PART II

Rights and Obligations of States in Cyberspace

Jovan Kurbalija

E-Diplomacy and Diplomatic Law in the Internet Era

1. Introduction

In the long history of diplomacy,[1] the development of information and communication technology has profoundly influenced the way representation, negotiations and other diplomatic functions have been conducted. The most important tools in this evolution include the telegraph, the telephone, the radio, the television, and the fax. Each triggered a dynamic interplay of continuity and change in the evolution of diplomacy: continuity in the main functions of diplomacy (the peaceful settlement of disputes) and changes in the way it is performed (the use of new tools). The internet is the latest innovation in this historical evolution.[2, 3] The internet accounts for over 20% of the gross domestic product (GDP) growth in the world's largest economies.[4] With close to three billion users,[5] every third person on this planet is already connected to the internet, and each day over one and a half million people are victims of cyber crime.[6] In developed and developing countries the internet is becoming vital to the functioning of societies and integral to most aspects of daily lives, and it can be deemed the backbone of the global economy.

The internet has profoundly changed information and communication,[7] both of which are pillars of diplomacy. The search for information typically starts with a search engine such as Google or Bing. Wikipedia is often used as an overview of issues and processes, a place to start searching for more detailed information. Our storage banks

[1] Almost all early civilisations used some form of proto-diplomacy, including negotiations and the protection of negotiators (immunity). See also: R. Numelin, *The Beginnings of Diplomacy. A Sociological Study of Intertribal and International Relations* (Oxford: Oxford University Press 1950).

[2] For more information see *Evolution of technology and diplomacy*, a series of blogs and webinars on the interplay between communication technology and diplomacy, conducted in 2013 by Dr Jovan Kurbalija. <http://www.diplomacy.edu/2013/evolution> accessed 09 November 2013.

[3] On the evolution of diplomatic methods see: H. Nicolson, *The Evolution of Diplomatic Method* (London: Constable & Co Ltd, 1954); M.S. Anderson, *The Rise of Modern Diplomacy: 1450-1919* (London: Longman Group, 1939); K. Hamilton and R. Langhorne, *The Practice of Diplomacy* (London: Routledge, 1995); G. Berridge, *Diplomacy: Theory and Practice* (3rd ed., Basingstoke, UK: Palgrave Macmillan, 2005).

[4] Pascal-Emmanuel Gobry, 'The Internet is 20% of economic growth' *Business Insider* (24 May 2011) <http://www.businessinsider.com/mckinsey-report-internet-economy-2011-5> accessed 09 November 2013.

[5] According to the Internet World Stats on 30 June 2012 there were 2,405,518,376 internet users worldwide. Their data are based on sources from International Telecommunication Union, Nielsen Online, GFK and local ICT regulators, among others. See <http://www.internetworldstats.com/stats.htm> accessed 09 November 2013.

[6] W. Jones, 'This Week in Cybercrime: Cybercrime's Industrial Revolution' *IEEE Spectrum* (30 June 2013) <http://spectrum.ieee.org/riskfactor/telecom/security/this-week-in-cybercrime-cybercrimes-industrial-revolution> accessed 09 November 2013.

[7] cf T. Van Dinh, *Communication and Diplomacy in a Changing World* (Norwood, NJ: Ablex 1987) p.8. ('Communication is to diplomacy as blood is to the human body. Whenever communication ceases, the body of international politics, the process of diplomacy, is dead, and the result is violent conflict or atrophy.').

for documents, emails, and photos have also changed, moving from hard drives to cloud servers. The way we communicate is increasingly shaped by mobile telephones, Skype and other internet tools. The core relevance of information and communication for diplomacy, and the revolution affecting both of them in the internet era, set the stage for the present analysis of the influence of the internet on diplomacy in general and on diplomatic law in particular. It remains to be seen if these changes will trigger just one more evolutionary step in the long history of diplomacy, or if they will catalyse revolutionary change in how, where, and by whom diplomacy is performed. While it will take time for diplomacy to adjust to the internet, some questions require immediate response, as is shown by the revelations of Edward Snowden[8] on PRISM[9] and other internet surveillance activities:[10] how can the protection of diplomatic communication and information be ensured in the era of digital surveillance? Can provisions of the 1961 *Vienna Convention on Diplomatic Relations* (VCDR)[11] remain relevant in the internet era? These and other questions are the subjects of this chapter.

While there are many open questions, the research on the impact of the internet on diplomacy (as on overall society) is in its formative stage. This is reflected by the diverse terminology which has gradually developed. The impact of the internet on diplomacy is very often described as 'e-', 'virtual', 'cyber', or 'digital' diplomacy. Yet while these prefixes describe the same phenomenon – the internet – we tend to use 'e-' for commerce, 'cyber' for crime and war, 'digital' for development divides, and 'virtual' for internet spaces. Usage patterns are starting to emerge. In everyday language, the choice of prefix might be casual but, in internet politics, the use of prefixes has begun to show specific meaning and relevance.

The etymology of the word *cyber* goes back to the ancient Greek meaning of *governing*. 'Cyber' came to our time between the covers of Norbert Weiner's book *Cybernetics*, which deals with information-driven governance.[12] In 1984, William Gibson introduced the word cyberspace in his science-fiction novel *Neuromancer*.[13] The use of the prefix 'cyber' grew parallel to the internet. In the late 1990s, almost anything related to

[8] Edward Snowden is former contractor of the US National Security Agency (NSA) who disclosed information about massive surveillance conducted by the NSA and partner institutions. For a series of articles on Edward Snowden see the *Guardian* <http://www.theguardian.com/world/edward-snowden> accessed 18 October 2013.

[9] PRISM stands for 'Planning Tool for Resource Integration, Synchronisation, and Management'. PRISM is the NSA's operation aimed at accessing the personal data stored at the servers of US internet companies (Microsoft, Yahoo, Google, Apple, Facebook, Skype, Paltalk, AOL).

[10] Other major internet surveillance activities, revealed by E. Snowden, include wiretapping of the internet backbone cables carrying the major internet traffic through two programmes: UPSTREAM performed by the United States National Security Agency (NSA) and TEMPORA performed by the United Kingdom's Government Communications Headquarters (GCHQ).

[11] *Vienna Convention on Diplomatic Relations*, 500 U.N.T.S. 95.

[12] N. Weiner, *Cybernetics or Control and Communication in the Animal and the Machine* (Cambridge, MA: MIT Press, 1965).

[13] W. Gibson, *Neuromancer* (New York, NY: Ace Books, 1983).

the internet was ‘cyber’: cyber community, cyber law, cyber sex, cyber crime, cyber culture etc. In the early 2000s, ‘cyber’ gradually disappeared from general use, yet it remained alive in security terminology. This is most likely because of the 2001 Council of Europe’s *Convention on Cybercrime*, still the only international treaty in the field of internet security.[14] Today, many States issue *Cyber Security Strategies*;[15] the International Telecommunication Union (ITU) has its *Global Cybersecurity Agenda*;[16] the North Atlantic Treaty Organization (NATO) has its *Policy on Cyber Defence*.[17]

‘E’ is an abbreviation of electronic. Its first and most important use is in e-commerce, as a description of the early commercialisation of the internet. In the European Union’s (EU’s) Lisbon Agenda (2000),[18] ‘e-’ was the most frequently used prefix. ‘E-’ was also the main prefix in the declarations of the World Summit on the Information Society (WSIS, Geneva 2003 and Tunis 2005).[19] [20] WSIS implementation is centred on action lines, including e-government, e-business, e-learning, e-health, e-employment, e-agriculture, and e-science. ‘E-’ is not as present as it used to be; even the EU has recently abandoned it, trying, most likely, to distance itself from the partial success of the Lisbon Agenda.

Digital refers to 1 and 0 – two digits that form the basis of the whole concept of information and communication technology (ICT) and the internet. Ultimately, all software uses these two digits. In the past, digital was used mainly in development circles to describe the ‘digital divide’. In the last few years, however, digital has started conquering the internet’s linguistic space. The EU has a ‘Digital Agenda for Europe’.[21] The United Kingdom (UK) has digital diplomacy.[22]

[14] Council of Europe, *Convention on Cybercrime* of 23 November 2001.

[15] See a list at NATO CCD COE, *National Strategies & Policies* <http://ccdcoe.org/328.html> accessed 09 November 2013.

[16] ITU, *Global Cybersecurity Agenda* <http://www.itu.int/osg/csd/cybersecurity/gca/> accessed 09 November 2013.

[17] cf NATO, *NATO and cyber defence*, <http://www.nato.int/cps/en/SID-12A1F016-A72FF943/natolive/topics_78170.htm> accessed 09 November 2013.

[18] *Lisbon European Council 23 and 24 March 2000 Presidency Conclusions* <http://www.europarl.europa.eu/summits/lis1_en.htm> accessed 09 November 2013.

[19] For the main WSIS declarations and outcome documents see: Geneva 2003 (Geneva Declaration of Principles and Geneva Plan of Action) and Tunis 2005 (Tunis Commitment and Tunis Agenda for the Information Society) <http://www.itu.int/wsis/index.html> accessed 10 November 2013.

[20] For the research on the use of prefixes in the WSIS and IGF processes, see DiploFoundation’s research project ‘Emerging Language of Internet Diplomacy’ *Diplo* (Malta, 2013) <http://www.diplomacy.edu/IGFlanguage> accessed 09 November 2013.

[21] European Commission, A Digital Agenda for Europe - Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions (26 August 2010) COM/2010/0245 f/2 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245R%2801%29:EN:NOT> accessed 18 October 2013.

[22] Foreign Commonwealth Office, *Foreign Commonwealth Office Digital Diplomacy* (no date) <http://blogs.fco.gov.uk/digitaldiplomacy/> accessed 18 October 2013.

An interchangeable use of prefixes can be noticed in the United States (US) State Department which has an *e*Diplomacy department,[23] refers to *digital* diplomacy in the main ICT document and department,[24] and employs a *virtual* embassy to Iran.[25]

The following section depicts the impact of the internet on diplomacy. The third section discusses the status of diplomatic missions in the internet era and the impact of the internet on core diplomatic functions, namely representation, negotiation, protection of nationals, and information gathering. The fourth section provides an analysis of the impact of the internet on diplomatic privileges, immunities, and facilities, and the final section offers some remarks on the future of diplomatic and consular law in the internet era.

