BRIDGING THE GAP: AN ANALYSIS OF CYBERSECURITY IN WEB TECHNOLOGIES FOR CYBER DIPLOMACY

Carmen-Elena CÎRNU[1], Ioana-Cristina VASILOIU[1,2]
[1] National Institute for Research and Development in Informatics – ICI Bucharest, Romania
carmen.cirnu@ici.ro
[2] Bucharest University of Economic Studies, Romania
ioana.vasiloiu@csie.ase.ro

Abstract: Cyber diplomacy is evolving as an increasingly important element of international relations, and the security of web-based technologies used in this field is crucial. This article examines cybersecurity gaps in preparation, settings, hardware and software solutions, communication channels, and human resource training for using web-based technologies in cyber diplomacy. The study highlights the potential risks and vulnerabilities associated with these technologies and identifies best practices and strategies for mitigating cyber threats. The article provides insights into the importance of cybersecurity in cyber diplomacy and suggests a framework for improving cybersecurity preparedness and response.
Keywords: Cyber diplomacy, Cybersecurity, Web technologies, Cyber threats.

INTRODUCTION

Web technologies have revolutionised how diplomats communicate and empowered them to transcend geographical and time barriers. This digital transformation has made diplomacy more accessible and cost-effective, particularly for smaller or resource-constrained countries. Diplomats can now engage in virtual meetings, conferences, and negotiations, fostering global collaboration and the exchange of ideas.

Web technologies have also created new opportunities for public diplomacy, which involves interacting with foreign audiences to promote national interests and values. Social media platforms such as Facebook, Twitter, LinkedIn and Instagram have become essential tools for diplomats to reach foreign audiences and promote their country's interests. Diplomats can use social media to share information, promote cultural events, and engage in public diplomacy campaigns.

The use of web-based technologies in diplomacy has indeed brought about significant benefits, but it has also given rise to new challenges, particularly in the realm of cybersecurity. Diplomats are now tasked with ensuring the security of their communications and data, and protecting against the ever-increasing cyber threats and attacks. The growing reliance on web-based technologies for diplomacy has underscored the critical need for robust cybersecurity measures, including encryption, secure communication channels, and stringent cybersecurity protocols.

Thus, web technologies have transformed the practice of diplomacy, making it more accessible, efficient and innovative. However, their use also requires careful consideration of cybersecurity risks and measures to protect sensitive information and communications.

Cyber-attacks on web-based technologies in cyber diplomacy are becoming more frequent and sophisticated, posing a significant threat to diplomatic communications and information security and confidentiality. These cyber-attacks can take many forms, including phishing, malware, ransomware, denial-of-service attacks, and hacking.

One of the main reasons for the growing threat of cyber-attacks on web-based technologies in cyber diplomacy is the increasing reliance on digital platforms and tools for communication and collaboration. This trend has created more opportunities for cybercriminals to exploit vulnerabilities in web-based technologies and gain unauthorised access to sensitive information.

Another contributing factor is the need for cybersecurity training for many diplomatic organisations and their partners. Many organisations lack adequate cybersecurity measures to protect against cyber threats, such as effective firewalls, encryption protocols, and employee training programs.

The rise of state-sponsored cyber-attacks is also a growing concern in cyber diplomacy. Nation-states increasingly use cyber-attacks as a tool for political and economic espionage, and diplomatic organisations are often the target of these attacks.

In summary, the growing threat of cyber-attacks on web-based technologies in cyber diplomacy is a significant concern, and organisations must take proactive measures to protect against these threats. This requires a comprehensive approach to cybersecurity that includes technical measures, organisational policies, employee training programs, and collaboration and information sharing between diplomatic organisations and their partners.

WEB TECHNOLOGIES IN CYBER DIPLOMACY

Today's interconnected world promotes the use of web technologies in international relations, namely in cyber diplomacy, thus facilitating diplomatic activities, communication and collaboration in cyberspace.

Next, this article addresses the leading technologies used in the field of cyber diplomacy and how they have changed international relations, adapting them to the 21st century.

