A BLOCKCHAIN-BASED APPLICATION AS PART OF A DIGITAL DIPLOMACY APPROACH TO FACILITATE AND ADVANCE CYBER DIPLOMACY

Carmen Elena CÎRNU, Paul-Cristian VASILE
National Institute for Research and Development in Informatics – ICI Bucharest
carmen.cirnu@ici.ro, paul.vasile@ici.ro

Abstract: Cyber Diplomacy is a domain of diplomacy concerned with the intersection between international relations and the research, implementation and regulation of digital technologies, as well as the management of their consequences, including advanced ones such as Artificial Intelligence and blockchain. This article presents a blockchain-based application meant to facilitate the digital component of cyber diplomacy, by allowing diplomats to communicate securely in an ever-more challenging environment for communications security.
Keywords: Blockchain, Cyber diplomacy, International relations, Internal communications.

INTRODUCTION

The world and its underlying systems-of-systems are undergoing profound structural and functional transformations for a variety of reasons. One of these reasons is digitalization, and it is taking place in the context of rapid advancement of digital technologies, connectivity and the penetration of digital technologies in all geographic spaces and in all walks of life (Georgescu et al., 2019b). As a result of the digital revolution, cyber issues have come to the forefront of state concerns, through elements such as cybercrime, protection against hackers and terrorists, cyber-attacks as a tool of inter-state conflict in the context of hybrid warfare, and also the underlying risk for cascading disruptions stemming from the tighter couplings between infrastructure systems which cyber interconnectivity promotes (Georgescu et al., 2020b). However, these many issues cannot be decided and resolved simply at national level. Since cyberspace is only in a limited sense circumscribed by geographical space, through the location of physical infrastructure, this environment simultaneously promotes connectivity divorced from geography and is much less amenable to jurisdictional authority and decision making, which is a key tool for states. Therefore, states must cooperate, to the largest possible extent, in order to collectively address the great risks, vulnerabilities and threats engendered by the dependence on networked transborder infrastructure systems that support economic, political and social life. This cooperation, and even more nuanced forms of cooperation, such as those limiting or regulating aggression against each other, falls under the umbrella of the Cyber Diplomacy (CD) concept, which describes the sum total of the attempts to manage, in an international relations setting, the consequences of digitalization.

In addition to the practices of Cyber Diplomacy, it also requires tools and instruments of various nature to support diplomats and other cyber diplomacy practitioners. This article presents one such tool, for secure communications within a Ministry of Foreign Affairs, but

easily converted for other uses, and based on blockchain technology in order to ensure the security of information transmission.

Within the National Institute for Research and Development in Informatics ICI Bucharest, the Cyber Diplomacy Center aims to advance research into this field and to invest in capability creation to support CD and related research, including in practical terms. The application presented herein was the result of an internal project as part of a series of deliverables for the Center. The application is functional, but has not been implemented for live testing, so it can be considered at demonstration level. While it can benefit from new features, it is currently feature-complete as a minimum viable product that could be implemented by a Ministry of Foreign Affairs or converted to support communications for any governance-related network, such as in critical infrastructure protection, public administration among territorial units or crisis and emergency response facilities.

DIGITAL VERSUS CYBER DIPLOMACY

The product described in this article is an application which supports a service facilitating the practice of cyber diplomacy. The application itself is an example of digital diplomacy, which we would define as the use of novel digital technologies and means to support traditional diplomatic activities (Georgescu et al., 2020b). Cyber Diplomacy, which the application especially supports, alongside other forms of diplomatic work, consists of activities specifically related to the regulation between states and other subjects of international relations of the risks, consequences and opportunities generated by emerging digital technologies, such as Artificial Intelligence and blockchain (Georgescu et al., 2020a).

Barrinha and Renard (2017) consider that "cyber-diplomacy is an emerging international practice that is attempting to construct a cyber-international society, bridging the national interests of states with world society dynamics – the predominant realm in which cyberspace has evolved in the last four decades". van der Meer (2016, p. 102) argues that defense and deterrence must give way to diplomacy in cybersecurity affairs in the long term in order to ensure international security. "Cyber arms races" and "tit for tat" escalations are destabilizing factors (Georgescu et al., 2019b). These can only be addressed and mitigated through diplomatic overtures, aimed at building confidence, generating appropriate international norms and other results of diplomatic processes. The former especially enhance "interstate cooperation, transparency and predictability, with the aim to reduce the risks of misperception, escalation, and conflict entailed by cyberthreats" (van der Meer, 2016, p. 103).