2. Impact of the Internet on Diplomacy

The impact of the internet on diplomacy affects three main areas: the changing environment for diplomatic activities, new topics on diplomatic agendas, and new tools for diplomacy.[26]

2.1 The Changing Environment for Diplomatic Activities

The changing *environment* for diplomatic activities refers to the impact of technology on the economy, sovereignty, and concepts of power. Diplomacy does not exist in a vacuum. It is influenced by particular social, political, and economic circumstances. This changing environment for diplomatic activities is affected by the emergence of *defining technologies* that determine economic, social, and political success. They have included – historically – land, population, raw materials, energy, and financial capital.[27] The control of defining technologies has usually meant a strong influence of social and political developments. The defining technology of our era is the information technology, including the internet, with the central importance of knowledge.[28]

[23] United States Department of State, *Major Programmes of IRM's Office of eDiplomacy* <http://www.state.gov/m/irm/ediplomacy/c23840.htm> accessed 10 November 2013.

[24] United States Department of State, *IT Strategic Plan: Fiscal Years 2011-2013 – Digital Diplomacy* <http://www.state.gov/m/irm/rls/148572.htm?goMobile=0> accessed 09 November 2013.

[25] United States, *Virtual Embassy of the United States to Iran* <http://iran.usembassy.gov/> accessed 10 November 2013.

[26] See also J. Kurbalija, 'The Impact of the Internet and ICT on Contemporary Diplomacy' in P. Kerr and G. Wiseman (ed.) *Diplomacy in a Globalizing World Theories and Practices* (New York: Oxford University Press 2012), 141-159.

[27] J.D. Bolter, *Turing's Man: Western Culture in the Computer Age* (London: Duckworth, 1984).

[28] cf P.F. Drucker, *The New Realities: In Government and Politics, in Economics and Business, in Society and World View* (Oxford: Heinemann Professional Publishing 1989), p.167. In his description of a knowledge society, Drucker observed that knowledge has become the capital of a developed economy, and that knowledge workers form the group that sets society's trends.

An impact of the defining technologies on diplomacy is illustrated by the level of influence of particular industrial sectors on diplomacy. For example, a few decades ago, the promotion of the interests of the US automobile industry abroad was high on the US diplomatic agenda. Nowadays, the internet industry has more influence on US diplomacy, in both bilateral and multilateral negotiations. Similar trends can be noticed in other countries.

2.2 Internet Governance: A New Topic on the Diplomatic Agenda

New topics are appearing on diplomatic agendas as a result of the growing impact of the internet on modern society. This follows a general trend of extending diplomatic agendas, which David D. Newsom explains as follows:

> For most of the twentieth century, the international diplomatic agenda has consisted of questions of political and economic relations between nation-states — the traditional subjects of diplomacy. After the Second World War new diplomatic issues arose, spurred by the technical advances in nuclear energy and electronics.[29]

Internet-related topics on diplomatic agendas are usually addressed in the context of global internet governance (IG), which includes the following questions: who governs the internet? Who are the actors likely to influence its future development? What will be their policies with regard to connectivity, commerce, content, funding, security, and other issues central to the emerging digital society?

Today, internet governance includes close to 50 policy issues that can be classified in five main groups: infrastructure and standardisation, legal, economic, developmental, and socio-cultural.[30]

Internet governance includes new cyber issues dealing with the proper functioning of the internet (e.g. managing internet names and numbers, net neutrality) and traditional ones whose governance has been affected, or even transformed, by the advent of the internet (e.g. crime, intellectual property, commerce, and privacy protection). Most IG issues are multidisciplinary, combining technical, security, legal, economic, and social aspects.

IG was put on the global diplomatic agenda during the WSIS, which was organised around two main summit events: one in Geneva in 2003 and the other in Tunis in 2005. At the Tunis event, the WSIS established the Internet Governance Forum (IGF) as the

[29] D. Newsom, 'The New Diplomatic Agenda: Are Governments Ready?' *International Affairs* (January 1989) p.29.

[30] J. Kurbalija, *An Introduction to Internet Governance* (Malta: DiploFoundation, 2011), pp. 27-29.

main global body which addresses the governance of the internet in a holistic way.[31] The establishment of the IGF was a result of a compromise between government-centred and non-governmental approaches to IG (the so-called 'Tunis compromise'). The government-centred approach, promoted predominantly by developing countries, argued that the internet should be governed by international organisations under the United Nations (UN) umbrella. The non-governmental approach, favoured by developed countries and in particular by the US, argued for a preservation of existing IG with the close involvement of the business sector and civil society.

The 'Tunis compromise' has been increasingly challenged. First, at the World Conference on International Telecommunications (WCIT)[32] in Dubai in December 2012, an attempt was made to increase the ITU's involvement in managing internet-related matters. The result was polarised votes at WCIT, mainly along the lines of developed/developing countries.[33] Second, the revelations of massive internet surveillance re-energised discussion on the future institutional framework for IG. In the forthcoming period a series of events will take place at which the future institutional arrangements for IG will be discussed. Following a joint initiative by the Internet Corporation for Assigned Names and Numbers (ICANN) and Brazil, Brazil will host the Global Multistakeholder Meeting on the Future of Internet Governance (Sao Paolo, 23-24 April 2014), aimed at discussing universal internet principles and future IG institutional arrangements.[34] In 2015, the WSIS +10 events are likely to be dominated by discussions on the future of IG, including the future role of the IGF.[35]

2.3 New Tools for Diplomacy

As it did with other professions, the internet brought new tools to diplomacy. E-mail is now the main communication tool used in diplomatic services. Diplomats use search engines to find information, and increasingly use teleconferencing, social media, and other ICT and internet tools. These technologies impact the way modern diplomacy operates. The internet introduced new means of conducting diplomacy. Diplomatic signals are sent via Twitter and blogs. Resolutions and other diplomatic texts are drafted using Google Docs and other online drafting tools.

[31] See Tunis Agenda for the Information Society (Articles 72-78) <http://www.itu.int/wsis/docs2/tunis/off/6rev1.pdf > accessed 10 November 2013.

[32] See <http://www.itu.int/en/wcit-12/Pages/default.aspx>.

[33] 89, mainly developing, countries voted for amendment of the International Telecommunication Regulations (ITR); 55, mainly developed, countries voted against the proposed amendments of the ITR.

[34] See <http://www.brasil.gov.br/governo/2013/11/brasil-vai-sediar-conferencia-sobre-governanca-na-internet>.

[35] The first WSIS summit meeting took place in 2003. The reviews of the WSIS are collectively called WSIS+10, although there is no specific schedule or agenda for the process. For a news article announcing the 'start' of the process, see <http://www.ifla.org/news/start-of-wsis10-review-meeting-at-unesco-hq-in-paris-france> accessed 10 November 2013.

3. Diplomatic Law

Diplomatic law covers three main areas: (1) the establishment of diplomatic relations and the status of diplomatic missions; (2) the performance of diplomatic functions; and (3) diplomatic immunities, privileges, and facilities. Diplomatic law has developed gradually through the crystallisation of practices, and the creation of customary rules. The codification of customary diplomatic law started at the Congress of Vienna (1814–1815) when the rule of diplomatic rank and order of precedents[36] were codified in the *Vienna Regulation* of 1815. This was followed by the 1928 *Havana Convention on Diplomatic Officers*[37] and the *Harvard Research Draft Convention on Diplomatic Privileges and Immunities* of 1932.[38] After World War II, two main instruments were adopted to regulate the diplomatic status of the international organisations: the *Convention on the Privileges and Immunities of the United Nations* of 1946[39] and the *Convention on the Privileges and Immunities of Specialised Agencies* of 1947.[40] The latest comprehensive codification of diplomatic law was conducted by the 1961 *Vienna Convention on Diplomatic Relations* (VCDR)[41] which deals with the status and functioning of diplomatic missions exchanged by States. With 187 State parties and a high level of adherence, the VCDR is considered to be one of the most successful international legal instruments. Violations of the provisions, as in the case of Iran taking US diplomats hostage in Teheran (1979–1981) are rare. As the International Court of Justice (ICJ) indicated in the *Teheran Hostage* case, diplomatic immunities are 'essential for the maintenance of relations between States and are accepted throughout the world by nationals of all creeds, cultures and political complexions'.[42]

The VCDR deals with the status and functioning of the diplomatic missions exchanged by States, which are, together with consular relations, the traditional and main features of diplomatic services. However, twentieth century diplomacy extended beyond bilateral diplomatic relations through the exchange of two States' embassies and consulates. The

[36] An 'order of precedence' is a hierarchical list of diplomats and other dignitaries. It is used for seating arrangements at events and such occasions attended by diplomats and other officials. Order of precedence was a sensitive issue prior to the Congress of Vienna. It was the cause of tension among diplomats, including conflicts among States. The Vienna Regulations of 1815 established rules, order, and stability in this field.

[37] The Havana Convention, to which 14 South American States became party, was an interim solution for the lack of rules in this field. It codified some regional customs, such as diplomatic asylum, which remains specific to this region. See <http://www.oas.org/Juridico/english/sigs/a-25.html> accessed 10 November 2013.

[38] The 'Harvard Convention' was a private codification which made significant impact on the subsequent codification of diplomatic law. More information on the codification can be seen C. E. Baumann, *The Diplomatic Kidnappings: A Revolutionary Tactic of Urban Terrorism* (The Hague, Netherlands: Martinus Nijhoff, 1973) p.37.

[39] *Convention on the Privileges and Immunities of the United Nations*, 1 U.N.T.S. 15.

[40] *Convention on the Privileges and Immunities of the Specialized Agencies*, approved by the General Assembly of the United Nations on 21 November 1947, see <http://www2.kobe-u.ac.jp/~nmika/linked_files/Special_Lecture2010/Treaties/Convention_Priviledges_Immunties_Specialized_Agencies.pdf> accessed 10 November 2013.

[41] *Vienna Convention on Diplomatic Relations*, 500 U.N.T.S. 95.

