STRENGTHENING RESILIENCE IN DIGITAL CLIMATE DIPLOMACY: A CYBERSECURITY PERSPECTIVE

Alexandru STANCIU, Sorin TOPOR, Ella Magdalena CIUPERCĂ
National Institute for Research and Development in Informatics – ICI Bucharest, Romania
alexandru.stanciu@ici.ro, sorin.topor@ici.ro, ella.ciuperca@ici.ro

Abstract: While international cooperation and the exchange of information between nations is the essence of contemporary diplomacy, climate diplomacy facilitates dialogue on various topics related to climate change and the environment. A significant part of the communication on this topic is based on digital technology, therefore a number of cyber threats can create wide-ranging problems between partners that can culminate in armed conflicts. At the level of dialogue partners, collaborative efforts to share best practices, cyber threat intelligence and cybersecurity capacity building initiatives will strengthen the global framework for international cooperation and climate diplomacy. The research proposed in this article aims to establish a conceptual framework within which international collaborative efforts can enhance collective resilience against cyber threats targeting information flows for digital climate diplomacy. Additionally, it is believed that promoting cyber literacy through the media can help educate the public on critical thinking, fact-checking, and skill-building to combat the spread of misinformation and disinformation about climate change.

Keywords: Diplomacy, Digital diplomacy, Climate diplomacy, Digital climate diplomacy, Cyber threats, Cybersecurity.

INTRODUCTION

Traditionally, the term "diplomacy" derived from the Greek word "diploun" (which means "to fold") and it was initially referred to a folded passed travel objects and documents. It often represented a travel permit that bestowed special privileges, usually granted by princes. Over time, the term broadened to include all formal documents issued by chancelleries, especially those containing agreements between rulers, until today when diplomacy has evolved into a distinct framework of communication between sovereign states and/or non-state international actors, with the purpose to promote and safeguard state interests, as well as to express dissatisfaction with the dynamics of their interactions. Diplomacy serves as a channel for clarifying positions, evaluating opinions, obtaining desired information, and persuading international actors to adopt specific stances within their relationships (Fransworth, 1992). According to Roach, Griffiths & O'Callaghan (2014), diplomacy encompasses not only the conduct, but also the substance of foreign affairs, being a comprehensive approach to managing and addressing various aspects of international affairs.

As a crucial component of governing communities, diplomacy has continuously adjusted to the transformations experienced by society and each technological revolution that has impacted communities has also had an impact over the field of diplomacy. In the 19th century, the emergence of steamships and railroads enhanced diplomatic mobility, while the invention of the telegraph enabled swift and direct communication (Jönsson & Hall, 2005). Diplomacy has expanded its agenda to include various responsibilities such as ceremonial duties, information gathering, fostering cultural and commercial relations, and promoting

https://doi.org/10.54852/ijcd.v4y202307

confidence in international law. These expanded functions reflect the increasingly complex interactions among actors within the international system, extending beyond traditional state actors.

More recently, globalization has changed the traditional specificity of diplomacy including from the perspective of subjects considered compatible with the field of international relations. Under the impact of increasing interdependence between nations, issues on the international agenda have multiplied and required much more attention than ever before. The issue of global security, sustainability, climate change, supporting sustainable development, conflict prevention and cooperation in pressing environmental issues have become more than ever constant presences on the diplomatic agenda (Argyros, Grossman & Rohatyn, 2007).

In addition, the nowadays revolution in communication technologies, including the advent of 24/7 news networks, the Internet, and the World Wide Web, has also significantly influenced diplomacy. These advancements have led to a new era of diplomacy, often referred to as digital diplomacy, which encompasses various aspects, including the use of social media platforms, online diplomacy initiatives, virtual meetings and conferences, and the dissemination of information through digital channels. It has expanded the reach and speed of diplomatic interactions, allowing for broader engagement and increased transparency.

On the other hand, the use of digital technologies can present a number of risks for the environment, such as:

1. Increased energy consumption: the cloud computing infrastructure, increasing data storage capabilities, processor power, and increasing number of communication networks can contribute to higher greenhouse gas emissions and energy consumption, impacting climate crises;

2. E-Waste: Rapid advances in digital technologies are shorting the product life cycles and an increasing the waste, especially from electronic devices (e-waste). Their improper handling and destruction can pollute the environment and cause health hazards for the population;

3. Technology block: Over-reliance on certain digital technologies can lead to lock-in effects concerning the adoption of new, greener solutions that can slow down the transition to a low-carbon economy.

