United Nations S/2004/22

Security Council

Distr.: General
13 January 2004

Original: English

Letter dated 7 January 2004 from the Chairman of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism addressed to the President of the Security Council

I write with reference to my letter of 9 October 2003 (S/2003/1007). The Counter-Terrorism Committee has received the attached fourth report from Estonia submitted pursuant to paragraph 6 of resolution 1373 (2001) (see annex). I would be grateful if you could arrange for the present letter and its annex to be circulated as a document of the Security Council.

(*Signed*) Inocencio F. **Arias**
Chairman
Security Council Committee established pursuant to
resolution 1373 (2001) concerning counter-terrorism

04-20591 (E) 100204

0420591

Annex

Note verbale dated 2 January 2004 from the Permanent Mission of Estonia to the United Nations addressed to the Chairman of the Counter-Terrorism Committee

The Permanent Mission of the Republic of Estonia to the United Nations presents its compliments to the Chairman of the Committee and has the honour to forward its fourth report regarding the implementation of resolution 1373 (2001) (see enclosure).

Enclosure

ESTONIA

On behalf of the Counter Terrorism Committee (CTC), I would like to thank you for your letter dated 6 March 2003 (S/2003/275) enclosing the third report of the Government of Estonia submitted in response to the letter from my predecessor as Chairman of the Committee, dated DDMM 200? (S/AC.40/2002/MS/OC.nn) pursuant to paragraph 6 of Resolution 1373 (the Resolution).

The CTC, with the assistance of its panel of experts, has considered carefully Estonia's previous reports and other relevant information.

The CTC, for the purposes of managing its work, has divided the implementation of the Resolution into three broad stages (Stages A, B and C). These stages correspond roughly to the different aspects of national activity aimed at raising counter-terrorist capacity, with each stage building on previous activity.

"Letter dated 16 January 2003 from the Chairman of the Security Council Committee established pursuant to Resolution 1373 (2001) concerning counter- terrorism addressed to the President of the Security Council" (S/2003/72) a description of Stages A, B and C is provided. A copy of this letter is enclosed.

The CTC urges all States to proceed with the implementation of the Resolution 1373 at their fastest capable speed. The CTC has therefore agreed on the following comments and questions focusing on the next set of priorities aimed at furthering the implementation of the Resolution by the Government of Estonia.

States must ensure that any measure taken to combat terrorism comply with all their obligations under international law, and should adopt such measures in accordance with international law, in particular international human rights, refugee, and humanitarian law.

In this context the CTC will be grateful for further information from the Government of Estonia concerning the following:

1. IMPLEMENTATION MEASURES

EFFECTIVENESS IN THE PROTECTION OF THE FINANCIAL SYSTEM

1.1 The CTC is pleased to note in Estonia's report, dated 6 March 2003, page 3, section 1.2 that harmonizing amendments to the Money Laundering Prevention Act that will be submitted to Parliament shortly to bring Estonia into compliance with the implementation of Sub-paragraph 1 (a) of the Resolution which requires States to prevent and suppress the financing of terrorist acts. In this context the CTC would be grateful for an update on the progress of this piece of legislation.

The draft has been presented to the Parliament. The second reading of the draft was completed on 19 November 2003, and the amendments are expected to become effective by 1 January 2004.

EFFECTIVENESS OF COUNTER-TERRORISM MACHINERY

1.2 The CTC is encouraged to note that Estonia has a National Action Strategy for counter-terrorism. The CTC would be grateful for an outline of the National Action Strategy adopted by the Government Security Commission, without compromising any sensitive information.

The National Action plan (Strategy) was formulated, right after the 11 September 2001 terror attacks in the United States, by the Government Security Commission, which had been convoked on an ad hoc basis. The purpose of the NAS was the swift increasing of cooperation and the exchanging of information between Estonia's various domestic institutions so as to

prevent potential acts of terrorism, and also to improve appropriate cooperation and exchange of information between the three Baltic States. By now, this document has become obsolete, and therefore does not have any major significance.

