(2006) 10 SYBIL 117–132

DIPLOMATIC AND CONSULAR LAW IN THE INTERNET AGE

by WON-MOG CHOI*

The web of our life is of a mingled yarn, good and ill together.[1]

The evolution of diplomacy may involve taking advantage of technological developments such as the Internet. The Internet has become an indispensable means of diplomatic negotiations and communications with various interest groups. In this new environment, the traditional law of diplomacy and consular affairs must also evolve through new interpretation of existing rules. If some of those rules are deficient or insufficient to regulate "Internet diplomacy", new rules ought to be created. International rules on the inviolability of premises, inviolability of documents and archives, freedom of official correspondence, privilege of tax exemption, and immunity from judicial jurisdiction must be newly interpreted and applied so as to reflect the cyber diplomacy environment. In addition, new rules of inviolability for the "cyber diplomatic or consular bag" must be created.

I. INTRODUCTION

With the phenomenal growth of communication technology, the Internet has unprecedented potential to affect education, politics, society and the everyday lives of people as no other medium has had in the past.[2] One of the reasons for this is the Internet's usefulness in helping many people overcome geographical barriers and share information freely. With the Internet, it is no longer necessary to maintain costly physical establishments or contact points for sharing and exchanging information. Virtual contact points in cyber-space enable people to communicate easily, even with multiple parties simultaneously. The Internet may also enable an information seeker to eliminate the "middle-man", such as bureaucracy, while trying to reach a foreigner or a foreign region.

With this distinct phenomenon, the Internet is burgeoning as one of the channels for conducting diplomacy. An increasing number of States are exchanging diplomatic documents with their foreign missions in electronic forms through the Internet. The volume and frequency of Internet communication between foreign missions and nationals of the sending State residing in the receiving State are also steadily increasing. Citizens may easily express

* Associate Professor of Law, Ewha Womans University, Seoul, Korea; S.J.D. (Georgetown); Attorney-at-law (New York Bar); Member of Editorial Board of the Journal of International Economic Law (Oxford). Formerly of the Korean Ministry of Foreign Affairs. E-mail: wmchoi@ewha.ac.kr. This paper is a refinement of an earlier study, which was supported by the Korea Information Strategy Development Institute (KISDI), and the basic idea of which was presented at the Symposium of New Challenges to International Law and Relations in the Internet Age, hosted by the KISDI and the Transnational Law and Business University (Seoul, Korea, 4 October 2004).

1 William Shakespeare, All's Well that Ends Well, Act 4, Scene. 3.

2 The Internet, originally a U.S. Department of Defense project, is a collection of electronic networks established for communication and information dissemination. See International Organization of Securities Commissions (IOSCO), "Report on Enforcement Issues Raised by the Increasing Use of Electronic Networks in the Securities and Futures Field", online: IOSCO <http://www.iosco.org/public docs/1997-report on enforcement issues-document03.html> (on file with the Fordham International Law Journal).

their opinions about diplomatic issues through the Internet. The rise of this new medium in diplomacy is attracting increasing attention in diplomatic communities.

What are the impacts that the Internet has on diplomacy? How will traditional forms of diplomacy change and adjust themselves in the emerging environment of "Internet diplomacy"? How can we apply the *Vienna Convention on Diplomatic Relations* (VCDR)[3] and *Vienna Convention on Consular Relations* (VCCR)[4]—the primary international laws on diplomacy and consular affairs—to such an environment? What about diplomatic agents conducting diplomacy in cyber space? Are they protected by the laws of diplomacy? What are their rights and obligations? Are diplomats destined to disappear with the development of even more advanced communication technologies such as a "super-Internet"? Or, will they survive and prosper, taking advantage of mass communication through the Internet? What would be the impact of the Internet on the obligations of pacific settlement of international disputes under the United Nation Charter? These are indeed challenging questions.

This paper attempts to shed light on the interdependent relationship between the Internet and diplomacy from a legal perspective, and to provide answers to the above questions. The paper is divided into four sections. In the first section, the impact of the Internet on diplomacy will be evaluated in general. In the second section, the relationship between the Internet and diplomacy will be analysed. The focus will be on the law of diplomatic immunity and privilege. In this regard, relevant provisions under the VCDR and the VCCR that have most bearing on that issue will be identified and analysed. In the third section, the international law of dispute settlement will be reviewed with regard to the interplay between the Internet and the law of diplomacy. For this purpose, several provisions under the United Nation Charter will be reinterpreted. The last section will summarise all of the analyses and provide suggestions for the future of diplomacy in the Internet environment.

II. Impact of the Internet on Diplomacy—The Emergence of "Internet Diplomacy"

Communication is vital to diplomacy. The nature of the Internet has rendered it an indispensable means of communication in this modern age and has given rise to the burgeoning of what we have termed "Internet diplomacy". Other factors contributing to this development are, among others, widespread access to telecommunications and availability of telecommunication equipment at low prices that enhance the capacity of many countries to participate in the Internet diplomacy. I will now describe how this new trend has emerged in diplomatic negotiations.

A. *Cyber Negotiations*

The Internet facilitates negotiations. Many logistical contacts may be made via Internet communication at the preparatory stage of diplomatic negotiations, which saves time and costs for diplomats. In addition, negotiations themselves may be conducted over the Internet, which reduces travelling time and costs for diplomats. Furthermore, communication over the Internet, unlike face-to-face debates between negotiators, is less confrontational and thus may facilitate the negotiation process.. Antagonistic public protests in negotiating countries in relation to such negotiations may also be avoided because negotiations conducted over the Internet are unlikely to attract the same degree of public attention as diplomatic meetings.

[3] *Vienna Convention on Diplomatic Relations*, 18 April 1961, 500 U.N.T.S. 95 [VCDR].
[4] *Vienna Convention on Consular Relations*, 24 April 1963, 596 U.N.T.S 261 [VCCR].