[42] ICJ*, Case concerning United States Diplomatic and Consular Staff in Tehran,* Judgment, I.C.J. Reports 1980, p.3, para. 86.

main development was the fast growth of multilateral diplomacy, especially since 1945, with new forms of representation of States via permanent missions, and the need to regulate the diplomatic status of international organisations and their officials.[43]

These developments triggered the adoption of other diplomatic law conventions based on the provisions of the VCDR: the 1963 *Vienna Convention on Consular Relations* (VCCR),[44] the 1969 *Convention on Special Missions* (CSM), and the 1975 *Convention on Relations of States with International Organizations* (CRSIO).[45] In addition to these core instruments, diplomatic law also includes the 1977 *Convention on the Prevention and Repression of Offences against Internationally Protected Persons including Diplomats*.[46] The main focus of the present analysis will be the VCDR. Reference will be made to other conventions when they differ from the VCDR regulations.

3.1 Status and Organisation of Diplomatic Relations

According to Article 2 of the VCDR,[47] the process of establishing diplomatic relations between States is a matter of agreement between the governments concerned. Typically, diplomatic relations follow mutual recognition of two countries, especially after the newly declared independence of one of them. Establishing diplomatic relations does not require the opening of diplomatic missions in the respective capitals. In fact, many countries, due to limited human and financial resources, cannot maintain an extensive network of diplomatic missions. For example, Malta has diplomatic relations with 162 countries which are covered by 25 resident diplomatic missions (embassies and high commissions),[48] 19 non-resident ambassadors based at regional hubs (e.g. Japan is covered from the embassy in Beijing), and 13 non-resident ambassadors based in the capital (Valletta).[49, 50]

[43] In addition, new actors in global diplomacy have emerged, with claim to be recognised as diplomatic actors: special envoys, regional/local entities, rebel groups, and civil society, among others.

[44] *Vienna Convention on Consular Relations*, 596 U.N.T.S. 8638.

[45] *Convention on Relations of States with International Organizations*, UN Doc. A/CONF.67/16 (14 March 1975).

[46] *Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, Including Diplomatic Agents*, 1035 U.N.T.S. 167.

[47] *Vienna Convention on Diplomatic Relations*, 500 U.N.T.S. 95.

[48] Malta also has seven permanent missions to international organisations.

[49] For an analysis of diplomatic challenges of small States see 1. V. Camilleri, *How Small States Influence Diplomatic Practice: A Look at The Fourth Round of Accession Negotiations to the European Union* (Paper presented at the International Conference on the Diplomacy of Small States, Malta, 8-9 February) <http://www.diplomacy.edu/poolbin.asp?IDPool=357> accessed 18 April 2013.
2. A. Henriksen, 'Diplomacy and Small States in Today's World' in *The face of man, Vol. 2, The Dr. Eric Williams Memorial Lectures 1993 – 2004* (Trinidad and Tobago: Central Bank of Trinidad and Tobago, 2005) <http://textus.diplomacy.edu/thina/TxFsetW.asp?tURL=http://textus.diplomacy.edu/thina/txgetxdoc.asp?IDconv=3224> accessed 18 April 2012.
3. A.N. Mohamed, 'The Diplomacy of Micro-States' (Clingendael Discussion Papers in Diplomacy, No. 78. 2002) <http://www.clingendael.nl/publications/2002/20020100_cli_paper_dip_issue78.pdf> accessed 18 April 2012.

[50] Data from the website of the Maltese Ministry of Foreign Affairs, <http://www.foreign.gov.mt/default.aspx?MDIS=741> accessed on 11 November 2013.

The trend of finding new ways of maintaining diplomatic relations is driven by pressures to reduce government expenditures, including expenses for diplomatic services. New innovative ways that increasingly rely on the intensive use of digital tools have been emerging. One is the use of missions in multilateral posts as hubs for a range of diplomatic or consular activities that cannot be conducted bilaterally (e.g. permanent missions to the UN in New York are used for this purpose by many small States). A second is the use of regional hubs to cover countries in the region (e.g. the ambassador in New Delhi could cover Southern Asian countries as a non-resident ambassador). A third innovative practice is diplomatic coverage from the capital, via a non-resident, so called 'roving', ambassador (this practice of using a roving ambassador is often referred to as the 'Scandinavian model', as it was first endorsed by Sweden). A fourth is the use of honorary consuls, recruited from the expatriate population, or even extra-national, cultural, business, or professional communities. A fifth is contracting some services, either from friendly nations (e.g. consular services) or from specialised private operators (e.g. lobbying activities).

Today's information and communication technologies are opening up a sixth alternative – that of virtual embassies, i.e. embassies that do not have physical premises. A virtual embassy would still have an ambassador. In a *real* embassy, the ambassador resides (physically) in the embassy located in the territory of the receiving State. In a *virtual* embassy, the ambassador would remain in the capital city of his or her own country and communicate with the other country by electronic means.

The experiments with virtual embassies led in two directions. First, the technology-driven approach led towards establishing virtual embassies on Diplomacy Island of Second Life, an online virtual world. The first example was the virtual embassy of Maldives[51] followed by Sweden, Estonia, the Philippines, Macedonia and Columbia. These virtual embassies were virtual reality replicas of real buildings with the possibility of interacting with cyber diplomats. This experiment has not been developed further, mainly due to the limitations of Second Life as an internet platform. Second, a function-based approach built virtual embassies as websites. For example, the US has 40 Virtual Presence Posts established to 'improve our engagement with specific communities where the U.S. has no physical diplomatic facilities'.[52] In December 2011 the US established a completely virtual embassy in Iran, a country where it has no physical diplomatic representation.[53]

[51] B. Muralidhar Reddy, 'Maldives opens "virtual embassy"' *The Hindu* (25 May 2007) <http://www.thehindu.com/todays-paper/tp-international/maldives-opens-virtual-embassy/article1847030.ece> accessed 10 November 2013.

[52] Major Programs of IRM's Office of eDiplomacy' (U.S. Department of State, 2013) <http://www.state.gov/m/irm/ediplomacy/c23840.htm> accessed 10 November 2013.

[53] The US interests in Iran are protected by the Swiss embassy in Teheran. The US virtual embassy to Iran is located at <http://iran.usembassy.gov> accessed 10 November 2013.

The interplay between new technological developments, especially in the field of virtual reality, and the need to perform diplomatic functions in a more effective way, will affect the future of 'virtual embassies'. It is very likely that virtual embassies will be used for 'blended diplomatic representation' by using virtual tools for maintaining contact between the visits of non-resident ambassadors ('roving' ambassadors). Blended representation could combine the best of the two forms of representation: traditional (physical contact, developing personal rapport) and online (low cost, continuous communication).

3.2 Core Diplomatic and Consular Functions in the Internet Era

Scholarly writings provide numerous classifications of diplomatic functions. The classification used in this chapter is based on Article 3 of the VCDR which depicts the following diplomatic functions as:

(a) representing the sending State in the receiving State;

(b) protecting in the receiving State the interests of the sending State, and of its nationals, within the limits permitted by international law;

(c) negotiating with the Government of the receiving State;

(d) ascertaining by all lawful means conditions and developments in the receiving State, and reporting thereon to the Government of the sending State; and

(e) promoting friendly relations between the sending State and the receiving State, and developing their economic, cultural and scientific relations.

3.2.1 Representation

From the earliest days, representation has been a vital function of diplomacy. Representation involves speaking and acting on behalf of the sending State. Formally, it includes participation in the official functions of the receiving State on behalf of the sending State. Such participation is a sign of goodwill, and can enhance further relations between the sending and the receiving States. Accordingly, Costas Constantinou defines diplomacy through communication and representation: 'At its basic level, diplomacy is a regulated process of communication between at least two subjects, conducted by their representative agents over a particular object.'[54]

The most common form of representation, through resident diplomatic missions, has already been challenged by several emerging practices.[55] However, driven by technological advances, questions arise about what impact the internet will have on diplomatic representation, and whether the official websites of the Ministries of

[54] C. M. Constantinou, *On the Way to Diplomacy* (Minneapolis USA: University of Minnesota Press, 1966) p.25.

[55] See section 3.1.

Foreign Affairs (MFAs) and diplomatic missions can be deemed another form of State representation.

Websites currently provide the main presence of diplomatic services on the internet. There is a considerable number of diplomatic websites, including approximately 150 MFA websites, and more than 3000 diplomatic and consular mission websites. Most MFA websites offer basic foreign policy texts, press releases, a *who's who* of the MFA, travel information, information for foreigners and more. Initially, websites were created as internet versions of the traditional one-to-many diplomatic communication, but they are now shifting towards more interactive communication through integration with social media such as blogs and Twitter.

If a State's official website is its representation on the internet, this raises many questions about the way in which diplomatic representation is conducted. For example, what is the legal status of the US virtual embassy to Iran, and other web-based representations introduced under the Virtual Presence Points programme? Could the internet blocking of the website of the US Virtual embassy to Iran be considered a refusal to accept this type of diplomatic relations? The practice of virtual representation could contribute to the increasing invalidation of Article 41(2) of the VCDR, which specifies that '[…] all official business [...] shall be conducted with or through the Ministry of Foreign Affairs […]'. This paragraph has already been rendered obsolete by the practice of modern diplomacy, in which diplomats communicate directly with various ministries and individuals in the receiving country. The use of official websites for representation could further bypass this norm.

Another important aspect of diplomatic activities on the internet is the relevance of online content to the development of international customary law. Currently, it is not clear whether information published on a website or Facebook page can be considered an official statement by a ministry, and therefore, a possible indication of an *opinio iuris* of, and/or contribution to, the establishment of consistent practice by a State, these aspects being preconditions for the development of international customary rules. So far, there are no examples of the use of online communication as supporting evidence for the development of international customary law.