The social networks

According to Hodzic (2017), the evolution of diplomacy focuses on using social media platforms, targeting public actors and establishing cyber threats and conduct as new domains of international politics. In this sense, diplomatic missions and ministries of foreign affairs use platforms such as Facebook, Twitter, Linked In, and Instagram because they offer the possibility of reaching a broad audience and enabling real-time communication. Bjola (2017) claimed that less than ten years after the launch of social networks, 90% of UN member states were present on Twitter and 88% on Facebook.

A study carried out by Statista (2023) shows that, in 2022, Facebook was the most used social media platform for news consumption in Romania, followed by YouTube.

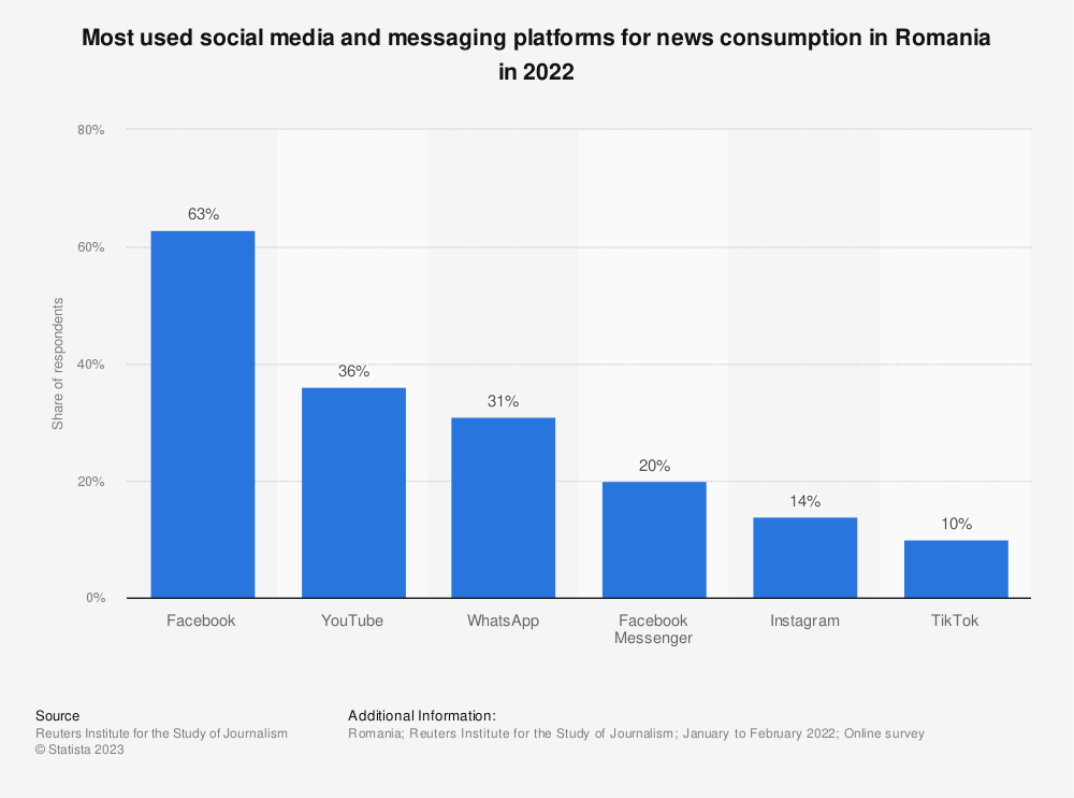

Figure 1. The most used social media and messaging platforms for news consumption in Romania in 2022 (Statista, 2023)

Since 63% of Romanians use Facebook to find news, a simple search on this platform, using the keywords "embassy of Romania", identified 95 pages. Of these, 31 are unofficial pages created by unauthorized persons, which poses a danger regarding the misinformation that can be transmitted through these channels.

