Global Journal of Human-Social Science: F
Political Science
Volume 25 Issue 4 Version 1.0 Year 2025
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 2249-460X & Print ISSN: 0975-587X

Cyber Diplomacy in Africa: The Role of the African Union in Shaping Regional and Global Cyber Norm

By Saron Obia Messembe & Gabriel Cyrille Nguijoi

Abstract- Cyberspace has rapidly emerged as a critical arena for international diplomacy, requiring the necessity for diplomats to redefine and adapt foreign-policy relations practices and strategies. With the rise of cyber threats, including hacking, cyber-warfare, and cyber-attacks, the growing need of cyber diplomacy has become particularly urgent. The African Union has taken important steps to integrate cyber issues into its broader diplomatic agenda, positioning itself as a key actor and player in regional and global cyber governance. This article thus analyses the African Unions' (AU) role in shaping the continent's cyber diplomacy, and its narrative grounded in the English School's distinction between international society and world society. It focuses on its efforts to create regional norms, and also collaborate with other international bodies. The paper globally argues that cyber diplomacy sits, not only, at the intersection of these two social orders, but the AU, together with Regional Economic Communities (RECs) and national institutions must institutionalize diplomatic capacities to translate continental norms into operational resilience. Building on normative analysis and empirical evidence, the paper tries to define cyber diplomacy and distinguishes it from e diplomacy; traces the institutional emergence of cyber diplomacy in AU processes and selected member states; maps gaps between AU instruments (Malabo Convention, AU digital/ data agendas) and national practice; and proposes an operational AU cyber diplomacy agenda.

Keywords: *diplomacy, hacking, cybersecurity, cyber-diplomacy, foreign policy.*

GJHSS-F Classification: *LCC Code: JZ1308, JZ1318*

Strictly as per the compliance and regulations of:

Cyber Diplomacy in Africa: The Role of the African Union in Shaping Regional and Global Cyber Norm

Saron Obia Messembe [α] & Gabriel Cyrille Nguijoi [σ]

Abstract- Cyberspace has rapidly emerged as a critical arena for international diplomacy, requiring the necessity for diplomats to redefine and adapt foreign-policy relations practices and strategies. With the rise of cyber threats, including hacking, cyber-warfare, and cyber-attacks, the growing need of cyber diplomacy has become particularly urgent. The African Union has taken important steps to integrate cyber issues into its broader diplomatic agenda, positioning itself as a key actor and player in regional and global cyber governance. This article thus analyses the African Unions' (AU) role in shaping the continent's cyber diplomacy, and its narrative grounded in the English School's distinction between international society and world society. It focuses on its efforts to create regional norms, and also collaborate with other international bodies. The paper globally argues that cyber diplomacy sits, not only, at the intersection of these two social orders, but the AU, together with Regional Economic Communities (RECs) and national institutions must institutionalize diplomatic capacities to translate continental norms into operational resilience. Building on normative analysis and empirical evidence, the paper tries to define cyber diplomacy and distinguishes it from e diplomacy; traces the institutional emergence of cyber diplomacy in AU processes and selected member states; maps gaps between AU instruments (Malabo Convention, AU digital/ data agendas) and national practice; and proposes an operational AU cyber diplomacy agenda.

Keywords: diplomacy, hacking, cybersecurity, cyber-diplomacy, foreign policy.

I. Introduction

Cyberspace has rapidly emerged as one of the recent year's critical frontlines in international relations, carrying along both exceptional opportunities and risks. The rise of cyber threats such as hacking, cyber-attacks, and cyber-warfare, urge mainstream diplomatic strategies and practices to adapt in order to address these growing challenges. As Africa reinforces its digital and technological infrastructures, the need for a coherent cyber diplomatic framework becomes more pressing than ever, especially the AU, and its pillars, (regional institutions).

The role of diplomacy in cyberspace is much less prominent in the media than stories of cyber incidents. In 2015, US and China reached a cyber security deal, one of the most contentious issue in their bilateral relations. For years, both parties accused each other of network infiltration and accessing confidential information from companies and government agencies. The US had accused China of compromising a number of weapon systems, such as the F-35 and the PAC3 missile (Meyers, 2015).