Cyber Diplomatic processes are ultimately necessary for the systemic governance of the global critical infrastructure system-of-systems on which our economic, social and political lives have come to depend, and which is interdependent, complex, transborder, and requires a multistakeholder approach to begin managing the risks, vulnerabilities and threats it entails (Georgescu et al., 2019a). The service which the application presents in this article supports such processes by facilitating secure communication, by being scalable, customizable and amenable to further development, while enabling a response to the deteriorating security environment also for diplomatic processes.

THE CYBER DIPLOMACY APPLICATION

The architecture of the CD Application is systematized in Figure 1.

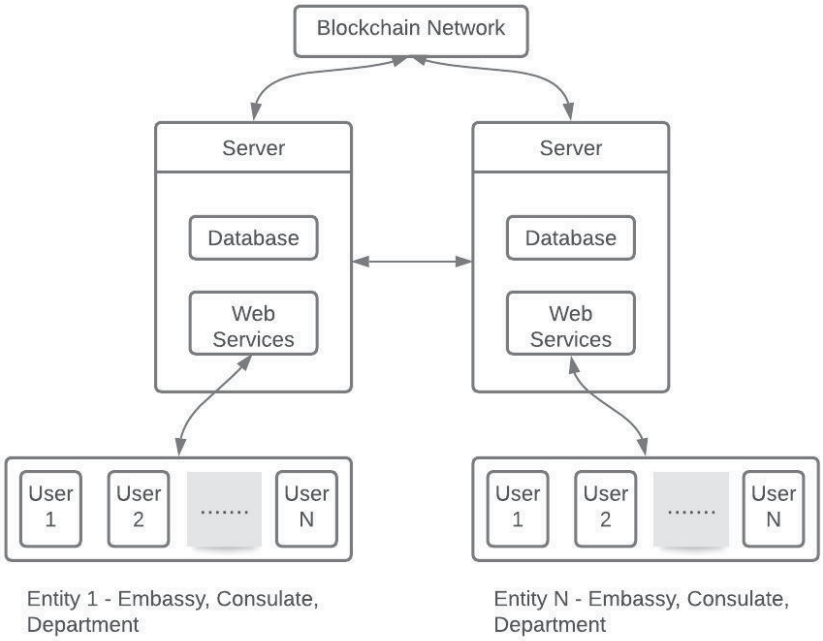


Figure 1. *The architecture of the Cyber Diplomacy service*

There are three main components:

- The blockchain network – provides information transmission for the Cyber Diplomacy service (supported by the application). The blockchain contains a growing ledger of information, divided into blocks and secured cryptographically. Secure storage of information, data transfers and links between authorized entities and users are facilitated by the blockchain network. More information can be found in the next section.
- The servers – provide services to client applications on the same computer or on different ones. The servers have multiple components, including databases and web services modules. The servers handle data transmission, as the blockchain only transmits the public key required for decrypting the data, allowing messages to be of varying types and sizes.
- The entities – in this case, the entities are part of a diplomatic network, representing embassies, consulates, departments within them or within the Ministry of Foreign Affairs. Users are defined as part of entities and privileges and hierarchies are assigned to enable management within the service of the flow of information. Entities and users interact with web services through various devices connected to the application platform.

The application was designed to feature the blockchain component in the background and would not be noticed by the average user. As part of the development process, a typical list of capabilities of usability, comfort and security were added, including login processes, systems to add users and control privileges, and systems to manage the messages received (though no archive function has been implemented at this stage).

Figure 2 shows the login screen of the application and the screen for identity confirmation.

