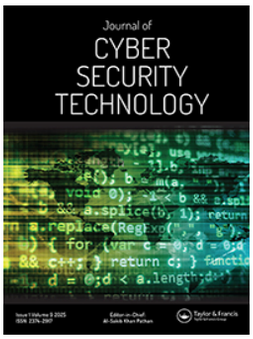

Journal of Cyber Security Technology

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/tsec20

Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing

Petar Radanliev

To cite this article: Petar Radanliev (2025) Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing, Journal of Cyber Security Technology, 9:1, 28-78, DOI: 10.1080/23742917.2024.2312671

To link to this article: https://doi.org/10.1080/23742917.2024.2312671

Published online: 05 Feb 2024.

JOURNAL OF CYBER SECURITY TECHNOLOGY
2025, VOL. 9, NO. 1, 28–78
https://doi.org/10.1080/23742917.2024.2312671

Taylor & Francis
Taylor & Francis Group

Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing

Petar Radanliev [a,b]

[a]School of Management, University of Bath, Bath, UK; [b]Department of Computer Science, University of Oxford, Oxford, UK

ABSTRACT

Cyber diplomacy is critical in dealing with the digital era's evolving cybersecurity dangers and possibilities. This article investigates the impact of Artificial Intelligence (AI), the Internet of Things (IoT), Blockchains, and Quantum Computing on cyber diplomacy. AI holds the potential for proactive threat identification and response, while IoT enables international information sharing. Blockchains enable secure data sharing and document verification, but they also pose new threats, such as AI-driven cyber-attacks, IoT privacy breaches, blockchain vulnerabilities, and the potential for quantum computing to break encryption. This article conducts case study reviews in combination with secondary data analysis and emphasises the value of international cooperation in developing global norms and frameworks to control responsible technology adoption. Cyber diplomacy can promote cybersecurity, protect national interests, and foster mutual trust among nations in the digital sphere by capitalising on possibilities and reducing threats.

ARTICLE HISTORY
Received 31 July 2023
Accepted 27 January 2024

KEYWORDS
Quantum computing; Artificial Intelligence (AI); blockchain technologies; AI BOM / SBOM; cyber diplomacy

1. Introduction to cyber diplomacy

1.1. What is cyber diplomacy?

Cyber Diplomacy is a term used to describe the application of diplomatic techniques and negotiations in international relations that deal with and regulate cyberspace-related issues. According to some studies, cyber-diplomacy also covers cyber warfare and agreements on the rules of engagement because without proper rules of engagement, 'the international community could end up in error with an unwanted conventional or nuclear war' [1].

Cyber Diplomacy is usually applied to managing the difficulties and obstacles presented by the cyber world and aims to promote responsible actions, preserve cybersecurity, and ensure stability in cyberspace. Without

CONTACT Petar Radanliev radanliev@yahoo.com School of Management, University of Bath, UK

cyber diplomacy in developing national cybersecurity policies, adversaries can apply complex social engineering tactics and present advanced persistent threats and even political threats for national cybersecurity environments [2].

International cooperation is promoted in cyber diplomacy to mitigate mutual threats and challenges. Nations collaborate on developing cyber standards, guidelines, and agreements that support a safe and secure online environment. In 2024, this is specifically focused on artificial intelligence (AI) [3], because AI is simply software, and we have longstanding concerns in regards to 'artificial intelligence methods in distributed denial of service (DDOS) assault and defense' [4].

Cyber Diplomacy is used to establish mutually beneficial agreements through diplomatic means of dialogue and to communicate between nations during situations of cyber disagreements between different nations. Cyber Diplomacy is a conflict resolution strategy that attempts to prevent conflicts in cyberspace from developing into bigger geopolitical problems.

International cyber governance, including the development of cyber laws, treaties, and regulations, is significantly influenced by cyber diplomacy. Such governance structures are crucial for preserving order and reducing the risks connected to cyber activity.

Establishing confidence-building measures is a common step in cyber diplomacy, and this is crucial for reaching agreements between nations and fostering mutual trust, reducing scepticism, and increasing openness in individual cyber activities. Such activities might involve information exchange, team training, and hotlines to avoid misunderstandings and errors in judgment.

One of the major issues in cybersecurity is the identification of cyberattacks. Cyber Diplomacy aims to address the attribution problem by building mechanisms to make people accountable for hostile cyber operations. To combat cyber threats effectively, cyber diplomacy promotes cooperation between governments and private corporations because the private sector plays a major part in cyberspace. Hence, public-private collaborations can make the exchange of knowledge and experience in cybersecurity easier.

Cyber Diplomacy promotes capacity building in developing nations to improve their cybersecurity skills and strengths. This assistance can come from sharing expertise, training, and technology transfer. Cyber diplomacy also discusses topics relating to freedoms and rights in cyberspace, including decentralisation and internet governance, freedom of expression, ethics, and privacy. Cyber diplomacy is aimed at creating a balance between individual rights in cyberspace and national security. Table 1 summarises the key roles of Cyber Diplomacy.

In Table 1, we outline the key components and define how cyber diplomacy promotes international agreements, responsible behaviour among states and non-state entities, and cooperation, stability, and security in cyberspace. Cyber

Table 1. Key aspects of cyber diplomacy.

Component	Description of activity
International Cooperation	Collaboration amongst nations to address common cyber threats and challenges. Establishing norms and agreements for cyberspace.
Conflict Resolution	Seeking peaceful resolutions to cyber incidents and disputes through diplomatic channels and negotiations.
Cybersecurity Governance	Shaping international cyber governance, including the development and implementation of cyber laws, treaties, and regulations.
Confidence Building Measures	Establishing agreements to build trust, reduce suspicion, and enhance transparency in cyber activities.
Attribution and Accountability	Addressing the issue of identifying the true source of cyberattacks and holding malicious actors accountable.
Public-Private Partnerships	Encouraging collaboration between governments and private companies to effectively tackle cyber threats.
Capacity Building	Promoting cybersecurity capabilities in less developed countries through technology transfer, training, and knowledge sharing.
Digital Rights and Freedoms	Balancing national security with individual rights in cyberspace, including issues of privacy, freedom of expression, and governance.

diplomacy is essential in determining how the future of the globally interconnected world will be shaped as cyberspace evolves.

1.2. Concepts related to cyber diplomacy

Cyber Diplomacy is strongly related to Cybersecurity, but the two functions are fundamentally different. Cybersecurity prevents unauthorised access, computer hacking, and information theft on computer systems, networks, and databases. Various cybersecurity strategies and technologies are employed to protect data and limit disruptions in cyberspace. While cybersecurity focuses on the technical and operational aspects of securing digital systems, cyber diplomacy deals with the diplomatic implications of managing cyber threats.

Another concept closely related to cyber diplomacy is digital diplomacy. However, the functions are very different. Digital diplomacy, often called e-Diplomacy or Diplomacy 2.0, uses governments' and diplomats' social media, online platforms, and digital technology to interact with international audiences, promote communication, and carry out diplomatic outreach. Digital diplomacy is a broader notion that includes technology for diplomatic goals, whereas cyber diplomacy concentrates on cyberspace issues and security.

The third closest concept to Cyber Diplomacy is Cyber Norms. Cyber norms are the established values and guidelines that direct governmental action in cyberspace. These standards seek to mould ethical behaviour and stop malevolent online activity. Cyber Diplomacy is crucial in promoting and negotiating these standards among governments. However, as we can see in Table 1, the Cyber Diplomacy function covers a much greater area.

In Table 2 we summarise the key concepts and functions closely related to Cyber Diplomacy, but they represent very different functions. These functions often confuse people who work in other areas unrelated to cyber.

Table 2. Summary of Cyber functions related to Cyber Diplomacy.

Concept	Description
Cybersecurity	Protecting systems and data from cyber threats. Focuses on technical measures for security.
Cyberwarfare	Use of cyber capabilities for military objectives. Part of information warfare.
Cyber Espionage	Legal principles governing state behaviour in cyberspace.
Digital Diplomacy	Using digital tech for diplomatic engagement and outreach.
Information Warfare	Using tech to influence opinions and perceptions of populations.
Cyber Norms	Agreed principles and rules governing state behaviour in cyberspace.
Cybercrime	Criminal activities through digital means. Includes hacking and online fraud.

Table 2: Summary of Cyber functions related to Cyber Diplomacy.In recent years, we have seen increased engagements in Cyber Diplomacy from the United Nations, the United States, and the European Union. In 2021, the EU published a new strategy on cybersecurity. In 2022, the US Department of State released a new report on 'International Norms for State Behaviour in Cyberspace' [5], and the UN General Assembly adopted a resolution on 'Principles of responsible state behaviour in cyberspace' [6]. This year, 2023, the European Union and the United States re-engaged in cyber security dialogue to strengthen cooperation on cyber security issues, such as incident response. The United States also helped first talk with China in over two years on reducing the risk of miscalculation and escalation in cyberspace. Apart from national efforts, there is also a significant effort from non-governmental organisations (NGOs), and businesses operating in related areas.

1.3. Understanding the digital realm's impact on international relations

The widespread use of the internet and the quick development of technology have radically altered how nations connect and carry out diplomacy. The importance of the online environment in influencing international relations has been demonstrated by several important factors (outlined in Figure 1), and Digital Diplomacy is just one of these factors.

A vital aspect of international relations today is the digital economy. Digital trade, cross-border e-commerce, and data transfers are important economic expansion and international trade drivers. Disputes over data privacy and digital trade regulations significantly impact international diplomacy.

The digital sphere has enabled unprecedented global connectivity by enabling cross-border real-time communication and information sharing between people, governments, and organisations. As a result of this interconnection, the speed of international connections and diplomacy has increased.

Governments and diplomats use digital technologies, social media, and online platforms to interact with international audiences, share information, and carry out diplomatic outreach. Direct communication with ordinary people

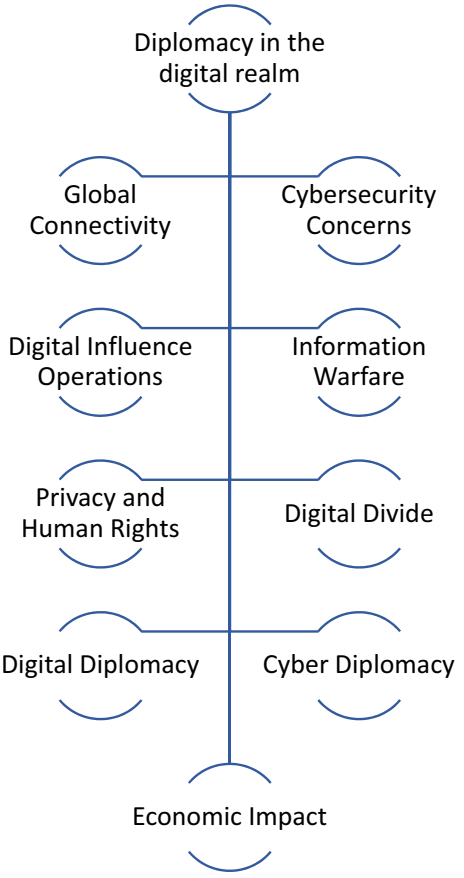

Figure 1. How the digital realm is influencing international relations.

is made possible by digital diplomacy, which also encourages more openness in diplomatic exchanges.

The use of social media and online platforms to influence public opinion and interfere in the internal affairs of other nations has come under diplomatic scrutiny. Cyber diplomacy includes addressing digital influence efforts. Cyber diplomacy focuses on managing and negotiating cyber-related concerns in international relations. This involves setting cyber norms, encouraging ethical and political conduct, and collaboratively resolving cyber crises. As a result, privacy and human rights have become issues in the digital world. When it comes to surveillance and data privacy, nations struggle to strike a balance between preserving individual rights and enforcing national security measures.

International security also faces additional challenges primarily because of technological advances. Cyber risks like cyberterrorism, cyberwarfare, and cyber espionage present serious national and international security concerns. To successfully address and mitigate these cyber risks, nations must work together. Information warfare has increased because of the advances in

digital technologies, in which states and non-state actors utilise information and disinformation campaigns to impact public opinion and political outcomes in other nations. Without further focus on cyber diplomacy, we can expect tensions to arise in diplomatic relations because of this digital evolution.

1.4. The significance of international cooperation in cyberspace

As the digital domain continues to play an increasingly important role in many parts of our lives, especially in the economy, security, and communication, countries must work together to handle the specific challenges it brings.

Cyber risks are not geographically confined; hackers can target any nation or organisation, regardless of location. By working internationally, countries can combine their resources, intelligence, and skills to detect, prevent, and respond to cyber-attacks with global implications. Cyber issues affect every country. International collaboration allows for exchanging best practices, information, and experience to enhance cyber resilience. Learning from one another's triumphs and errors might assist nations in strengthening their cybersecurity measures and mitigating potential risks.

In the cyber world, data moves across boundaries. The internet is a global resource that must be governed collaboratively. International cooperation is critical in developing policies addressing challenges related to Internet governance, such as domain name systems, internet protocol allocations, and net neutrality. Therefore, to establish data protection and privacy standards, collaboration across borders can ensure that personal information is handled responsibly and under international regulations. Cyber incidents can easily develop into crises with far-reaching consequences. Cooperation among nations helps coordinate crisis management and incident response activities, thereby preventing further damage and assisting in data recovery.

1.5. Exploring the impacts of emerging technologies on cyber diplomacy: the impact of Artificial Intelligence (AI), the Internet of Things (IoT), Blockchains, and Quantum Computing on cyber diplomacy

This section integrates with the existing structure by expanding on the technological aspects discussed in the introduction and subsequent chapters. It provides a detailed analysis of how each technology impacts cyber diplomacy, backed by recent academic studies and publications. The section concludes by emphasising the necessity of international collaboration and the development of global norms and frameworks to address the challenges posed by these emerging technologies.

1.5.1. The role of artificial intelligence in shaping cyber diplomacy

Artificial Intelligence (AI) has become a pivotal element in cyber diplomacy, influencing various aspects, from threat detection to international negotiations. AI's ability to analyse vast datasets rapidly is instrumental in identifying potential cyber threats, aiding diplomatic efforts in cybersecurity. Recent studies, such as those by Bommasani et al. [3], highlight AI's role in compliance and regulatory frameworks, which are crucial in international cybersecurity agreements.

1.5.2. Internet of Things (IoT) and Its diplomatic implications

The proliferation of IoT devices has significant implications for cyber diplomacy. IoT devices contribute to an interconnected global network, raising concerns about cross-border data flows and international standards for device security. Yadav [2] emphasises the complexity of IoT in national cybersecurity, highlighting the need for international cooperation in standardising IoT cybersecurity practices.

1.5.3. Blockchain technology's influence on cyber diplomacy

Blockchain technology introduces a novel secure data sharing and verification paradigm for cyber diplomacy. The immutability and transparency of blockchain can enhance trust in international agreements and shared documents. However, as Suhag and Daniel [4] point out, the technology also presents new challenges regarding AI-driven cyber-attacks, necessitating a revaluation of diplomatic strategies in the blockchain era.

