DIPLOMATIE: REFRAMING SECRECY IN
THE AGE OF DIGITAL DIPLOMACY

A mini-thesis submitted in fulfilment of the requirements for the award of a
Master of Political Science at the University of the Western Cape, Bellville, South Africa
Presented to the Faculty of Economic and Management Science on the 10th of December 2015

by Victor A. Leray
under the supervision of Professor Jolien Pretorius
Declaration

I hereby declare that this research project is entirely my own work and appropriate credit has been given to the references of the work of others.

No part of this research should be reproduced without my consent.

Due to the high level of confidentiality required during the making of this research project, a personnel statement of ethics has been issued.

According to my strong personal convictions, I also want to stress that this mini-thesis has been created and written on a computer using free software only.

“Information is power. But like all power, there are those who want to keep it for themselves.”

Aaron Swartz
Acknowledgments

I would like to warmly thank

Professor Joelien Pretorius for her supervision,
Her Excellency Elisabeth Barbier, Ambassador of France to the Republic of South Africa,
Her Excellency Dolana Msimang, former Ambassador of the Republic of South Africa to France,
Christian Randrianampizafy, Director of the Alliance Française in Cape Town,
Xavier d’Argoeuves, Consul of France in Cape Town,
Eric Herrouin, former Deputy Consul of France in Cape Town,
Erica J. Barks-Ruggles, former Consul General of the United States of America in Cape Town,
Thomas Gomart, historian of International Relations,
Xavier de La Porte, journalist and writer

for their precious contribution to this work.
List of tables and diagrams

Figure 1. The 10 least Internet-connected countries in the world
Figure 2. The 10 most Internet-connected countries in the world
Figure 3. Global comparison over six countries
Figure 4. Facebook and Twitter in six countries (as of November 2015)
Figure 5. E-diplomatic influence of six countries (as of November 2015)
Figure 6. The Diplomatie principles
Figure 7. Screenshot of the early web version of Diplomatie
Figure 8. The specially-modified Samsung Android Tablet with “Cryptosmart” software
Table of Contents

Abstract ................................................................................................................................................ 7
Keywords .............................................................................................................................................. 8
Chapter 1 .............................................................................................................................................. 9
  1.1 Introduction ................................................................................................................................... 9
  1.2 Background and contextualization .............................................................................................. 10
  1.3 Statement of the problem ........................................................................................................... 12
  1.4 Aims and objectives ..................................................................................................................... 14
  1.5 Hypotheses and claims ................................................................................................................ 14
2. Theoretical and conceptual framework ......................................................................................... 15
3. Research methodology .................................................................................................................. 18
  3.1 Sampling ................................................................................................................................... 18
  3.2 Data collection ............................................................................................................................ 19
  3.3 Data analysis ............................................................................................................................ 20
4. Limitations of the study ................................................................................................................. 21
Chapter 2 – The era of digital diplomacy ........................................................................................... 22
  2.1 Early diplomacy and its evolution ................................................................................................ 22
  2.2 The emergence of digital diplomacy and the importance of the digital revolution ............... 27
  2.3 The practice of digital diplomacy................................................................................................. 31
    2.3.1 Adopting a digital diplomacy policy ...................................................................................... 31
    2.3.2 Digital diplomacy in practice ................................................................................................. 34
  2.4 The effects of the digital revolution on the conduct of foreign affairs ....................................... 39
    2.4.1 Transparency and communication ....................................................................................... 39
    2.4.2 Sovereignty ........................................................................................................................... 42
    2.4.3 Cyber-war .............................................................................................................................. 46
Chapter 3 – Secrecy in the era of digital diplomacy .......................................................................... 52
  3.1 Secrecy in diplomatic history ....................................................................................................... 52
  3.2 After WikiLeaks: new aims, new strategies ............................................................................... 56
  3.3 Information at the heart of diplomacy ........................................................................................ 60
  3.4 The impact of the increase of information flows around the globe ............................................ 61
  3.5 The necessary secrecy of diplomatic correspondence ............................................................... 63
  3.6 Public diplomacy and diplomacy of influence .......................................................................... 65
  3.7 Diplomacy confronted by the emergence of new networks ....................................................... 67
  3.8 A necessary democratic contract ............................................................................................... 68
Chapter 4 – Diplomatie: a case study ............................................................................................... 69
4.1 Building and restoring legitimacy ................................................................................................ 73
4.2 Diplomatie in action ..................................................................................................................... 77
   4.2.1 Connectivity .......................................................................................................................... 77
   4.2.2 Mobility ................................................................................................................................. 81
   4.2.3 Security .................................................................................................................................. 83
4.3 Critics ............................................................................................................................................ 88
4.4 Diplomatie and Africa’s progressive digitalization ........................................................................ 89
Chapter 5 – Conclusions ..................................................................................................................... 91
Abstract
The increasing importance of media, especially digital media in society has been studied widely, from identity formation to activist movements. In international relations, digital media studies have focused considerably on public digital diplomacy and social networks, sometimes neglecting a crucial step: the making, the processing and the transmission of the sacrosanct and secret diplomatic data. This study aims to explore how digital revolutions impact on the way diplomats communicate and share information. The dependent question will revolve around the notion of secrecy; the independent question will analyse secrecy in the era of digital diplomacy. A statistical database was built and semi-structured interviews with American, French and South African diplomats have been conducted. It aims to highlight three thematic fields. The first one looks into organization, legitimacy, sovereignty and governance issues raised by the emergence of new technologies. The second one looks into the redefinition of secrecy in our digital era. The third part is a case study that will investigate how software, open platforms and processing of computerized data redefine, modernize and legitimize the way diplomats work, share information and engage with the general public for the greater good. The main assumption is that public action will only be legitimate in society if – and only if – society recognizes the state as a true network actor.
Keywords

*Diplomatie* (online platform), Digital diplomacy, Open data, Going digital by default (concept), knowledge management, Information and Communications Technologies (ICT), Secrecy, Connectivity, Security, Legitimacy, Sovereignty, Governance, Citizen empowerment, Actor Network Theory (ANT).
Chapter 1

1.1 Introduction

In 2002, the United States Department of State created a task-force on what was called at the time “e-diplomacy”. Ten years later, American digital diplomacy is led by more than 200 federal employees in Washington, District of Columbia and more than 900 working in United States diplomatic missions across the globe, making the United States the unchallenged leader in the field. From a traditional diplomatic point of view, such a capacity assures this country of a durable worldwide influence. Digital revolution accelerates the diffusion of powers to all social actors, which long remained in the hands of states. Diplomats can hardly ignore this decentralized and new practice that affects their everyday work. Soon after the WikiLeaks scandal and Edward Snowden’s revelations from 2010 to 2015, people have become increasingly curious and sometimes even suspicious about what diplomats do, create, and – most of the time – do not share. Governments now have to face a growing appetite for this highly sovereign information. Embracing the digital openness is no longer a “nerdy” fantasy: it is now a matter of legitimacy, sovereignty and governance. In 2015, more than a billion people have a Facebook account and almost 800 million are connected on Twitter. This study aims to (re)define the notion of secrecy associated with traditional diplomacy and to help understand in a comprehensive way how new online resources can be used to modernize, improve and legitimize public action. With the above mentioned, this study hereby draws the assumption that public action will only be legitimate in society if – and only if – society recognizes the State as a network actor. This study adopts the constructivist Actor-Network Theory (ANT) as an explanatory structure of analysis. Actor-Network Theory combines both a sociological and technical approach in such a way that neither social nor technical positions are privileged. By being hypotheses-testing and analytical, this study employs both quantitative and qualitative data.
1.2 Background and contextualization

Digital diplomacy represents a complex and challenging new step in the art of diplomacy. Many scholars and journalists have called this move “Diplomacy 2.0”\(^1\) or “Networking diplomacy”.\(^2\) In 2013, former Chilean Ambassador Jorge Heine explained its principles:\(^3\) it is “a transition from a traditional diplomacy of clubs, rarely public and limited to a few governmental actors, to a multilateral diplomacy which involves an increased number of actors, mostly non-governmental, which is sometimes public and trying to increase exchanges between countries.” To understand this statement, it is crucial to raise two simultaneously and complementary aspects: the first one tends to consider that digital diplomacy is the continuation, an avatar of public diplomacy through new information and communication technologies. Indeed, an increasing number of states are using electronic tools and web-based services to communicate and interact worldwide with both national and foreign societies. This can be verified by the fact that a lot of diplomats have Facebook pages and Twitter accounts broadcasting a different diplomatic voice: Michael MacFaul, former United States Ambassador to Russia and Jon Benjamin, former Ambassador of the United Kingdom to Chile represent good examples of these “digital diplomats” who act as innovators out of the daily routine in their ministries, embassies, consulates, and international organizations.\(^4\) But this first definition has to be expanded dramatically to a second one as states are more and more challenged to accept critique coming from various social actors, who are claiming their rights to participate in the elaboration and the conduct of international affairs. In this meaning, digital diplomacy could be considered as the end of the states’ reserved area. This is the true revolution: such “exposed diplomacy” uses networks as a lever for the expansion of freedom around the world. New expressions and idioms like “open data” or “smart power” have become familiar. In 2014, the Ministry of Foreign Affairs of France launched a new internal platform called Diplomatie.\(^5\) By taking a giant leap forward in the way civil servants create and share information, French diplomats abandoned cables, unsafe emails and hand-written memos. Taking all these elements into consideration, this study also aims to (re)define the notion of secrecy and to help understand in a comprehensive way how new online resources can be used to modernize, improve and legitimize

\(^1\) Weisbrode, Kenneth (March 28 2010). Diplomacy 2.0. The Guardian
\(^2\) Heine, Jorge, Andrew F. Cooper, Ramesh Thakur (2013). The Oxford Handbook of Modern Diplomacy. United Kingdom, Oxford University Press
\(^3\) ibid
\(^4\) Rogin, Josh (January 13 2012). Meet the U.S. Ambassador to Russia, Michael McFaul. Foreign Policy
\(^5\) to be pronounced [diplomasi] according to the International Phonetic Alphabet
public action.
1.3 Statement of the problem

The recent spread of digital initiatives in foreign ministries is often argued to be nothing less than a revolution in the practice of international relations: because information is increasingly digital and most of what diplomats produce is in digital form, it is now possible to harness these previously isolated pieces of information using off the shelf as well as customized digital tools. Digital technology has also changed the ways firms conduct their business, how individuals conduct their social relations and how states conduct internal governance. Nevertheless, states are only just realizing their potential to change the ways all aspects of interstate interactions are conducted. In particular, the adoption of digital diplomacy (for example the use of social media for diplomatic purposes) has been implicated in changing practices of how diplomats engage in information management, public diplomacy, strategy planning, international negotiations or even crisis management. Despite these significant changes and the promise that digital diplomacy offers, little is known, from an analytical perspective, about how internal digital diplomacy really works.

The Internet opposes a set system of values. New trends and radical transformations are emerging due to numerous technical innovations, especially on social networks. They were made possible by the speed of data, new and improving storage capacities and spectacular cost reductions. While the United States remain the most advanced country in the field of digital diplomacy, other states like China or even Russia are also prominent on the World Wide Web. The Internet has destabilized many diplomats as its development was realized thanks to a system of multi-stakeholder rules including actors from civil society and corporations in the broad sense. They broke into the diplomatic sphere with a relative indifference, and many diplomats were sceptical pretending not to see the yearning of actors beyond the diplomatic sphere to directly affect the course of foreign policies. At the top of these emerging matters is the notion of secrecy. Jealously kept for centuries, diplomatic secrets are now at the heart of the WikiLeaks and Snowden affairs. For the first time in history, public opinion has the opportunity to access sensitive and classified information. The digital landscape has become a leaky place. And in it, government just cannot get away with what it used to. While governments’ bad behaviour has always been revealed eventually, it is easier than ever to reveal even peace-making government activities in the digital age, whole hog and in real time. Exposure in the digital landscape, for good or for ill, is simply more likely to occur today. In a quest for better safety, governments are becoming more secret. And secrecy is not just a practice, but a

6 Hanson, Fergus (2012). Revolution @State: the Spread of Ediplomacy. Lowy Institute
7 Please refer to the case study in Chapter 2
culture, an operational mode of being. The broad question of this thesis revolves around the notion of secrecy; the more specific question analyses secrecy in the era of digital diplomacy. The statement of the problem is therefore: how do diplomats deal with this information they create and share? What are the best tools to embrace the digital revolution in the field of foreign affairs? It is essential to start with the assumption that digital revolutions changed the way diplomats see and analyse our societies.
1.4 Aims and objectives

The study will be guided by the following aims:

1. To redefine the notion of secrecy in the digital age;
2. To analyse emerging norms in the fields of connectivity, security, sovereignty, governance and practice of digital diplomacy;
3. To anticipate major coming changes in the field of digital diplomacy;
4. To analyse how new communication tools redefine the diplomat's work.

1.5 Hypotheses and claims

The study makes the following claims:

1. Secrecy, in the digital era where information-sharing is an increasingly normal part of daily life, is no longer the norm;
2. Legitimacy, influence, sovereignty and governance are the four most crucial issues raised by the emergence of new technologies in the field of diplomacy and foreign policies;
3. In order to be efficient and to anticipate the main challenges of this digital era, diplomats must master and work with a set of three new values: security, mobility and connectivity;
4. Digital diplomacy modernizes and enhances the management of public diplomacy.
2. Theoretical and conceptual framework

This study clearly follows a constructivist approach, both in its methodology and its theory. According to Emanuel Adler, “constructivism occupies the middle ground between rationalist approaches (whether realist or liberal) and interpretive approaches (mainly postmodernist, poststructuralist and critical), and creates new areas for theoretical and empirical investigation.”\(^8\)

Constructivism seeks to understand the origins and the real meaning of international relations through sociological approaches neglected by neorealists and neoliberal institutionalists. It is nevertheless important to examine the neorealist approach when it comes to cyber-terrorism and security. According to James Adams, the Internet is “cyber-space has become a new international battlefield” where every state stands alone or with its alleged allies and desperately tries to build up its cyber strength and defences while fearing that every breakthrough made by another state poses a direct threat to their security. From the constructivist point of view, this analysis may appears as too restrictive. According to Adler, constructivism is not a theory like many others, but brings a social perspective in order to explore identities, norms and various interests in the field of international relations.\(^9\) The social construction of knowledge and social reality are the common ground of social constructivism.\(^10\) The very name “constructivism” calls for this fundamental notion of “reality-build” approach of international relations. Of course, constructivism is not limited to the study of international relations. Its main classical philosophical theorists were Emmanuel Kant (1724 – 1804), Ludwig Wittgenstein (1889 – 1951), sociologists like Max Weber (1864 – 1920), Georg Simmel (1858 – 1918) and Émile Durkheim (1858 – 1917). More recently, Jürgen Habermas’ ideas of “tech-nization of the lifeworld” implies that technology is neutral within its own sphere: the study will therefore draw from this assumption. As the Internet is a unique tool for sharing information, it is also a privileged medium that has developed a life of its own and an ever-evolving identity: the Internet must be viewed as having its own customs, defined by various social actors. These actors must come together to promote Internet’s continued development and ensure its safety, integrity, quality and openness. It is also important to understand that in many cases, the information spread online and the actions taken by many users are in some way affected by the culture and identity of the Internet, shaped not only by states, but also by international organizations and institutions, non-

---

\(^8\) Adler, Emanuel (September 1997). Seizing the Middle Ground: Constructivism in World Politics. European Journal of International Relations September, pp. 319-363


\(^10\) ibid
governmental organizations and even associations like WikiLeaks or private individuals like Edward Snowden.

Following this rationale, this study adopts the Actor-Network Theory (ANT) as an explanatory framework of analysis. It is sometimes specified as sociology of translation and is primarily connected with the work of French scholars Bruno Latour\textsuperscript{11}, Michael Callon\textsuperscript{12} and John Law.\textsuperscript{13} According to Law, the essential characteristic of Actor-Network Theory is the equitable analysis of human and nonhuman actors. They are esteemed as equal actors in networks which want to achieve a common purpose. Actor-Network Theory theorists regard both technology and society as a combined socio-technical system and that separating them then the approach becomes invalid. Actor-Network Theory “deals with the socio-technical by denying that purely technical or purely social relations are possible, and considers the world to be full of hybrid entities.”\textsuperscript{14} One of the main assumptions at the heart of the Actor-Network Theory – which is also shared with other constructivist approaches – is to consider that society does not provide a framework within which the actors move and act. In other words, society is always a temporary result of on-going actions. This methodology is reliable in a sense that it provides a meaningful context in which the participation of all the actors could be taken into account, as well as a theoretical explanation of the facts and cases that relate to the analysis of the Internet characteristics. It also allows theoretical deductions that connect the facts and cases in a rich way that produces and brings together coherent pieces of information. Actor-Network Theory is also referred to as enrolment theory where the interrelated roles of actors and their strategies are defined and negotiated.\textsuperscript{15} A regard that technical determinists argue that the development of technology follows its own logic and that the technology determines its use. Actor-Network Theory is appropriate to use for this study because it identifies and acknowledges the key human actors and non-human actors within an organization and the effect on the potential social issues that might occur. Actor-Network Theory is used to investigate issues in digital diplomacy process that incorporate human actors such as citizens and bureaucrats advancing their goals and policies, how the interaction between these actors affects

the digital diplomacy process, and identifies the factors that influence this same process.16
3. Research methodology

This study employs both exploratory and descriptive designs where the use of exploratory design was appropriate to understand – and in some situations, justify – the use of secrecy in a digital age, while descriptive research was used to determine the evolution of digital practices to provide comprehensive frequencies and help the reader to visualize these evolutions.

3.1 Sampling

The populations for this study consisted of American, French and South African high-ranked public officers and diplomats working for their respective Ministries of Foreign Affairs (or equivalent). Simple and stratified sampling were supposed to be employed to select the respondents in this study. Stratified sampling is used to ensure that the various entities in the population are well represented in the sample and to ensure accuracy. With simple random sampling, a random sample was selected such that every element in the population had an equal chance of being included into the sample and the respondents selected were each interviewed discretely. It quickly appeared that these methods were not the most appropriate nor the most convenient to respond to technical questions with such a small – and intentionally limited – sample. For this reason, only snowball sampling (also called chain-referral sampling) was employed as a non-probability sampling technique where existing study subjects “accidentally” recruit future subjects from among their social and/or professional acquaintances: “I’m going to refer you to [people], he (she) will know better.”

Being a part of a diplomatic structure was of a tremendous help in the making of this study. Being in direct contact with diplomats made the sample group growing just like a rolling snowball: as the sample builds up, enough data are gathered to be useful for research. This sampling technique is often used in hidden populations which are difficult for researchers to access, like high-profile officials and diplomats. Interviewees were selected for a good reason tied to purposes of research and with appropriate variability: these variables were quite obvious from the beginning. Snowball sampling also allows the researcher to make estimates about the social network connecting the hidden population. The use of memos, referring to the memoing practice inspired by Glaser and Strauss’s Grounded Theory was also very helpful. A special diary was updated after each interview indicating progressions, ideas, notes, sketches and perspectives necessary for to the

good conduct of the writing process.

3.2 Data collection

This study employed both quantitative and qualitative data. The mechanisms employed in data collection included interviews and an extensive use of existing information over the Internet. Official and trusted sources coming from the World Bank, International Monetary Fund, 2014 United States Central Intelligence Agency fact book were employed to build comprehensive and precise digital databases. Frequency tables, percentages and graphs were used to present the results. This information was tabulated and processed with the help of LibreOffice Calc (the free and open-source equivalent of Microsoft Excel) and Stata 13 for Linux.\textsuperscript{19} Stata is a proprietary general-purpose statistical software package created in 1985 used in the fields of economics, sociology and political science. Stata's capabilities include data management, statistical analysis, graphics, simulations, regression, and custom programming.

The sample was designed according to geographic convenience: most of the interviews were conducted in Cape Town, South Africa, while only two of them were conducted in France, at the South African Embassy in Paris. “One-to-one”, open-ended interviews were privileged and resulted in the collection of precious explanations, stories and anecdotes. As some questions were quite precise and needed a lot of input and pre-existing knowledge, only 18 questions were asked: all of them were answered. Discussions were not conducted in a classic way, but completely free: most interviews had no time limit and stopped when the topic was exhausted. Skype interviews were required only twice in order to ask additional questions to respondents. Email correspondence was negligible. The use of Twitter was also precious to contact Thomas Gomart, historian of International Relations and journalist Xavier de La Porte: these two personalities are usually not easy to reach due to their busy schedule. The use of Twitter for this research perfectly illustrated the new shortcuts that social media allow to take in the field of digital diplomacy.