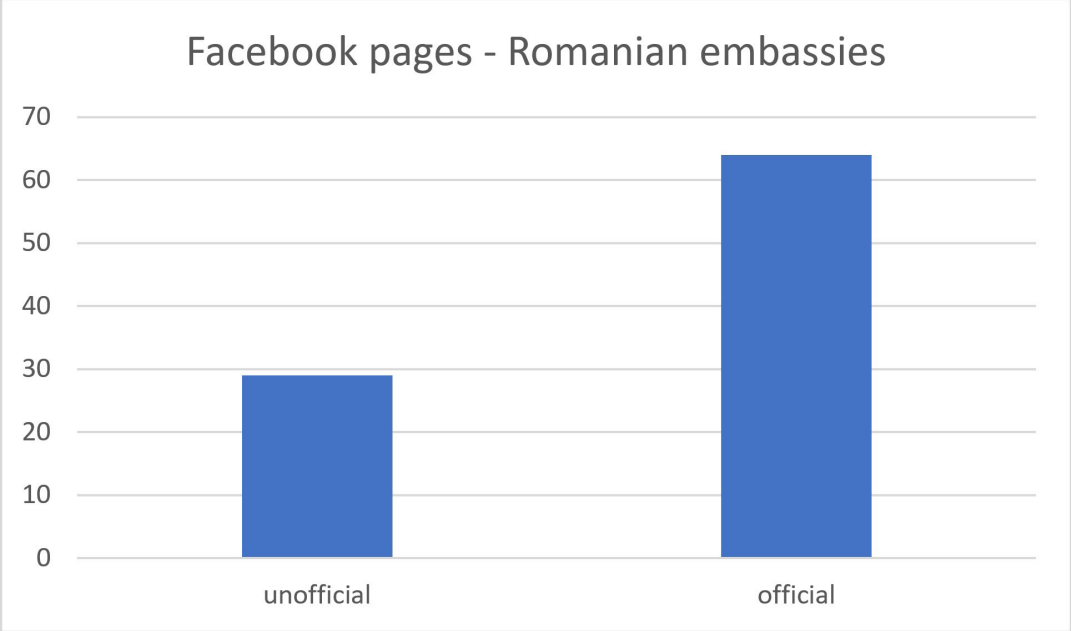

Figure 2. Romanian Embassies Facebook pages - official accounts vs unofficial

To support the hypothesis of the existence of the ever-increasing danger of disinformation, researchers from the Oxford Internet Institute (2020), within the university of the same name, monitored the organization of social network manipulation in the period 2017-2020, concluding that in 81 countries social media was used to spread computational propaganda and disinformation about politics. There were only 70 countries in this situation in 2019.

Video conferencing platforms

The new technologies category includes the platforms used for conferences and video meetings, such as Skype, Microsoft Teams, Webex, and Zoom. They became prevalent during the Covid-19 pandemic when there were restrictions on travel and in-person meetings, normalizing online interactions even for sensitive issues, and can be used for negotiations, conferences or bi/multilateral meetings. One such example is the concept of visual diplomacy, addressed by Danielson and Hedling (2021), analysing the virtual meeting of the leaders of the Group of Twenty (G20) major economies on March 26, 2020, where the unprecedented situation facing the entire world map was debated – the coronavirus pandemic. Thus, traditional diplomacy constantly evolved in the digital age, with virtual platforms playing an essential role in overcoming barriers and providing new opportunities for diplomatic engagement and collaboration.

The risk with these technologies is that cybercriminals may use these applications to mask malicious files. According to Statista, in 2020, Skype was the most used platform for cybercrime – 46%, followed by Zoom – 14%. Moreover, the same year, Kaspersky detected 1.66 million unique malicious files that were spread under the guise of popular messaging and online conferencing applications, usually used for work. (2020)