To these online negotiators, the time difference between different regions in the world is no barrier. During working hours, they may make an offer by sending an e-mail, which may be responded to by their counterparts at night. All that needs to be done by the former is to come to the office the next morning and, upon reading the response, prepare an agreed minute or decide whether or not to make a counter-offer. This arrangement is not a bad option for busy negotiators.

Since the Internet is worldwide and is available twenty-four hours a day for very little cost, a negotiator could have access to his or her counterpart from across the world. At any rate, with the Internet, negotiation channels are always open. An additional benefit of using the Internet as a negotiation channel is that it guarantees a certain degree of confidentiality in negotiations. E-mails, unlike faxes or telephone calls, are not as easily intercepted, especially where the files attached to the email are encrypted.

B. *Diplomacy in Public Opinion*

The Internet also offers opportunities for enhanced outreach to the general public, and these opportunities may be positively utilised by diplomatic communities. For example, the Internet may be used for educating the general public on certain issues which bear direct or indirect implications for diplomacy, or for drawing consensus on nationwide diplomatic issues. The greater the extent of connectivity of the public to the Internet, the better they can be informed for decision-making purposes. This, in turn, may contribute towards building a more effective diplomacy that enjoys domestic public support or a policy made more robust because of the benefit of public scrutiny and comment. Today, diplomacy needs to be more transparent. Contemporary democracy does not support nor encourage the continuation of diplomacy in a way it has been conducted. In other words, diplomacy can no more be conducted solely within the realm of inter-state communication with the presumption of invisibility of other stakeholders in the global community such as non-governmental organisations and public interest groups. No negotiations can be absolutely confidential and impervious to public attention.

C. *Consular Affairs*

The primary function of consuls is to protect nationals residing in foreign countries. The Internet has made it easier to discharge consular functions. Most nationals can easily report their loci or problems to consulates through consular web-sites and e-mails. Furthermore, a consulate may find out demands of their nationals and problems of its services in a more convenient way through the consulate web-page or e-mails, which may be shared with other consulates. Oftentimes, e-mail is used as a speedier mode of contact with desk officials in the headquarters. In addition, foreign ministries in most countries are equipped with an Intranet system, by which most of their staff can contact one another and share information.[5] Prompt responses from the headquarters also enable consulates to take quick actions to meet particular demands or problems at hand.

D. *Developing Countries and Diplomacy*

The Internet may contribute towards creating a more level playing field in the world of diplomacy. Setting up the minimal infrastructure that is required to link with the

[5] The Korean Foreign Ministry's intranet system is called "FATIS" (Foreign Affairs and Trade Information System), connecting 71 out of 146 Korean missions abroad. Source: Interviews with officials in charge of the FATIS system.

Internet, developing countries have the opportunity to leapfrog the "hard wire" technology that has been set up mostly by the developed countries. There is no need to have sophisticated technical infrastructure to utilise the Internet. For developing countries, therefore, the Internet represents an opportunity for development in many fields including diplomacy.

Taking advantage of the facilitated negotiations and enhanced transparency generated by Internet diplomacy, developing countries would be able to perform more powerful diplomatic activities and engage with developed countries on a more level playing field than previously. These days, there is a general tendency for many developing countries to form certain groups and participate in multinational negotiations as one group. This trend enables developing countries to duly reflect their interests and opinions in the negotiations, which makes the world diplomatic order fairer and more balanced. In this process, Internet diplomacy plays a significant role in converging opinions and drawing support for a variety of development agendas.

III. The Internet and The Law of Diplomatic Immunity and Privilege

A. *Inviolability of Premises*

It is widely accepted under international law that the premises of diplomatic missions and consular posts are inviolable. Inviolability usually means exemptions from the jurisdiction of the receiving State. If such inviolability is not given to such missions or posts, they will have substantial difficulties in performing their functions.

Thus, the VCDR declares that "the premises of the mission shall be inviolable"[6], and the privilege of inviolability extends to the private residence of diplomats.[7] A similar proclamation is made by the VCCR, except that there is no extension of inviolability to the private residence of consuls.[8] Since the Vienna Conventions are widely considered to be codification of customary international law in this field, it can be said that diplomatic and consular missions enjoy inviolability in every nation in the world, regardless of whether the nation concerned is party to the Vienna Conventions or not.

Elaborating on the meaning of "inviolable", the VCDR states that "the agents of the receiving State may not enter them, except with the consent of the head of the mission."[9] Thus, the first element of inviolability is the freedom of the premises from entry by authorities of receiving State. Even when crimes are being committed inside the premises of the diplomatic mission, the only way by which receiving State agencies can enter diplomatic missions is to obtain consent of the head of the mission. In the case of the premises of consular posts, the VCCR guarantees its inviolability but with certain limitations:

> the authorities of the receiving State shall not enter that part of the consular premises which is used exclusively for the purpose of the work of the consular post except with the consent of the head of the consular post or of his designee or of the head of the diplomatic mission of the sending State.[10]

Thus, for the premises of consular posts, it is possible that officials of the receiving State may enter the premises without obtaining the consent of the head of the post, as long as the officials secured the consent of the head of diplomatic mission or designee of head of

[6] Art. 22(1) of the VCDR.

[7] Art. 30(1) of the VCDR states: "The private residence of a diplomatic agent shall enjoy the same inviolability and protection as the premises of the mission."

[8] Art. 31(1) of the VCCR states: "Consular premises shall be inviolable to the extent provided in this article."

[9] *Ibid.*

[10] Art. 31(2) of the VCCR.

consular post. In addition, the officials may enter, even without the consent of anyone, any part of the premises of a consular post which is *not* used exclusively for the purpose of consular work. For example, the officials might enter the kitchen or dining room of consular posts without consent, if they have legitimate reasons to do so.