With online presence, diplomatic services are also more exposed to potential fraud that could endanger their representation roles. As an example, in 2011 the Indian Consulate General in Geneva published a notice in the *International Herald Tribune*, advising the public about a fraudulent website using the consulate's name.[56] What can the Indian government do in a situation such as this? Can India force the takedown of the fake website of the Indian Consulate in Geneva and, if so, through what means? If the

[56] Although the article in the *International Herald Tribune* is no longer accessible, a scan of the public notice can be seen at <http://deepdip.wordpress.com/2011/12/03/internet-fraud-in-diplomacy/> accessed 09 November 2013.

fraudulent website is registered under the '.ch' domain, the government of India may take action based on Article 28 of the VCCR and request the receiving State to provide 'full facilities for the performance of the functions of the consular post'. The closest analogy to the 'real' world would be that India would demand the closing of any building which falsely claimed to be the Indian Consulate General. But in the online world, this is not likely to be effective. Governments cannot just order national internet registrars to remove a website. If the fraudulent website were registered under a generic domain (.com, .org, .net), the situation would be even more complicated, since the responsible registrars might be located abroad, under foreign jurisdiction. The possibility for legal action, even at the level of theoretical speculation, is almost non-existent.[57]

3.2.2 Protection of Nationals and Consular Assistance

The protection of nationals, and consular assistance, deal with defending or safeguarding any assets or interests of the sending State and its nationals (as well as their assets and interests) from disadvantageous consequences (or from disadvantageous situations, actions, or injuries).

Consular assistance focuses mainly on the protection of interests and the wellbeing of nationals of the sending State. From once being the 'Cinderella' of traditional diplomacy,[58] consular protection has evolved into the recognition that it is a vital part of diplomatic services.[59] The current relevance of consular activities was catalysed by growing public demand for the protection of citizens, and effective response to crises. Easier and more affordable travel, in particular air transport, increased citizens' mobility and their need for consular protection. With instant social and traditional media coverage, natural and political crises worldwide became part of domestic politics. The protection of nationals caught in a crisis easily garners high media and political visibility. MFAs are under increasing pressure to provide more services with limited resources. This tension is probably why the consular field has been an area of many innovations in diplomacy, including the introduction of e-visas, the strengthening of the role of honorary consuls, and the use of social media for communication with nationals.

For example, social media has proven to be highly effective in crisis situations. A crisis situation, natural or political, affects a broad range of people, and communication is an essential part of dealing with it. Faced with danger, people organise themselves by using all available e-tools, including mobile phones, Twitter, and Facebook, very often

[57] J. Kurbalija, 'Internet Fraud in Diplomacy' (Reflections on Diplomacy, 03 December 2011) <http://deepdip.wordpress.com/2011/12/03/internet-fraud-in-diplomacy/> accessed 10 November 2013.

[58] M. Heijmans and J. Melissen, 'Foreign Ministries and the Rising Challenge of Consular Affairs: Cinderella in the Limelight' in K. S. Rana and J. Kurbalija (eds), *Foreign Ministries: Managing Diplomatic Networks and Optimizing Value* (Malta: DiploFoundation, 2007) pp.192–206.

[59] For a long time, consular activities have been considered less important than diplomatic ones. In MFAs, the main career path was related to bilateral and multilateral diplomacy. Consular activities started regaining relevance in recent years.

in innovative ways. In the case of natural disasters, notable examples include the Asian tsunami (2004) and the earthquakes in Chile (2010)[60] and Haiti (2010).[61] In political crisis situations, an example of the prominent use of e-tools was the Arab Spring (2010-2011).[62] These examples demonstrate an essential role for social media in diplomatic services, whether diplomats are involved in humanitarian assistance, in support for their citizens, in conflict prevention, or in other situations.

Further, the internet and social media have revolutionised the relationship between the diaspora and their home country. Previously sporadic contact has evolved into more regular interaction. In this time of financial crisis, with the growing importance of remittances, the migrants' role in the political and social life in their home country has been increasing in importance. The use of social media for connecting the diaspora provides a lot of opportunities. It is still an underused area of e-diplomacy, although there are some examples of its use, such as the extensive use of Facebook by the US and the UK to connect with expatriates, both for disseminating information and for providing a forum for conversation.[63]

The use of social media in this field has raised some new controversies. One illustrative case was the reporting by the US Embassy in Beijing on air-pollution based on data collection by air-sensors at the Embassy premises.[64], [65] Chinese officials said that such practice breached Article 41 of the VCDR which requires that diplomats should act in accordance with the laws of the receiving State and conduct their official business via the MFA.[66] US officials replied by shifting discussion from the diplomatic to the consular field. They justified the sharing of air-pollution data on the basis of assisting

[60] 'Twitter tells the real-time story of the quake's human toll' *France 24* (28 February 2010) <http://www.france24.com/en/20100227-twitter-disaster-info-chile-earthquake-america-south-tsunami-internet> accessed 11 November 2013.

[61] 'Twitter Helps in Haiti Quake Coverage, Aid' *The Wall Street Journal* (14 January 2010) <http://blogs.wsj.com/digits/2010/01/14/twitter-helps-in-haiti-quake-coverage-aid/> accessed 11 November 2013.

[62] 'Facebook, Twitter Help the Arab Spring Blossom' *Wired Magazine* (16 April 2013), <http://www.wired.com/magazine/2013/04/arabspring/> accessed 11 November, 2013.

[63] See, for example, the 'UK in Bahrain' – Facebook page <https://www.facebook.com/ukinbahrain/> accessed 18 October 2013.

[64] J. Kurbalija, 'Is tweeting a breach of diplomatic function?' *Diplo* (Malta, 2012) <http://www.diplomacy.edu/blog/tweeting-breach-diplomatic-function#_ftn1> accessed 17 October 2013.

[65] K. Bradsher, 'China asks other nations not to release its air data' *N.Y. Times* (2012) <http://www.nytimes.com/2012/06/06/world/asia/china-asks-embassies-to-stop-measuring-air-pollution.html?_r=3&> accessed 17 October 2013.

[66] China's reaction reflects its cautious approach to, and potential dilemmas with, the position of diplomats in the internet era. The complaint was lodged by the Vice-minister for the Environment, not the MFA. Usually, in the case of a breach of the Vienna Convention (1961) protests are lodged by diplomatic note, or in more extreme cases, by declaring foreign diplomat(s) *persona non grata* (in this case, the US environmental representative, perhaps?). The Chinese authorities decided to send a diplomatic signal (i.e. express uneasiness) without escalating the conflict, see Kurbalija, *supra* note 64.

American citizens in China, something they are entitled to do according to Article 5 of the VCCR.[67]

3.2.3 Negotiation

Negotiation is considered the main function of diplomacy both in bilateral and in multilateral diplomatic relations. Quincy Wright defines diplomacy as 'the art of negotiation, in order to achieve the maximum of group objectives with a minimum of costs, within a system of politics in which war is a possibility.'[68] Hedley Bull defines diplomacy as 'the management of international relations by negotiations.'[69] While the function of negotiation – reaching agreement – involves important human input based on particular skills and talents, many activities surrounding multilateral and bilateral negotiations are of a routine nature and appropriate for automation. The process of multilateral negotiation can be highly automated through the use of online tools to facilitate logistical support, distribute materials, and to enable the participation of non-governmental organisations and others. In this context, online tools cannot alter the actual negotiating methods, but they can change the environment in which the negotiation is prepared and conducted.

The first major use of computers in an international negotiation was at the Earth Summit in Rio de Janeiro (1992), where mailing lists were used to follow the negotiations and engage the global community. The use of mailing lists was further developed at major UN conferences on human rights (1993), population (1994), women (1995), and social development (1995). However, the main breakthrough in the use of the internet came during the WSIS meetings in 2003 and 2005, and at IGF meetings, which have been held annually since 2006. Perhaps the reason for this breakthrough is that it seemed logical that negotiations discussing the internet should use the internet as a tool. The WSIS and IGF meetings set new standards in e-diplomacy and inspired the use of new e-tools in other areas of multilateral negotiations, such as climate change, migration, and human rights.

During the WSIS, the internet was available in conference rooms, through the widespread use of wireless technology ('wireless fidelity' – WiFi, also known as 'wireless local area network' – WLAN). It made international negotiations more inclusive and open through the participation of an increased number of civil society and business sector representatives, including those who could not, for financial or other reasons, physically

[67] Article 5 of the *Vienna Convention on Diplomatic Relations*, 500 U.N.T.S. 95.

[68] Q. Wright, 'The Role of International Law in Contemporary Diplomacy' in S.D. Kertesz and M.A. Fitzsimons (eds.), *Diplomacy in a Changing World* (Indiana, USA: University of Notre Dame) p.55.

[69] H. Bull, *The Anarchical Society: A Study of Order in World Politics* (New York: Columbia University Press 1977) p.162.

participate in the meetings,[70] as they began to participate online. For diplomats at the WSIS and IGF meetings, the WiFi connection provided constant contact with their MFAs and other government departments dealing with WSIS issues. In some cases, a WiFi network of notebooks enabled the coordination of initiatives among representatives physically present in a conference room. Exchanges of SMSs, tweets, and emails complemented and sometimes replaced the traditional ambiance of short chats between diplomats from different countries, *tête-à-tête* exchanges, and corridor diplomacy. Because physical movements can reveal the dynamics of negotiations or even form part of diplomatic signalling, this aspect of *in situ* diplomatic negotiation started changing with the use of the internet in conference rooms.[71] The experience from WSIS and the IGF meetings also shows that, despite all the promises of virtual conferencing and other multimedia technologies, today – even more so than in the past – text remains diplomacy's central tool. Most exchanges between preparatory sessions are done via mailing lists and e-mail. The IGF is supported by very active social media discussions, using text-intensive tools, such as discussion lists, blogs, and Twitter.[72]

Another development which highlights the relevance of text is the emergence of verbatim reporting at IGF meetings. This development may have a substantive impact on multilateral diplomacy and negotiations. Verbatim reporting is the process whereby all verbal interventions are transcribed simultaneously by special stenographers and immediately displayed on a large screen in the conference room, as well as broadcasted via the internet. [73] While delegates are speaking, transcripts of their speeches appear on the screen. Verbatim reporting has had an important effect on the diplomatic *modus operandi.* The awareness that what is said will be preserved in print, makes many participants more careful in choosing the level and length of their verbal interventions. Verbatim reporting also increases the transparency of diplomatic meetings.

Additionally, the internet has potential applications in the conversion of verbal agreements to a written format; this is one of the crucial phases in the negotiation process. Group editing applications enable negotiators to work collaboratively on a text by changing the text and adding comments.