\textsuperscript{19} Please refer to this mini-thesis' spreadsheet database
3.3 Data analysis

As previously mentioned, this study employed both quantitative and qualitative data. Quantitative and qualitative methodologies are not antithetic or divergent, rather they focus on the different dimensions of the same phenomenon. Sometimes, these dimensions may appear to be confluent. But even in these instances where they apparently diverge, the underlying unity may become visible on deeper penetration. This emphasis has developed with the growing attention focused on “triangulation” in research.\(^{20}\) Triangulation is the combination of methodologies in the study of the same phenomenon. The assumption is that the effectiveness of triangulation rests on the premise that the weaknesses in each single method would be compensated by the counter-balancing strengths of another. At the same time, possible weaknesses resulting from one method can easily be checked and “auto-balanced” by the second one. The making of databases contributed in a foundational way to personal knowledge, pushing for more questions and hypotheses. By analysing current trends on how 141 governments access and make use of Internet resources, it also provided a solid background from where questions and rationales were elaborated.\(^{21}\) Quantitative data were also essential to make the reader understand what digital diplomacy is by providing real-life examples illustrating this ongoing revolution. The processing and digestion of data contributed is crucial to measure variables such as countries using Twitter or Internet accessibility, to verify existent theories and hypotheses; it also was a very unique opportunity to question how governments make use of Internet and big data resources in order to better understand the dynamics under the use of various social media. As the research question is also underlying on the accumulation of living experiences from a large set of people, the use of qualitative data is complementary to collecting and analysing raw numbers: the established databases had to be explained and detailed with the help of respondents’ testimonials and beliefs.


\(^{21}\) Please refer to this mini-thesis' spreadsheet database in Chapter 2
4. Limitations of the study

The main limitation of this study was primarily to collect raw data in order to establish a strong and reliable database on the use of digital technologies in diplomacy around the world. Most of these data are hidden, or owned by private corporations such as Twitter, Facebook, Google or commercial-orientated databases. Many web activity reports are available; nevertheless, these files and databases are not considered as open-data, and are not free to obtain. There is an obvious lack of structured and free and accessible data in the field of digital diplomacy. Consequently, the use of several sources, sometimes more than a dozen, was required to build a database. Thanks to several media online applications,²² it was possible to gather and analyse these data in a comprehensive way: again, triangulation played an essential role in bringing these bits of information together. The second limitation of this study comes from the participants themselves. A few diplomats were interviewed, and the majority of them were above the age of fifty. It was sometimes difficult for them to express a clear impression or even to seize the real problems brought on by digital diplomacy. Some of the respondents had little information hence giving out data which was not satisfactory and needed more input: here again, the use of triangulation was more than necessary.

Chapter 2 – The era of digital diplomacy

The Internet has been one of the crucial drivers for modern diplomacy and its use, advantages, disadvantages, weaknesses and upheavals in the inside world of digital diplomacy will therefore be discussed in this second chapter.

2.1 Early diplomacy and its evolution

“Diplomacy is a way to set and achieve foreign policy goals. In this respect, the basic tasks of diplomats have been to provide information and to negotiate.”23 From an historical perspective, diplomacy also relies on the clear delimitation of an inner circle: “Diplomacy is a collective exercise but is accessible only to those who embody or represent sovereignty”.24 One of the most typical characteristics of diplomacy is the production of a very particular political disquisition that is not elaborated or aimed to be public, shared or even disclosed.25 Due to the digital explosion of information and communication technologies, and more especially after the WikiLeaks case in 2010,26 this “exclusive relationship” was torn apart once and for all.27 From the realist perspective, diplomacy is the science of relations between states, regarding their respective interests and their common abidance to international law, treaties and conventions.28 Knowing these rules ensures the appropriate conduct of political negotiations. To be more precise, diplomacy is the science of relations, or in a simpler way, the art of negotiations – the art to command, to lead and to follow all political negotiations with an appropriate amount of culture and knowledge. Modern diplomacy starts from the Middle Age, when it became a real science in the hands of specialists, mainly priests and bishops. When negotiations became too intense or too technical, special delegates, ministries or ambassadors were sent to undertake the parleying. Diplomacy’s main goal is to ensure happiness, harmony and cordial cooperation of the people, while at the same time providing security, peace and dignity for all.29 Diplomatic agents’ main goal is to lead negotiations in respect of these

23 Christodoulides, Nikos (2005). The Internet and Diplomacy. American Diplomacy
26 WikiLeaks' official website: https://wikileaks.org
28 Definition given by Oxford English Dictionary, 2014
29 ibid
principles, and to safeguard the application of treaties and all conventions in order to prevent any infringement to these laws that could endanger citizens. In this regard, diplomacy is considered as a science, but cannot be liable to strict rules: its customs are loose and therefore have to be very well known by all diplomats. These customs notably include the art of writing notes, cables, acts of correspondence and communications between governments, cultural, economic or even military codes and agreements. According to the very nature and gravity of the possible complications resulting from international tensions, diplomatic affairs can lead to heart-to-heart negotiations, still in an inner circle, far from the press and the general opinion. The best incarnation of this very restricted club could be found in the five permanent members of the United Nations Security Council, which are China, France, Russia, United Kingdom and the United States of America.30

It is very important to make a clear distinction between diplomacy, foreign policy and international relations. While foreign policy is a plan of action adopted by one nation in regards to its diplomatic dealings with other countries and is established as a systemic way to deal with issues that may arise with other countries, diplomacy can be considered as a major tool to promote and effect a country’s foreign policy to other countries or groups of countries. International relations describe the relationship and interaction between these countries. Diplomatic missions are generally classified into two main types: embassies and consulates, each intending to fulfil a set of political, cultural and administrative missions.

Remaining the most important codified legislation pertaining to diplomacy, article 3 of the Vienna Convention on Diplomatic Relations of 1961 describes the role of an embassy as follows: “The functions of a diplomatic mission consist, inter alia, in representing the sending State in the receiving State; protecting in the receiving State the interests of the sending State and of its nationals, within the limits permitted by international law; negotiating with the Government of the receiving State; ascertaining by all lawful means conditions and developments in the receiving State, and reporting thereon to the Government of the sending State; promoting friendly relations between the sending State and the receiving State, and developing their economic, cultural and scientific relations.”31

Although the Vienna Convention was finalized in 1961, way before the late 20th century’s information revolution, every single one of these six dispositions can be seen through the lens of digital diplomacy and apply to our digital world, thanks to the wide definitions they provide.

The second type of diplomatic mission is called a consulate. The main aim of a consulate is also to
represent a home country in a host country. A consulate is established primarily to provide a service to citizens and support the bilateral relation development focusing particularly on trade. The consul is the representative of the citizens living in the host country: his mission is therefore very different from the ambassador’s. The impact of digital diplomacy on diplomatic missions has also resulted in the creation of virtual diplomatic missions.32

Diplomatic representations are usually accessible via the Internet. For many of them, it is possible to interact directly with the diplomatic or consular personnel. South Africa’s most strategic missions are located in Beijing, Berlin, Buenos Aires, Canberra, Lagos, London, New York and Paris: some of these embassies operate their own websites with little coordination with the Department of International Relations and Cooperation located in Pretoria. They adopt their own layout, colours, content and URL address.33

In the case of France, the United Kingdom and the United States of America, all websites are connected via the same platform operated by the Department of State or the relevant Ministry of Foreign Affairs. Each embassy has a dedicated website, directly accessible from the main website. The layout, the colours, the content and URL address are unified.

In this regard, the constructivist point of view is easily identifiable: representation’s “digitalization” is being expressed and displayed according to a set of identities and specific values.

The table below shows a few examples of diplomatic missions' websites.

<table>
<thead>
<tr>
<th>Embassy's location</th>
<th>South Africa</th>
<th>France</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beijing</td>
<td>none</td>
<td>ambafrance-cn.org</td>
</tr>
<tr>
<td>Berlin</td>
<td><a href="http://www.suedafrika.org">www.suedafrika.org</a></td>
<td>ambafrance-de.org</td>
</tr>
<tr>
<td>Ottawa</td>
<td><a href="http://www.southafrica-canada.ca">www.southafrica-canada.ca</a></td>
<td>ambafrance-ca.org</td>
</tr>
<tr>
<td>Washington D.C.</td>
<td><a href="http://www.saembassy.org">www.saembassy.org</a></td>
<td>ambafrance-us.org</td>
</tr>
</tbody>
</table>

This is precisely where digital diplomacy meets public diplomacy: questions of visibility and representation on the World Wide Web are now crucial. The digital age has therefore allowed

32 Virtual Embassy of the United States Tehran, Iran. www.iran.usembassy.gov
diplomatic missions to extend their representation and influence to the Internet in order to target and service the Internet community. Although virtual diplomatic missions may be virtual representations of their physical counterparts, statements issued through virtual diplomatic missions are not legally binding to the same effect as the ones issued from traditional diplomatic missions. Statements and other information posted on the Internet by diplomatic missions carry the same bearing as real life embassies and consulates in order to ensure greater consistency with functions carried out in a more traditional way. Certain virtual diplomatic missions sometimes broadcast “less official” messages like personal opinions, pictures and videos using social media like Facebook, Twitter, Instagram, etc.

As the number of Internet users is becoming more important, the use of Internet platforms is also a good way to maintain a strong link between the home country and its citizens living abroad. Missions’ websites are therefore used to access a whole range of online services and information: it is possible to book an appointment to renew a passport or an identification card, a driving license, declare an emergency, inquire about a fiscal procedure, plan a journey abroad, or vote. Some visas application can even be submitted and approved online, without any other administrative formality. In this domain, the Kenyan e-government is an excellent example of the African’s emerging digital transition. This digitalization greatly simplifies the political and consular work by removing certain tasks from the physical consulate or embassy.

The information revolution has also demanded that diplomatic missions protect the interests of their country in the online world. In dangerous areas, many views and opinions are available in a very short lap of time: the role of the diplomatic mission is to deal with this amount of information and to clarify the situation if needed to avoid a crisis.

The digital revolution also impacted the way bilateral negotiations are carried out. Open forums, chat sessions, online polls and referendums have emerged as excellent ways to perform certain groundwork in the area of negotiation.

The information revolution also has a growing impact on the function of bilateral relation development in its various forms of politics, commerce, economy and cultural relations. It has now become relatively easy to provide online information to help investors and foreign businesses to consider investing in the home country. The Business France online platform opened in 2014: its aims is to advise on entrepreneurial initiatives for French and non-French businesses and to develop

34 Wankiku, Rebecca (September 9 2014). Kenya increases e-government efforts, burnishing international image. ITWorld
foreign investments.\textsuperscript{35} The cultural branch of the French diplomacy also enjoys a good online reputation: French Institutes (Instituts Français) and Alliances Françaises also rely on an extensive network of e-learning platforms to promote French language abroad. This presence is more than crucial in non-French speaking African countries.

Speed and security are also playing a major role in the exchange of information process. While the Vienna Convention on Diplomatic Relations only refers to diplomatic bags and to the protection of diplomatic correspondence, new challenges are yet to come with the increasing digitalization of diplomatic communication. In order for diplomats to provide information, it must first be collected and carried. Diplomacy therefore heavily relies on various methods of communication, and any technological upheaval is undoubtedly leaving its mark on the evolution of foreign affairs. When the telegraph was first invented, the world of diplomacy went through a revolution in the sense that diplomats could send and get any information in a matter of minutes at a cheap cost. Organized postal service, mail steamers and telegraph successively led to major changes in the way diplomats communicate. The telephone revolutionized the world of communications, as instant voice dialogue had become possible. From the late 1960s till today, the Internet opens the doors on a second world where almost everything is possible. This tremendous progress had and still has a considerable impact on diplomacy. This change has also brought the need to revise foreign policies in order for countries to keep in line with the evolution of international relations, but also to deal with critical issues such as sovereignty, security and cyber-crime over this revolutionary, sometimes hostile, perpetually changing and non-physical new territory.

2.2 The emergence of digital diplomacy and the importance of the digital revolution

The nature of international relations has been forced to change in order to cater for the removal of speed and distance barriers involved in the general diplomatic process. At times, this may disrupt the well-established and complex way in which diplomatic parties react with one another. According to Richard Solomon, President of the United States Institute of Peace and former United States foreign service officer, “Information about breaking international crises that once took hours or days for government officials and media to disseminate is now being relayed real-time to the world not only via radio and television, but over the Internet as well. Ironically though, for policy-makers, instant dissemination of information about events both far and near is proving to be as much a bane as a bounty.”

Thanks to the information revolution, questions about foreign policy are now part of the larger, lively discussion of what digital diplomacy really is. At its broadest, digital diplomacy signifies the altered diplomacy associated with the emergence of a networked globe. At its narrowest, it comprises the decision-making coordination, communication and practice of foreign affairs as they are conducted with the aid of information and telecommunications in the wake of the changes brought about by the computer and telecommunications industries. The information revolution however, has not unfolded in a vacuum. Instead, it has taken place alongside secular processes and events such as globalization. The convergence of small, mobile and powerful communications technologies around the Internet is one obvious source of change, but there are several other important aspects of these broad transformations.

According to French international relations specialist Thomas Gomart, it is important to consider that digital diplomacy is the continuation, an avatar of public diplomacy through new information and communication technologies. According to Hans N. Tuch, author of “Communicating with the World”, public diplomacy is defined as “official government efforts to shape the communications environment overseas in which American foreign policy is played out, in order to reduce the degree to which misperceptions and misunderstandings complicate relations between the U.S. and other nations.” From a constructivist point of view, the foreign policy process has expanded beyond the realm of governments to include the media, multinational corporations, non-governmental organizations and faith-based organizations as active participants in the field.

---

37 Gomart, Thomas (2013). De la diplomatie numérique. Revue des Deux Mondes
number of states are using electronic tools and web-based services to communicate and interact worldwide with foreign societies. Historically, digital diplomacy finds its roots in the digital revolution, also known as the third industrial revolution. It consists in the change from analog, mechanical, and electronic technology to digital technology which began anywhere from the late 1950s to the late 1970s with the adoption and proliferation of digital computers and digital record keeping that continues to the present day.

It is necessary to develop this assumption from a more technical and historical perspective. During the past decades, the world has witnessed what is probably the biggest ever man-made invention: the digital computer, which enables mankind to delegate tasks to a machine that will perform humanly impossible processes. The formal invention of the microprocessor by Intel Corporation in 1971 impacted a wide number of areas; today, a large number of devices such as mobile phones, cars, watches and even fridges possess a computing unit. Information is stored in a binary digital format that has various advantages: by that mean, information can be sent to various recipients and be accessed by virtually anyone with the appropriate permissions and resources. Networked computers complement the properties of digitally stored information in order to allow the transmission of information at an increasingly fast pace through private networks (with limited access) or public networks, such as the Internet. Although the conception of the Internet dates back to the 1960s, it was only until the 1990s that the Internet gained popularity, slowly leading to the information revolution. The main pillar of the fifth information revolution was the World Wide Web, created by European Organization for Nuclear Research (commonly known as CERN). The enabling of text and pictures to be transmitted simultaneously via the Internet was an unprecedented achievement which had the potential to attract the attention of businesses and the general public. Through its system of hypertext, information went more and more decentralized and wireless; new communication tools have allowed a free flow of content and information to circulate all around the globe: nothing has given an idea more potential to spread and develop a life of its own than the Internet. As a result and for the greater good, information is no longer limited to privileged government officials but is also accessible by the general public: this has led governments to lose the monopoly over information they once enjoyed through “traditional state-owned media” like public television channels or newspapers.

For this reason, and according to constructivists, the digital revolution has practically turned

information into a source of national power and influence. International power is now determined in terms of accessibility to the world’s communication infrastructure and the dominance of countries with regards to technology.\footnote{Martin, Todd (February 2 2001). Virtual Diplomacy. Canada: A Student Journal of International Affairs, Volume 2} Traditional military and financial powers are being replaced by soft power. With its emphasis on information and knowledge, the new communications environment is making soft power more practical. Indeed, the digital revolution holds the key to soft power, making it possible to appeal directly to a multitude of actors. However, some scholars such as Harold Innis and Marshall McLuhan challenged the idea that communications would lead to a democratic diffusion of power.\footnote{Innis, Harold (1952). The Strategy of Culture. University of Toronto Press} Innis saw what he called the “tragedy of modern culture” as the influence of the electronic media in undermining space and time in the interests of commercial and political power. McLuhan took a similar sceptical view of the new electronic age. He was a pragmatic realist who recognized the threat as well as the promise of new technologies. He pointed out that a global network could lead to a new tribalism, hindering rather than helping the open exchange of information and the mediation of human difference.\footnote{Dizard, P. (2001). Digital Diplomacy: U.S. Foreign Policy in the Information Age, Praeger Publishers, USA.pp.182-185} These phenomena can be seen through countries such as Russia and China. Russia presents a mixed picture at the turn of the century with censored opposition press, open internet networks and street-corner freedom of speech. The most powerful media instruments, television and radio, are largely manipulated by government and corporate interests. China represents a more intriguing patter. Official controls over information flow remain largely in place. However, the communist leadership faces an uncomfortable dilemma in reconciling strict censorship with the need to upgrade the national communications network in ways that match the demands of an expanding economy. It is interesting to note that as of October 2014, China ranks first in the world by the number of mobile phones in use.\footnote{"Mobile phone users in China October 2014". Statista. October 2014} In the process, the country’s leaders are more than likely to lose control over their ability to manage information, an essential element in maintaining their grip on political power.\footnote{Madanmohan Rao (1999). Internet Governance: The struggle over political economy of cyber-space, p.9} According to the determinist view, military security is an area where digital diplomacy will play a more active role in the coming years. The defence department in the United States has moved steadily to integrate advanced information technologies as central elements in its operational plans. The computer chip and digital systems for ground combat are as radical and important as the machine gun in World War I. The result has been
the emergence of a new strategic doctrine, called the revolution in Military Affairs. The realist scholars seem to rest on the notion that open information flow faces many challenges in the new century. That until now, resources have largely benefited powerful interests, particularly governments and corporations. These institutions have had the money and the will to take advantage of electronic resources for their own purposes. As a result, they are primarily responsible for creating and exploiting the present basic (backbone) network at home and abroad. This backbone facility is now being widened and its purposes transformed as it reaches out to mass audiences through a web of smaller networks. The network is extending, at various speeds into other societies. Moreover, its capabilities reach far beyond telephone services to include a full range of information services that can be plugged into a digital circuit. This changeover has brought astonishing growth of the internet. From small origins as a data network, it is now a multimedia resource, available to hundreds of millions of users worldwide. For realists, these changes are creating conditions for an unprecedented event in human history. It is the prospect of an electronic network that will allow everyone on earth to communicate with one another. Realists argue that there is still no clear defined view of the medium range impacts of this change. Even though both realists and idealist differ on the impact of information flow through digital technology, it is clear that it enhances public diplomacy especially through social media. Social media has become an important strategic asset and an effective means of strategic communication for increased international and domestic public opinion. Digital government generally involves using information and communication technologies to transform both back-end and front-end government processes and provides services, information and knowledge to all government customers like businesses, the general public, government employees and other government agencies. Digital government uses a range of information technologies, such as the Wide Area Networks, Internet, and mobile computing to transform government operations in order to improve effectiveness, efficiency, service delivery and to promote democracy.

2.3 The practice of digital diplomacy

The practice of digital diplomacy can be observed at multiple levels. Its main feature is to connect different actors by combining local speeches and global approaches. Starting from a state level, digital diplomacy is often presented as an avatar of public diplomacy, or in other words, as a means to establish a direct contact with citizens using social networks to implement strategies of influence. A difference persists between the official discourse and practice.