1.3 Effective implementation of Sub-paragraph 2 (b) of the Resolution requires States to take the necessary steps to prevent the commission of terrorists' acts. The CTC is encouraged to see that, as noted in it's first report on page 8, Estonia has taken steps to protect its aviation sector by meeting the requirements in Annex 17 of the Convention on International Civil Aviation. The CTC would be grateful for an update on the progress Estonia is making in this regard. The CTC would be grateful for an outline of the steps Estonia is taking to address maritime and seaport security to protect vessels and facilities from terrorist acts as required by the Safety Of Life At Sea (SOLAS) Convention of 1974,Chapter XI-2 of which Estonia is a signatory?

1. The Estonian Parliament has ratified all international aviation security related conventions, in addition to the provisions of international conventions. The national legal basis for aviation security is organised as follows:

The primary legislation for aviation security in Estonia is the Aviation Act, which was adopted by Parliament in 1999. Regulation No. 44 of the Government of the Republic, "Procedures for aviation security", is considered to be the regulation governing implementation of the Aviation Act.

The National Civil Aviation Security Programme (NCASP) was adopted by the National Civil Aviation Security Committee on 30 May 2003.

Currently, the Aviation Act does not comprise any details concerning the sharing of responsibilities between all entities involved in aviation security and the key security measures that shall be implemented to protect civil aviation against acts of unlawful interference. Therefore, a working group was established with the objective of amending the Aviation Act by introducing a new chapter on aviation security. In the process of the development of the Act, all the provisions and latest amendments of Annex 17 are taken into account, as well as the regulation and recommendations established by the EU and the European Civil Aviation Conference (ECAC). This revision should be submitted to the Government of the Republic by the beginning of 2004 for approval, and for subsequent submission to the Parliament.

The National Aviation Security Committee is responsible for the development of the nation's aviation security policy, and the co-ordination and promotion of activities in the field of aviation security. The Security Police Board is responsible for responding to actual incidents and specific threats (e.g., terrorist acts).

2. Estonia acceded to the 1974 SOLAS Convention and its 1978 Protocol on 19 November 1991. Both entered into force for Estonia on 16 March 1992.

Estonia has been observing the requirements of the SOLAS Convention's 1988 Protocol, even before they became effective for Estonia on 20 November 2003. Since the SOLAS Convention has often been changed in the IMO, and since the SOLAS Protocol requires a participating state to enforce certain regulations domestically, then the proper enactment of the Protocol makes it necessary to amend domestic legislation (for instance, in connection with the requirements derived from the ISPS Code).

A. The Maritime Safety Act's Amendment Act (which should be presented to the *Riigikogu* in April 2004; presently, the amendments are being partially incorporated in conjunction with the Maritime Safety Act's Amendment Act, which is being processed in the *Riigikogu* Financial Committee) has been enacted within the framework of the aforementioned preparations, which makes it possible to improve the safety of maritime navigation and vehicles.

B. In connection with Estonia's harbours, new regulations are also being formulated on the basis of the existing Security Act, which makes it possible to coordinate the specific sphere dealing with the work and security of Estonia's harbours, with the enactment conditions of the SOLAS Convention's 1988 Protocol. These legislative initiatives should enter into force by July 2004.

1.4 Sub-paragraph 2 (e) of the Resolution requires States to ensure that any person who participates in the financing, planning, preparation or perpetration of terrorist acts is brought to justice. In this regard, the CTC

would be grateful for an outline of what specific training measures Estonia provides its administrative, investigative, prosecutorial and judicial authorities to implement the Sub-paragraph of the Resolution?

For example:

A. The typologies and trends in terrorist financing methods and techniques,

B. Techniques for the tracing of assets, which represents the proceeds of crime or which are used to finance terrorism, with a view to ensuring that such property is frozen, seized or confiscated?

Investigative authorities are exploring the trends of financing terrorism.