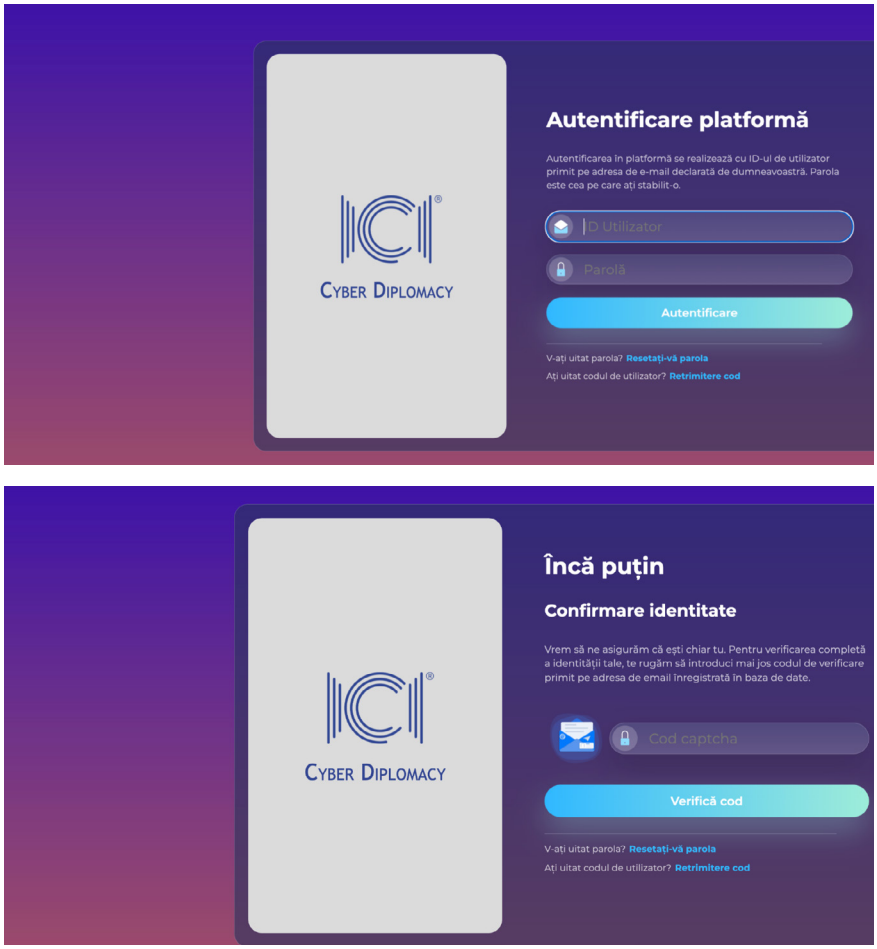
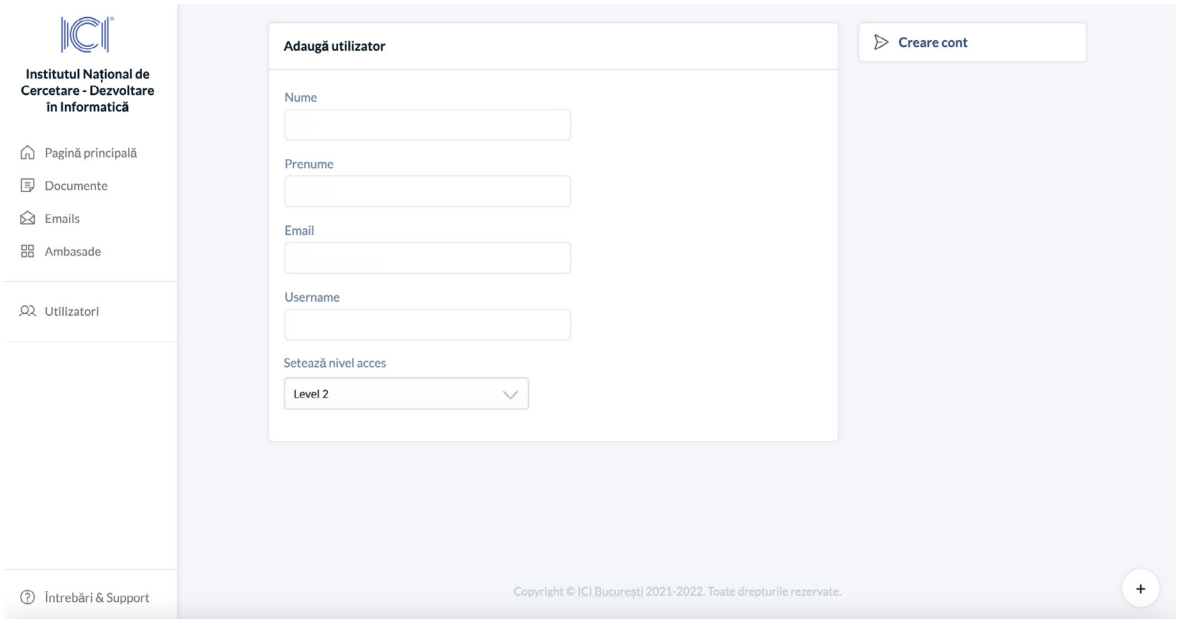


Figure 2. *a) Login screen for the application (up); b) Screen for identity confirmation (down)*

Figure 3 presents the main menu screen for a particular user.