To apply these legal points to the subject of this article, one may envision a situation in which a diplomatic mission or consular post is used as a place for the commission of Internet-related crimes. For instance, computers inside a diplomatic mission may be used for the production of serious computer viruses or for the execution of cyber terror against communication facilities in the receiving State. Even if intelligence agents of the receiving State have reliable evidence of these criminal activities, the only way they can enter the premises of the mission is to obtain the prior consent of the head of the mission.

Where cyber crimes are committed on the premises of consular posts, the agents have more options. Firstly, entry into parts of the premises of consular post unrelated to consular function, is not restricted. Thus, the agents may enter these parts and gather more evidence from there. Secondly, agents may enter parts of the premises used exclusively for consular function, after obtaining the consent of either the head of the post or his designee, or the head of the diplomatic mission of the sending State. This means that the agents might enter the part of the premises used exclusively for consular function even against the will of the consulate general, if the ambassador of the same country permits such an entry.

Of course, there is always a diplomatic option: if the crime involved is serious enough, the receiving State may grant *persona non grata* to the staff of the mission or post,[11] or close down the mission or post to enter the premises.

The second element of inviolability involves the "protect[ion] [of] the premises of the mission against any intrusion or damage and [prevention] [of] any disturbance of the peace of the mission or impairment of its dignity".[12] The VCDR declares that states are under a "special duty to take all appropriate steps" to protect this element of the inviolability.[13] This duty is also stated in the VCCR.[14] This second element of inviolability is closely linked with the first element in that the latter is the inviolability privilege of the mission or post against intrusion by the receiving State agency whereas the former is the right against intrusion by any private person or entity. It is thus logical to interpret the two elements in a harmonious way in any overlapping situations. For instance, in the course of taking measures to prevent any persons or objects from intruding on the diplomatic mission or consular post, agents of the receiving State must obtain consent of the head of the premises if entry into the premises is necessary.[15]

What if there is an emergency situation going on inside the premises, such as "case[s] of fire or other disaster requiring prompt protective action"?[16] In this regard, the VCCR states that authorities may enter the premises of a consular post without any consent because the consent of the head of the consular post is "assumed".[17] On the other hand, the VCDR is silent on that issue. Some have argued that in an emergency situation, the consent of the head of the diplomatic mission may be presumed and the officials may enter the premises of diplomatic missions on the basis of necessity. Others oppose this view because such

[11] See *infra* note 61.
[12] Art. 22(2) of the VCDR.
[13] *Ibid*.
[14] Art. 31(3) of the VCCR states: "Subject to the provisions of paragraph 2 of this article the receiving state is under a special duty to take all appropriate steps to protect the consular premises against any intrusion or damage and to prevent any disturbance of the peace of the consular post or impairment of its dignity."
[15] The VCCR makes it clear that the special duty of the receiving state in paragraph 3 is subject to the consent requirement in paragraph 2, which is not explicitly stated under the VCDR.
[16] *Supra* note 10.
[17] "The consent of the head of the consular post may however be assumed in case of fire or other disaster requiring prompt protective action."; *ibid*.

exceptions may be easily abused by the receiving State agencies.[18] With regard to this difficult issue, the author is of the view that the situation in which consent may be "assumed" for entry into diplomatic missions must be strictly limited to such situations in which there is a threat to human lives, and not mere threat to assets of the mission, if prompt protective action were not taken.[19] This action must be limited to the extent that is strictly necessary to remedy the situation. The author believes that such interpretation is justified on the ground of humanitarianism and achieves the best balance between the two opposing views on this issue.

In any case, the interesting issue with regard to the subject of this article is the scope of the concept of "emergency". Can cyber terrorism or web viruses be considered as "other disaster[s] requiring prompt protective action"? In a situation where certain persons are trying to spread cyber bombs or computer viruses into the computer system inside the diplomatic mission or consular post, it is certain that agents of the receiving State have a "special duty to protect the premises" against such "intrusion or damage" and to prevent such "disturbance of the peace" of the premises. If it is necessary to enter the premises to perform the duty, must agents then *always* obtain consent of the head of the mission before entry?

It is difficult to see how the drafters of the VCCR could have intended the term "other disaster" to cover a situation such as a *cyber disaster*, since the convention was drafted in an age which had not seen the advent of computer viruses.[20] It would be more logical to say that the term "other disaster" includes only *natural* disasters, given the use of "fire" as an illustration.

However, we are living in a different time, one in which not only natural disasters but also artificial disasters such as cyber terror and computer viruses may paralyze the functions of consular posts if not promptly dealt with. In fact, the dictionary meaning of the word "disaster" is not confined to *natural* disasters. It is certainly true that a situation involving cyber terrorism or widespread computer virus requires prompt protective action.

In this sense, the VCCR can be interpreted in such a way that, in emergency situations in which computers or communication system of the consular post are exposed to the imminent and urgent danger of a serious computer virus or cyber bomb, agents of the receiving State may enter the premises of the *consular* post without consent. It would be necessary for them to temporarily shut down computers or communication lines of the premises as a prompt protective action.

In doing so, the receiving State must exert all necessary efforts not to abuse this exception. Thus, if state agents enter consular premises on the false pretext of addressing a cyber threat, it will breach the inviolability obligation under the treaty, and constitute state responsibility.[21]

[18] See, for example, Ian Brownlie, *Principles of Public International Law*, 5th ed. (Oxford: Oxford University Press, 1998), part VI; Gore-Booth, ed., *Satow's Guide to Diplomatic Practice*, 5th ed. (London: Longman, 1979) at 110; David H. Ott, *Public International Law in the Modern World* (London: Pitman, 1987) at 162–163. This position was confirmed by the ICJ in *U.S. Diplomatic and Consular Staff in Tehran* [1980] I.C.J. Rep. 3. Despite this ICJ decision (an ICJ decision is not a precedent and the rejection of the proposal does not necessarily mean that only absolute immunity was intended) and the drafting history of the VCDR, no consensus has yet to be reached on this controversial issue, see Barry E. Carter, Phillip R. Trimble & Curtis A. Bradley, *International Law*, 3rd ed. (New York: Aspen Publishers, 1999). During the UN Conference on Diplomatic Intercourse and Immunities (Vienna Conference), a proposal to allow such an exception for an emergency situation was raised but not adopted.