The tracing of terrorist funds and financial assets is based upon intelligence gathering, and the monitoring and assessing of transactions taking place in credit institutions. Since the financing of terrorism is, innately, a very shady and surreptitious activity, it is very important to discover, at the early stages, any possible attempts to perpetrate such crimes. Therefore, intelligence gathering is given a very high priority in Estonia, and Estonia has adopted an integrated system, which makes use of various investigative techniques.

The draft amendments to the Money Laundering Prevention Act (MPLA) provide, that the FIU shall be notified by the persons specified in the MLPA, about any signs they may identify as referring to terrorist financing. The draft law entitles the FIU to draft a sample list of signs referring to terrorist financing, which is to be available on the web site of the FIU.

1.5 In regard to the effective implementation of Sub-paragraph 2 (e) of the Resolution could Estonia provide the CTC with an outline of what steps it is taking to address the challenges of detecting, monitoring and apprehending those involved in terrorist financing and bringing them to justice? For example, are there any special strategies or investigative tools used to enable financial, regulatory, law enforcement, and border agencies to work together to implement Sub-paragraph 2 (e)?

In 2002, the Financial Supervision Authority issued guidelines on the prevention of money laundering, specifying and explaining the obligations of credit and financial institutions in the due course of a business relationship with a client: identifying the client, and up-dating information about the client concerning money laundering. With regard to terrorist financing, prospective amendments to the Money Laundering Prevention Act (MLPA) will incur upon the subjects of financial supervision and others subject to the MLPA similar obligations, both for the prevention of money laundering and the prevention of terrorist financing. At the beginning of 2003, the International Sanctions Act was implemented, which regulates the procedures for persons that are subject to international sanctions, *inter alia*, for terrorism and terrorist financing. Although the International Sanctions Act probably needs amending, it, nevertheless, provides a legal basis for detecting those involved in terrorist financing.

On the basis of the international Sanctions Act, the Government has issued a number of orders stating the need to apply restrictions on persons and other subjects that have been ruled to be subject to international sanctions determined by the UNO Security Council or the Council of the EU.

Estonia has no special strategies for inter-agency co-operation, although various government agencies have approved the Memoranda of Understanding, which specify the exchanging of information between, and the establishment of joint working groups and action teams. Therefore, it can be said that Estonia has adopted a multi-agency approach for tackling the financing of terrorism. As a result, Estonian law enforcement agencies, in order to make use of resources more efficiently, are working closely together in the course of carrying out relevant investigations.

1.6 In regard to the implementation of Sub-paragraph 2 (e) of the Resolution, the CTC would be pleased to know, for the period 1 January 2001 until 31 December 2002;

b) The number of prosecutions of terrorists or their supporters:

None

c) The value of funds and assets frozen or seized:

None

d) The number of on-going and/or completed investigations:

None

e) The number that required international coordination:

None

1.7 As related to the effective implementation of Sub-paragraph 2 (e) of the Resolution, the CTC would appreciate an outline of any laws enacted to address cyber crimes and an outline of the provisions that prevent terrorists from misusing the Internet and other electronic systems.

The only Estonian law pertaining to this matter is the Penal Code, which deals with the following cyber crimes:

§ 178. Manufacture of material involving child pornography, or making child pornography available

(1) A person who manufactures, stores, hands over, displays, or makes available in any other manner pictures, writings or other material, or reproductions of material depicting a person of less than 14 years of age in an erotic or pornographic situation shall be given a pecuniary punishment or be imprisoned for up to one year.

(2) The same act, if committed by a legal person, is punishable by pecuniary punishment.

§ 206. Computer sabotage

(1) Unlawful replacement, deletion, damaging, or blocking of data or programs in a computer, if significant damage is thereby caused; or the unlawful entry of data or programs in a computer, if significant damage is thereby caused, is punishable by a pecuniary punishment, or by up to one year of imprisonment.

(2) The same act, if committed with the intention of interfering with the work of a computer or telecommunications system, is punishable by a pecuniary punishment, or with up to 3 years' imprisonment.

