CTBT ON-SITE INSPECTION
-PROTECTION OF CONFIDENTIALITY AND INFORMATION RELEVANCY-

Sukeyuki ICHIMASA
Research Fellow
CTBT National Operation System of Japan,
Center for the Promotion of Disarmament and Non-Proliferation (CPDNP),
Japan Institute of International Affairs (JIIA)

INTRODUCTION

Japan is attaching great importance to Comprehensive Nuclear Test-Ban Treaty (CTBT) as part of the Nuclear Non-Proliferation Treaty (NPT) regime and ardently contributing to the establishment of verification regime and also making various diplomatic efforts in the area of out reach activity for early entry into force of CTBT.

After entry into force, CTBT will play an important part of NPT regime. Since UN General Assembly adopted[1] this treaty in 1996, intensive effort has been made over years to promote the treaty's entry into force. CTBT will come into force in 180 days after it has been ratified by the Annex II 44 states[2], which are identified in the table 1 of the International Atomic Energy Agency (IAEA) April 1996 edition of 'Nuclear Power Reactors in the World'.

CTBT prohibits any nuclear explosion in any environment. CTBT has 4 elements of verification – International Monitoring System (IMS), Consultation and Clarification (C&C), Confidence Building Measures (CBMs) and On-Site Inspection (OSI) - to verify the compliance with the treaty and protocols. What is important is that the verification regime shall be capable of meeting the verification requirement stipulated in the treaty and everything should be set at entry into force of this treaty[3].

IMS will finally consist of 321 monitoring stations and 16 radionuclide laboratories that monitor the globe for evidence of a nuclear explosion. IMS uses seismic, radionuclide, hydroacoustics and infrasound monitoring technologies. Data monitored by IMS network is transferred to and accumulated in the International Data Centre (IDC) in Vienna, Austria. All of the IMS data and its processed products will be available to the states signatories through the IDC. This mechanism enables the state signatories to analyze any ambiguous event, whether it is man-made or not[4].

---

[1] Resolution 50/245. 125th plenary meeting (10 September 1996).
[2] 176 member states, 125 total ratification and 33 Annex II ratification at the point of November 26, 2005.
[3] *See,* CTBT paragraph 1 of the article 4.
[4] Wang, Jun "CTBT Verification Regime: Preparations and Requirements" *On-Site Inspections: Common Problems, Different Solutions.* Disarmament Forum, 1999. Pp.41.

CBMs[5] will go into use in dual purposes. First, CBMs will be a help to resolve any non-compliance concerns arising from the IMS data analysis. Secondly, CBMs will be the assistance of calibration for the IMS stations in the world.

C&C will play an important role whether to confirm that the possible violator has conducted the nuclear test explosion or not. In some cases, C&C will occasionally be carried out beforehand of requesting an OSI.

OSI will act as a powerful deterrence to any potential violator[6]. OSI is the 'last resort'[7] to verify the compliance with the treaty. Using IMS data and any relevant technical information obtained by National Technical Means (NTM) of verification in a manner consistent with generally recognized principles of international law, every state signatory has a right to request the Executive Council (EC) to conduct an OSI[8] at any time. Among aforementioned verification elements, OSI will be the most appropriate method to collect the direct evidence of non-compliance because the inspector can step into the territory of the Inspected State Party (ISP) and acquire the direct evidence. OSI thus draw fully upon the strength of sophisticated inspection technologies in the field of suspected nuclear test site, point of strategic importance and any other politically or commercially sensitive location to the ISP. In this context, during the course of preparing the CTBT OSI regime, information management is always the question in issue.

OSI information management is supposed to be stipulated by the OSI operational manual. Although an elaboration process of the OSI operational manual has started since 2001, CTBT working group B[9] spent more than five years to finish the first reading and introduce the 'second round' procedure. Since the external evaluation of OSI[10] has been conducted in 2003, development of the OSI regime, which will consist of the OSI operational manual, methodology, equipments and training has came under review[11]. Particularly, the OSI operational manual is a key focus to establish the future

---

[5] Usually, in the light of arms control and disarmament regime, CBMs has three factors of its notion: 1) The need for information, 2) Confidence building as a process, 3) Transparency as an intermediate step.
Wulf, Herbert "transparency in Armaments and other confidence-building measures" *Nuclear Disarmament Obstacles to Banishing the Bomb*, I.B. Tauris London, 2000. Pp.86.

[6] Melamud, Mordechai "Background Paper on On-Site Inspection (OSI) Main Elements and Expectation" Report of CTBT Commission, 2001. (Website) http://www.ctbtcommission.org/melamudpaper.htm

[7] CTBT Article IV paragraph 35 set out as follows; "The sole purpose of an on-site inspection shall be to clarify whether a nuclear weapon test explosion or any other nuclear explosion has been carried out in violation of Article I and, to the extent possible, to gather any facts which might assist in identifying any possible violator."

[8] *See*, CTBT Article IV paragraph 34.

[9] CTBTO Preparatory Commission annual report (top page)
(Website) http://www.ctbto.org/reference/annual_report2003.html

[10] CTBTO Preparatory Commission annual report in 2004 (MP4 OSI)
(Website) http://www.ctbto.org/reference/annualreport/ar_2004_mp4.pdf

[11] Independent Commission on the Verifiability of the CTBT 'Final Report' The Verification Research, Training and Information Centre (VERTIC), November 2000 (pp.6) (Website) http://www.ctbtcommission.org/FinalReport.pdf

OSI regime because every aspects of the regime should be based upon each prescription of the OSI operational manual.

Therefore, this article draws focus on the CTBT OSI mechanism, especially on the issue of protecting OSI confidential information[12]. Consulting the precedents taken from the relevant arms control and disarmament treaty, this article argues about the future framework of OSI confidential information protection in the CTBT Organization (CTBTO)[13]. The view and analysis expressed on this article are that of the author's personal remarks and does not necessarily represent those of the CPDNP.

1. SUBJECT OF PROTECTION - 'OSI CONFIDENTIAL INFORMATION'

As it is clearly stipulated on the Treaty, sole purpose of OSI is to clarify whether a nuclear weapon test explosion or any other nuclear explosion has been carried out in violation of the treaty provision, and gather any facts which might assist in identifying any possible violator. In the light of its intrusive nature of OSI[14], information relevant to the purpose of OSI should be protected under the stringent confidential information management system in the Technical Secretariat (TS). However, due to the difficulty of identifying the relevancy of the information correctly during the course of OSI, subject to be protected under the system is somewhat controversial.

One of the most difficult issues of building the OSI regime is information management. In order to fulfill its mandate, OSI will deal with the ISP's sensitive information[15], not only for the commercial confidence but also the national security confidential information. Unlike the precedent UN arms control and disarmament organization such as the IAEA and the Organization for the Prohibition of Chemical Weapons (OPCW)[16], CTBT OSI has to deal with the undeclared 'suspected' nuclear-testing site (In accordance with the Treaty, Inspection Area (IA) should be limited to maximum 1000 square kilo meters) in the territory of sovereign nation. This unique nature makes CTBT OSI much more difficult than other precedents especially when the Inspection Team (IT) access to the ISP's sensitive information that is not possible to make clear-cut distinction whether it is relevant to the purpose of OSI or not.

Depending on the circumstances, the ballistic missile launching silos will exist within

[12] Information managed inside of the TS as the confidential information. This provision is based upon CTBT Article II paragraph 6.

[13] Preparatory Commission (Prepcom) for the CTBTO is established in Vienna. (Website) http://www.ctbto.org/

[14] *See*, CTBT Article IV paragraph 58.

[15] Information designated by the ISP as the sensitive information. This provision is based on CTBT Article IV paragraph 7 and paragraph 52 (b).

[16] Hart, John "On-site Inspections in arms control and disarmament verification" VERTIC Research Reports, number 4 Oct 2002. (pp. 21)

the bounds of IA and more or less the ISP will try to block the IT access to such a point of strategic importance that is not relevant to the purpose of OSI. In such a case managed access[17] measures will be exercised by the ISP. On the contrary, the IT has to request its access to the point that the managed access measure is applied by the ISP in order to confirm that the location and installation is not relevant to the purpose of OSI.
In the light of protecting the sovereignty of the ISP, it is essential to consolidate the mechanism of OSI confidential information management. In accordance with the OSI mandate, the IT has to collect the OSI relevant information in the IA within a limited amount of time and limited number of inspectors[18]. Therefore, taking the balance between the consolidation of acquiring the OSI relevant information by the IT and protecting the sensitive information of the ISP from access made by the IT is critical.

(1) Confidential Information Management in the Technical Secretariat (TS)
Considering the magnitude of the matter and the intrusive nature of OSI, the TS's stringent OSI confidential information management system is essential to protect the information provider's sovereign authority.
Information obtained from the IA thorough inspection activity should be designated to appropriate level of confidential information category by the ISP. Procedure of designating OSI confidential information to its appropriate destination has to be initiated by the information provider[19]. Each category should come up with the appropriate level of physical and logical protection against unauthorized disclosure of the information.

(2) Relevancy for the OSI Purpose
In accordance with the Treaty and Protocol, the ISP has to cooperate with the IT[20] during OSI activity in the field. On the other hand, IT has to clarify whether a nuclear test explosion has been carried out and to gather any facts relevant to the violation[21]. In this context, the Treaty gives an inherent right to the ISP of protecting her sensitive information irrelevant to the purpose of the inspection. With this regard, this article argues about the necessity to define a concrete policy of information handling during the course of inspection. More specifically, even if it has regarded as sensitive by the

[17] Managed Access is the provision that prescribes the interaction with regard to the access between ISP and IT. Same provision is found in both of the Chemical Weapon Convention and Nuclear Safeguards.
[18] In accordance with the treaty text, maximum 40 inspectors are allowed to engage in the OSI field activity. (CTBT Part 2 of the Protocol paragraph 9.)
[19] Considering the modality of information protection in the TS, information provider should be qualified as state signatory.
[20] *See.* CTBT Part 2 of the Protocol paragraph 11 and paragraph 61 (g).
[21] *See*. CTBT Article IV paragraph 35.

ISP, the information corrected by the IT is clearly relevant to the purpose of OSI, the ISP can not prevent it to be taken from the IA and reported to the EC in the proper way.
In the IA, sometimes it is quite difficult to give a clear distinction between the OSI 'relevant' and 'irrelevant' information, which is particularly protected under the ISP's domestic regulation. Depending on where one stands, contradiction of relevancy judgment may always exist between two parties. Therefore, until after the final decision of the Director General (DG) is deliberated, any classified information designated by the ISP should be kept in the TS's stringent OSI confidential information management system.

(3) Information Obtained through the National Technical Means (NTM)
Also the information obtained through NTM[22] of the state parties should be stringently secured under the TS's OSI confidential information management system. In this case, protecting the NTM information provider's anonymity is very important[23], and also the fact that the TS had acquired the NTM information should be kept secret between the provider and the TS.
Therefore NTM information should never be quoted on any inspection reports and it should never be considered as the direct evidence of the Treaty violation.

2. PROTECTION OF ON-SITE INSPECTION CONFIDENTIAL INFORMATION
Logical consistency shows that the every information obtained in the field should be consolidated into the head quarter of OSI activity, namely the Operation Support Centre within the CTBTO in Vienna. Unify the management of information includes both of OSI confidential information claimed by the ISP and any other information contributed by the state signatories' NTM. This section treats of the procedures of classification / de-classification of OSI confidential information and overall view of the operation of handling OSI confidential information.

(1). Classification and De-classification
According to the precedent disarmament and non-proliferation organizations, the TS's OSI confidential system will consist of following 3 categories[24] (*See*. Diagram 1):

[22] *See*. CTBT Article IV paragraph 5 - 6.
[23] NTM is the application of sophisticated monitoring technologies to verify compliance.
Rueckert, George L "On-site Inspection in theory and practice; a primer on modern arms control regimes", Praeger, London 1998. (PP.44)
[24] 3.3.2.1. "Marking of Confidential Information" indicates the same philosophy of defining the classification. In the OPCW case, lowest classification has named as "OPCW restricted".
(Website) http://www.opcw.org/html/global/p_series/pc10/pc10_bwp2.html

(i) OSI Limited Information
(ii) OSI Protected Information
(iii) OSI Highly Protected Information

Information provider should have the right to designate the category of classification. The ISP will evaluate the possible damage of the unauthorized deliberation, and then make her choice of distinctive category of the TS's OSI confidential information management system. On the other hand, in case the information provider has recognized that the previously arranged classification is not necessary any more, she can request the TS for de-classification. Modification and improvement of the previously arranged classification category is also within the scope of information provider's authority.

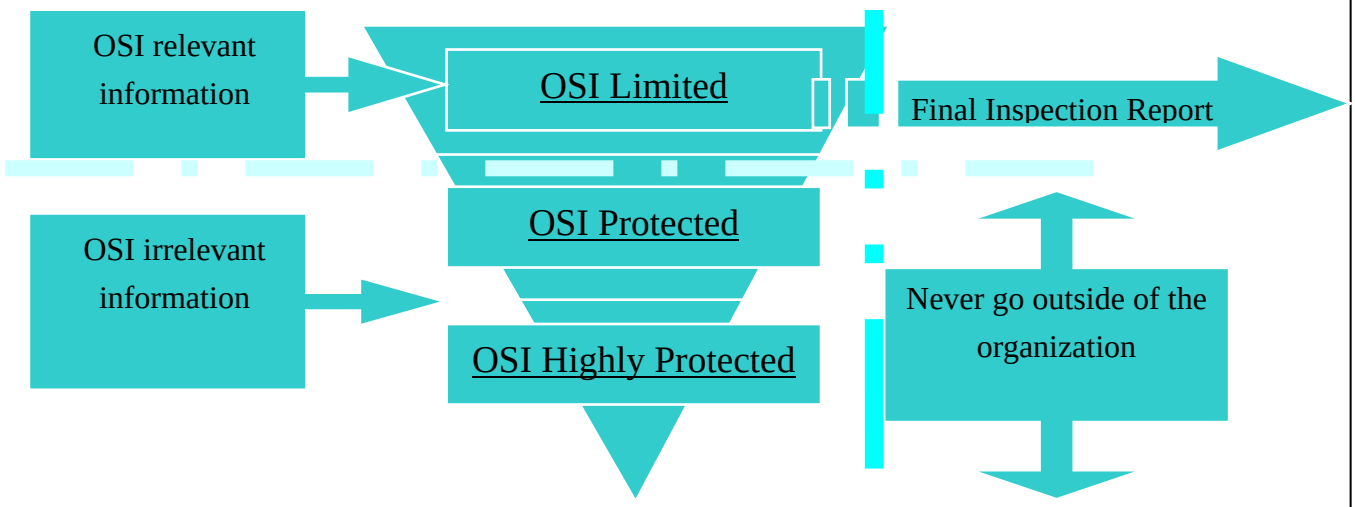
(i) OSI Limited Information is the lowest classification of OSI confidential information in the TS. Basically, this category of information consists of the OSI relevant information, which is designated by the information provider (member states). After the inspection activity has terminated, the DG prepares his Final Inspection Report using the information of this category as he sees appropriate. In this sense this category of information will eventually be distributed to the member states as 'for the official use only'[25] information.

(ii) OSI Protected and (iii) OSI Highly Protected Information should be considered as separate category of the above (i) OSI Limited information. One of the major differences is the degree of the protection. These categories of the information should never go outside of the TS, unless the information provider approves and de-classify it. The other difference is the attribution of the information. These categories of the information are consisted of the OSI irrelevant information. Difference between (ii) and (iii) is mainly depended upon the level of physical and logical protection.

In addition, secret already leaked out is no longer the confidential information. Therefore when the truth came out that the OSI Protected / Highly Protected information has leaked out, any information even if it is appointed to the Highly Protected category should be changed into the lowest level of classification, namely OSI Limited category.

[25] In accordance with CTBT Article II paragraph 7, "Each State Party shall treat as confidential and afford special handling to information and data that it receives in confidence from the Organization in connection with the implementation of this Treaty. It shall treat such information and data exclusively in connection with its rights and obligations under this Treaty". This provision indicates that the official use only information provided by the organization should be considered and treated as the "confidential information" by the member states.

Diagram.1 Confidential Information Management in Technical Secretariat



(2) 'Need to Know' Principle

In the light of 'Need to Know' principle, inspector, inspection assistant and the TS staff should be authorized by the DG to access the appropriate level of information. In order to maintain the efficiency and effectiveness of OSI, inspector should have an adequate level of access right to OSI confidential information based on the 'Need to Know' principle[26]. Therefore, even if the ISP designates all of the information obtained in the IA as the category of 'OSI Highly Protected', inspector will be able to continue the planned inspection activity and fulfill the mandate.

(3) International Standard for the Information Protection (ISO/IEC 17799)

International standard "Information Technology - Code of Practice for Information Security Management (ISO/IEC 17799)" is a material made up of practical measures for information protection, which has been implemented to several disarmament and non-proliferation organization.

Not only the handling of confidential information, but also the physical and logical protection, distribution, retention, compliance, destruction, transmission, electronic data custody will be the relevant items to be considered. The international standard reiterates

[26] This principle has generally applied to other arms control and disarmament treaties. For example, the IAEA safeguard additional protocols also taking "Need to Know" basis with United States.
(Website) http://www.nti.org/e_research/official_docs/dos/dos01292004_ap.pdf

the importance of maintaining the 1) confidentiality, 2) Integrity and 3) Inviolability of the information. These key points should be reflected to the unique information safety management system of the CTBTO in future.

3. ACTION IN THE EVENT OF UN-AUTHORIZED DISCLOSURE OF OSI CONFIDENTIAL INFORMATION

During the course of OSI, it is impossible to deny the possibility of divulging of confidential information. In preparation for such unauthorized disclosure of OSI confidential information is thus essential to tighten the lid on inspector, inspection assistant and any other CTBTO staff whom involved with the OSI business. Maximize the secrecy of OSI confidential information and expecting the preventive effect to the violation, this section make a study on two levels of action against the leakage.

When the state party charges a case to the DG for the possible unauthorized disclosure of OSI confidential information, investigation will be promptly initiated to determine the facts and the nature of the incident[27] in order to ascertain the compliance of information security measurement by the organization. Also, if the state party requests a reimbursement of such damage caused by the unauthorized disclosure, the EC have to make a judgment[28] of the appropriateness of the stated value and then take an action as described later.

Likewise the inspector, inspection assistant, TS staff member should be also covered by the privileges and immunities[29]. However, if the divulging of OSI confidential information has occurred, the DG may waive them in those cases when he is of the opinion that immunity would impede the course of justice and that it can be waived without prejudice to the implementation of the provisions of this Treaty. This extreme case indicates the most serious situation, which is impossible to compensate the damage caused by certain staff or inspector and thus the DG has to assign responsibility to the person actually committed to the leakage.

As a matter of fact, if the TS committed the violation of OSI confidentiality, and information provider has called the organization to account for its failure, the EC (or the DG) has to establish a committee to seek an explanation. However considering the magnitude of the matter, basically such compensation is almost impossible. Assumably,

[27] Indeed there is no clear-cut measure in the treaty text to seek an explanation for the divulging of OSI confidential information. For example, the IAEA has an experience of carrying out this method for years.
[28] *See.* CTBT Article VI “Settlement of Disputes”.
[29] *See*. CTBT Part 2 of the Protocol paragraph 27 and paragraph 31.

such a damage caused to the ISP might affect directly the national security interest or commercial interest. Usually, there is no remedy on such damage. Even if that is the case, no government can accept liability for damages to the organization.
All that the DG and the committee can do is to find out the person who has committed violation and in the worst case, waive his/her privileges and immunities as is explicitly stated in paragraph 26 to 31, part 2 of the Protocol and demise his/her jurisdiction to the complaining state party. In this regard, Criminal Extradition Treaty would be a good reference for the governments to prepare domestic laws to turn over the national inspectors and inspection assistants.

4. ISSUES FOR FUTURE CONSIDERATION

Looking at OSI confidential information and its protection from all angles, still there are remaining several substantive matters to be considered. With regard to the conceptual part of information management, judgment of relevancy to the OSI purpose is one of the most controversial issues. Also in the same context, subject of reporting and recommendation made by the IT and the DG is a matter of concern.
From the viewpoint of actual information management, modality of confidentiality undertaking between the DG and the OSI participants should be considered. In case of unauthorized OSI confidential information disclosure directly caused by TS staffs, it is necessary to make an investigation about the availability of organizational compensation and understand its difficulty.

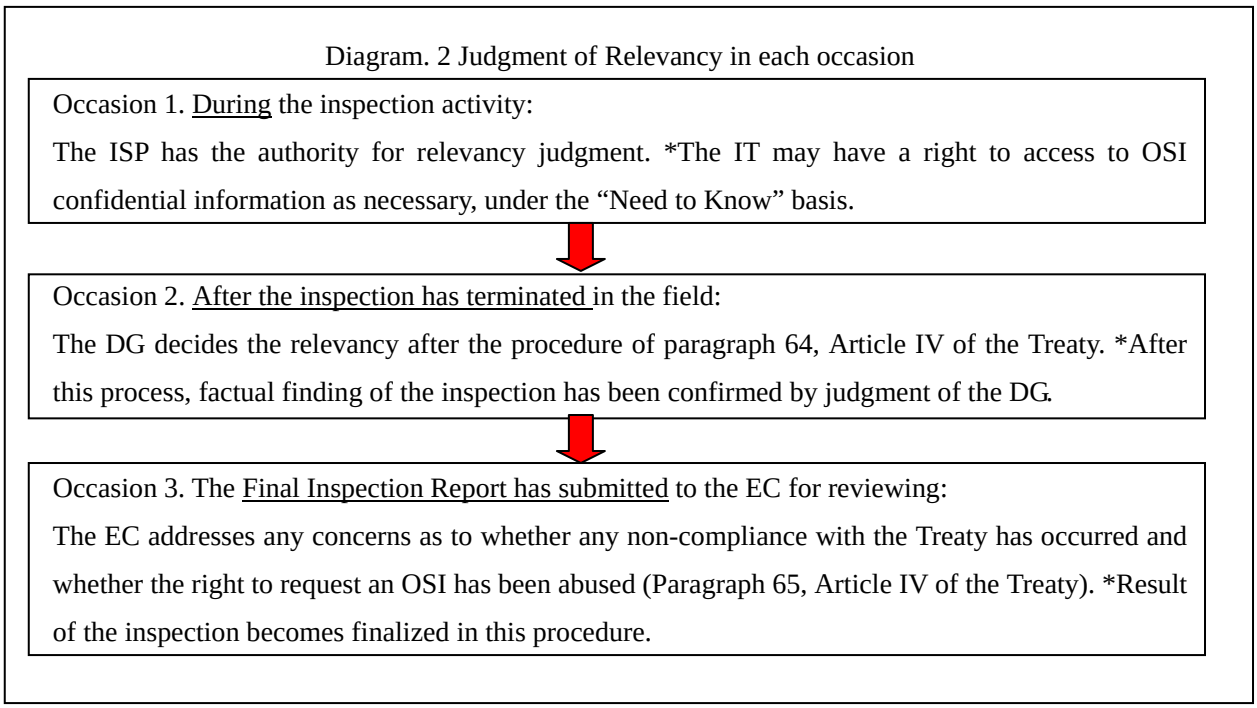
(1)Judgment of the OSI Relevant Information

After the termination of the field inspection activity, the DG prepares his Final Inspection Report and delivers it to the EC (see Diagram.2). In this process, most of the sensitive information specified by the ISP, which has been designated into the certain category of the TS's confidential information criteria might be de-classified or extracted without disclosing anything sensitive, by mutual consent between the DG and the ISP representative.
Circulation of the Final Inspection Report is somewhat controversial. In accordance with the case of CTBT, inspection report should be distributed to the member of the EC (51 states signatories representing each region) and other state signatory at the same time. In other words, distribution of the Final Inspection Report means, everything written in the paper will be open to the more than 100 states as for 'official use only' information.

(2) Inspection Reports

In the course of inspection activities, inspector will be acquainted with the information, which might be difficult to distinguish the OSI relevant information from the OSI irrelevant and sensitive information of the ISP. Therefore, information obtained in the IA should be handled by the TS's OSI confidential information management system with appropriate level of protection at first, which has been designated by the ISP in accordance with his domestic information regulation. Using this information with appropriate measures for access control, inspector can continue their investigation. Then conclusively, the DG distinguishes the information relevancy[30] and prepares the Inspection Reports in his name.

Diagram. 2 Judgment of Relevancy in each occasion



Inspection Reports consist of several types of information, including 1) a description of activities conducted by the IT, 2) the factual findings of the IT relevant to the purpose of OSI, 3) an account of the cooperation granted during the inspection, 4) a factual description of the extent of the access during the inspection and 5) any other details relevant to the purpose of OSI[31].

[30] Definition of "factual findings" is somewhat controversial because it will change according to the situation. If the inspection can provide reasonable and scientific assurance that the suspected nuclear test explosion is absent, the purpose of the OSI is success and not a failure. Lfft, Edward "Iraq and the values of on-site inspection" Arms Control Today, Arms Control Association, November 2004. (Website) http://www.armscontrol.org/act/2004_11/lfft.asp?print

[31] CTBT Article IV Paragraph 62 "report of an on-site inspection " stipulates that those 5 types of information shall be contained in the inspection reports.

Sole reason to disclose the inspection relevant information is to create a report to the EC. In the case of CTBT, several formats of report will be created and distributed to the EC and other state signatories in each specific occasion as appropriate (paragraph 64, Article IV of the Treaty). This report should never contain the inspection 'irrelevant' sensitive information of the ISP.

(3) Confidentiality Undertakings

In accordance with precedent examples of the OPCW[32] and the IAEA[33], when an OSI has been approved by the EC, inspector, inspection assistant, TS staff and internal / external supporting staff should sign a covenant of the confidentiality undertaking with the DG. This confidential undertaking shall include the following pledges:

> 1) Breach of my obligation not to disclose confidential information without appropriate authorization, as provided for in the terms and conditions of my employment with the Organization, including this undertaking, may result in the imposition of disciplinary measures as provided for in the staff regulation and rules (etc).
>
> 2) Legal proceedings could be initiated against me in any applicable national jurisdiction, during or after my employment with the organization, in the event of a breach of my obligation not to disclose confidential information without appropriate authorization, and that, for such purpose, the Director General may waive any immunity, which may pertain to me.

With the stringent arrangements such as the waiver of privileges and immunities, confidentiality of the information will function in the OSI regime.

(4) Communication and Data Transmission

The Treaty and the Protocols permit the secured communication between the IT and the DG (the TS) at anytime they wish[34]. Both of the IT, the DG and the TS has assured the inviolability of communication in accordance with the Vienna Convention on Diplomatic Relations. Considering the contextual approach of this provision, even if the ISP requests to disclose the encryption key, the IT, the DG and the TS has no obligation for sharing it. Nowadays, there are several means of international communication and most of them allow the IT to use the high-speed transmission of raw data obtained[35] by

[32] Confidentiality undertaking of the OPCW
(Website) http://www.opcw.org/na_infopack/3_legal_series/OPCW-The%20Legal%20Texts/English/24-1.pdf

[33] Confidentiality undertaking of the IAEA
(Website) http://www.iaea.org/About/Policy/GC/GC42/Documents/gc42-12.html

[34] CTBT Part 2 of the Protocol paragraph 27 (c) formulates as follows; “The papers and correspondence, including records of the IT shall enjoy the inviolability accorded to all papers and correspondence of diplomatic agents pursuant to Article 30 paragraph 2 of the Vienna Convention on Diplomatic Relations. The IT shall have the right to use codes for their communications with the Technical Secretariat;”

[35] Although it is controversial issue, there are precedent examples in the IAEA Safeguards and the OPCW routine inspections. Lfft, Edward “The universe of on-site inspections” Arms Control Today, Arms Control Association,

the inspection techniques. Actually, data transmission from Base of Operations to the TS is not explicitly prohibited by Treaty and the Protocols. In fact, considering the limited number of inspector deployed in the IA, cross checking of the Results of the Observation Measurement and Analysis (ROMA)[36] between the Base of Operations and the operation support center in the CTBTO is essential[37]. Using the 'Need to Know' principle and the TS's OSI confidential information management system, this procedure of communication and data transmission will function effectively.

CONCLUSION

For past few years, protection of OSI confidential information is one of the most complicated and controversial issues. In the light of its intrusive nature, OSI confidential information management is deeply committed to national security and commercial interest of the states signatories. Most important thing is to take the balance between the consolidation of effective and efficient the OSI regime and protection of national sovereignty of state signatories. If the reinforcement of the IT's capability to correct the relevant information is too intrusive to the states worrying about to be inspected, sovereignty of state signatories will be exposed to risk and the OSI operational manual will not be approved by the Conference of the States Parties. On the other hand, if the reinforcement of the ISP's power and function is too excessive to protect her sensitive information, the inspection activity will not function effectively and advocates of CTBT OSI will be disappointed at the conference.

As a matter of reality, Treaty and the Protocols are the results of compromise during the past negotiation in Geneva. Sometimes it is very difficult to differentiate the original meaning of the Treaty languages such as 'to protect sensitive installation', 'to protect the confidentiality of information', 'prevent disclosure of confidential information and data' and so on. However looking at the practical issues involved with the inspection, it is necessary to eliminate the ambiguity over those controversial topics.

Again, without taking the balance with effectiveness of inspection and protection of national sovereignty, it is definitely difficult to establish the OSI regime, powerful

---

November 2004. (Website) http://www.armscontrol.org/act/2004_11/lfft.asp?print

[36] Conceptually, ROMA is document, which consists of results of observation, measurement and analysis including certain conclusion derived from each OSI activity in the field. In accordance with the CTBT Part 2 of the Protocol paragraph 60 (g), inspection record should be shared with the ISP representative at its request. Then if the ISP wish to clarify the fact written in the IT record, ISP can make recommendations at any time to the IT regarding the possible modification to of the inspection plan and re-examine the conclusion (see CTBT Part 2 of the Protocol paragraph 61 (a)). With this regard, ROMA would be a most suitable solution for this process.

[37] In accordance with the treaty, CTBT Article II paragraph 43 (f) gives clear details about the TS obligation to provide its technical support to the IT during the OSI activity.

enough to maintain a deterrent. OSI is the fort of ‘last resort' to verify the compliance with the CTBT. In consideration of facilitating the real-life of inspection, protecting OSI confidential information under the stringent system inside of the TS is a centerpiece to be considered.

CTBT OSI is the best case where how an effective and well-balanced verification system would be introduced. In the light of the treaty’s entry into force, smooth progress in improving of the OSI system is vital to promote the ratification of remaining Annex II states. As was mentioned in the beginning, the OSI operational manual comprises the heart of the OSI regime. Therefore, elaboration process of the OSI operational manual should be accelerated in good shape without further delay. Also a practically visualized concept of confidential information protection should be somehow established as one of the core problem of the OSI operational manual.