use of such powers."

[14] See the list of treaties: <conventions.coe.int/Treaty/Commun/ListeTraites.asp?MA=20&CM=7&CL=ENG>, 11 April 2008.

[15] *European Convention on Mutual Assistance in Criminal Matters*, signed on 20 April 1959, Strasbourg. <conventions.coe.int/Treaty/en/Treaties/Html/030.htm>; *Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters*, signed on 17 March 1978, Strasbourg, <conventions.coe.int/Treaty/EN/Treaties/HTML/099.htm>; *Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters*, signed on 8 November 2001, Strasbourg. <conventions.coe.int/Treaty/EN/Treaties/HTML/182.htm>

[16] Estonia ratified the convention and its additional protocol on 19 February 1997, both of them entered into force for Estonia on 27 July 1997; the second additional protocol was ratified on 9 June 2004 and entered into force for Estonia on 23 July 2004. RT II 1997, 7, 36

2000.[17] Russia has not ratified the second additional protocol to the convention[18]; therefore, the discussion below follows the version of the convention that is binding for the relations between Estonia and Russia.

According to article 1 of the convention, the contracting parties undertake to afford each other the widest measure of mutual assistance in proceedings in respect of offences the punishment of which, at the time of the request for assistance, falls within the jurisdiction of the judicial authorities of the requesting Party. According to article 3.1, the requested Party shall execute in the manner provided for by its law any letters rogatory relating to a criminal matter and addressed to it by the judicial authorities[19] of the requesting Party for the purpose of procuring evidence, among other things. In chapter V of the convention regulating the procedure of cooperation in criminal matters, the framework for requests for mutual assistance is laid down; according to the list in article 14, the identification of the concerned person is not an essential condition of transmitting a legal assistance claim; nevertheless, the letter rogatory should include a reference to the criminal offence and a summary of facts. In addition, article 15.4 clearly refers to the possibility to request for investigation preliminary to prosecution; those requests may be communicated either directly between the judicial authorities[20] or through the International Criminal Police Organisation (Interpol). Articles 18 and 19 lay down that the authority which receives a request for mutual assistance shall transmit the request to the relevant authority and that reasons shall be given for any refusal of mutual assistance. According to article 2 of the convention, assistance may be refused in two cases: if the request concerns an offence which the requested Party considers a political offence, an offence connected with a political offence, or a fiscal offence (Russia has identified the criteria to determine the possible crimes that correspond to those characteristics in a declaration made to the convention); or if the requested Party considers that execution of the request is likely to prejudice the sovereignty, security, public order or other essential interests of herself as a receiving country. According to article 26 of the convention, the convention shall, in respect of those countries to which it applies, supersede the provisions of any treaties, conventions or bilateral agreements governing mutual assistance in criminal matters between any two Contracting Parties.

Therefore, the letter rogatory, transferred according to the Council of Europe Mutual Legal Assistance Convention, would in all likelihood not have given a justification for Russia's refusal to satisfy the request on grounds of the argument referred to in the first argumentation of the analysis. Nevertheless, taking into account Estonia's previous experience with letters rogatory submitted to Russia on the basis of the convention, as well as the bilateral Agreement on Mutual Legal Assistance, it would not have guaranteed a positive answer from Russia. The experience of the international legal cooperation department of the Estonian Ministry of Justice, whose task is to coordinate international cooperation in criminal matters, indicates a tendency of Russia to express a wide selection of creative reasons for refusing assistance in cases where cooperation is contrary to her interests. These were described, in generic terms, in the discussion quoting the letter from the Ministry of Justice to the European Commission[21]; specific examples include, *inter alia*, a proposal to annul a judgment of an Estonian court as a prerequisite for fulfilling the letter rogatory, referring to the fact that Russian legislation foresees such procedural activities at an earlier stage of criminal procedure.

Although the transfer of a letter rogatory according to the Agreement on Mutual Legal Assistance (and refusal on the letter) would not exclude further activities within the framework of the convention, in the case discussed in this article those were deemed unfruitful by the Public Prosecutor's Office as according to their evaluation, the refusal of Russia to grant the request were not based on a genuine judicial impediment but rather on an expression of will to not cooperate.

---

[17] Convention and its additional protocol are ratified on 10 December 1999.

