Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 176 (2020) 60–69

Procedia Computer Science

www.elsevier.com/locate/procedia

24th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems

Cyber Diplomacy: A Systematic Literature Review

* Amel Attatfa[a], Karen Renaud[a], Stefano De Paoli[b]

[a]School of Design and Informatics,
[b]School of Business, Law and Social Sciences
Abertay University, Bell Street, DD1 1HG, Scotland

Abstract

Diplomatic action in international relations is a global security priority in the inter-connected world. The birth of cyber diplomacy, occurred in the year 2007, which will always be remembered due to a wide-ranging cyber attack on Estonia. Indeed, Estonia is known for being one of the most wired countries in Europe. The attack consisted of crippled computer networks because of hackers which paralysed numerous amount of government and corporates sites. The escalation in these kinds of attacks highlighted the need for governments to formulate national cyber strategies. This sprang from the realisation that cyberspace, like the physical world, also has military and strategic dimensions and requires countries to work together to defeat cyber opponents.

Attacks within cyberspace are subject to strategically-formulated threats, which go beyond the usual physical terrorist-type threats. Global progress, democracy and peace are at stake. This makes cyber diplomacy a major issue for countries' foreign policies, due to the interdisciplinary nature of the domain. A number of aspects are relevant in this respect: policies, politics and sociology (dread), diplomacy, digital/cyber science, multilateralism and world history.

This paper reports on a systematic literature review that was carried out to reveal the dimensions of current cyber diplomacy research. While a number of studies have introduced and defined "Cyber Diplomacy" and its associated diplomatic actions, none have sought to distinguish this field from the more traditional and well established diplomacy concept. This is a significant gap in the literature, which will be the topic of future research.

Keywords: Cyber Diplomacy

1. Introduction

The contemporary definition of diplomacy delineates the concept as *the process of conducting negotiations between representatives of States* [29]. It is interdisciplinary, and has enjoyed attention from social science [34], global affairs [6] and politics [30] researchers.

*Corresponding Author
Email Address: 1905477@uad.ac.uk

1877-0509
10.1016/j.procs.2020.08.007

Diplomacy faces diverse challenges. For instance, the "international responsibility to protect" is a key point for diplomats, in addition to the immigration/emigration issues which are "major diplomatic challenges internationally" [36], and the COVID-19 global pandemic which is exercising governments across globe at time of writing [23].

It is crucial for countries to realise that their economies, global competition, and cyberspace security rely on a functioning and secure cyber space. Internet access, and the use of emergent technologies, is on the political agendas of all countries, whether they are cyber powers (e.g. United States, China, Russia, France, Israel, United Kingdom) or merely active consumers of Internet-enabled technologies [18].

The modern issues of 'sustainable development', the environmental concerns, the global pandemics, the economy and the expansion of international law are seen as major diplomatic challenges [36]. Over the last two decades, a new diplomatic domain has been added to this list: **cyber diplomacy**.
The Research Questions (RQ*i*) this paper explores are:

Research Question 1 (RQ1): *What are the dimensions of cyber diplomacy, as revealed by existing research?*

Research Question 2 (RQ2): *Which aspects of cyber diplomacy have not received any attention from researchers?*

This paper offers a comprehensive overview of current research into cyber diplomacy. We commence, in Section 2, by introducing the field of cyber diplomacy. Section 3 outlines the methods used to carry out our literature review. Section 4 reports on our findings, and Section 5 reflects on them. Finally, Section 7 concludes by outlining the implications of the research.

2. Cyber Diplomacy

Cyberspace provides digital/cyber tools to facilitate a more effective implementation of diplomatic strategies, generating, at the same time, a whole range of government-led measures that can benefit from the diplomat's standard and well understood techniques and mentality [33].

2.1. Core Terms

The distinction between "regular/standard" diplomacy and cyber diplomacy is straightforward: if the cyber dimension is the core reason for the diplomacy, it is cyber diplomacy.