1.5.4. Quantum computing: a new frontier in cyber diplomacy

Quantum computing presents both an opportunity and a challenge for cyber diplomacy. Its potential to break conventional encryption poses a significant threat to national security, requiring international cooperation to develop quantum-resistant cryptographic standards. Lancelot [1] discusses the implications of quantum computing in cyber warfare and international engagement rules, underlining its impact on future diplomatic relations.

2. Research methodology

The paper begins with a comprehensive review of existing academic and policy-oriented works in the fields of Cyber Diplomacy, AI, Machine Learning, Cryptography, and Cybersecurity. This review establishes a foundational understanding of the current state of research and practice in these areas. The comparative analysis distinguishes Cyber Diplomacy from traditional diplomatic methods, highlighting its unique applicability in addressing modern digital challenges.

The study uses a case study approach to examine real-world scenarios where Cyber Diplomacy has been instrumental in mitigating risks associated with advanced technologies. This method enables a deeper understanding of the

practical applications and implications of Cyber Diplomacy in various geopolitical contexts. By examining specific cases, the study identifies patterns and principles that are applicable more broadly in the realm of international cyber relations.

The methodology integrates insights from international relations, computer science, cybersecurity, and legal studies, acknowledging the interdisciplinary nature of the subject. This cross-disciplinary approach ensures a holistic understanding of how technological advancements intersect with diplomatic efforts.

To collect data, the study employs qualitative research methods, including interviews with experts in Cyber Diplomacy, Cybersecurity, and Technology Policy, and analysis of policy documents, treaties, and international agreements. This data offers a nuanced perspective on the ways in which nations are dealing with the challenges posed by emerging technologies in the diplomatic arena.

Drawing on insights from the literature review, case studies, and data analysis, the study develops a theoretical framework. This framework explains the relationship between Cyber Diplomacy and technological advancements, detailing the dual nature of these technologies as sources of both risks and opportunities.

The study evaluates and synthesises the findings, drawing conclusions about the role of Cyber Diplomacy in addressing digital challenges and making recommendations for future research and policy development.

3. International laws and norms in cyberspace

3.1. Cyber diplomacy actors: states and their roles in cyber diplomacy

Nation-states play a critical role in cyber diplomacy. They engage in diplomatic efforts to handle cyber dangers, negotiate cyber norms agreements, and encourage responsible cyber behaviour. States formulate cyber plans and policies and discuss cyber with other countries. Diplomats and diplomatic corps represent their governments in international forums and internet conversations. They participate in cyber-related debates, develop contacts with other countries, and advocate for their country's interests in cyber concerns.

Cyber Diplomacy is facilitated by organisations such as the United Nations (UN), the European Union (EU), and the International Telecommunication Union (ITU). They facilitate worldwide cyber norms and governance debates, talks, and initiatives. In addition, internet forums, such as the Internet Governance Forum (IGF), provide a forum for diverse actors, such as governments, the commercial sector, civil society, and academia, to discuss and define cyberspace policies. The media also influences public opinion and increases awareness about cyber concerns. Coverage of cyber occurrences, policies, and international cyber talks can influence public and government opinions and actions.

3.2. Cyber diplomacy actors: non-state actors' influence on cyber international relations

Private enterprises and corporations can have an important role in the Internet. They contribute to cyber diplomacy by forming public-private partnerships, sharing threat intelligence, and working with governments to improve cybersecurity and safeguard key infrastructure. Civil society organisations, such as academic institutions, advocacy groups, and cybersecurity communities, perform an important role in Cyber Diplomacy. They raise awareness, share expertise, and campaign to preserve digital rights and liberties.

Non-governmental organisations (NGOs) and think tanks contribute to cyber diplomacy by conducting research, giving expert analysis, and advocating for safe cyber practices. They frequently provide policy suggestions and work with governments and international agencies. In Cyber Diplomacy conversations, cybersecurity experts, researchers, and technical specialists share useful insights and ideas. Their knowledge contributes to developing policies, tactics, and international cybersecurity activities.

3.3. Existing international cyber laws and treaties

There are various international cyber laws and treaties in place that try to address cyber concerns and promote responsible cyber behaviour. In Table 3 we summarise the most known international laws and treaties that can be related to cyber.

Some of the treaties in Table 3 have a secondary effect on cybersecurity by addressing child exploitation and transnational organised crime, highlighting the interconnection of multiple legal frameworks in cyberspace. As the digital world evolves, international efforts to create new accords and enhance current ones will be critical in ensuring the global community has a secure and stable cyberspace.

4. Cyber crisis management and response

4.1. Strategies for handling cyber incidents and crises

Data breaches and ransomware attacks, along with sophisticated state-sponsored cyber espionage, are just a few examples of cyber incidents. International crisis management is focused on three key areas: international cooperation, legal frameworks, and public awareness. International cooperation includes working with other governments to share cyber threat information, investigate cybercrime, and prosecute cybercriminals. Legal frameworks involve drafting and implementing cybercrime-related laws and regulations. Public awareness includes informing the public about cyber risks and how to protect oneself against such risks.

Table 3. Summary table of various international cyber laws and treaties related to cyber diplomacy.

Treaty/Agreement	Description
United Nations Group of Governmental Experts (UN GGE) Reports [7]	The UN GGE has published several reports that provide guidelines and recommendations on responsible state behaviour in cyberspace. These reports highlight the importance of adhering to international law and norms in cyberspace.
Tallinn Manual [8]	The Tallinn Manual is a comprehensive analysis of how international law applies to cyber operations. It was prepared by experts and provides guidance on issues like sovereignty, self-defence, and the law of armed conflict as they relate to cyberspace.
Convention on Cybercrime (Budapest Convention) [9]	The Budapest Convention is the first international treaty addressing cybercrime. It aims to harmonise national laws, improve international cooperation, and enhance capabilities for investigating and prosecuting cybercrime.
United Nations Convention on the Law of the Sea (UNCLOS) [10]	While not specifically focused on cyberspace, UNCLOS includes provisions related to the use of information and communication technologies in maritime operations.
Joint Comprehensive Plan of Action (JCPOA) [11]	This agreement, also known as the Iran Nuclear Deal, includes provisions relating to cybersecurity in the context of nuclear facilities.
European Union General Data Protection Regulation (GDPR) [12,13]	Though not exclusively a cyber treaty, GDPR regulates the protection and privacy of personal data in the EU and has extraterritorial reach for companies handling EU citizens' data.
Wassenaar Arrangement [14]	This is not a treaty but an export control regime that regulates the trade of conventional arms and dual-use goods and technologies, including certain cybersecurity-related items.
Organisation of American States (OAS) Cybersecurity Program [15]	The OAS has a cybersecurity program that aims to promote regional cooperation and capacity-building efforts to address cyber threats in the Americas.
African Union Convention on Cyber Security and Personal Data Protection [16]	Adopted in 2014, this treaty aims to harmonise cybersecurity and data protection efforts across African countries.
United Nations Convention Against Transnational Organised Crime (Palermo Convention) [17]	Does not specifically address cybercrime but includes provisions that are relevant to the investigation and prosecution of cybercrimes committed by organised criminal groups. Requires state parties to criminalise the use of computers for money laundering and to cooperate in investigating and prosecuting these offenses.
Convention on the Rights of the Child (CRC) [18]	Protects the rights of children, including their right to privacy. Article 34 of the CRC prohibits the sexual exploitation of children, including child pornography. The CRC has been ratified by 196 countries, making it one of the most widely ratified human rights treaties.
Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography [19]	Supplements the CRC by prohibiting the sale of children, child prostitution, and child pornography. Requires state parties to take measures to protect children from these practices.

Some of the organisations that work in this space include:

- The United Nations Office on Drugs and Crime (UNODC): addressing cybercrime.
- The United Nations Interregional Crime and Justice Research Institute (UNICRI): addressing cybercrime.
- The Council of Europe Convention on Cybercrime (Budapest Convention): international treaty on cybercrime.
- Organisation for Economic Co-operation and Development (OECD): Guidelines for the Security of Information Systems and Networks.
- International Telecommunication Union (ITU): the ITU Cybersecurity Framework

Given the importance of digital technologies in the economy and society, we can realistically expect many new organisations to be created. The focus will, however, remain similar among most of these organisations. The focus is on prevention, detection, response, and mitigation. Prevention of cyber incidents is usually conducted by implementing security measures, educating users, and sharing information. Detection at the moment is predominately focused on the speed of detection, because hackers would be able to exploit a vulnerability until is detected and patched. Detection involves monitoring for suspicious activity, conducting regular security audits, and having a plan in place for responding to cyber incidents. Response usually involves isolating infected systems, restoring data from backups, and notifying affected users. The final step is mitigation, and it usually refers to having plans to communicate and rebuild systems and data, and usually includes some form of cyber insurance. A more detailed summary of the steps that are performed at each stage is included in Table 4, where individual strategies are described in detail.

As cyber incidents and crises transcend national borders, robust and coordinated responses are required to reduce their impact. Standardising methods for dealing with cyber incidents globally is critical to ensuring a unified and harmonised approach to cybersecurity across states. International standardisation allows smooth collaboration, information sharing, and mutual support during cyber crises by defining uniform principles, best practices, and frameworks. It promotes a collective defensive mechanism, increasing global cyber resilience and the ability to combat cyber threats successfully. Furthermore, standardisation fosters transparency and uniformity in incident response, critical for developing confidence between governments and stakeholders. In Table 5, we describe the leading international standards that enable the global community to face cyber problems collectively and protect the digital realm's integrity, security, and stability.

Table 4. Summary of strategies for handling cyber incidents and crises.

Strategy	Description
Preparation and Planning	Proactively prepare and develop a comprehensive incident response plan that outlines roles, responsibilities, and procedures for different stakeholders. Conduct regular cyber incident response drills and simulations to ensure readiness.
Incident Identification and Assessment	Establish robust monitoring and detection systems to identify cyber incidents promptly. Monitor network traffic, conduct log analysis, and use intrusion detection systems to detect suspicious activities. Rapidly assess the scope and severity of the incident to determine the appropriate response.
Containment and Mitigation	Take immediate action to contain the incident's impact and prevent further damage. Isolate affected systems, shut down compromised accounts, or disconnect from the network if necessary. Implement mitigation measures to limit the attacker's access and control.
Forensics and Investigation	Conduct thorough forensic analysis to understand the attack vectors, identify the extent of the breach, and preserve evidence for potential legal proceedings. Engage cybersecurity experts and law enforcement, if required, to investigate the incident thoroughly.
Communication and Reporting	Maintain clear and transparent communication during the cyber incident or crisis. Notify relevant stakeholders, including customers, partners, employees, and regulatory authorities, about the incident promptly. Maintain open lines of communication throughout the incident response process.
Coordination and Collaboration	Establish a centralised incident response team that includes representatives from IT, legal, communications, and senior management. Collaborate with external partners, such as law enforcement agencies or cybersecurity firms, as needed.
Recovery and Remediation	Develop a recovery plan to restore affected systems and services to normal operations. Prioritise critical systems and data for restoration. Conduct post-incident reviews to identify lessons learned and implement necessary security improvements.
Public Relations and Reputation Management	Have a well-defined public relations and reputation management strategy to address media inquiries and maintain stakeholders' trust. Cyber incidents can significantly impact an organisation's reputation.
Legal and Regulatory Compliance	Ensure compliance with applicable laws and regulations while handling cyber incidents. Report incidents to regulatory authorities as required and cooperate with law enforcement during investigations.
Continuous Improvement	Analyse the incident response process after resolving a cyber incident to identify areas for improvement. Use the lessons learned to update incident response plans, security measures, and training programs for staff.

These multinational initiatives give useful norms and guidelines for dealing with cyber emergencies and incidents. Using these best practices, organisations can improve their incident response skills and collaborate globally during cyber emergencies. Creating such standards promotes uniformity and speed in reacting to cyber-attacks, resulting in a more secure cyber environment.

4.2. Building trust and cooperation during cyber emergencies

During cyber emergencies, trust and cooperation are critical for successful incident response and limiting the effects of cyber threats. Individual data breaches and large-scale cyberattacks on critical infrastructure can all result in various cyber emergencies.

Communication is important during global cyber emergencies, and we need to have established communication channels. Such channels must include

Table 5. International efforts to standardise handling cyber incidents and crises.

Standard/Guideline	Description
ISO/IEC 27,035 [20]	This standard, published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), provides guidance on the processes and principles for incident management, including planning, detection, reporting, assessment, and response.
NIST Special Publication 800–61 Revision 2 [21]	Published by the National Institute of Standards and Technology (NIST) in the United States, this document offers guidelines for Computer Security Incident Handling, including preparation, detection, analysis, containment, eradication, recovery, and post-incident activities.
ENISA Incident Handling Guide [22]	The European Union Agency for Cybersecurity (ENISA) has developed a comprehensive guide on incident handling, which provides practical advice and recommendations to support incident response efforts.
FIRST Incident Handling Standards [23]	The Forum of Incident Response and Security Teams (FIRST) has developed a set of guidelines and standards for incident response to facilitate global collaboration and consistency in cyber incident handling.
OASIS Cyber Threat Intelligence (CTI) Technical Committee [24]	OASIS (Organization for the Advancement of Structured Information Standards) has established the CTI Technical Committee to develop standards for sharing cyber threat intelligence, which is a critical aspect of incident response.
CIS Controls [25]	The Center for Internet Security (CIS) has developed a set of best practices known as the CIS Controls, which includes specific recommendations for incident response and management.
CERT Coordination Center (CERT/CC) Incident Response Handbook [26,27]	The CERT/CC at Carnegie Mellon University provides a comprehensive handbook on incident response, outlining a structured approach for handling cyber incidents.
ITU-T X.1500 Series [28]	The International Telecommunication Union (ITU) has developed the X.1500 series of standards, which focuses on the management of cybersecurity incidents and includes guidelines for incident detection, reporting, and handling.
ICANN Incident Response Plan [29]	The Internet Corporation for Assigned Names and Numbers (ICANN) has an incident response plan to address security incidents related to the internet's domain name system (DNS).

government agencies, private sector entities, law enforcement, and international partners. Communication must be clear and fast to share threat intelligence and incident updates and coordinate response actions.

Communication channels must include information sharing and collaboration between national and international private and public sectors. This includes the development of a culture of information sharing and collaboration, specifically on threat intelligence, indicators of compromise, and lessons learned from previous incidents. Such communication channels require the establishment of public-private partnerships. Private organisations typically possess important threat intelligence and technical expertise that can greatly enhance incident response operations. Governments should provide regulatory direction and enable information sharing to increase private sector resilience.