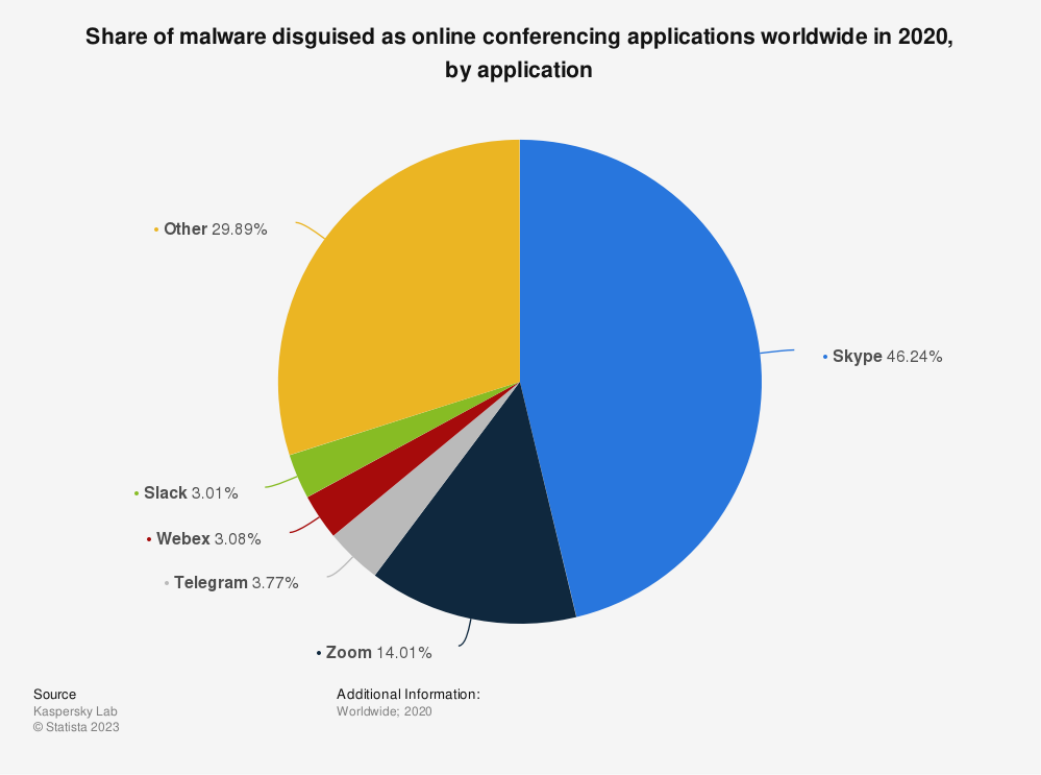

Figure 3. Share of malware disguised in online conferencing applications worldwide in 2020, by application (Statista, 2023)

Secure messaging/communication apps

Westcott (2008) argues that there are no secrets on the Internet since, regardless of whether it is encrypted, anything sent over the Internet can be compromised. Radunovic (2010) believes that despite strong and fairly affordable encryption technologies, the risks increase with the value that the perpetrators can obtain if they succeed in breaching the confidentiality of the Ministries of Foreign Affairs and with the respective resources invested in cyber-attacks. Thus, diplomats' negligent use of unsecured web tools carries with it the risk of disclosing confidential information to third parties. This is especially important given that quantum computing promises to make most existing encryption methods obsolete, and hackers are already harvesting data they cannot decrypt at the moment in order to extract value once it will be possible to do so. Awareness of the issues facing even currently secure communications, as well as the importance of quantum-secure encryption methods for diplomatic communications going forward will be very important.

Virtual embassies

Virtual embassies are not a new concept, with Sweden launching the first virtual embassy in 2007 within the videogame world of Second Life (Manor, 2019), followed by the Maldives opening Diplomacy Island in the same game, and the United States of America opening the Virtual Embassy for Iran in 2011. At the same time, Israel also opened a virtual embassy on Twitter to communicate information to the Gulf countries Bahrain, Kuwait, Oman, Qatar, United Arab Emirates and Abu Dhabi. (Constantinou et al., 2016).

The benefits of these tools are numerous, from continuous accessibility and real-time responses to increased openness and efficiency that lead to greater credibility. In proportion to these are the disadvantages: privacy and cybersecurity measures to prevent attacks, the existence of certain groups that do not have the Internet and cannot be reached in this way, and the scepticism of some people. (Pawar & Singh, 2023).