Cyber diplomacy incorporates the use of diplomatic tools and mindsets to resolve issues arising from the international use of cyberspace [31]. The use of cyber tools to promote broader diplomatic agendas, as well as the use of diplomatic techniques and mental modes to analyse and manage cyberspace problems, are separate but interdependent activities.

A related but different term is digital diplomacy, which is defined as "*the use of social networking sites in order to foster dialogue with online publics*" [16, p.332]. Riordan [31], clarifies the distinction between cyber and digital diplomacy, explaining that digital diplomacy refers to *the use of digital tools and techniques to do diplomacy* while cyber diplomacy refers to *the use of diplomatic tools and the diplomatic mindset to resolve issue arising from cyberspace*. Our paper focuses on the latter: **cyber diplomacy.**

2.2. Diplomacy

Diplomatic action in international relations has become a priority because of the security of states being at stake [32]. It is clear that this security is deeply intertwined with cyberspace and the need to protect critical infrastructures, and the wider population, from the impact of nation-state cyber attacks.

This begs the question of the extent and reach of cyber diplomacy, which is considered as an essential instrument in international relations, and its influence in bringing together different and diverse actors.

2.3. The Paris Call

The Paris Call for Cyber Peace is a cyber initiative launched by France, during a speech delivered by French President Emmanuel Macron. The Call was held at the Internet of Trust on 12 November 2018 at UNESCO, in Paris, in the presence of UN Secretary-General Antonio Guterres. This followed the initiative of the Group of Governmental Experts (GGE) in 2017, after failing for lack of consensus.

This key cyber diplomacy initiative is encapsulated in the Paris Call [21], a French diplomatic endeavour, which places France at the forefront (advocating the use of *soft power*, or *power by cooptation*, a notion proposed by Joseph Nye [26]). Cybersecurity is a key issue in diplomatic relations, as identified by the French *White Paper on Defence and National Security* [15] as a national priority. The Paris Call is characterised by:

- Involvement of a gathering of a multitude of actors, both private and public.
- The highlighting of the need for international law to apply automatically in cyberspace.
- The positioning of France as a leader in cyber issues on the international front, as compared to other cyber powers leaders (e.g. United States, France, Israel, China, Russia, United Kingdom).

It has become fundamental to understand the nature of cyber diplomacy and to extend our understanding of this emerging field. Answering the two research questions mentioned in the introduction will help achieve this, by providing a snapshot of existing research into the extent and nature of diplomatic action, as it applies to international cyberspace relations.

3. Research Methodology

A systematic literature review was carried out following the approach proposed by [33, 17]. The goal of the systematic literature review was to provide answers to the two research questions enumerated in the introduction.

Given the embryonic state of this particular research field, it was important to include gray literature in addition to research published in peer reviewed venues. We thus included industry reports, websites and books so that we did not miss any key research. Hence, a variety of academic databases, such as Cairn.info, Scopus and general search engines, such as Google Scholar, were used to gather relevant sources.

We collected material with a timeline between 2010-2019, in order to capture newly published literature, as well as work published early in the development of the field. The methodology adopted in the systematic review is depicted in the prisma in Figure 1.

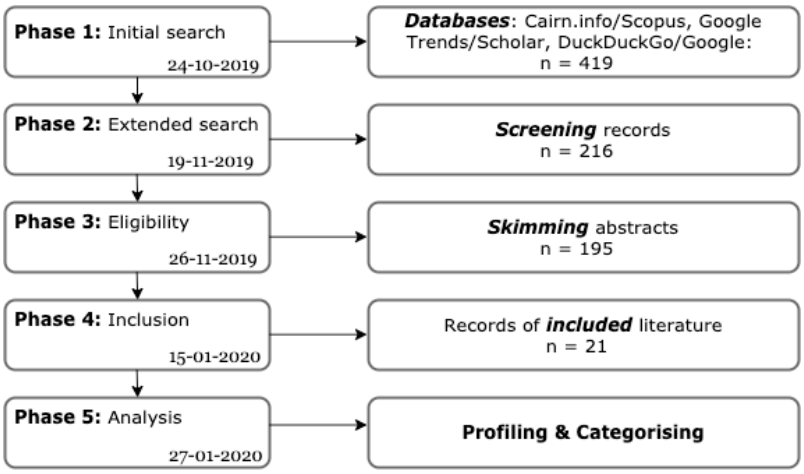


Fig. 1. Systematic Review Prisma

The research methodology includes the following phases:

1. **Phase 1 (Identification):** 419 results were found by searching all databases using the keywords: "diplomacy + digital" and "diplomacy + power".