When sharing information and collaborating during cyber emergencies, we must recognise and respect each country's sovereignty and privacy concerns. We must also ensure that information-sharing practices are under applicable laws and regulations. To test the effectiveness of this collaboration, we need to

organise multinational cyber exercises and simulations to strengthen cooperation and confidence among participating countries. These exercises allow different countries to evaluate their crisis response capabilities in a controlled setting and cooperatively identify areas for development. We need to define each stakeholder's roles and responsibilities during cyber emergencies. By defining the incident response roles at the national and international levels, we ensure that all stakeholders know their respective contributions and expectations.

Incident response mechanisms must encourage openness in incident reporting and response efforts while holding individuals accountable for malicious cyber activity. Sharing information about cyber issues openly helps to create trust and allows others to learn from past mistakes. There is an element of continuous learning and improvement of cyber incident response capabilities. This includes sharing best practices and lessons learnt from previous incidents with others to help them improve their reaction techniques.

One of the most important tools for developing trust and cooperation is the creation of mutual aid and assistance agreements at the national and international levels. These agreements describe how governments or organisations will assist one another during cyber emergencies by giving cybersecurity professionals resources or essential information.

By implementing these methods and actively encouraging trust and cooperation, the global community could strengthen its collective resilience and reaction to cyber emergencies. Effective collaboration in such emergencies is essential for reducing the impact of cyber threats and protecting the digital infrastructure on which our societies rely.

5. National cyber strategies

- Development and implementation of effective national cyber policies.

The first cyber policy to review is the United States (U.S.) National Cybersecurity Strategy 2023 document [30].

In the United States, the National Cybersecurity Strategy 2023 presents a structured and ambitious path for strengthening the country's cyber defences. In this section, we look at the specific activities in the National Cybersecurity Strategy 2023 that indicate the United States' commitment to improving its cybersecurity capabilities. Notably, the policy emphasises the necessity of investing in cybersecurity research and development, which underpins the nation's pursuit of cutting-edge solutions to combat emerging cyber threats. Furthermore, the National Cybersecurity Strategy 2023 emphasises the importance of increased cyber threat information sharing and better cooperation between the public and commercial sectors to establish a more comprehensive cyber defence ecosystem.

The policy aims to close the cybersecurity skills gap by prioritising the advancement of cybersecurity experts' training, assuring a trained and knowledgeable workforce capable of efficiently defending against cyberattacks. National Cybersecurity Strategy 2023 emphasises enhancing the resilience of critical infrastructure by protecting important systems and networks from potential cyber disturbances. This evaluation offers insights into the activities stated in the NCSS 2023, highlighting the country's unwavering commitment to boosting its cybersecurity posture and safeguarding the digital landscape.

The National Cybersecurity Strategy 2023 is a strategic framework for protecting the United States in cyberspace and is based on five pillars, which resemble the areas of focus discussed in earlier sections. These include:

- **Resilience**: be resilient to cyber threats to withstand and recover from attacks.
- **Prevention**:prevent cyber threats.
- **Detection**:detect cyber threats as early as possible.
- **Response**:respond to cyber threats quickly and effectively.
- **Mitigation**: mitigate the impact of cyber threats.

The success of the National Cybersecurity Strategy 2023 as a comprehensive and ambitious strategy for securing the United States in the digital sphere is dependent on the engagement and cooperation of all stakeholders, including the governmental, corporate, and civil society sectors. This emphasises the necessity for coordinated measures to combat cyber-attacks and secure critical infrastructure. The primary lessons from the National Cybersecurity Strategy 2023 highlight the increasing complexity of the cyber threat scenario, which necessitates a collaborative approach to national security.

The second national cyber strategy to evaluate is the UK National Cyber Strategy 2022 [31], which is a strategic framework for protecting the United Kingdom in cyberspace. Similarly, to the U.S. National Cybersecurity Strategy 2023, the UK National Cyber Strategy 2022 is based on the following four pillars:

- **Resilience**:be resilient to cyber threats to withstand and recover from attacks.
- **Prevention**:prevent cyber threats from occurring.
- **Detection**:detect cyber threats as early as possible.
- **Response**:respond to cyber threats quickly and effectively.

Another almost identical aspect between the two strategies is the focus on investing in cyber research and development, improving the sharing of

information about cyber threats, providing more training, and increasing resilience. The remaining aspects of the UK National Cyber Strategy 2022 are almost entirely based on the cybersecurity practices discussed in earlier sections, including focus on:

- Adapt in the increasingly sophisticated and dangerous cyber threat landscape.
- Collaborations between the government, the private sector, and civil society.
- Provides a roadmap for how the United Kingdom can achieve cybersecurity goals.
- Focus on the importance of international cooperation in addressing cyber threats.
- Commitment to working with other countries to share information and investigate cybercrimes.

More analytically, what is missing in the UK National Cyber Strategy 2022 is a clear commitment to specific regulatory requirements in the U.S. National Cybersecurity Strategy 2023. One specific example is the Software Bill of Materials (SBOM) [32–34], which is a requirement in the U.S. and SBOM is not even mentioned in the UK National Cyber Strategy 2022. One valid reason for missing out on compulsory requirements is when this strategy was developed. The U.S. version was published in 2023, and the UK version in 2022. However, upon further research, we find that SBOM was announced in 2022 - Executive Order 14,028. Executive Order 14,028 [35]went into full effect in August 2022, and the UK National Cyber Strategy 2022 was published in December 2022. Given the importance of this executive order, one would expect the UK National Cyber Strategy 2022 to reflect on this, especially given the special relationship between the U.S. and the UK. The commitment to working with other countries is fundamentally dependent on standardising the regulations, especially those that do not create any conflict and improve a country's cybersecurity posture.

The European Union (EU) has proposed multiple strategies in the previous five years. The most recent addition is the EU Cyber Solidarity Act [36], which consists of solidarity through a cyber emergency mechanism, cybersecurity shield, incident review mechanism, and funding for EU states. The cyber emergency mechanism is a critical step forward in strengthening the European Union's cybersecurity planning and response capabilities. One of its important components is to improve preparation by rigorously testing businesses in crucial industries such as finance, energy, and healthcare. The system attempts to uncover potential gaps and vulnerabilities that could expose these sectors to cyber threats through extensive testing, allowing for targeted and preventive security solutions. In addition, the creation of an EU Cybersecurity Reserve comprised of trustworthy service providers adds a substantial degree of assistance.

This collection of incident response resources can be quickly deployed at the request of Member States or Union Institutions, allowing for a coordinated and efficient response to major cybersecurity incidents. Furthermore, the Cyber Emergency Mechanism encourages and simplifies Member States' reciprocal aid. The mechanism supports a collective approach to cyber defence by encouraging information sharing, knowledge exchange, and coordinated action, thus strengthening the EU's overall cyber resilience. These critical features make the Cyber Emergency Mechanism an important step towards protecting the EU's digital landscape and allowing the area to tackle the evolving cyber threats it faces.

The European Cyber Shield is grounded on collaborative efforts of different Security Operations Centres. These Security Operations Centres, dispersed throughout the EU, will collaborate under several multi-country platforms funded by the Digital Europe Programme, complementing national funding to ensure comprehensive coverage. The primary objective of the Cyber Shield is to enhance the detection, analysis, and response to cyber threats. Leveraging advanced technologies like Artificial Intelligence (AI) and data analytics, these Security Operations Centres will promptly identify and share threat warnings with authorities across borders, enabling a swift and coordinated response to significant threats. Notably, the Cyber Shield's first phase, initiated in November 2022, saw the selection of three consortia comprising cross-border Security Operations Centres from 17 Member States and Iceland, marking a crucial milestone in the program's implementation and paving the way for a more resilient and secure digital landscape within the EU.

5.1. Key components of a comprehensive cyber strategy

A comprehensive cyber strategy includes several key elements working collectively to confront dynamic and emerging cyber threats effectively. First, it entails undertaking extensive risk assessments and exploiting threat information to detect weaknesses and keep up with the ever-changing threat landscape. Creating a strong national cybersecurity policy and framework gives a clear vision and priorities for protecting key assets.

Collaboration between the public and private sectors is essential for sharing information, resources, and expertise and creating a united front against cyber attackers. This also enhances the process of protecting essential infrastructure sectors such as electricity, finance, healthcare, and transportation, which are critical to boosting national resilience. Adding to this, creating a well-defined incident response strategy and cyber crisis management processes allows for identifying, reacting, and recovering from cyber catastrophes to occur as quickly as possible. The comprehensive cyber strategy also requires capacity building and training initiatives to provide government

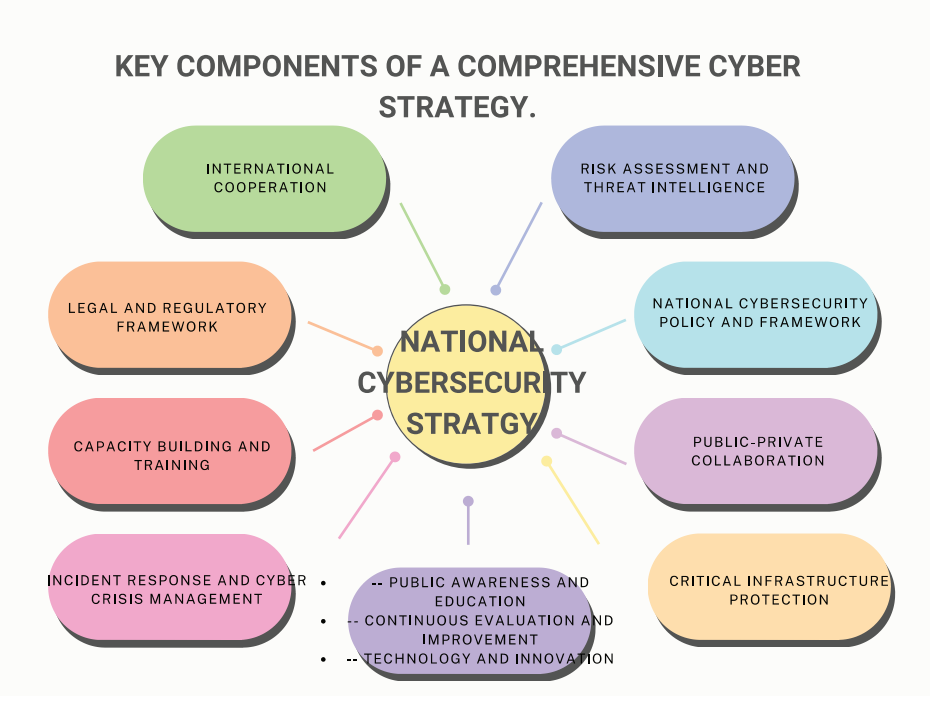

Figure 2. Mapping the requirements for national cybersecurity strategies.

employees, law enforcement, and the commercial sector with the information and skills to tackle cyber threats.

A comprehensive cyber strategy is grounded on a comprehensive legal and regulatory framework that addresses cybercrime, data protection, and privacy concerns, establishing a legal foundation for punishing cyber offenders and protecting personal data. International cooperation and information exchange enables global collaboration in countering cyber threats. Citizens are educated about cyber hazards through public awareness programmes, producing a cybersecurity-conscious society.

In addition, continuous evaluation and improvement ensure that the cyber strategy stays adaptable and robust in the face of increasing threats and technological advances. Modern technologies such as artificial intelligence (AI), machine learning, and data analytics improve cybersecurity and fortify defence against cyber threats. In Figure 2, we can see the main components of successful national cybersecurity strategies. Nations may enhance their cyber defences and create a resilient digital landscape by incorporating these critical components into a comprehensive cyber plan.

The components outlined in Figure 2, are extracted from the case study reviews of the earlier analysis of various international cyber laws and treaties related to cyber diplomacy. The elements are also compared and related to the U.S. National Cybersecurity Strategy 2023, the UK National Cyber Strategy 2022, and the EU Cyber

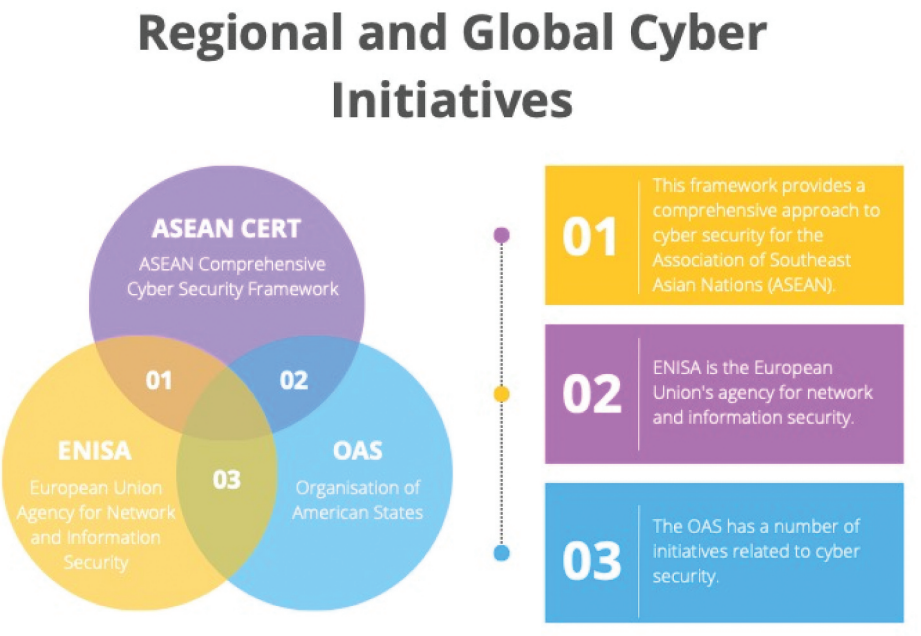

Figure 3. Regional cyber initiatives.

Solidarity Act. In the future, this mapping needs to be updated with the key components from other national strategies, including the national strategies of China, India, and other major players in cyber diplomacy.

6. Regional and global cyber initiatives

6.1. Collaborative efforts to address cyber threats at regional and global levels

There are many regional and global cyber initiatives, and many are already discussed in the previous sections. In this section, we focus on three regional initiatives and three global initiatives. In Figure 3, we outline the three regional initiatives that will be reviewed in this section.

The reason for choosing these three frameworks in Figure 3, is that the combination of these frameworks represents the largest percentage of the world, including the USA, EU and Asia. The ASEAN Comprehensive Cyber Security Framework (ASEAN CERT) is an outstanding initiative demonstrating the Association of Southeast Asian Nations' (ASEAN) commitment to addressing the region's growing cybersecurity challenges. The framework provides a comprehensive and collaborative approach to improving ASEAN member nations' cybersecurity resilience. ASEAN CERT improves the region's ability to respond to cyber incidents by encouraging information sharing, capacity building, and coordination among national Computer Emergency Response Teams

(CERTs). Furthermore, the framework encourages public-private partnerships, guaranteeing that governments and private sector entities collaborate to address cyber threats and protect critical infrastructure.