[19] It should be noted that in the case of entry into consular posts, not only threats to human lives but also those to consular assets would suffice for consent to be assumed, provided that those threats are sufficiently urgent.

[20] The VCCR was adopted in 1963.

[21] Of course, facing such a situation, agents may enter the premises of the consular post upon securing the consent of the head of the diplomatic mission or designee of the head of the consular post. In addition, the officials may enter, without consent, the part of the consular premises which is not used exclusively for the purposes of consular work, if they have legitimate reasons to do it. See *supra* note 10.

On the other hand, it can be argued that cyber attack or threat to *diplomatic* missions is not enough to give the receiving State authorities a right of entry under presumed consent. Cyber terrors can only bring about financial loss, which does not satisfy the condition of threats to *human lives* as suggested above.[22]

It should be noted that this "disaster exception" only applies to situations where the diplomatic mission or consular post falls victim to a cyber disaster originating from outside. In other words, situations in which the mission or post itself generates cyber disaster to the outside are not covered. This is obvious since the purpose of the exception is to protect the premises of the consular post,[23] not to protect premises beyond.

The third element of inviolability is the immunity from search, requisition, attachment or execution. The VCDR states that "the premises of the mission, their furnishings and other property thereon and the means of transport of the mission shall be immune from search, requisition, attachment or execution."[24] Thus, even after entering the premises of diplomatic mission with the consent of its head, agents are not allowed to perform search, requisition, attachment or execution on the properties of the mission such as computers and communication facilities, which are found to be related to cyber crimes. In a disaster situation in which human lives are threatened, agents upon entry with assumed consent are allowed to take only "protective" actions inside the premises without performing search, requisition, attachment or execution.

Consular properties enjoy similar immunities, but it should be noted that they are not immune from expropriation for purposes of national defence or public utility as long as the expropriation does not impede the performance of consular functions, and adequate compensation is promptly paid.[25]

Hence, if agents find that certain computers or facilities of the consular post are related to cyber crimes, they may expropriate the properties with appropriate compensation for the purpose of national defence. However, agents who have entered the premises with assumed consent in a cyber disaster situation may not expropriate any properties because expropriation is an action beyond the "protective" action that is permitted in such situation.

B. *Inviolability of Archives and Documents*

According to the VCDR, the archives and documents of the mission shall be "inviolable at any time and wherever they may be".[26] By the same token, the VCCR states that "the consular archives and documents shall be inviolable at all times and wherever they may be".[27] The word "documents" here should be understood to include electronic documents such as computer files and diskettes. It does not matter whether or not the electronic files are saved in the form of disposable files. Web-pages or binary codes saved in the main system computer of the mission or post also enjoy this privilege of inviolability. Therefore, all sorts of electronic documents cannot be opened, searched, or requisitioned against the will of diplomats or consuls.

[22] See *supra* note 19 and accompanying text.

[23] Note that Art. 31(2) of the VCCR refers to "protective action", and a logical understanding of "assumed" consent would lead to such conclusion.

[24] Art. 22(3) of the VCDR.

[25] Art. 31(4) of the VCCR states: "The consular premises, their furnishings, the property of the consular post, and its means of transport shall be immune from any form of requisition for purposes of national defence or public utility. If expropriation is necessary for such purposes, all possible steps shall be taken to avoid impeding the performance of consular functions and prompt adequate and effective compensation shall be paid to the sending state."

[26] Art. 24 of the VCDR.

[27] Art. 33 of the VCCR.

C. *Freedom of Communication*

1. *Official correspondence*

The Internet is used mostly as a means of communication. Thus, it is closely related with freedom of communication in diplomacy. In this regard, the VCDR prescribes:

(1) The receiving State shall permit and protect free communication on the part of the mission for all official purposes. In communicating with the Government and the other missions and consulates of the sending State, wherever situated, the mission may employ all appropriate means, including diplomatic couriers and messages in code or cipher. However, the mission may install and use a wireless transmitter only with the consent of the receiving State.
(2) The official correspondence of the mission shall be inviolable. Official correspondence means all correspondence relating to the mission and its functions.[28]

This freedom of communication extends to private "papers", "correspondence", and "property" of diplomats.[29]

Similar provisions are stated in the VCCR:

(1) The receiving State shall permit and protect freedom of communication on the part of the consular post for all official purposes. In communicating with the government, the diplomatic missions and other consular posts, wherever situated, of the sending State the consular post may employ all appropriate means including diplomatic or consular couriers, diplomatic or consular bags and messages in code or cipher. However the consular post may install and use a wireless transmitter only with the consent of the receiving State.
(2) The official correspondence of the consular post shall be inviolable. Official correspondence means all correspondence relating to the consular post and its functions.[30]

Hence, diplomatic missions and consular posts have the right to enjoy freedom of communication for official purposes. In other words, the receiving State has an obligation not to impede this right and must take all necessary measures to protect this right from any intrusion or possible impediment by any private person or entity.

In these days, communication through the Internet is becoming a widespread practice in diplomacy and consular works, as mentioned in Section II. Indeed, e-mails are frequently substituted for paper documents between foreign missions and capitals. To that extent, diplomatic bags or messages in cipher have become less frequently used. In such an environment, it is vital that the receiving State does not hamper the Internet connection used by diplomatic missions or consular posts. Furthermore, the receiving State must take appropriate steps to prevent any person or organisations from impeding Internet communications for diplomacy. As e-mails are "messages in (binary) code" in essence, a diplomatic mission or consular post "may employ all appropriate means" to communicate *through e-mails* with the capital, other missions or posts of sending State, wherever situated.[31] [IA2] As both the VCDR and the VCCR define "official correspondence" as "all correspondence relating to the mission or consular post and its

[28] Art. 27(1) and 27(2) of the VCDR.
[29] Art. 30 (2) of the VCDR states: "His papers, correspondence and, except as provided in paragraph 3 of Art. 31, his property, shall likewise enjoy inviolability."
[30] Art. 35 (1) of the VCCR.
[31] *Supra* notes 27 and 29.

functions",[32] it can include e-mails if the mission or post uses these as a means of correspondence with the headquarters or other mission or post. In such cases, the e-mails are "inviolable".[33]

However, if e-mail or Internet connections are made through a "wireless transmitter", such connections and the installation of such transmitter must be made only "with the consent of the receiving State".[34]

It should be noted that this freedom includes the right of communication with nationals of the sending State residing in the receiving State. The VCCR makes this point clear by stipulating that "consular officers shall be free to communicate with nationals of the sending State and to have access to them" and that "nationals of the sending State shall have the same freedom with respect to communication with and access to consular officers of the sending State".[35] Thus, the receiving State must not hamper Internet communications between consuls and nationals of the sending State. Furthermore, it must take appropriate measures to prevent a private person or entity from hampering such communications.

2. *Diplomatic or consular bags*

"Diplomatic bags" or "consular bags" are heavily used as a means of correspondence between a state's capital and its foreign missions and amongst missions. The packages constituting the diplomatic or consular bag must "bear visible external marks of their character and may contain only diplomatic or consular documents or articles intended for official use".[36] The diplomatic bags or consular bags "shall not be opened or detained".[37] Thus, diplomatic or consular bags enjoy inviolability in general. But, in the case of consular bags, there is an important limitation to this inviolability: if the competent authorities of the receiving State have "serious reason to believe that the bag contains something other than the correspondence documents or articles", they may "request that the bag be opened in their presence by an authorized representative of the sending State".[38] If this request is refused by the authorities of the sending State, the bag shall be "returned to its place of origin".[39]

One of the reasons why the extent of inviolability of diplomatic bags or consular bags is at issue is because such bags are known (although rarely) to have been used to carry illegal materials such as weapons, drugs, or hard currencies. Thus, it is important to check against possible abuse of the inviolability while protecting the right of communication through diplomatic or consular bags. In this light, the VCCR maintains a balance between the right of inviolability and the duty of official use by enabling authorities to reject introduction of bags containing illegal materials into their territory. When ordered to open a bag for inspection, staff from the consular post should either open the bag to show its contents or return the entire bag to the sending State. It should be noted that the receiving State may exercise this right of rejection only upon having *serious reason* to believe that "the bag contains something other than the correspondence documents or articles".[40]

Although this balance is not explicitly stated in corresponding provisions (paragraphs 3 and 4 of Article 27) under the VCDR[41], one can interpret, having a similar balance in

[32] *Ibid*.
[33] *Ibid*.
[34] *Ibid*.
[35] Art. 36 (1) of the VCCR.
[36] Art. 27(4) of the VCDR; Art. 35 (4) of the VCCR.
[37] Art. 27(3) of the VCDR; Art. 35 (3) of the VCCR.
[38] The VCCR, *ibid*.
[39] *Ibid*.
[40] *Ibid*.
[41] *Supra* notes 36 and 37. Cf. *supra* note 38.

Table 1.
THE INTERNET AND THE INVIOLABILITY OF PREMISES

		Cyber Crime inside Premises	Cyber Disaster affecting Premises
Diplomatic Mission	Condition of Entry	Entry only with consent of the head	Entry only with consent of the head
	Possible Action	No expropriation	Only protective action
Consular Post	Condition of Entry	(1) Entry with consent of the head; or	
		(2) Entry without consent of the head if: i) entry into parts used for non consular function; ii) there is consent of his designee or ambassador.	Entry without consent is possible
	Possible Action	Expropriation with Compensation	Only protective action

mind, these provisions as follows. Because what is prohibited under these provisions is the opening or detaining of diplomatic bags, the receiving State may *send it back promptly* (*i.e.*, without detaining) if the state has *clear evidence* to believe that the diplomatic bag contains illegal materials.[42] One should note that mere "serious reason to believe" is not sufficient to return the *diplomatic* bag, but instead "clear evidence" is required. The reason why a stricter requirement is imposed for the case of diplomatic bags is because the VCDR has no provision of exception to the inviolability, *i.e.*, the diplomatic bags cannot be requested to be opened in any case, as opposed to the VCCR in which the receiving State may request to open consular bags.[43] Since the VCCR arranges a subsequent procedure to confirm illegal materials by opening a consular bag in question, mere serious reason to believe illegality would be sufficient to trigger the procedure. At any rate, the representative of the sending State would have due opportunity to prove the legality of the bag by opening it. On the other hand, in the case of the VCDR, according to the interpretation of which, only the request of returning the diplomatic bag is possible, it would be too harsh to the sending State to enable the receiving State to return the bag out of mere "serious reasons to believe" the illegality. Hence, it would be fair to ask the receiving State to present *clear evidence* in order to take such a drastic measure of returning the diplomatic bag.

It is interesting to see that some of the important functions of diplomatic or consular bags are gradually being replaced by Internet communications. Many documents or papers that have traditionally been physically carried by diplomatic bags are now transmitted

[42] In such situations, the sending State will have the chance to withdraw the illegal material from the bag and resend it.

[43] Of course the sending state representative has the right to refuse such request and return the bag. See *supra* note 39 and accompanying text.

electronically through the Internet. As a large volume of documents, pictures, or audio-visual information can be transmitted instantly through the Internet, it is not surprising that electronic transmission is becoming more popular.[44]

Given this general trend, one might suggest the establishment of a new system of using a "diplomatic *cyber* bag" or "consular *cyber* bag" in reference to existing diplomatic or consular bag system. Under the new system, the diplomatic or consular post or the sending State may designate a cluster of electronic files or information as a "diplomatic or consular cyber bag" with a "visible external mark of its character", *e.g.*, with specific file names accompanying electronic governmental signatures, and transmit it regularly to each other. The practical effect of such a designation would be that the status of "official correspondence" could be automatically accorded to such clusters of electronic information and thereby, an enhanced protection of inviolability would be given to such clusters. In particular, the receiving State, notwithstanding its security check program for ordinary e-mails, must not open or detain a diplomatic or consular cyber bag, but may only intercept and transmit it back to the original sender if the competent authorities of the receiving State: (1) have "clear evidence" that the bag is misused (in the case of diplomatic cyber bag); or (2) have "serious reason to believe" such misuse and if the sending State representative refused to open the bag (in the case of consular cyber bag). Thus, cyber bags carrying contents unrelated to official diplomatic or consular functions such as private information, spying information or contents, child pornography, gambling, computer virus, or cyber bombs may be blocked with proper evidence or reasons in accordance with due process.

D. *Tax Exemption*

Diplomatic missions are exempted from taxes for activities performed in the course of their official duties.[45] In addition, diplomats and family members forming part of their household are personally exempted from taxes imposed by the receiving State. It should be noted, however, that there are several exceptions to this personal privilege of diplomats and their family.[46] Among these exceptions, the following two are relevant for the purposes of the present article: (i) indirect taxes of a kind which are normally incorporated in the price of goods or services; (ii) charges levied for specific services rendered.[47] A similar privilege of tax exemptions and its exceptions are accorded to consular posts and consuls and their family under the VCCR.[48]

[44] According to an analysis, the cost of sending a 42-page document from Ottawa to Tokyo over the Internet is 260 times less than if it were sent by traditional post. It is also 720 times faster to transmit the document electronically. This shows the extent of savings in terms of time and money that has been made possible as a result of the new technology. See World Trade Organization, *Seminar on Electronic Commerce and Development* (held on 19 February 1999), WT/COMTD/18, online: WTO <http://www.wto.org/english/tratop_e/ecom_e/wtcomtd18.doc>. Of course, the internet has its limitations. Since it cannot transmit certain physical objects as they are, diplomatic bags are indispensable to the transportation of such physical objects.

[45] Art. 28 of the VCDR states "The fees and charges levied by the mission in the course of its official duties shall be exempt from all dues and taxes."

[46] Art. 34 of the VCDR. See also Art. 37(1) of the VCDR.

[47] Other exceptions are: (i) dues and taxes on private immovable property situated in the territory of the receiving State, unless he holds it on behalf of the sending State for the purposes of the mission; (ii) estate, succession or inheritance duties levied by the receiving State; (iii) dues and taxes on private income having its source in the receiving State and capital taxes on investments made in commercial undertakings in the receiving State; (iv) registration, court or record fees, mortgage dues and stamp duty, with respect to immovable property. See Art. 34, *ibid.*

[48] Arts. 32, 39 and 49 of the VCCR.

Thus, as long as the diplomatic *missions* or consular *posts* use the Internet for official purposes, they will enjoy the benefit of exemption of taxes that are levied on the use of the Internet.[49] And, if they are neither indirect taxes nor charges levied for specific services rendered, taxes will be exempt for the benefit of *diplomats, consuls*, and their *families*.

E. *Immunity from Criminal or Civil Jurisdiction*

1. *Diplomats*

Diplomats and family members forming part of their household enjoy immunity from the criminal jurisdiction of the receiving State.[50] They also enjoy immunity from the civil jurisdiction of the receiving State, except in the case of: (i) certain real property actions, (ii) certain actions relating to succession, and (iii) actions relating to any professional or commercial activity exercised by the diplomatic agent in the receiving State outside his official functions.[51]

Thus, if diplomats or their family members commit cyber crimes or other Internet-related criminal offenses, they are immune from the criminal jurisdiction of the receiving State. As a result, a criminal case by the receiving State must be dismissed by reason of such immunity. Furthermore, they are "not liable to any form of arrest or detention" in the first place because their "persons are inviolable".[52] If actions committed in cyber space by diplomats or their family members result in civil responsibility such as defamation, they can also enjoy immunity from civil jurisdiction. It should be noted that sometimes such actions might not enjoy immunity if those actions are related to "any professional or commercial activity exercised outside his official functions".[53]

2. *Consuls*

In general, consuls enjoy immunity from the judicial jurisdiction of the receiving State only "in respect of acts performed in the exercise of consular functions".[54] Such immunity is excluded if it is a civil action arising out of a contract concluded by a consul in which they "did not contract expressly or impliedly as an agent of the sending State", or a civil action for "traffic accident" damage.[55] Therefore, cyber crimes or civil offenses committed by consuls will enjoy immunity from criminal or civil jurisdiction only if they are performed in the exercise of official functions. Consuls who have committed cyber crimes or civil offenses are "not liable to arrest or detention pending trial, except in the case of a grave crime, and pursuant to a decision by the competent judicial authority".[56] Therefore, it is possible to arrest consuls, who have committed such "grave crime" as, for example, *cyber terrorism*, by a court decision even before the trial. They may be put into prison.[57]

[49] It must be noted however that in the case of consular posts, "represent payment for specific services rendered" is not exempted. See Art. 32(1) of the VCCR.
[50] Art. 31(1) of the VCDR.
[51] *Ibid.*
[52] Art. 29 of the VCDR.
[53] See *supra* note 51.
[54] Art. 43(1) of the VCCR.
[55] Art. 43(2) of the VCCR.
[56] Art. 41(1) of the VCCR.
[57] Art. 41(2) of the VCCR states: "Except in the case specified in paragraph 1 of this article, consular officers shall not be committed to prison or liable to any other form of restriction on their personal freedom save in execution of a judicial decision of final effect". Art. 42 of the VCCR states: "Any arrest or detention of consuls must be promptly notified to the sending state."

While diplomats and their family members are not obliged to give evidence as witnesses, consuls may be called upon to attend as witnesses in the course of judicial proceedings.[58] Thus, diplomats and their family members may decline to be witnesses in cases involving Internet-related crimes or civil actions, as opposed to consuls.

These immunities do not mean that crimes committed by or civil liabilities of diplomats and their family or consuls are exempt from the jurisdiction of the sending State.[59] Their immunity from the jurisdiction of the receiving State may be waived expressively by the sending State.[60] Hence, it is always possible that cyber crimes or other misbehaviors by diplomats or consuls are punished, or held liable, in the sending State or even in the receiving State if the waiver is granted. Also, the receiving State may discipline such crimes or misbehaviors by declaring the diplomat or consul as "*persona non grata*", in which event the sending State has to either recall them or terminate their functions and status.[61]

3. *International criminal law*

The rapid development of international criminal law has been dazzling. Recently, the *Statute of International Criminal Court* (ICC Statute) came into force.[62] The Statute provides that the Court has jurisdiction with respect to four crimes: the crime of genocide, crimes against humanity, war crimes, and crimes of aggression.[63] Among these, the crime of aggression has to be defined and conditions have to be set out for its application.[64] As a precondition to the exercise of jurisdiction by the Court, the Statute requires that the above crimes occurred in the territory of a state party to the Statute or the criminal be a national of a state party.[65] If this condition is met, the Court may exercise jurisdiction in accordance with referral by a state party or prosecutor of the Court. Also, the UN Security Council has the right of referral, in which case the above precondition is not required.[66]

The Court exercising jurisdiction may punish not only individuals who committed the crime, but also those who "ordered, solicited, induced, aided, abetted, or assisted" the commission of such a crime.[67] Their official capacity is "irrelevant", which means that

[58] Compare Art. 31(2) of the VCDR with Art. 44(1) of the VCCR. Where a consulate officer is called upon as witness and he or she declines to do so, no coercive measure or penalty may be applied to him. The authority requiring the evidence of a consular officer must avoid interference with the performance of his functions. It may however be possible to take such evidence at the consul's residence or at the consular post, or to accept a statement from him in writing. See Art. 44(1) and (2) of the VCCR.

[59] See Art. 31(4) of the VCDR. The same interpretation is possible under the VCCR, although the VCCR has no comparable provision with Art. 31(4) of the VCDR.

[60] Art. 32 of the VCDR.

[61] Art. 9 of the VCDR; Art. 23 of VCCR.

[62] *Rome Statute of the International Criminal Court,* July 17, 1998, 2187 U.N.T.S. 90 (entered into force July 1, 2002)("ICC Statute").

[63] Art. 5 (1) of the ICC Statute. Among these, crimes against humanity include the following acts: "committed as part of a widespread or systematic attack directed against any civilian population, with knowledge of the attack: (a) Murder; (b) Extermination; (c) Enslavement; (d) Deportation or forcible transfer of population; (e) Imprisonment or other severe deprivation of physical liberty in violation of fundamental rules of international law; (f) Torture; (g) Rape, sexual slavery, enforced prostitution, forced pregnancy, enforced sterilization, or any other form of sexual violence of comparable gravity; (h) Persecution against any identifiable group or collectivity on political, racial, national, ethnic, cultural, religious, gender as defined in paragraph 3, or other grounds that are universally recognized as impermissible under international law, in connection with any act referred to in this paragraph or any crime within the jurisdiction of the Court; (i) Enforced disappearance of persons; (j) The crime of apartheid; (k) Other inhumane acts of a similar character intentionally causing great suffering, or serious injury to body or to mental or physical health"; Art. 7(1) of the ICC Statute.

[64] Art. 5(2) of the ICC Statute.

[65] Art. 12(1) of the ICC Statute.

[66] Art. 13 of the ICC Statute.

[67] Art. 25 of the ICC Statute. In order to punish such persons, their intent and knowledge are required as mental elements, see Art. 30 of the ICC Statute.

various immunities, including diplomatic or consular immunities, "shall not bar the Court from exercising its jurisdiction over such a person".[68]

Therefore, if diplomats or consuls should use the Internet to order, solicit, induce, aid, abet, or assist the commission of genocide, crimes against humanity, or war crimes conducted by a national of a state party of ICC Statute or in the territory of a state party of ICC Statute, those diplomats or consuls may be punished despite the immunity from criminal jurisdiction that they usually enjoy.[69]

IV. The Internet and The Law of Settlement of International Disputes

The Charter of the United Nations is the primary source of international law with respect to the settlement of disputes among nations. According to the Charter, the parties to "any dispute, the continuance of which is likely to endanger the maintenance of international peace and security" have an obligation, first of all, to seek a solution by peaceful means.[70] Thus, disputes between states regarding the use or connection of the Internet are subject to this obligation of peaceful settlement insofar as the continuance of them is "likely to endanger the maintenance of international peace and security".[71] During this process of pacific settlement, Internet diplomacy will have a greater role, as time goes by, in facilitating negotiations between disputing countries.

If an Internet-related dispute between states becomes aggravated such as to "threaten or breach the peace" despite efforts at pacific settlement, the Security Council may determine the existence of the threat or breach, and subsequently make recommendations or decisions to "maintain or restore international peace and security".[72] Such decisions by the Security Council are binding upon UN member states.[73] If Security Council decisions are not carried out by disputing parties, the Council may take "measures not involving the use of armed force".[74] These measures may include "complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations".[75] Among these non-military measures, what is of concern for the subject of the present article is the "complete or partial interruption of … other means of communication". Certainly, as the Internet is one type of "other means of communication", UN members may jointly interrupt Internet connection or communication with the recalcitrant state in accordance with Security Council's direction. Failure to conform in spite of all these efforts may lead to the use of military force as a final resort in accordance with the Council's decision.[76] At this stage, the Internet could play a role in facilitating military communications and providing a means of waging "cyber war" for the benefit of the international society.

[68] Art. 27 of the ICC Statute.

[69] It should be noted, however, that for the surrender of the criminal from the receiving State to the Court, the receiving State must obtain the cooperation of the sending State in the form of a waiver of diplomatic immunity. See Para. 1 of Art. 98(1) of the ICC Statute. In reality, this acts as a significant procedural hurdle to the punishment of errant diplomats or consuls.

[70] Such peaceful means listed by the Charter are "negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice"; Art. 33(1) of the UN Charter.

[71] The Security Council may, when it deems necessary, call upon the parties to settle such dispute by peaceful means. Art. 33(2) of the UN Charter.

[72] See Art. 39 of the UN Charter. Also note that decisions of provisional measures may be made by the Security Council, see Art. 40 of the UN Charter.

[73] Art. 25 of the UN Charter.

[74] Art. 41 of the UN Charter.

[75] *Ibid.*

[76] Arts. 42-47 of the UN Charter.

V. Conclusion

The Internet is constantly improving. Given its great potential for growth, any prediction of the future of the Internet is necessarily speculative. For example, the possibility of the "Super Internet" project, by which more communication channels and human activities would be integrated and exchanged, has been raised recently. The evolution of diplomacy may involve taking advantage of this technological development. Cyber diplomacy has become an indispensable part of the daily lives of diplomats and consuls.

In this new environment, the traditional law of diplomacy must also evolve through new interpretation of existing rules. If some of those rules are deficient or insufficient to regulate Internet diplomacy, new rules ought to be created. In this light, this paper has identified several provisions under the existing law of diplomatic or consular immunity and privilege that are applicable to the Internet environment. They are the rules on the inviolability of premises, inviolability of documents and archives, freedom of official correspondence, privilege of tax exemption, and immunity from judicial jurisdiction. New interpretations of these rules have also been suggested.

Firstly, the inviolability principle of the premises of diplomatic missions or consular posts may be extended to apply to "cyber crimes" committed inside the premises. To cover a "cyber disaster" situation under the umbrella of the VCCR, the author applied the "assumed consent" exception under the VCCR to such a situation. As a result, agents of the receiving State may enter the premises of consular posts without express consent in order to take protective actions for computer or communication systems inside the premises. This "cyber disaster exception" does not allow for the entry into the premises of diplomatic missions, because under the VCDR there is no ground of interpretation or practical necessity for such an exception.

Secondly, through proper interpretation of provisions under the VCDR and the VCCR, the privilege of inviolability of diplomatic or consular documents may apply to all types of "electronic documents" including computer files or diskettes.

Thirdly, official correspondence in the form of e-mail exchanges or Internet communication of diplomatic missions or consular posts is protected as an element of freedom of communication for diplomacy or consular works. For this purpose, current provisions under the VCDR and the VCCR may apply to Internet-based correspondence. As a consequence, Internet-based correspondence of missions or posts enjoy the benefit of protection against intrusion or impediment by the receiving State agents or any private person. This freedom also applies to communication between diplomatic missions or consular posts and nationals of the sending State residing in the receiving State. With regard to freedom of communication, the author considers that it is necessary to create new rules for the "cyber diplomatic or consular bag". The privilege of inviolability of the diplomatic or consular bag needs to be extended to accommodate the "cyber bag" idea. Alternatively, the cyber bag system may be created by analogy with the system of the diplomatic or consular bag under the VCDR and the VCCR. If necessary, these Conventions may be amended to materialize the idea.

Fourthly, rules on the diplomatic or consular privilege of tax exemption and its exceptions may apply to Internet connections by missions or posts and diplomats or consuls.

Fifthly, rules on the diplomatic or consular immunity from the criminal or civil jurisdiction of the receiving State may also apply to cyber crimes or civil misbehaviors committed by diplomats, consuls, or their family members. As a result, diplomats and their family enjoy full immunity from criminal jurisdiction of the receiving State with regard to their cyber crimes, whereas their civil misbehaviors in cyber space may be subject to civil jurisdiction of the receiving State if they fall under one of the exceptions of the VCDR, including the professional or commercial activities outside official functions. Consuls committing cyber crimes or civil misbehaviors enjoy only official duty immunity under the VCCR. Also, rules

under the VCDR and the VCCR on arrest and detention, witness, and waiver of immunity may apply to such crimes or misbehaviors.

The traditional diplomatic or consular immunity from criminal jurisdiction becomes irrelevant insofar as international criminal law applies. Diplomats or consuls, performing cyber activities assisting genocide, crimes against humanity, or war crimes, are subject to individual punishment by the International Criminal Court.

The Internet has also affected the international law of dispute settlement by increasing the possibility of disputes regarding the international use or connection of the Internet and by providing the United Nations with more means to execute non-military as well as military sanctions against a disputing state which refuses to carry out the Security Council's decision.

After all, the web of our life is of a mingled yarn, good and ill together.[77] In this era of endless technological revolution, it is important to use Internet technology for the good of the global community. In this regard, diplomacy carries out an important part of the task, purporting to connect the good in the world community.

[77] *Supra* note 1 and accompanying text.