2. **Phase 2 (Screening):** After initial screening, it was found that 48.45% of papers (203) from phase 1 were irrelevant due to being out of scope or context. A further, more focused, search was subsequently performed using specific keyword combinations "cyber diplomacy"+ country, "Cyber Power" + country.

3. **Phase 3 (Eligibility):** The 419 results were reduced to 216 by analysing the abstracts of the documents. Only relevant studies were retained.

4. **Phase 4 (Inclusion):** All the remaining papers (195) were now recorded in a structured and systematic format. The papers were now read, and the final weeding out process eliminated all but 21 papers.

5. **Phase 5 (Profiling table):** A profiling table was created for the 21 sources that were considered relevant to the research topic and were retained for detailed analysis (Table A.6).

4. Findings

As mentioned in the previous section, only 21 studies were retained for intensive analysis. These studies were classified into groups in terms of: (1) relevance, (2) country where the study was conducted, and (3) methodology adopted.

4.1. Country

In terms of countries or regions where the studies were conducted: nine in France, four in the UK, one in Canada, one in the Netherlands, one in Switzerland, two in the US, one from a collaboration between Romania and the USA, and two in Australia and Oceania.

Most of the studies ([32], [33], [17], [2], [3], [35], [25], [10], [26], [7], [14]) did not have a specific focus on a particular country, or countries more generally. However, some of them mentioned countries as part of supporting evidence ([4], [1], [22], [24], [37], [9]).

4.2. Paper Focus

The publications are divided into five categories, reflecting their focus. Of 21 resources:

1. **Cyber Diplomacy - Definition**: Four (4) studies explored the core meaning of the term "Cyber Diplomacy" (e.g. definition, terminology, impact).

2. **Cyber Diplomacy - Methods**: Three (3) studies addressed methodologies, which helped to reveal the key dimensions used to elaborate and highlight relationships between similar terms.

3. **Cyber Diplomacy - Security and Power factors**: Five (5) studies introduced these two crucial elements in the interaction between "Diplomacy" and "Cyber". Indeed, within cyberspace, security, and to a certain extent, cyber security, is one of the main objectives pursued by the diverse cyber powers.

4. **Cyber Diplomacy - Multilateralism, international relations and international law**: Three (3) studies highlight the need for the field to be further investigated in depth. For instance, multilateralism is a way for countries, and other actors, to work together as a community within international relations where numerous challenges and issues are confronted and exposed in today's connected world. Hence, international law is also pertinent, because it is question of regulating cyberspace. Therefore, States and governments are not in favour of creating a new form of international law. Laws that already exist could feasibly be adapted to the current situation. Organisations, big corporations, and private actors in general are more likely to pursue a new International Code of Conduct, distinct from the existing ones.

5. **Cyber Diplomacy - Diplomacy and the Internet**: Six (6) studies outline the fundamental dimensions of Cyber Diplomacy. Indeed, diplomacy and Internet are the pillars supporting a comprehensive structuring of the Cyber Diplomacy research domain.

Table A.6 in the Appendix provides a brief review of the key findings of each paper to provide a precis of the insights each offers.