[18] See the chart of signatures and ratifications at <conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=182&CM=1&DF=22/03/2010&CL=ENG>[19] In accordance with article 24 of the convention, Estonia has notified that competent authorities of Estonia responsible for carrying out the obligations under this convention are the courts, the Public Prosecutors' Office, the Ministry of Justice and the Ministry of Interior Affairs (instrument of ratification, deposited on 28 April 1997).

[20] According to the general rules of procedure, the Ministry of Justice of the requesting party sends a letter of claim or an application to the Ministry of Justice of the state to whom the claim is addressed, (article 15 paragraphs 2-4, 7).

[21] See *supra* note 5.

Therefore, while the question of whether the Agreement could be amended to better take into account the peculiarities of identifying persons is cyber crime cases could be answered in the positive – after all, the Agreement on Mutual Legal Assistance has been amended on one occasion in order to "enhance its efficiency"[22] – it is doubtful whether such an amendment would have more effect than dropping one item in the list of possible arguments for refusal. As explained above, the wording of the Agreement has not hindered procedural activities in cases where there is mutual interest for cooperation. A casuistic approach where refusals would give rise to a case-by-case review of the Agreement on Mutual Legal Assistance have more potential for producing a permanent state of review discussions than actual improvement in the cooperation practice.

2.3 International police cooperation through Interpol

Cooperation through Interpol enables the successful transfer to the law enforcement authorities of states that are members to the Interpol, inquiries and requests of professional assistance that could generally be performed (satisfied) without a sanction of a competent authority and without having to implement coercive measures.

In order to carry out a certain procedural act through Interpol, it is necessary to have a legal base in an international multilateral statutory act or in a bilateral agreement between the relevant parties; Interpol has no universal competence in the field of procedural activities.

As can be seen, cooperation through Interpol would in some cases enable to speed up law enforcement activities in cyber crime investigation, but recourse to Interpol cooperation could not have provided a qualitatively different result in the particular case due to the fact that Interpol cooperation largely relies on the very same treaty regimes than the pre-trial investigations, and is therefore likely to counter the same problems.

2.4 International soft law instruments

While soft law instruments of international organisations – such as recommendations, resolutions, standards, guidelines, etc – are merely of a recommendatory character, do not have a binding effect on national governments and are not enforceable in national courts, they do reflect a level of international consensus in a given matter and are expected to have an impact on international relations and the evolvement of international law. Considering this, it is justifiable to consider them in the interpretation of existing treaties in a way that strengthens rather than undermines the observance of a consensus understanding in international legal practice.

A number of international organisations are actively involved in the development of the global cyber environment in general and cyber security in particular. Some are more narrowly focused on security matters (such as NATO[23] or OSCE[24]), others have a wide-scope competence – such as the United Nations that gathers the widest auditorium of nations, or the Council of Europe[25] as a regional organisation.

In 2001, the United Nations General Assembly adopted a resolution on combating the criminal misuse of information technologies.[26] The resolution in particular highlights the need for adequate criminal law measures, placing special attention to strengthening law enforcement and national practice. According to the resolution, states should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies, and that mutual assistance regimes ensure the timely investigation of the criminal misuse of information technologies and the timely gathering

[22] Preamble of the Additional Protocol to the Agreement on Mutual Legal Assistance and Legal Relations in Civil, Family and Criminal Matters. Signed on 3 October 2001; RT II 2002, 14, 58.
[23] North Atlantic Treaty Organisation. Estonia is a NATO member since 2004; the Russian Federation participates in the Partnership for Peace (PfP) program since 1994.
[24] Operation for Security and Cooperation in Europe. Despite its name, the OCSE is the largest regional security organisation in the world with 56 participating states from Europe, Central Asia and North America. Estonia is a member since 1991; the Russian Federation (as a successor of the Union of Soviet Socialist Republics) since 1973.
[25] The Council of Europe involves 47 European countries as members. Estonia is a member since 1993; the Russian Federation since 1996.
26 A/RES/55/63: Combating the criminal misuse of information technologies. Resolution adopted by the General Assembly on the 81st plenary meeting on 4 December 2000; <www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf>

and exchange of evidence in such cases. Similar positions were upheld in the follow-on resolution of the General Assembly in 2003.[27]

These resolutions appear to give grounds for interpreting the agreements in a way that supports cooperation in identification of persons. Another deduction can be made from these provisions: replying to mutual assistance requests should occur without undue delay.