2.3.1 Adopting a digital diplomacy policy

The emphasis by the Obama administration on digital diplomacy is rooted in the concept of smart power initially to regain the moral authority lost by the United States during the Bush administration years.\(^{48}\) It is defined by the Centre for Strategic and International Studies as “an approach that underscores the necessity of a strong military, but also invests heavily in alliances, partnerships, and institutions of all levels to expand American influence and establish legitimacy of American action.”\(^{49}\) According to former Assistant Secretary of State for African Affairs Chester A. Crocker, smart power “involves the strategic use of diplomacy, persuasion, capacity building, and the projection of power and influence in ways that are cost-effective and have political and social legitimacy” — essentially the engagement of both military force and all forms of diplomacy.\(^{50}\) To be implemented, this smart power is based on the principle of connectivity and its ability to generate connections: it imposes its agenda by promoting adherence.\(^{51}\) For Washington, it was positioned “as an information and ideological hub”\(^{52}\) and use of digital diplomacy to serve “a global media empire”\(^{53}\), able to not only shape world opinion but especially to define new objectives. American digital diplomacy claims to support efforts of “democratization” throughout the world and made Internet freedom a priority, especially in its relation to China. In May 2009, Hillary Clinton presented a program – 21st Century Statecraft\(^{54}\) – which emphasized the need to go beyond the traditional state-to-state diplomatic framework to establish, with the help of connectivity, a more direct

---

\(^{48}\) Nossel, Suzanne (April 12 2012). Smart Power. Foreign Affairs


\(^{51}\) Slaughter, Anne-Marie (January-February 2009). America’s edge : Power in the networked century, Foreign Affairs

\(^{52}\) Nocetti, Julien (May 2011). La diplomatie d’Obama à l’épreuve du Web 2.0, Politique étrangère

\(^{53}\) Hanson, Fergus (March 2012). Revolution @State: The spread of e-diplomacy, Lowy Institute for International Policy

\(^{54}\) Freedom on the Net: A Global Assessment of Internet and Digital Media (Freedom House Publication)
relationship from state to individuals. In January 2010, she delivered a founding speech on Internet freedom, which advocated the abolition of digital borders and denounced the risks of a rising iron curtain on information.\textsuperscript{55} In the name of free speech and freedom to assembly, governments should not prevent people from connecting. These rights are the very foundation of the United States, which supports the skeleton of American democracy as Tocqueville noted: “the legislature will never attack these principles without attacking society itself”.\textsuperscript{56} In many ways, the Internet is both the ambivalent product of the American political culture and the expression of its imperialist tradition. This leads the American diplomacy to position itself on the Internet as a symbol in order to oppose authoritarian emerging powers like China or Russia. According to Marc Hecker, this position is reminiscent of a Cold War rhetoric and disguised violence used by Washington against Moscow.\textsuperscript{57} Concurrently, digital diplomacy aims to defend the huge economic and commercial American interests and contributes to maintain its military supremacy. There is no doubt that the global domination of the digital world represents a strategic dimension in the ideological, political, economic, cultural and societal leadership established by the United States over the world. Shortly after the United States and Canada (who did pioneering institutionalisation of digital networks within their foreign ministry before the turn of the 21\textsuperscript{st} century), the United Kingdom entered in the field of digital diplomacy, which has led some scholars to present the British digital diplomacy strategy as a new avatar of the Royal Navy over the Internet.\textsuperscript{58} The Foreign and Commonwealth Office defines digital diplomacy as a continuation of traditional diplomacy through a whole set of new media:\textsuperscript{59} Internet is seen as a medium to solve international problems in a remote way. The official line on this subject brings a clear and pragmatic approach of the question, by illustrating brilliant and concrete achievements in the field.\textsuperscript{60} Internet is clearly presented as an opportunity to intensify the influence of British diplomacy through four types of action: listen, publish, promote discussion and evaluate.\textsuperscript{61} In France, digital diplomacy did not benefited of the same resources. In May 2010, former French Ministry of Foreign Affairs Bernard Kouchner positioned himself on the ground support to dissidents, victims of censorship or repression of authoritarian regimes.\textsuperscript{62} The

\textsuperscript{55} Secretary Clinton To Deliver Remarks on Internet Freedom on Thursday, January 21st 2010
\textsuperscript{56} De Tocqueville, Alexis (1835). De la démocratie en Amérique, deuxième partie, chapitre IV, De l’association politique aux États-Unis. Presses de France
\textsuperscript{57} Rid, Thomas and Hecker, Marc (2009). War 2.0: Irregular Warfare in the Information Age. Westport, Praeger
\textsuperscript{58} Manor, Ilan (November 9 2014). Cyber Armies: Are Militaries Now Part of Digital Diplomacy? Digdipblog.com
\textsuperscript{59} Hughes, Stuart (May 24 2013). Digital diplomacy: here to stay and worth the risk? BBC Blogs
\textsuperscript{60} Digital Diplomacy – The FCO’s digital strategy: http://blogs.fco.gov.uk/digitaldiplomacy/digital-strategy
\textsuperscript{61} “What is digital diplomacy?”, http://digitaldiplomacy.fco.gov.uk/en/about/digital-diplomacy
\textsuperscript{62} Renard, Hervé (May 10 2010). Bernard Kouchner, défenseur d’un “Internet universel et ouvert”. Le Nouvel
influence of the French Ministry of Foreign Affairs on this issue quickly weakened. In May 2011, former French president Nicolas Sarkozy presided over the first eG8 with the ambition to “civilize the Internet.”  

63 This public announcement was not acted on and ultimately reflects a narrow conception of the international system and its dynamics. 64 Diplomatic personalities also promoted the use of digital practices. This is also the case of Carl Bildt, former Minister of Foreign Affairs of Sweden (more than 160 000 subscribers on Twitter) or Michael McFaul, former United States Ambassador to Russia (more than 36 000 subscribers on Twitter). Examples could be multiplied, but Carl Bildt and Michael McFaul are good examples of “the art of tweeting”, who understood how perfectly integrated social networks can combine official positions and personal opinions. Social networks allow the spectacular advent of personalities from outside the diplomatic sphere. This is obviously the case of Wael Ghonim (more than seven hundred and fifty thousand subscribers on Twitter), a cyber-dissident who was the symbol of the Egyptian revolution of 2011. After being elected one of the most influential people in the world by the Time Magazine in 2011, he was hired by Google and now works in California.  

65 Various initiatives already exist to map and measure the influence of e-diplomacy in the world. The digital channel “Twitplomacy” by the Burson-Marsteller agency follows the numerical relationships between international leaders; 66 but maybe the most powerful web application in the field remains the Agence France-Presse “E-diplomacy hub” which seeks to measure the real-time impact of Twitter on bilateral exchanges. 67 Thanks to this precious tool, it was possible to build comprehensive databases to understand how countries and diplomats make use of digital technologies.

---

63 Solon, Olivia (January 7 2011). Does the Internet need to be civilized? Wired Magazine
64 Lamothe, Patrice and Gomart, Thomas (June 7 2011). Internet n’a pas à être “civilisé”. Le Monde
2.3.2 Digital diplomacy in practice

In order to put words on the ongoing digital revolution, it seemed quite essential to use a quantitative approach by using compiled databases. A few countries were selected in order to compare and rate their digital diplomacy capacities. They were selected according to their active Internet population, access to the World Wide Web and for their geographical situations. The first database aims to highlight disparities of digital diplomacy’s repartition in the world and was conducted among 141 countries. The main goal is to study the rate of Internet penetration among a given country but also to assess the digital divide’s impact on diplomacy. While European countries are clearly the most connected countries in the world, mainly African sub-Saharan countries stay on the edge of the digital revolution, creating a digital divide. The United Kingdom remarkably stands out with the most important number of Twitter-connected embassies; both of these tables also show the overwhelming importance of cell phones in modern communications, putting the accent on mobility.

<table>
<thead>
<tr>
<th>country</th>
<th>population</th>
<th>twitter</th>
<th>Internet</th>
<th>mobile</th>
<th>embassies</th>
<th>region</th>
</tr>
</thead>
<tbody>
<tr>
<td>Burkina Faso</td>
<td>16,468,000</td>
<td>1</td>
<td>35</td>
<td>0</td>
<td>0</td>
<td>Africa</td>
</tr>
<tr>
<td>Cambodia</td>
<td>14,139,000</td>
<td>1</td>
<td>58</td>
<td>0</td>
<td>0</td>
<td>Asia</td>
</tr>
<tr>
<td>Congo, Dem. Rep.</td>
<td>65,965,000</td>
<td>1</td>
<td>17</td>
<td>1</td>
<td>0</td>
<td>Africa</td>
</tr>
<tr>
<td>Ethiopia</td>
<td>82,950,000</td>
<td>1</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>Africa</td>
</tr>
<tr>
<td>Iraq</td>
<td>32,031,000</td>
<td>2</td>
<td>75</td>
<td>2</td>
<td>0</td>
<td>Asia</td>
</tr>
<tr>
<td>Malawi</td>
<td>14,901,000</td>
<td>2</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>Africa</td>
</tr>
<tr>
<td>Benin</td>
<td>8,850,000</td>
<td>3</td>
<td>80</td>
<td>0</td>
<td>0</td>
<td>Africa</td>
</tr>
<tr>
<td>Côte d’Ivoire</td>
<td>19,738,000</td>
<td>3</td>
<td>76</td>
<td>0</td>
<td>0</td>
<td>Africa</td>
</tr>
<tr>
<td>Mali</td>
<td>15,370,000</td>
<td>3</td>
<td>48</td>
<td>0</td>
<td>0</td>
<td>Africa</td>
</tr>
<tr>
<td>Mauritania</td>
<td>3,460,000</td>
<td>3</td>
<td>79</td>
<td>0</td>
<td>0</td>
<td>Africa</td>
</tr>
</tbody>
</table>

Figure 1. The 10 least Internet-connected countries in the world, listed by country, population, number of twitter users, Internet connections per 100 people, cell phone connections per 100 people, number of Twitter-connected embassies and region of the world (as of November 2015).
Figure 2. The 10 most Internet-connected countries in the world, listed by country, population, number of twitter users, Internet connections per 100 people, cell phone connections per 100 people, number of Twitter-connected embassies and region of the world (as of November 2015).

The second database aims to compare digital strategies over six different countries, including Brazil, China (replaced by Turkey on figures 4 and 5), France, South Africa, United Kingdom and the United States of America. It also provides a comprehensive understanding of the key role played by multinational corporations like Facebook and Twitter in the field of digital diplomacy.
As presented above in this bar chart, the United States still widely dominate both in term of physical diplomatic missions abroad, but also on the Internet. Despite having fewer physical representations than France, United Kingdom is more likely to expand and develop its virtual network. As China slowly opens its door to western companies like Twitter, its number of digital representations is growing rapidly. Brazil and South Africa are also on their way, aiming to rely on their extensive diplomatic network to develop their influence on the World Wide Web and social networks.
The case study of China was not very relevant as this country is still using its closed networks like Weibo: Facebook is a banned website under official government's censorship program. For this reason, the role of Turkey, another major digital diplomacy player was analysed. Once again, the United States of America clearly dominate this ranking by imposing their own technologies. If Turkey stays as the second most influential digital diplomatic country on the Internet (see figure 5), Brazil is ranked second for its extensive use of social media.

### Figure 4. Facebook and Twitter in six countries (as of November 2015).
E-diplomatic influence is here calculated on the basis of composite index of officials and experts databases. Not surprisingly, the United States still rank as the number one in the field, followed by Turkey. The above figure needs to be understood as a momentary capture: Internet trends are known not to be stable.

<table>
<thead>
<tr>
<th>country</th>
<th>influence</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>1</td>
</tr>
<tr>
<td>Turkey</td>
<td>2</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>10</td>
</tr>
<tr>
<td>Brazil</td>
<td>16</td>
</tr>
<tr>
<td>France</td>
<td>26</td>
</tr>
<tr>
<td>South Africa</td>
<td>41</td>
</tr>
</tbody>
</table>

Figure 5. E-diplomatic influence of six countries (as of November 2015).
2.4 The effects of the digital revolution on the conduct of foreign affairs

Due to the digital revolution, new issues recently emerged. Among them are transparency, sovereignty and cyber-war.

2.4.1 Transparency and communication

Transparency is required in both official foreign relations and when dealing with public and private sectors: as most governments now have the technological means to implement more transparency, diplomats are not exempt of participating in this new information revolution: more than ever, they must take into account and listen to public opinion and justify their actions, as the general public has acquired the freedom to exert pressure on governmental decisions, particularly in those involving international commitments or national interests. The involvement of non-state actors such as corporations, non-governmental organizations, special interest groups, social movements and even private citizens contributed to make diplomacy less state-centric. At the same time, this change has made it more difficult for diplomats to manage and control foreign affairs. The information revolution has turned information into a source of national power and influence: traditional military and financial powers are being complemented by soft power. In general, the information revolution has also allowed the Internet and other information technologies to become a powerful engine in causing change in foreign affairs arena by transforming people’s values, identities, and social practices. An always growing information infrastructure makes it possible for diplomats to interact not only on the official governmental but also with the general public.

The information revolution has created a new fundamental characteristic in international relations: speed. Diplomatic reactions and decisions must now be taken in a matter of seconds. As a consequence, global media provide news from distant lands more quickly than ever provoking instant diplomatic decisions. Diplomats are under a constant pressure to take swift decisions. A quick response is many times required due to various reasons. The general public expects a response to an incident or event: failure to provide such a response through an official statement within a reasonably short amount of time could lead to instability and disappointment from the public and loss of good faith and trust of the government. Political scientist Eytan Gilboa sums up this situation: “If foreign policy experts, intelligence officers, and diplomats make a quick analysis based on incomplete information and severe time pressure, they might make bad policy recommendations. Conversely, if they take the necessary time to verify and integrate information and ideas from a variety of sources, and produce in-depth reliable reports and recommendations, they may find that
their efforts have been futile if policy makers have had to make immediate decisions in response to challenges and pressure emanating from coverage and global television.”\(^{68}\) Apart from the speed characteristic, another side effect of the information revolution is the increased risk of being misunderstood. With the constant pressure of diplomats into public diplomacy, information which was traditionally intended for diplomatic recipients is now being delivered also to the non-diplomatic community. It may prove rather difficult for an individual not familiar with diplomatic terms or practices to fully grasp the concept and intentions of diplomats. Diplomats are required to acquire new skills in adapting their feedback for perusal of the general community, as misinterpretation of information may have more serious effects and conflict may arise as a result. The diplomatic community must also exercise more care when communicating with the public in general as diplomats are now open to much further scrutiny than what was previously the norm. Moreover, besides other diplomatic opponents, sources which may scrutinize diplomats are increased to the media and public in general, together with non-government and other organizations.

The information revolution has had its side effects on diplomacy. This seems to be the true revolution: this exposed diplomacy uses networks as a lever for the expansion of freedom around the world. But this new diplomacy also has its dark sides, which have recently emerged. If the use of networks can promote freedom around the world, it can also monitor these networks, listen to foreign embassies, international institutions or even Angela Merkel’s cell phone.\(^{69}\) The WikiLeaks scandals and the Snowden affair have revealed that the new diplomacy was not freed from old habits, increased by what technology allows today. This new diplomacy also required a reconciliation of the United States government with major digital companies – Google, Facebook, Twitter, Apple, etc – because they are action levers. Using the principle of revolving doors demonstrates the inter-penetration of public and private sector’s ambiguous relationships: former United States Secretary of State’s Policy Planner Jared Cohen resigned to work at Google; Amazon hired Jay Carney, Former President Barack Obama Press Secretary,\(^{70}\) closely followed by former United States Secretary of State Condoleezza Rice who joined the board of Dropbox.\(^{71}\) For more


\(^{70}\) Streitfeld, David (February 26 2015). Amazon Hires Jay Carney, Former Obama Press Secretary. The New York Times

\(^{71}\) Bilton, Nick (April 18 2014). Protests Continue Against Dropbox After Appointment of Condoleezza Rice to Board.
than 15 years, Internet impact on policies and world politics has become more than obvious. Today, more and more governments and diplomatic missions make a daily use of social media like Facebook, YouTube or Twitter. Some countries like the United States have even developed their own network of remote or “online” consulates and embassies.\(^\text{72}\) Thanks to the information revolution, questions about global television and foreign policy are now part of the larger, lively discussion of what digital diplomacy is.\(^\text{73}\) If regular concept of public diplomacy can be defined as a “top-down” or vertical model orchestrated by states in a crypto or para-state way, the main characteristic of digital diplomacy is that it applies a “down-top”, or horizontal model orchestrated by individual actors. In other words, digital diplomacy makes the conception of foreign diplomacy less foreign by arousing emotions, orientating media judgments, and bringing a global and targeted approach to world affairs.\(^\text{74}\) For example, reacting to the worst terror attacks in France in decades that claimed the lives of more than 120 people on November 14 2015, Twitter users launched the hashtag “#Paris.” In the minutes following the attacks, Facebook activated its “Safety Check” feature allowing the site’s users in the area of the attacks to mark themselves as safe on their profiles. This marked the first time the tool was enabled for violent attacks. Twitter’s news-curation tab, known as “Moments,” featured tweets, images and videos from news agencies and bystanders that showed snippets of the attacks’ aftermath. These tools were heavily relayed by the French Presidency, the Ministry of Foreign Affairs of France, the White House and the United States Department of State. It is known as one of the most important digital mobilization ever created so far.\(^\text{75}\)

---

\(^\text{72}\) Virtual Embassy of the United States Tehran, Iran. www.iran.usembassy.gov


\(^\text{74}\) Ryan, Evan and Frantz, Douglas (February 18 2014). Digital Diplomacy: Making Foreign Policy Less Foreign, U.S. DoS

2.4.2 Sovereignty

In our modern era, diplomacy, sovereignty and governance are closely intertwined.\(^76\) Having a diplomatic body remains a sovereign prerogative of a territory governed by civil law and protected by an armed force. In the digital field, states want to control critical infrastructure on their territory. Meanwhile, they try to take positions in a soiless transnational cyber-space. In this definition, information and communications technologies promote the development of an “imperialist interpenetration”\(^77\) which is no longer satisfied with a simple territorial supremacy, but multiplying the connections in order to develop network strategies. According to Chinese Academy of Social Sciences academic Lang Ping, if one applies Clausewitz’s concept of key terrain to cyber-space, “it is clear the United States has absolute superiority”.\(^78\) In cyber-space, technology determines one’s capacity to maintain sovereignty, with key terrain incorporating data centres, network service providers, submarine cables, supply chains, labour sources, technological innovation and international standard-setting bodies. In the same article, former president of the Chinese Academy of Engineering Fang Binxing argues that United States dominance over the Internet’s multi-stakeholder model undermines that model’s independence and allows the United States to manipulate stakeholders under United States domestic law. The Snowden revelations gave a particular resonance to Chinese protestations against the domination of cyber-space by a United States cyber-hegemony, notably ensured by the Internet Corporation for Assigned Names and Numbers (also known as ICANN). The ICANN is an American non-profit organization that is responsible for coordinating the maintenance and methodologies of several databases with unique identifiers related to domain names of the Internet, ensuring the network's stable and secure operation. Every registered domain name in the world goes through this database, raising obvious sovereignty and hegemony concerns on the role of the United States in the ruling of this centralized organization. At the June 2014 United Nations Workshop on Information and cyber-security, in Beijing, Vice Foreign Minister Li Baodong condemned the massive-scale surveillance activities by an “individual country,” which have “severely infringed on other countries sovereignty and their citizen’s privacy. Rather than reflecting on its behaviours that undermine the sovereignty of other countries and privacy of citizens, it has painted itself as a victim and made groundless accusations