§ 207. Damaging a connection to a computer network

Damaging or obstructing a connection to a computer network or computer system is punishable by a pecuniary punishment.

§ 208. Spreading of computer viruses

(1) Spreading of a computer virus is punishable by a pecuniary punishment, or by up to one year of imprisonment.

(2) The same act, if committed:

1) At least twice, or

2) In a manner, which causes significant damage, is punishable by a pecuniary punishment, or by up to 3 years' imprisonment.

§ 213. Computer-related fraud

A person receiving proprietary benefits through entry, replacement, deletion or blocking of computer programs or data, or other interference with a data processing operation, and thereby influencing the result of the data processing operation shall be given a pecuniary punishment, or be imprisoned for up to 5 years.

§ 217. Unlawful use of a computer, computer system, or computer network

(1) Unlawful use of a computer, computer system, or computer network by way of removing a code, password, or other protective measure is punishable by a pecuniary punishment.

(2) The same act, if it:

1) Causes significant damage, or

2) Is committed by using a state secret or a computer, computer system, or computer network containing information prescribed for official use only, is punishable by pecuniary punishment or up to 3 years' imprisonment.

§ 219-230. Offences related to infringements of copyrights and related rights - chapter 14 from the Penal Code, which prescribes offences against intellectual property.

§ 284. Passing on of security codes

Unlawful passing on of security codes of a computer, computer system, or computer network, if committed for the purpose of personal gain, and in a manner, which causes significant damage, or results in other serious consequences is punishable by a pecuniary punishment or up to 3 years' imprisonment.

§ 315. Unlawful special or exceptional surveillance activities

Unlawful special or exceptional surveillance activities, conducted by a person with the official right to engage in surveillance, are punishable by pecuniary punishment or up to 3 years' imprisonment.

Illegal interception - punishable as an illegal surveillance activity

1.8 With reference to the implementation of Sub-paragraph 2 (e) of the Resolution, the CTC would be pleased to learn if Estonian law provides for the operation of special courts in relation to the trial of terrorist, bail for terrorists, the use of undercover operations and the interception of communications for the purpose of preventing terrorism.

Terrorism and terrorism related crimes are dealt with in the criminal court system, since they are legally defined as criminal offences.

All abovementioned special operations may be made use of, but the court must authorize their use. Undercover operations and the interception of communication networks may also be used in the fight against drug trafficking or any other type of crime.

1) The prosecution of a terrorist organisation requires a special court, since any proceedings dealing with the prosecution of a criminal organization calls for a panel of three judges. This is possible, since a terrorist organisation may be qualified as a type of criminal organization.

Code of Criminal Procedure

§ 23. Courts of First Instance
Pursuant to §§ 255 and 256 of the Penal Code, a court with a panel of three judges shall adjudicate criminal matters.

2) Bail for terrorists is excluded in the new the Code of Criminal Procedure, which comes into force 1 July 2004.

§ 135. Bail

(2) "Bail" means a sum of money paid as a preventive measure by a suspect, an accused, or another person on behalf of him or her to the deposit account of the court. Bail shall not be imposed on a suspect or accused in the case of the criminal offences prescribed in §§ 89, 90, 96, 114, 214, 237 (terrorism), 244, 246, 255, 256 and 405 (explosion) of the Penal Code

3) Undercover operations and interception of communication is allowed for the purpose of preventing terrorism.

Surveillance Act

§ 14. Recruitment for secret co-operation in surveillance activities

(1) Surveillance agencies have the right to recruit adults, with their consent, for voluntary temporary or permanent secret co-operation in surveillance activities.

Security Authorities Act

§ 23. Simulating person, agency or body

(1) In order to simulate a person for the purposes of performing the functions of a security authority, a corresponding entry shall be made in the commercial register, or the non-profit associations' and foundations' register, on the basis of an application by the relevant minister. If simulation is no longer necessary, the relevant minister shall delete the entry, pursuant to the general procedure, on the basis of an application.