The use of new e-tools for negotiation should be approached carefully, and within appropriate contexts. Diplomacy is a profession that often requires discretion. While openness is the guiding principle of good governance, reality shows that most of the successful diplomatic deals have been done discretely, far removed from the public

[70] J. Kurbalija, 'World summit on Information Society and the Development of Internet Diplomacy' in M. Gatt and R. Fsadni Azad (eds.), *Governing the Internet* (Malta: Academy for the Development of a Democratic Environment, 2011) ch. 2 <http://thinkingeurope.eu/sites/default/files/publication-files/governing_the_internet.pdf> accessed 10 November 2013.

[71] *Ibid*.

[72] Kurbalija, *supra* note 30.

[73] Kurbalija, *supra* note 26, p.152.

eye.[74] There are many reasons why negotiations should be discreet. Sometimes, discreetness is needed to protect the interlocutor on the other side of the table.[75] In many cases negotiators spend a lot of time finding face-saving formulas for the audience back home.[76] Discreetness usually helps to prevent effective negotiations from turning into a show for the general public. It should be borne in mind that the core of diplomacy is not popular in many societies, especially when it is contrasted with national interest, pride, and glory. Reaching a compromise and maintaining discretion in negotiations are very often closely linked.[77] This considered, it is easy to envisage negotiations that could not be conducted efficiently in front of web cameras. The decision whether to use technical tools for negotiation will be probably in itself part of the negotiation.

Most procedures for diplomatic negotiations are drafted for an event where negotiators are present in the same physical location. Online tools provide the possibility for remote participation. They open a new set of procedural and legal questions: can remote participation be considered the same as *in situ* participation? Can negotiating parties submit amendments online?[78] Is online voting the same as *in situ* voting? Since the use of e-tools is both a reality and a necessity in modern diplomatic negotiations, legal and procedural questions will have to be addressed either by introducing amendments to existing procedural rules or developing new rules and practices.

3.2.4 Information Gathering

Information gathering is a traditional diplomatic activity listed in the VCDR and in most definitions of diplomacy. While information was a scarce resource throughout history, the current period is characterised by the massive production of information in electronic formats. The former difficulty of obtaining information has, to a large extent, been replaced by the challenge of managing, validating and processing what is now available. This abundance of information is as problematic as scarcity once was: important information can be lost in sheer quantity. Fast and precise access to necessary information is *conditio sine qua non* of the proper functioning of an MFA and other participants in foreign policy.

Over the last ten years, diplomats have shifted from relying on internal, mainly traditional, resources to relying on information available outside diplomatic services, mainly on the internet. Sophisticated search engines such as Google, Bing and Yahoo! have made possible precise and timely access to needed information. Diplomats also

[74] *id*, ‘How will Wikileaks affect diplomacy?’ *Diplo* (Geneva, 1 December 2010). <http://www.diplomacy.edu/blog/how-will-wikileaks-affect-diplomacy> accessed 09 November 2013.

[75] *Ibid*.

[76] *Ibid*.

[77] *Ibid*.

[78] Some of these issues have been already discussed in the organisations that are the most advanced in using online tools, such as the International Telecommunication Union.

often use new services such as Wikipedia, a web-based encyclopaedia with over 13 million articles written in many languages by contributors around the world, as a starting point and orientation, before continuing to more in-depth research.[79] It is very relevant for diplomats because, in most cases, it provides complete and up-to-date coverage of main diplomatic events and policy developments. Very often, Wikipedia contains first-hand information from people on the spot. Only a few large diplomatic services can provide coverage of international events comparable to Wikipedia. Of course, it is necessary to verify information from Wikipedia while comparing it with information from other sources. The blogosphere is another highly relevant source of information and opinion available for diplomats. Unlike anonymous Wikipedia articles, blogs are attributed; some blogs are written by respected and influential authors. Blogging as a media channel is now a well-established and recognised communication tool. Today there are more than 100 million blogs with often informal, but well-established, ranking procedures.[80] Blogs are particularly influential in specialised policy fields such as climate change, migration, and food security. They influence policy and agenda-shaping in international negotiation. Another emerging approach is to combine access to open data with advanced data-mining techniques. New policy insights could be gained by accessing previously unrelated data in a new context.

The Snowden revelations of the information surveillance of embassies and missions put in focus the difference between lawful and clandestine information gathering, as well as between diplomacy and intelligence. The former British diplomat Sir Reginald Hibbert provided the following breakdown of information gathering in diplomacy:[81] (1) 90% of information is gathered by using lawful means, of which 50% is gathered from public sources; 10–20% from confidential contacts of diplomats; 20–25% from leaks and indiscretion; (2) 10% of information is obtained through covert and clandestine operations, usually referred to as intelligence.

These two main ways of gathering information lead to a complex interplay, and even tension, between diplomacy and intelligence. Intelligence has been developing rapidly since the nineteenth century when many European countries established a so-called *cabinet noir* within their secret police for surveillance of foreign diplomatic correspondence.[82] Intelligence gathering grew in strength during the two World Wars and during the Cold War, and started competing with diplomacy. As described by

[79] Wikipedia <http://www.wikipedia.org> accessed 17 October 2013.

[80] See for an example of a blog ranking 'Technorati Top 100' (Technorati 2013) <http://technorati.com/blogs/top100/> accessed 09 November 2013.

[81] Hibbert's information source breakdown was prepared in the 1990s before the explosive growth of the internet. It is very likely that the importance of public sources has increased, especially with new possibilities of generating intelligence through the use of data-mining tools. R. Hibbert, *Intelligence and National Security* (London: Hodder and Stoughton, 1990) p.112.

[82] K. Hamilton and R. Langhorne, *The Practice of Diplomacy* (London: Routledge, 1995), pp.122-124.

Hibbert, 'secret intelligence, from being a somewhat bohemian servant and associate of the great departments of state, gradually acquired a sort of parity with them.'[83]

Diplomacy and intelligence are two closely related but separate functions of a State's foreign affairs apparatus. They involve different methods, institutional frameworks, and skills. The overlap between diplomacy and intelligence exist when an intelligence officer uses a diplomatic cover by acting as diplomatic staff. Intelligence officers get diplomatic titles in order to benefit from diplomatic protection and immunities.[84] Diplomacy and intelligence increasingly compete for resources and influence with policymakers.

The VCDR draws a clear dividing line between diplomatic and intelligence functions. Article 3(1) specifies that diplomats should acquire information *by all lawful means*.[85] Information gathering by diplomats can be conducted in a confidential way, but it should not be clandestine (espionage) and illegal. This distinction is particularly important when clandestine operations become public, as through the recent revelations about the US National Security Agency (NSA) surveillance by the whistleblower Edward Snowden. The public knowledge of such operations could trigger questions of State responsibility for a breach of the VCDR. It could be also a reason why both US and UK authorities have been expressing general regret, while avoiding specific apologies to officials or countries allegedly targeted by the surveillance operation. Such apologies could be tacit official confirmations of such practice that could trigger use of international legal remedies by the affected countries.

Snowden's recent revelations include cases of surveillance of diplomatic communications at the G20 meeting in London in 2009,[86] the offices of 38 diplomatic missions in the US[87] and the Heads of State of Brazil and Mexico.[88] This brings into focus the ever persistent question of acceptable ways of acquiring information. Intelligence gathering was always part of diplomatic practice. However, the VCDR clearly outlawed intelligence gathering which does not use 'lawful means'. There are also strong elements for arguing that international customary law prohibits surveillance of a Head of State or Government. The protection of the secrecy of diplomatic communication and the impact of the

[83] Hibbert, *supra* note 81, p.114.

[84] During the Cold War, it was typical to have massive expulsions of Soviet Union and Western diplomats, who were intelligence officers working under diplomatic cover. One of the largest was the expulsion of 105 Soviet diplomats from London in 1971.

[85] The VCCR is more specific than the VCDR by indicating in Article 5 that 'by all lawful means' refer to 'commercial, economic, cultural and scientific life of the receiving state'.

[86] E. McAskill, N. Davies, N. Hopkins, J. Borger J. Ball, 'GHCQ interception foreign politicians' communications at G20 summit' *The Guardian* (16 June 2013) <http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits> accessed 17 October 2013.

[87] *Ibid*.

[88] V. Bevins and T. Wilkinson 'New Snowden documents allege US spying on Brazil, Mexico' *LA Times* (2 September 2013) <http://articles.latimes.com/2013/sep/02/world/la-fg-wn-ff-snowden-spying-brazil-mexico-20130902> accessed 17 October 2013.

Snowden revelations on diplomatic immunities and privileges will be discussed *infra* in more detail (section 4.3.2).

3.2.5 Diplomatic Reporting

The internet has definitely affected diplomatic reporting. It has made it more effective, more immediate, more cost-effective, and less formal. In the past, diplomats competed with journalists to obtain current news. In the late 1990s, a shift occurred with real time coverage of world events 24/7 (so called 'CNN effect'). The next shift in diplomatic reporting came with the emergence of Wikipedia and social media, which further focused diplomatic reporting on analysis and evaluation that cannot be otherwise found on the internet.

Their constant connectivity with their capital has also made diplomats more present in decision-making processes back home. This is augmented by a ready access to the aggregated knowledge and experience of their colleagues and their counterparts via wikis, blogs, and information aggregators. That, for example, an expert on Asian affairs can be called to the table quickly to give an opinion on a crucial matter, or indeed that the diplomatic circle of knowledge is expanding to include academics and other subject-matter professionals, can only better serve the cause of diplomatic analysis and reporting.

A recent survey of 105 diplomats from five regions (the Americas, Europe, Africa, the Middle East, and Asia) shows the major impact of the internet on diplomatic reporting.[89] The vast majority claimed that it has made their work more effective, more immediate, more cost-effective, less formal, and more pressurised (see Table 1).

No change	Less	More	
4%	5%	91%	Effective
6%	1%	92%	Immediate
5%	9%	86%	Cost effective
9%	84%	6%	Formal
17%	20%	63%	Pressurised

Table 1. How has the internet affected diplomatic reporting?

[89] M. Murphy, 'How has the Internet affected diplomatic reporting?' *Diplo* (Malta, 01 July 2013) <http://www.diplomacy.edu/blog/how-has-internet-affected-diplomatic-reporting> accessed 17 October 2013.

4. Immunities, Privileges and Facilities

The provisions of the VCDR and related diplomatic conventions regulate the aspects of immunities, privileges, and facilities. While these three concepts are sometimes used in overlapping ways in practice, the VCDR distinguishes between them as follows:

- Immunities are exemptions from the jurisdiction of the foreign State. Immunities include inviolability, the giving of evidence, and the execution of judgements in civil proceedings. In practice, a distinction is made between immunities granted to entities, organs, and their premises; immunities granted to diplomats and their dependents; and immunities granted to their activities.
- Privileges refer to the exemption from certain laws and regulations of the receiving State. These are privileges to the extent that others, especially the citizens of the receiving State, do not enjoy. Exemption from taxation by the receiving State is another example of diplomatic privileges. Others are the non-applicability of certain social security laws of the receiving State and the exemption from civic duties.
- Facilities are typically courtesies extended by the receiving State to enable diplomatic missions and their agents to carry out their functions smoothly. Requirements, such as assisting the mission in finding suitable premises, facilitating free communications, and allowing free travel within the receiving State, are examples of facilities.

This section will first elaborate on State immunity, followed by the immunities of Heads of State and Government. It concludes with an analysis of immunities, privileges, and facilities of diplomatic and consular missions and staff.

4.1 State Immunity

Until the twentieth century, States enjoyed absolute immunity for any act; such an absolutist conception of sovereignty deprived individuals and corporate entities of any remedy when a public administration failed to honour its legal obligations under ordinary contracts. However, it gradually became accepted that whenever a State authority acted in the same way as a private person or entity (e.g. in commercial activities), it should not enjoy immunity. By the end of the nineteenth century, the concept of qualified immunity had been introduced in international law. During the twentieth century, qualified immunity gradually replaced absolute immunity, introducing the distinction between acts *iure imperii,*[90] where the State exercises its sovereign power and *iure gestionis*, where the State behaves as if it were a private entity.[91, 92]

The question of sovereign immunity may appear in internet issues. If a State acts in order to protect its online facilities, it is done in an *iure imperii* capacity which provides a State with necessary immunity. Most other cyber activities will be considered *iure gestionis*, so a State will not be able to enjoy immunity.

4.2 Immunities of Heads of State and Government

The distinction between the immunity of States and that of Heads of State is a new development in international law. In the past, Heads of State had the same immunity as the State. In modern international law, these two types of immunities are different.[93]

No mention of Heads of State occurs in the VCDR. The UN *Convention on Special Missions* of 1969 mentions, in Article 21, that Heads of State enjoy ‘privileges and immunities accorded by international law to Heads of State on an official visit’, but it does not elaborate further.[94] However, it is widely accepted that international customary law grants privileges and immunities to Heads of State, a practice which originated during the times of absolute monarchies, when the sovereign enjoyed absolute immunity.[95] This approach is confirmed by international jurisprudence. In the *Congo* case, the ICJ reaffirmed the principle of immunity of a Head of State and other high officials. The Court stated: ‘in international law it is firmly established that [...] certain holders of high-ranking offices, such as the head of State, head of government and minister of foreign affairs, enjoy immunities from jurisdiction in other states, both civil

[90] An example of an act *iure imperii* is the use of the army in an armed conflict. In 1989, in the case of the Argentine Republic v. Amerada Hess Shipping Corporation, the United States Supreme Court found no difficulty in granting immunity to Argentina against a claim filed by the owner of a tanker that the Argentine Air Force had attacked and damaged on the high seas during the Falklands War.

[91] The main problems of classification occur in the grey zones that come before the courts. A poignant example is the situation where States purchase military tanks. It is not always clear whether these transactions should be treated as cases of *iure imperii* (strengthening the armed forces) or as cases of *iure gestionis* (entering into commercial transactions). Two approaches have been used in determining the nature of State actors in this grey zone. First, an objective test may check the nature of a particular act, for example, to determine whether it is a commercial act. A second, subjective, test may be based on the purpose of a particular act. These two approaches are useful in solving many problems, but some issues remain open. For example, according to the objective test the purchase of army boots is considered *iure gestionis* (a commercial transaction). According to the subjective test, however, it could be an act *iure imperii* since army boots are purchased to perform one of a State's sovereign functions (defence).

[92] See P. Malanczuk, *Akehurst's Modern Introduction to International Law* (London: Routledge, 1997), p.120.

[93] It is also relevant that in certain countries, for example the United States, the Head of Government is also the Head of State, that is, the President. In some other countries, the position of Head of Government is separate from that of a largely ceremonial Head of State (in the United Kingdom, for example, the Head of State is the Queen).

[94] *Convention on Special Missions*, 1400 U.N.T.S. 231.

[95] See Malanczuk, *supra* note 92, p.119.

and criminal.'[96, 97] Immunities of Heads of State and Government should be analogous to diplomatic immunities and include immunity from criminal and civil jurisdiction; inviolability of residence, person, and movable property; freedom of communication, etc.

The alleged surveillance of the Presidents of Brazil, Mexico and others by the NSA could raise the question of a breach of international customary rules guaranteeing immunities for Heads of State.[98] Respective revelations triggered official diplomatic protests, the postponement of the visit of the Brazilian President to the US, and the first diplomatic actions in the UN system (discussion in the UN Security Council, address by the President of Brazil at the UN General Assembly).

4.3 Diplomatic Immunities, Privileges and Facilities

4.3.1 Inviolability of Hardware and Digital Assets

The immunities accorded to the mission premises are endorsed in Article 22(1) of the VCDR which States that the mission premises shall be inviolable. Denza elaborates on what the concept of inviolability entails: 'Inviolability in modern international law is a status accorded to premises, persons or property physically present in the territory of a sovereign state, but not subject to its jurisdiction in the ordinary way.'[99] Furthermore, according to Article 22(2) of the VCDR, the receiving State has a special duty to protect the mission from any intrusion or damage, and to prevent any disturbance of the peace of the mission, or the impairment of its dignity. In practice, receiving States have rigorously followed the principle of the inviolability of missions and any exceptions usually occur by accident or by mistake. Probably the most memorable recent event that illustrates the failure of a receiving State to protect the premises of a diplomatic mission took place between 4 November 1979 and 20 January 1981, when the militant university students seized the US Embassy in Tehran. The students later received support from the Khomeini regime. In its *Teheran Hostages* judgment, the ICJ specified that the 'Iranian government failed to take appropriate steps to protect the premises, staff, and archives of the United States mission against attack by the militants, and to take steps to prevent or stop the attack.'[100]

[96] *Arrest Warrant of 11 April 2000 (Democratic Republic of the Congo v. Belgium)*, Judgement, I.C.J Reports 2002, p. 21.

[97] A. Cassese 'When may senior State officials be tried for international crimes? Some comments on the *Congo v. Belgium* case.' (2002) 13 *European Journal of International Law* 853–975.

[98] Reuters, 'NSA spied on communications of Brazil and Mexico Presidents' *The Guardian US* (2 September 2013) <http://www.theguardian.com/world/2013/sep/02/nsa-spied-mexico-brazil-presidents> accessed 17 October 2013.

[99] E. Denza, *Diplomatic law: Commentary on the Vienna Convention on Diplomatic Relations* (Oxford: Clarendon Press, 1998), p.112.

[100] Teheran Hostage Case, *supra* note 42, para. 86.

Inviolability of diplomatic premises also extends to computers, printers, and other information technology facilities located on the mission premises. However, it is not clear whether inviolability could be extended to digital assets which are located outside the mission on, for example, internet servers in a cloud. For the protection of this type of digital asset, the closest analogy is the protection of bank accounts, which are held outside the premises of the mission. The VCDR did not regulate the status of such bank accounts – presenting circumstances which required additional interpretation of the Convention. Denza argues[101] that decisions of national courts and international practice confirm the international customary rule that inviolability can be extended to bank accounts if they are used for activities of diplomatic missions.[102] Article 25 of the CSM goes beyond the VCDR regulation and includes inviolability to 'other property used in the operation of the special mission'. Digital assets can enjoy the same protection as bank accounts. However, some digital assets such as electronic documents could enjoy wider protection via the provision of Article 24 of the VCDR that guarantees protection of diplomatic archives 'at any time and wherever they may be'. Even in the case of the closing of a diplomatic mission, diplomatic archives that include electronic documents will enjoy diplomatic immunity.

Consular posts do not enjoy as broad inviolability as diplomatic ones. Based on the Article 31 of the VCCR there are two major differences between the status of premises of diplomatic missions and those of consular missions. First, the inviolability of consular mission premises covers only those parts used for the work of the consulate, rather than the entire premises; second, and more importantly, consent to enter premises is assumed in the case of fire or other disasters.

It remains open to interpretation whether the right of the receiving State to enter consular premises in the case of 'fire and *other disasters*' (Article 31 of the VCCR, emphasis added) also covers a potential cyber disaster in the form of a major cyber attack and internet disruption. The provision of the right for emergency entry to consular premises was drafted in the view that most consular premises are located in the building with other tenants (unlike diplomatic missions which typically use villas or separate houses).[103] In the case of a fire on consular premises, other flats and offices could be endangered if there is not timely reaction by fire-fighters or other emergency services. One can argue that the same spirit that inspired the drafters of this provision (limited inviolability of consular premises in the case of disaster) could be used for dealing with cyber disasters when they create a risk for others. Digital facilities on consular premises could be used as a source of cyber attacks that could endanger the receiving State's internet system.

[101] Denza, *supra* note 99, pp.133–134.

[102] The inviolability of embassies' bank accounts was confirmed by the German Federal Constitutional Court in 1977 in the case: Philippine Embassy Bank Account. An Austrian court took a similar decision in the case Republic of 'A' Embassy Bank Account Case.

[103] This practice has been changing. In the main diplomatic centres (e.g. Geneva, Brussels, New York) embassies and permanent missions are increasingly located in business buildings alongside business offices.