\(^{77}\) Bellanger, Pierre (2012). De la souveraineté numérique, Le Débat, #3, p. 141
against or defamed other countries.”79 This statement asserts that states have rights in cyber-space and, by implication, that the Internet has borders. Minister of China’s State Internet Information Office Lu Wei commented at the second China-South Korea Internet round-table that “just as the 17th century saw the extension of national sovereignty over parts of the sea, and the 20th over airspace, national sovereignty is now being extended to cyber-space.”80 Beijing’s rhetoric in relation to the Internet stems from a now firmly entrenched view of cyber-space as part of a country’s territory, and Minister Lu’s comments are aimed at pursuing change in global Internet governance among territorial lines. In this definition, information and communications technologies promote the development of an “imperialist interpenetration”81 which is no longer satisfied with a simple territorial supremacy, but multiplying the connections in order to develop network strategies. Diplomats see cyber-space as a “common space”, just as trans-boundary waters. Pirates are indeed cruising in these areas of seas and oceans. This realist approach considers that digital diplomacy needs to be discussed or debated only between great powers in main political and diplomatic institutions like the United Nations. This approach only considers digital diplomacy as an “attached field of competences” structured by states in international relations. But in reality, digital diplomacy is about to transform the very nature of the international system: it is before everything else a technology that spectacularly spreads in all social bodies and in all societies. Nonetheless, this revolution did not spread evenly. According to constructivist sociologist and international relations specialist Pierre Bellanger, Europe now undergoes a scissors effect of a strategic and political nature under digital influence.82 Indeed, a digital gap is widening between “western Europe” countries such as Belgium, France, Great Britain, Germany, Netherlands and Eastern Europe.83 On a more strategic analysis, most European countries do not seem to have realized the emergency to organize their industry to reach a critical size, enabling them to retain their autonomy of decision and avoid being “silently skinned” by the United States and China. Digital sovereignty quickly leads to the notion of cyber-war,84 illustrated by the proliferation of cyber-attacks.85 For many diplomats and cyber-strategists, cyber-war is only the continuation of war by using information and communications technologies with, however, two fundamental differences: it does not result in a frontal opposition

79 Official statement from Vice Foreign Minister Li Baodong, Ministry of Foreign Affairs of China, June 5 2014
80 Official statement from Minister of China’s State Internet Information Office Lu Wei, December 10 2013
81 Bellanger, Pierre (2012). De la souveraineté numérique, Le Débat, #3, p. 152
82 Bellanger, Pierre (2012). De la souveraineté numérique, Le Débat, #3, p. 175
83 Please refer to this mini-thesis’ spreadsheet database
85 Ventre, Daniel (2011). Cyberwar and Information Warfare, Willey-ISTE

Page 43
of the belligerents and would not, at least for the moment, make direct victims.\textsuperscript{86}

When it comes to digital diplomacy, sovereignty also implies the notion of governance, action and reactivity. In raw numbers, the future of Internet governance depends largely on the diplomatic positions of several major world powers. English is no longer the dominant language on the Web, and a country like China has the largest number of Internet users. Using a sophisticated system of censorship and numerous technical innovations, Beijing seeks to partition and conquer the Web in Chinese. Other states, such as Iran, Russia, Turkey and Saudi Arabia are also seeking the same goal using different methods to control the Internet. During the past ten years, there has been an increased role that public opinion and legislatures play in modern diplomacy. According to Tim Berners-Lee, inventor of the World Wide Web, political fragmentation now threatens directly the very spirit of the Web.\textsuperscript{87} According to Berners-Lee, physical laws must prevail on the Internet: in other words, a web application should work the same way in China or in Chile.\textsuperscript{88} A major challenge lies in the future of current transnational Internet norms, mainly regulated by the United States and regularly jeopardized by the Chinese and Russian attempts to “sovereignize” the Web. The takeover by the governments at the expense of multi-stakeholder principles that accompanied the extraordinary growth of the Internet over the past twenty years demonstrates their political adaptability and technical efficiency. During the past ten years, and thanks to the digital explosion, there has been an increased role that public opinion and legislatures play in modern diplomacy. The first is the result of innovative technology and the highly scalable Internet, which is done by the contribution of various actors and institutions that are very little known to the general public. Internet governance is based on a new principle of governance called “multi-stakeholder”. Internet standards have been defined and developed by the Internet community itself, including through the ICANN, but has no control over the published content. Internet governance affects the management of uses and content on the web. Nevertheless, it is stirred by two contradictory logics. On the one hand, the extension of the principle of multi-stakeholder governance as stipulated in the World Summit on the Information Society held in Tunis in 2005.\textsuperscript{89} To ensure the plurality of views, the Summit decided to create the Internet Governance Forum, meeting every year and putting on an equal footing over 1500 participants from governments, civil society, private sector, Internet service

\textsuperscript{86} Rid, Thomas (2013). Cyber War Will Not Take Place. Oxford University Press
\textsuperscript{87} Halliday, Josh (22nd November 2010). Tim Berners-Lee: Facebook could fragment web, The Guardian
\textsuperscript{88} Force Hill, Jonah (2012). Internet fragmentation, highlighting the major technical, governance and diplomatic challenges for US policy makers”, John F. Kennedy School of Government, Harvard University, p. 10-13
\textsuperscript{89} McCarthy, Kieren (July 1 2005). Bush administration annexes Internet. The Register
providers and international organizations. The last forum was held in Baku, Azerbaijan, in November 2012. On the other hand and according to Daniel Thierer, the comeback of states to regulate the Internet, including the pretext of the fight against certain content like child pornography or terrorists groups, is very visible and arousing deep scepticism from non-state actors. From his libertarian ideals of limited government, individual liberty, free markets and peace, Thierer considers the threats to free speech and online commerce posed by international government attempting to impose such territorial statutes and standards within cyber-space and clearly demonstrates defiance towards a global Internet regulation initiative.\textsuperscript{90} Initiatives in the matter of Internet regulation emanate from states eager to break Western domination and influence. In September 2011, China and Russia, along with Uzbekistan and Tajikistan, filed a proposal in the context of the General Assembly of the United Nations, and aimed to establish an intergovernmental code of conduct to define the behaviour of states on the World Wide Web. Concurrently, India, Brazil and South Africa advocated the creation of a UN committee relating to the Internet.\textsuperscript{91}

The takeover by the governments at the expense of multi-stakeholder principles that accompanied the extraordinary growth of the Internet over the past twenty years demonstrates their political adaptability and technical efficiency. What is yet to be seen is whether a similar restructuring of power can take place in a digitally enabled world, without its empowering chaos, messiness, and disorder being lost.

\textsuperscript{90} Thierer, Adam (2003). Who Rules the Net?: Internet Governance and Jurisdiction. Cato Institute

\textsuperscript{91} Mueller, Milton (September 17 2011). India, Brazil and South Africa call for creation of “new global body” to control the Internet. Internetgovernance.org. Accessed on November 24 2015
2.4.3 Cyber-war

Cyber-war is neither a cold nor an open-war: it is a cool war. Almost every state in the world has intelligence services in order to spy other countries or organizations: this is what the world will remember after Edward Snowden’s release of classified material in June 2013. This young system administrator came to international attention after disclosing to several media thousands of classified documents that he acquired while working as a National Security Agency contractor. The general public was then aware of the existence of a worldwide system of global surveillance entirely based on digital networks and data. The secret documents of the American National Security Agency provided to the media by Snowden describe actions taken by the American secret services with regard to the diplomatic representations in Washington and New York. According to classified National Security Agency files, spyware (contraction of spy and software) were installed in the European Union building in New York where the 28 ambassadors of European Union member countries negotiate on a common policy on the United Nations Organization. The National Security Agency also infiltrated the United Nations’ internal computer network between New York and Washington. Therefore, American’s main intelligence agencies were able to have access to discussions and emails and to internal documents on computers.

Cyber-space has become a new battlefield for states and non-state actors, and not only in the field of espionage. Beyond attacks and counter strikes, both coming from the United States and China, cyber-security represents a major issue involving states, but also corporations, consumers, citizens, and terrorists. According to French cyber-defence specialist, Daniel Ventre, these revelations are only a “semi-surprise”: for many years, the National Security Agency and the Federal Bureau of Investigation were working on several programs designed to digest and analyse billions of data. In March 2012 – a year before Snowden’s revelations – Wired Magazine announced the construction of the biggest and most sophisticated United States Spy Centre on the planet. One of the key sentences of this article was: “The National Security Agency has become the largest, most covert, and potentially most intrusive intelligence agency ever.” This United States cyber-strategy is also a private war: as the Snowden affair suggested, the biggest hi-tech companies in the world are also involved in this global spying. Among them are Google, Apple, Microsoft, IBM, Dell, AT&T, and

92 Greenwald, Glenn (May 18 2014). Edward Snowden: the whistleblower behind the NSA surveillance revelations. The Guardian
94 Bamford, James (March 15 2012). The NSA Is Building the Country’s Biggest Spy Center (Watch What You Say). Wired Magazine
Verizon. According to Dean Cheng,\(^{95}\) the Snowden case has certainly managed to reshuffle the cards. Countries like China are now taking the opportunity to turn every accusation of spying back to the United States. But China’s use of digital threats is significantly different from the United States strategy. By manipulating cyber-economic and cyber-military weapons, Chinese officials tend to make use of their national and public resources first. National People’s Army of China is directly involved in a worldwide espionage program for economic development of Chinese interests.\(^{96} \)\(^{97}\) These recent efforts clearly indicate a Chinese perception of cyber-war and cyber-information that is much broader than cyber itself. The Chinese are trying to get the ability to understand and therefore to manipulate the fundamental perception of decision taking. Cyber is here one of the tools: seeking military and commercial blueprints, but also to anticipate and to reach the most secret information on the planet in order to understand and maintain their position in the world.\(^{98}\)

In the world of cyber-weapons, one was particularly highlighted in 2010: the Stuxnet worm designed to infiltrate and destroy nuclear centrifuges in Iran. Stuxnet was extremely innovative: it was the first known cyber-attack in the world that could create physical destruction. Stuxnet was not designed to harm, to corrupt or to steal information, but only to seek and destroy. Stuxnet was using thousands of lines of code, extremely well written, and very difficult to detect, or even to analyse to stay undercover.\(^{99}\) One of the most interesting (and perhaps one of the most terrifying) characteristics of cyber-weapons is the inability for states or security companies to locate or even determine the origin of such attacks. Nevertheless, it is possible to speculate that Israeli and United States intelligence were behind this program: these two countries have a strong interest in stopping the Iranian nuclear development program.\(^{100}\) Stuxnet also appears as the first well-documented cyber-attack to be politically motivated.\(^{101}\) South Africa is particularly under the spotlights. According to Bernard Sathekge,\(^{102}\) South Africa is one of the most targeted countries globally for cyber phishing crime attacks, as are the United States of America (with more than 77 percent of world cyber-attacks), Great-Britain, Canada, Poland and France. In February 2010, the South African government released a notice of intention in order to establish a comprehensive national cyber-

\(^{95}\) Dean Cheng (May 23 2013). China Renews Cyber Attacks Against U.S. Heritage Fondation Journal
\(^{96}\) Dean Cheng (February 23 2013). Chinese Cyber Attacks: Robust Response Needed. Heritage Fondation Journal
\(^{97}\) Dean Cheng (May 29 2013). China Hacks U.S. Defense Department. Heritage Fondation Journal
\(^{98}\) Rid, Thomas and Hecker, Marc (2009). War 2.0: Irregular Warfare in the Information Age. Westport, Praeger
\(^{100}\) ibid
\(^{101}\) ibid
\(^{102}\) Sathekge, Bernard (April 30 2014). South Africa: A cyber crime hot spot. The New Age
security policy. In the first sections, the report mentions the following: “South Africa does not have a coordinated approach in dealing with cyber-security. Whilst various structures have been established to deal with cyber-security issues, the structures are inadequate to deal with cyber-security issues holistically”. Another note mentions that “the development of interventions to address cyber-crime requires a partnership between business, government and civil society. Unless these spheres of society work together, South Africa’s efforts to ensure a secured cyber-space will be severely compromised”. Following these repeated warnings, the South African government published a draft of the Cybercrimes and cyber-security Bill in October 2015. The bill is part of a set of laws and policy initiatives in South Africa that aim to regulate the ever-expanding online economy, and the surge in cyber-related crimes from a South African (and global perspective). The current legal framework to combat cyber-crime is a hybrid of legislation. Nevertheless, common law has not kept pace with the dynamic nature of cyber-crime. According to the report received, the Bill is a product of calls by various stakeholders for government to enact specialized legislation and to align South Africa with international practice. If passed, it would codify numerous offences or “cybercrimes”, like unlawful access and interception of data, broadly defined in this context to include personal and financial information. It would also provide extensive powers of investigation for the government and imposes various obligations on electronic communications service providers regarding aspects which may impact on cyber-security. It would also regulate jurisdiction of the courts, specifically in relation to cross-border offenses. This is another example of the effects of these inter-connections at a global scale: states, but also corporations and citizen have to remain fully involved in order to fight against cyber-crime. The draft does not mention any sort of information regarding diplomatic or governmental data protection strategy. The legal status of whistle-blowers like Edward Snowden is also not included at this point. While the Internet affords people living in different circumstances around the world to access to the same information, it also acts as an equalizer between governments and non-state actors. Government databases and public utilities can be invaded and disrupted by sophisticated attacks launched by foreign governments or even by computer-literate teenagers. This level of exposure and uncertainty creates a new security dilemma faced by all states. In his article “Virtual

103 Cyber-security policy of South Africa (February 19 2010). Government Gazette #536, Republic of South Africa
104 Cybercrimes and cyber-security bill (October 20 2015). Ministry of Justice, Republic of South Africa
105 Ibid
Defence," James Adams adopts a strict neorealist approach to deal with issues of cyber-terrorism and security, and while he does lessen the security dilemma, he creates a tense, distrustful, and ultimately unsustainable international system. To deal with these security threats, the Internet must be viewed as having its own customs: states must come together to promote its continued development and ensure their security, which is possible by using elements of the constructivist school of thought. As a neorealist, James Adams views the Internet as an anarchic system and declares, “cyber-space has become a new international battlefield.” In the absence of a governing body or law-enforcement force, the Internet corresponds to the realist security model. In this configuration, every state has to stand alone (or with its allies as defiance is still the norm) and tries its best to build up cyber strengths and defences while fearing that every move made by another state poses a direct danger to their security. Adams adopts this realist fear and points out “overwhelming military superiority and a leading edge in information technology have made the United States the country most vulnerable to cyber-attacks.” Drawing from past examples, Adams demonstrates this risk and the difficulties of prevention. In 2010, the Stuxnet worm has shown that governments are still vulnerable to cyber-attacks. Stuxnet seems to have been aimed predominantly at Iranian nuclear facilities and is considered by many to be the first direct example of cyber-warfare. As part of their investigation into the virus, Kaspersky Labs determined that due to its high level of sophistication, “the attack could only have been conducted with nation-state support.” This becomes a diplomatic nightmare because it proves that even a state with reduced computing capacities (like North Korea) is able to attack another with impunity and not leave a single trace as to the attack’s origin. If this is the case, neorealist theory predicts that there will be a total breakdown in international trust and institutions as every state, fearing imminent, unknown attacks, draws back and builds up its own strength. Given United States defence spending rates, it is unlikely that any country will surpass the United States in conventional military might in the near future. According to neorealist principles, hostile countries would begin spending resources to develop cyber-weapons that will give them an asymmetrical advantage and potentially defeat the United

107 ibid
108 ibid
110 Maclean, William (September 25 2010). Iran “First Victim of Cyberwar”. The Scotsman
States without firing a single bullet. To solve this situation, Adams strongly recommends an expansion of the Department of Defence’s powers to monitor the Internet at the cost of certain civil liberties, showing some obvious weaknesses of this position. Neorealists only consider states in their analysis and never non-state actors. The self-proclaimed Islamic State of Iraq and the Levant (also referred as ISIL, ISIS or Daesh) illustrates the ambiguous and blurry definition imposed by the neorealist paradigm. According to Max Weber, conequering and subjugating people is not necessarily an acceptable definition of statehood: therefore the Islamic State cannot be recognized as a state but as a terrorist organization that still represents a major threat in the field of cybersecurity. For this reason, the neorealist paradigm may only be appropriate in analysing conventional wars since it is difficult for non-state actors to raise a meaningful number of troops or arms against state powers. On the cyber battlefield, anyone is capable of preparing and leading a virtual attack. For the moment, states have more financial and technological resources, but corporations (especially multinational companies), terrorist organizations and individuals are now equally able to cause serious damage given a certain degree of computer knowledge. Offensive and defensive realists both discuss the idea of first strike capability as a way to end a security dilemma and ensure that an enemy cannot retaliate. According to Constantine J. Petallides, “it is nearly impossible to see or anticipate an incoming attack in cyber-space, and given the global nature of the Internet, a state can never hope to disconnect another and prevent an enemy from preparing its own cyber counteroffensive.” In their article “The Information Revolution, Security, and International Relations,” Eriksson and Giacomello stress the importance of cooperation to mitigate the threat of cyber-attacks. They emphasize that “government alone cannot secure cyber-space,” but do not propose a real alternative. According to Constantine J. Petallides and from a neoliberal point of view, this security dilemma could potentially be resolved through the creation of international institutions. As the constructivist school emphasizes the importance of symbols, ideas, and their meaning, Eriksson and Giacomello see “symbolic politics as highly relevant for studying digital age security.”

112 ibid, p. 104
116 ibid, p. 236
developed a life of its own and a changing identity. From a constructivist point of view, interactions between states, other states, and non-state actors must evolve to fit the Internet age.\footnote{ibid, p. 237} While there is a security dilemma, neorealist theories do not offer the proper ways to deal with non-state actors who use the Internet to launch cyber-attacks, nor does it offer solutions to deal with dangerous ideologies which have the potential to be just as damaging. The neorealist dilemma also does not take into account the existence of various stakeholders that still contribute to shape the Internet. One of the best example in the field is the Anonymous group. With no set infrastructure or headquarters, hierarchy, or set membership, this informal group is “the first internet-based superconsciousness.”\footnote{Landers, Chris (April 2 2008). Serious Business: Anonymous Takes on Scientology (and Doesn't Afraid of Anything). Baltimore City Paper} Comprised of varied people around the world, the group shares the idea that they are part of a worldwide movement that claim to be responsible for major hacks around the globe in order to defend Internet neutrality and freedom of information. Their hacking of Amazon.com and the MasterCard online banking services are still present in the minds of cyber-analysts.\footnote{Turner, Lauren (January 24 2013). Anonymous hackers jailed for DDoS attacks on Visa, Mastercard and Paypal. The Independent} Along with WikiLeaks, ISIS and many other informal groups, Anonymous successfully demonstrates how a non-state actor can promote and fight for an ideal through the Internet and have a real world impact. From this perspective, it seems that the constructivist principle of international cooperation and transparency are the only ways to avoid the threat of cyber-terrorism. Cooperation seems to be the key word on this uncertain landscape, adopting constructivist ideals and viewing the Internet as a breeding ground for ideas that can take on an unstoppable momentum of their own, can the international community realistically expect peace, security and transparency.

Recent events, including accusations of spying and the leaking of sensitive government documents have demonstrated that security and secrecy endure as a crucial, yet overlooked aspect of digital diplomacy. The third chapter will now examine the evolution of secrecy in the context of two emerging trends: the information revolution and an increasing need for security.

\footnotetext{117 ibid, p. 237}  
\footnotetext{118 Landers, Chris (April 2 2008). Serious Business: Anonymous Takes on Scientology (and Doesn't Afraid of Anything). Baltimore City Paper}  
\footnotetext{119 Turner, Lauren (January 24 2013). Anonymous hackers jailed for DDoS attacks on Visa, Mastercard and Paypal. The Independent}
Chapter 3 – Secrecy in the era of digital diplomacy

It is essential to start with the assumption that a culture of secrecy undermines diplomacy by shuttering up windows diplomats need kept open.

3.1 Secrecy in diplomatic history

In June 2013, federal contractor Edward Snowden leaked roughly 200,000 classified documents describing activities of the United States government’s National Security Agency. Chief among them were papers detailing a clandestine digital surveillance program known as PRISM: a massive data collection sweep that scooped up phone records of millions of United States citizens – whether they were suspected of crimes or not. As former Assistant Secretary of Defence Paul Stockton wrote, the idea that “if we build a fence around us, we’ll be secure... is outmoded. It is broken and it needs to be replaced”.\textsuperscript{120} Fifteen years ago, Senator Daniel Moynihan wrote, “Secrecy is for losers.... For people who do not realize how important information really is.... We put openness in peril by poking along in a mode of an age now past”.\textsuperscript{121} To secure a nation, governments cannot retreat into an outdated mode of secrecy. They must come to grips with the mode of openness that defines the age it is in. Diplomacy does not deal with physical fences, but the metaphor holds up: the idea that erecting a culture of secrecy around diplomacy will keep a nation secure is outmoded and needs to be replaced. By massively leaking secret diplomatic cables coming from its administration, WikiLeaks could rightly claim its identity from the Founding Fathers of American diplomacy. Between the 1776 independence and the Constitution of 1787, George Washington, Benjamin Franklin, George Mason and a few republicans laid the principle of the refusal of secrecy in international negotiations. This refusal reflected the United States disregard for the habits of European diplomacy, where secret treaties were customarily concluded by monarchs or emperors who did not have to be accountable to anyone. The Italian Renaissance – which invented the modern notion of ambassador – had confirmed a paradigm in which foreign affairs were a preserved domain for the Prince. Secrets were intentionally veiled behind reasons of state. For American Revolutionaries, that secrecy harboured absolutism and authorized all turpitude among nations. In a sentence, secrecy was described as responsible for tearing apart the Old Continent. Diplomacy was not to be a broad daylight activity.

\textsuperscript{120} Bjola, Cornelia and Holmes, Marcus (2015). Digital Diplomacy: Theory and Practice. Routledge, p.53  
\textsuperscript{121} Moynihan, Daniel Patrick (1999). Secrecy: The American Experience. Yale Press University, p.132
Ambassador Louis the XIV of France, François de Callières wrote in 1716: “Secrecy is the weapon of diplomatic negotiations” and that “an able minister will make sure that no man shall penetrate into his secrets before a proper time.”

Independent after a long war, the United States of America wanted to set up a new diplomacy and put into effect the principles of the Enlightenment as described by French philosopher Gabriel Bonnot de Mably. In his 1757 “Public Law in Europe”, he declared the following: “It would be a great proof of wisdom that nations across Europe repeal secrecy and prohibit its use across Europe.”

Being the first ambassador of the United States to France from 1776 to 1785 and one the most respected diplomat in the world, Benjamin Franklin wanted to negotiate a crucial trade treaty between France and the United States against Great Britain. At this occasion, he declared “I always abide by the same rule: I will never take care of a case that will make me blush when making it public.”

During the 1787 constitutional debates, American republicans reaffirmed their preference for open diplomatic negotiations. Analysing this period in his book, Corneliu S. Blaga rightly observed: “Unlike European diplomatic cables, those of the Americans were for the maximum publicity. Cables were written with the intention and belief that circumstances would place them one day under the eyes of United States citizens and the world.” However, the WikiLeaks and Snowden affairs show this intention and noble aspiration has purely disappeared.

In order to understand the erosion of these principles in international relations, it is important to refer to another critical moment in history. Still largely inspired by Enlightenment philosophers and the Revolution of 1776, former United States President Woodrow Wilson presented to Congress, on January 8 1918, his famous “Fourteen Points” placing the ban of secret diplomacy at the forefront. Several months later, the same president secretly negotiated the Treaty of Versailles with French Prime Minister Georges Clemenceau and British Prime Minister Lloyd George, keeping important discussions away from all other delegations and even from their own entourages. Jules Cambon, French Foreign Minister in the inter war period noted in 1926: “We realize that the day there would be no secret negotiations there would be no negotiation at all.”

123 Bonnot de Mably, Gabriel (1746). Droit public de l’Europe. PUF, Paris
On April 27 1961, former United States President John Fitzgerald Kennedy spoke before the American Newspaper Publishers Association in these words: “The very word “secrecy” is repugnant in a free and open society; and we are as a people inherently and historically opposed to secret societies, to secret oaths and to secret proceedings. We decided long ago that the dangers of excessive and unwarranted concealment of pertinent facts far outweighed the dangers which are cited to justify it. Even today, there is little value in opposing the threat of a closed society by imitating its arbitrary restrictions. [...] For we are opposed around the world by a monolithic and ruthless conspiracy that relies primarily on covert means for expanding its sphere of influence--on infiltration instead of invasion, on subversion instead of elections, on intimidation instead of free choice, on guerrillas by night instead of armies by day. It is a system which has conscripted vast human and material resources into the building of a tightly knit, highly efficient machine that combines military, diplomatic, intelligence, economic, scientific and political operations. [...] Nevertheless, every democracy recognizes the necessary restraints of national security – and the question remains whether those restraints need to be more strictly observed if we are to oppose this kind of attack as well as outright invasion. [...] No President should fear public scrutiny of his program. For from that scrutiny comes understanding; and from that understanding comes support or opposition. And both are necessary. [...] I not only could not stifle controversy among your readers – I welcome it. This Administration intends to be candid about its errors; for as a wise man once said: “An error does not become a mistake until you refuse to correct it.” We intend to accept full responsibility for our errors; and we expect you to point them out when we miss them. [...] Without debate, without criticism, no Administration and no country can succeed – and no republic can survive.”128

From John Fitzgerald Kennedy to John Forbes Kerry, there is not a single diplomat who does not know the usefulness and legitimacy of secrecy. But this old tradition of secrecy faces a contemporary injunction for transparency, driven by two major factors. The first factor corresponds to the legacy of the Enlightenment: people have the right to know about the duties and responsibilities of governments. This factor never ceased to gain power as societies democratized. The second factor can be found in the development of new information and communications technologies, which multiply the impact of any breach of secrecy: the WikiLeaks and Snowden affairs bring us the latest (and the best?) illustration possible. They are expected not to be the last. At the time of writing,

WikiLeaks raised a 100,000 Euros reward for Europe's most wanted secret: the Transatlantic Trade and Investment Partnership also know under its acronym TTIP.\textsuperscript{129}

The WikiLeaks scandal brings both a consequence and a risk. The consequence is that diplomatic chancelleries and major multilateral negotiations actors should continue to seek a better balance between secrecy and legitimacy. The risk is the growing stigmatization of such resulting transparency. Public and private actors came to deplore “the dictatorship of transparency”, while it is precisely – when applied to political power – a condition of any democratic society. Information transparency provides a redoubtable antidote against abuses that allow power to remain secret: conflicts of interest, arbitrary appointments and sanctions, diversion of public funds by and for special interests, corruption, extortion, etc. All these thrive in secrecy, but decay when transparency mechanisms expose it to day light.

\textsuperscript{129} Liat, Clark (12th August 2015). WikiLeaks crowdfunding €100,000 reward for TTIP secrets, Wired
3.2 After WikiLeaks: new aims, new strategies

WikiLeaks has been criticized before for revealing sensitive information. For these leaks and others, many have praised the organization. On July 25 2010, WikiLeaks.org published the “Journal of the war in Afghanistan” – a considerable amount of incident reports describing the daily life of the United States military. This diary made the front page of The Guardian, Le Monde, The New York Times and Der Spiegel. Abundantly commented by the international press, such disclosure sparked a broad debate on the rising power of participatory media, digital journalism and digital diplomacy. Most discussions were influenced by myths of the digital age which originate in a very deterministic and naive vision of technology.

The first myth was to believe that “participative media” whose content is coproduced by users and contributors have a specific power. There has been much speculation about what WikiLeaks revealed about the role of new cooperative media, particularly in the coverage of armed conflicts. The question is not uninteresting, but illustrates a widespread confusion that tends to consider that all forms of “social” media like blogs, Twitter, Facebook, YouTube or WikiLeaks are all in the same basket. According to determinists and instrumentalists, because these media make use of the same technologies, they should form a homogeneous ensemble. But unlike other cooperative media, any document published on WikiLeaks goes through an extensive process. This approach highlights the fanciful dystopian vision according to which humanity would see the advent of an “open world” where everyone would work to spread all kind of information throughout the globe by publishing whatever he or she likes. WikiLeaks’ influence does not rely on the technology, but on the trust readers may put in the authenticity of documents they choose to download and read. From the beginning of the Iraq war, several videos showing coalition forces engaged in illegal and extremely violent acts of aggression were uploaded on the video platform YouTube. Yet none of these documents had as much impact as another similar published by WikiLeaks, simply because information has value only if it is verifiable. “Social” media are not all equal in information: it would be wrong to attribute the same or equal degree of influence to them.

The second myth is that nation-states are disappearing. Much of the discourse that glorifies Internet is based on the idea that we now live in a world without borders. According to Jay Rosen, professor at New York University, WikiLeaks would even be “the first newspaper escaping all state power.” It is quite the opposite: nation-states are far from disappearing. WikiLeaks officials have understood this: their website site is based in Sweden where it enjoys the exceptional level of security that Swedish law provides to “whistleblowers.” The Swedish company PRQ hosts its servers and any
document sent to the site goes through servers located in Belgium, also to ensure the protection of sources. Finally, WikiLeaks’ founder Julian Assange has chosen to present most of the WikiLeaks’ content in Iceland. This country enacted a set of laws designed to make it a heaven for whistleblowers and investigative journalists. Numerous examples illustrate the role played by states and national laws in the digital world, from the decision of the United Arab Emirates and Saudi Arabia to ban the use of instant messaging on BlackBerry devices and the temporary prohibition of Twitter and YouTube in Turkey. While it is true that WikiLeaks’ structure was originally designed to bypass some national legislation through digital technology, it is also intended to take advantage of the laws of other countries. The site is neither above nor beyond the law: it “draws” in all legal frameworks that are the most favourable to it.

The third myth is that journalism is dead, or on the verge of dying. The example of WikiLeaks shows that technology forces us to redefine and to clarify the meaning of “journalism”, but it also confirms the central role of this profession in the dissemination of information. Several weeks prior to upload classified documents on the war in Afghanistan, WikiLeaks sent them to four major international newspapers and not to “alternative” publications. WikiLeaks has not chosen four newspapers for their political orientation, but because the four media possessed the organizational, professional and economic resources to disseminate and make the documents available to the general public. Wisely, because if these documents had been directly put online, media outlets around the world would have rushed to the information, producing a chaotic set of scattered and confused analysis. Attention has focused instead on the four newspapers which had had the time and the means to analyse and summarize all the documents. It is very interesting to note that Edward Snowden made exactly the same use of media in his case. On May 20, 2013, Snowden flew to Hong Kong where he was staying when the initial articles based on the leaked documents were published beginning with The Guardian on June 5. Within months, documents had been obtained and published by media outlets worldwide, most notably The Guardian (Britain), Der Spiegel (Germany), The Washington Post and The New York Times (United States), O Globo (Brazil), Le Monde (France), and similar outlets in Sweden, Canada, Italy, Netherlands, Norway, Spain, and Australia.

The fourth myth is that due to the impressive quantity of released data, WikiLeaks changed the political, diplomatic and military in a radical way compared to what Edward Snowden, a modest government contractor working for the United States National Security Agency did. If the WikiLeaks affair is unprecedented in diplomatic history that deeply embarrassed the United States but did not call in question its diplomatic or military strategies, the same logic does not apply to the very nature
of Snowden’s revelations. The classification level and sensitivity of the material Snowden downloaded and its details about the country’s most critical intelligence-gathering efforts have captivated not only diplomats and military officers, but also the global imagination. It is also important to note that while both Snowden and Assange have been hailed as heroes by those who favour more transparency and more accountability, both have demonstrated different attitudes about the possible impact their leaked information could have. Snowden has said he is working with journalists who are using their discretion in deciding what parts of the leaked information should be published. Edward Snowden’s opinions also differ from WikiLeaks founder Julian Assange: “We do not share identical politics. I am not anti-secrecy. I’m pro-accountability. I’ve made many statements indicating both the importance of secrecy and spying, and my support for the working-level people at the National Security Agency and other agencies. It is the senior officials you have to watch out for.” In other words, the idea that access to raw information itself proves to be as naive as the one that assigns the same intrinsic power to technology. Information, like technology, is useful only with the knowledge and skills that make it of a relevant use. The digital universe is not a fluid horizontal domain without borders: the WikiLeaks and Snowden episodes remind us that structures, borders and laws have lost none of their significance.

After the WikiLeaks and Snowden’s scandals, the main question is to determine if secrecy can be ethical or not. Many voices have castigated diplomatic secrecy, which is suspected to escape the democratic control of citizens in the conduct of international affairs insert references to these voices. The WikiLeaks affair delighted advocates of transparency, whether they are activists of a “cyber-space” that escapes the constraints of traditional, “old-school” public debates or are simply critical towards classic public governance. Others have seized the opportunity to challenge a “traditional” conception of diplomacy. In the course of the debate on the diplomatic function in the aftermath of the Tunisian and Egyptian revolutions, the French Minister of Foreign Affairs stated that “the role of diplomats is not simply to describe the day to day routine of what is happening in the world. Let’s not have the nostalgia of a bygone era. Today, diplomacy has new and exciting missions. Its role is to anticipate in order to help the decision of politicians. Its prospective function, which had gradually withered, must become major again.” At the very same time, a special adviser to former French President Nicolas Sarkozy observed that “diplomacy is a technique, whereas foreign policy, as its name suggests, is policy. […]"
Let me be clear: the diplomat is here to enlighten the decision and to implement it, not to take it.”

From these cutting remarks on diplomacy, it is important to underline two major points:

Firstly, globalization of real-time information allowed by digital technologies challenges the processing of this information, especially for journalists and diplomats. Alternatively, procedures of these jobs are also changing, especially to guarantee data security, integrity and accessibility in a connected world. It is challenging to preserve diplomatic secrets in a rising context of cyber-warfare and cyber-attacks that are not only mandated by foreign powers, but also by citizens with computerized techniques as – if not more – advanced than governmental infrastructures. Governments now face a crucial dilemma: mixing together the increasing demand for transparency in the public debate and a reasonable level of security requires adapted policies, technological means and political philosophy to determine who should process and validate information that could possibly shed light on public debate. In other words, the question is about the nature of information itself: is democracy demanding raw or “digested” information before going public?

Secondly, diplomatic secrecy based on the “reason of state” may be exempt from public debate and democratic control. To remain legitimate and moral, its boundaries are constantly redefined according to interests that need to be protected. This notion is not easy to define, as the context is shifting just as information continues to flow. Diplomacy without secrets is utopia; but secret diplomacy seems doomed to failure. Between these two pitfalls and in order to avoid public mistrust, disinterest and emerging crises of confidence, the new mission for diplomats is to promote, in parallel with negotiations between states, an ambitious public diplomacy, in accordance with values and aspirations of the people.

131 Guaino, Henri (February 27 2011). “La politique étrangère de la France”. Le Monde
3.3 Information at the heart of diplomacy

Whatever the circumstances, information is at the heart of diplomacy. Unlike the journalist who chooses its topics according to the circumstances or instructions of writing, the diplomat’s mission is to cover at all times the full facts concerning the interior, social, economic, cultural and foreign situation of the country in which he is accredited. Diplomats are not competing with journalists: even if they often share the same sources or can be a source for one another, they rarely process the information in the same way: the journalist must work quickly, and by that mean taking the risk to create shortcuts or misinterpretations. The journalist must entice the reader with fine words or with a sensational headline; he can also be an activist and claim radical positions. On the other hand, the diplomat should never be or try to be seductive, or in a quest for the sensational. He must be accurate and elegant while concise but exhaustive. A diplomat will not express an opinion, but an insight; he will be forgiven for taking the time to report something apparently insignificant, but will be blamed for having neglected all or part of a reality. The quality of diplomats’ sources is essential: an uninformed diplomat is at best useless and at worst harmful to the interests of the state he represents.

In most democratic countries, where information flows freely and where diplomats have no limitation of access, the quality of information depends on the diplomat’s relationships and acquaintances; the better he is introduced to decision and opinion makers, the better his position is to decipher politics and provide his government the means to understand and anticipate the evolution of a given situation. Diplomat’s language abilities, general culture and interpersonal skills open many doors and, consequently, lead to confidences and to the transmission of secrets. Confidence and trust, especially among allies, is strongly required.

In non-democratic countries, where propaganda subdues the quality of information and where diplomats are considered by definition as hostile foreign agents, public relations are less decisive than the ability to circumvent the barriers built by the host country. Access to officials, when it is necessary, is usually regulated by a fussy protocol and brings very little in terms of information; the press is usually muzzled. In such circumstances, diplomats’ talent is then to “provoke” contacts wherever it seems possible for him to make his way: the knowledge about the country, patience and tolerance are essential tools for building individual confidence within a collective distrust environment. The information the diplomat collects is inevitably patchy, localized, and sometimes questionable: it is nevertheless an essential element to assess – and possibly criticize – the official
discourse. In these cases, discretion or secrecy, according to the sensitivity of the information entrusted, is the rule, which is motivated by the obvious concern for the protection of sources. Transparency is possible if the source explicitly requests it (this may be the case of human rights activists who contact diplomats as a part of their mission).

These considerations may seem irrelevant at first, but they help to explain and understand the duty of confidentiality of the diplomat: he has not, as some would like to think, turpitude to conceal or to hide, but employs security simply because of the very fragility of the confidence he is in charge of. Being important in a democratic country or restricted in an undemocratic country, confidence is the main ingredient to understand a given situation; compromising it inevitably leads to failure of the diplomat’s goals.

3.4 The impact of the increase of information flows around the globe

“Connectivity” has become a major factor to participate and engage in the exchange of information. While lots of diplomats use social media, some of them particularly master this domain. French top-diplomat Gérard Araud, currently Ambassador of France to the United States of America is well-known for his typical outspokenness. Shortly after the November 2015 terrorist attacks in Paris, a gun control tweet from Republican presidential candidate Donald Trump went viral: “Isn’t it interesting that the tragedy in Paris took place in one of the toughest gun control countries in the world?” The statement prompted a tweeted response from Gérard Araud, who called the author of the remark “a vulture” and “repugnant in its lack of any human decency.” As diplomats cannot avoid social media, they must print their marks in the public online domain. Most diplomats get this by now – official Twitter and Facebook accounts are by 2014 accepted practice. This is really problematic, as diplomats are among the few foreigners – along with specialized researchers – to be able to connect without intermediaries to primary sources of information because of their linguistic and cultural skills. Journalists and businessmen are mostly relying on secondary sources. With the exception of states where communication infrastructures are deficient, controlled or almost non-existent (like in North Korea, Burma, Sudan, etc) and where the standard of living

132 Green, Stephanie (November 6 2014). Don’t Call Him the Gay Ambassador: Gérard Araud, France’s Head Envoy to the U.S., Wants to Bring Diplomacy into the 21st Century. Vogue Magazine
133 Fletcher, Joe (November 15 2015). French Ambassador Slams Trump Over Viral Tweet About France’s Gun Laws. Addicting Info
prohibits the possession of a digital terminal (mobile phone or computer), expanding the web 2.0 has significantly opened the IT field. But this aperture has, in the same movement, altered patterns of production and consumption of information. Being “online”, information has become more immediate than ever, raw and massive.

If the journalist has no other choice but to adapt to this evolution by formatting articles so that they remain both competitive and legible, the diplomat maintains – at least for now – a certain stand back attitude that gives a real value to his (her) work. Of course, this does not mean that diplomats should stay away from information streams: it is quite the contrary. Diplomats should stay connected to record the continuous flow of international news or even participate in the online information production mechanism to engage with the public. But more than ever, this commitment requires the diplomat to identify the best sources, to assess their relevance and to provide a relevant social, economic or cultural grid which will not be dependent or relying on immediacy. In other words, the diplomat must bring essential data that normal information flows are no longer able to provide: a capacity for anticipation and foresight rooted in the intimate knowledge of the context and enriched by the experience of past situations.

Recent technological developments upset the ideal of physical protection of secrecy: the shield of cryptology has no effect on viral intrusions; USB sticks or flash drives replaced the microfilm and photocopies, and reduced to a few seconds the length of a copy of a thousands of pages; cloud computing now eliminates physical media storage and allows definitive suppression in a single click; hackers now penetrate system through “virtual machines”, making them more elusive than spies or traitors, simply because their digital footprints lead nowhere. Drastically reducing the cost of access to these technologies enables any person with technical knowledge to build a network, to manage it and, paradoxically, to remove it from the state's control; the anonymity of sources has been made possible by software designed so that no police officer can hack it. In a 2014 classified document released by WikiLeaks, the National Security Agency suggests that the fundamental security service provided by the onion router Tor remains intact. The Tor project is a non-profit organization that conducts research and development into online privacy and anonymity. It is designed to stop people – including government agencies and corporations – learning user’s location or tracking browsing habits. Based on that research, it offers a technology that bounces internet users' and websites' traffic through “relays” run by thousands of volunteers around the

134 Ferguson, Niels and Schneier, Bruce (2004). Practical cryptography. Vuibert, p. 338
world, making it extremely hard for anyone to identify the source of the information or the location of the user. Ironically, the original technology behind Tor was developed by the United States navy and has received about sixty percent of its funding from the State Department and Department of Defence.135 When it launched in 2002, the Tor project’s emphasis was on protecting internet users’ privacy from corporations rather than governments. Tor can mask users’ identities, but also host their websites via its “hidden services” capabilities, which means sites can only be accessed by people on the Tor network. This is the so-called “dark web” element, and it is not unusual to see Tor pop up in stories about a range of criminal sites.136 Other National Security Agency's top-secret documents call Tor “the king of high-secure, low-latency Internet anonymity”137. Except to return to pencil and paper, or stick to heart-to-heart conversations, confidentiality of public correspondence is not guaranteed because of their inclusion in digitized networks. What is gained in speed and collaboration is lost in protection and security. The proliferation of Internet platforms allowing both “participatory journalism” (like Glenn Greenwald's Intercept) and “data journalism” (like WikiLeaks) is the direct consequence of these developments. In this context, traditional media are trying – with difficulty – to enhance their role as “gatekeepers” of information for the general public. The diplomat, meanwhile, does not covet the keys that provide access to information; its mission is to explain, understand and anticipate. He builds or maintains bridges over which states are required to meet and interact.

3.5 The necessary secrecy of diplomatic correspondence

Once the information is collected and used for its quality and relevance, it is transmitted by the diplomat to relevant authorities by means that justify its protection. This important point is probably the one that is least understood and therefore less accepted by public opinion; the massive disclosure of United States cables by WikiLeaks for the sake of transparency and freedom of the press has undoubtedly strengthened the widespread feeling that the classification of these documents is not justified, only to hide the reality of international affairs made on citizens' behalf. The public accepts that medical confidentiality and trade secrets must be protected in all circumstances because it is private business that may affect everyone directly. On the other hand,

135 Dredge, Stuart (November 5 2013). What is Tor? A beginner’s guide to the privacy tool. The Guardian
136 Krotoski, Aleks (April 24 2014). Andrew Lewman on Tor and anonymity online. The Guardian
137 Ball, James; Schneier, Bruce; Greenwald, Glenn (4th October 2013). NSA and GCHQ target Tor network that protects anonymity of web users. The Guardian
it is commonly accepted that diplomatic secrecy should be disputed because it is about public affairs which would, by definition, remain impersonal. It is omitted that any diplomatic report (cable, email, maintenance report) transforms the information into political advice, which cannot be made public by essence. The central question that underlies this notion of confidentiality is the “need to know” in the process of developing a public policy. For the sake of the common good, it is necessary to exclude the interference of private interests that are often contradictory; when politicians ask their government to provide them with assessment criteria, sometimes options or recommendations, judgments and opinions that are expressed have no value outside of this chain because they are only ephemeral components of a decision. Indeed, public debate on foreign policy is legitimate and indispensable, but debate on the elaboration of the political decision is not. That debate can be conducted by historians when diplomatic archives become available, usually fifty years after a certain event, sometimes earlier when the government wishes to make an exception to this limit.

In February 2011, the Swedish government decided to declassify archives relating to the collapse of the Soviet Union. These restrictive provisions on diplomatic archives do not mean that the state is indifferent to the ever more assertive requirement of transparency of public action: on the contrary, in addition to diplomatic reports to inform the government in the conduct of its foreign policy, diplomats must also produce briefing notes and talking points for the public. This “public diplomacy” was almost non-existent twenty years ago. It has become essential and is growing in importance as information networks and channels continue to develop.
3.6 Public diplomacy and diplomacy of influence

Diplomatic correspondence targets simultaneously three different audiences: the government and Parliament as immediate recipients; the general public, both domestic and international; and foreign policy historians who will have the responsibility to bring judgment on a specific action. The new digital age radically challenges the balance of this triptych. Governments have become direct victims of the “CNN effect”: the saturation of Western viewers with non-stop, real-time news footage of wars and military actions on television and the Internet. In turn, these images constitute a powerful plea for action. By that mean, news media can drive foreign policy, are governments oblivious to partial news coverage. Governments are now drowning under a flow of information, waiting for less analysis and expecting more anticipation. In June 2009, tweets from Iran marked with hashtag “#cnnfail” began attacking the global news network for being an early absentee in reporting the protest against the re-election of Mahmoud Ahmadinejad. Despite being illegal, the Iranian “twitosphere” was alive with thousands of eyewitness accounts, but CNN remained silent about the disputed election. Twitter faulted CNN for not only being slow with its coverage, but also for not pursuing a sceptical line. Twitter revealed public frustration in real time, like a street focus-level focus group. Nevertheless, this treatment of the information is fast but may be chaotic, and even sometimes subjective: Twitter can be seen as a tool of the masses for the masses. On the other hand, “online” public opinion is looking for insights or judgments that raw information does not provide. The researcher, being confronted with the acceleration of history, has to challenge the “over-classification” of public documents. In every case, secret correspondence is compromised. “E-diplomats” are now recognized by public opinion less in terms of the number of classified cables they address to political leaders but more on the influence they are able to deploy on public opinion. This development is major, because it brings diplomats under the spotlights of public debate, far from the closed and comfortable atmosphere of chancelleries. The “sovereign” power of diplomats, which consisted in advising the prince in the privacy of his office and on the basis of secret information must now take life in full light in order to win the battles of ideas. This is where the notion of diplomacy of influence – or soft power – comes into play. The idea of soft power is generally attributed to Harvard’s Kennedy School of Government professor Joseph Nye, who defines it as “the ability to affect others to obtain the outcomes one wants through attraction rather than

139 Show, Nancy (2010). From the CNN Effect to the Twitter Effect. Routeledge. p. 97-104

Page 65
coercion or payment.” A country’s soft power, he argues, “rests on its resources of culture, values, and policies.”140 Soft power is not exactly policy but rather a consequence of policies. Countries can, of course, do things to promote themselves, but this can be risky. If, for example, the Voice of America were to be perceived as arrogant by those it was seeking to influence, Nye explains, and then it would not exert soft power. There is a fine line between soft power and propaganda.

Soft power is not a recent American invention. After the Franco-Prussian war, France founded the Alliance Française, which has outposts in many countries; and during World War I, many other nations acted in a similar manner, establishing their own cultural offices around the world to develop soft power. In the United States, the idea really took shape in the 1930s, where the Roosevelt administration held the position that “America’s security depended on its ability to speak to and to win the support of people in other countries.”141 Ultimately, soft power is not just getting people to do what they normally would not but also about aligning their interests with your own, often as a result of a long and trusting relationship. This means that the decline or disruption of these relationships can undermine soft power. For example, as Nye outlines, when the United States was seeking support for the Iraq war after the September 11, 2001, attacks, whether it was Mexico’s UN vote or the use of Turkish airspace, “the decline of American soft power created a disabling rather than an enabling environment for its policies.”142 Unlike traditional diplomacy, where the hierarchy of power and the control of information were made perfectly clear and followed a strict hierarchy, diplomacy of influence suggests that the state is no longer the sole holder of public speech or official opinion. Power is no longer defined in terms of hard power (like military forces, Gross Domestic Product) but also in terms of attractiveness, or ability to project values, or to set global standards. This soft power is now a new credible way to measure and determine the shifting of influence.

3.7 Diplomacy confronted by the emergence of new networks

If the WikiLeaks affair initially shocked diplomats by its description of a careless mode of management of the United States' classified information systems resulting in multiple security audits and the reaffirmation of the principle of secrecy, it has, in a second phase, accelerated the awareness that an active presence on new networks should be more than necessary. Diplomacy does not deal with physical fences: the idea that erecting a culture of secrecy around diplomacy will keep a nation secure is outmoded and needs to be replaced. The Tunisian and Egyptian revolutions in the beginning of 2011 have reinforced the belief that diplomacy could not be absent from vectors of opinion: far from the traditional ambassador monopoly on public speech, opinions on digital networks are facing immediate comments, challenges and instant protests. This does not disqualify the work of diplomats. It is quite the opposite: integrating these new vectors of opinion will strengthen diplomacy. But this move involves the mobilization of many people: by opening official diplomatic blogs in fifty missions abroad, the Ministry of Foreign Affairs of France has found the right tone to stimulate the interest of the audience. The purpose is to open windows on the day-to-day work of diplomats in various sectors: political, cultural, economic, scientific, etc. These blogs tend to demystify the excessive secrecy that still enfolds an embassy, or even a small consulate. Diplomacy in the digital age does not change the heart of the business old diplomacy, which will continue to revolve around understanding and conciliation. What changes, to use a diplomatic terminology, is the target of these digital vectors. Meanwhile, the availability of diplomatic correspondence to the general public, not deliberately leaked but declassified in a comprehensive way seems to be an appropriate answer to the public's appetite and curiosity. It is very ironic that since December 2010, even mainstream media adopted WikiLeaks' reading grid by commenting – and by that mean, sharing – classified information.

3.8 A necessary democratic contract

If public diplomacy necessitates talent, persuasion and efficiency in the making of a durable and trusted relationship with public opinion, state diplomacy will still be able to operate with a high level of confidentiality with a lower risk of public exposure and scandal. In the end, it is when the relationship is disputed that the threat of a leak is the greatest. WikiLeaks had the involuntary merit to raise the fundamental question of diplomatic ethic based on two principles: the loyalty of diplomats, which can be controlled but must be justified, and the active support of citizens. If this – sometimes fluctuating – support can be expected, it should be relentlessly pursued.
Chapter 4 – Diplomatie: a case study

By providing concrete examples, this fourth chapter aims to explain how diplomats can better handle new digital means of communication and treatment of information in their day-to-day work. Digital diplomacy transforms the way diplomats create and share information. By its prominent status and mission, diplomacy is well situated to meet crucial and upcoming challenges in our digital age. In June 2014, the Ministry of Foreign Affairs of France, also called Le Quai d’Orsay, undertook a giant leap forward to answer these challenges. The “inter-ministerial portal of diplomatic correspondence”, also called Diplomatie, is a professional social network aiming to better share data and analysis that are daily compiled and produced by French diplomats in order to allow the whole state administration but also non-state actors to anticipate worldwide new developments and act wisely. It also aims to collate exchanges between different French foreign policy players in one place, from formal letters to cables and notes. The Digital revolution brings many potential: fluidity, rapidity, agility, openness, transversality that traditional internal communication does not allow. Rather than relying on “step by step” methods, new digital tools give the necessary opportunity to go “network by network” and “work groups to work groups” in order to create common intelligence. This is precisely why Diplomatie was designed – for the sake of efficiency, collaboration and openness, and because the application of the ongoing digital revolution is perceived as urgent. Modernization of the public sector through digital means was quickly enforced at the highest level. By creating the interministerial web portal for diplomatic correspondence, the Ministry of Foreign Affairs of France wanted to open up access to some of the diplomatic network’s work while strengthening the security of communications.144 Allowing access to some of the diplomatic correspondence is part of the Ministry of Foreign Affairs’ general strategy aimed at making use of the advantages offered by digital technology to modernize its network and strengthen its international action. By successfully mobilizing its infrastructure, research and economic means to develop and implement Diplomatie, France made a step further in its – assumed – projection of soft power and diplomatic cultural influence.

The opportunities as well as the risks associated with the digital revolution have prompted a reform of the methods of producing and circulating diplomatic correspondence. After two years of

144 Nicolas Chapuis talks about Diplomatie at “Congrès International Pluridisciplinaire en Qualité, Sûreté de Fonctionnement et Développement”, March 22 2013
developments based on best practices for handling information on the digital networks, Diplomatie was launched. At the time of its introduction, it was the first unified network for interministerial communication in the diplomatic field. Its goal is to provide government officials and non-state actors with collaborative tools to produce and share their correspondence in a secure environment. A year and a half after its effective launch, Diplomatie can be considered as a successful “going digital by default” initiative. This success lies in its goals and comprehensive cycle of development. Qualified external figures – from all sectors interested in international action like the media, businesses, associations, and the research sector – are now able to access certain content at the invitation of diplomats within communities created for this purpose. As a result, it intensified the approach that has been adopted for some time now aimed at sharing the documentary resources of the French diplomatic network with the key actors and experts in international politics, in support of French economic diplomacy and diplomacy of influence. This access to diplomatic correspondence has been gradually opened up. Indeed, it primarily was the responsibility of ambassadors and directors to organize the data sharing communities through which the exchange of information would be as productive as possible for each of their members. The first communities were created during the second half of 2014. As of October 2015, the audience has been expanded for correspondence that is not classified; it relates to topics of general interest regarding which France’s diplomatic network provides analyses and comments that are worthy of being communicated to those who, in one way or another, provide their expertise and contribute to efforts to promote France’s international influence.

The Diplomatie portal is an open source project which integrates electronic document management in a professional social network. According to Nicolas Chapuis, this new platform presents significant advantages for the whole state administration in the following manner:

- It ranks diplomatic information, providing decision-makers with relevant information quickly, differentiating clearly between correspondence requiring action and other types of documents;
- It is at the same time a response suited to the needs expressed by administration employees and a productivity factor, thanks to its interministerial nature. The platform enables the registration of

---

145 These conclusions are based on the experience (participant observation) during two internships in 2014 at the French Consulate and Alliance Francaise in Cape Town
147 Interview, June 2 2014, Cape Town
real professional networks in *ad hoc* virtual spaces and modular communities, reduces email use, promotes easy accessibility via mobile devices and the sharing of information.

- It is an innovation factor: by welcoming in its opinion the innovative solution proposed by *Diplomatie*, the Interministerial Directorate for Information and Communications Systems (DISIC) invited the project’s partner administrations to show, both internally and externally, how the public administration is capable of exploiting the digital levers of modernization.

- It integrates the latest generation security equipment and software for information systems, including in terms of mobility, in liaison with the French Network and Information Security Agency (ANSSI).

French diplomatic services definitively putted an end to cables, unsafe emails and written memos: French diplomats are now sending “notes” via *Diplomatie*. The portal is a mix between Facebook, Twitter, LinkedIn, Google+ or Dropbox. Each diplomat has a profile to publish notes or remarks, to chat with colleagues using audio and video conference tools, to share declassified documents with the press, to create communities of interest while sorting information according to multiple criteria, to communicate sensitive information to other state administrations in a click and to browse in a pertinent manner all the available resources. In other words, *Diplomatie* is the direct answer to new emerging issues raised by the emergence of the “Web 2.0”. Rather than thinking the World Wide Web as a hard boundaries system, Web 2.0 tends to demonstrate that the Internet has multiple gravitational cores, just like the solar system. In this system, the Internet is seen as a participative and cost-effective platform where the user can control its own data. According to Tim O'Reilly, “hyperlinking is the foundation of the web. As users add new content, and new sites, it is bound in to the structure of the web by other users discovering the content and linking to it. Much as synapses form in the brain, with associations becoming stronger through repetition or intensity, the web of connections grows organically as an output of the collective activity of all web users.”

Another defining characteristic of the Web 2.0 era is that it is delivered as a service and not as a product anymore: Wikipedia succeeded to be Britannica Online, personal websites migrated to blogs, and blogs migrated to social network platforms offering free services like Facebook, Instagram, Twitter, etc. This fact leads to a number of fundamental changes in the business model, not only on the Internet but also in the non-digital world. This very difference between the physical

---

148 Interview, July 4 2014, Cape Town
149 O'Reilly, Tim (2005). Design Patterns and Business Models for the Next Generation of Software. Web Squared: Web 2.0 Five Years On
and digital environment forced governments to find new solutions and adapt their services to the new needs of the computer age. The need to modernize public action is pushing every level of government to look for new solutions. To build for the future, governments need a digital strategy that embraces the opportunity to innovate more with less and at a lower cost. The “going digital by default” strategy on which Diplomatie is based can be summarized in three major points.

- Enable the people and an increasingly mobile workforce to access high-quality digital government information and services anywhere, anytime, on any device.
- Ensure that as the government adjusts to this new digital world, citizen seize the opportunity to procure and manage devices, applications, and data in smart, secure and affordable ways.
- Unlock the power of government data to spur sharing, collaboration, innovation, bring new ideas and improve the quality of civil servants’ work (including diplomats).

A digital by default approach has many practical advantages for citizens: they can fill their taxes online, request a new passport directly from their personal computer, access their medical records from a smartphone, get a license, have a form signed or engage in direct and public talks with (local) government officials. Diplomatie's assigned mission was to take on the challenge all these issues while operating on an extremely sovereign perimeter. Indeed, diplomatic correspondence is by definition the private domain of the head of state and of its ambassadors. This upheaval was finally made possible four years after the first WikiLeaks worldwide scandal. The French government took quite a long time to implement a digital strategy for intergovernmental communication.

While the Diplomatie initiative can be qualified as a giant leap ahead, leaving traditional leaders like the United States behind, the French administration just recently filled a digital gap that existed for too long. From the early 2000s until 2012, the French government unsuccessfully tried to implement several digital strategies in order to modernize its large and world-dispatched administration. Audacious but costly, most of these projects never saw the day of light. Many reasons were invoked at the time: reluctant bureaucracy, lack of willingness, budget and time. A similar initiative led by the French Ministry of Defence was launched in 1996 and led to an unprecedented financial waste of public funds. Over a decade and until the program was fully operational, the Ministry of Defence had lost approximately half a billion euros in trying to unify its computing systems. Several audits and special commissions pointed out the lack of leadership, vision and cost-control. After such a

150 Nicolas Chapuis talks about Diplomatie at “Congrès International Pluridisciplinaire en Qualité, Sûreté de Fonctionnement et Développement”, March 22 2013
151 Interview, February 27 2015, Paris
discouraging achievement, there is no need to say that Diplomatie was closely scrutinized. In 2007,
following a senatorial report, the Quai d’Orsay opened its first digital consulate. Despite being
symbolic but quite successful, this last initiative remains marginal. Indeed, it is necessary and urgent
to make public action more efficient. Diplomatie was not developed to create quality, but to make
quality possible. In other words, the goal was not to create norms, but to set the means to achieve
quality, efficiency and security for a better public action.

4.1 Building and restoring legitimacy
The gap between “Internet time” and “government time” is widening. As the technology analyst
Larry Downes argued in his 2009 book The Laws of Disruption, information-age “technology changes
exponentially, but social, economic, and legal systems change incrementally.”152 His examples
ranged from copyright law, where bottling up published works is growing harder, to online privacy,
where personal information is flowing faster than the ability of the law to control it.
This section explains how public action is legitimate vis-à-vis the citizens and diplomats, and how it
can be measured. Many scholars and researchers still focus on the emerging part of the iceberg,
such as social media and communication, while very few lines have been written about the making
of internal procedures and policies. At the same time, the elaboration of external and internal digital
diplomacy which mainly consists in drafting confidential strategies remains a secret for almost
everybody, except for diplomats. In order to understand this paradox, we need to investigate the
core of diplomats’ job values and principles. Again, the internal/external distinction is crucial.
Diplomatie was created to address legitimacy issues in order to share the good source of
information generated by diplomats, but also to enhance their ability to work in an ever-changing
environment. Before elaborating the guidelines for the making of Diplomatie, Nicolas Chapuis –
former head of the Department of Digital Systems at the Ministry of Foreign Affairs – commissioned
a survey amongst two thousand French diplomats. The question was the following: “Are you happy
to go to work every morning?” Fifty percent of them answered “no” to this question and gave
various reasons for it: weariness, feeling of being overtaken, growing disrespect and suspicion from
public opinion, budget cuts, etc. In order to make public action legitimate again, governments need
to make sure that diplomats are happy to go to work every morning. According to Nicolas Chapuis,

152 Downes, Larry (2009). The Laws of Disruption: Harnessing the New Forces that Govern Life and Business in
the Digital Age, Basic Books
the second aim of Diplomatie is to “create smiles on faces and make the daily job more comfortable”. The second legitimacy issue focuses on interaction with public opinion. The main assumption is that public action will only be legitimate in society if society recognizes the state as a true network actor. Figures are simple: as of the second quarter of 2015, Facebook had 1.49 billion active users; Twitter had over 270 million. In October 2015, Google announced that more than fifty percent of search requests were made from a mobile device. As a matter of consequence, public institutions indisputably need to maintain and expand their presence on the Internet. They will otherwise create a preoccupying legitimacy gap. In their intriguing essay “The End of Hypocrisy: American Foreign Policy in the Age of Leaks,” political scientists Henry Farrell and Martha Finnemore suggest that damages coming from the WikiLeaks and Snowden scandals come not so much from any specific revelation, but because they “undermine Washington’s ability to act hypocritically and get away with it.” They argue that hypocrisy has been especially damaging to America’s soft power precisely because it is America: a nation that repeatedly seeks legitimacy through its ideals, like rule of law, democracy and free trade. If government actions undermine the law, democracy or free trade, the nation’s legitimacy is undermined too.

Once legitimacy is restored among citizens, diplomats and between citizens and diplomats, the question is how is it possible to assess and measure the efficiency of a modern digital diplomacy policy? French diplomat Nicolas Chapuis suggests two hypotheses. The first one is diplomats' global satisfaction. This indicator is easy to determine: the Ministry of Foreign Affairs just has to ask the question. In July 2015, a year after the launch of Diplomatie, the same internal poll “Are you happy to go to work every morning?” showed a significant increase in job satisfaction: the overall rating is now seventy-five percent (it was fifty percent the year before). The second one looks at global influence: if a government aims to develop a good relationship with an audience, it first needs to be “out there” and in the relevant public sphere. Diplomatic presence does not directly lead to a better image or favourable opinion, but without enough exposure, the public diplomatic strategy will ultimately fail. Traditionally, “presence” is realized mainly through mass communication, cultural exchanges or educational programs. The emergence of efficient transparency and digital

153 Interview, June 2 2014, Cape Town
154 Farrell, Henry and Finnemore, Martha (November-December 2013). The End of Hypocrisy. Foreign Affairs
155 Nicolas Chapuis talks about Diplomatie at “Congrès International Pluridisciplinaire en Qualité, Sûreté de Fonctionnement et Développement”, March 22 2013
communication extends the scope of diplomatic presence over space and time. In the digital age, presence-expansion becomes an even more critical condition for diplomats to make their voice heard. In other words, the credibility and authority of diplomats would very likely suffer if they fail to stay in touch with constantly changing digital technologies. Not only would their message not be heard, but they also would lose out to competing information campaigns.

Apart from these two hypotheses lies a third dimension: conversation-generating. One of the most appreciated features of the new public diplomacy is not only its engagement with the audience, but the sharing of information with this same audience. Good public diplomacy cannot be a pointless and boring monologue but must be dialogue-based. It has to facilitate a multidirectional communication between parties and to stimulate collaboration initiatives. Diplomatie, thanks to its interactive feature, has much to offer in this regard as it can generate a quasi-continuous dialogue between diplomats and foreign publics. This also allows diplomats to readjust the focus of their agenda, reduce misinformation and enhance mutual understanding. It is this particular feature that enables social media to realize the goal of public diplomacy in a different way from traditional methods. At the same time, social media is not necessarily easy to use as a tool of public diplomacy. In fact, it might involve even more human resources and financial investment than traditional media-based tools as its objectives, methods and operations require a complex digital infrastructure and well-trained staff to carry out the missions. Again, this is where diplomats' happiness and efficiency meet these crucial legitimacy issues. This last point is particularly important as it goes to the heart of the argument about the transformative role of communication and information sharing in foreign policy in general and in public diplomacy in particular.

With Diplomatie, France now has the means to create, digest and dispatch enough diplomatic intelligence to better capture the narrative flow of world affairs – and make the best out of it. It is also a necessary and unquestionable vector of influence. As described in the first chapter, there is a growing appetite for governmental information: public opinion, businesses, non-governmental organizations want to read diplomatic correspondence. Furthermore, it is more than essential that citizens to know about what their diplomats really do behind their desks. Eric Herrouin, former Deputy Consul of France in Cape Town, declared in July 2014: “I have to justify and explain what I do every single day. Many people still believe diplomats only eat Ferrero Rocher and party thanks to taxpayers' money: this is why it is vital to explain what we really do here.” Since digitized

156 These conclusions are based on the experience (participant observation) during two internships in 2014 at the French Consulate in Cape Town
information is easy to manipulate and search, since it can be shared with many people simultaneously, and since it can reveal so many useful things, many people should be able to benefit from it as a kind of public good.

The notion of power also lies in accordance with the legitimacy principle. Indeed, there is a great disparity between states when speaking about digital diplomacy: it is regrettable to see that some countries are still in the 20th century, even if some fragments of these states have already embraced the digital revolution. Diplomatie also intends to lead by example and to encourage new and audacious initiatives in the digital sector. Therefore, the other challenge is to make sure that states will successfully adopt digital strategies to fit into the 21st century. More than ever, people want information to break free: a diplomatic outpost producing a thousand – valuable – cables per year should be able to make this information available to more than the three government officials who may be concerned. This “information overdose” is common to many foreign services around the world. Dolana Msimang, former Ambassador of the Republic of South Africa to France, confirmed this assumption. Diplomatie was also designed to reduce the amount of data that diplomats and officials cannot digest and to focus on the qualitative aspect of diplomatic correspondence. Diplomatie, by seeking efficiency and quality, answers that equation: expanding readership is expanding influence – and by that mean, legitimacy.

157 Interview, February 27 2015, Paris
### 4.2 Diplomatie in action

During the making of *Diplomatie*, a comprehensive study on the goals and expectations was elaborated. It starts with two basic assumptions: innovation and interministeriality, the two pillars, while connectivity, mobility and security are the three imperatives (see figure below).

![Figure 6. The Diplomatie principles](image)

#### 4.2.1 Connectivity

As explained in the second chapter, the Web 2.0 revolution has constituted the explosion in popularity of the recently developed social media platforms that led to an increased digital connectivity but also a heavy reliance on electronic applications in many areas of human activity. The Web 2.0 describes World Wide Web sites that emphasize user-generated content, usability, and interoperability: standardization, usability and participation are key-terms. Although Web 2.0 suggests a new version of the World Wide Web, it does not refer to an update to any technical specification, but rather to cumulative changes in the way Web pages are made and used. Examples of Web 2.0 include social networking sites, blogs, wikis, folksonomies, video sharing sites, hosted services, Web applications, and mashups. The inherent benefits of the Web 2.0 revolution for “digital diplomats” include the assistance and speed in connecting them – and between them – with the wider public during their postings, to listen to how policies are perceived or received on the ground or how bilateral relations are understood. On a more internal level, France is not the only country launching a professional diplomatic platform. Diplopedia, billed as the Encyclopedia of the
United States Department of State, is a wiki running on a state internal Intranet, called “OpenNet”. It houses a unique collection of information pertaining to diplomacy, international relations, and Department of State tradecraft. The wiki may be used by United States foreign affairs agencies domestic and abroad with state intranet access. It is not open to the public. Congressional testimony from Jimmy Wales, the co-founder of Wikipedia, notes the difference between vertical and horizontal information sharing and suggests that Diplopedia could be a successful e-government endeavour as it is an excellent example of sharing information horizontally across agencies. The Diplomatie platform goes even further by creating the notion of virtual communities (an embassy equals a community). By that mean, diplomats are no longer passive in the treatment of information: they also actively participate in the making of a common and sometimes public database of knowledge and fact books. For more than a hundred years, French foreign affairs ministers have been complaining about the increasing volume of incoming information. In 1934, Joseph Paul-Boncour even sent a message to each of his ambassadors, declaring: “Stop spamming me, or I’ll make you pay for these telegrams you’re sending over!” Until July 2014, the central administration of the Ministry of Foreign Affairs of France in Paris was receiving more than a thousand cables per day. Only three of them were supposed to be read by the President. Under the authority of the chief of staff, three diplomats were working full-time to read, prioritize and dispatch this overwhelming quantity of information. Traditional cables were used for almost everything: political notes, cultural agenda, accounting, and even private requests regarding career advancement. From the very beginning, Diplomatie was designed to “re-sacralise” the notion of the “diplomatic cable” and compile the entire production of diplomatic intelligence coming from the Quai d'Orsay. All the steps are covered, from production, sharing and archiving through professional social networks. Such networks originated in the private sector. Many major corporations and businesses adopted it from 2006: Apple, Samsung, Total, Dassault, etc. Traditional secure messaging like emails do not provide the advanced features available today to ensure de-compartmentalization and information management; Diplomatie now provides appropriate means

158 A wiki is a website which allows collaborative modification of its content and structure directly from the web browser. For example, the encyclopedia project Wikipedia is by far the most popular wiki-based website in the world
159 Wales Senate Testimony regarding “E-Government 2.0: Improving Innovation, Collaboration, and Access” U.S. Senate Committee on Homeland Security and Governmental Affairs, December 11 2007
162 Nicolas Chapuis talks about Diplomatie at “Congrès International Pluridisciplinaire en Qualité, Sûreté de Fonctionnement et Développement”, March 22 2013
for diplomats who operate in a network and regardless of place or time. The diversity of the topics and the very nature of interministerial missions require a collaborative and cooperative network: the 14 000 agents connected to the portal are free to build virtual work spaces, optimize and share knowledge databases for which they are responsible. *Diplomatie* clearly follows a constructivist approach of knowledge-building: as the social construction of knowledge and social reality are the common ground of social constructivism, *Diplomatie* proposes that online environments should support multiple perspectives or interpretations of reality, knowledge construction, and context-rich, experience-based activities.

A “connected” and dematerialized network is vital for diplomats. Most embassies around the world use a local Intranet to communicate and share data. Stasis and inflexibility are the main problems of an Intranet system, simply because they are based on a hierarchical organization chart which does not help to de-compartmentalize the outpost structure: horizontality and transversality are – so to say – non-existent.

In order to share data and information, *Diplomatie* uses “tags”, or “keywords” based on metadata. In other words, the system uses the same methods as Google or as a social network like Facebook, from which *Diplomatie* claims its origins, philosophy and operating methods. Once the *Diplomatie* account clearance is obtained from the Ministry of Foreign Affairs, the diplomat is enlisted in the “workgroup” corresponding to its posting (for example French Consulate in Cape Town). The community director (the Consul in this case) then assigns a level of protection (Public or Restricted) and digital signature abilities on behalf of the group. As this group function includes social tools (audio and video chat, access to wikis and blogs), the diplomat can start producing and reading diplomatic correspondence. The agent is free to solicit subscriptions to “Communities of Interest”, which are organized according to international issues (for example “South Africa”, “terrorism”, “Ebola”, etc). More than two hundred communities have been opened since July 2014. These subscriptions give the diplomat rights to know more about the correspondence published on the network. Requests are approved by the director of the requested community. Groups and communities show “labels” that automatically capture all marked correspondences; every additional correspondence or “notes” now replace traditional and unsafe emails. Notifications are pushed to the platform in two different ways. The “For information” label informs the diplomat that a new message has been posted on the group. The “For action” label requests the diplomat to

163 Two types of metadata exist: structural metadata and descriptive metadata. Structural metadata is data about the containers of data. Descriptive metadata uses individual instances of application data or the data content
perform a special task or answer an assigned question. This system therefore allows effective prioritization, as well as follow-ups: everyone can now monitor projects' progression in real time. It is important to note that despite its core values of openness, Diplomatie still remains under a strict control: it is not possible to access the platform without the direct agreement coming from the relevant authority.\textsuperscript{164} In other words, Diplomatie can be seen as a semi-open platform where a clearance remains necessary. In order to ensure interministeriality, a collaborative mode is also available: by this mean, an embassy can co-write or amend a document hand in hand with another governmental administration or agency. For example, the defence attaché can now communicate directly with its ministry while keeping its ambassador “in the loop”. Digital and authenticated signatures are available for every diplomat. Nicolas Chapuis described emails as “the most invasive and pollutant tool ever designed.”\textsuperscript{165} A 2013 internal study demonstrated that French diplomats can spend up to three hours per day working on emails, while they spend only twenty minutes in meetings. Diplomatie is therefore not only a powerful communication tool, but also a factor of re-socialization between diplomats.

Diplomatie was partly inspired by Diplopedia, a wiki running on the United States Department of State Intranet. It houses a unique collection of information pertaining to diplomacy, international relations, and Department of State tradecraft. This wiki provides so much flexibility that several offices throughout the community are using it to maintain and transfer knowledge on daily operations and events. Just like Diplomatie, anyone with access to read it has permission to create and edit articles after registering and acquiring an account with Diplopedia. Since Diplopedia is intended to be a platform for expressing the various points of view of the Department, Diplopedia does not enforce a pure neutral point of view about policy. Instead, viewpoints are attributed to the offices and individuals participating, with the hope that a consensus view will emerge. Positions or views in an article that do not fairly represent the consensus of the relevant community of interest are to be clearly marked with the author, office, or agency whose views they represent. In January 2009, Diplopedia was among 27 online technologies named as "The Best Government Tech of the Bush Years" by Wired Magazine.\textsuperscript{166} Despite its huge success (more than five thousand contributors

\textsuperscript{164} These conclusions are based on the experience (participant observation) during two internships in 2014 at the French Consulate and Alliance Française in Cape Town
\textsuperscript{165} Nicolas Chapuis talks about Diplomatie at “Congrès International Pluridisciplinaire en Qualité, Sûreté de Fonctionnement et Développement”, March 22 2013
\textsuperscript{166} Thompson, Nicholas (January 27 2009). The Best Government Tech of the Bush Years. Wired. Retrieved February 5
and twenty thousand articles since September 2006), Diplopedia remains extremely closed compared to Diplomatie; its structure is also much more vertical and the sharing of information between several other federal agencies' wikis (Intellipedia for the Central Intelligence Agency, Bureaupedia for the Federal Bureau of Investigation) remains quite limited at this stage.

4.2.2 Mobility
“From now on, French diplomats will be connected. I want them to be reachable, regardless of time or location. Even on the back of a camel, in the middle of Sahara desert!” joked Foreign Affairs Minister Laurent Fabius. Diplomatie is the first “state cloud”: this notion involves a complete dematerialization of the job. As international negotiations are becoming denser and nomadic, the days when ambassadors or consuls were glued to their office are gone.

Diplomatie “look and feel” adopts a portable interface: a search bar and three main icons (Documents, Groups and Profile) make the platform tablet and mobile ready (please refer to the illustration below).

---

2009

167 About Diplopedia: http://www.state.gov/m/irm/ediplomacy/115847.htm
Figure 7. Screenshot of the early web version of Diplomatie. The search bar is at the top; the three buttons “My desktop”, “My communities” and “My public profile” are intended to provide a user-friendly experience.

The notion of “work station” has completely disappeared: the diplomat 2.0 is now mobile-ready. Ambassadors, consuls and top officials all have a modified and encrypted Android latest generation tablet to access their digital workspace at all time. Cryptographic tools and Virtual Private Networks guarantee the highest standards of data protection. Diplomatie is not available on Apple devices as this platform is closed-source and based on the “security through obscurity” principles that could cause major software vulnerabilities.

169 These conclusions are based on the experience (participant observation) during two internships in 2014 at the French Consulate in Cape Town.
Figure 8. An example of mobility: the specially-modified Samsung Android Tablet with “Cryptosmart” software. Please note the first applications displayed on the screen (from right to left): Diplomatie, Diplonet (the Ministry’s intranet), Elise (traditional secured email service) and Ariane (a free portal provided by the Crisis Centre established by the Ministry of Foreign Affairs of France. Travellers can share data about their travels abroad). As of July 2015, all these services have been merged with Diplomatie.

4.2.3 Security
On July 15th 2014, The Guardian published an article “Germany may revert to typewriters to counter hi-tech espionage.” This topic is closely related to cyber-war and cyber espionage. In other words, how do we make sure that diplomats are using the most secure means of communication? According to Marc Saint-Criq, former head of the Regional Technology Support Centre based at the Embassy of France in Pretoria, perfect software and hardware protection against threats, attacks and data theft is nearly impossible to guarantee. On the other hand, there are simple and reliable ways to improve and reduce these risks. The first one is to prevent physical intrusions: closing every office door, using a strong login password and military-developed hard drive encryption is now a common practise amongst French diplomats. In the wake of the Stuxnet affair, the use of simple and common devices such flash drives has been completely forbidden. In 2013, a former intern at the French Consulate in Cape Town had to suffer the consequences of the new policy after he

170 Interview, July 11 2014, Cape Town
plugged his personal and virus-infected flash drive on his office computer. After detecting the infection in real-time and being put under maximum alert for six hours, the Pretoria Regional Technology Support Centre sent a vehement message to all French civil servants in Southern Africa, reminding the potential security disaster that could have occur.\textsuperscript{171}

The second way to reduce security threats lies in the philosophy, the strategy of digital protection itself. While the principle of “security through obscurity” remains a standard among governments\textsuperscript{172}, the Ministry of Foreign Affairs of France decided to lead the way and develop its brand new professional network based on open standards and adopting a “secure by design” scheme, as described by David Wheeler\textsuperscript{173}. This concept assumes that software has been designed from the ground up to be secure. Malicious practices are taken for granted and care is taken to minimize impact when a security vulnerability is discovered or on invalid user input. Generally, designs that work well do not rely on being secret: it is the Linux – and more generally the open-source conception of how software should be assembled, compiled and distributed. This no-secrecy principle is not mandatory, but proper security usually means that everyone is allowed to know and understand the design because it is secure. This has the advantage that many people are looking at the code, and this improves the odds that any flaws will be found sooner. This conception does also mean that attackers can obtain the source code, which makes it easier for them to find vulnerabilities as well, even if they can be corrected almost immediately. According to Nicolas Chapuis, former head of the Department of Digital Systems at the Ministry of Foreign Affairs of France, confidentiality remains the basis of each diplomatic correspondence, but with a different approach: a diplomat will not talk about classification of documents, but about their protection.

The distinction between classification and protection is indeed fundamental: all diplomatic outposts are supported by computer information systems. These systems enable missions to carry out their missions and account for their resources. With computer networks and information systems comes security risk: sensitive data can range from information pertaining to states secrets, information associated with managing financial resources or data regarding emergency preparedness. If this type of sensitive information were inappropriately disclosed, browsed, or copied for improper or criminal purposes, it could be used to disrupt critical government operations such as those supporting homeland security, financial services, public safety or emergency services. Following the

\textsuperscript{171} Interview, July 11 2014, Cape Town
\textsuperscript{172} Schneier, Bruce (2002). Secrecy, Security and Obscurity & The Non-Security of Secrecy
WikiLeaks’ scandal, security incidents involving this form of sensitive data can undermine any diplomatic service resulting in diminished confidence and impact on current operations. The Ministry of Foreign Affairs of France defines the term “Restricted” as “protected information that affect the national interest or the conduct of governmental activities but that has not been specifically authorized to be kept secret in the interest of national defence or foreign policy.”

Although unclassified, “restricted content” may not be appropriate for public release and could possibly embarrass public officials if inadvertently released.

In order to innovate without compromising on the required standards of protection, constant attention was given to secure access while ensuring that once connected, diplomats should be able to work unhindered. To prevent any leaks, national security institutions within governments logically take steps to self-fortify. This might include more physical defences – like fences – and more cyber defences – like firewalls. But today, many social engineers tend to consider human loyalty as the greatest threat for data security, integrity and confidentiality. Precisely, Diplomatie was developed based on new rules and uses: the experience attests that security is stronger when it contributes to meeting the need of sharing and not just the right to know. After WikiLeaks, “let’s now feed the beast” could easily be the new motto of Diplomatie: rather than having quality and useful information leaked by reprehensible means, let’s try to share it. For a simple reason: the digital landscape does not make leaks happen, but it enables them to happen on a worldwide scale. Once information is out, it is simply not possible to burn some files and make the leak go away. This makes the digital landscape scary for governments, and for good reasons. In addition to the speed and scale of their spread, leaks of all kinds – big and small – can do damage. Edward Snowden proved that leaking sensitive information can start a chain reaction of unexpected circumstances.

From the very beginning, Diplomatie was developed internally with a 3 million euros budget. Several private contractors took part in the project. Diplomatie’s infrastructures rely on two massive data centres. The main one is located in an underground and secretly-kept location in Paris. The backup data centre is located in the western part of France, in Nantes. According to Marc Saint-Criq, former head of the Regional Technology Support Centre based at the Embassy of France in Pretoria, the Ministry of Foreign Affairs is a daily target for hackers: authentication through passwords,
certificates and high-level encryption is therefore required.\textsuperscript{176} Developed thanks to open-source software, \textit{Diplomatie}'s “secure by design” do not rely on being secret: in opposition to the principle of “security through obscurity”, everyone is allowed to know and understand the way it works. In other words, its source code remains open: this has the advantage that many people are looking at the code to improve the software and by that mean reduce vulnerability risks. Being extremely light-weight and flexible, \textit{Diplomatie} works on every computer, Android tablet or mobile phone, as long as the user of the device holds a valid and encrypted certificate from the Ministry of Foreign Affairs that proves the device “sane” and secure.

Every document produced by the Ministry is protected per nature. \textit{Diplomatie} deals with only two levels of information protection (public and restricted) while the French Ministry of Defence, intelligence agencies and the highest executive branches use a six scale classification system (public, restricted, confidential, secret, top-secret, very top-secret). Terminology is very important: while classification implies a strict application of the CIA principle (data Confidentiality, Integrity and Availability), protection aims to control the access to information that might result in loss of an advantage or level of security if disclosed to others. \textit{Diplomatie} is therefore not designed to create and share classified information. French diplomatic top-secret and very top-secret correspondence only represents one percent of the Ministry’s correspondence: this data is managed by another system and remains totally secret. It is easy to argue that such a “parallel system” could make \textit{Diplomatie}'s ideals of openness extremely theoretical and overestimated. The official position of the Ministry of Foreign Affairs of France is clear on this issue: “This special channel is exclusively dedicated to classified information, not “protected-only” information. \textit{Diplomatie} fits well with the transparency, but not secrecy principle. And secrecy we still need. For legal and security reasons, this kind of sensitive information cannot use the same networks to reach the ministry, the government and the presidency. Furthermore, \textit{Diplomatie} aims to be the only platform to gather as much information as we can: it was designed to handle the whole French diplomatic correspondence and close the multitude of Internet services we had before. Our information system was rationalized to its best in order to reduce bureaucracy and inefficiency in the treatment of data: \textit{Diplomatie} is working very well in this field. No one wants to recreate the messy alternative channels we were using.”\textsuperscript{177}

\textsuperscript{176} \textit{ibid}
\textsuperscript{177} These conclusions are based on the experience (participant observation) during two internships in 2014 at the French Consulate in Cape Town

Page 86
Answering how *Diplomatie* could eventually prevent other governments' agencies (National Security Agency, Central Intelligence Agency, Federal Security Service of the Russian Federation, also known as FSB, etc) to spy on French diplomats' activities, Marc Saint-Criq answered in a smile: “We cannot be a hundred percent sure that our new system will prevent or deter other governments to spy on us. But *Diplomatie* will make their job way more complicated as information is now centralized on a single cloud server, and not dispatched on thousands of computers. I do not really care if the Americans are spying on us, as we do the same thing and already share top-secret information between allies. On the other hand, countries like China or Russia could present other problems, not to use the word “threats”. But we just do not want another Snowden to publish our protected information.”}

178 These conclusions are based on the experience (participant observation) during two internships in 2014 at the French Consulate in Cape Town
4.3 Critics
A year after the introduction of Diplomatie, the final assessment is very positive. Following a short survey made at the French Consulate in Cape Town in August 2015, more than eighty percent of the respondents declare themselves satisfied in the day-to-day use of Diplomatie.\textsuperscript{179} However, it appears that the transition went slower than expected, something facing reluctance among the personnel. First of all, the transition process to Diplomatie left no choice but to leave the old and existent system behind all of the sudden. Indeed, the Schumann system was declared outdated and unavailable the day Diplomatie was introduced. Even if the appropriate training had been provided, all civil servants did not react the same way. Some of them were reluctant to change from an operational – yet heavy – system to a new one that was announced to be revolutionary from the very start. Complaints about the search engine and the general interface rapidly emerged. According to Marc Saint-Criq, these “youthfulness” issues have been fixed in the months following the launch of Diplomatie. The first and maybe most violent reaction was “look and feel” related: some diplomats simply did not appreciate the general interface of the web-based version, finding it too “minimalist”. Indeed, several unnecessary manipulations were required to execute a routine task such as sending a note to a colleague. The second critic regarded the search engine. As previously described, Diplomatie adopts a “Google” interface, namely a search bar and three icons to launch the desired services. Diplomatie’s search engine proved to be quite unpredictable during the first few months after its launch: the tolerance to misspellings was indeed very low. The software was not able to associate simple requests and to make the link between two different spellings or formulations: “Embassy of France in South Africa” would not be automatically associated with “French Embassy in Pretoria”. This misconception and lack of coherence led to some frustrating experiences. Nevertheless, these defects were quickly corrected. The next sub-chapter will be dealing with the possible replication of Diplomatie at an African scale; indeed, if Diplomatie is useful as a benchmarking tool for France (and for France only), it should not be taken as the only one example.

\textsuperscript{179} These conclusions are based on the experience (participant observation) following two internships in 2014 at the French Consulate and Alliance Francaise in Cape Town
4.4 Diplomatie and Africa’s progressive digitalization

If Diplomatie works well, it is mainly because France has the financial and technical means to undertake such radical changes in the field of state digitalization. It is therefore interesting to look at the potential of similar projects from an African perspective. For Africa, where diplomacy is one of the – if not the – most viable instrument(s) of foreign policy and where security concerns have long since transcended the traditional state-centric paradigm, such reflection is of strategic importance. Indeed, there is an emerging digital diplomacy in Africa, although government efforts remain quite rare and unequal.

As described in chapter 2.3.2, the digital divide affects the rate of Internet penetration among a given country but also its diplomatic services. The digital divide refers to inequality in access to, or ability to use, information and communication technologies. In Africa, the digital divide mostly relates to states’ lack of technological infrastructures and finances to build and maintain such costly installations.

While some African countries have narrowed this gap in recent years, such as Kenya that has an internet penetration rate of 47.3 percent, other African countries still lag behind the rest of the world. Being Kenya’s direct neighbour, Ethiopia presents the singularity of having one of the lowest penetration rates in the world with 3.7 percent. By comparison, South Sudan, which lacks the most basic government services, has an internet penetration rate of 15.9 percent. There are only ten countries with lower internet penetration than Ethiopia. Most of them, such as Somalia and North Korea are handicapped by decades-long civil wars or completely sealed off from the outside world. Such is also the case with the Ivory Coast (4.2 percent penetration), Eritrea (5.9 percent) and Rwanda (9.0 percent). As a whole, Africa has a penetration rate of 26.5 percent as opposed to Europe’s 70.5 percent and 87.7 percent in North America. Leading economies in Africa reveal a preoccupying digital gap: Nigeria has a penetration rate of 8.3 percent while South Africa stays in the low average with 23.7 percent. Nevertheless and for the greater good, all African governments in Africa can access the Internet could possibly finance the use of social media tools. This may explain recent findings indicating that African Ministries of Foreign Affairs are sometimes as active on Twitter and Facebook as their peers from other parts of the world.

The lack of basic infrastructures is not the only reason for such low penetration rates: the spectre

180 All statistics come from the Internet World Stats website. http://www.internetworldstats.com
of state surveillance is also very present. In October 2015, the New York Times reported that the Ethiopian and Moroccan intelligence services have targeted journalists and political opponents with invasive systems that allow the government to collect their information, remotely activate computers’ camera and microphone, record keystrokes, and monitor online activity.\textsuperscript{181}

The knowledge gap is also preoccupying: digital and computer literacy differs from a place to another, from a generation to another. Even if online environments enable large amount of people to benefit from the Internet’s resources, digital capabilities are required. Populations leaving without such knowledge and digital tools are unfortunately condemned to be left behind. On the other hand, it is possible that richer nations who have been online for longer durations and whose staff is more familiar with digital environments will be more capable to analyse big data: in this case, the gap could also extend to diplomats themselves and slow down the increasing digitalization of Africa.

Specific plans of digital training may aid in bridging the digital divide. Specific budgets and well-trained civil servants are more than needed to lead and determine a modern and effective digital strategy. They should then analyse their ministries’ capabilities and move to reduce possible gaps through intensive training and accompaniment of diplomats now venturing online for the very first time.

Chapter 5 – Conclusions

Based on the results from data analysis and findings of the research, this study has revealed that digital diplomacy is not an emerging tool anymore: rooted in society, it will continue to be an evolving dynamic to promote accountability and openness to the people: these two principles are the sole conditions to make “diplomacy of action” a reality.

Firstly, it was observed that digital diplomacy is not a utopic dream anymore: as social media and the extensive use of the Internet have become indispensable, diplomatic structures – as well as diplomats themselves – tend to embrace the digital revolution through the use of information and communication technologies like blogs, Facebook, Twitter and YouTube that enhanced citizen participation. In the online environment, many of the same dynamics are at work. Because these networks are enabled by information technology, they also have a different relationship to space. In a digital network, information is both abundant and evolving at an increasingly fast pace. News of world events has become a commodity, and the evolution of ideas, ideologies, beliefs, and politics is happening almost in real time. Software programs, group behaviour, and individual action are all adapting to a world of massive real-time data flows and what is amounting to a new pace of evolution. Groups like Anonymous thrive in this instability and uncertainty and can take advantage of the traditional actors who require predictable knowledge of the future to remain powerful.

The national security risk posed through hacking, cyber-espionage and other cyber-space attacks poses great risks to government in losing vital and secret information: this issue needs to be addressed at an international level.

Secondly, it was observed that the notion of secrecy did not die, but rather evolved to fit our digital age. Improvements are more than necessary in this field: the constructivist approach posits that international dynamics are historically and socially constructed rather than purely a function of either human nature or state power. Technology became pervasive enough for most people to use Internet-connected devices and citizens willingly (if not always consciously) exchanged their personal data for free online services. The same technological system that empowers people to disrupt traditional and state institutions has been shown to be incredibly effective at providing the backbone of a surveillance state. When Edward Snowden showed the extent, breadth, and audacity of the United States surveillance empire, he wasn’t just revealing a program he saw as unconstitutional or unethical. He was providing the data required to understand how the United
States government had chosen to respond to the challenges of digitally empowered actors. Just as the Syrian government had chosen to use digital networks as a domain to control, the United States government had, in a post 9/11 state of panic and fear, decided to exert power over the network itself. As Edward Snowden said: “These programs were never about terrorism: they’re about economic spying, social control, and diplomatic manipulation. They’re about power.”

Thirdly, and in order to bring an appropriate response to the WikiLeaks and Snowden scandals, governments started to act. By introducing an innovative, mobile, open-source and secure communication platform for diplomats and civil society actors, France – in an unexpected and surprising move – decided to step into the 21st century. Knowledge management, horizontality in the sharing of information are slowly being implemented. At the start of a potentially long struggle for relevance and legitimacy, states will have to choose between seeking absolute control and giving up some power in order to preserve, and hopefully enhance, the new digital order.

Areas of further research that were identified include law enforcement and the fight against cyber-crime that hinders digital diplomacy. Crucial further research should be done to explore new techniques and procedures that will enhance the process of digital diplomacy such as dedicated internet speeds that will ensure reliability and efficiency, especially in African countries.

Five hundred years ago, Johannes Gutenberg introduced modern book manufacturing in Europe. It is still widely considered as one of the most important revolutions in history. Books spread across the Old Continent, shattering information management. For the first time, citizens were given the opportunity to question the official discourse made of political and religious intolerance. This upheaval led to two centuries of civil wars and forced about six hundred thousand French Huguenots to leave their country because of their religious and philosophical beliefs. Many of them immigrated to South Africa.

Eleven years ago, a Harvard sophomore created a silly Internet program to rate classmates on campus and later founded a forty billion dollars empire: digital networking was born. It did not only change the way people communicate: it enabled the citizens to conquer a new space of social,

182 Snowden, Edward (December 17 2013). An Open Letter to the People of Brazil. Folha de S. Paulo
cultural, political and economic expression. Without a doubt, the advent of social media is responsible for the most important innovation in diplomacy since the cable wire. The utility of digital diplomacy in managing change will be reflected not in the numbers of diplomats using the appropriate tools but what the tools allow diplomats to accomplish. Outcomes, in other words, represent the future of digital diplomacy and will determine whether it lives up to its significant and exciting promise: to keep governments open.
References and bibliography

Books
• Bellanger, Pierre (2012). *De la souveraineté numérique*. Le Débat, #3, p. 152
• Bonnot de Mably, Gabriel (1746). *Droit public de l’Europe*. PUF, Paris
• Collins, Sean and McCombie, Stephen (2012). *Stuxnet: the emergence of a new cyber weapon and its implications*, *Journal of Policing, Intelligence and Counter Terrorism*, 7:1, 80-91
• De Tocqueville, Alexis (1835). *De la démocratie en Amérique, deuxième partie, chapitre IV, De l’association politique aux États-Unis*. Presses de France
• Ferguson, Niels and Schneier, Bruce (2004). *Practical cryptography*. Vuibert, p. 338
• Heine, Jorge, Andrew F. Cooper, Ramesh Thakur (2013). The Oxford Handbook of Modern Diplomacy. United Kingdom, Oxford University Press
• Madanmohan Rao (1999). Internet Governance: The struggle over political economy of cyberspace
• O'Reilly, Tim (2005). Design Patterns and Business Models for the Next Generation of Software. Web Squared: Web 2.0 Five Years On
• Rid, Thomas and Hecker, Marc (2009). War 2.0: Irregular Warfare in the Information Age. Westport, Praeger
• Rid, Thomas (2013). Cyber War Will Not Take Place. Oxford University Press

Page 95
• Show, Nancy (2010). *From the CNN Effect to the Twitter Effect*. Routledge. p. 97-104
• Schneier, Bruce (2002). *Secrecy, Security and Obscurity & The Non-Security of Secrecy*
• Thierer, Adam (2003). *Who Rules the Net?: Internet Governance and Jurisdiction*. Cato Institute
• Ventre, Daniel (2011). *Cyberwar and Information Warfare*, Willey-ISTE
• Ziemkendorf, Mario (2007). *Actor Network Theory*. Druck und Bindung Publishers, Norderstedt Germany

**Journal articles**

• Ball, James; Schneier, Bruce; Greenwald, Glenn (4th October 2013). NSA and GCHQ target Tor network that protects anonymity of web users. *The Guardian*
• Bamford, James (March 15 2012). The NSA Is Building the Country’s Biggest Spy Center (Watch What You Say). *Wired Magazine*
• Dean Cheng (May 23 2013). China Renews Cyber Attacks Against U.S. *Heritage Fondation Journal*
• Dean Cheng (February 23 2013). Chinese Cyber Attacks: Robust Response Needed. *Heritage Fondation Journal*
• Dean Cheng (May 29 2013). China Hacks U.S. Defence Department. *Heritage Fondation Journal*
• De La Chapelle, Bertrand (2012). Gouvernance Internet: tensions actuelles et futurs possibles, *Politique étrangère, n° 2*
• Dredge, Stuart (November 5 2013). What is Tor? A beginner’s guide to the privacy tool. *The Guardian*
• ElBaradei, Mohamed (April 21 2011). Wael Ghonim: Spokesman for a Revolution. *Time Magazine*
• Eriksson, Johan and Giacomello, Giampiero (July 2006). The Information Revolution, Security, and International Relations. *International Political Science Review Vol. 27, No. 3*, pp. 231
• Farrell, Henry and Finnemore, Martha (November-December 2013). The End of Hypocrisy. *Foreign Affairs*
• Fletcher, Joe (November 15 2015). French Ambassador Slams Trump Over Viral Tweet About France’s Gun Laws. *Addicting Info*
• Gomart, Thomas (2013). De la diplomatie numérique. *Revue des Deux Mondes*
• Green, Stephanie (November 6 2014). Don’t Call Him the Gay Ambassador: Gérard Araud, France’s Head Envoy to the U.S., Wants to Bring Diplomacy into the 21st Century. *Vogue Magazine*
• Guaino, Henri (February 27 2011). “La politique étrangère de la France”. *Le Monde*
• Guzzini Stefano (2000). A reconstruction of Constructivism in International Relations, *European Journal of International Relations, vol.6, n°2*
• Halliday, Josh (November 22 2010). Tim Berners-Lee: Facebook could fragment web, *The Guardian*
• Hanson, Fergus (March 2012). Revolution @State: The spread of ediplomacy, *Lowy Institute for International Policy*
• Hawke, Jack (April 23 2010). Internet Underground Takes on Iran. *MSN 9News*
• Hocking, Brian and Melissen, Jan (July 2015). Diplomacy in the Digital Age. *Netherlands Institute of International Relations Clingendael*
• Hughes, Stuart (May 24 2013). Digital diplomacy: here to stay and worth the risk? *BBC Blogs*
• Jilo Ipu, Christopher (2013). E-diplomacy In East Africa: Case Study Of Kenya, *University of Nairobi*
• Krotoski, Aleks (April 24 2014). Andrew Lewman on Tor and anonymity online. *The Guardian*
• Lamothe, Patrice and Gomart, Thomas (June 7 2011). Internet n’a pas à être “civilisé”. *Le Monde*
• Landers, Chris (April 2 2008). Serious Business: Anonymous Takes on Scientology (and Doesn’t Afraid of Anything). *Baltimore City Paper*
• Liat, Clark (12th August 2015). WikiLeaks crowdfunding €100,000 reward for TTIP secrets, *Wired*
• Maclean, William (September 25 2010). Iran “First Victim of Cyberwar”. *The Scotsman*
• Martin, Todd (February 2 2001). Virtual Diplomacy. *Canada: A Student Journal of International Affairs, Volume 2*
• McCarthy, Kieren (July 1 2005). Bush administration annexes Internet. *The Register*
• Moses, Asher (February 10, 2010). Hackers bring down government websites. *The Age*
• Mueller, Milton (September 17 2011). India, Brazil and South Africa call for creation of “new global body” to control the Internet. Internetgovernance.org. Accessed on November 24 2015
• Nocetti, Julien (May 2011). La diplomatie d’Obama à l’épreuve du Web 2.0, *Politique étrangère*
• Nossel, Suzanne (April 12 2012). Smart Power. *Foreign Affairs*
• Pearce, Matt (April 8 2014). Edward Snowden: “I am not anti-secrecy. I’m pro-accountability”. *Los Angeles Times*
• Petallides, Constantine J. (2012). Cyber Terrorism and IR Theory: Realism, Liberalism, and
Constructivism in the New Security Threat. Student Pulse, Vol. 4, No. 3, page 1

- Renard, Hervé (May 10 2010). Bernard Kouchner, défenseur d’un “Internet universel et ouvert”. *Le Nouvel Observateur*
- Rogin, Josh (January 13 2012). Meet the U.S. Ambassador to Russia, Michael McFaul. *Foreign Policy*
- Slaughter, Anne-Marie (January-February 2009). America’s edge : Power in the networked century, *Foreign Affairs*
- Snowden, Edward (December 17 2013). An Open Letter to the People of Brazil. *Folha de S. Paulo*
- Solon, Olivia (January 7 2011). Does the Internet need to be civilized? *Wired Magazine*
- Wankiku, Rebecca (September 9 2014). Kenya increases e-government efforts, burnishing international image. *ITWorld*
http://www.vanityfair.com

- Weisbrode, Kenneth (March 28 2010). Diplomacy 2.0. The Guardian

**Online resources**

- About Diplopedia: http://www.state.gov/m/irm/ediplomacy/115847.htm
- Burson-Marsteller “Twitplomacy: Mutual Relations on Twitter”. http://twiplomacy.com
- Secretary Clinton To Deliver Remarks on Internet Freedom on Thursday, January 21st 2010: http://www.state.gov/r/pa/prs/ps/2010/01/135379.htm
- Agence France-Presse E-diplomacy Hub: http://ediplomacy.afp.com
- Virtual Embassy of the United States Tehran, Iran. www.iran.usembassy.gov
- Cyber-security policy of South Africa (February 19 2010). Government Gazette #536, Republic of South Africa
- Cybercrimes and cyber-security bill (October 20 2015). Ministry of Justice, Republic of South Africa
• Wales Senate Testimony regarding “E-Government 2.0: Improving Innovation, Collaboration, and Access” U.S. Senate Committee on Homeland Security and Governmental Affairs, December 11, 2007


• The President and the Press: Address before the American Newspaper Publishers Association. President John F. Kennedy, Waldorf-Astoria Hotel, New York City, April 27, 1961