Likewise, the United Nations General Assembly resolution on a global culture of cyber security and the protection of critical information infrastructures[28] adopted in 2003 stresses the need for regional and international efforts to facilitate tracing of attacks on critical information infrastructures, disclosure of tracing information to other States where relevant, and having adequate substantive and procedural laws and trained personnel to enable States to investigate and prosecute attacks on critical information infrastructures and to coordinate such investigations with other States.[29] It is relevant to note that the resolution addresses critical information infrastructures in the widest sense, explicitly covering elements that fell target to the attacks in Estonia in 2007, such as banking and financial services. According to the resolution, it is up to each nation to determine its own critical information infrastructures, but a commitment to the activities listed above is without prejudice to the particular national definition of critical information infrastructure, its substance or procedure of its adoption.

The Council of Europe Convention on Cybercrime refers to the following recommendations of the Council of Europe:

- Recommendation No. R (85) 10 Concerning the Practical Application of the European Convention on Mutual Assistance in Criminal Matters in Respect of Letters Rogatory for the Interception of Telecommunications;
- Recommendation No. R (88) 2 on Measures to Combat Privacy in the Field of Copyright and Neighbouring Rights;
- Recommendation No. R (87) 15 Regulating the Use of Personal Data in the Police Sector;
- Recommendation No. R (95) 4 on the Protection of Personal Data in the Area of Telecommunication Services, with Particular Reference to Telephone Services;
- Recommendation No. R (89) 9 on Computer-related Crime that gives guidelines for governments of member states to define computer-related crimes;
- Recommendation No. R (95) 13 Concerning Problems of Criminal Procedure Law Connected with Information Technology.

Considering again the non-binding nature of these documents and the fact that Russia has declined to ratify the Cybercrime Convention and withdrawn her signature from the treaty, these documents offer little practical value in the particular disagreement over the Estonian 2007 letter rogatory regarding cyber attack investigations. However, considering a wider perspective, they provide useful support to the development of international practice regarding international cooperation in matters of cyber crime, and thereby help to shape international custom and a culture of cooperation.

3. Conclusions and proposals

While there is a significant number of legal instruments and mechanisms on international level intended to facilitate cooperation between nations in investigating and prosecuting crime, only a few of these instruments have been drafted with distinct regard to cyber crime. While not an impediment in itself, this factor may nonetheless be a root for problems in several regards.

Firstly, both the environment where cyber activities take place, and the activities themselves by nature disregard national boundaries. The interconnectedness of computer networks across service providers in different countries ensures smooth global service functionality, but with the same token, it

[27] A/RES/56/121: Combating the criminal misuse of information technologies. Resolution adopted by the General Assembly on the 88th plenary meeting on 19 December 2001; <www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf>. See section 2 in particular.

[28] A/RES/58/199: *Creation of a global culture of cybersecurity and the protection of critical information infrastructures*. Resolution adopted by the General Assembly on the 78th plenary meeting on 23 December 2003; <daccess-dds-ny.un.org/doc/UNDOC/GEN/N03/506/52/PDF/N0350652.pdf?OpenElement>

[29] See sections 7 and 9 of the Annex to the Resolution providing elements of protecting critical information infrastructures

also facilitates cyber activities of malicious nature. The networks and equipment that carry data from the point of origin via the most expedient route to its destination do not differentiate data flow by the geographic location of the network or equipment or the nationality of the service provider. With the possibility to direct data traffic through networks located in different countries, the actors can design, for a certain malicious purpose, a suitable cyber activity chain where the jurisdiction of the relevant players would first of all be difficult to detect and secondly, involve countries that have a favourable reputation of refusing cooperation.

This factor by itself makes the cyber realm especially sensitive to the efficiency of international cooperation in criminal matters.

There are ways to interpret the legal documents discussed above in a way allowing exchange of information and potentially supporting the chain of evidence to prosecute cyber criminals, but the margin of interpretation is rather broad. Even where the quality and degree of harmony of national substantive and procedural law are sufficient to investigate and prosecute a cyber offence, with a possibility to disguise political unwillingness into legal-technical arguments, is never certain that the criminal proceedings will not halt at a dead end. In the current context where politically motivated cyber attacks are a persistent trend, nations are more and more dependent on other jurisdictions' ability and willingness to cooperate in criminal proceedings.

Even more so, nations are not able to perform investigation beyond their jurisdictional boundaries and therefore have no effective way to prosecute perpetrators without assistance of other nations and international organisations.

It is too early to recommend specific remedies, such as the principle of comity to be applied in similar situations, but it is apparent that assistance in investigating politically motivated cyber incidents needs additional attention on international level in terms of both law and policy.