The continuous change of the specific and content of diplomacy triggers the analysis of a new type of diplomacy situated at the intersection between digital technologies, climate change research and action policy topics, namely **digital climate diplomacy**.

This concept as well as its main components will be presented further. Since it is based on the use of digital technologies, a systematic approach to the issue of cybersecurity related to climate infrastructures is essential. In this regard, the main threats and vulnerabilities they face and the necessary measures to reduce the identified risks will be analyzed in order to be able to define a conceptual framework in which digital climate diplomacy and climate infrastructures are resilient to cybersecurity attacks.

DIGITAL CLIMATE DIPLOMACY

Digitization has brought about innovations in diplomatic practices, leading to the emergence of the concept of digital diplomacy, a concept that is frequently overlapping with terms such as e-diplomacy, diplomacy 2.0, and Twitter diplomacy.

In this sense, a number of countries, especially Western countries, have implemented certain reforms in their diplomatic services, based on the introduction of digital technologies. For example, the US diplomatic service has integrated a number of online tools on their website, while the US Institute of Peace, an influential institution funded by the US federal government, has developed, in the early 90s, an initiative for virtual diplomacy – The Virtual Diplomacy Initiative (Waller, 2007). In Europe, Lithuania modernized its consular service based on the use of digital technologies (Rimkunas, 2007), and Germany updated its internal communication procedures within the foreign service, after the introduction of local computer networks in 2002 (Rana, 2007). Since 2003, Canada has maintained an interactive website on its foreign affairs and international trade (Garson, 2007). Obviously, these initiatives are in addition to the increasingly widespread use of social media platforms to communicate directly with target audiences in different countries. Although there are many states that have initiatives to implement new digital technologies in their diplomatic activity, this is just a simple beginning, which has led to the launch of a new concept, that of digital diplomacy. Digital diplomacy should serve as a framework for understanding the innovations in the functions, capabilities, and organization of diplomacy in the era of widespread digital technology adoption.

As a rule, digital diplomacy takes place in online meetings, but it also manifests itself through social networks such as Twitter, WhatsApp, Facebook, YouTube, LinkedIn, etc. Through these platforms, diplomatic messages are exchanged for the development of contact networks and for easy interaction with the public. Diplomats and government officials use them to communicate directly with citizens, promote their foreign policy and get real-time feedback. Under this aspect, an online public diplomacy, in which digital communication tools can support and influence the positions and policies of a state, can be taken into consideration (Georgescu, Vevera & Cîrnu, 2020).

The use of artificial intelligence, data analysis, data collection, etc. technologies can help diplomats gain a better understanding of international developments, social and political trends and make informed decisions in the field of foreign policy, and the implementation technologies such as blockchain can ensure transparency, authentication and security of information exchange in cyberspace.

As a global problem, mitigating climate change requires international cooperation to coordinate efforts, share resources, and execute effective strategies. Through diplomacy, countries could adjust their efforts to share valuable climate data and research, and collaborate to improve climate models, leading to better predictions and strategies for mitigation and adaptation.

Therefore, the concept of climate diplomacy or environmental diplomacy have emerged with the objective to engage the wider public in the debate around climate changes. The concept of climate diplomacy does not have a single inventor or originator. It has emerged as a response to the pressing global issue of climate change and the recognition of the need for international cooperation to address its challenges and with diplomatic efforts and negotiations undertaken by governments, it tackles international organizations, and various stakeholders to address climate change, reduce greenhouse gas emissions, and promote sustainable practices. It has evolved over time through the collective efforts of policymakers, scientists, activists, and diplomats working together to tackle climate-related issues on the global stage.

Like all global issues today, in the cyberspace there is a wealth of information and opinions with the respect to climate change (especially on social networks). This is why, digital diplomacy can also aid in the negotiation and cooperation to promote sustainable technologies such as renewable energy, as well as carbon capture and storage technology.