The formation of ASEAN CERT is an important step towards strengthening cybersecurity across the region, enabling a safer and more secure digital environment for ASEAN states and their inhabitants. On the other hand, continuous evaluation and investment in cybersecurity resources will be critical to the framework's long-term performance and adaptability in the face of emerging cyber threats. Overall, the ASEAN Comprehensive Cyber Security Framework illustrates ASEAN's dedication to collective cybersecurity efforts, creating a solid foundation for regional collaboration and resilience in an ever-changing cyberspace context.

The European Union Agency for Network and Information Security (ENISA) [22,37]is a critical component of the EU's cybersecurity infrastructure. ENISA, as the designated network and information security agency, plays a critical role in assisting the European Commission and Member States in addressing various cybersecurity concerns. Its comprehensive role includes creating shared standards and best practices critical for coordinating cybersecurity activities across the EU.

ENISA encourages innovation and remains at the forefront of cybersecurity improvements through coordinating research and development projects. Furthermore, the agency's training and awareness-raising initiatives are important in improving cyber literacy and preparation within the EU community. ENISA's resolute commitment to developing cybersecurity resilience and collaboration makes it vital to protecting Europe's digital infrastructure and data from ever-changing cyber threats. Its ongoing efforts to establish a cyber-safe EU are critical in constructing a resilient and secure digital future for the area.

The Organisation of American States (OAS) is important in advancing cyber security activities among its member countries. Notably, the Inter-American Committee against Terrorism (CICTE) of the Organisation of American States (OAS) demonstrates its commitment to resolving cyber security concerns. With a specialised cyber security working group, the OAS is actively involved in fostering collaboration and sharing best practices among member states. Furthermore, the organisation provides technical help to its member countries, offering valuable support and knowledge on cyber security issues. The Organisation of American States (OAS) proved an important ally in bolstering cyber resilience across the Americas by encouraging collaboration and providing technical guidance. Its dedication to promoting cyber security programmes highlights its importance as a regional partner in protecting key infrastructure and data from cyber threats.

These three initiatives were selected because we haven't discussed these specific initiatives in this review study. In Table 6, we review and compare the main differences between these three regional initiatives. The main difference

Table 6. Comparison of the differences between the three regional initiatives, ASEAN CERT, ENISA, and OAS.

Organisation	Regional Focus	Mandate and Activities	Membership and Governance	Geopolitical Context
ASEAN CERT	Association of Southeast Asian Nations (ASEAN)	Fostering collaboration among ASEAN member states in sharing information, capacity building, and coordination of national CERTs.	Limited to ASEAN member states; Operates under the governance of the ASEAN community.	Addressing cybersecurity challenges specific to the ASEAN region.
ENISA	European Union (EU)	Providing support and expertise to the European Commission and EU member states on network and information security. EU member states; Operates under the governance of the European Commission.	Addressing network and information security concerns within the EU; Promoting cybersecurity cooperation among EU member states.	
OAS	Americas (North, Central, South America, and Caribbean)	Initiatives related to cybersecurity, including the Inter-American Committee against Terrorism (CICTE) and a cybersecurity working group.	Comprises 35 member states from the Americas; Operates under the governance of its member states.	Addressing cybersecurity challenges in the diverse geopolitical context of the Americas.

becomes immediately obvious, ENISA is not designed to consider the geopolitical context. ENISA is designed with a focus on EU membership and governance. Similarly, the ASEAN CERT and OAS are also designed as regional initiatives, but their context expands into the geopolitical context of the ASEAN region and the geopolitical context of the Americas. In contrast, ENISA is not designed to consider the context of the European continent but the context of the EU member states. We can anticipate this to change in the future, and this study could serve as a guidance document for developing the pilot program for expanding the focus of ENISA to include components relevant to the geopolitical context.

Table 6: Comparison of the differences between the three regional initiatives, ASEAN CERT, ENISA, and OAS. In Table 6, we reviewed and compared three regional initiatives about cyber. There are undoubtedly many more regional initiatives, and we will discuss other initiatives in other parts of this review study. The limitation to three regional initiatives in this section is predominately to reduce the review content and to avoid duplication of the discussion.

In Figure 4, we outline the three global initiatives we selected to review in this section: the Global Forum on Cyber Expertise (GFCE), the Cybersecurity Tech Accord, and the Cybersecurity and Infrastructure Security Agency (CISA). The reason we have chosen these global initiatives was their acceptance on a global level.

The GFCE is a global project that promotes cyber security by connecting governments, the commercial sector, and civil society. The GFCE serves as

Figure 4. Review of three global cyber initiatives.

a forum for exchanging information and best practices, as well as developing new initiatives to combat cyber threats.

The Global Forum on Cyber Expertise (GFCE) is an important worldwide project that brings together governments, the corporate sector, and civil society to enhance and promote global cybersecurity. This collaborative network is an important hub for exchanging technical information, expertise, and best practices in cybersecurity. The GFCE enables stakeholders to improve their cyber defence capabilities and respond effectively to changing cyber threats by facilitating information sharing and boosting cross-sectoral cooperation.

Furthermore, the forum promotes creating novel cybersecurity programmes and frameworks to address complex and developing digital concerns. The technical focus of the GFCE on capacity building, training, and cybersecurity policy creation provides participating institutions with the skills and tactics they need to strengthen their cyber resilience. As a result, the GFCE greatly contributes to the worldwide cybersecurity community's joint efforts in securing digital infrastructure and safeguarding sensitive data in an ever-changing threat landscape.

The Cybersecurity Tech Accord is an industry-led project promoting cybersecurity standards among technology companies. The Cybersecurity Tech Accord has different advantages in promoting cybersecurity practices among technology companies. One of its key assets is the industry-led strategy, which enables major technology companies to engage and share their cybersecurity experience proactively. The programme establishes a collective commitment to improving cybersecurity resilience and safeguarding consumers and users

from cyber-attacks by bringing together these essential players. Furthermore, the emphasis on establishing principles for greater cybersecurity practises demonstrates the Tech Accord's commitment to setting high cybersecurity standards within the technology industry.

However, the Tech Accord has certain inherent flaws. As a private-sector-led project, its impact may be confined to the technological corporations who join, leaving out smaller enterprises and businesses that may lack the resources to participate. Furthermore, the initiative's voluntary nature may result in various levels of dedication and adherence to cybersecurity principles, potentially resulting in inconsistencies in cybersecurity practices across the industry. The private-sector-led structure may have difficulty efficiently coordinating cybersecurity activities among varied technology companies with varying interests and ambitions.

To maximise its impact, the Tech Accord may need to address the participation of smaller enterprises and develop measures to ensure that all participating organisations adhere to cybersecurity principles consistently.

The Cybersecurity and Infrastructure Security Agency (CISA) is a US federal agency focusing on defending the nation's critical infrastructure and improving cybersecurity resilience across different industries. In its role as a significant government organisation responsible for securing critical infrastructure and strengthening cybersecurity resilience in the United States, CISA demonstrates various capabilities. One of its key assets is its narrow focus on protecting the nation's essential infrastructure. CISA ensures a targeted and planned approach to mitigating cyber threats that could seriously impact national security and public welfare by focusing on essential sectors such as energy, transportation, and communications.

Furthermore, CISA's collaborative approach is of considerable benefit. CISA fosters a comprehensive and coordinated effort to solve cybersecurity concerns by collaborating with federal, state, local, tribal, and territory governments and corporate sector partners. This multi-stakeholder model pools skills and resources from several organisations to form a strong network of cybersecurity defenders.

CISA's emphasis on technical competence, risk assessment, and incident response skills strengthens the nation's cybersecurity preparation. CISA enables organisations to proactively detect vulnerabilities, assess risks, and respond quickly to cyber incidents by providing specialised support and guidance to public and commercial institutions.

However, CISA has a few weaknesses. It could encounter bureaucratic problems as a government agency in coordinating activities across different levels of government and multiple business sector organisations. Furthermore, because of the scale of its focus on critical infrastructure, it may accidentally overlook cybersecurity risks in other industries or among smaller companies.

CISA's focus on vital infrastructure and collaborative approach are significant qualities that allow it to play a critical role in increasing the nation's cyber resilience. Nonetheless, removing bureaucratic roadblocks and establishing broad cybersecurity coverage across all sectors might strengthen the United States' cybersecurity posture even further.

6.2. Case studies of successful cyber initiatives

The first case study is the Multi-State Information Sharing and Analysis Centre (MS-ISAC).

The Multi-State Information Sharing and Analysis Centre (MS-ISAC) is a successful cyber initiative in the United States that focuses on improving cybersecurity resilience across state, local, tribal, and territorial (SLTT) administrations. MS-ISAC, founded in 2003, is a central centre where its members can share essential cybersecurity information, threat intelligence, and best practices. The initiative's success is based on its capacity to foster a collaborative environment where SLTT companies may proactively communicate insights, incident reports, and cyber threat remedies. The timely alerts and proactive cybersecurity advice provided by MS-ISAC have greatly contributed to lowering cyber risks and enhancing the overall cyber posture of SLTT governments around the country.

2nd Case Study: Cyber Green

Cyber Green is a successful global initiative that addresses the growing concern about the sustainability of cyberspace. This programme, launched in 2018, brings together cybersecurity professionals, environmental researchers, and industry stakeholders to investigate and minimise the environmental impact of cybersecurity practices. The success of Cyber Green is based on raising awareness about the carbon footprint of cyber activities and developing solutions to reduce energy consumption and electronic trash generation linked with digital infrastructure. Cyber Green contributes to a more environmentally conscious and responsible cybersecurity landscape by promoting eco-friendly cybersecurity practices and fostering sustainable approaches to information technology.

Case Study 3: United Kingdom's National Cyber Security Centre (NCSC)

The United Kingdom's National Cyber Security Centre (NCSC) is a successful government-led project dedicated to protecting the country from cyber-attacks. NCSC, established in 2016, is critical in providing technical expertise, threat intelligence, and direction to government and private sector organisations. The initiative's success is due to its proactive approach to cyber defence, which includes cybersecurity awareness programmes, incident response capabilities for organisations, and frequent advisories on developing cyber threats. Collaboration between the NCSC

and industry, academia, and foreign partners increases the nation's cyber resilience while contributing to the global fight against cybercrime.

These case studies highlight the effectiveness of different cyber projects, each addressing separate cybersecurity concerns and contributing to a safer and more resilient digital ecosystem. Whether focusing on information sharing, environmental sustainability, or national defence, these programmes highlight the value of collaboration, innovation, and a shared commitment to avoiding cyber risks.

7. Public-private partnerships in cyber diplomacy

7.1. The role of private sector entities in cyber diplomacy

Private sector organisations play an important role in cyber diplomacy, helping to shape international cybersecurity policies and practices. Their engagement arises from their substantial cyberspace presence and impact and their experience in designing and operating digital technology. In Figure 5, we summarise the areas of cyber diplomacy that benefit from Public-Private Partnerships.

Private sector organisations frequently have significant threat intelligence and data on cyber occurrences that they can share with governments and international organisations. They help improve early warning systems and contribute to a more comprehensive understanding of cyber dangers by partnering with governments, which aids in the creation of successful cyber policies.

The private sector actively contributes to creating cybersecurity standards and best practices. They contribute technical expertise and industry knowledge to developing guidelines that promote secure practices across sectors and

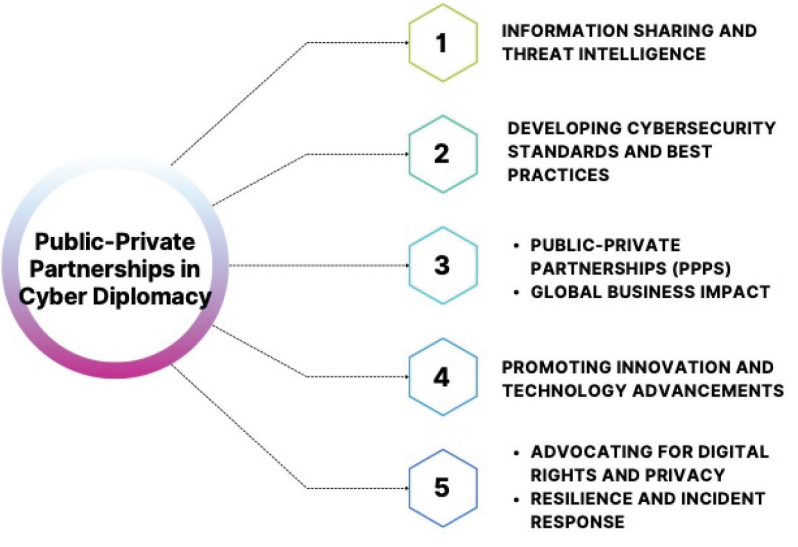

Figure 5. Areas of cyber diplomacy that benefit from public-private partnerships.

jurisdictions. Partnerships between governments and private sector groups are essential in addressing common security risks. These partnerships promote the interchange of information, resources, and knowledge, allowing for a better-coordinated response to cyber crises and a more integrated approach to cybersecurity.

Private-sector firms drive cybersecurity technology innovation, developing new tools and solutions to combat increasing cyber threats. Their efforts develop cyber defence capabilities, helping governments and society worldwide.

Private sector organisations are often the advocates for digital rights and privacy protections. Their participation in conversations about internet governance and data protection aids in striking a balance between national security concerns and individual liberties. Because of their global reach, private sector firms can influence cybersecurity norms and practices across borders. Businesses operating on a global scale face a variety of cybersecurity standards, necessitating diplomatic measures to promote cybersecurity policy harmonisation and consistency.

Private-sector organisations are actively involved in cyber incident response operations. Their experience dealing with cyber threats and breaches adds to a more resilient and coordinated worldwide strategy for mitigating cyber events. Private sector firms provide distinct viewpoints, resources, and technical knowledge in cyber diplomacy. Their partnership with governments and international organisations is critical to improving global cyber resilience, establishing trust, and protecting the digital world for public and commercial interests.

8. Cyber intelligence sharing

8.1. Challenges and benefits of sharing cyber threat intelligence

One of the main benefits of cyber intelligence sharing is access to shared threat intelligence. This offers organisations a more comprehensive perspective of the cyber threat landscape, allowing for improved decision-making. Another benefit is the increased capacity for early threat detection. Sharing cyber threat intelligence enables organisations to spot emerging attacks earlier and take proactive countermeasures. This improves and enhances the incident reaction time. Sharing threat intelligence on time allows for a faster and more effective reaction to cyber incidents, limiting the potential impact and minimising damage.

Cyber threat intelligence sharing encourages a collaborative approach to cybersecurity, boosting collective defence efforts among organisations and nations. This also enables proactive mitigation plans. Armed with external intelligence, organisations can change their cybersecurity plans and actions to counter specific threats. Sharing threat intelligence allows organisations to learn from each other's experiences, resulting in skill growth and enhanced knowledge in cybersecurity.