All of these limitations caused Sweden to close its virtual embassy after six years and the Virtual Embassy for Iran to fail. (Constantinou et al., 2016)

CYBERSECURITY GAPS IN DIPLOMACY – PEGASUS CASE STUDY

Pegasus is a highly intrusive spyware (surveillance) program that gives users full and unrestricted access to all sensors and information on the targeted mobile phone. It turns the smartphone into a constant surveillance device, accessing the camera and microphone, geolocation data, emails, messages, photos, videos, passwords and applications (Council of Europe, 2023).

In July 2021, reports were published revealing that Pegasus had been used against political opponents, lawyers, diplomats, heads of state and nearly 200 journalists from 24 countries. Forbidden Stories (2021) and its partners have identified potential NSO Group clients in 11 countries: Azerbaijan, Bahrain, Hungary, India, Kazakhstan, Mexico, Morocco, Rwanda,

Saudi Arabia, Togo and the United Arab Emirates. According to The Washington Post, 14 former or current heads of state and government, including French President Emmanuel Macron and former Belgian Prime Minister Charles Michel (President of the European Council), appeared on the list of potential targets. (Washington Post, 2021)

The allegations were denied, with the NSO Group stating that the mission is to help governments protect citizens, with data collected only from individuals suspected of being criminals and terrorists (NSO Group, 2021).

Hypothesis 1: The use of Pegasus by governments to spy on foreign diplomats, politicians and journalists has strained diplomatic relations between countries.

There have been numerous incidents of governments allegedly using Pegasus to monitor foreign officials, leading to severe diplomatic tensions. These allegations caused major diplomatic rifts, including the withdrawal of ambassadors and the suspension of diplomatic ties. For example, in 2021, Pegasus acted as a catalyst, exacerbating pre-existing tensions between Algeria and Morocco, as Moroccan authorities were alleged to have used the program to target Algerian officials and influential figures. The New Arab article illustrates how cyber espionage, when added to geopolitical rivalries, can lead to significant diplomatic consequences. The scandal has made it even more difficult for Algeria and Morocco to engage in constructive dialogue or find common ground on critical issues, thus maintaining a state of heightened tension in North Africa.

Hypothesis 2: The erosion of trust can hinder diplomatic negotiations and collaborative efforts on global issues.

The World Economic Forum's Global Risks Report 2023 looks at how the erosion of trust from digital surveillance technologies like Pegasus affected international cooperation. It highlights the challenges posed by the widespread use of such technologies and their implications for global governance. The potential for misuse will be particularly problematic for users living in countries with inadequate regulatory frameworks or authoritarian tendencies. Forms of digital repression to quell politically motivated uprisings, such as the use of spyware to track activists' activities, are already causing significant human rights violations in the Middle East.

Hypothesis 3: A country's use of Pegasus to spy on individuals within another country's borders violates that nation's sovereignty, further escalating tensions.

National sovereignty is a fundamental principle of law and international relations. When a state uses Pegasus software to surveil individuals within another state's borders, it violates that nation's sovereignty. This violation of sovereignty is particularly egregious when it targets high-ranking officials, as it not only violates national borders but also undermines diplomatic relations and trust. Reuters discusses a French prosecutor's investigation into a complaint that Moroccan authorities used software to spy on French President Emmanuel Macron and other French officials.

Hypothesis 4: There is a need for regulation, which requires diplomatic efforts to negotiate and implement global regulatory frameworks.

The international community has recognized the need to regulate surveillance technologies like Pegasus to prevent abuses and protect human rights. The proposed measures include establishing an international legal framework to oversee the use of such technologies and ensure that they are used responsibly. Diplomatic efforts are crucial to achieving global consensus and implementing these regulations, which could include transparency requirements, oversight mechanisms, and penalties for misuse.

The European Parliament, following the June 2023 inquiry into the use of Pegasus, made significant recommendations to EU Member States, EU institutions and other relevant actors. These recommendations emphasize the need for a robust regulatory framework to govern the use of spyware and ensure its alignment with human rights standards.