Increasingly, climate diplomacy chooses the digital way for campaigns in favor of combating climate change, sending messages to educate citizens, offering platforms with real-time information on air quality, water quality or weather forecasting.

Digital climate diplomacy includes diplomatic efforts aimed at managing and mitigating the impacts of climate change. With the growth of digital technology and the rise of virtual spaces, climate diplomacy has extended into the digital realm in several ways, such as digital conferences and forums, online collaborative platforms, but also climate data sharing, digital advocacy and awareness, e-learning and capacity building or virtual simulation exercises, as presented in Figure 1.

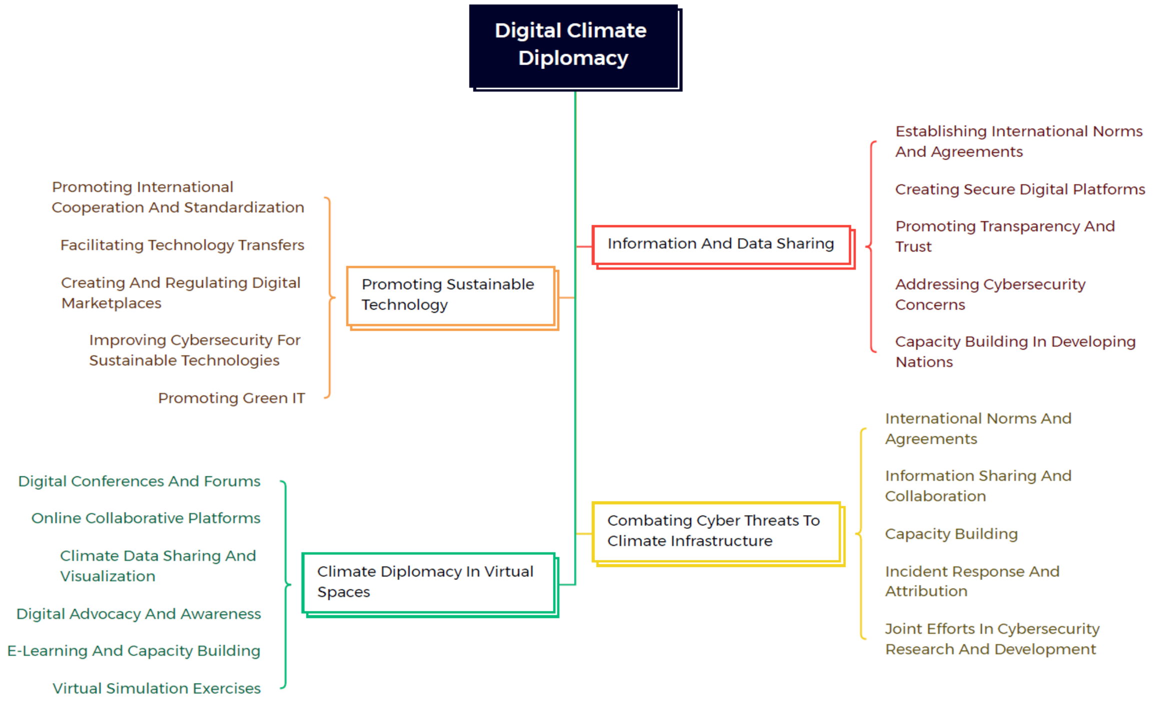
Digital Climate Diplomacy
Information And Data Sharing
Establishing International Norms And Agreements
Creating Secure Digital Platforms
Promoting Transparency And Trust
Addressing Cybersecurity Concerns
Capacity Building In Developing Nations
Promoting Sustainable Technology
Promoting International Cooperation And Standardization
Facilitating Technology Transfers
Creating And Regulating Digital Marketplaces
Improving Cybersecurity For Sustainable Technologies
Promoting Green IT
Combating Cyber Threats To Climate Infrastructure
International Norms And Agreements
Information Sharing And Collaboration
Capacity Building
Incident Response And Attribution
Joint Efforts In Cybersecurity Research And Development
Climate Diplomacy In Virtual Spaces
Digital Conferences And Forums
Online Collaborative Platforms
Climate Data Sharing And Visualization
Digital Advocacy And Awareness
E-Learning And Capacity Building
Virtual Simulation Exercises

Figure 1. Conceptual framework of digital climate diplomacy

Virtual meetings and conferences have become a key platform for international climate diplomacy, especially due to the COVID-19 pandemic, during which a number of important international climate meetings shifted to virtual formats (United Nations Climate Change, 2020). At the COP27 UN Climate Summit in Egypt, Slovenia showcased an inventive approach to hosting events and enhancing company and institutional presentations through the advanced metaverse platform, MetaCOP27 (Government of the Republic of Slovenia, 2022), a digital pavilion that facilitates improved, high-tech presentations for businesses and organizations and allows real-time interaction between individuals, fostering the growth of business communities through a decentralized operational mode, and adding value to their respective global value chains through digital representation. Online platforms can host simulation exercises where participants play the role of negotiators to understand the dynamics of international climate negotiations. Examples include also the World Climate Simulation (Climate Interactive, 2023), a role-playing exercise of the UN climate change negotiations.

Platforms such as the Climate Action Network (CAN), which connects NGOs worldwide in a shared push for sustainable climate policy, rely on virtual spaces to facilitate communication, coordinate efforts, and share expertise and resources.

Examples of virtual platforms allow for sharing and visualizing climate data on a global scale:

- The Global Climate Observing System (GCOS) provides comprehensive climate observations, where and when they are needed;
- The Global Earth Observation System of Systems (GEOSS) portal makes this information accessible to scientists, policymakers, and the public worldwide, and social media platforms are being used to mobilize public opinion on climate issues, to apply pressure on decision-makers, and to promote climate-friendly behaviors.

As the reliance on digital technology grows in every sector, so does the potential risk of cyber-attacks. This includes vital environmental monitoring systems, power grids (especially those shifting towards renewable sources), and other infrastructure crucial for addressing climate change. To this end, digital diplomacy plays an important role in creating international norms and agreements to combat such threats.

Digital climate diplomacy can work towards creating international norms and agreements on how states should act in cyberspace, especially concerning critical climate infrastructure. These agreements could establish "red lines" for state behavior, stating that attacks on critical climate infrastructure are against international law, and could invoke collective responses. Countries can use diplomatic channels to share information about potential threats, vulnerabilities, and effective defenses including using specialized agency such as the European Union Agency for Cybersecurity (ENISA).

International collaboration can be fostered to advance the state of cybersecurity research and development and adopt innovative solutions for protecting climate infrastructure from cyber threats. For example, the US and Israel have a joint program, the US-Israel Cybersecurity Cooperation Enhancement Act (United States Congress, 2016), which aims to boost cybersecurity research and development.

Sharing of data and modeling techniques through digital platforms can help nations understand their vulnerabilities and assess risks more effectively (the Climate Risk and Early Warning Systems –CREWS). The United Nations Office for Disaster Risk Reduction (UNDRR) brings countries and partners together to reduce disaster risk and losses, to ensure a safer, sustainable future, using their Sendai Framework Monitor as a tool for countries to report on their progress in implementing the Sendai Framework for Disaster Risk Reduction (United Nations Office for Disaster Risk Reduction, 2015).

Digital climate diplomacy should also play an essential role in both climate change mitigation and adaptation to the impact of climate changes, and the main dimensions of these efforts are through:

- Promotion of Green Technologies: adoption of international standards and agreements to facilitate the development, transfer, and use of green technologies (International Renewable Energy Agency – IRENA promotes the widespread adoption and sustainable use of all forms of renewable energy, as they provide a platform for international cooperation, a center of excellence, and a repository of policy, technology, resource, and financial knowledge on renewable energy);
- Data Sharing for Emissions Tracking: enable more effective sharing and use of data on greenhouse gas emissions, enabling more accurate tracking of progress towards emission reduction goals. For instance, the Global Carbon Project gathers and shares data on global carbon emissions and their impacts; the Carbon Disclosure Project (CDP) runs a global disclosure system for investors, companies, cities, states, and regions to manage their environmental impacts and it has built the most comprehensive collection of self-reported environmental data in the world; the Global Climate Observing System (GCOS) coordinates global climate data from multiple sources; INSPIRE – Infrastructure for Spatial Information in the European Community, a European Union initiative, aims to make available, harmonize and share geographic information among European organizations and member countries for better policy-making. The open science movement is a real help in this direction and examples as the Budapest Open Access Initiative (2002) and the Initiatives of the Max Planck Society (2003) are good practices to make scientific knowledge freely available;
- Advocacy and Awareness: for emissions reduction in international forums and using digital platforms to raise awareness about the importance of mitigation; for example, the United Nations' ActNow campaign (United Nations, 2023);
- Incentivizing Decarbonization: could take many forms, such as trade benefits for countries that reduce emissions or comply with certain environmental standards, and penalties or restrictions for those that don't (The Paris Agreement, facilitated by diplomatic efforts, encourages countries to intensify their efforts to reduce emissions) (French Ministry for Europe and Foreign Affairs, 2018);
- Collaborative Research and Development (R&D): developing common standards for research, sharing research results, or jointly funding research initiatives. Mission Innovation, (2023) is a global initiative of 24 countries and the European Commission, working to dramatically accelerate global clean energy innovation;
- Enhancing Transparency: establishing common reporting standards, creating platforms for data sharing, or working out agreements on how to verify countries' self-reported data as specified by the Enhanced Transparency Framework (ETF) under the Paris Agreement (World Research Institute, n. d.);
- Sharing Adaptation Strategies: facilitate the exchange of information about effective adaptation strategies and their implementation, sharing research findings, case studies, and best practices. The Climate Adaptation Knowledge Exchange (Climate Adaptation Knowledge Exchange, 2023) is a community-driven platform that helps users find

resources, share their own experiences, and interact with experts; the Global Adaptation Network (GAN) is an open-ended network for sharing knowledge on adaptation;

- Promoting Transfer and Adoption of Sustainable Technology: that help countries adapt to the impacts of climate change, implementing technologies that enhance resilience in agriculture, water management, and infrastructure design. It can also significantly contribute to the promotion of sustainable technologies by facilitating agreements between nations to cooperate on sustainable technology research and development, creating a more unified approach to tackling global environmental challenges. This can lead to standardization in sustainable technologies, making it easier for nations to adopt them. The International Telecommunication Union (ITU) works on the standardization and development of technologies, including those related to sustainability like ICTs for environmental sustainability and climate change monitoring; The Green Grid is an example of a non-profit, open industry consortium of end-users, policy-makers, technology providers, facility architects, and utility companies collaborating to improve the energy efficiency of data centers and business computing ecosystems;

- Capacity Building: can support efforts to build capacity in developing countries, helping them to adapt to the impacts of climate change by supporting education and training programs, improving access to relevant data and information, and providing technical assistance. To this end, the Global Green Growth Institute (GGGI) works with countries to build their capacity and develop inclusive and sustainable green growth plans;

- Promoting Climate Finance: negotiations about climate finance, which is crucial for supporting adaptation efforts, especially in developing countries. This might involve negotiations about who will contribute to international climate funds, how these funds will be distributed, and how their use will be monitored and evaluated. The Green Climate Fund (GCF), established within the framework of the United Nations Framework Convention on Climate Change – UNFCCC, is an international fund that assists developing countries in adaptation and mitigation practices to counter climate change;

- Facilitating Cross-Border Cooperation: In some cases, adaptation to climate change requires cooperation across borders. For example, countries that share river basins need to coordinate their water management strategies to deal with changing rainfall patterns. Digital climate diplomacy can facilitate these kinds of cross-border cooperation, like the Nile Basin Initiative (NBI), which is an intergovernmental partnership of 10 Nile Basin countries, providing a forum for negotiation and coordination on how to manage and share the benefits of the common Nile Basin water resources;

- Supporting Climate Services: facilitate international cooperation to improve climate services, such as by sharing weather data, improving forecasting models, and training meteorologists (the World Meteorological Organization – WMO);

- Addressing Loss and Damage: negotiate international approaches to deal with these losses and damages (The Warsaw International Mechanism for Loss and Damage, WIM, 2023, under the UNFCCC, addresses loss and damage associated with impacts of climate change in developing countries that are particularly vulnerable to the adverse effects of climate change).

In the above-mentioned areas, digital climate diplomacy can help countries to work together, share resources, and coordinate their efforts to mitigate and adapt to climate change, as its role is multifaceted, involving everything from information sharing and capacity building, to complex negotiations about finance, incentives, and cooperation agreements.

ADDRESSING CYBER THREATS TO CLIMATE INFRASTRUCTURE

Climate infrastructure, which encompasses a broad array of systems, from meteorological data collection networks, to renewable energy plants and smart grids, is increasingly relying on digital technologies and Internet connectivity. While this brings efficiency and sophistication, it also exposes these critical infrastructures to potential cyber threats.

The most important risks and vulnerabilities that represent challenges for climate infrastructure are:

1. Technologies inadequate to contemporary cyber-attacks: Malicious actors, individual hackers or grouped in criminal or terrorist organizations, can strike critical digital infrastructures, communication networks and databases involved in climate diplomacy. Cyber-attacks can disrupt critical infrastructures operations, compromise sensitive information and undermine trust between nations. Climate diplomats can be targeted by e-mails, SMS messages (SMS Phishing) or deceptive online platforms, voice messages (Voice Phishing) or deep-fake products, all of which posing risks to data security and privacy. Ransomware attacks can cripple digital systems and disrupt climate infrastructure operations, causing financial losses or other potential compromises of sensitive information. DDoS attacks or other forms of interference can disrupt virtual meetings, cause delays and other negative effects on diplomatic processes;

2. Data and information specific to climate diplomacy can also be affected by breaches of cybersecurity procedures and data leakage. They can influence climate negotiations and strategies with serious diplomatic consequences. Unauthorized access or leaks of sensitive information can damage reputations, hinder diplomatic efforts and weaken international cooperation on climate change;

3. Disruption of virtual meetings can have disastrous effects on diplomatic negotiation by interfering with the proper functioning of video conferencing platforms and communication channels;

4. Disinformation campaigns through digital channels can exploit digital communication platforms, influencing public opinion and undermining trust in scientific data, by spreading false or misleading information about climate change;

5. The increasing reliance on digital communication platforms and virtual meetings in climate diplomacy may reduce the frequency of interpersonal diplomatic engagements. Although digital platforms offer convenience and budget savings, it is not possible to completely replace them due to the benefits of human, face-to-face interactions. Only these can quickly build mutual trust, foster personal connections and facilitate nuanced negotiations. Finding a balance between digital and physical diplomacy is critical to ensuring effective climate diplomacy outcomes;

6. The use of digital technologies in climate diplomacy raises some ethical considerations such as responsible data collection and use, algorithmic biases and legal privacy concerns. The standards and procedures adopted must ensure transparency and facilitate the application of ethical norms regarding the use of digital technology in climate governance. Digital technologies used in climate diplomacy are vulnerable to cyber threats and attacks. Ensuring robust cybersecurity measures and building resilience against cyber incidents are critical to protecting critical climate data, infrastructure and communication channels. Digital technologies such as remote sensing, satellite imagery, other early warning systems, as well as data analysis processes play a vital role in monitoring and verifying climate change. The integration of artificial intelligence in climate modeling and prediction of specific events must be done only with respect to ethical considerations in environmental climate governance;

7. Climate diplomacy relies on strong data security measures to protect against cyber-attacks and unauthorized access to climate-related data, and the lack of generally valid agreements in the field can undermine trust and cooperation between nations. It is important to recognize that the field of cybersecurity is a dynamic one and a proactive and adaptive approach, periodic assessments and updates of security strategies are essential factors to face specific risks in the evolution of climate diplomacy;

8. Finally, yet importantly, systems can also be subject to internal threats from insiders with access to digital databases. Through negligence or malicious intent, they may either abuse access privileges, manipulate data and information, or facilitate the leakage of sensitive information. Implementing strict access control procedures, monitoring mechanisms, and adopting educational programs to raise employee awareness of the associated cyber threats can help mitigate these cyber vulnerabilities.

Among the measures that can mitigate the value of the attacks or reduce the stated digital risks, the following can be proposed:

- Implementation of robust cybersecurity measures including firewalls, encryption, access controls, intrusion detection systems. The use of secure communication protocols and of encrypted communication channels helps maintain the confidentiality and integrity of climate diplomacy discussions and negotiations;

- Regular backup and recovery of data through specific procedures help establish robust data recovery mechanisms and can mitigate the effects of cyber incidents. Backing up critical climate data and storing it securely in physically separate locations can ensure data availability, even in the event of a cyber-attack or data loss;

- Conduct regular vulnerability assessments and penetration tests. They can identify the weak points of the digital systems and allow the timely remediation of the identified problems;

- Employee training and awareness and ensuring a heightened level of awareness of the effects of common cyber threats and social engineering techniques used in other events can mitigate the effects of risks from human error and insider threats;

- Incident response planning through appropriate plans, procedures and measures that can ensure a rapid and effective response to specific events, reducing the potential impact on climate diplomacy and data security operations.

Continuous monitoring and adaptive governance involve regularly monitoring cyber threats, technological advances and emerging risks, with the integration of updated cybersecurity measures and policies into climate diplomacy. At the same time, prioritizing cybersecurity measures and proactive measures to avoid specific risks can increase the resilience of climate diplomacy, maintain data security and stimulate international collaboration in combating climate change.

Third-party risk management can be achieved by delegating the competences of independent specialized services. They will continuously check and manage third party providers and essential service providers, as well as the accepted level of cybersecurity. Assessing their cybersecurity practices, contractual obligations and data protection measures will minimize the associated risks by outsourcing digital services in climate diplomacy.

Continuing skills training programs are also essential for diplomats. Given the nature and evolution of cyber threats, for policy makers and climate professionals engaged in diplomatic activities, collaboration with cybersecurity experts can provide valuable insights and guidance on identifying and addressing cyber risks in climate diplomacy. This collaboration can help design and implement robust cybersecurity strategies tailored to the specific needs and challenges of climate diplomacy. Another form of collaboration is with specialized entities, from the private sector, in public-private partnerships. Thus, expertise, resources and advanced cybersecurity solutions can be leveraged to enhance the security of digital infrastructures and data protection in climate diplomacy. At the same time, participation in cyber exercises and simulations can help test and strengthen the training of diplomatic entities in identifying an appropriate response to cyber incidents, in order to improve the overall resilience of digital systems and the personnel that serve them.

CONCLUSIONS

International cooperation and information sharing between nations can help identify and address cyber threats in climate diplomacy. At the level of dialogue partners, collaborative efforts may include the exchange of best practices, cyber threat intelligence, and security capacity building initiatives. In addition, international cybersecurity cooperation will strengthen the global framework for international cooperation and can facilitate the exchange of cybersecurity information and best practices that will find applicability in climate diplomacy. Collaborative efforts can enhance collective resilience against diverse cyber threats, such as those resulting from military conflicts (the war in Ukraine). Thus, the development of international cybersecurity policies, regulations, and legal norms can provide guidance and enforcement mechanisms for addressing cyber risks in climate diplomacy.

The importance of public engagement and participation in climate diplomacy should not be overlooked. Digital technologies provide avenues for increased citizen engagement and participation through online platforms, social networks and digital campaigns to increase education and stimulate dialogue for climate action. In this sense, ensuring inclusion and accessibility for diverse communities is vital for effective public engagement. Bridging the digital divide and encouraging international cooperation by improving digital infrastructure, expanding Internet access and improving digital literacy in disadvantaged regions bring added value to climate diplomacy operations. In addition, promoting cyber literacy through the media can help educate the public about critical thinking, fact-checking, and building skills to combat the spread of misinformation about climate change.

REFERENCE LIST

Argyros, G., Grossman, M. & Rohatyn, F. (15 October 2007) *The Embassy of the Future*. Center for Strategic and International Studies (CSIS). Report, p. 1. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/embassy_of_the_future.pdf [Accessed 17th June 2020].

Budapest Open Access Initiative. (2002) *Budapest Open Access Initiative*. https://www.budapestopenaccessinitiative.org/ [Accessed 21st June 2023].

Climate Adaptation Knowledge Exchange – CAKE. (2023) *About CAKE*. http://www.cakex.org/about [Accessed 22nd June 2023].

Climate Interactive. (2023) *World Climate Simulation*. https://www.climateinteractive.org/programs/world-climate/ [Accessed 21st June 2023].

Fransworth, D. (1992). *International Relations: An Introduction*. 2nd ed. Chicago, Nelson-Hall.

French Ministry for Europe and Foreign Affairs (2018). *Paris Call for Trust and Security in Cyberspace*. https://pariscall.international/en/ [Accessed 21st June 2023].

Garson, R. (2007) Canada' s Foreign Ministry: Online and Interactive. In: Rana, K. S. & Kurbalija, J. (eds.) *Foreign Ministries: Managing Diplomatic Networks and Optimizing Value*. Malta and Geneva, DiploFoundation, pp. 212-224.

Georgescu, A., Vevera, V. & Cîrnu, C. E. (2020) The diplomacy of systemic governance in cyberspace. *International Journal of Cyber Diplomacy*, 1(1), 79-88.

Government of the Republic of Slovenia (18 November 2022). *Slovenia launched METACOP27 - First ever COP event in metaverse*. https://www.gov.si/en/news/2022-11-18-slovenia-launched-metacop27-first-ever-cop-event-in-metaverse/ [Accessed 21st June 2023].

Initiatives of the Max Planck Society. (2003) *Berlin Declaration on Open Access to Knowledge in the Sciences and Humanities*. https://openaccess.mpg.de/Berlin-Declaration [Accessed 21st June 2023].

Jönsson, C. & Hall, M. (2005) *Essence of Diplomacy*. USA, Palgrave MacMillan.

Mission Innovation. (2023) *About Us*. http://mission-innovation.net/about-mi/ [Accessed 21st June 2023].

Rana, K. (2007) MFA Reform – Global Trends. In: Rana, K. S. & Kurbalija, J. (eds.) *Foreign Ministries: Managing Diplomatic Networks and Optimizing Value*. Malta and Geneva, DiploFoundation, pp. 20-43.

Rimkunas, A. (2007) *The Modernization of the Lithuanian Consular Service in Response to Global Challenges*. In: Rana, K. S. & Kurbalija, J. (eds.) *Foreign Ministries: Managing Diplomatic Networks and Optimizing Value*. Malta and Geneva, DiploFoundation, pp. 186-191.

Roach, S. C., Griffiths, M. & O'Callaghan, T. (2014). *International Relations: The Key Concepts*. New York, Routledge.

United Nations. (2023). *ActNow Climate Campaign*. https://www.un.org/en/actnow/ [Accessed 21st June 2023].

United Nations Climate Change. (2020) *Climate Dialogues*. https://unfccc.int/conference/un-climate-change-dialogues-2020-climate-dialogues [Accessed 21st June 2023].

United Nations Office for Disaster Risk Reduction. (2015) *Sendai Framework for Disaster Risk Reduction 2015 – 2030*. https://www.undrr.org/publication/sendai-framework-disaster-risk-reduction-2015-2030 [Accessed 21st June 2023].

United States Congress. (2016) *H.R.5843 – United States-Israel Cybersecurity Cooperation Enhancement Act of 2016*. https://www.congress.gov/bill/114th-congress/house-bill/5843/ [Accessed 21st June 2023].

Waller, J. M. (2007) *The Public Diplomacy Reader*. Washington DC, Institute of World Politics Press.

Alexandru STANCIU

Is scientific researcher 3rd degree in ICI Bucharest. He received a PhD in System Engineering at the Politehnica University of Bucharest in 2013. He is interested in, and has contributed to such domains as: cloud architectures for distributed control systems, Big Data administration and analysis, IoT, blockchain technology.

Sorin TOPOR

Is a cyber security specialist in the "Protection of Critical Infrastructures" Service at the National Institute for Research and Development in Informatics - ICI Bucharest, specializing in security studies, electronic warfare and defense against terrorism. He graduated his PhD in Military Sciences at the ”Carol I” National Defense University in 2000. In the last 20 years he has held various leadership positions in academic education. He was project director and member of various research teams for international and national projects. He also published 9 books and over 100 specialist works.

Ella Magdalena CIUPERCĂ

Is the Head of Critical Infrastructure Service of ICI Bucharest being specialized in security studies, sociology and social psychology (especially the study of innovation and social change). She defended her PhD in sociology at Bucharest University in 2004. In the last 20 years, she held different management positions in higher education. Over the last years, she has been a project director and member of different research teams for international and national projects. Also, she published more than 50 books and articles.