Sharing cyber threat intelligence supports public-private cooperation, combining the skills and resources of both sectors to tackle cyber threats effectively. Organisations can avoid duplicating efforts and expenditures in investigating and managing the same dangers by sharing threat intelligence.

Balancing these problems and rewards necessitates a complete approach considering legal, technical, and policy considerations. Encouragement of a trusting culture, the development of clear norms for sharing, and the provision of incentives for participation can all help to overcome hurdles and establish a successful cyber threat intelligence sharing ecosystem.

There also many challenges associated with cyber intelligence sharing. Organisations may hesitate to disclose sensitive cyber threat intelligence due to concerns about trust and the possible risks of disclosing vulnerabilities to others.

In addition, different jurisdictions may have different laws and regulations on data sharing, privacy, and liability, making cross-border threat intelligence sharing frameworks difficult to implement. Cyber threat intelligence frequently originates in various formats and patterns, making it challenging to consolidate and analyse data efficiently across several organisations.

Choosing the appropriate level of classification and sensitivity for shared threat intelligence can be difficult, as some information may be sensitive to specific entities. Organisations may lack sufficient incentives to share threat intelligence, particularly if there are no tangible benefits or rewards for participation. One of the largest issues remains the attribution problem. Attributing cyber threats to individual actors or entities can be difficult, leading to uncertainty and possibly intelligence misinterpretation.

8.2. International efforts to promote intelligence cooperation

There are numerous ongoing efforts to promote intelligence cooperation. Figure 6 helps visualise four ongoing international efforts to promote cyber intelligence cooperation. Although there are more international efforts, Figure 6

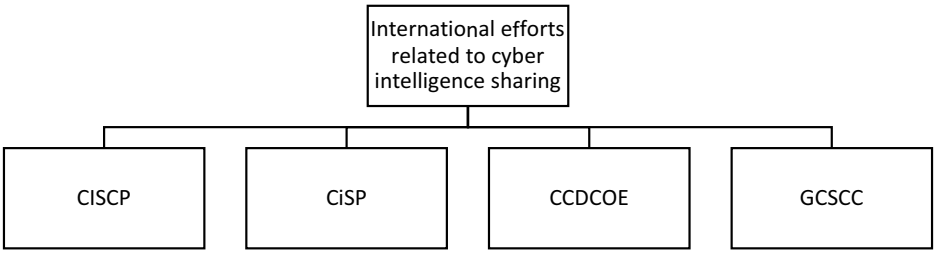

Figure 6. Ongoing efforts to promote intelligence cooperation.

is intended to help visualise the most prominent efforts and to start the discussion on what is missing in these international efforts. Hence, Figure 6 is not conclusive, but it represents a starting point for building the standardisation approach for addressing cyber risk from new and emerging technologies.

The text below discusses the four approaches from Figure 6 in more detail. One is the U.S. Cybersecurity Information Sharing and Collaboration Programme (CISCP). CISCP is a United States government effort that promotes information sharing between federal agencies and private-sector organisations to improve cybersecurity. Second is the UK NCSC Cyber Security Information Sharing Partnership (CiSP), a platform in the United Kingdom that allows organisations to share cyber threat information and best practices.

Another effort is CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence). CCDCOE is a NATO-accredited cybersecurity research and training facility that promotes member-country collaboration and information exchange. One ongoing academic effort is the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford. The Cyber Green programme examines national cybersecurity capacity and supports the global exchange of information on best practices and cyber capability. GCSCC is a cybersecurity capacity-building centre advocating an increase in the global scale, pace, quality, and impact of cybersecurity capacity-building activities. It has developed a first-of-its-kind approach for assessing cybersecurity capacity maturity across five dimensions to enable nations to self-assess, benchmark, better plan investments and national cybersecurity plans, and define priorities for capacity development.

9. Cyber diplomacy challenges and roadblocks

9.1. Attribution issues in cyberspace

Cyber diplomacy is confronted with several challenges and barriers capable of impeding successful international collaboration and the development of a secure and stable cyberspace. Cyber diplomacy is a challenging field due to several factors. One factor is the international character of cyber threats. Since cyber-attacks can originate anywhere globally, tracing and prosecuting hackers is difficult. The second factor is the lack of a unified international agreement defining what constitutes a cyber-attack or how to respond. This makes international cooperation on cyber security issues harder. The third factor is that cyber-attacks can be used for political purposes. Cyber-attacks can achieve political objectives such as disrupting elections or inciting societal discontent. This makes distinguishing between criminally motivated cyber assaults and politically driven cyber-attacks difficult. Apart from these, various other factors are summarised in Figures 7 and 8.

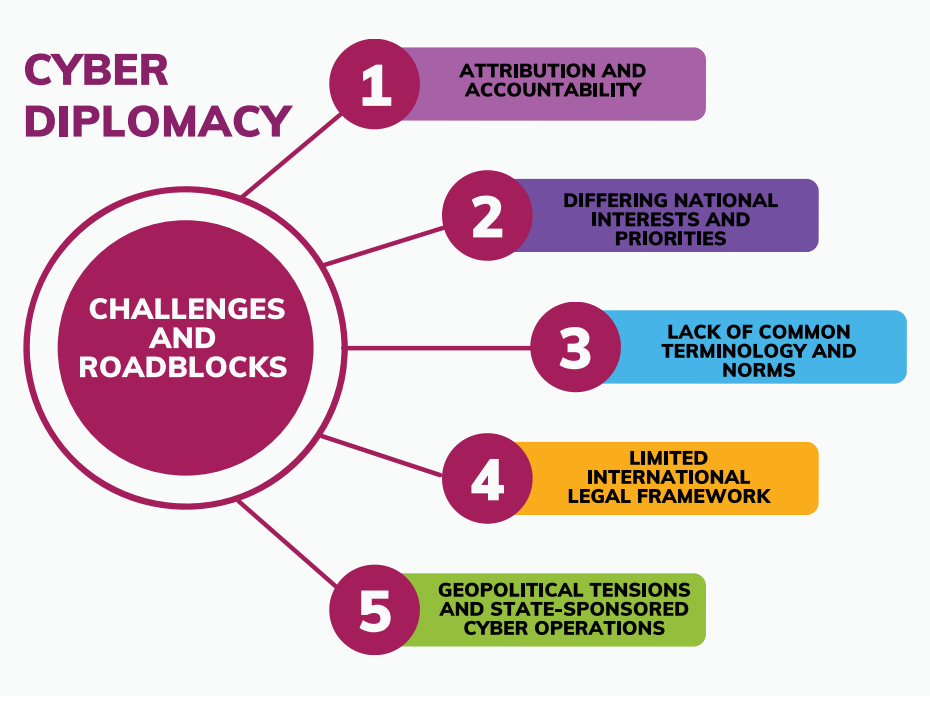

Figure 7. Cyber diplomacy challenges and roadblocks.

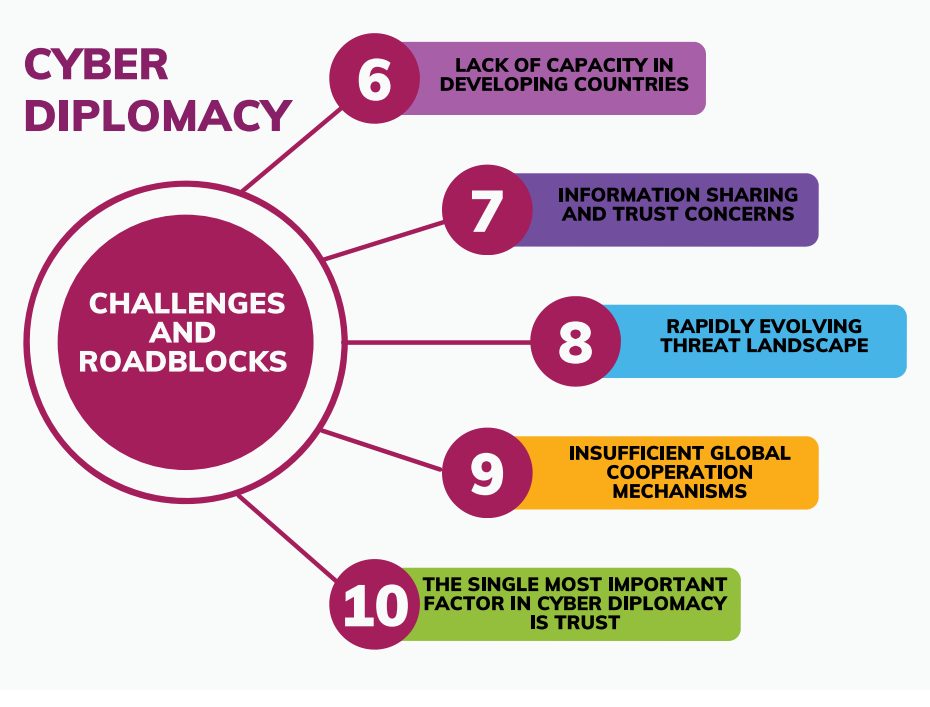

Figure 8. Cyber diplomacy challenges and roadblocks.

Attributing cyberattacks to specific actors or states accurately is one of the most difficult tasks in cyberspace. Because of the anonymity and simplicity of concealing one's identity in cyberspace, it is difficult to hold criminals accountable for their conduct, making implementing punishments for hostile cyber activities difficult.

When it comes to cybersecurity, nations' interests and priorities can differ. Balancing national security concerns with global cooperation can be difficult, resulting in various approaches to cyber diplomacy. The lack of widely acceptable vocabulary and norms in cyberspace impedes successful international communication and comprehension. This makes establishing common ground and shared norms for cooperation difficult. The international legal framework for cyber operations is continually changing, and gaps and inconsistencies exist in how existing rules apply to cyberspace. This renders setting guidelines for acceptable behaviour and establishing legal channels for addressing cyber issues difficult.

While the private sector is an important stakeholder in cyberspace, it can be difficult to coordinate and incentivise private businesses to participate actively in cyber diplomacy. Balancing business objectives with national security considerations may stymie productive public-private collaborations. Geopolitical conflicts might cross into cyberspace, resulting in state-sponsored cyber operations and intervention in the digital infrastructure of other countries. Such operations have the potential to worsen disputes and damage international trust.

Developing countries may lack the resources, experience, and infrastructure to handle cybersecurity concerns effectively. Closing the capability gap and providing proper capacity-building support is critical for a more inclusive and cooperative cyber diplomacy scene. Due to trust and sovereignty issues, countries may be unwilling to exchange important cybersecurity information. Fear of exposing vulnerabilities or relying on others for cybersecurity assistance might stifle information sharing.

Because cyber risks are dynamic and continuously growing, they require constant adaptation and response. Keeping up with new threats and implementing effective preventive measures can be an ongoing challenge for cyber diplomats. While numerous multinational initiatives exist, more comprehensive and inclusive global collaboration frameworks are required to handle cyber issues collectively. Building on existing institutions and creating new forums for conversation and collaboration can lead to more successful cyber diplomacy.

9.2. Overcoming geopolitical tensions in cyber negotiations

Overcoming geopolitical tensions in cyber discussions is a difficult and delicate endeavour, but it is critical for developing international collaboration and

effectively combating cyber threats. Figure 8 summarises strategies and approaches for overcoming geopolitical tensions in cyber negotiations.

As outlined in Figure 9, open and productive discussion is essential for addressing global problems. Diplomatic efforts should be directed towards identifying common ground and areas of mutual interest in cybersecurity. Creating regular communication and discussion avenues can help nations create trust and understanding.

Shifting the emphasis away from geopolitical issues and towards technological cooperation might be beneficial. Cyber diplomacy needs to be focused on encouraging joint research initiatives, cyber threat information exchange, and collaborative efforts to strengthen cybersecurity capabilities to build bridges and foster collaboration. Once such initiatives are identified, participation becomes very important, especially in global forums, such as the UN Group of Governmental Experts (UN GGE) or regional organisations. Such events provide a neutral platform for cyber negotiations. These venues can aid in the facilitation of discourse, the bridging of differences, and the promotion of consensus on cybersecurity concerns.

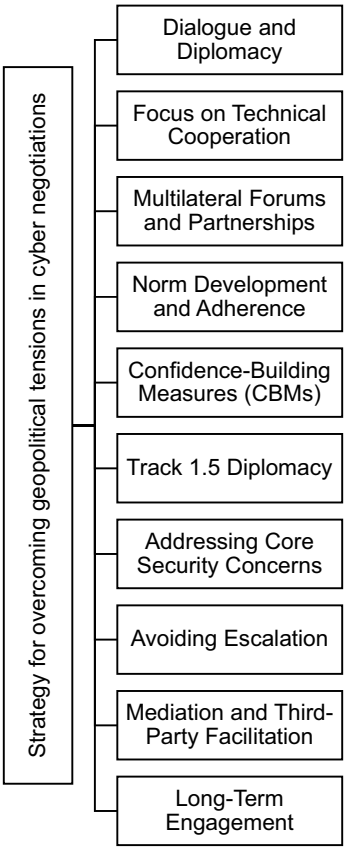

Figure 9. Summary of strategies and approaches for overcoming geopolitical tensions in cyber negotiations.

Encouragement of the establishment and adherence to international norms of responsible state behaviour in cyberspace can contribute to a shared understanding of proper behaviour. Nations can collaborate to develop rules that improve cybersecurity while discouraging malevolent behaviour. Implementing CBMs can help governments establish confidence and lessen tensions. These efforts may include the construction of hotlines for direct communication during cyber incidents, cooperative cyber exercises, and exchanging cybersecurity policy information.

In addition, Track 1.5 diplomacy can provide significant insights and create innovative solutions by involving non-governmental professionals and organisations in cyber negotiations. Non-governmental players can provide unbiased viewpoints and help governments overcome the gap.

Recognising and resolving nations' primary security concerns can also help to reduce hostilities. Understanding each country's unique cybersecurity concerns and weaknesses might help to establish a more compassionate negotiation atmosphere.

Parties should avoid actions that could exacerbate tensions further during discussions. Engaging in good-faith debates and using restraint in cyberspace can help to build an environment favourable to healthy dialogue. When tensions are high, neutral third-party mediators or facilitators can help bridge gaps and create compromise. Mediators can assist in steering conversations away from political issues and toward practical solutions. Overcoming geopolitical conflicts in cyber agreements frequently necessitates long-term commitment. To overcome deep-seated divisions, perseverance and ongoing efforts to discover common ground and build trust are required.

Nations can overcome geopolitical difficulties and develop a more cooperative and secure cyberspace by taking a patient and collaborative approach. Cyber diplomacy is critical in developing understanding, trust, and cooperation among governments to address today's global cybersecurity concerns effectively.

10. Future trends in cyber diplomacy

To clarify the contribution of this paper, I created a network diagram, which effectively displays the relationship between emerging technologies and cyber diplomacy, as discussed in the article 'Cyber Diplomacy: Defining the Opportunities for Cybersecurity and Risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing'.