Figure 3. *Main menu for users*

Figure 4 presents the main interface elements for registering entities and users, with several characteristics related to privileges.



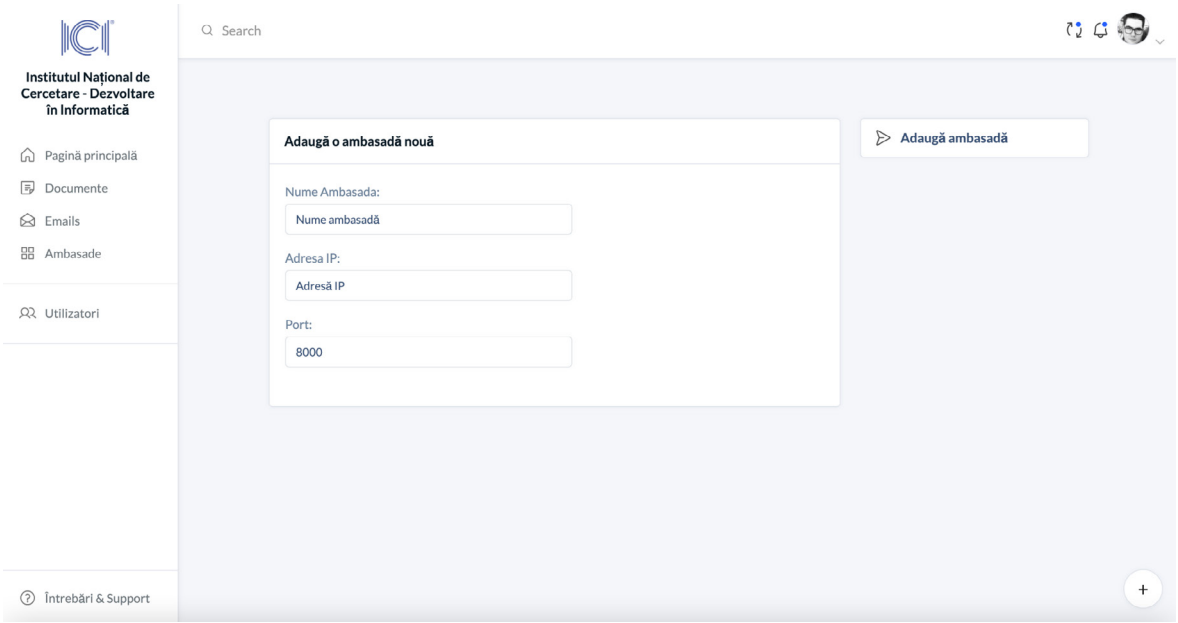


Figure 4. *Interfaces for adding new a) users (up) and b) new embassies (down)*

Figure 5 shows the main interface elements for users, related to message management and creation. Messages, in the current version, can be text and multimedia based. For multimedia content, picture files up to 2 Mb and video files up to 100 Mb are supported.