In 2014, five Chinese hackers were indicted by the Department of Justice over hacking into a number of high-profile companies, such as the United States Steel Corporation (Segal, 2016). Meanwhile, China has often ink or voice counter-claims of being a victim of US intrusions (Singer and Friedman, 2014, p. 189). The agreement struck between President Barack Obama and President Xi Jinping foresees cooperation and mutual assistance in investigations on cybercrime, while both sides committed to restrain from cyber-enabled economic espionage. A monitoring mechanism was established to ensure the proper implementation of this agreement, and a hotline was created to deal with the escalation of issues in cyberspace (White House, 2015).

African diplomats must rethink the cybersecurity directives of the different states. In 2023, *the African Union (AU) internet connectivity was compromised by BlackCat Group (also known as ALPHV)*, though the consequences were mitigated by Interpol and partners.

IN 2012, A Forum Code Security *"hacker known as direxer, exploited a Web vulnerability and took down 103 government of Kenya websites overnight sitting unfixed programming errors in code"*. Meanwhile, in 2015 the popular Indonesian hackers from Gantenger's Crew hacked and defaced the President of Kenya's site (LTN, 2015). The defaced webpage revealed digital footprints on the hacked Kenyan President site. They replaced the page with one of their own. The reason behind the hack was expose to the authorities their expertise and mastery of the 'game', as reported by Hack Read reports.

This article aims at discussing the role of diplomats and diplomacy in addressing cyber issues,

Author α: Researcher at Research Institute for European and American Studies (RIEAS), Theorist Coordinator at Cyber Jurisprudence International Initiative (Egypt), Nkafu Policy Institute (Cameroon).
e-mail: sirmessembe@gmail.com
Author σ: (PhD.), Research Officer, National Institute of Cartography, Institute of Diplomatic and Strategic Studies, Cameroon, African Center for the Study of the United States (ACSUS), South Africa, European Center for the Populism Studies (ECPS), Belgium.
e-mail: gabrielcyrilnguijol@yahoo.fr

following the changing dynamics in the International Relations (IR) literature. More specifically, it seeks to reconfigure the African Union narrative on emerging trends and how they adapted to a new policy domain. This comes at a time in which diplomacy is changing in terms of its practices (with the progressive adaptation to new technologies), but also in terms of the areas it covers and actors it deals with (Hocking et al., 2012). Cyber-diplomacy can simply be seen as the latest instalment, albeit a particularly important one, in what is the progressively changing role of diplomacy in the digital age.

The framing on the evolution of cyber-diplomacy will adopt an English School perspective. While diplomacy has often been treated as a mere "constant" (Sending et al., 2015, p. 3) by International Relations scholars, more interested in analysing the origins of power politics and the evolution of warfare. The English School globally distinguishes between 'international society,' focused on 'states relations', and 'world society,' which ranges from non-state actors to broader global issues. By situating this paper at the intersection of these two conceptual approaches, we gain insight into the evolving role of the AU as it navigates the complexities of digital governance.

Whereas the former "is about the institutionalization of mutual interest and identity among states and puts creation and maintenance of shared norms, rules and institutions at the Centre of IR theory" (Buzan, 2014: p.12), the latter "takes individuals, non-state organizations and ultimately the global population as a whole as the focus of global social identities and arrangements and puts transcendence of the state system at the Centre of IR theory" (Buzan, 2014, p. 13). Taking this school of thought as the starting point for our analysis, this paper argues that cyber-diplomacy sits at the intersection between these two societies.

Although both international society and world society are contested concepts around which much has been written, it is not the purpose of this article to engage in theoretical considerations about the ontological and normative basis of both. Ian Clark's summative assessment in which he takes the world society to refer to the "non-state social world that takes a transnational form, and is distinct from the society of states" will be adopted (Clark, 2007, p. 22). For our discussion, it is mostly important to understand international society and world society as analytical concepts that are simultaneously present in international relations. The piece will explore the concept of cyber-diplomacy and how it differs from concepts: digital diplomacy, e-diplomacy, as well as how this brave new world is being interpreted by those on the ground, the first generation of cyber-diplomats.

II. Defining Cyber Diplomacy

Cyber diplomacy is different from e-diplomacy, and includes negotiating international frameworks for digital governance, cybersecurity, and internet freedom. In Africa, this practice requires addressing both state-centric concerns, including national security, and global issues, such as cybercrime, internet governance, and the digital divide.