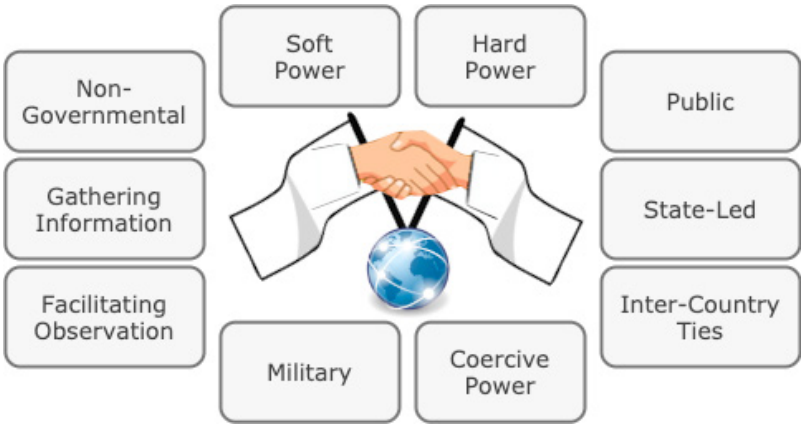


Fig. 2. Cyber Diplomacy Dimensions

4.3. Categorising Papers

Lohmann [20] introduces features of diplomacy, which allows us to sort the 21 papers. In order to achieve this, a mind map was constructed to isolate the dimensions of diplomacy, representing the different and diverse features of diplomacy, without including cyber (Figure 2). Tables A.1, A.2, A.3, A.4 and A.5 reflect the dimensions of cyber diplomacy, as revealed by the analysis.

What emerges from this analysis is that the four studies focusing solely on cyber diplomacy exemplify similar criteria, which is that cyber diplomacy is primarily state-led. This explains that the research area of cyber diplomacy has its roots in regular or standard diplomacy, having adapted itself to the needs and requirements of the merging of the physical and cyber worlds.

In particular, [31, 27, 25, 10] had two features in common: state-led (official), and non-governmental diplomacy (except for [25]). This means that the initial essence in these studies is to put into perspective, or to mention features of, state-led diplomacy (or official diplomacy), or non-governmental diplomacy. Others had another feature: inter-country ties [27, 25, 10]. These addressed the expansion of political, economic and cultural ties between countries.

4.4. Discussion

The well understood, required and expected traditional diplomacy criteria, standards, skills, and abilities are not necessarily well-suited for the types of diplomacy that mutate and change in this connected world with evolving and emergent cyber-attacks, viruses, and threats. The resulting consequences and damages will be as much virtual as physical, and can not simply be managed as it would be with more traditional physical threats. Indeed, the observation evidence is quite clear. Due to the newness of this field, the methods used, even within the few studies we analysed, are limited and relate to past concepts, norms, theories. We can not be sure that they are appropriate for use in this domain, or settle only for theory/concept based studies, as we need more empirical research to better understand cyber diplomacy. For instance, cyber diplomacy in international cyberspace relations has never been investigated using a combination of interviews, observations and analysis of the literature. For instance, with regard to the need for empirical evidence, studies by [31] and [10] can be expanded by supporting the theory with evidence such as interviewing diplomats, observing

diplomats, and considering targeted case studies. Hence, our taxonomy helps us to identify relevant methods by describing the field as a whole.

Moreover, the five categories of references listed previously prompted further informations to the concepts and theories around the core subject - cyber diplomacy - which are mainly multilateralism [3]; security [2], [1], [22], [26], [7]; and capacity building [28]. In addition, [4], [25] and [14] focus on diplomacy as a base of foreign relations and policies. Whereas [35], [27] and [24] address the digital strategies and changes that have consequences within cyberspace.

This is why Barat-Ginies [5] poses the question related to the viability of international law. This question correlates with the discussion that actors (either public or private) want, either to build a certain regulation, appropriate norms, rules, laws - especially for states and governments. Other actors argue for an International Code of Conduct, i.e. international law (e.g. China, Russia for instance), and what big corporations such as GAFAM (Google, Amazon, Facebook, Apple, Microsoft) call for. Some groups are more inclined to a new International Code of Conduct (e.g. the Shanghai Organisation, of which China and Russia are members). In contrast, other actors, thus, maintain the right to keep their national/state sovereignty intact and secure.

Vaïsse [37] provides a definition of multilateralism in order to lay the foundations for this concept. Castells [9] studies the sociology of networks dealing with the historical, sociological, cultural, technological and economic fields and how they have been transformed by networks. These two publications offer a global perspective of the subject and are ahead of the rest, in terms of international relations and establishment of concrete explanation, from a cyber perspective.

5. Answering the Research Questions

We now return to our two research questions:

RQ1: *What are the dimensions of cyber diplomacy, as revealed by existing research?*

The dimensions revealed by our investigation are depicted in Figure 2. This demonstrates the adaptive, versatile, useful and relevant nature of the field.

RQ2: *Which aspects of cyber diplomacy have not received any attention from researchers?*

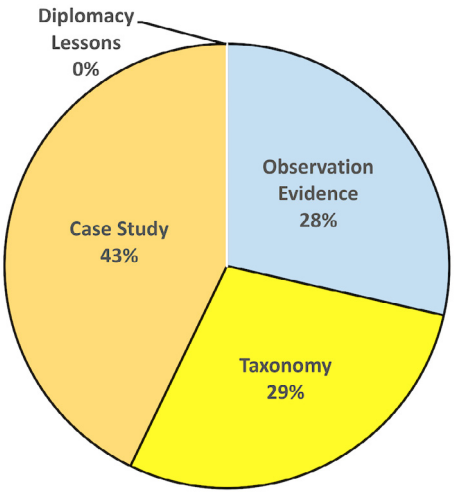
As shown in Figure 3, the neglected aspects of cyber diplomacy are linked to diplomatic action in international cyberspace relations. Specifically, this means that in a interrelated world, collaboration, constructive work and effective action are the keys towards a better understanding of this newly emerging field.

Figure 3 summarises the paper *foci* encompassing: observation evidence (6 papers), taxonomy (6 papers), and case studies (9 papers). Lessons from standard diplomacy, traditional diplomacy, or even pre-cyber diplomacy have not been covered. This is a gap in the literature. The well established tried and tested methods used to study other kinds of diplomacy do not necessarily relate to the standards of cyber diplomacy. The exact mappings ought to be investigated.

Nevertheless, a focus on cyber security is missing, especially in conjunction with cyber power, and joint definitions of what constitutes cyber threats and efforts to build consensus (e.g Convention on Cybercrime, ETS No.185). These are essential, given the link between cyber diplomacy and cyber security, and of its interdisciplinary aspects.

6. Reflection & Future Work

The twenty-one publications we reviewed reflect the extent of cyber diplomacy. Therefore, considering that there are few experts and studies with a focus on cyber diplomacy itself, it is crucial to incorporate notions, theories, and inputs orbiting the research subject and helping cover, and more generally, surround the key aspects of cyber diplomacy. Future work could advance pursuing a number of directions. Three examples are:



Nature of Findings	Number of Papers
Observation Evidence	6
Taxonomy	6
Case Study	9
Diplomacy Lessons	0

Fig. 3. Categorisation of Sources

1. The first would be to apply Actor-Network Theory (ANT) [19, 11] and the sociology of networks [9]). Bueger [8] portrays the Actor-Network Theory as a symmetrical theory of representation. Indeed, this theory explains that state diplomacy needs tools to properly represent a state. However, there is also a need to include not only state or public actors, but also for professional and private actors to be representatives within the international community.
2. The second one would be security theory [7] and cybersecurity [22, 12]. This theory's main purpose is to foster more security and peace within cyberspace.
3. The third would be to focus on multilateralism, or even new multilateralism [37], and cyber power [26]. These are two correlated concepts, because both imply the need to involve interconnections, relations, and exchanges between two or more entities.

Table A.6 can be considered a starting point for maturing the cyber diplomacy field. The direction the research has taken so far includes studies and analyses of diplomatic actions (of a state, government, corporation, civil society, etc.) that have made an impact on international negotiations.

These may result in agreements, treaties or initiatives and take place in a interlinked world, within cyberspace (e.g. The Paris Call, in November 2018 [21]). An example of this type of study is an analysis of the ongoing and current work of the UN agencies on putting in place a new initiatives [13]. This involves state/government other actors from the private sector such as corporations and civil societies (e.g. OEWG). The purpose of this initiative is to find common ground and try to resolve issues arising from cyberspace (including cyber attacks, etc.).