The European Parliament has addressed specific recommendations to the main EU member states (Poland, Hungary, Greece, Spain and Cyprus) regarding their legislative frameworks and ongoing investigations into spyware abuse. It called for adopting conditions for the legal use, sale, purchase and transfer of spyware, setting a deadline for all member states (the end of 2023) to meet four key conditions.

At the same time, it emphasized the need for common EU standards for regulating and limiting the use of spyware, given the EU dimension of its use (judicial cooperation in criminal matters and the internal market). It suggested that authorizations for the use of spyware should only be granted in exceptional cases and for investigations into a limited and closed list of clearly and precisely defined severe crimes that pose a real threat to national security.

The European Parliament's recommendations underscore the urgent need for a comprehensive regulatory framework to govern the use of surveillance technologies such as Pegasus. By setting strict conditions and common EU standards, the European Parliament aims to prevent abuses, protect human rights and ensure that spyware is only used in exceptional cases involving serious crimes that pose a real threat to national security. These measures are crucial for restoring trust, maintaining diplomatic relations and upholding the principles of sovereignty and human rights.

BRIDGING THE CYBERSECURITY GAP

To reduce the cybersecurity gap, a strategic framework can be developed and implemented through international collaboration, thus choosing the most appropriate measures.

These measures may include ongoing risk assessments to identify and assess potential threats, advanced encryption for all communication and correspondence, developing and updating cybersecurity training programs for all staff, screening HR to ensure that no employee becomes a threat, creating and updating incident response plans in the event of security breaches, working with cybersecurity experts to stay abreast of trends, changes and adaptations of these measures.

Table 1. Strategic framework - proposal for reducing the cybersecurity gap

Tactic	Measure
Establish a risk assessment team	1. Identify team members: cybersecurity experts, members of the IT department, as well as other non-technical representatives
	2. Assignment of response coordination roles, process follow-up.
Defining the objectives	1. Identifying and centralizing the systems and processes to be included in the process
	2. Establishing objectives: identifying potential vulnerabilities, assessing the impact and developing possible strategies
Identifying and classifying assets	1. Conduct an inventory of hardware, software, data and network assets
	2. Classification of assets by security level
Identifying and analysing potential threats	1. Continuous monitoring and identification of various threats that could have a significant impact
	2. Using threat modelling techniques based on factors such as espionage tactics, geopolitical context and insider threats.
Vulnerability assessment	1. Continuous monitoring of vulnerabilities, pen-testing actions, and considering IT systems and networks.
	2. Using external vulnerability databases to stay informed all the time.
Impact Analysis	1. Making a risk diagram, considering the threats and the impact they could have.
	2. Assessing the potential consequences of each threat, taking into account data loss
Developing mitigation strategies	1. Prioritization of risks based on the likelihood of occurrence, followed by developing tailored mitigation strategies to address the most critical first.
	2. Establishing an alert system to notify responsible personnel when unusual activities are detected to allow for rapid intervention and appropriate response.
Constant monitoring and updating	1. Implement automated solutions to monitor system activity, including network traffic, security logs, and user behaviour.
	2. Establishing a procedure to regularly update software and manage systems to correct known vulnerabilities and benefit from the latest security patches.
Professional Training	1. Design and implement a continuous training program for IT staff covering various aspects of cybersecurity, including basics, advanced technologies and trends in the field.
	2. Encouraging and supporting employees in obtaining relevant cybersecurity certifications and credentials, such as Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), or CompTIA Security+
Reporting and Auditing	1. Develop and implement a standardized cybersecurity incident reporting system to facilitate incident collection and reporting.
	2. Use of third parties or internal audit teams to conduct reviews of security systems, procedures and practices and identify any gaps or weaknesses.
International Collaboration	1. Develop bilateral or multilateral partnerships and agreements between countries to encourage information sharing and cooperation in investigating and countering malicious cyber activities.
	2. Organizing international cybersecurity exercises and simulations involving teams and experts from different countries to test and improve incident response capabilities and coordination between agencies and organizations involved.

In the face of growing cyber threats, establishing a comprehensive cybersecurity framework is essential for safeguarding critical assets and information. The outlined strategic measures focus on key areas such as risk assessment, asset management, threat identification, vulnerability assessment, impact analysis, mitigation strategies, continuous monitoring, professional training, reporting and auditing, and international collaboration. Each of these measures addresses distinct aspects of cybersecurity, ensuring a holistic approach to threat management and response.

The first step in the proposed framework is to establish a dedicated risk assessment team. This team, composed of cybersecurity experts, IT department members, and non-technical representatives, is a testament to the value placed on diverse perspectives. Their primary responsibilities include identifying and centralising critical systems, defining objectives to uncover vulnerabilities, and conducting continuous monitoring. By recognising the unique

contributions of each team member, it can be fostered a sense of belonging and importance, leading to a more comprehensive risk management strategy.

Asset management is another critical component involving identifying and classifying hardware, software, data, and network assets. Organisations can prioritise their protection efforts more effectively by maintaining an updated inventory and categorising assets by their security level. This provides that the most critical assets receive the highest level of security, diminishing the risk of considerable breaches. Continuous monitoring and regular updates enhance this strategy by keeping systems resilient against evolving threats.

Professional training and constant monitoring are not just tasks, but vital components of robust cybersecurity. Implementing a continuous training program ensures that IT staff are up-to-date with the latest cybersecurity practices and technologies. Supporting staff in obtaining relevant certifications, such as CISSP and CEH, is a testament to the commitment to their professional growth and defence capabilities. Automated solutions for monitoring system activity, combined with regular software updates, help in identifying and mitigating threats in real-time, ensuring that the security posture is always at its peak. By emphasising the direct benefits of these measures, it can make the audience feel the value of their continuous learning and vigilance.

International cooperation has a key role in the contemporary cybersecurity landscape. Developing partnerships and agreements between countries promotes information sharing and collective efforts to counter malicious activities. Organising international cybersecurity exercises allows teams from different nations to test and improve their response capabilities, fostering better coordination and mutual support in the face of global cyber threats. This collaborative approach enhances individual national security and contributes to a more secure and resilient international cyber environment.

The implications of implementing this comprehensive cybersecurity framework are profound. Organisations can significantly reduce their cyber-attack vulnerability by adopting these strategic and tactical measures. A proactive and well-coordinated approach ensures possible threats are recognised and mitigated before they can cause substantial harm. Continuous improvement through training, monitoring, and international collaboration ensures that the defence mechanisms evolve with the threats. Eventually, this leads to a more protected digital landscape where organisations can confidently and resiliently operate against cyber adversaries.

CONCLUSIONS

Web technologies have brought about fundamental changes in the field of diplomacy, facilitating communication and collaboration among diplomats across great distances and different time zones. These technologies have reduced the need for travel and increased efficiency, making diplomacy more accessible and cost-effective, especially for countries with limited resources. Diplomats use web platforms for virtual meetings, conferences and negotiations, enabling the rapid exchange of ideas and international collaboration.

Despite the risks, web technologies have played a pivotal role in diplomacy. They have not only brought about efficiency and accessibility but also facilitated the emergence of public diplomacy through social media platforms. Moreover, they have demonstrated their adaptability and the use of new tools to maintain international dialogue and cooperation, even in times of crisis. This positive impact underscores the need to balance the benefits with robust security measures.

To counterbalance the benefits, web technologies bring cybersecurity challenges and risks: various cyber threats (phishing, malware, ransomware, denial-of-service attacks, hacking), lack of sufficient preparation, state-sponsored attacks, disinformation and propaganda.

For example, the Pegasus spyware highlighted the significant risks associated with cyber surveillance. Governments' use of this software to spy on diplomats, politicians and journalists has led to diplomatic tensions and the erosion of international trust. Regulating the use of these technologies is crucial to prevent abuses and protect human rights.

In conclusion, the task of ensuring cybersecurity within cyber diplomacy is not one that can be undertaken in isolation. It is imperative to adopt a robust and collaborative strategic framework at the international level. This includes implementing ongoing risk assessments, using advanced encryption, developing staff training programs, and rigorous HR vetting. It also necessitates the constant updating of incident response plans and close collaboration with cybersecurity experts to stay abreast of technological developments. The constant adaptation and modification of these measures will help reduce vulnerabilities and effectively protect diplomatic communications and information in the digital age.

REFERENCE LIST

Constantinou, C., Kerr, P. & Sharp, Pl. (2016) *The SAGE Handbook of Diplomacy*. 10.4135/9781473957930. https://www.researchgate.net/publication/308347785_The_SAGE_Handbook_of_Diplomacy

Council of Europe (2023) *Pegasus and similar spyware and secret state surveillance*. https://rm.coe.int/pegasus-and-similar-spyware-and-secret-state-surveillance/1680ac7f68

Danielson A, Hedling, E. (2022) Visual diplomacy in virtual summitry: Status signalling during the coronavirus crisis. *Review of International Studies*. 48(2), 243-261. doi:10.1017/S0260210521000607

Forbidden Stories (2021) *The Pegasus project: A worldwide collaboration to counter a global crime*. https://forbiddenstories.org/the-pegasus-project-a-worldwide-collaboration-to-counter-a-global-crime/

Hodzic, N. (2017) *Cyber-Diplomacy: Framing the Transformation*. Budapest: Central European University. https://scholar.google.ro/scholar_url?url=https://www.etd.ceu.edu/2017/hodzic_nejra.pdf&hl=en&sa=X&ei=0Sw-ZuzAHIfHy9YP0IeViAc&scisig=AFWwaebT2kfU0r1ppBsuPLCNqyYM&oi=scholarr

Manor, I. (2019) The Digitalization of Public Diplomacy. *Palgrave Macmillan Series in Global Public Diplomacy.* ISBN 978-3-030-04404-6. https://www.researchgate.net/profile/Ilan-Manor/publication/330377221_The_Digitalization_of_Public_Diplomacy/links/5e29af5d299bf152167858e8/The-Digitalization-of-Public-Diplomacy.pdf

NSO Group (2021) *NSO Group Transparency and Responsibility Report*. https://www.nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf

Radunovic, V. (2010) *The role of information and communication technologies in diplomacy and diplomatic services*. Master dissertation. University of Malta. Malta. https://www.diplomacy.edu/wp-content/uploads/2021/06/30112010141720_Radunovic_28Library29.pdf

Statista (2023) *Global malware masqueraded as online collaboration applications 2020, by application.* https://04116kijv-y-https-www-statista-com.z.e-nformation.ro/statistics/1203757/online-collaboration-applications-malware-deception-global/

Statista (2023) *Most used social media and messaging platforms for news consumption in Romania in 2022*. https://04116mrrf-y-https-www-statista-com.z.e-nformation.ro/statistics/1198565/romania-social-media-platform-for-news-consumption/

The Washington Post (2021) *On the list: Ten prime ministers, three presidents and a king. Among 50,000 phone numbers, the Pegasus Project found those of hundreds of public officials*. https://www.washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware/

Westcott, N. (2008) *Digital Diplomacy: The Impact of the Internet on International Relations*. OII Working Paper No. 16. http://dx.doi.org/10.2139/ssrn.1326476

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 I, 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.

Ioana-Cristina VASILOIU is a PhD Student at the Bucharest University of Economic Studies in the field of Economic Informatics. She graduated with a master's degree in International Economic Diplomacy from the Faculty of International Business and Economics of the same university. She also benefited from an ERASMUS+ scholarship, which allowed her to study in Poland. She is a graduate of the Faculty of International Business and Economics. Currently, she works for the National Institute for Research and Development in Informatics - ICI Bucharest, where she is involved in research on various topics, from cybersecurity and cyber diplomacy to high-performance computing. She was an Assistant Professor at the Bucharest University of Economic Studies, teaching Economic Information Systems at The Faculty of Economic Cybernetics, Statistics and Informatics.

She is a co-author of the books "Counter-information protection in organisations" and "Exploring the legislative dimension of cyber diplomacy worldwide: universal, regional, and local instruments" and a trainer.