The diagram showcases a central hub labelled 'Cyber Diplomacy', surrounded by four technological spokes representing key technologies, such as AI, IoT, Blockchain, and Quantum Computing. These spokes demonstrate the direct influence and relevance of these technologies in the realm of cyber diplomacy.

The diagram uses various threads to connect the spokes and to the central hub, representing the interactions and impacts these technologies have on one another and cyber diplomacy. This effectively illustrates the complex and dynamic nature of the cybersecurity landscape.

An outer ring encircles the central hub and technological spokes, segmented into 'challenges' (such as AI-driven attacks, IoT privacy concerns, and blockchain vulnerabilities) and 'solutions' (like International Collaboration and Developing Norms). This ring highlights the ongoing issues and potential strategies within the field of cyber diplomacy.

The diagram emphasises the importance of international cooperation and the development of global norms in cyber diplomacy, which are crucial elements in addressing the challenges posed by these advanced technologies. An annotation at the bottom of the diagram highlights the article's innovative approach to integrating multiple cutting-edge technologies within the framework of cyber diplomacy and emphasises the necessity of international cooperation.

From an educational standpoint, the diagram serves as a useful tool by simplifying and visualising complex interrelations between advanced technologies and their implications in cyber diplomacy. It helps readers understand how these technologies intersect and influence global cyber governance.

By organising the information in a network diagram, the figure clarifies the complex dynamics between technologies, challenges, and solutions in cyber diplomacy. This makes it easier for readers to grasp the interdependencies.

Using a network diagram with a central hub, spokes, and an outer ring provides a visually engaging way to represent the information, making the learning experience more enjoyable and accessible.

The diagram underscores the interconnected nature of AI, IoT, Blockchain, and Quantum Computing with cyber diplomacy, highlighting the multifaceted challenges and solutions in this domain.

Overall, the Figure 10 contributes to a deeper understanding of the article's content by visually mapping out the intricate relationships between emerging technologies and their impact on cyber diplomacy.

This diagram in Figure 10 illustrates the interconnectedness of various topics discussed in the article 'Cyber Diplomacy: Defining the Opportunities for Cybersecurity and Risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing'. The central hub in the diagram highlights the paramount importance of Cyber Diplomacy. Surrounding the hub are 'technological spokes' representing AI, IoT, blockchain, and quantum computing and their specific opportunities and risks in Cyber Diplomacy.

Interlinking threads between the technologies and the central hub symbolise the flow of information and impact. An outer ring denotes the challenges and solutions related to these technologies, such as AI-driven attacks, IoT privacy concerns, blockchain vulnerabilities as challenges, and international collaboration and developing norms as solutions.

The diagram underscores the significance of international cooperation and the development of global norms in Cyber Diplomacy. Finally, the diagram features a section at the bottom that highlights the article's novelty, explaining its comprehensive approach and integration of multiple technologies in Cyber Diplomacy.

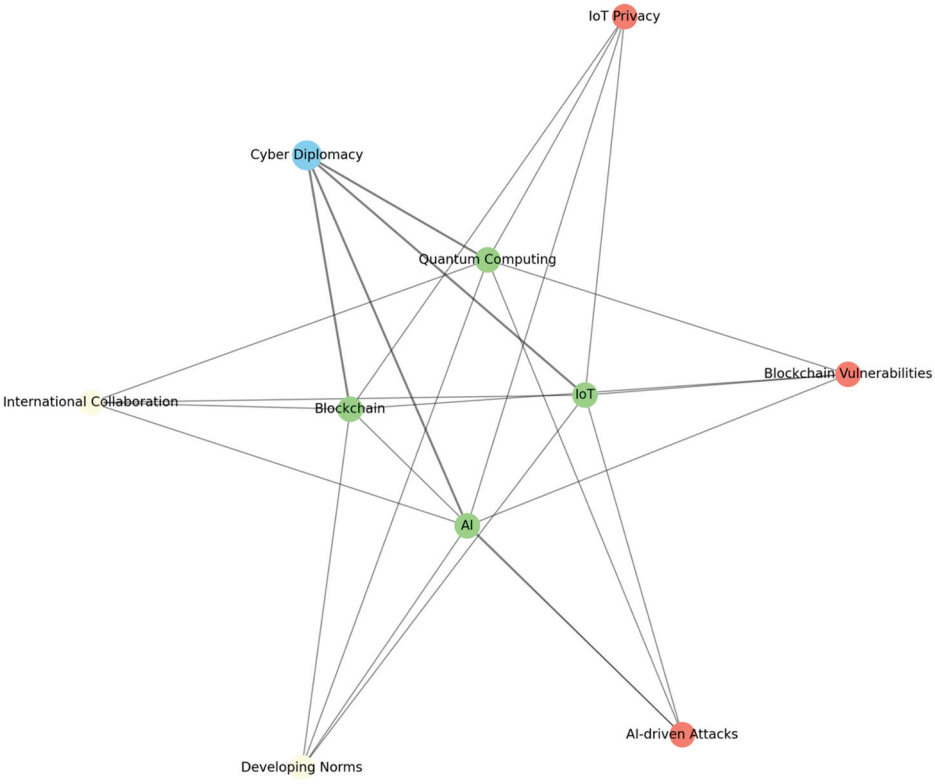

Figure 10. Integration of technologies in cyber diplomacy with emphasis on international cooperation.

10.1. Artificial intelligence and its impact on cyber diplomacy

Several future developments are anticipated to affect the landscape of cyber diplomacy as the field of cybersecurity evolves. These developments will substantially impact international cooperation, policy, and responses to growing cyber threats.

One of the anticipated future trends is the emergence of international cyber norms. The creation of internationally recognised cyber norms will gain traction. Nations will work more closely to develop common principles and standards guiding responsible state behaviour in cyberspace. This will help to standardise cybersecurity and improve predictability in cyberspace interactions.

Partnerships between the public and commercial sectors will become even more important in cyber diplomacy. Governments will work more closely with the commercial sector to exchange threat intelligence, best practices, and resources. These collaborations will use the private sector's expertise and capabilities to strengthen national and global cyber defence.

Another emerging area is the focus on artificial intelligence (AI) and automation. Incorporating AI and automation into cybersecurity will have far-reaching

consequences for cyber diplomacy. Nations must address concerns such as AI ethics, the possible threats of autonomous cyber systems, and the development of rules for the appropriate use of AI in cyber operations.

Cyber diplomacy will increasingly address digital governance, data protection, and privacy issues. Nations will try to find a balance in cyberspace regarding national security interests and the protection of individual rights.

To confront emerging cyber threats such as supply chain assaults, ransomware, and nation-state-sponsored cyber operations, cyber diplomacy will need to evolve constantly. Diplomatic efforts will be directed towards coordinating responses to new threats. Non-state actors, such as civil society organisations, academics, and commercial sector firms, will play a larger role in cyber diplomacy debates. These actors will bring various perspectives and help shape effective cyber policies.

Geopolitical tensions will continue to have an impact on cybersecurity debates. Cyber diplomacy must traverse complex political processes while promoting cooperation to handle global cyber issues. Diplomatic initiatives will use emerging technologies like blockchain and secure communication platforms to boost trust and transparency in cyber discussions and information exchange.

Regional and bilateral cybersecurity treaties will become increasingly important, allowing states to address region-specific cyber issues and encourage more personalised and cooperative cybersecurity methods. Developing countries will place more importance on cybersecurity capacity building as cyber dangers continue to cross borders. Developed countries and international organisations will spend in helping less developed countries improve their cybersecurity and resilience.

Artificial intelligence (AI) can be used to collect and analyse vast quantities of data to identify and track cyber threats, negotiate cyber security agreements, establish, and implement disarmament accords, and resolve cyber conflicts. In Table 7, we describe the effect of AI and its main impacts on cyber policy.

Overall, the potential benefits of deploying artificial intelligence in cyber diplomacy exceed its associated risks. However, being aware of the risks and taking precautions to mitigate them is critical. AI can be a great tool for diplomats to handle cyber security concerns with careful strategy and deployment.

Table 7. The impact of AI on cyber diplomacy.

Impact	Description
Threat intelligence	AI can be used to collect and analyse large amounts of data to identify and track cyber threats. This information can then be used to develop more effective strategies for preventing and responding to cyber-attacks.
Negotiation	AI can be used to help diplomats negotiate cyber security agreements. For example, AI can be used to identify areas of common ground and to develop compromise solutions.
Disarmament	AI can be used to help countries develop and implement disarmament agreements. For example, AI can be used to monitor compliance with agreements and to detect violations.
Conflict resolution	AI can be used to help countries resolve cyber conflicts. For example, AI can be used to mediate negotiations and to develop peace agreements.
Benefits	• Increased efficiency • Improved decision-making • Enhanced creativity

10.2. Preparing for the challenges of quantum computing

As this developing technology presents both substantial potential and risks to cybersecurity, cyber diplomacy is critical in preparing for the difficulties of quantum computing. The immense computing power of quantum computing can break standard encryption schemes, rendering many present cybersecurity solutions obsolete. In Figure 11, we can visualise some of the challenges presented by quantum computing. These are evaluated in more detail further in the text.

International cooperation for developing and standardising quantum-resistant encryption algorithms can be facilitated via cyber diplomacy. Nations may speed research and innovation in quantum-safe cryptography by collaborating, assuring an easy transition to post-quantum security measures. Diplomatic initiatives can help to build global cybersecurity standards, and best practices that account for the impact of quantum computing. In the quantum era, developing a consistent framework for protecting digital communications and sensitive data will be critical.

Diplomacy may foster public-private partnerships for solving quantum computing's problems. Governments, research institutions, and private-sector groups can work together to develop quantum-resistant technologies and share experience in dealing with quantum threats. Initiatives that

Figure 11. Cyber diplomacy and the challenges of quantum computing.

promote quantum research and development in cybersecurity can benefit from cyber diplomacy. Nations can collaborate to share knowledge, resources, and experience to expedite development towards quantum-solutions.

Diplomacy has the capacity to raise worldwide awareness about the risks of quantum computing to cybersecurity. Countries can work together to develop cybersecurity education and awareness programmes to keep corporations, governments, and individuals informed and prepared.

Diplomatic efforts can focus on developing countries' capacity building to guarantee that they do not fall behind in the quantum revolution. Assisting these countries in improving their cybersecurity skills will help to create a more robust global cyberspace. International policy coordination on quantum computing can be aided by cyber diplomacy. Nations can collaborate to handle quantum technology's legal, ethical, and privacy issues.

Diplomatic channels can provide systems for coordinated incident response and threat exchange in the context of quantum cyberattacks. Countering quantum threats requires rapid information exchange and reaction coordination.

Quantum computing has civilian as well as military applications. To ensure responsible and ethical use of quantum breakthroughs, diplomacy can address concerns about dual-use technology. Cyber diplomacy may ensure that quantum cybersecurity rules and governance structures are inclusive, representing the interests of all states, especially those with limited quantum capabilities.

Diplomatic efforts may ensure a secure and robust digital future in the era of quantum computing by fostering international collaboration, promoting research and development, and setting global cybersecurity standards.

10.3. Internet of things and its impact on cyber diplomacy

The Internet of Things (IoT) is a network of physical devices, automobiles, appliances, and other objects integrated with sensors, software, and connections to collect and share data over the Internet. IoT has evolved significantly in recent years and has the potential to transform a variety of businesses by offering real-time data, automation, and increased decision-making skills. The Internet of Things is rapidly increasing, with billions of gadgets now linked to the Internet. This growth has a huge impact on cyber diplomacy.

IoT devices, by definition, blur the limits of jurisdiction, making established legal frameworks difficult to apply to IoT-related cyber concerns. Cyber diplomacy is critical in facilitating negotiations among states to build cross-border legal procedures capable of dealing with cybercrime and ensuring justice is delivered.

The rapid evolution of IoT technology necessitates cross-border collaboration in research and innovation. Cyber diplomacy promotes international

collaboration among academia, the commercial sector, and governments, encouraging sharing experiences and best practices to improve IoT security and effectively confront emerging cyber threats. In Figure 12, we present the challenges triggered by IoT systems and their relationships to cyber diplomacy.

IoT devices vastly increase the attack surface for cyber threats. Bad actors will have more entry points to exploit vulnerabilities as more devices connect. International cooperation and diplomatic efforts are required to establish cybersecurity standards and procedures to secure IoT systems.

The Internet of Things operates globally, with devices and networks frequently crossing national borders. Because of this interconnection, countries must collaborate to confront transnational cyber threats and implement joint cybersecurity measures. Users' privacy is often compromised when IoT devices capture enormous amounts of personal data. Cyber diplomacy is critical in negotiating international agreements and legislation to safeguard user data and set cross-border data privacy standards.

IoT devices are manufactured all around the world, with complex supply chains. To ensure the security and integrity of these supply chains, diplomatic initiatives to build confidence and collaboration among governments are required. Many Internet of Things devices are employed in critical infrastructure

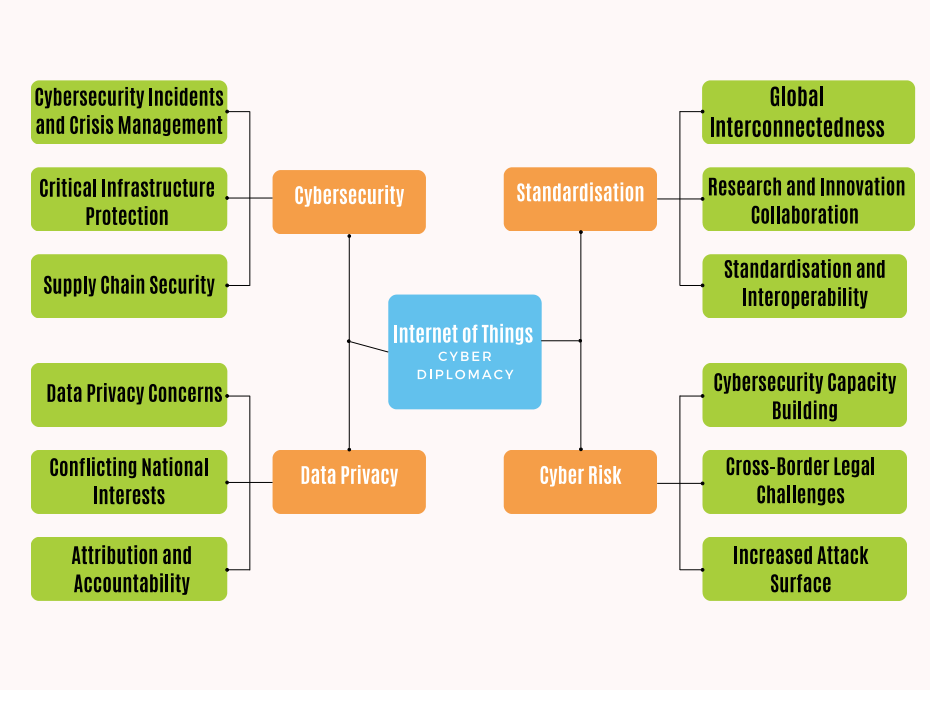

Figure 12. Impact of IoT on cyber diplomacy.

such as power grids, transportation systems, and healthcare. Protecting these important systems from cyber threats requires collaboration, including international cooperation and political measures.