Andre Barrihna and Thomas Renard (2017) consider diplomacy as the attempt to adjust conflicting interests by negotiation and compromise, as for the English School, at the core of international politics; it is a central institution in the definition and maintenance of international society (Hall, 2006; Neumann, 2002, 2003; Watson, 1982). Hedley Bull has a different narrative, as he perceives diplomacy is "*a custodian of the idea of international society, with a stake in preserving and strengthening it*" (2002[1977], p. 176). According to him, there are five main functions to the diplomatic practice: to facilitate communication in world politics, to negotiate agreements, to gather intelligence and information from other countries, to avoid or minimise "friction in international relations" (2002[1977], p. 165) and, finally, to symbolise the existence of a society of states.

There are emerging narratives in international relations and diplomacy which are contrary to that Hedley Bull. Diplomacy narrative has changed from a selected group of fellows, particularly white men elegantly discussing and negotiating the main issues in international politics in cocktail parties and at official receptions (Andre Barrihna and Thomas Renard, 2017, P.4). It is not even just about relations between states. It now has to take into account "wider relationships and dialogues, involving such entities as regional and international organizations - be they intergovernmental (IGOs) or non-governmental (NGOs) -multinational firms, sub-national actors, advocacy networks, and influential individuals" (Jönsson and Langhorne, 2004, p. vii). There are, entrepreneurs such as AppsTech by Cameroonian, Rebecca Enonchong, that are reconfiguring states, national and international tech organizations cyber landscape.

Cyber-diplomacy can be defined as diplomacy in the cyber domain or, in other words, the use of diplomatic resources and the performance of diplomatic functions to secure national interests with regard to the cyberspace. Such interests are generally identified in national cyberspace or cybersecurity strategies, which often include references to the diplomatic agenda. Predominant issues on the cyber-diplomacy agenda include cybersecurity, cybercrime, confidence-building, internet freedom and internet governance.

Cyber-diplomacy is therefore conducted in all or in part by diplomats, meeting in bilateral formats or in multilateral fora (such as in the UN). Beyond the traditional remit of diplomacy, diplomats also interact

with various non-state actors, such as leaders of internet companies (such as Facebook or Google), technology entrepreneurs or civil society organisations. Diplomacy can also involve empowering oppressed voices in other countries through technology (Owen, 2015). While this sets quite a broad reach of activities, it does allow us to firmly situate cyber-diplomacy as an international society institution, even when interacting with world society actors. We exclude from our definition the more technical interactions between line ministries (such as justice, telecoms or economy) or official agencies (such as Computer Emergency Response Teams) from different countries, when diplomats are not involved. This is important as it helps differentiate purely diplomatic activities from those that take place between government departments and agencies of different countries, interactions that in many cases predated diplomatic ones as we further explain below, but whose primary concern is to address technical rather than political issues. We recognize that there is a certain 'grey area' where some of these activities may complement or combine themselves. This 'grey area' leads in practice to some tensions between national stakeholders on issues of competence and representation. However, that observation is not fundamentally unlike what is observed in other policy areas, such as the environment or trade.

There is a tendency to conflate two very different ideas: the use of digital tools by diplomats and foreign ministries, and the diplomacy of cyberspace. Following our definition, this article focuses exclusively on the latter, whereas the former fits within what could be labelled as 'e-diplomacy'. Also called 'digital diplomacy', it refers to the use of new technologies and social media by diplomats, in the context of their traditional activities, including for consular purposes (Hocking and Melissen, 2015; Sandre, 2015; Seib, 2016). According to Tom Fletcher, e-diplomacy was officially born on 4 February 1994 when the then Swedish prime minister Carl Bildt sent the first diplomatic email to US President Bill Clinton congratulating him for lifting the embargo against Vietnam (2016, p. 28). Much of the debate on new diplomacy has been based on this growing reliance on technology for the fulfilment of diplomatic duties (Copeland, 2015, p. 453). Related to it, some see in the necessary adaptation to these technologies (and rationale behind them) the key factor in guaranteeing the predominance of state power in an increasingly networked world (Hocking and Melissen, 2015; Owen, 2015).

Cyber-diplomacy is a relatively new concept. The term had been used before, but essentially to describe 'e-diplomacy' activities. In a 2002 book entitled *Cyber diplomacy: managing foreign policy in the twenty first century*, for instance, several scholars reflected already on the impact of the internet and new technologies on the objectives, tools and structures of diplomacy (Potter, 2002). The term has also been used to describe the evolution of public diplomacy activities in the digital age (Kleiner, 2008). These early studies focused mostly on the broader digital transformation, but they did not address the diplomatic processes necessary to deal with the emerging international aspects of cyber issues.

New narrative of cyber-diplomacy is slowly emerging, contrary to lack of literature during the past decade. Discourse mostly focused on foreign policy dimension of the cyber agenda, before policy-orientation studies emerge on the case for cyber-diplomacy. One of the earliest such studies, published in 2010 by the East West Institute, expressed this new interest in clear terms:

> *Because of high levels of cross-border connectivity in the cyber world, new approaches for cybersecurity must factor in the international dimension. Thus, instead of exclusively focusing on cyber defense or cyber war, it is also important to begin to develop cyber diplomacy. Few governments have even thought about the diplomatic dimension of cybersecurity, and they certainly haven't developed diplomatic strategies commensurate with the threat (Gady and Austin 2010, p.1).*

There is a reconfiguration of diplomatic practices in order to adapt to new trends, challenging the gap between practice and theory. The different regional and international blocs of researchers have inked numerous articles on cyber policies, on relations between certain countries and on specific aspects of international relations in cyberspace. There is no standard definition or concept of cyber-diplomacy, however, African countries need to rethink how diplomats and foreign offices are taking charge of these relatively new issues. More clarity on the definition and purposes of cyber-diplomacy would be useful to those who practice it, whereas the literature on diplomacy and international politics may benefit from hindsight from a new policy domain.

III. African Cyber-Diplomacy: Why and When

When considering the emergence of cyber-diplomacy, it is important to first understand the underlying logic of cooperation in this policy domain. Cyberspace cumulates a number of characteristics that frame diplomatic engagement among stakeholders. To begin with, it is a global domain connecting nations and citizens worldwide in a variety of manners, generating interactions and frictions between them. Furthermore, cyberspace is usually considered as a "global common", defined as a "resource domain to which all nations have legal access" (Buck, 1998, p. 6). Cyberspace is then comparable to other global commons such as the high seas, airspace and outer space. This requires minimum rules and regulations, in order to ensure access to all and avoid conflict, which

can only result from diplomatic negotiations. Those international society principles clash with cyberspace's contested nature in which its major powers promote competing visions, interests and values for the cyberspace. With emerging actors some of the relevant characteristics of this realm, which are but not limited to: attribution of cyberattacks and intrusions, hindering trust among stakeholders; the advantage of offense over defence security are gradually mitigated, though global vulnerabilities are still high because of the proliferation of new software. However, there is a challenge at the international realm, the reliability of states on deterrence by retaliation when it comes to cyberspace, even if attribution and deterrence are possible (van der Meer, 2016; Nye 2017). All these characteristics make both international cyber relations and the governance of the cyberspace extremely complex and fragile, but at the same time make diplomacy all the more necessary, particularly with regard (but not limited) to confidence-building mechanisms and the development of international norms and values.

In World Order, Henry Kissinger gives perhaps the clearest reasoning underpinning the rise of cyber-diplomacy, emphasizing that the absence of dialogue and diplomacy would be detrimental to the cyberspace, but also to the broader world order:

> *The road to a world order may be long and uncertain, but no meaningful progress can be made if one of the most pervasive elements of international life is excluded from serious dialogue. (…) Absent some articulation of limits and agreement on mutual rules of restraint, a crisis situation is likely to arise, even unintentionally; the very concept of international order may be subject to mounting strains (Kissinger, 2014, pp. 345-6).*

The logic of diplomacy in cyberspace is indisputable and yet its practice is very new. This is not due to a sudden change in the above-mentioned characteristics, but rather to the evolution of the governing structures of the cyberspace over time. In the early days, internet was essentially unregulated and its governance largely informal. The main stakeholders were not states, but engineers; it was firmly situated within the realm of world society. Over time, governments became more involved and the cyberspace more regulated. International meetings multiplied, giving way to a plethora of new fora on cyber issues where government technical experts from various line ministries convened to discuss a range of cyber issues, from network security to online criminality. Some of these meetings became structured such as *the Oliver Tambo Declaration adopted by the Conference of African Ministers in charge of Information and Communication Technologies held in Johannesburg, South Africa on 5 November 2009; the Addis Ababa Declaration adopted on 22 June 2012 on the Harmonization of Cyber Legislation in Africa and the Malabo Convention of the African Union*. However, institutionalization of these meetings, align with the paradigm shift of cyber agenda or culture which "politicized struggles", ignited the narrative of cyber diplomacy (Deibert, 2015).

African countries are not exempted from the 'game' of the twenty-first century, that of developing comprehensive cybersecurity strategies, as the cyberspace and infrastructures reveal to be strategic assets and could be vulnerable. Before then, states Cybersecurity Strategy mainly focused on the national dimension, such as developing cyber capabilities, improving government coordination, and strengthening cooperation with the private sector. However, the international dimension of cyber issues was taken in to consideration, in order to vitalize cooperation with international partners. Being member states to the UN, Sub Saharan countries are engaging in cyber issues, particularly cyber-security and opportunities for diplomatic engagement. African Union member states can easily draw inspiration from the UN Group of Governmental Experts (UN GGE) meetings, which expressed willingness for the first time in 2010 to work together to reduce the threat resulting from cyber-attacks, and to work towards a set of voluntary norms of responsible State behaviour in the cyberspace. An initiative proposed by Russia in 2011 during a UN General Assembly Resolution (66/24) (Meyer, 2015, pp. 55-58).

Cyber-diplomacy began in the US, based on publication of the US International Strategy for Cyberspace in 2011, which focus entirely on the international aspects of cyber issues. The strategy identifies a number of priorities (economy, network protection, law enforcement, military, internet governance, international development, and internet freedom), while relying on three pillars to pursue these objectives: diplomacy, defence and development (3Ds). The strategy is explicit on the use of diplomatic tools and resources in pursuit of cyber-related agenda. The US strategy led to the creation of the position of the Office of the Coordinator for Cyber Issues within the US State Department, while the Coordinator Christopher Painter became de facto the world's first cyber-diplomat. The office for cyber issues was assigned five key tasks (US State Department website, 2017):

- Coordinating the Department's global diplomatic engagement on cyber issues.
- Serving as the Department's liaison to the White House and federal departments and agencies on these issues.
- Advising the Secretary and Deputy Secretaries on cyber issues and engagements.
- Acting as liaison to public and private sector entities on cyber issues.
- Coordinating the work of regional and functional bureaus within the Department engaged in these areas.

Some Sub Saharan African countries are changing the dynamics, by adopting cybersecurity strategies addressing the international ramifications of cyber issues, and even stand-alone international strategies. However, the African Union is gradually reconfiguring cyber-diplomacy as the European Union's member states adopted Council Conclusions on Cyber Diplomacy in 2015 – the first time in which the term 'cyber diplomacy' was used in an official government document.

One of the main reasons for the institutional emergence of Cyber-Diplomacy was that too many departments and desks were dealing simultaneously with cyber issues, without coordination and overarching direction. More so, the creation of a focal point within the ministries of foreign affairs (MFA) was perceived as a manner to avoid fragmented reporting from the embassies abroad on cyber-related matters, and therefore to gain a more comprehensive view of the cyber developments and dynamics. AU members can explore the two main approaches to institutional streamlining in MFAs: either the creation of a new department centralizing all cyber-related activities, similarly to other thematic departments; or the establishment of a coordination unit, based on the principle that cyber issues are cross-cutting. It will be essential for African states to validate the principle that cyber issues are cross-cutting in order to develop a better framework and secure the cyberspace.

The emerging trends appeals for proper restructuring of the cybersecurity narrative of African states and the notion of cyber-diplomacy. The cyber-space is a new war yard, which cyber-diplomats have to redefine the traditional narrative of diplomacy, including maintaining peace and building mutual confidence between stakeholders, in a completely new environment, that is the digital space.

IV. Conclusion

The Rise of Cyber-Diplomats in Africa

There has been a paradigm shift in activities of cyber-diplomacy between international and world societies. More importantly, in the manner in which the operate, with concepts, technologies and practices, that more often than not were defined within the realm of cyber-diplomacy.

According Barry Buzan (2014, p. 165-166), the past decades have been marked with an emergent level of interaction between international society and world society as "People everywhere now understand that they are embedded in a single global economy (like it or not), and up to a point that they are also embedded in a single global culture and a single global environment (again, like it or not)." Although, "[t]here isn't a ready-made cosmopolitan alternative to the states-system", Buzan believes "there is increasing interplay and in some ways merger between the different pluralisms in the interstate and world society domains" (2015, p. 166). Indeed, many of the norms that regulate and give legitimacy to international society developed from world society (Clark, 2007, p. 13).

Cyberspace activities have mostly been conducted following a world society rationale best captured by the so-called multi-stakeholder model governing the internet, although states are now trying to come to terms with the importance of the field by incorporating it into the international society realm. All this, without excluding the realist international system, the sphere in which states co-exist and interact without a concern for shared values or norms. Whereas cases such as the *May 2015 when some renowned Indonesian hackers from Gantenger's Crew hacked and defaced the President of Kenya's site* evidence that state activity in cyberspace must not be limited normative law, reason cyber-diplomacy is redefining different tendencies in order to ensure a peaceful co-existence, defined by clear rules and principles: from a system of interactive units to a society of states. In that regard, cyber-diplomacy is to cyberspace what diplomacy is to international relations: a fundamental pillar of international society. Worth noting that the preamble of the African Union (AU) Convention on Cyber Security and Personal Data Protection highlights *the Principle of the African Information Society Initiative (AISI) and the Regional Action Plan on the Knowledge Economy (ARAPKE)*.

Unlike other areas of international life, cyberspace is constituted by a rather incipient set of binding normative arrangements and Africa states are gradually adapting to this realm. For instance, armed forces around the world are developing their own cyber capabilities, there are no *"parallel diplomatic processes to develop the agreed parameters for such operations"* (Meyer, 2012, p. 16), much is yet to be done to change the dynamics.

Conventions and national law have been promulgated to regulate the cyberspace, which had until then isolated the narrative of diplomacy. In 2013, the Head of the EU external cyber coordination revealed that 'there are very few nations where national cyber coordination is efficient and the state is able to speak with one voice in all international fora' (Tiirmaa-Klaar, 2013, p. 516). This appeals for a new wave of cyber-diplomats to engage in bilaterally and multilaterally discourse worldwide.

This paper argues that the structuring of cyber diplomacy is essential to Africa's engagement in global digital governance. For the AU to be a leading actor in this space, it must prioritize institutionalizing cyber diplomacy, fostering regional cooperation, and building capacity at the national level. Through these measures, Africa can contribute meaningfully to shaping the future of global cyber diplomacy.

References Références Referencias

1. Kibe (2018) An Experiment to Determine the Effect of Ethical Hacking on IT Administrator's Patch and Vulnerability Management Attitudes, a case of a leading telecommunications company. Masters of Science in Information Systems of the School of Computing and Informatics, University of Nairobi.
2. Ahmad, K., JayantShekhar, Kumar, N., Yadav, K.P. 2011. Policy Levels Concerning Database Security; International Journal of Computer Science & Emerging Technologies (E-ISSN: 2044- 6004) 368 Volume 2, Issue 3, page(s); 368-372.
3. Ajzen, I., Fishbein, M. 1980.Understanding Attitudes and Predicting Social Behavior. Englewood Cliffs, N.J.: Prentice-Hall.
4. Bulgurcu B., Cavusoglu H., Benbasat I. 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly [Online] Available from https://s3.amazonaws.com/academia.edu.documents/30986994/bulgurcucavusoglubenbasat.pdf?
5. Collier, M., Endler, D. 2014. Hacking Exposed: Unified Communications & VoIP Security Secrets & Solutions. McGraw Hill, New York.
6. Kharpal, A. 2015. Ethical hacking: Are companies ready? [Online] Available from https://www.cnbc.com/2015/06/17/are-companies-still-scared-of-white-hat-hackers.html [Accessed: 4th January 2018].
7. Prasad, M., Manjula, B. (2014). Ethical Hacking Tools: A Situational Awareness. Int J. Emerging Tec. Comp. Sc. & Elec.11, 33-38.
8. Bull, H. (2002 [1977]). The Anarchical Society. A Study of Order in World Politics.3rd Edition. Basingstoke: Palgrave.
9. Buzan, B. (2014). An introduction to the English school of international relations: the societal approach. Cambridge: Polity Press.
10. Carr, M. (2017). Cyberspace and International Order. In Suganami, H., Carr, M. & Humphreys, A. (eds.), The Anarchical Society at 40. Contemporary Challenges & Prospects (pp. 162-178). Oxford: OUP.
11. Clark, I. (2007). International Legitimacy and World Society. Oxford: OUP.Copeland, D. (2015). Digital Technology. In Cooper, A.F., Heine, J. & Thakur, R.(eds.) The Oxford Handbook of Modern Diplomacy (pp. 453-472). Oxford: OUP.
12. Deibert, R. (2015). The geopolitics of cyberspace after Snowden. Current History, January, 9-15.
13. Dunne, T. (1998). Inventing International Society. A History of the English School. Basingstoke: Macmillan Press Ltd.
14. Dunn Cavelty, M. (2007). Cyber-security and threat politics: US efforts to security the information age. London: Routledge.
15. Eriksson, J. & Giacomello, G. (eds.). (2010). International Relations and Security in the Digital Age, London: Routledge.
16. Fletcher, T. (2016). Naked Diplomacy. Power and Statecraft in the Digital Age. London: William Collins.
17. Gady, F.S. & Austin, G. (2010). Russia, the United States and cyber diplomacy: opening the doors, New York: East West Institute.
18. Hall, I. (2006). Diplomacy, Anti-diplomacy and International Society. In Little, R. & Williams, J. (eds.). The Institutions of Anarchical Society (pp. 141-161).Basingstoke: Palgrave Macmillan.
19. Harold, S.W., Libicki, M.C. & Stuth Cevallos, A. (2016). Getting to yes with China in cyberspace. Santa Monica: RAND Corp.
20. Hocking, B. & Melissen, J. (2015). Diplomacy in the digital age. The Hague: Clingendael Institute.
21. Hocking, B., Melissen, J., Riordan, S. & Sharp, P. (2012). Futures for diplomacy. Integrative Diplomacy in the 21st century. The Hague: Clingendael Institute.
22. Kello, L. (2013). The Meaning of the Cyber Revolution. International Security, 38(2), 7-40.
23. Kissinger, H. (2014). World Order. New York: Penguin Press.
24. Kleiner, J. (2008). The Inertia of Diplomacy. Diplomacy & Statecraft, 19(2), 321-349.
25. Meyer, P. (2012). Diplomatic Alternatives to Cyber-Warfare. The RUSI Journal, 157(1), 14-19.
26. Meyer, P. (2015). Seizing the Diplomatic Initiative to Control Cyber Conflict. The Washington Quarterly, 38(2), 47-61.
27. Mueller, M. (2017). Will the Internet Fragment? Sovereignty, Globalization and Cyberspace. Cambridge: Polity Press.
28. Neumann, I. (2002). The English School on Diplomacy (Clingendael Discussion Paper 79). The Hague: Clingendael Institute
29. Potter, E.H. (2002). Cyber-diplomacy: Managing Foreign Policy in the Twenty-first Century. Montreal: McGill-Queen's University Press.
30. Pouliot, V. & Cornut, J. (2015). Practice theory and the study of diplomacy: A research agenda. Cooperation and Conflict, 50(3), 297-315.
31. Sandre, A. (2015). Digital Diplomacy. Conversations on Innovation in Foreign Policy. Lanham: Rowman & Littlefield.
32. Adam Segal (2016) The Hacked World Order How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age, Philadelphia: Public Affairs.
33. Seib, P. (2016). The Future of Diplomacy. Cambridge: Polity.
34. Sending, O.J., Pouliot, V. & Neumann, I.B. (2015). Introduction. In Sending, O.S., Pouliot, V. & Neumann, I.B. (eds.). Diplomacy and the Making of World Politics (pp. 1-28). Cambridge: CUP.

35. Singer, P. & Friedman, A. (2014). Cybersecurity and Cyberwar. What Everyone Needs to Know. Oxford: Oxford University Press.
36. State Council of China. (2010). White Paper on the Internet in China. Beijing: Information Office of the State Council of the People's Republic of China.
37. Tiirmaa-Klaar, H. (2013). Cyber diplomacy: agenda, challenges and mission. In Ziolkowski, K. (ed). Peacetime Regime for State Activities in Cyber-space: International Law, International Relations and Diplomacy (pp. 509-31). Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. Office of the Coordinator for Cyber Issues: https://www.state.gov/s/cyberissues/, accessed on 20 February 2017.
38. White House. (2009). Cyberspace policy review: Assuring a trusted and resilient information and communications infrastructure. Washington DC: The White House.
39. White House. (2011). International strategy for cyberspace. Washington DC: The White House.
40. White House. (2015). FACT SHEET: President Xi Jinping's State Visit to the United States. Washington DC: The White House Office of the Press Secretary, 25 September.
41. Van der Meer, S. (2016). Enhancing International Cyber Security. A Key Role for Diplomacy. Security and Human Rights, 26, 193-205.