A direction for future work could be to follow the international sessions, meetings, and conferences to witness progress (solutions, issues) and to analyse these. This might constitute combining a new Group of Governmental Experts (GGE) and the UN Open-Ended Working Group (OEWG) while targeting the diplomatic actions of specific countries which are cyber powers, as well as being involved in these initiatives.

7. Conclusion

The research reported here explored the dimensions of cyber diplomacy evidenced by both research and gray literature. We highlight the fact that cyber diplomacy is not purely a technical issue, confirming what Riordan argues [32]. So far, technical experts appear to have shaped cyberspace, but it would be a mistake to let them continue to shape offshoots of this core domain. Doing so would result in state and government actors lacking structure and abilities related to non-technical security and power tools. There is a need for research into diplomatic action, encouraging diplomatic attention across the international community.

References

[1] Abrahamsen, R., Williams, M.C., 2009. Security beyond the state: Global security assemblages in international politics. International Political Sociology 3, 1–17.
[2] Al-Rodhan, N.R., 2007. The five dimensions of global security: proposal for a multi-sum security principle. LIT Verlag Münster.
[3] Badie, B., 2007. Le multilatéralisme: nouvelles formes de l'action internationale. La Découverte.
[4] Balzacq, T., Charillon, F., Ramel, F., 2018. Manuel de diplomatie. Presses de Sciences Po.
[5] Barat-Ginies, O., 2014. Existe-t-il un droit international du cyberespace? Herodote 152/153, 201–220.
[6] Barrinha, A., Renard, T., 2017. Cyber-diplomacy: the making of an International Society in the digital age. Global Affairs 3, 353–364.
[7] Battistella, D., 2015. Chapitre 14/la sécurité. Théories des relations internationales 5, 491–522.
[8] Bueger, C., 2013. Actor-network theory, methodology, and international organization. International Political Sociology 7, 338–342.
[9] Castells, M., 2002. La galaxie internet, trad. de l'anglais par p. Chemla, Paris, Fayard .
[10] Cirnu, C.E., 2017. Cyber Diplomacy – Addressing the Gap in Strategic Cyber Policy. The Market for Ideas 7-8.
[11] Crawford, C., Ritzer, G., 2005. Encyclopedia of social theory. a: Actor network theory. vol. 1.
[12] Gallaher, M.P., Link, A.N., Rowe, B., 2008. Cyber security: Economic strategies and public policy alternatives. Edward Elgar Publishing.
[13] Geneva Internet Platform, undated. UN GGE and OEWG. https://dig.watch/processes/un-gge Accessed 16 April 2020.
[14] Hanson, F., 2011. The new public diplomacy. Lowy Institute for International Policy.
[15] Hollande, F., 2013. French white paper. defence and national security. http://www.defense.gouv.fr/english/content/download/206186/2393586/file/White\%20paper\%20on\%20defense\%20\%202013.pdf Accessed January 2020.
[16] Kampf, R., Manor, I., Segev, E., 2015. Digital diplomacy 2.0? A cross-national comparison of public engagement in Facebook and Twitter. The Hague Journal of Diplomacy 10, 331–362.
[17] Khan, K.S., Kunz, R., Kleijnen, J., Antes, G., 2003. Five steps to conducting a systematic review. Journal of the Royal Society of Medicine 96, 118–121.
[18] Kluz, A., Firlej, M., 2015. The impact of technology on foreign affairs: five challenges. Foreign Policy Association. Retrieved from www. foreignpolicyblog. com .
[19] Latour, B., 1999. On recalling ANT. The Sociological Review 47, 15–25.
[20] Lohmann, S., 2017. Understanding diplomacy in the 21st century. https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/WP_Diplomacy21_No11_Sascha_Lohmann_01.pdf Accessed January 2020.
[21] Macron, E., 2018. Paris call. for trust and security in cyberspace. https://pariscall.international/en/ Accessed January 2020.
[22] Van der Meer, S., 2015. Enhancing international cyber security: A key role for diplomacy. Security and Human Rights 26, 193–205.
[23] New York Time, 2020. Worldwide Confirmed Coronavirus Cases Top 2 Million. https://www.nytimes.com/2020/04/15/world/coronavirus-cases-world.html.
[24] Nocetti, J., 2014. Puissances émergentes et internet: Vers une "troisième voie"? Politique étrangère 4, 43–55.
[25] Nocetti, J., 2018. Introduction. Politique étrangère 3, 10–13.
[26] Nye Jr, J.S., 2010. Cyber power. Technical Report. Harvard University. Belfer Center for Science and International Affairs. Cambridge, MA.
[27] Pahlavi, P.C., 2003. Cyber-diplomacy: A new strategy of influence, in: Canadian Political Association, General Meeting, Halifax, NS.
[28] Pawlak, P., 2016. Capacity building in cyberspace as an instrument of foreign policy. Global Policy 7, 83–92.
[29] Pigman, G., 2010. Contemporary diplomacy. Polity.
[30] Renard, T., 2018. EU cyber partnerships: assessing the EU strategic partnerships with third countries in the cyber domain. European Politics and Society 19, 321–337.
[31] Riordan, S., 2016. Cyber diplomacy vs. digital diplomacy: a terminological distinction. USC CPD Blog (May 12). http://uscpublicdiplomacy.org/blog/cyber-diplomacy-vs-digital-diplomacy-terminological-distinction Accessed in November 2019.
[32] Riordan, S., 2019. Cyberdiplomacy: managing security and governance online. John Wiley & Sons.
[33] Saunders, M., Lewis, P., Thornhill, A., 2007. Research methods. 7 ed., Pearson, Harlow, UK.
[34] Sharp, P., 1999. For diplomacy: Representation and the study of international relations. International Studies Review 1, 33–57.
[35] Taillat, S., 2017. L'impact du numérique sur les relations stratégiques internationales. Strategique 117, 137–153.
[36] Thakur, R., Cooper, A.F., Heiner, J., et al., 2013. Introduction: the challenges of 21st-century diplomacy, in: The Oxford handbook of modern diplomacy. Oxford University Press.
[37] Vaïsse, M., 2017. Les relations internationales depuis 1945-15e éd. Armand Colin.

Appendix A. Tables

Table A.1. References: Cyber Diplomacy

Features of Diplomacy	Riordan *et al.* [31]	Pahlavi [27]	Nocetti [25]	Cïrnu [10]
State-Led (Official)	✓	✓	✓	✓
Non-Governmental	✓	✓	✓	✓
Military			✓	
Soft Power		✓		
Hard Power				
Public (Diplomacy)		✓		
Coercive Power				
Gathering Information				
Inter-Country Ties		✓	✓	✓
Facilitating observation				

Table A.2. References: Definitions and Methods

Features of Diplomacy	Hanson [14]
State-Led (Official)	✓
Non-Governmental	
Military	
Soft Power	
Hard Power	
Public (Diplomacy)	✓
Coercive Power	
Gathering Information	✓
Inter-Country Ties	✓
Facilitating observation	✓

Table A.3. References: Security and Power components

Features of Diplomacy	Al-Rodhan [2]	Abrahamson & Williams [1]	Van Der Meer [22]	Nye [26]	Battistella [7]
State-Led (Official)		✓	✓	✓	✓
Non-Governmental		✓	✓	✓	
Military	✓				✓
Soft Power				✓	
Hard Power				✓	
Public (Diplomacy)					
Coercive Power		✓		✓	
Gathering Information					
Inter-Country Ties					
Facilitating observation					

Table A.4. References: Multilateralism and International relations/law

Features of Diplomacy	Badie & Devin [3]	Barat-Ginies [1]	Vaïsse [37]
State-Led (Official)	✓	✓	✓
Non-Governmental	✓	✓	✓
Military	✓	✓	✓
Soft Power			
Hard Power			
Public (Diplomacy)			✓
Coercive Power		✓	
Gathering Information			
Inter-Country Ties	✓		✓
Facilitating observation	✓	✓	

Table A.5. References: Diplomacy and Internet

Features of Diplomacy	Balzacq *et al.* [4]	Taillat [35]	Pawlak [28]	Nocetti [24]	Castells [9]
State-Led (Official)	✓	✓	✓	✓	✓
Non-Governmental	✓	✓	✓	✓	
Military		✓		✓	
Soft Power					
Hard Power					
Public (Diplomacy)	✓	✓		✓	
Coercive Power					
Gathering Information					✓
Inter-Country Ties	✓		✓		✓
Facilitating observation			✓		✓

Table A.6. Profiling Table

Source Summaries
[2] This book aims to put into perspective a new, highly and innovative security principle: "The Multi-Sum Security Principle", which classifies global security into five dimensions (human, environmental, national, transnational, and transcultural security) promoting cooperative interaction between States and peaceful coexistence between cultural groups and civilisations.
[3] This book revolves around the concept of multilateralism regarding the new aspects of the international action around the world, impacting diplomacy, NGOs, and media. Two objectives are to propose marking insights from thirteen experts in political science, economics, history and law; and to identify certain reflections towards the deep meaning of multilateralism in a new world system we live in, influenced by all sorts of conflicts.
[4] This book is the first French-language Handbook of Diplomacy, which covers all the dimensions of the diplomatic institution in the 21st Century, setting it in its historical evolution and presenting its classical aspects as well as its new forms of expression.
[1] This article focuses on the privatisation and globalisation of commercial private security instead of the battlefields.
[35] This paper explores the impact of the digital domain on the international strategic landscape, by proposing three arguments including the expenditure of the digital space, the mindset of actors, and the political and strategic configuration.
[27] This paper analyses the concept of Cyber-Diplomacy described as a new and central strategy of influence, within current international affairs, which is developed by governments. Indeed, diplomatic tools and mindsets change constantly in the hyper-connected world in order to comply with new challenges and sets of national interests.
[5] This paper explains the resourceful adaptability of international law regarding new challenges within the hyper- and inter-connected world, while also focusing on Geneva conventions, Tallinn manual linked to CyberWarfare, the NATO Cyber defence centre of excellence as illustration or case studies.
[22] This paper brings to light the threatening aspect of cyber aggression regarding international security and stability. In other words, the particular action of national cyber policies towards deterrence is questioned regarding its efficiency. That is why diplomacy, alongside confidence-building measures and international norms, have potential in delivering constructive and substantial results in the long term.
[28] This article explores the nexus that international debates regarding cyber-related issues and cyber capacity building share. Hence, it focuses on the projects held by the Council of Europe and International Telecommunication Union surrounding capacity building being potentially useful as a foreign policy tool.
[25] This introduction is a first peace of the French Think-tank paper about Cybersecurity. Indeed, the author describes the state of cyberspace and accentuates at the end by reminding about cyber diplomacy.
[10] This articles points out the fact that although cyber-diplomacy is a new topic, it has already advanced in leaps and bounds worldwide in an attempt to define and to summarise the efforts constantly made to solve a new type of conflict, namely those taking place in cyberspace.
[24] This articles explain the leading role of in Internet Governance, while taking into consideration the majority of non-Western countries Internet users, and the the different perspectives of diverse countries.
[26] This book revolves around the term "cyber power" by explaining its importance in world politics and involving different aspects of powers that have particular characteristics, type of diffusion and illustration of powers.
[7] This book focuses on the understanding of the contemporary world based on theories of international relations. Moreover, this chapter 14 deals with security in international relations, which is a key matter for a majority of the world's nations.
[14] This book is about public diplomacy and its novelties or new features allowing for quick evolutions, opportunities and changes, at the same time outlining the wired world we live in.
[37] This books presents a global synthesis of international political relations since 1945, while being directly turned to current news.
[9] This book centres around the new forms of social hierarchy developed in the network society (with a warning of shortcoming of sources and data), through interacted ideas of the Internet, economy and society.