The problem becomes obvious when we try to identify the source of a cyber-attack, which can often be significant. Attacks based on IoT can be routed through multiple countries, making it difficult to hold criminals accountable. Cyber diplomacy can help to encourage conversations and agreements on how to deal with attribution issues.

Various manufacturers make IoT devices and frequently employ distinct connection protocols. Global standards must be discussed and agreed upon through diplomatic channels to ensure smooth interoperability and better security. Developing countries may lack the resources and knowledge to address IoT-related cybersecurity challenges successfully. Cyber diplomacy can encourage knowledge sharing, capacity building, and technology transfer to increase global cybersecurity capabilities.

Different countries' priorities and approaches to IoT rules and standards may differ. Cyber diplomacy is becoming increasingly important in resolving disputes and finding common ground for global cybersecurity cooperation. Diplomatic channels become critical for crisis management, information exchange, and coordinated responses among impacted countries in the event of large-scale IoT-related cybersecurity disasters.

Because of the growing deployment of IoT, the cybersecurity landscape has changed, necessitating a collaborative and diplomatic approach to addressing the accompanying difficulties. International collaboration and cyber diplomacy are critical for developing global norms, standards, and regulations to ensure IoT technology's safe and responsible development and deployment.

10.4. Blockchain technology and its impact on cyber diplomacy

Blockchain technology is a distributed ledger system that allows for secure and transparent transactions without a central authority. While it is usually connected with cryptocurrencies such as Bitcoin, its application is significantly broader than digital money. Blockchain technology has numerous applications and has the potential to alter cyber diplomacy significantly.

Blockchain is extremely resistant to tampering and hacking because of its decentralised design and cryptographic procedures. As cyber threats increase, deploying blockchain in critical infrastructure and communication systems can improve cybersecurity by maintaining data integrity and lowering the danger of cyber-attacks that interrupt diplomatic communications.

Diplomatic missions frequently work with sensitive information and cross-national contact. Blockchain-based identity management systems have the potential to provide a more secure and tamper-proof method of confirming

Figure 13. Blockchain technology's transformative impact on cyber diplomacy.

identities and restricting access to classified material, lowering the risk of identity-related cyber breaches. Many documents, treaties, and agreements are exchanged between governments in cyber diplomacy. Blockchain technology can create a tamper-proof record of these papers, assuring their legitimacy and giving a trustworthy audit trail for checking their origin and integrity.

Figure 13 depicts the transformative impact of blockchain technology on cyber diplomacy. At its heart, blockchain is a decentralised and distributed ledger system that enables secure and transparent transactions without a central authority. Aside from its link with cryptocurrencies such as Bitcoin, blockchain has many uses that have important consequences for diplomatic practises. Blockchain's potential in promoting trust, transparency, and efficiency in international relations is clear, from enhanced cybersecurity through its decentralised and cryptographic nature to secure digital identity management, tamper-proof document verification, and self-executing smart contracts for diplomatic agreements.

Figure 13 also includes some less-known values from blockchain technologies, including the potential for optimising international trade and supply chain management, safe voting methods, and improving the transparency of international

relief and humanitarian initiatives. To make this potential a reality, we need more collaborative efforts in developing international norms and guidelines for responsibly using blockchain technology in cyber diplomacy.

Smart contracts are contracts that execute themselves based on established criteria and situations. These contracts have the potential to automate and enforce the implementation of diplomatic agreements and treaties, decreasing the need for intermediaries and the danger of conflicts or misunderstandings between countries. By offering real-time tracking and transparency, blockchain can help to streamline international trade and supply chain procedures. Maintaining fairness and confidence in trade practices can ease cross-border trade deals and improve diplomatic relations.

Trust is essential in international relations. The openness and immutability of blockchain can foster confidence between countries by providing a tamper-proof record of actions, assuring transparency in diplomatic engagements and agreements. Blockchain-based technologies can aid in the fight against disinformation and false news by offering a secure platform for media organisations and governments to validate the legitimacy of news sources and content.

Blockchain can be used to construct secure and transparent voting systems that defend against voter fraud and preserve the integrity of the voting process in circumstances when digital voting is necessary for diplomatic purposes. Blockchain technology can potentially improve the transparency and effectiveness of international humanitarian and relief activities. Donors may follow the cash movement via blockchain-based solutions, ensuring they reach their intended beneficiaries securely.

The potential impact of blockchain on cyber diplomacy needs international cooperation in developing standards and rules for its implementation. Cyber diplomacy can help to facilitate conversations and agreements on global interoperability and blockchain technology governance.

Blockchain technology can transform many aspects of cyber diplomacy by improving security, increasing transparency, automating processes, and building trust between governments. However, diplomatic initiatives must continue developing international standards and frameworks for their responsible and effective application in international relations.

11. Building cyber trust

11.1. Strategies for fostering trust in cyberspace

Building cyber trust among consumers, businesses, and governments is critical in today's connected world for encouraging collaboration, cooperation, and effective cybersecurity measures. Trust facilitates the exchange of sensitive cyber threat intelligence and information and is the foundation of successful cyber efforts.

Transparency in cybersecurity practises, rules and intentions fosters confidence. Organisations and governments should freely engage with stakeholders about cybersecurity measures and swiftly disclose any breaches or events. Nations must act responsibly in cyberspace by adhering to international norms and agreements. Responsible behaviour fosters international confidence and decreases the likelihood of escalation in cyber disputes.

Building cyber trust requires collaboration between the public and private sectors. Governments and corporations can collaborate to exchange threat intelligence, best practices, and resources, thereby enhancing overall cybersecurity efforts. Building confidence among nations requires engaging in cyber diplomacy and developing international cooperation. Diplomatic actions can aid in preventing cyber conflict escalation and foster coordination in the fight against global cyber threats.

Assisting less developed countries in developing their cybersecurity capabilities displays a commitment to global cyber trust. This requires planning for initiatives that enhance capacity and promote a more inclusive and secure internet.

During cyber emergencies, effective incident response and collaboration can boost trust. In this regard, coordination of reactions and timely information sharing reflects a commitment to collective defence. Adopting common cybersecurity standards and best practices promotes confidence among organisations and governments. Standardisation facilitates teamwork and assures a minimum degree of security.

Prioritising data privacy and security fosters trust among users, consumers, and citizens. Strong data security procedures reflect a commitment to protecting sensitive information. Organisations can demonstrate their commitment to security and best practices by acquiring third-party cybersecurity evaluations and certifications.

Raising public knowledge about cyber risks, safety precautions, and the significance of cybersecurity fosters trust and empowers people to protect themselves online. Showing a commitment to continuous development in cybersecurity practises and learning from previous occurrences can boost trust by demonstrating a commitment to staying ahead of new threats.

11.2. Confidence-building measures among states

National confidence-building measures are critical in decreasing tensions and boosting cooperation in cyberspace. Confidence-building measures are agreements and acts that try to increase mutual trust, transparency, and communication between different governments to avoid misunderstandings and miscalculations in cyber activities. The government can voluntarily communicate information on cybersecurity policies, plans, and threat assessments. Sharing information about cyber risks and vulnerabilities

improves situational awareness and fosters international understanding. Creating channels for reporting cyber incidents and coordinating responses fosters cooperation and aids in addressing cybersecurity concerns collaboratively.

Regular cyber talks and diplomatic channels aid in developing partnerships and a better knowledge of each other's cyber policies and objectives. Establishing direct contact channels, such as hotlines, for quick and dependable communication during cyber emergencies improves the ability to de-escalate tensions and avoid misconceptions. States can sign agreements defining areas of engagement, such as joint cybersecurity exercises, capacity-building efforts, and technical cooperation, for cybersecurity cooperation. Some governments implement no-first-use policies, promising not to employ cyber capabilities to launch offensive acts in cyberspace, promoting stability and lowering the risk of escalation.

Adherence to internationally recognised norms of responsible state behaviour in cyberspace, as defined in UN GGE reports, strengthens mutual trust and confidence. Informing other states as soon as possible about cyber events originating on one's territory displays a willingness to address cybersecurity challenges cooperatively. Establishing regional or multinational cybersecurity collaboration platforms allows for regular engagement, information sharing, and cyber coordination. By modelling real-world cyber occurrences and reactions, collaborative cyber exercises promote trust and improve collective cyber defence capabilities. Developing crisis management techniques allows authorities to manage cyber crises more effectively, reducing potential damage and escalation. The exchange of best practices in cybersecurity policy, regulation, and technology promotes collective learning and the implementation of successful cybersecurity measures.

Building trust among governments is critical for minimising cyber dangers and increasing stability in the global digital ecosystem. These methods help to a more secure and cooperative cyberspace by building trust and open communication, minimising the possibility of cyber conflicts, and promoting responsible behaviour in the digital sphere.

12. Cyber diplomacy and traditional diplomacy

The theoretical framework in this section provides a detailed exploration of the crucial concepts of cyber diplomacy and their interplay with technological fields such as AI, machine learning, cryptography, and cybersecurity. Each section is meticulously defined, blending aesthetics with informative content from experts.

When it comes to AI, the focus is on evaluating the risks and opportunities associated with implementing AI technologies. The conversation highlights the dangers of AI-directed attacks while also considering the benefits of data

analysis and proactive threat identification. There are many opportunities that AI can provide, including predictive analytics and policy decision-making.

In the case of machine learning, the emphasis is on the risks associated with data privacy and the opportunities in predictive analytics and policy decision-making. The discussion highlights the advantages of using machine learning to make policy decisions based on accurate data analysis while also acknowledging the risks associated with implementing machine learning technologies, such as data privacy.

Cryptography addresses the risks, challenges, and opportunities of secure communications, data integrity, and quantum decryption. Cryptography is an indispensable aspect of information security, and its role has become increasingly important as more sensitive information is transmitted over the internet.

Cybersecurity focuses on the risks associated with network vulnerabilities while also considering the opportunities in threat management and resilience building. The discussion emphasises the need for robust cybersecurity measures to protect against cyberattacks that could compromise sensitive information.

Cyber Diplomacy serves as a unifying theme, emphasizing global efforts in tech regulation, international cooperation, and norm development. The discussion highlights the significance of international cooperation in developing and implementing effective cybersecurity measures to protect against cyber threats.

This section provides a comprehensive exploration of the critical concepts of cyber diplomacy and their integration with technological fields such as AI, machine learning, cryptography, and cybersecurity. The discussions provide insights into the risks, challenges, and opportunities of implementing these technologies while emphasising the need for international cooperation in developing effective cybersecurity measures.

The theoretical framework in Figure 14 integrates AI, Machine Learning, Cryptography, and Cybersecurity with Cyber Diplomacy, to explain the complex interplay between emerging digital technologies and international cybersecurity policies. It highlights the dual nature of these technologies – as both a source of risks, such as AI-driven attacks and quantum decryption vulnerabilities, and a wellspring of opportunities, including advanced data analysis and secure communications. The framework underscores the critical role of Cyber Diplomacy in unifying global efforts to mitigate these risks and harness the potential benefits. Its primary contribution lies in identifying specific areas where diplomatic strategies can effectively regulate, guide, and respond to technological advancements. This approach is novel in its comprehensive encapsulation of the dynamic relationship between state-of-the-art technologies and the evolving landscape of global cyber governance. It brings new insights into how international cooperation and policy development can be strategically aligned with technological progress to enhance global cyber resilience and security.

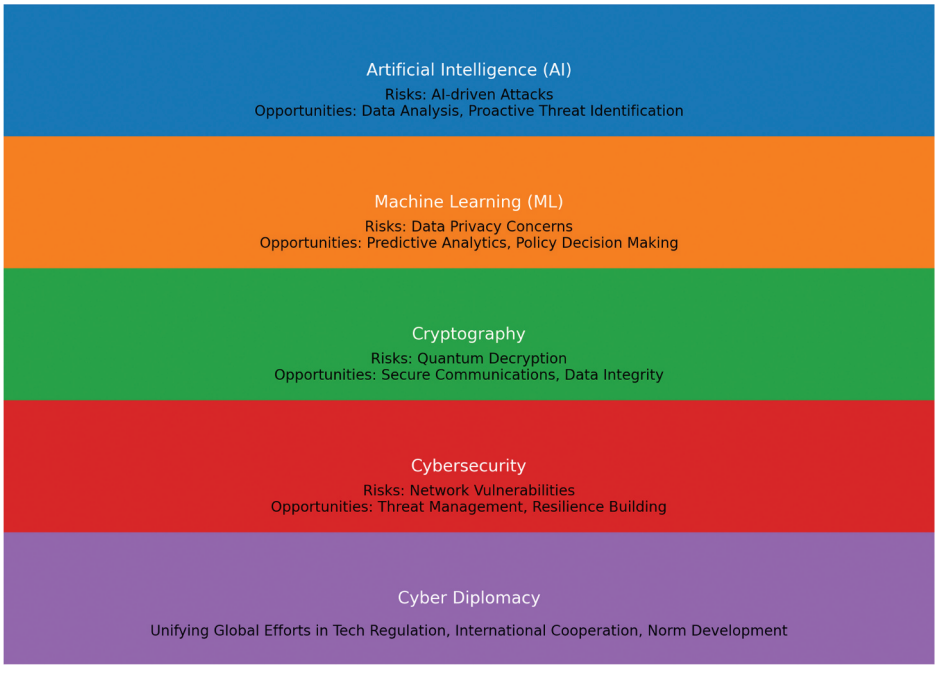

Figure 14. Theoretical framework for integrating cyber diplomacy with emerging technologies.

12.1. The interconnectedness between cyber and traditional diplomacy

Traditional diplomacy and cyber diplomacy are two complementary ways that states utilise to solve issues and challenges in the international arena. While traditional diplomacy addresses many global concerns, cyber diplomacy focuses particularly on cyberspace and cybersecurity. In Table 8, we can see a comparison of cyber diplomacy and traditional diplomacy.

Table 8. Summary table comparing cyber diplomacy and traditional diplomacy.

Aspect	Cyber Diplomacy	Traditional Diplomacy
Scope of Focus	Cyberspace, cybersecurity, internet governance	Political, economic, social, security issues
Communication Channels	Virtual meetings, secure messaging platforms, cyber channels	Face-to-face meetings, formal diplomatic communications
Focus on Technology	Central focus on cyber technologies and their impact	May involve discussions on technology-related issues
Security Concerns	Directly vulnerable to cyber threats during engagements	Susceptible to security risks, may not involve cyber threats
Multilateral and Bilateral Approaches	Multilateral and bilateral efforts in developing international norms	Common in both multilateral and bilateral approaches
Role of Diplomats	Specialised in cyber issues and cyber policy	Handle a wide range of diplomatic tasks
Time and Speed	Requires rapid response and swift actions	Negotiations and processes may take time

Both cyber diplomacy and traditional diplomacy are important components of international relations, each with a distinct focus and role in tackling global concerns and encouraging international collaboration.

