A Cyber-Diplomacy and Cybersecurity Awareness Framework (CDAF) for Developing Countries

Hendrik Zwarts, Jaco Du Toit and Basie Von Solms
University of Johannesburg, South Africa
hzwarts@yahoo.com
jacodt@uj.ac.za
basievs@uj.ac.za

Abstract: Cybersecurity is high on the agenda of national and international security policy discussions – mostly lead by diplomats. The practise of diplomacy has evolved since the Internet has become the backbone of society as we know it. Technological evolution has resulted in a significantly bigger and more accessible cyberspace, but the ability of governments and institutions to respond to and function in an expanding cyberspace seems to be lagging behind. The practice of diplomacy has similarly changed fundamentally and created a cyber-diplomacy environment where there is an increased utilization of inter alia social media platforms to achieve foreign policy goals. There is not enough attention given to practical processes to guide the new breed of diplomats in the evolving world of cyber-diplomacy and there is a need to improve the cybersecurity awareness of diplomats in all countries, but this article will focus primarily on developing countries. To mitigate potential cyber threats to diplomacy, diplomats need to be subjected to cyber-diplomacy orientation as well as functional cyber awareness training. Preliminary research conducted suggests that there is a gap between the existing and required cyber-diplomacy and cybersecurity awareness levels of diplomats from developing countries. The purpose of the article is to present a cyber-diplomacy and cybersecurity awareness framework (CDAF) that can be used by developing countries to equip their diplomats to play a more constructive role within the international cyber-diplomacy domain. The CDAF comprises of two distinct components, namely cyber-diplomacy and cybersecurity awareness, but this article will focus primarily on the cyber-diplomacy capacity building aspect of the CDAF. The CDAF was developed by following a design science research approach where a real-world problem was identified followed by an in-depth literature review to identify objectives and possible solutions to the problem. The subsequent outcomes were used to design and development of the CDAF. The article concludes with a critical evaluation of the proposed framework as well as how it can be incorporated into the developing cybersecurity knowledge modules of the Global Forum on Cyber Expertise (GFCE).

Keywords: cyber-diplomacy, cybersecurity, awareness, framework, cyber conflict, CDAF

1. Introduction

Countries should first and foremost be responsible for their citizens' safety and security; in an ever-changing world that is becoming more and more digitalised this includes protecting their citizens in cyberspace (Buzatu, 2021). While the world's economies continue to develop an increasing dependence on technology the development of cybersecurity capacity across the whole of cyberspace is critical to avoid what the Global Cyber Security Capacity Centre (GCSCC) refer to as "*cyber-ghettos*" – environments where cyber-harm may become prevalent and from where cyberattacks can easily be launched (Global Cyber Security Capacity Centre (GCSCC), 2021).

However, many countries lack the capacity to protect their own information and communication technologies (ICT) networks, to learn about cybersecurity threats and respond effectively to them through bilateral, regional and global engagements at both a technical and/or diplomatic level. The absence of such capacity leave state institutions and critical sectors (Buzatu, 2021). This lack of cybersecurity expertise is not isolated to technical issues, but also relates to a lack of cyber-diplomacy capacity – especially in developing countries.

This article will present a cyber-diplomacy and cybersecurity awareness framework (CDAF) that can be used by developing countries to equip their diplomats to play a more constructive role within the international cyber-diplomacy domain. The CDAF comprises of two components, namely cyber-diplomacy and cybersecurity awareness, but this article will focus primarily on the cyber-diplomacy capacity building aspect of the CDAF. The opening segment of the article reflects on the evolution of cyber-diplomacy followed by a discussion on different cybersecurity capacity building initiatives. The focal part of the article is the discussion and presentation of the CDAF.

2. Cyber-diplomacy – the new frontier

This section deals with evolvement of traditional diplomacy into cyber-diplomacy and the critical role that it plays within the modern, digitalised world. Cyber-diplomacy can be defined as "*diplomacy in the cyber domain* *and the use of diplomatic resources and the performance of diplomatic functions to secure national interests with regard to the cyberspace*" (Barrinha & Renard, 2017). It is closely interrelated to cybersecurity which is defined by the EU Cybersecurity Act (Regulation 2019/881, Article 2(1)) as "*the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats*". The rational of diplomacy being practiced in cyberspace is indisputable and yet it is a relatively new field. A brief recap of how diplomacy changed over time will contextualise the importance for countries to participate and contribute towards diplomacy in cyberspace i.e., cyber-diplomacy.

Wight (1979) defined diplomacy as "*the attempt to adjust conflicting interests by negotiation and compromise*" (Wight, 1979, p. 89). The objectives of diplomatic practice are:

- to enable communication in international politics,
- to negotiate treaties,
- to collect intelligence and information on countries,
- to circumvent and reduce conflict in international relations and,
- to represent the actuality of a civilization of states (Barrinha & Renard, 2017).

This view on diplomacy evolved over time and in 2004 Jönsson and Langhorne stated that diplomacy was no longer an activity solely undertaken by a select group of people as it has changed to encompass wider relationships and dialogues involving a broader array of entities such as regional and international intergovernmental (IGOs) or non-governmental (NGOs) organizations, multinational firms, pressure groups, advocacy networks and influential individuals (Jönsson and Langhorne, 2004). From this it can be deduced that (cyber) diplomats interact with any combination of the following role players on cyber related issues:

- Diplomats from other countries through bilateral or multilateral forums such as the UN.
- Various non-state actors such as leaders of internet companies (Facebook, Google)
- Technology entrepreneurs.
- Civil society organizations.
- Individuals

Over the last 20 years the Internet has become the backbone of society as we know it; it impacts on everyday economic-, social and political life, global mobility, communication, the Internet of things (IoT) and the storage of big data. This technological evolution has also resulted in a significantly bigger and more accessible cyberspace (Nye, 2014). Governments and institutions were initially slow to respond to and manage the swift advances in technology related to cyberspace (Nye, 2014) which resulted in a cyber-governance void in terms of the practice of diplomacy in cyberspace.

The practice of diplomacy created a cyber-diplomacy environment where there is a "*growing use of social media platforms by countries to achieve its foreign policy goals and proactively manage its image and reputation*" (Adesina, 2017). The revolution in ICTs is one of the significant factors currently impacting on diplomatic processes. It revolutionized the way people communicate and share information, thereby changing local and international political, social and economic playing fields. With the increased digitalization of diplomacy, the cyber threat to diplomacy also increased significantly (Adesina, 2017).

Nowhere as the Internet was initially unregulated and its governance mostly informally managed by software engineers over time governments became involved and cyberspace became more structured. As the occurrence of international meetings increased discussions by government IT experts on cyber issues also increased. The exponentiation and institutionalization of these meetings together with the expansion of cyber topics resulted in an increase in "online" political tussles which paved the way to cyber diplomacy (Deibert, 2015). Cyber issues were initially treated as technical issues then as peripheral aspects of national policies, before they were acknowledged as key foreign policy focus areas; diplomats stepped in because cyberspace became a diplomatic sphere (Barrinha & Renard, 2017). The development and growth of various social media platforms have also created a mutual jurisdiction for diplomacy between states and within states (Goundar, Chandra, Bhardwaj, Saber, Appana, 2020).

Unfortunately, the ability of governments and institutions to respond to and manage these rapid advances in cyberspace has lagged behind (Nye, 2014). This cyber governance void also transpires to the practice of diplomacy. The practice of diplomacy has likewise changed fundamentally as a result of digitalisation and created a cyber-diplomacy environment where there is a "*growing use of social media platforms by countries to achieve its foreign policy goals and proactively manage its image and reputation*" (Adesina, 2017). This revolution in information and communication technologies (ICTs) was one of the significant factors impacting on diplomatic processes. It revolutionised the way people communicate and share information, thereby changing local and international political, social and economic playing fields. With the increased digitalisation of diplomacy, the cyber threat to diplomacy also increased significantly (Adesina, 2017). Diplomats are busy changing traditional policy environments, methods, and processes to deal with the impact of digitalisation. This also necessitates a reform in the modus operandi of diplomatic services (Leira, 2019). The development and growth of various social media platforms have also created a jurisdictional communality for diplomacy between states as well as within a state (Goundar, Chandra, Bhardwaj, Saber, Appana, 2020). The "business as usual" days of conducting diplomatic functions have made way for a new frontier i.e. cyber diplomacy and there is a need to improve the cyber awareness of diplomats. To mitigate potential cyber threats to diplomats, they need to be subjected to cyber-diplomacy orientation as well as functional cyber awareness training. This will augment their level of cyber diplomacy as well as the security and integrity of dialogue, negotiations and other diplomatic processes (Al-Muftah, Weerakkody, Rana, Sivarajah, Irani , 2018).

From the discussion on the evolvement of cyber-diplomacy it is clear that all countries should participate and contribute towards diplomacy in cyberspace. Existing literature suggest that there are limited cyber awareness tools, training or support available for diplomats from developing countries to improve the overall quality of the dialogue and the benefits drawn from international discussions in support of better cybersecurity in the international arena. The only way to fill this void is through the development and utilisation of a structured capacity building framework focused on cyber-diplomacy and cybersecurity awareness. The next section will look at various capacity building components that could be used to formulate and develop such a CDAF.

3. Building cyber-diplomacy and cybersecurity capacity

Cybersecurity capacity building initiatives are fairly new, starting in 2013 with the formation of the Oxford GCSCC. Since then developing cybersecurity capacity is high on the agenda of most governments, international organizations (IOs) and companies. Numerous capacity-building initiatives, such as the International Telecommunications Union (ITU), the Potomac Institute, the Diplo Foundation, the Australia Strategic Policy Institute and the GFCE attest to the progress made towards capacitating countries in terms of cybersecurity. The main components encompassed in these capacity enabling efforts include aspects such as policy and strategy, sociocultural outlooks, knowledge and skills, protocols, law enforcement and technical criteria and capabilities (Dutton, Creese, Shillair & Bada, 2019). Dutton et al (2019) suggest that cybersecurity capacity building can be approached by differentiating between the dimensions defining cybersecurity, the broader policy environment that is influencing cybersecurity and the diversity of actors relevant to each of these dimensions. By adapting this approach critical attributes can be identified for incorporation into a CDAF. The following three subcategories will be discussed briefly:

- Dimensions of cybersecurity capacity building
- Capacity building role-players
- Cyber-diplomacy in developing countries

3.1 Dimensions of cybersecurity capacity building

Cybersecurity capacity building has evolved to the point where emergent frameworks include much more than technical cybersecurity aspects. Digitalisation and social media uptake in almost all aspects of modern-day living necessitated a paradigm shift w.r.t. cybersecurity capacity building to include aspects such as cybersecurity strategy and policy, awareness, legal and regulatory structures, threat response etc. (Dutton et al., 2019). The digitalisation of diplomatic processes has also questioned the capacity and preparedness of cyber-diplomats to effectively function in cyberspace; including the effectiveness of traditional diplomatic training methods. In an effort to identify capacity building dimensions and themes for the CDAF the following models and programs were dismembered:

- The Cybersecurity Capacity Maturity Model for Nations (CMM)

- The GFCE's agenda for cyber capacity building
- The Association of Southeast Asian Nations (ASEAN) Cyber Capacity Programme (ACCP)
- The twenty-one knowledge areas (KAs) of the CyBOK

The CMM differentiates between five capacity building dimensions, namely "d*eveloping cybersecurity policy and strategy, boosting responsible cybersecurity culture, creating cybersecurity knowledge and capabilities, creating operational legal and regulatory frameworks and risk mitigation through standards and technologies"* (Global Cyber Security Capacity Centre (GCSCC), 2021, p5).

The GFCE's agenda for cyber capacity building revolves around inter-connected themes that can be applied to national, regional and/or global cyber security developments i.e.:

- Cybersecurity policy and strategy
- Incident management and infrastructure protection
- Cybercrime
- Cybersecurity culture and skills, and
- Cybersecurity standards.

The focus areas of the ACCP include aspects such as cyber policy, cyber legislation, strategy development and cybersecurity incident response (Interpol, 2021)

Perhaps one of the most frequently used models to elucidate cybersecurity awareness training components is the twenty-one KAs of the CyBOK as it outlines a range of topics within the general scope of cybersecurity (Martin et al., 2021). The components of the CyBOK that cross cuts with the CMM, GFCE agenda and ACCP include standards, best practices, risk assessment and mitigation, regulatory requirements, social and behavioural factors impacting security, security culture and awareness, protecting if databases and data, malware and attack technologies etcetera. The following section will briefly look at the potential role-players that can contribute towards cybersecurity capacity building.

3.2 Capacity building role-players

Although the CDAF does not specifically address who is responsible for cybersecurity capacity building it is important to keep it in mind when developing specific KAs or learning outcomes. The Annual Conference of the GCSCC that was held at the University of Oxford in 2018 elaborates on the composition and interactions between various actors that should contribute towards build cybersecurity capacity (Global Cyber Security Capacity Centre, 2018). In the end the collection of actors can be simplified into three distinct groups, namely donors, implementers and recipients. The individuals responsible for cyber-diplomacy and cybersecurity capacity building will vary from country to country as well as from organisation to organisation. Table 1 presents the potential links between some of the more prominent cyber-diplomacy and cybersecurity awareness dimensions/themes and the potential role-players involved with each dimension/theme.

Table 1: Cyber-Diplomacy and cybersecurity awareness role-players

Dimensions/Themes	Role-Players						
	Experts	Researchers	Trainers	Networkers	End Users	Sponsors	Policymakers & Diplomats
Cybersecurity Policy & Strategy	x	x		x			x
Cybersecurity Culture	x	x		x	x		x
Legal & Regulatory Framework	x	x					x
Cybersecurity Standards	x	x	x	x			x
Cybersecurity Capacity Building	x	x	x	x		x	x
Incident/Risk Management	x	x					x
Cybercrime & Cyberattacks	x	x			x		x

Note: Derived from Dutton et al. (2019), Interpol (2021), GFCE (2017) and GCSCC (2021)

From Table 1 it is clear that policymakers and diplomats play a vital role within in cyberspace and cybersecurity. Whether all diplomats are suitably equipped to engage on all the intricacies of these dimensions is debateable. To contextualise the target audience of the CDAF the next section will take a concise look at cyber-diplomacy and cybersecurity in developing countries.

3.3 Cyber-diplomacy in developing countries

Every country in the world is exposed to cyberspace and is reliant on it to function in an interconnected world. The significance of cybersecurity awareness has increased over the last decade as governments, businesses and individuals' day-to-day activities around the world have moved more and more online. The challenge is that in most emerging economies these entities lack organizational, technological and human resources to secure their online activities and systems (Veale & Brown, 2020). The developing world has joined first world countries in relying on ICTs for the improvement of their populations' quality of life and economic growth. To access cyberspace developing countries predominantly uses services made by the developed world making them dependent on western-designed systems and protocols to regulate their actions in cyberspace. Cyber-diplomacy is needed to maintaining a constant dialogue between countries to develop norms of accountable government behaviour in cyberspace and addressing disagreements between role-players (Barrinha & Renard, 2020). Diplomatic interaction in global affairs is therefore an international security priority. Within this inter-connected world all countries strive towards advancing their own political and economic agendas – a function that is primarily steered by diplomats - in cyberspace. Cyberspace provides digital apparatuses to facilitate the effective execution of diplomatic strategies (Attatfa et al., 2020). Diplomats are busy changing traditional policy environments, methods, and processes to deal with the impact of digitalisation (Leira, 2019). Cyber-diplomacy is therefore an emerging field that gained momentum through its online application. Each country's uptake and implementation of cyber-diplomacy follows a different approach due to differences in foreign policies and perspectives on technology, but developed countries have progressed at a more rapid rate than most developing countries (Al-Muftah, Weerakkody, Rana, Sivarajah, Irani, 2018). It appears that there is no specific and/or not enough attention given to edify new diplomats in the evolving movement towards cyber-diplomacy. In the next section a CDAF will be presented that can be utilised to improve the cyber-diplomacy and cybersecurity awareness capacities of diplomats in developing countries.

4. A cyber-diplomacy and awareness framework for developing countries

Literature research conducted on the skills and capacity of diplomats in developing countries suggests that there is a gap between the existing and required cyber security awareness levels of these countries (Attatfa et al., 2020), (Zhang et al., 2021), (Sabillon et al., 2019). The integration of developments in cyber diplomacy and cybersecurity, as well as the available capacity building models resulted in the conception of the following CDAF that can promote the practice of cyber-diplomacy within developing countries:

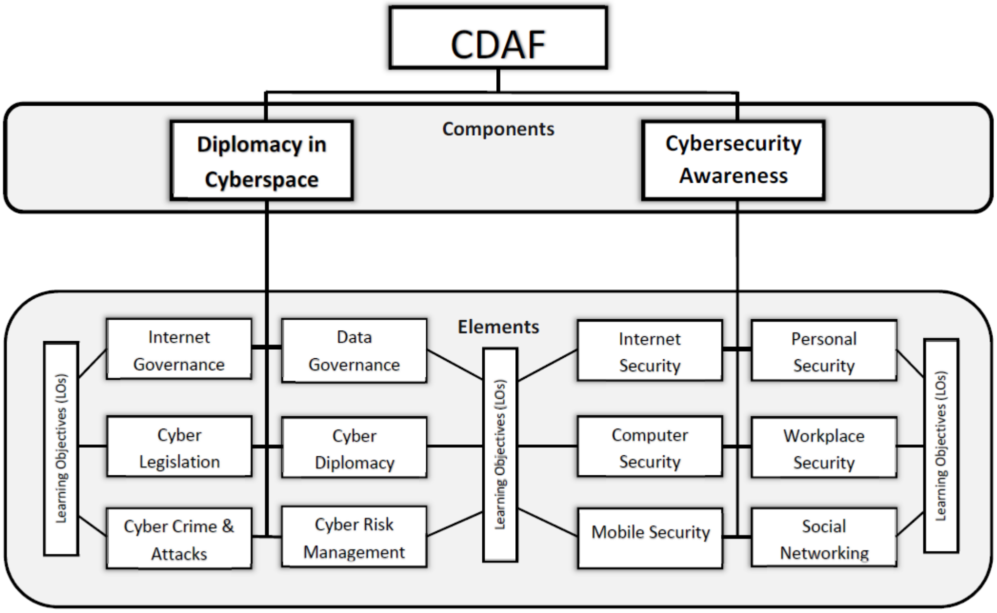

Figure 1: High-level view of cyber diplomacy and awareness framework (CDAF)

The CDAF can be broken down into components, elements and learning objectives:

- Components depict the combined subcategories of the core elements that encompass a country's cyber-diplomacy and cybersecurity awareness focus. In this case two components were identified, namely *Diplomacy in Cyberspace* and *Cybersecurity Awareness*.
- Elements provides a breakdown of the components into concentrated entities that are easier to delineate and understand. Certain elements can be more important or less important for a specific country depending on their cyber and diplomacy maturity level. The CDAF lists the following six elements under each of the two components:

Diplomacy in Cyberspace:

- 1. Internet Governance
- 2. Data Governance
- 3. Cyber Legislation
- 4. Cyber Diplomacy
- 5. Cyber Crime and Attacks
- 6. Cyber Risk Management

Cybersecurity Awareness:

- 1. Internet Security
- 2. Personal Security
- 3. Computer Security
- 4. Workplace Security
- 5. Mobile Security
- 6. Social Networking

Only the elements identified under *Diplomacy in Cyberspace* will be discussed further in the next section in an effort to explain how the framework can be tailor-made and/or adapted to meet specific requirements.

- Learning Objectives (LO) denotes the most basic parts of the CDAF and describes the attributes that could be included under an element. LO are not rigid nor finite and as such could be changed depending on the target groups' skills level on the particular element.

4.1 Constructing the CDAF

The components and elements of the CDAF were identified by linking the objectives and functioning of diplomacy in cyberspace with the dimensions of cybersecurity capacity building. The attributes of each of the elements were identified as the LOs necessary to encapsulate the essence of that specific element. The process to formulate elements and LOs for the *Diplomacy in Cyberspace* component is presented in Table 2.

Table 2: Breakdown of diplomacy in cyberspace element

Elements	Diplomatic Objective(s)	Learning Objectives
Internet Governance	Communication on international politics	Define cyberspace and its major components Provide an overview of the Internet & the major policies & procedures that governs it Identify the role players governing cyberspace Capacitate diplomats to participate in dialogue on internet governance issues
Data Governance	Collect intelligence and information on countries	Provide guidelines for the handling & storage of sensitive state-owned data Address diplomats' responsibilities toward data protection and data privacy Develop procedures and systems to protect ICT infrastructure & data Identify threats to information that is posted online

Elements	Diplomatic Objective(s)	Learning Objectives
		Describe how open-source information can be used for diplomatic purposes
Cyber Legislation	Circumvent and reduce conflict in international relations	Provide an overview of all the legislation/ policies w.r.t. cyber diplomacy Contextualise cyber legislation in relation to the regulatory framework of the diplomats' own country Formulize and institute cybersecurity legislation Establish regional & international jurisdictional cybersecurity cooperation Derive implementable regulations/SOPs in support of legislation Capacitate diplomats to engage their counterparts on legal issues w.r.t. cyberspace
Cyber Diplomacy	Represent the actuality of a civilization of states Negotiate treaties Communication on international politics	Differentiate between cyber diplomacy and digital diplomacy Contextualise diplomatic functions within cyberspace Explain how the interconnectivity of systems and interdependence of actors across cyberspace influences cyber diplomacy Describe cyberspace operations as a standard tool of diplomacy Explain how online tools, software, applications and systems can be applied to diplomatic activities Include best practices on digital negotiation Identify opportunities within cyberspace to augment diplomatic functions
Cyber Crime & Attacks	Circumvent and reduce conflict in international relations	Identify cyber security threats for online diplomatic actions as well as best practices on how to counter them Identify the major types of cybercrimes and cyber attacks Contextualise the role of diplomacy in cyber attacks List and discuss the main role players involved in cybercrime and cyberattacks Describe best practices to counter cybercrimes and cyber attacks Establish procedures and systems to deal with cyber incidents
Cyber Risk Management	Circumvent and reduce conflict in international relations	List cybersecurity threats for online diplomatic actions as well as best practices on how to counter them Provide an overview of the best practices regarding cyber risk management Provide guidelines for the development of a Cyber Risk Management Plan for diplomats Raise awareness on the benefits and dangers of AI & the IoT

Only the elements and LOs identified under *Diplomacy in Cyberspace* will be discussed further to explain how the framework can be applied and adapted to meet specific requirements of diplomats in a particular country.

4.2 Application of the CDAF

To demonstrate how the CDAF can be used the Cyber Diplomacy element will be applied to a South African (SA) perspective.

In SA the Department of International Relations and Cooperation's (DIRCO) is responsible for the recruitment, training and deployment of diplomats. DIRCO's mission is to "*formulate, coordinate, implement and manage South Africa's foreign policy and international relations programmes, and promote South Africa's national interest and values and the African Renaissance*" (DIRCO, 2020, p20)They have a Diplomatic Academy and

International School that presents training programmes aimed at capacitating SAs diplomats to contribute to the country's domestic priorities. Their 2020/2021 Annual Report elaborates on challenges concerning adapting to online activities. A number of references to digital-, economic-, public and virtual diplomacy are made, but the word "cyber" is mentioned only once in the 358 page report (DIRCO, 2020). The fact that cyber-diplomacy is not very high on DIRCOs agenda should be a concern. It does not suggest that SA diplomats are not involved in discussions on cybersecurity and/or cyberspace; diplomats from SA has been involved in various forums and committees related to cybersecurity and on on 11 June 2021 a virtual discussion with a SA delegate that attended the UN OEWG on Cyber Diplomacy indicated that a CDAF could add value to the efforts of DIRCO to capacitate their diplomats in terms of a broader view of cyber diplomacy as well as the technical and cyber awareness issues related to practising diplomacy in cyberspace. This poses the question whether there is a focused approach to equip SA diplomats to engage their international counterparts on issues related to cyberspace? The CDAF can provide a framework to either verify that the most important aspects of Cyber Diplomacy for instance are covered by the Diplomatic Academy or it can be used to create content-specific workshops or for altering existing programs.

Some of the following LOs that are listed in the CDAF under the Cyber Diplomacy element can be adopted to a SA context:

- 1. Differentiate between cyber diplomacy and digital diplomacy. Available literature submits that SA diplomats are familiar with the digital aspect of diplomacy – they know how to conduct online meetings, post information on different social media platforms, utilise digital data etcetera, but their understanding of cyber diplomacy as a concept seems to be lacking. The CDAF makes a clear distinction between cyber diplomacy and digital diplomacy.
- 2. Contextualise diplomatic functions within cyberspace. SA diplomats are trained in certain diplomatic programmes where they focus on South Africa's foreign policy and engagements with other international role-players. In this regard they are part of a number of forums such as the Southern African Development Community (SADC), African Union (AU), United Nations Security Council (UNSC) and BRICS. Cyber diplomacy in some of the countries that SA have diplomatic relations with has adapted swiftly and cyber issues are now decisively on their diplomatic agendas. SA and most of the developing countries face several challenges in this regard hampering their contribution and participation in the cyber diplomacy space (Borg Psaila, 2021). The CDAF can provide diplomats with a broader view of cyberspace and identify opportunities to augment their diplomatic functions.
- 3. Explain how the interconnectivity of systems and interdependence of actors across cyberspace influences cyber diplomacy. There needs to be a clear understanding amongst diplomats on cybersecurity aspects countries face; this includes legislative issues, cross-border investigations (because cyberspace transcends all borders), cyber threats to critical infrastructures, cyber countering measures etcetera (Borg Psaila, 2021). The CDAF can lay a solid foundation and create cybersecurity awareness in the digital environment where diplomats perform their functions.
- 4. Explain how online tools, software, applications and systems can be applied to diplomatic activities. Technology creates opportunities to interact with anyone - leading to cyberspace as a ground for international diplomacy. Social media networks are driving the growth of cyber diplomacy and in 2018 it was estimated that more than 70% of the world's head of states were using Twitter (Norwich University, 2018). The CDAF can provide diplomats with a holistic view of the latest and most secure online tools, software, applications and systems can be applied to diplomatic.
- 5. Include best practices on digital negotiation. The way nations relate diplomatically is changing. This is because cyber diplomacy is changing the way in which diplomats connect with their counterparts and the way governments communicate to their citizens. Statements by DIRCO that "*it is important that every effort is made to ensure the continuation of traditional diplomacy*" (DIRCO, 2020, p45) suggests that there is a void in terms of the value and application of cyber diplomacy. The CDAF can capacitate diplomats to effectively utilise digital negotiation to reach their diplomatic objectives.

As the CDAF is still under development, it can only be critically evaluated after a full draft version is available. At that stage a contact within DIRCO will be used to evaluate the CDAF in the live environment.

5. Conclusion

This article presented a CDAF that can be used by developing countries to equip their diplomats to play a more constructive role within the international cyber-diplomacy domain. Throughout the article it was echoed that different countries might have progressed further or are lacking behind on the terrain of cyber diplomacy, but the fact remains that every country in the world is present in cyberspace – whether a country represents himself in cyberspace or is a spectator depends on the cyber diplomacy capacity of that country.

References

Adesina, O. S. (2017). Foreign policy in an era of digital diplomacy. *Cogent Social Sciences*, *3*(1). https://doi.org/10.1080/23311886.2017.1297175

Al-Muftah, H., Weerakkody, V., Rana, N. P., Sivarajah, U., & Irani, Z. (2018). Factors influencing e-diplomacy implementation: Exploring causal relationships using interpretive structural modelling. *Government Information Quarterly*, *35*(3), 502–514. https://doi.org/10.1016/j.giq.2018.03.002

Attatfa, A., Renaud, K., & de Paoli, S. (2020). Cyber diplomacy: A systematic literature review. *Procedia Computer Science*, *176*, 60–69. https://doi.org/10.1016/j.procs.2020.08.007

Barrinha, A., & Renard, T. (2017). Cyber-diplomacy: the making of an international society in the digital age. *Global Affairs*, *3*(4–5), 353–364. https://doi.org/10.1080/23340460.2017.1414924

Barrinha, A., & Renard, T. (2020). The Emergence of Cyber Diplomacy in an Increasingly Post-Liberal Cyberspace. *Council on Foreign Relations*, 1–6. https://www.cfr.org/blog/emergence-cyber-diplomacy-increasingly-post-liberal-cyberspace

Borg Psaila, S. (2021). *Improving the practice of cyber diplomacy: Training, tools, and other resources PHASE I*. www.diplomacy.edu

Buzatu, A.-M. (2021). Promoting Openness , Prosperity , Trust and Peace and Security in Cyberspace. In *International Cyber Security Policy and Diplomacy Capacity BuildingProgram since 2014* (Issue April). http://www.ict4peace.org/

DIRCO. (2020). *ANNUAL REPORT 2020 / 21 DEPARTMENT OF INTERNATIONAL RELATIONS AND COOPERATION (DIRCO)*. http://www.dirco.gov.za/department/report_2020-2021/annual_report2020_2021.pdf

Dutton, W. H., Creese, S., Shillair, R., & Bada, M. (2019). Cybersecurity Capacity: Does It Matter? *Journal of Information Policy*, *9*(May 2021), 280–306. https://www.jstor.org/stable/10.5325/jinfopoli.9.2019.0280

Global Cyber Security Capacity Centre (GCSCC). (2021). *Cybersecurity Capacity Maturity Model for the Nations (CMM) 2021 Edition* (Issue CMM 2021 Edition). https://gcscc.web.ox.ac.uk/cmm-2021-edition

Global Cyber Security Capacity Centre, G. (2018). Collaborative Approaches to a Wicked Problem: Global Responses to Cybersecurity Capacity Building. *Annual Conference of the Global Cyber Security Capacity CentreSecurity Capacity Centre*, *February*, 1–35. https://doi.org/10.2139/ssrn.3660000

Interpol. (2021). *Fostering regional cooperation against cybercrime in Southeast Asia*. https://www.interpol.int/en/Crimes/Cybercrime/Cyber-capabilities-development/ASEAN-Cyber-Capacity-Development-Project

Leira, H. (2019). The Emergence of Foreign Policy. *International Studies Quarterly*, *63*(1), 187–198. https://doi.org/10.1093/isq/sqy049

Martin, A., Rashid, A., Chivers, H., Schneider, S., Lupu, E., & Danezis, G. (2021). *Introduction to CyBOK Knowledge Areas* (p. 22). The National Cyber Security Centre 2021. www.cybok.org

Norwich University. (2018). *Norwich University online*. https://online.norwich.edu/academic-programs/masters/information-security-assurance/resources/articles/role-of-computer-forensics-in-crime

Nye, J. S. (2014). The Regime Complex for Managing Global Cyber Activities. *CIGI Publications*, *1*, 1–15.

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. J. M. (2019). An effective cybersecurity training model to support an organizational awareness program: The Cybersecurity Awareness Training Model (CATRAM). A case study in Canada. *Journal of Cases on Information Technology*, *21*(3), 26–39. https://doi.org/10.4018/JCIT.2019070102

Veale, M., & Brown, I. (2020). Cybersecurity, Internet Policy Review. *Alexander von Humboldt Institute for Internet and Society*, *9*, 0–22. https://doi.org/https://doi.org/10.14763/2020.4.1533