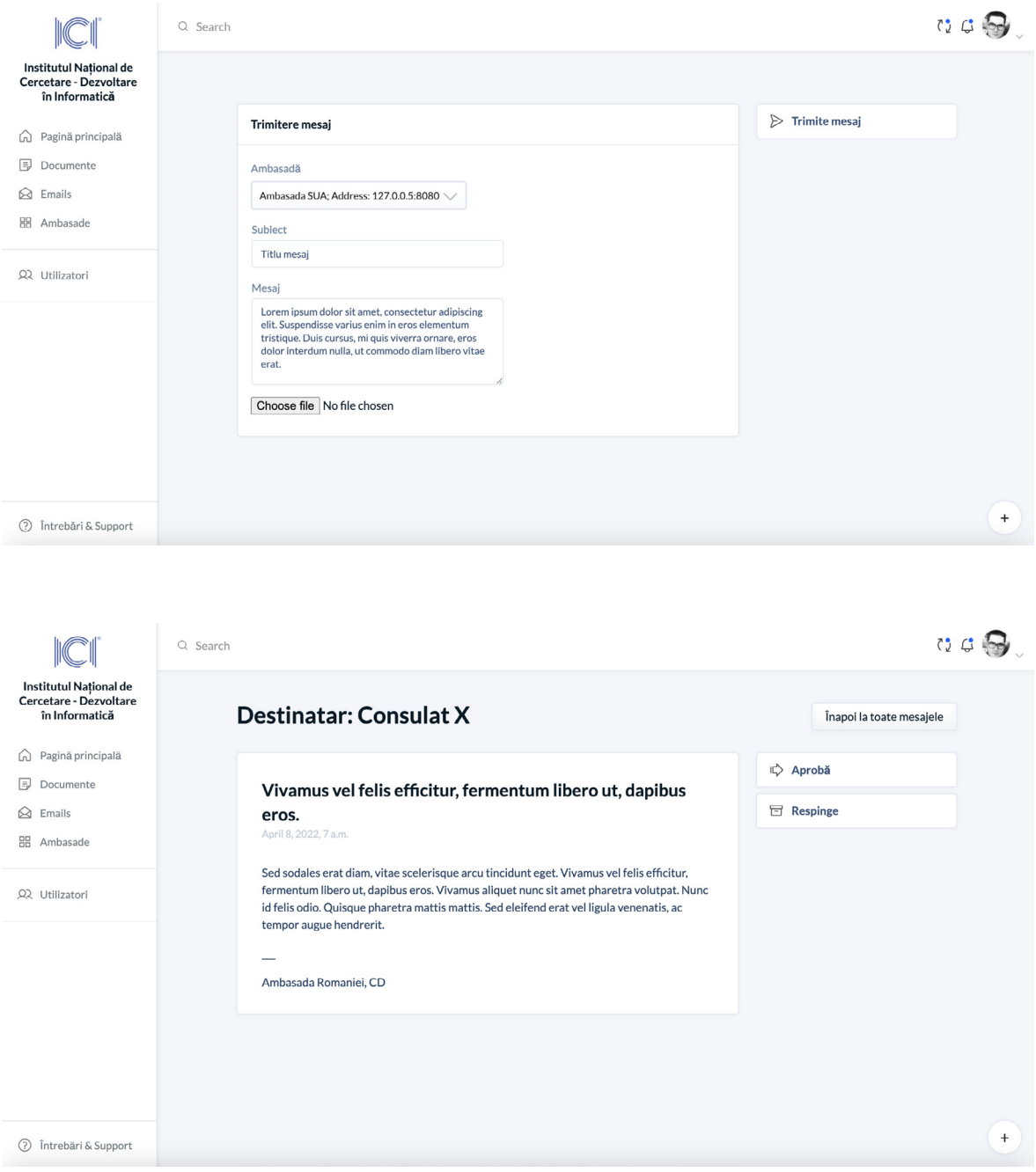


Figure 5. *Interfaces for a) composing (up) and b) sending (down) messages*

THE BLOCKCHAIN COMPONENT

The novelty of the application lies in its use of a back-office blockchain component as a means for ensuring the safety, integrity, traceability and confidentiality of the information transmitted. Blockchain or distributed ledger technology is a way in which the integrity of

a database can be maintained without the intervention of a corruptible centralized authority, enabling trustworthy but decentralized transactions that support a wide variety of applications, such as smart contracts, origin tracing, financial instrument exchange, secure public records and, in our case, the secure transmission of messages (NIST, 2018). It does this through the existence of multiple ledger instances that have to be updated in unison through the use of advanced mathematical calculations in which the blockchain nodes are engaged in order to ensure that only legitimate transactions get processed.

ICI Bucharest has a vast expertise in the development and implementation of blockchain based applications, considering the fact that the institute is hosting the first European Blockchain Services Infrastructure node from Romania and initiated three blockchain laboratories that cover the technical, governmental and the dissemination sides of the blockchain technology.

The blockchain solution chosen for the application is implemented using the instruments provided by the Hyperledger project. Hyperledger is defined as a technological hub which encourages the blockchain initiatives that have the potential to reach a certain level of maturity to become open-source blockchain solutions. This project provides multiple advantages in implementation like performance, scalability, trust and mechanisms for selecting data. The main instruments that were used for the implementation of the proposed solution are Hyperledger Indy and Hyperledger Aries. Hyperledger Indy facilitates and integrates self-sovereign identity in blockchain infrastructures, while Hyperledger Aries offers a series of tools in order to ensure data exchange, peer-to-peer communication and interoperability between different types of blockchain platforms (Dhillon et al., 2017).