12.2. Cyber-power as a new dimension of state influence

Cyber-power provides a new dimension of state influence in today's interconnected world. It refers to a country's ability to wield influence, project strength, and achieve strategic goals by utilising cyberspace and cyber capabilities. As the digital sphere becomes more important in shaping international relations, cyber-power has become important in defining a state's global standing.

Cyber-powerful states can use their technological prowess to acquire strategic advantages in various disciplines, including the military, economic, political, and social realms. This authority transcends physical borders, allowing countries to project their dominance globally. States can conduct offensive cyber operations such as cyber espionage, information warfare, and disruptive cyberattacks without resorting to traditional military force. Countries with strong cyber capabilities can also use cyber power as a deterrent, discouraging enemies from participating in hostile activities owing to the threat of cyber reprisal.

Cyber power has the potential to affect a state's economic competitiveness drastically. Advanced cyber capabilities can encourage innovation, attract foreign investment, and promote economic growth. States can use cyber-power to form global narratives, influence public opinion, and participate in cyber diplomacy to push their interests and perspectives in international affairs. States with strong cyber capabilities can better defend their key infrastructure and digital assets against cyber threats, ensuring national security and stability.

Cyber-power improves a country's intelligence-gathering capabilities by allowing for the targeted collection of sensitive information from foreign governments, entities, and individuals. Smaller governments or non-state groups can engage in asymmetrical warfare, providing substantial challenges to larger, technologically advanced foes. Demonstrating cybersecurity knowledge and encouraging good cyber behaviour boosts a country's soft power, fostering worldwide trust and collaboration.

Countries with significant cyber skills have a competitive advantage in the digital economy, resulting in increased innovation, technological developments, and digital services. Cyber-powerful nations can actively establish global cyber norms and influence the development of international cyber laws and agreements.

As technology progresses and states increasingly integrate cyberspace into their national strategies, the concept of cyber-power evolves. Building and maintaining cyber-power necessitates substantial investments in research, education, infrastructure, and the training of qualified cyber experts. Cyber-power

will play an increasingly important role in state influence and international relations as cyberspace continues to alter geopolitics.

13. Conclusion: shaping a secure digital future

Cyber diplomacy is critical in dealing with the complexity of the digital environment in international relations. It encourages responsible behaviour, safeguards cybersecurity, and assures cyberspace stability. All important components are international cooperation, conflict resolution, cybersecurity governance, confidence-building measures, attribution, public-private partnerships, capacity building, and defending digital rights and freedoms. As the internet connects the world, international collaboration in cyberspace is critical for detecting, preventing, and responding to cyber threats. Data moves across borders, prompting joint efforts to solve internet governance issues and develop data protection and privacy standards.

Nation-states, international organisations like the UN, and forums like the Internet Governance Forum all play important roles in developing cyber diplomacy. As the digital world evolves, the agility of cyber diplomacy will be critical in tackling new dangers and possibilities while encouraging trust and collaboration among governments to ensure a secure and stable digital environment.

Non-state actors are also important in cyber international relations. Private firms and corporations support cyber diplomacy by forming public-private partnerships, exchanging threat intelligence, and partnering with governments to improve cybersecurity and protect key infrastructure. Academic institutions, advocacy groups, and cybersecurity communities are all examples of civil society organisations that play an important role in cyber diplomacy. They promote awareness, share knowledge, and campaign to protect digital liberties and rights. Non-governmental organisations (NGOs) and think tanks contribute to cyber diplomacy talks through research, expert analysis, and policy suggestions, working with governments and international organisations.

Existing international cyber laws and conventions seek to address cyber problems while encouraging responsible internet behaviour. The United Nations Group of Governmental Experts (UN GGE) publications, the Budapest Convention on Cybercrime, the European Union General Data Protection Regulation (GDPR), and the International Telecommunication Union (ITU) Cybersecurity Framework are some significant examples. These agreements lay the groundwork for responsible state behaviour in cyberspace, address cybercrime, safeguard data privacy, and encourage cybersecurity best practices.

As the digital world evolves, the continued creation and refinement of international cyber laws and treaties will be critical in ensuring the global community has a secure and stable cyberspace. Effective national cyber policies,

such as those developed by the United States and the United Kingdom, focus heavily on collaboration among government, corporate sector, and civil society parties. Building trust and collaboration is critical during cyber emergencies because communication channels and mutual aid agreements promote information sharing and coordinated responses to cyber threats, ultimately enhancing the global community's collective resilience in cyberspace.

The paper focused on the important components of a comprehensive cyber strategy that can successfully address the dynamic and growing cyber threats that governments confront worldwide. Staying ahead of cyber threats in an ever-changing landscape requires conducting risk assessments and exploiting threat intelligence to uncover weaknesses. A comprehensive national cybersecurity policy and framework give the vision and goals to defend vital assets effectively. Furthermore, encouraging collaboration between the public and commercial sectors allows for information sharing, resource pooling, and coordinated operations against cyber attackers, ensuring the security of critical infrastructure sectors critical to national resilience.

Implementing a well-defined incident response strategy and cyber crisis management systems enables rapid detection, response, and recovery from cyber disasters. Capacity building and training activities are critical for equipping government employees, law enforcement, and the private sector with the skills and information to build a solid defence against cyber threats. A comprehensive legal and regulatory framework addressing cybercrime, data protection, and privacy concerns is the foundation for penalising offenders and protecting personal data.

Continuous examination, refinement, and integration of current technologies such as artificial intelligence, machine learning, and data analytics will be critical in bolstering cybersecurity and remaining adaptive in the face of emerging threats in the future. As the cyber landscape evolves, coordination and joint efforts among states will be critical in constructing a more secure and resilient digital future for the global community. Nations may work together to ensure a secure and prosperous digital environment for everybody by learning from successful cyber projects and addressing the challenges and tensions of cyber diplomacy.

Finally, the integration of artificial intelligence (AI) and the challenges offered by quantum computing will determine future trends in cyber diplomacy. International cyber norms will emerge to promote responsible state behaviour in cyberspace, encouraging collaboration and standardising cybersecurity practises. Collaborations between governments and the commercial sector will improve cyber defence capabilities by exchanging threat intelligence and resources. Incorporating AI and automation will transform cyber diplomacy, prompting the formulation of AI ethics norms and resolving concerns regarding autonomous cyber systems. Furthermore, cyber diplomacy will focus on digital governance, data protection, and privacy to find a balance between national

security concerns and individual rights. To address increasing cyber dangers, diplomatic efforts will expand to coordinate responses and include non-state actors in developing successful cyber policy. To prepare for quantum computing problems, international cooperation, standardisation of quantum-resistant encryption, and the development of cybersecurity capabilities in developing nations will be required. Through openness, responsible behaviour, and public-private partnerships, consumers, corporations, and governments can create collaboration and cooperation in cyberspace. Furthermore, confidence-building actions between governments are needed to encourage mutual trust and cooperation between nations.

13.1. Limitations

Despite its great potential, cyber diplomacy is limited in many ways, which may restrict its effectiveness. Traditional diplomatic methods are being challenged by the quick speed of technical breakthroughs and the ever-evolving nature of cyber threats. Furthermore, in the cyber arena, the issue of trust and suspicion among states can stymie genuine collaboration and information sharing. Attributing the origin of cyber-attacks complicates diplomatic operations even more, and the inclusivity of cyber diplomacy may be limited, potentially omitting vital perspectives from non-state players. Overcoming these constraints will necessitate continuous improvement in diplomatic methods, increased interstate cooperation, and the creation of strong international structures to confront cyber threats efficiently.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by the Economic and Social Research Council [ES/V003666/1].

ORCID

Petar Radanliev http://orcid.org/0000-0001-5629-6857

References

[1] Lancelot JF. Cyber-diplomacy: cyberwarfare and the rules of engagement. J Cyber Secur. 2020 Oct;4(4):240–254. doi: 10.1080/23742917.2020.1798155

[2] Yadav S. Social automation and APT attributions in national cybersecurity. J Cyber Secur. 2024 Jan;1–26. doi: 10.1080/23742917.2023.2300494

[3] Bommasani R, Klyman K, Zhang D, Liang P. Stanford Center for Research on Foundation Models. Stanford Center for Research on Foundation Models; 2023. https://crfm.stanford.edu/2023/06/15/eu-ai-act.html.
[4] Suhag A, Daniel DA. Study of statistical techniques and artificial intelligence methods in distributed denial of service (DDOS) assault and defense. J Cyber Secur. 2023 Jan;7 (1):21–51. doi: 10.1080/23742917.2022.2135856
[5] US Department of State. Bureau of cyberspace and digital policy - United States Department of State. [cited 2023 Jul 24]. [Online]. Available: https://www.state.gov/bureaus-offices/deputy-secretary-of-state/bureau-of-cyberspace-and-digital-policy/.
[6] United Nations. The UN norms of responsible state behaviour in cyberspace | Australian strategic policy institute | ASPI. 2022 [cited 2023 Jul 24]. [Online]. Available: https://www.aspi.org.au/report/un-norms-responsible-state-behaviour-cyberspace
[7] United Nations. Group of governmental experts on developments in the field of information and telecommunications in the context of international security: note/: by the secretary-general. UN; 2015 Jul. [cited 2023 Jul. 24. [Online]. Available: https://digitallibrary.un.org/record/799853
[8] CCDCOE. The Tallinn Manual. 2013 [cited 2023 Jul 24]. [Online]. Available: https://ccdcoe.org/research/tallinn-manual/
[9] Council of Europe. Budapest Convention - Cybercrime. 2001 [cited 2023 Jul 25]. [Online]. Available: https://www.coe.int/en/web/cybercrime/the-budapest-convention
[10] United Nations. United Nations convention on the law of the sea. [cited 2023 Jul 24]. [Online]. Available: https://www.imo.org/en/ourwork/legal/pages/unitednationsconventiononthelawofthesea.aspx.
[11] JCPOA. What is the Iran nuclear deal? | council on foreign relations. [cited 2023 Jul 24]. [Online]. Available: https://www.cfr.org/backgrounder/what-iran-nuclear-deal.
[12] GDPR. What is GDPR, the EU's new data protection law? - GDPR.Eu. [cited 2023 Jul 7]. [Online]. Available: https://gdpr.eu/what-is-gdpr/
[13] ICO. Information Commissioner's Office (ICO): the UK GDPR," UK GDPR guidance and resources. [cited 2023 Jul 8]. [Online]. Available: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/consent/
[14] NTI. Wassenaar Arrangement. [cited Jul 2023 24]. [Online]. Available: https://www.nti.org/education-center/treaties-and-regimes/wassenaar-arrangement/.
[15] OAS. Organization of American States: cybersecurity program. Aug. 2009.
[16] African Union. African Union convention on cyber security and personal data protection | African union. [cited 2023 Jul 24]. [Online]. Available: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.
[17] United Nations. United Nations convention against transnational organized crime. [cited 2023 Jul 24]. [Online]. Available: https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html.
[18] United Nations. Convention on the rights of the child | OHCHR. [cited 2023 Jul 24]. [Online]. Available: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child.
[19] United Nations. Optional protocol to the convention on the rights of the child on the sale of children, child prostitution and child pornography | OHCHR. [cited 2023 Jul 24]. [Online]. Available: https://www.ohchr.org/en/instruments-mechanisms/instruments/optional-protocol-convention-rights-child-sale-children-child.
[20] ISO. ISO/IEC 27035-1: 2016 - information technology — security techniques — information security incident management — part 1: principles of incident management. [cited 2023 Jul 24]. [Online]. Available: https://www.iso.org/standard/60803.html.

[21] NIST. SP 800-61 Rev. 2, Computer Security Incident Handling Guide | CSRC. [cited 2023 Jul 24]. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/61/r2/final.
[22] ENISA. Good Practice Guide for Incident Management — ENISA. [cited 2023 Jul 24]. [Online]. Available: https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management.
[23] FIRST. Standards. [cited 2023 Jul 24]. [Online]. Available: https://www.first.org/standards/
[24] OASIS. OASIS cyber threat intelligence (CTI) TC | OASIS. [cited 2023 Jul 24]. [Online]. Available: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti.
[25] CIS. CIS Critical Security Controls. [cited 2023 Jul 24]. [Online]. Available: https://www.cisecurity.org/controls.
[26] West-Brown MJ, Stikvoort D, Kossakowski K-P, Killcrece G, Ruefle R, Zajicek M. Handbook for computer security incident response teams (CSIRTs). Carnegie Mellon University, Software Engineering Institute; 2003.
[27] Cichonski P, Millar T, Grance T, et al. Computer security incident handling guide recommendations of the national institute of standards and technology. doi: 10.6028/NIST.SP.800-61r2.
[28] ITU-T X.1500 Series. X.1500: overview of cybersecurity information exchange. [cited 2023 Jul 24]. [Online]. Available: https://www.itu.int/rec/T-REC-X.1500.
[29] ICANN. ICANN Computer Incident Response Team - ICANN. [cited 2023 Jul 24]. [Online]. Available: https://www.icann.org/resources/pages/cirt-2012-02-25-en.
[30] The White House. National cybersecurity strategy. 2023.
[31] Cabinet Office. National cyber strategy 2022 - GOV.UK. 2022. [cited 2023 Jul. 23. [Online]. Available: https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022
[32] NTIA. SBOM at a Glance. NTIA Multistakeholder Process On Software Component Transparency | Ntia.Gov/Sbom. [cited 2023 Jan 2]. [Online]. Available: https://tiny.cc/SPDX
[33] Meyers JS. Are SBOMs any good? Preliminary measurement of the quality of open source project SBOMs. Chainguard. [cited 2023 Jan 2]. [Online]. Available: https://www.chainguard.dev/unchained/are-sboms-any-good-preliminary-measurement-of-the-quality-of-open-source-project-sboms
[34] M. P. on S. C. T.-S. and F. W. G. NTIA. Survey of existing SBOM formats and standards-version 2021 survey of existing SBOM formats and standards credit: photo by Patrick Tomasso on unsplash NTIA multistakeholder process on software component transparency standards and formats working group. 2021. [cited 2023 Dec 24. [Online]. Available: https://www.ntia.gov/files/ntia/publications/sbom_formats_survey-version-2021.pdf
[35] Biden J. Executive order on improving the Nation's cybersecurity | the White House. The White House. [cited 2023 Jan 2]. [Online]. Available: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[36] EU Commission. Proposal for directive on measures for high common level of cybersecurity across the Union | Shaping Europe's digital future. 2020. [cited 2023 Jul 23]. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union
[37] ENISA. Cybersecurity of AI and standardisation — ENISA. [cited 2023 Apr 5]. [Online]. Available: https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation