

System for the Protection of Confidentiality under the 1993 Chemical Weapons Convention: Challenges of Confidence and Effectiveness

Dr. Dridi Mohammed Mokhtar

Faculty of Political Sciences and International Relations, University of Algiers 3

Abstract- This study deals with the system of protection of confidential information under the Chemical Weapons Convention of 1993, since it is one of the most important aspects addressed by the Convention as well as its crucial importance for effective verification of compliance with its provisions.

States Parties and other stakeholders need strong safeguards to prevent the disclosure of confidential information and data circulating in the context of the implementation of the CWC, whether it relates to national security or to the business and chemical trade. Similarly, Member States should be assured that verification, on-site inspections and other monitoring and oversight bodies will not seek further relevant information, and that the information obtained will remain confidential if necessary.

To ensure the protection of confidentiality, the Organisation for the Prohibition of Chemical Weapons (OPCW) has established a strict system to regulate the handling of confidential information by the Technical Secretariat, establishing rules and regulations to classify the confidentiality of information and data provided by States Parties or collected by the OPCW, as well as the mechanisms necessary to protect such information, and address various potential violations.

Although the CWC's confidentiality protection system is comprehensive and rigorous, the question remains about how effective it is in practical implementation and whether it actually responds to the concerns of States parties and stakeholders.

Key words: The Organisation for the Prohibition of Chemical Weapons (OPCW) -1993 Chemical Weapons Convention (CWC) –Protection of Confidential Information – Verification System on Compliance with the Convention.

ملخص- تتناول هذه الدراسة نظام حماية المعلومات السرية بموجب اتفاقية الأسلحة الكيميائية لعام 1993، بالنظر إلى أن هذا النظام هو أحد أهم الجوانب التي تتناولها الاتفاقية علاوة على أهميتها الحاسمة للتحقق الفعال من الامتثال لأحكامها.

تحتاج الدول الأطراف وأصحاب المصلحة الآخرون للحصول على ضمانات قوية لمنع إفشاء المعلومات والمعطيات السرية المتداولة في إطار تنفيذ اتفاقية الأسلحة الكيميائية، سواء ما تعلق منها بالأمن القومي أو بقطاع الأعمال والتجارة الكيميائية. وبالمثل، يجب أن تطمئن الدول أعضاء المنظمة إلى أن التحقق، وإجراء عمليات التفتيش الموقعي وغيرها من أنشطة هيئات الرصد والرقابة، لن تسعى للحصول على مزيد من المعلومات التي لا صلة لها بالموضوع، وأن المعلومات التي حصلوا عليها سوف تبقى سرية إذا اقتضت الضرورة ذلك.

لضمان حماية السرية، أنشأت منظمة حظر الأسلحة الكيميائية نظاما صارما لتنظيم التعامل مع المعلومات السرية من قبل الأمانة الفنية، فوضعت قواعد وضوابط لتصنيف سرية المعلومات والمعطيات المقدمة من الدول الأطراف أو التي تجمعها المنظمة نفسها، فضلا عن الآليات الضرورية لحماية هذه المعلومات، وكذا الإجراءات التي يجب اتخاذها لمعالجة مختلف الانتهاكات المحتملة.

على الرغم من أن نظام حماية السرية في اتفاقية الأسلحة الكيميائية جاء متكاملًا وصارما، فإن الإشكالية تبقى مطروحة حول مدى فاعليته أثناء التنفيذ العملي، وما إذا كان يستجيب فعلا لانشغالات الدول الأطراف وأصحاب المصلحة.

الكلمات المفتاحية: منظمة حظر الأسلحة الكيميائية - اتفاقية الأسلحة الكيميائية
عام 1993 - حماية المعلومات السرية - نظام التحقق.

Introduction

The Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (the 'Chemical Weapons Convention': CWC) concluded under the auspices of the United Nations, and entered into force in 1997,¹ is the first multilateral treaty to ban a whole category of weapons of mass destruction, thus constituting an important element of the current legal framework for arms limitation and disarmament in the world.

The Chemical Weapons Convention, referred to hereinafter as the Convention, in addition to its complete prohibition of chemical weapons, has created a very strict verification system which aims at ensuring that States parties respect their obligations in the destruction of their stockpiles of chemical weapons, their production and proliferation, as well as their control measures on toxic chemicals used in the business industry to ensure that they are not diverted for chemical weapons production.

The protection of confidentiality is a particular feature of the Convention. With regard to State secrets, provisions to protect confidentiality were necessary by virtue of the Convention's far-reaching verification provisions (in particular, the provisions on challenge inspection that can also be invoked for undeclared facilities, including secret military installations). At the same time, the Convention's provisions on international verification affect the chemical industry and its legitimate activities.

The issue of the protection of confidential information was perceived as particularly acute and crucial from the beginning

(1) As of April 2016, 192 states have given their consent to be bound by the CWC

of the Geneva negotiations on the CWC. The structure and scope of the verification regime on which the CWC will rely was a subject of major discussions. There was a widely shared awareness that the implementation of the CWC could pose the highest risk of loss of confidential information ever encountered in arms control. A difficult balance had to be reached between the degree of intrusiveness necessary for effective verification and the preservation of legitimate confidentiality.

Negotiators focused their attention on developing special mechanisms to protect the confidentiality of military and business data and information. The system was designed for the purpose of reducing the risk of disclosure of information that would harm the interests of States Parties and chemical business firms with respect to the security, technological or commercial competitive interests.

To that end, the Convention included several provisions relating to the handling and processing of sensitive information. In addition to the Annex on Confidentiality, the negotiators decided to refer the issue of the protection of confidentiality to the Conference of the States Parties, which had already issued at its first session a decision containing a basic text entitled “OPCW Policy on Confidentiality”.

²This decision contains a set of principles and binding guidelines for the Organisation’s organs, including the Technical Secretariat. This document , hereinafter referred to as the “Privacy Policy”, defines the policy pillars and guidelines to be followed by the Organisation with respect to the protection

(2) OPCW Policy on Confidentiality, decision of The Conference Of States Parties (C-1/DEC.13, 1997)

of the confidentiality in activities relating to the application of the Convention, classification of information by degree of confidentiality and processing, as well as actions to be taken in case of breach of confidentiality.

Based on this principle, the Convention sets out a balance between the disclosure necessary to enhance confidence in the Convention and to prevent disclosure of confidential information for the protection of national security and chemical business industry interests, taking into account constitutional obligations.

1. Determining the confidential nature of information

The Convention addresses the concept of information in a broad and comprehensive sense, including, *inter alia*, written documents, samples, photographs, audiovisual materials and computer materials, as well as any knowledge gained or communicated by any means of communication or any sensory means.³ The term information also applies to any information or data that any individual or organisation, including its employees and equipment may obtain, derive or retain in the implementation of the Convention. The term “data” appears in different contexts of the Convention. This term involves information provided in a particular structure or form, such as that contained in a national declaration. However, when interpreting the text from the point of view of confidentiality, there is no significant distinction between “information” and “data”. The information is confidential, under the Convention, if it is so described by the issuing State. Accordingly, any information received by the Organisation from a State about the activities of another State requires a bilateral description until the information in question has assumed

(3) Annex on the Protection of Confidential Information, Decision of the Conference of States Parties(«Confidentiality Annex”)

that status. Outside this scope, information may be considered confidential if the Director-General of the Organisation deems it reasonable to expect that unauthorized disclosure would cause damage to the State or a business firm to which it refers.

The sensitivity of an element of information is determined taking into account, *inter alia*, the degree of implied harm that disclosure may cause to a State Party or any subsidiary body, to the Convention or to the Organisation. Accordingly, all the information produced by the Organisation and its constituent elements are classified according to three specific categories that correspond to the degree of sensitivity of confidential information from the least sensitive to the most sensitive.

1.1 OPCW CLASSIFICATION SYSTEM FOR CONFIDENTIAL INFORMATION

All information acquired or produced by the OPCW,⁴ referred to hereinafter as the Organisation, and its constituent elements which are determined to be confidential must be given a classification, based on established categories which correspond to the level of sensitivity of confidential information. In its application, the classification system will not impair the requirement for effective verification of compliance with the Convention. The essential factors to be considered in determining the level of sensitivity of an item of information are: (a) the degree of potential damage which its disclosure could cause to a State Party, any other body of a State Party, including a commercial firm, or to any national of a State Party, or to the Convention or the Organisation; and (b) the

(4) The OPCW: Organisation for the Prohibition of Chemical Weapons is the implementing body of the Chemical Weapons Convention) based in The Hague, the Netherlands, it is an independent international supervisory organisation within the UN system but not a specialised UN agency.

degree of potential particular or selective advantage its disclosure could offer to an individual, a State, or any other body, including a commercial firm. These factors correspond to the factors used in determining the confidentiality of information.

Based on these guiding factors, and the specific classification criteria set out below, confidential information are classified according to the following categories, in increasing order of sensitivity: - OPCW RESTRICTED – OPCW PROTECTED – OPCW HIGHLY PROTECTED

1.2 Classification category: OPCW RESTRICTED:

This category comprises information of which the authorized disclosure would be prejudicial to the effectiveness or credibility of the Convention, or prejudicial to the interests of a State Party or of a commercial or governmental body or of a national of a State Party. Forms of information that might be classified OPCW RESTRICTED when they are acquired or generated by any means by the Organisation, are : (a) the initial and annual reports and declarations provided by States Parties under Articles III, IV, V and VI and in accordance with the Verification Annex, where these documents are considered by originating States Parties as being of this level of sensitivity; (b) general reports on the results and effectiveness of verification activities; and (c) information to be provided to all States Parties in accordance with other provisions of the Convention.

1.3 Classification category: OPCW PROTECTED:

This category comprises information of which the authorized disclosure may cause substantial damage to the effectiveness or credibility of the Convention, or to the interests of a State Party or of a business or governmental body or of a national of a State

Party. The following forms of information might be classified as OPCW PROTECTED when they are acquired or generated by any means by the Organisation: (a) the initial and annual reports and declarations provided by States Parties,⁵ where these documents are considered by the originating States Parties as being of this level of sensitivity; (b) unpublished technological information about production processes and facilities, and technical information about industrial products; (c) less sensitive or more general information related to commercial transactions and the cost factors of industrial processes and production; (d) detailed initial reporting on an inspection, including information on anomalies or incidents at facilities, and inspection reports.

1.4 Classification category: OPCW HIGHLY PROTECTED:

This category comprises sensitive confidential information of which the unauthorized disclosure would cause serious damage to the effectiveness or credibility of the Convention, or its aims and purpose, or cause serious damage from the point of view of national security or commercial secrecy to the interests of a State Party or of a commercial or governmental body or a national of a State Party. Examples of the forms of information that may be classified as highly protected are as follows: (a) the initial and annual reports and declarations provided by States Parties; (b) samples taken from inspected sites and returned samples from designated laboratories, and results from analysis of samples.

(5) Articles III, IV, V and VI of the CWC Convention; Verification Annex: Part II. "General Rules of Verification".

2. GENERAL PRINCIPLES FOR HANDLING CONFIDENTIAL INFORMATION

The OPCW requires the minimum information necessary to carry out its mandate. The staff members of the Secretariat shall have special obligations during their participation in verification activities, giving them access to confidential information, whether civilian or military, including information disclosed by the State Party pursuant to its obligations under the Convention, with respect to consultation and cooperation⁶, as well as to sensitive information that do not relate to the purposes of the Convention in the event of disclosure of such sensitive information.

Employees who have access to confidential information are obliged to exercise the utmost discretion with regards to all matters of official business. They must not communicate to any person any information known to them by reason of their official position which has not been made public. Technical Secretariat employees are also strictly required not to divulge confidential information to any uthorizedd person even after the end of their duties.⁷ In this respect, each staff member is required to enter into an individual agreement with the Technical Secretariat to protect confidentiality during each period of employment and within the next five years after completion of his / her function.⁸

The Convention provides the basis of the Organisation's obligations to respect confidentiality. Thus, the OPCW is obliged to limit its investigations to what is actually necessary with

(6) OPCW Policy on Confidentiality, Part VI, p.10

(7) (OPCW Policy on Confidentiality 2 C-I/DEC.13/Rev.1Annex page 23)

(8) See Convention, Annex on Confidentiality, <https://www.opcw.org>.

minimal interference.⁹ It must take every precaution to protect the confidentiality of information on civil and military activities and facilities coming to its knowledge in fulfilling its function according to the Convention.¹⁰

To ensure the protection of confidential information, the Convention had established a fundamental principle whereby the Technical Secretariat requests only as much information and data as is necessary for the effective discharge of its responsibilities. This basic principle implies that firstly, the level of sensitivity of confidential information is the criterion that governs the procedures in which information is made available to those who receive it and the means used to protect it. Secondly, it is necessary for those authorized to receive confidential information in accordance with the proof of their “need to know” identified in relation to the purposes of the Convention.

2.1 Need-to-know principle:

The need-to-know principle is the governing principle for determination of the scope of access and the recipients of dissemination of information. There is no absolute right within the Organisation to receive confidential information: no individual staff member of the Secretariat and no member of any organ of the Organisation is entitled by virtue of status or level alone to have access to any items of OPCW confidential information.¹¹

By and large, the right to access confidential information is granted according to the circumstances of each individual case in

(9) See paragraph 46 of Part X of the Verification Annex and paragraph 14 of the Confidentiality Annex.

(10) Paragraph 5 of Article VIII of the CWC

(11) Convention, OPCW Policy on Confidentiality, Part VI, paragraph 2.3

accordance with the determination of a functional “need to know”. There is an unconditional need to inform States parties of certain information, such as where the technical secretariat routinely provides States parties with the data they request regarding initial and annual declarations submitted by States parties. This necessity and related provisions are seen as creating an unquestionable need for knowledge for each State to ensure that States Parties continue to comply with the Convention.

2.2 dissemination of confidential information

As regards the dissemination of confidential information from the Technical Secretariat to the other organs of the Organisation, a contradiction may arise in the application of the provisions of OPCW Policy on Confidentiality.¹² On the one hand, the Technical Secretariat and its Director-General are responsible for the protection of confidential information, as the structure of the Organisation established in such a manner as to put the Technical Secretariat, headed by the Director-General, in the position of a subordinate of the Conference and the Executive Council (organs authorized to obtain the confidential information necessary for their function. As a result, the confidential nature of the information becomes somewhat relative, since the information, provided by the Secretariat to the Conference or The Council, loses its confidential nature by making it available to States Parties or to members of the Executive Council. Although the confidentiality policy does not address this situation, it is assumed that States parties, insofar as they are obliged to maintain the confidentiality of information received through official channels, are also obliged to maintain

(12) Convention, OPCW Policy on Confidentiality, Part VI, Op.Cit , par - graphs 1.3 and 1.4

the confidentiality of the information they have received from the Conference or the Executive Council.

In assessing the effectiveness of the system of confidentiality protection, it can be argued that based on the assumption that Member States receiving confidential information act in good faith in the implementation of their obligations, the confidentiality protection mechanism appears sufficient for confidential information of a commercial or competitive nature. However, this seems not to apply if the information is of a political nature or is related to national security of States. In such a case, this information could automatically become available to all representatives of States at the Conference or the Executive Council, and there seems to be no solution to this problem.

3.Administration of the confidentiality regime

Confidential information are transmitted in particular to the Technical Secretariat. The source of information could be declarations made by States Parties under the verification requirements of the Convention. This information can be the result of an on-site inspection, particularly in the reports of the inspection. Finally, information can be brought to the attention of the Secretariat by a Member State in the context of an illustrative procedure or on the occasion of the launching of a challenge inspection.¹³

(13) Article IX of the Convention grants each State Party the right to request an on-site challenge inspection of any facility or location under the jurisdiction of any other State Party in order to clarify and resolve any questions concerning possible non-compliance with the provisions of the Convention. Such inspections might be conducted anywhere and without delay by an inspection team designated by the OPCW Director-General in accordance with the Convention's Verification Annex.

3.1 Responsibility of the Technical Secretariat

The collection and reception of confidential information are critical to the completion of the verification process. Thus, the effectiveness of the safeguards surrounding the processing of such information is essential to maintaining an adequate level of trust among the parties concerned to ensure the proper functioning of this system. In its internal handling and processing of information, the Technical Secretariat in turn generate confidential information, especially in the carrying out of its activities of analysis and technical evaluation of the data obtained under the monitoring procedures.

Under the Director-General's supervision, the Technical Secretariat is entrusted with the primary responsibility for the protection of confidential information, where a system is developed for the circulation of confidential information within the Secretariat in accordance with the guidelines contained in the Convention, including the Privacy Policy and the Confidentiality Annex. The Director-General is also responsible for overseeing the extent of compliance with the confidentiality system within the Secretariat and has accordingly, the duty to submit an annual report on the implementation of this system.

Moreover, confidential information may be issued by the Technical Secretariat in the direction of the political organs of the Organisation or in the direction of Member States. The Confidentiality Policy confirmed that the issuance of confidential information by the Technical Secretariat to the Conference of States Parties or to the Executive Council is completed in accordance with the "general principles" governing the issuance of confidential information. However, the term "general principles"

was not clearly explicated in the decision. Most probably, this term refers at least to the two basic principles governing the conditions of access established in the policy of confidentiality, namely, the need to regulate access to classified information according to their classification; on the other hand, the dissemination of such information within the organisation should be strictly limited to those who need to know about it.¹⁴

3.2 Safeguarding of confidential information

The Technical Secretariat is also responsible for the safe storage of information relevant to the Convention. There is strict control over the access and processing of information by OPCW staff. The Technical Secretariat has developed procedures for file preservation, release and record-keeping in order to monitor access to information. Copies of confidential information may only be made under the supervision of another employee and must be authorized by an official member of the staff. The information must be processed and maintained in such a manner as to prevent identification of the entity to which the information relates. For each site in the Technical Secretariat, a formal description identifies the necessary access to confidential information.

The order and storage conditions, as well as all protection criteria for this information, vary in terms of the degree of sensitivity depending on the category to which they belong. The same applies to the way in which it can be accessed within the Secretariat. The requirements for each category are added to the general obligations applicable to all staff.

(14) OPCW Policy on Confidentiality, Part VI, P.22

3.3 Release of information outside the Organisation and Member States

The Organisation may recourse to release of information which it holds in connection with the implementation of the Convention. ‘Release’ of information by the OPCW refers to the approved disclosure of information beyond the Organisation itself, including all its constituent elements, and beyond the governments of States Parties (specifically, beyond governmental organisations and authorised entities or individuals within States Parties concerned with the operation of the Convention).

Confidential information outside the Organisation is released only in accordance with the “need to know” principle, meaning that the intended recipient has a clear need to know the confidential information in accordance with its role in the implementation of the Convention. When there is a clear need to release confidential information, the Director-General prepares a draft proposal for the release that has been consulted and reviewed by the parties concerned. The decision to release the proposed version should fully examine the factors of the confidentiality report and the classification of such information. Where necessary, the information proposed to be released should be processed in less sensitive forms so as to avoid disclosing any confidential information that is not relevant to the release.

4. Breaches and Violations of Confidentiality Obligations

A breach of the obligation to protect confidentiality includes any unauthorised disclosure of OPCW information to any individual, or government or private entity, regardless of the intention or the consequences of the disclosure. It can also be associated with misuse of information to gain a personal

advantage or to benefit or damage the interests of a third party. A violation of obligations concerning the protection of confidential information is deemed to have taken place if there has been non-compliance with the specified procedures for the handling, protection, release and dissemination of confidential information so as to create a clear risk of unauthorised disclosure, with or without such disclosure actually occurring. In practical terms, there is considerable overlap between a breach of confidentiality and a violation of obligations to protect confidential information.

The Convention identified two mechanisms to address different types of violations of an obligation to protect confidential information.¹⁵ The first one, concerns the authority of the Director-General to initiate an investigation, the second is carried out by the Commission for the settlement of Disputes.

4.1 Investigation by the Director-General

The Director-General is entrusted with specific powers, in accordance with the Confidentiality Policy, to initiate an investigation if he becomes aware that there is a reasonable possibility, or clear risk, of unauthorised disclosure of confidential information occurring, *inter alia*, in a manner: (a) which violates the policy or guidelines of the Organisation established for the handling, protection, release and dissemination of confidential information; or (b) which could adversely affect the object and purpose of the Convention or the interests of the Organisation, a State Party, or a commercial or governmental body or a national of a State Party, or could offer particular or selective advantage to

(15) In 2000, for instance the OPCW then Director-General in his report to the Conference of States Parties noted that 19 confidentiality incidents were recorded in 1999, most of them minor procedural breaches.

an individual, a State, or any other body, including a commercial firm.

The Director-General may initiate an investigation in case of violation by the staff of the Secretariat or by another person or entity uthorized outside the Secretariat or by a representative or official of a State Party. The Director-General may also investigate any allegation by any State Party of a breach of confidentiality. The purpose of the investigation is to establish whether there has been a breach of confidentiality or breach of the procedures for the circulation, protection, dissemination or release of confidential information and the seriousness of any violation, including the degree and nature of any damage caused. The investigation should also examine ways of strengthening the confidentiality system to prevent any recurrence of violations or breaches of the procedures.

4.2 Scope of the investigation

The aim of the investigation is to establish whether there has been a breach of confidentiality or a violation of the handling, protection, dissemination or release procedures for confidential information, and the severity of any breach including the degree and nature of any damage caused. The investigation should also consider ways of enhancing the confidentiality regime so as to prevent any recurrence of a breach or violation of procedures. During the investigation, the Director-General may take provisional restrictive measures throughout the investigation period, such as exemption from certain responsibilities for the staff member involved, or denial of access to certain information. Immediate action may be proposed in consultation with the Executive Council to protect all legitimate interests that may be affected by the alleged breach or breach of confidentiality.

The investigation procedure is kept confidential and subject to the application of the need –to know principle. The related report is prepared in two forms, full form which shows the facts that have been established in detail, and a modified one, in which certain confidential material are removed in order to ensure that confidential information related to the violation is not disclosed beyond the authorized. The full report must be treated as confidential and classified and dealt with in accordance with its sensitivity, and should be available only to those directly involved in the investigation. The report may be made available as amended to any State Party upon request. Any inquiry or report, which ends with a violation or breach, will result in four general categories of actions as appropriate:

4.3 Role of the Commission for the Settlement of Disputes Relating to Confidentiality

The CWC provided for the establishment of a “Commission for the Settlement of Disputes Relating to Confidentiality” hereinafter referred to as the “ Commission on Confidentiality” as a subsidiary organ of the Organisation of the Conference of the States Parties. Its primary task is to consider cases of violation of the confidentiality provisions of the Convention involving both a State party and an organisation. The Committee shall also consider the issues entrusted to it by the Conference in a confidentiality dispute and, finally, it may be chosen by two States Parties between whom a dispute arises on a question of confidentiality as a means of resolving their dispute.

In general principle, cases are brought before the Confidentiality Committee when a dispute arises over an investigation report made at the request of a State party concerning a breach of confidentiality by a staff member of the Technical Secretariat.

However, the annex relates to confidentiality stipulates that “the Committee shall consider cases of violation involving both a State Party and an organisation”. States parties may therefore raise cases of confidentiality directly before this Committee without the need for a prior request for investigation. In either case, we are in conflict between the Organisation and a State party and not between the latter and the staff of the Organisation.

The Commission’s powers in its mandate to resolve disputes related to confidentiality, as already mentioned, raises some questions regarding the scope of its function. According to the provisions relating to the protection of confidentiality, the Commission is entrusted with a wide range of actions, whereby it can resort to all appropriate means of settling disputes, from reconciliation to mediation to arbitration. However, the organisation’s policy on confidentiality clearly demonstrates its preference for mediation and completely neglects other mechanisms in resolving conflicts where the Organisation is a party. In addition, there are some ambiguities regarding the search for the appropriate means of resolving disputes.

5. Disciplinary measures against a breach of confidentiality:

If, at the end of the investigation, it is determined that a staff member of the Secretariat has committed a violation or breach of confidentiality provisions, the Director-General is obliged to take appropriate disciplinary action in accordance with the Staff Regulations and Rules of the Organisation, with the possibility of considering lifting their immunity. The lifting of immunity shall be considered only in the case of a serious breach and when individual responsibility is established and the damage caused is proven. The immunity should be lifted after confidential consultations with regard to the possible triggering of the relevant

national jurisdiction. The individual confidentiality agreement signed by the staff member should also be reviewed for possible use in the proceedings.

If the report finds that there has been a breach of confidentiality by a former staff member of the Secretariat, the Director-General may decide to take any action possible in accordance with the provisions of the Staff Regulations. Such actions may include deprivation of pension benefits earned by the staff member during his or her period of service with the Organisation or cancellation of remaining financial or other benefits.

5.1 Legal proceedings within national jurisdiction:

If the Director-General's investigation concludes that a natural or juridical person (including a commercial entity) is subject to the national jurisdiction of a State Party that appears to be responsible for a breach of confidentiality, or has obtained a private benefit from a breach of confidentiality or otherwise implicated in a violation, the State Party concerned may be requested to take the appropriate legal measures in accordance with the OPCW Confidentiality Policy.

If a natural or juridical person are found responsible for a breach of confidentiality which is or is in any other capacity within the jurisdiction of a State not party to the Convention, the Director-General may request the Executive Council or the Conference to hold consultations aimed at encouraging that State to initiate, or facilitate taking appropriate actions to assist in taking legal action resulting from the violation.

5.2 Action taken when a State Party appears responsible:

If the Director-General's investigation concludes that a State Party appears to be responsible or that a staff member appears to be responsible for a breach of confidentiality, that State Party shall, to the extent possible, assist the Director-General in resolving the matter,

Where a breach of confidentiality has been established by a staff member of the Technical Secretariat and has caused harm to a State Party or to one of its business firms or to a national of that State, that State shall not be entitled to claim financial damages to the Organisation.¹⁶ The reason why the Organisation cannot be held accountable is that it was intended to encourage States to seek ratification of the Convention in exchange for alleviating the burden of the financial contributions of States Parties to the financing of the Organisation. Thus, the possibility of reparation for damage to a particular State resulting from the disclosure of its confidential information is born by the official responsible for the disclosure of his own money, after being convicted by a national judicial body, and only after the lifting of his immunity. This situation seems to have been the best compromise reached by the negotiators on the conclusion of the Convention.

(16) The Confidentiality Annex, D 22

Conclusion

Confidentiality is in fact one of four central pillars of the CWC. This is reflected in its Confidentiality Annex, which, unlike NPT safeguards agreements,¹⁷ provides great detail about the extensive system for maintaining confidentiality at every level. Hence the OPCW has an Office of Confidentiality and Security, a Manual of Confidentiality Procedure (which has been almost continuously updated) and a Confidentiality Commission to monitor the maintenance of confidentiality, settle disputes about confidentiality and make recommendations on improvements. An Archive Management System registers and tracks electronically all confidential documents and materials received. Although the confidentiality system established by the OPCW is by no means perfect and there is always room for improvement, it has achieved a creditable record in information protection while maintaining effectiveness in verification.

(17) Although there is no mention of the principle of confidentiality in IAEA Statute, the safeguard (INFCIRC/66) agreement, concluded in 1965, obliged the IAEA to 'take every precaution to protect commercial and industrial secrets' (military secrets were notably absent because safeguards only applied to peaceful nuclear facilities).