As it is the case with a 'botnet', this could be done without knowledge of the officials of the consular office.[104]

4.3.2 Freedom of Diplomatic Communication

One of the postulates of diplomatic law is that diplomatic missions are entitled to free communication: communication that is unmonitored, unobstructed and free from surveillance or interference. Since Article 27 of the VCDR specifies that 'the mission may employ all appropriate means' of communication, this should include the use of the internet.

Article 27 of the VCDR introduces a special responsibility for the receiving State to 'permit and protect free communication on the part of the mission for all official purposes'. However, the internet architecture may bring problems for the receiving State in its duty to protect a mission's communication from possible interference and surveillance. Most diplomatic missions connect to the internet via local internet service providers, allowing easier access to diplomatic communication to a wide range of actors, including intelligence services and malicious actors. One early example of the limited possibilities for a receiving State to protect internet communication was the publishing in a Turkish newspaper of an intercepted email sent by the European Union delegation in Turkey in 2002.[105] The European Union demanded that the Turkish government take measures to enhance the security of its diplomatic representation in Ankara, pointing out that the correspondence was protected under the Vienna Convention.

The Snowden revelations of the online surveillance by the NSA brought the question of protection of diplomatic communications into sharper focus. These include allegations of reports of the electronic surveillance of 38 embassies and missions in the US whose communication was intercepted by the NSA,[106] and of extensive surveillance of local electronic communication by embassies of the US, UK, Canada and Australia in Bangkok, Beijing, Jakarta, Hanoi and other Asians capitals.[107] Leaked documents also

[104] 'A botnet (also known as a zombie army) is a number of internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the internet. Any such computer is referred to as a zombie - in effect, a computer 'robot' or 'bot' that serves the wishes of some master spam or virus originator. Most computers compromised in this way are home-based. According to a report from Russian-based Kaspersky Labs, botnets – not spam, viruses, or worms – currently pose the biggest threat to the internet. A report from Symantec came to a similar conclusion.' SearchSecurity, 'Definition botnet (zombie army)'. See <http://searchsecurity.techtarget.com/definition/botnet> accessed 18 October 2013.

[105] C. Collins, 'EU envoy's e-mail riles many Turks' *Chicago Tribune* (27 February 2002) <http://articles.chicagotribune.com/2002-02-27/news/0202270288_1_mails-e-mails-turkish-media> accessed 09 November 2013.

[106] E. MacAskill and J. Borger 'New NSA leaks show how the USA is bugging its European allies' *The Guardian* (30 June 2013) <http://www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies> accessed 17 October 2013.

[107] For more information see: 'Australian ambassador summoned amid Asia US spying reports' BBC <http://www.bbc.co.uk/news/world-asia-24757968> accessed 09 November 2013.

indicate heavy surveillance of multilateral meetings. In 2009, the UK's Government Communications Headquarters – the British e-spying agency – reportedly monitored mobile and computer communication of world leaders and diplomats attending the G20 meeting in London.[108]

The Snowden revelations raise the question of whether the internet surveillance of diplomatic missions and diplomats is in accordance with international law and the national law of the host State, where the mission and diplomats are based. In international law, the VCDR is clear in stipulating that surveillance of diplomatic communication and access to diplomatic documents could be deemed a breach of Article 27 of the VCDR. Internet surveillance is also in breach of Article 24 of the VCDR: 'The archives and documents of the mission shall be inviolable at any time and wherever they may be.'[109] Besides the host State, Article 40(3) of the VCDR requires third-party countries to protect diplomatic communication in transit. It extends protection of diplomatic communication to all places where internet communication passes. For example, diplomatic messages going from a diplomat's computer in Geneva, to a server in the US should, according to the respective interpretation of the VCDR, enjoy protection along the internet route. In such a case, Article 40 of the VCDR forms the basis for the legal assessment of the legality of the interception of e-mail communication outside of the country where the diplomat is accredited.

While the VCDR provisions are clear in making surveillance of diplomatic missions and diplomats illegal, some authors open discussion of legality of surveillance based on the fact that it is widely practiced by many States. Simon Chesterman stresses the limits of the development of international customary rules that could provide legal justification for surveillance: 'if the vast majority of states both decry it and practice it, State practice and *opinio juris* appear to run in opposite directions'.[110] Some other authors try to develop a legal basis for surveillance of diplomats by stressing that surveillance must be done within customary normative limits.[111] Although the surveillance of diplomats is practiced by many countries, it is not possible to find arguments for considering it legal under international customary law for the following reasons: first, existing treaty law – the VCDR – prohibits the surveillance of diplomats and diplomatic missions; second, the VCDR is the codification of international customary law. Surveillance of diplomats cannot be considered to be a new custom developed since the adoption of the VCDR. Surveillance is as old as diplomacy and if the customary rules on the surveillance of

[108] McAskill et. al., *supra* note 86.

[109] See section 4.3.3.

[110] S. Chesterman, 'The Spy Who Came in from the Cold War: Intelligence and International Law' (2006) 27 Michigan Journal of International Law, p. 1072.

[111] S. M. McDougal, H. D. Lasswell, and W. M. Reismann, 'The Intelligence Function and World Public Order', (1973) 45 Temple Law Quarterly 365.

diplomats existed, they could have been considered back in the 1961 when the VCDR was adopted.

On the national level, the Snowden revelations have also positioned the topic of freedom of diplomatic communication within the debate on freedom of the press versus national security. The UK government requested *The Guardian* to stop publishing sensitive documents revealed by Snowden,[112] but did not initiate legal proceedings as it did in 1987 when a former British spy, Peter Wright, who moved to Australia, published the book *Spycatcher* explaining the communication surveillance of diplomatic missions in London. After *The Guardian* and *The Observer* started publishing his memoirs, the British government filed court proceedings requesting that the publication of the confidential documents to be stopped. The High Court accepted *The Guardian*'s arguments that it is in the public interest to expose surveillance of foreign missions as a breach of both international and British law.[113] The ruling of the British court was supported by the European Court of Justice.[114]

The legal obligation of a host State to restrain from surveillance of diplomatic communication is clearly stated by F. Seysterd:

> The receiving State must not attempt to become acquainted with the contents of the communications--and it must take all reasonable precautions to prevent others from doing so. Thus the receiving State does not have tile right to censor ordinary mail, or to open the diplomatic bag, or to listen in to telephones or private conversations, or to copy or decipher telegrams. *If it employs these practices in respect of its own citizens, it must make an exception for diplomatic communications*.[115]

4.3.3 Use of Wireless Facilities by Diplomatic Missions

Article 27(1) of the VCDR governs the right to use a wireless transmitter. It presents the main technology-related provision of the VCDR and was one of the most controversial aspects in the negotiation of the VCDR.[116] Technologically advanced countries argued for full freedom of the use of wireless communication by diplomatic missions.[117] Developing

[112] The prime minister has called on the Guardian and other newspapers to show 'social responsibility' in the reporting of the leaked NSA files, to avoid high court injunctions or the use of D-notices to prevent the publication of information that could damage national security. For more information see <http://www.theguardian.com/world/2013/oct/28/david-cameron-nsa-threat-newspapers-guardian-snowden>.

[113] BBC, 'Government loses Spycatcher battle' (13 October 1988) <http://news.bbc.co.uk/onthisday/hi/dates/stories/october/13/newsid_2532000/2532583.stm>.

[114] European Court of Justice, *Case of Observer and Guardian v. the United Kingdom*, Judgement, 26 November 1991 <http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57705>.

[115] F. Seyersted 'Diplomatic Freedom of Communication' *Scandinavian Studies in Law* (Stockholm: Almqvist & Wiksell International 1970) 193, 209 [emphasis added].

[116] Denza, *supra* note 99, 1998, p. 175

[117] Amendment by United Kingdom: UN Doc. A/Conf. 20/C 1/L 291.

countries proposed a formulation which would require consent of the receiving State and observation of national laws and international telecommunication regulations. [118] At that time, wireless communication related mainly to radio transmission. In arguing for restricted wireless communication, developing countries maintained that they needed the right to grant permission in order to implement the provisions of Article 6 of the *Constitution of the International Telecommunication Union* which specifies that the State has responsibility to ensure that any telecommunication originating from its territory does not cause 'harmful interference to the radio services of other countries.'[119] In Article 48, the ITU Constitution mentions only military radio installations as exceptions which do not require application of the ITU Constitution.[120] On this basis, developing countries argued that the ITU Constitution applies to diplomatic wireless facilities since they are not mentioned as an exception in the ITU Constitution. This argument prevailed in the negotiations and Article 27(1) of the VCDR specifies that '[…] the mission may install and use a wireless transmitter only with the consent of the receiving State.' There are two possible consequences of this stipulation for internet communication.

The first is related to the use of wireless facilities in diplomatic missions for the electronic surveillance of local communication in the capital of the host country, as it is reported to be done by the US, the UK, Australia and Canada in the capitals of Asian countries.[121] The Chinese MFA reacted to this allegation by requesting that 'foreign embassies in China and their staff respect the Vienna Convention.'[122] There are two potential breaches of the VCDR: of Article 27(1), stating that a wireless transmitter should be used only for the communication of diplomatic missions; and of Article 41 (1) and (3), endorsing the duty of the diplomatic mission to observe local law. As a first reaction, the affected countries might issue a diplomatic protest note. The next step may require a mix of legal and technical measures that should prevent future electronic surveillance (e.g. assurances, including possible inspection, that the embassies' equipment is used only for wireless communication with the capital). The possibility of more radical measures was indicated by Bhagevatula Satyanarayana Murty: 'If electronic surveillance seriously threatens the security of the receiving State, it is likely to demand the closure of the mission.'[123]

The second likely consequence is related to the rapid development of new wireless technologies which may provide diplomatic missions with new types of wireless

[118] Amendment by India on behalf of 14 developing countries: UN Doc. A/Conf. 20/C 1/L 165.

[119] Article 2 of the *Constitution of the International Telecommunication Union*.

[120] *Ibid*, Article 48.

[121] For more information see 'Australian ambassador summoned amid Asia US spying reports' BBC (1 November 2013) <http://www.bbc.co.uk/news/world-asia-24757968> accessed 09 November 2013.

[122] *Ibid*.

[123] B.S. Murty, *The International Law of Diplomacy: The Diplomatic Instrument and World Public Order* (Martinus Nijhoff 1989) p.506.

communication. These would require the permission of host countries for their use, even if they become more like digital commodities than like the complex technical facilities they were back in the 1960s when the VCDR was drafted. Additionally, giving international telecommunication regulations priority over diplomatic law (as was done in the negotiation of Article 27(1) of the VCDR) may be used in the future by States to reduce the freedom of diplomatic communication on the basis of enforcing telecommunication standards and regulations.

4.3.4 Inviolability of Databases and Electronic Documents

Preparing and managing diplomatic documents has been substantially affected by the internet. Diplomats draft documents using word processors and store them on hard disks or servers in a cloud. Diplomatic documents are transmitted over the internet. A lot of negotiation is done by drafting diplomatic documents with the use of track changes and annotations.

It is only a few decades since documents were produced by a much slower process, starting with hand-writing the first draft, typing the official version, and storing it in the archive. This is, for example, how documents were prepared when negotiators were drafting the VCDR. In spite of major changes in technology, however, the VCDR's provisions on the protection of diplomatic documents are still appropriate in the internet era.

Archives and documents, including electronic ones, enjoy the strongest protection by the VCDR, which states in Article 24 that '[t]he archives and documents of the mission shall be inviolable at any time and wherever they may be.' Even in the case when a mission premises loses its diplomatic status due to a severance of diplomatic relations, the archives and documents retain their inviolability without a time limitation. Such high protection was inspired by the importance of confidentiality with regard to the work of diplomatic services. The initial draft of Article 24, which referred only to 'archives', was amended by adding 'documents' in order to also cover less formal documents that do not form part of official archives, such as negotiating drafts, 'non papers' and memoranda in draft.[124] This wide interpretation of the concept of an archive was restated by the International Law Commission in its work on the *Convention on the Succession of States*, where an archive is defined as 'documentary material of whatever kind amassed and deliberately preserved by State institutions in the course of their activities'. The phrase 'of whatever kind' includes electronic documents and e-mail.

Additional protection for archives and documents is provided by Article 30 of the VCDR that extends the inviolability to correspondence and papers, even those that may

[124] The VCCR provides more precise definition of archives in Article 1(1): '[…] all papers, documents, correspondence, books, films, tapes and registers of the consular posts, together with the ciphers and codes, the card-indexes and any article of furniture intended for their protection or safe-keeping.'

be private. One justification for including all correspondence and papers into the scope of the provision was to reduce the temptation of a receiving State to search papers and classify them as private or official.

If strictly applied, the provisions of the VCDR provide diplomats with a wide protection of their documents. The wording of Article 24, protecting diplomatic archives and documents 'wherever they may be' also includes databases, electronic documents and emails stored in cloud servers and services such as GoogleDocs. The application of the existing VCDR regulations creates some practical challenges.

First, in order to provide necessary protection, internet companies would need to identify documents and messages as diplomatic ones (e.g. documents on GoogleDocs or messages on gmail servers). The VCDR, including *traveaux préparatoires*, does not provide useful solutions for the identification of diplomatic digital assets. During the negotiations of the VCDR, France and Italy proposed an amendment requiring that diplomatic documents outside the premises of the mission 'must be identified by visible official signs.'[125] The proposal was not accepted. Thus, diplomatic archives and documents found outside the mission enjoy immunity, even if they are not clearly marked or otherwise identifiable as diplomatic documents. This decision does not help to solve the question of the immunity of diplomatic digital assets saved on servers in a cloud. Most likely, a new rule will develop either through 'instant customary law' or explicit regulation, requiring some type of digital identification of diplomatic archives and documents (e.g. special registration, using dedicated diplomatic servers).

Second, questions arise with regard to the universality of diplomatic immunities. According to Article 24 of the VCDR 'the archives and documents of the mission shall be inviolable at any time and wherever they may be'. 'Wherever they may be' makes diplomatic privileges very virtual, and opens a potential responsibility for any government, including beyond the receiving country where the diplomat is based, to protect digital documents stored on cloud servers or in transit over a network under their jurisdiction. In 1961, when the VCDR was drafted, physical limitations to the movement of documents and archives existed: they had to be typed up and distributed. Since these physical limitations no longer exist, the principle of universality of diplomatic protection may need to be re-examined and, possibly, limited.[126]

Thirdly, the question arises as to what governments can do to ensure immunity for electronic documents and archives. In international law, legal action based on diplomatic or consular immunities cannot be taken against private companies, for example, Google or Facebook, which may be involved in the breach of e-immunity. Obligations in

[125] UN Doc. A/Conf. 20/C 1/L 149 (Amendment of France and Italy); A/Conf. 20/14, p. 49.

[126] J. Kurbalija, 'Do e-mail and e-documents have diplomatic protection?' *Diplo* (Geneva, 13 June 2013) <http://www.diplomacy.edu/blog/do-e-mail-and-e-documents-have-diplomatic-protection> accessed 09 November 2013.

international law exist between States. National governments have a responsibility to ensure that individuals and institutions under their jurisdiction comply with international law, namely the VCDR. Thus would, for example, the US government be responsible for ensuring that any email of any diplomat, stored on, for example, a gmail server, be protected according to diplomatic immunity rules? The search for the answer to this question should start with Article 29 of the VCDR which states that governments must take 'all appropriate steps' to ensure the protection of diplomats. The VCDR *traveaux préparatoires* can help in the interpretation of the phrase 'all appropriate steps'. Belgium proposed the formulation that receiving States should take 'all steps' in order to ensure protection of diplomatic missions and diplomats.[127] In challenging the Belgian proposal, the UK representative suggested that the formulation 'all steps' would 'impose an impossible task on receiving state'.[128] Respecting the spirit of the way Article 29 of the VCDR was drafted, 'all appropriate steps' for protection of diplomatic digital assets should involve steps that could be technically implemented by the receiving State. An important pre-condition will be to provide a way to identify diplomatic digital assets, in order to help internet companies provide the diplomatic protection specified by the VCDR. National governments should also ensure responsibility for natural and legal entities under their jurisdictions, including internet companies, in the case of a violation of the immunity of diplomatic digital assets.

4.3.5 Exemption from Custom Duties for E-Purchase

Article 36 of the VCDR deals with exemption from customs duties and inspection. It states that articles intended for the use of the diplomatic mission and for the personal use of a diplomatic agent (or members of their family) are exempt from all customs duties, taxes, and related charges. This exemption does not apply to charges for carriage, storage, and similar services. Furthermore, according to Denza, Article 36 puts the receiving State under an obligation to permit entry of those articles intended for diplomatic use.[129] This regulation applies to online purchases as well. However, an online purchase faces the same limitations as a regular purchase of objects that are prohibited under the domestic law of receiving State (e.g. certain online materials). In such cases, Article 41 of the VCDR applies, stating (and being the overruling obligation) that a diplomat has to respect the laws and regulations of the receiving State.

5. The Future of Diplomacy and Diplomatic Law in the Internet Era

This chapter addressed the question whether the internet has triggers 'just another evolutionary step' in the long history of diplomacy, or actual revolutionary changes in

[127] UN Doc. A/Conf. 20/C 1/L 214.

[128] A/Conf. 20/14, p. 160.

[129] Denza, *supra* note 99.

the way how, where and by whom diplomacy is performed. Some diplomatic functions, such as information gathering, already have been profoundly affected by the internet. Others, such as representation and negotiation, have been less affected. The internet has also started to affect the three core elements of the organisation of diplomacy and its professional culture: hierarchy, exclusivity, and secrecy. Diplomatic services are organised hierarchically, according to rank, starting from attachés and ending with ambassadors. Internet tools – based on sharing of, and easy access to, information – are increasingly challenging hierarchical work processes in diplomatic services. Exclusivity is one of the characteristics of diplomacy that can be traced back to its aristocratic origins. This feature of diplomacy could create tensions with the more open, and less formal, social ethos fostered by internet communication. The most profound and visible impact of the internet is on the secrecy of diplomatic services. The WikiLeaks release of diplomatic cables and recent Snowden revelation are the most visible examples of the need to maintain secrecy.

With regard to diplomatic law, in spite of the major technological changes over the last five decades, the 1961 VCDR, the core instrument of diplomatic law, has survived the test of time. It is one of the most observed international legal instruments. The main, internet-driven, challenges to the VCDR will be related to the provisions on information gathering and communication.

When the VCDR was drafted, information gathering and communication were two separate activities. Information was gathered, analysed, and stored in the MFA's archives. Communication was conducted in person and principally through the use of telephone and telegraph. This is why these functions are regulated separately in Article 23 (information, i.e. archives and documentation) and in Article 27 (communication, i.e. official correspondence). Today, an interplay and overlap between communication and information can be identified. By storing data on a server in a cloud, both communication (i.e. transmitting data over the internet) and saving it in a digital archive (namely in servers in a cloud) are interlinked. Ideally, a possible new provision would regulate in an integrated way both the communication and information aspects of digital activities.

The internet has also introduced new forms of communication among diplomats, as well as between diplomats and the public. For example, Twitter has become a usual practical tool in diplomatic activities. By using Twitter and the internet in general to communicate with institutions, individuals and receiving States, diplomats could be in breach of Article 41(2) of the VCDR which states: 'All official business with the receiving State entrusted to the mission by the sending State shall be conducted with or through the Ministry of Foreign Affairs of the receiving State or such other ministry as may be agreed.'

This provision is the one which could be deemed most obsolete. It was already superseded in the pre-internet era by diplomats communicating more directly with institutions and individuals in the receiving State.

Despite frequent requests to amend the VCDR, not only due to technological developments, but also to abuse of privileges and immunities, it is difficult to envision major changes to the treaty. The VCDR is ratified by nearly all States and is, in general, observed. It is one of the pillars of international law. The most likely scenario is that the VCDR will be adapted to internet-driven changes through a modern interpretation of the existing provisions. Another possible development might be the adoption of an ‘internet protocol’ augmenting the VCDR, which would provide both clarification of the use of existing rules in the internet arena and provisions for regulating new, internet-related issues, such as virtual representation or the immunities of diplomatic documents stored in a digital cloud.