The usage of the Hyperledger project enabled ICI Bucharest to more easily build the Cyber Diplomacy Application as a usable and deployable service, while minimizing the expenditure of scarce own resources in terms of man-hours or underlying infrastructure.

The layers are also designed in a way that enables currently unknown requirements to be fulfilled in the most efficient way.

The entities are registered on the blockchain and get their own unique distributed identifier (DID) which assures the layer of authenticity and non-repudiation. A DID is generated cryptographically and represents a set of data which define the user (Der et al., 2017). Thus, each entity starts by internally generating a pair of keys consisting of a private and public key, cryptographically linked in such a way that the information signed by the private one is only verifiable by the public counterpart.

The onboarding process consists of generating the above identity and registering the DID and public key component to the Blockchain by submitting a DID Document transaction. This transaction is fundamental to the architecture of the application and will be interrogated automatically when any party wishes to verify the integrity of a message.

The blockchain consensus mechanism is based on the proof-of-authority paradigm, which specifies a dynamic set of entities that are responsible for validating transactions and creating new blocks in the network. In the context of our application, each critical infrastructure operator is also a blockchain node operator with validation attributes and obligations. This way, the concept of authority is introduced in the network and no unauthorized third party can inject malicious payload transactions (NIST, 2018).

THE WAY AHEAD

The application is already in a minimum viable product state and is ready for implementation. Given its nature, the best results will come for wholesale adoption by a geographically distributed organization and network. Its usefulness scales with the number of users. The current use case, presented in this article, was for Ministry of Foreign Affairs communication, and this can be extended to conversion for use by other public authorities or, internationally, for communications by international organizations, for instance in the United Nations system. However, there are also other use cases to which it is amenable, wherever we have communications with low volumes of data that are sensitive but not instantaneous.

One alternative use case that can be envisioned is the communication between critical infrastructure operator (mostly private) and the competent authorities or multiple upstream or downstream interdependent infrastructure operators. Since blockchain network communication precludes instantaneous communications (though not reasonably rapid ones), the critical infrastructure data transmission that can be mediated by a modified Critical Diplomacy Application includes security environment data, data on security measures, on ongoing threats and responses to them and on the status of the functioning of the critical infrastructures (such as industrial control system outputs – temperatures, pressures etc.)

Having an example like this in mind, we can argue for three main directions of development for the application, beyond contextual modifications for applications in new fields.

The first evolution is the inclusion of new types of supported messages, the main ones being machine-readable messages based on existing standards like Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Intelligence Information (TAXII) (CISA, 2021). This requires an ability to link the application to modules that are fed relevant information and convert the data to such outputs for inclusion, and the application can then send such messages regularly or automatically (whenever needed).

The second evolution is the creation of the modules to define these messages and the modules that can then read and interpret such messages (like STIX and TAXII) and output the relevant information. If the application is taken into the direction of increased modularity, it is also possible to enable third party entities to create linkable modules, thereby expanding the functionalities and usability of the application. There is a precedent in the form of the Automated Indicator Sharing program run by the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, which recommends third party providers of software that enables the formulation of standardized messages for their specific infrastructure for inclusion of the operator in the program (CISA, 2021). There is no blockchain component, relying instead on secure real-time communications that enable use also during crisis and emergency situations. However, the Cyber Diplomacy Application's use of blockchain will enable a future capability.

The third line of development is related to the use of the blockchain readability as a means of conducting long-range analyses of communications and of the evolution of a system being managed through this communication tool. This requires new features, such as archive functionalities, but also embedded tools that are accessible to normal users that enable the analysis of the blocks in the blockchain for whatever investigation the user requires, such as message integrity or establishing a trustworthy history of exchanges to identify "enemies within" or in a post-crisis evaluation exercise.

CONCLUSIONS

Cyber Diplomacy is a practice of growing importance in the context of strong digitalization and the rapid implementation of transformative technologies such as Artificial Intelligence or blockchain (Georgescu et al., 2020b), and in the context of a rapid shift in the cyber security environment, with new and diverse risks, vulnerabilities and threats (Georgescu et al., 2019b). Cyber Diplomacy enables international relations actors, entities and practitioners to develop the trust and coordinative capacity required for regulations, norms creation and collective action on the part of states and other relevant entities (Georgescu et al., 2020b).

This article presented a blockchain-based application for secure communications between entities within a diplomatic network such as that of a Ministry of Foreign Affairs. The application is in minimum viable product state and can be already deployed or further developed, as well as modified for use within other types of networks, such as decentralized networks globally or hierarchical networks governing, for instance, critical infrastructure protection. It is the product of the Cyber Diplomacy Center within ICI Bucharest and is one of a series of deliverables with which the center is trying to make its mark on the development of the Cyber Diplomacy field.

ACKNOWLEDGEMENTS

"This work was supported by a grant of the Ministry of Research, Innovation and Digitization, CNCS/CCCDI - UEFISCDI, project number PN-III-P3-3.6-H2020-2020-0187, within PNCDI III."

REFERENCE LIST

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

CISA - Cybersecurity and Infrastructure Security Agency (2021). *Automated Indicator Sharing Documentation. Department of Homeland Security*, USA. Retrieved from https://www.cisa.gov/publication/automated-indicator-sharing-ais-documentation.

Der, U., Jahnichen, S. & Surmeli, J. (2017). Self-sovereign Identity – Opportunities and Challenges for the Digital Revolution. *Arxiv*, p. 5. Retrieved from https://doi.org/10.48550/arXiv.1712.01767.

Dhillon, V., Metcalf, D. & Hooper, M. (Eds.). (2017). The Hyperledger Project. *Blockchain Enabled Applications*, 139-149. Florida: Apress Media.

Georgescu, A., Vevera, V. & Cirnu, C. E. (2019a). The paradigm of complex system governance, necessary in a cyber interconnected world. In Badea, D., Bucovetchi, O. & Iancu, D. (Eds.). *Capability Management and Managerial Capability in Critical Infrastructure Systems* (270-283). Sibiu: "Nicolae Bălcescu" Land Forces Academy Publishing House.

Georgescu, A., Vevera, V. & Cirnu, C. E. (2019b). The Proliferation of Cyber Weapons -Theory and Mitigation. *Romanian Cyber Security Journal*, *1*(2), 37-46.

Georgescu, A., Vevera, V. & Cirnu, C. E. (2020a). Cyber as a Transformative Element in the Critical Infrastructure Protection Framework. *Romanian Cyber Security Journal*, *2*(1), 37-44.

Georgescu, A., Vevera, V. & Cirnu, C. E. (2020b). The Diplomacy of Systemic Governance in Cyberspace. *International Journal of Cyber Diplomacy*, *1*(1), 79-88.

NISA - National Institute of Standards and Technology (2018). *Blockchain Technology Overview*. Retrieved from https://doi.org/10.6028/NIST.IR.8202.

Van der Meer, S. (2016). *Defence, Deterrence and Diplomacy: Foreign Policy Instruments to Increase Future Cybersecurity*. Clingendael Netherlands. Retrieved from https://www.clingendael.org/sites/default/files/pdfs/book_securing-cyberspace-chapter_July2016.pdf.

Carmen Elena CÎRNU
is Scientific Director and Vice President of the Scientific Council of the National Institute for Research and Development in Informatics – ICI Bucharest. She is a Senior Scientific Researcher II, with extensive experience in coordinating both international and Romanian research projects in the field of interoperability, cyber security and virtual education. She is the initiator and coordinating editor of the International Journal of Cyber Diplomacy and of the Cyber Diplomacy Center. She is a graduate of the Faculty of Philosophy, University of Bucharest, where she obtained her PhD degree in 2011 with a transdisciplinary thesis. Fellow of the Aspen Japan Institute, Guest Researcher of the Global Security Research Institute Japan, Keio University (2015, 2019), coordinator of research activities within EuroDefense Romania, with a broad experience both in the central public administration and in academia. She published articles, books, coauthored project deliverables and collaborated as a chief editor and reviewer for scientific publications.

Paul-Cristian VASILE
Graduated the Faculty of Mathematics and Informatics from the University of Bucharest and is currently a studying for the Software Engineering Master's degree. He holds a software engineer position at the National Institute for Research and Development in Informatics - ICI Bucharest. His work experience includes areas like blockchain technologies - where he developed a cyber-diplomacy tool, e-Learning platforms, digital forensics methods and cash registers cryptography. As of July 2020, he holds the Certified Ethical Hacker certification issued by EC-Council.