§ 25. Restrictions on the right to confidentiality of messages

(3) A person's right to the confidentiality of messages may be restricted by:

Examination of postal items;

Wire tapping, observing or recording of messages, and other information communicated by telegraph, telephone or other technical communication channels;

Wire-tapping, observing or recording of information communicated by any other means.

Code of Criminal Procedure

120. Police agent

"Police agent" means an official who collects evidence in a criminal proceeding by using a false identity. Identity documents and other documents may be issued in order to change the identity of a person.

A police agent may participate in legal relationships under a false identity. A police agent has all the obligations of an official of an investigative body, in so far, as the obligations do not require disclosure of the false identity.

EFFECTIVENESS OF CUSTOMS, IMMIGRATION AND BORDER CONTROLS

1.9 With reference to the implementation of Sub-paragraphs 2 (b) and 2 (g) of the Resolution, States are required to take steps to prevent terrorist acts and have effective border controls respectively, could Estonia please inform the CTC as to whether the list of potential terrorists maintained by the Estonian Border Guards (as stated on page 11 of its first report) is shared or integrated into other databases maintained by Estonian Customs and regulatory agencies. Further, in regard to Sub-paragraphs 2 (b) and (g), the CTC would be pleased to receive a progress report on the Estonian Customs proposal aimed at developing a working relationship with private companies, as well as, developing data analysis capability to address terrorism and other crimes.

Estonian Border Guard databases store data concerning terrorists and persons associated with terrorists, either for detaining them, or for conducting a thorough investigation of those persons. A periodic review and update of the abovementioned list is done together with the Security Police Board (*Kaitsepolitsei*).

The Customs Board does not have an online access to the list of terrorists composed by the Border Guard Board in co-operation with the Security Police Board. The information is shared with the Customs Board in case of need. This means, that the Border Guard Board replies to inquiries concerning specific cases dealing with the suspicion of terrorism made by the Customs Board.

Relationships with private companies – The Customs Board has concluded Memorandums of Understanding (MOU) with ***DHL International Eesti AS, Air Cargo Estonia AS, TNT Express Worldwide Eesti AS, Schenker AS, and AS Eesti Post*** (Estonian Postal Service). Co-operation agreements between the Customs Board and the telephone companies give Customs access to the electronic databases of these firms. Customs also has access to the ***AS Estonian Air*** (the Estonian national airline) passenger database.

Developing data analysis capability – The Customs Board has established an exchange of information with the Border Guard Board, Police Board, and Tax Board, and has access to the databases of telecommunication companies (*ELION AS, TELE 2*). Risk analysis is carried out both on the central and regional levels. Special software (Analysts' Notebook) has been introduced for these purposes. The selectivity module MODSEL of ASYCUDA (main declaration processing system) and the selectivity module RISK of the ENCTS (Estonian National Computerized Transit System) are used for operational and tactical analysis. All intelligence officials are connected to the e-mail based common communication network that ensures quick distribution of essential information.

The Customs Board has a contact person who collects and analyses information from the various Customs posts, and forwards relevant information to the FIU (Financial Intelligence Unit) in order to obtain information concerning possible violations relating to money laundering or terrorism financing (based upon the co-operation agreement between the Customs Board and Police Board). Customs does not deal directly with money laundering, and only forwards relevant information to the Police Board for further investigation.

1.10 Estonia, on page 10 of its first report, noted that it is taking steps to effectively implement Sub-paragraph 2(g) by providing Estonian Border Guards with the VSC-2000 and DIXI-05 document control system at key border points to detect forged and altered travel documents. The CTC would be pleased to know if Estonia plans to provide such cover at all points of entry? If so, when does Estonia anticipate completing this process?

All border crossing points and Border Guard stations providing border control service will be equipped with Money Checker (30 pieces). There is no intention to procure more DIXI 05 or VSC-2000.

VSC-4C or DOCUBOX 500 will be procured instead, and these will be distributed to major border crossing points, where there were no VSC-2000's.

The Travel Documents Evaluation Centre located in the Border Guard Board will acquire DOCUCENTER 3000 Digital, and the VSC-2000 still in use at the Travel Documents Evaluation Centre will be relocated to the Luhamaa Border Crossing Point (major BCP on the Estonian-Russian border).

1.11 Sub-paragraph 2 (g) requires states to have effective controls on the issuance of identity papers, could Estonia please provide the CTC with an outline of the provisions regarding the granting of citizenship or other civic rights? Can a foreigner, who is granted citizenship or other civic rights, change his name? What precautions are taken to establish the true identity of a person before new identity papers are issued to that person?

The change of the given name or surname of an Estonian citizen, or a person with a permanent residence permit, who is not a citizen of another state, is approved by the Minister of the Interior, on the basis of a respective request by that person. The Criminal Record Register of the Police Board will be informed of the changes of given names or surnames of adult persons in Estonia. Presently, an Estonian citizen, or an alien with a permanent residency permit, may change his or her name at one's will. The regulations pertaining to this activity will be changed and made stricter with the enactment of the Names Act (presently still a draft).

1.12 In order to effectively implement Sub-paragraph 2 (g) of the Resolution, what steps has Estonia taken to ensure its national identity papers and travel documents and similar documents (birth certificates, marriage certificates, driver's licenses, military service cards, etc.) meet minimum International Standards Organization (ISO) security standards aimed at making it impossible to duplicate or falsify, or obtain fraudulent documents?

Identity cards and travel documents comply with the standards of the United Nations International Civil Aviation Organisation (ICAO), of which Estonia is a member. The security of the ID cards and the new Estonian passports is very high; the new alien's passport will become effective in the very near future. Old passports, which are quite easy to falsify, are still in circulation in Estonia. The security of documents issued between 1992 and the first half of 1996 are low, as they are not machine-readable. Thus, their validity will expire in the very near future. At the moment, there are five types of vital statistics certificates in use in Estonia: birth, marriage, divorce, change of name, and death certificate. The security requirements used in printing these documents are satisfactory -- more than three different security features are used in the production of the documents.

1.13 The effective implementation of Sub-paragraph 3 (d) of the Resolution calls on States to become a party to the relevant international conventions and protocols relating to terrorism. In that regard, the CTC would appreciate receiving a progress report on the Ratification Act for the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf.

Domestic procedures for accession are in the final stage, and the *Riigikogu* (Parliament) ratified the Protocol on 12 November 2003. We expect to become Parties to the Protocol by the end of this year.

CONTROLS ON PREVENTING ACCESS TO WEAPONS BY TERRORISTS

1.14 The effective implementation of Sub-paragraph 2 (a) of the Resolution requires States, inter alia, to eliminate the supply of weapons to terrorists. Estonia, on page 7 of its first report, indicated it was taking steps to regulate brokerage activities and to establish internal compliance programs in the industrial sector with a view to addressing the export of arms and implements of war. The CTC would be grateful for a progress report on this initiative.

The effective implementation of Sub-paragraph 2 (a) of the Resolution requires States, *inter alia*, to eliminate the supply of weapons to terrorists. Estonia, on page 7 of its first report, indicated it was taking steps to regulate brokerage activities and to establish internal compliance programs in the industrial sector with a view to addressing the export of arms and implements of war. The CTC would be grateful for a progress report on this initiative.

Taking into account the newest developments in this sphere, the Estonian Government has passed a draft of the new export control law, which would, inter *alia*, abolish controls on dual use goods imports and introduce, in addition to individual

licenses, global and general authorizations. The new law also defines more clearly brokering controls, and establishes a brokering register. Currently, the draft is under parliamentary review, and expected to be adopted by the end of 2003.

1.15 How many investigations and/or prosecutions relating to arms violations, including hazardous materials, were conducted in 2002? How many of the investigations and/or prosecutions related to terrorism?

Violations related to export controls: three investigations and one prosecution. None of the investigations and prosecutions, which took place in 2002, was related to terrorism.

No investigations or prosecutions related to terrorism were conducted in 2002.