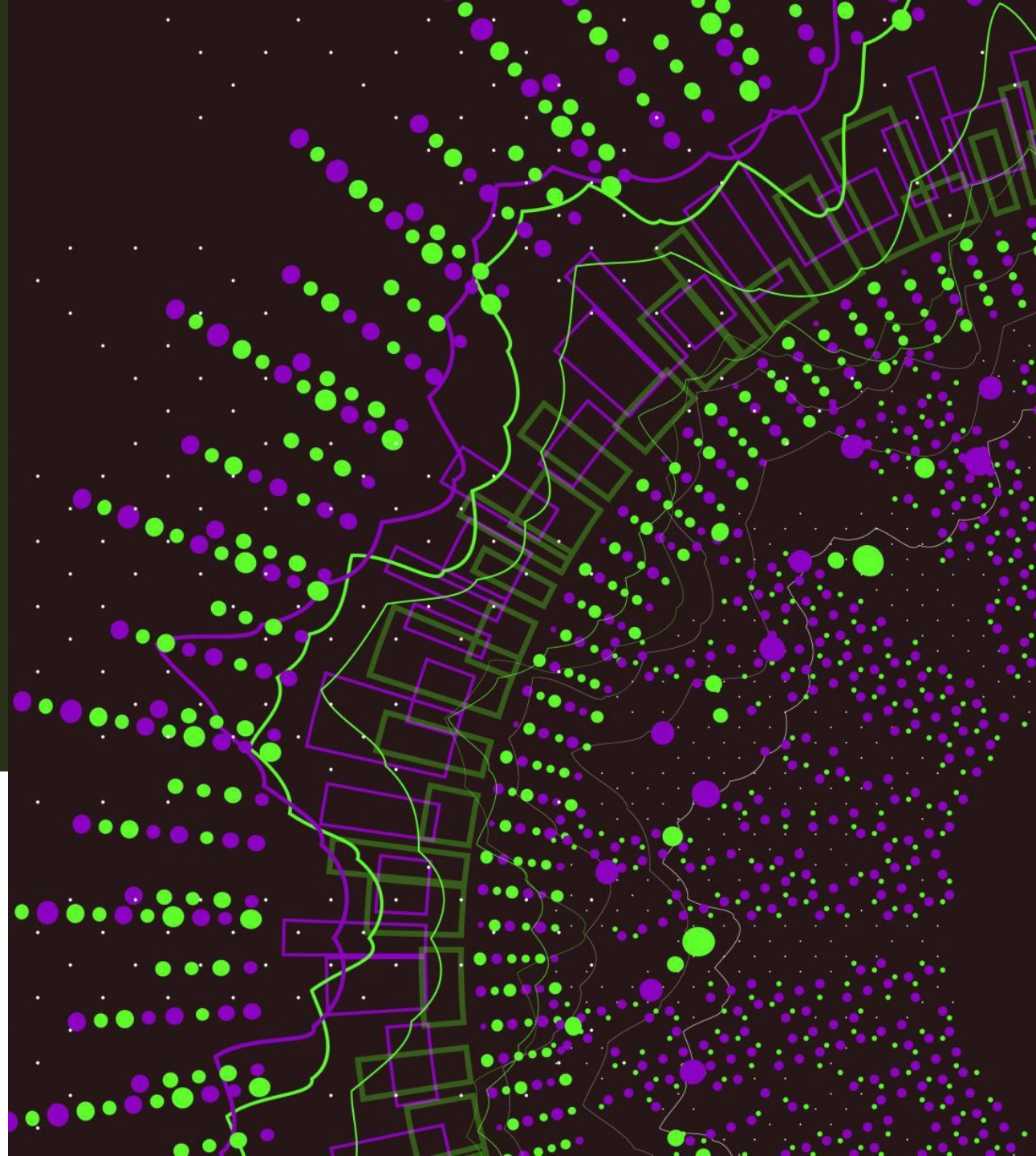
Cyber Diplomacy

Dr Petar Radanliev
University of Oxford

The final version of this work is published as:

Petar Radanliev (2024) Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing, Journal of Cyber Security Technology, DOI: 10.1080/23742917.2024.2312671

Cyber Diplomacy: Defining the Opportunities for Cybersecurity and Risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing



Abstract: Cyber diplomacy is critical in dealing with evolving cybersecurity dangers and possibilities in the digital era

Keywords: Cyber diplomacy, Cybersecurity, Cyber risk, Internet of Things , Quantum Computing, Artificial Intelligence , Blockchain technologies

Introduction to Cyber Diplomacy

What is Cyber Diplomacy?

Cyber Diplomacy is a term used to describe the application of diplomatic techniques and negotiations in the context of international relations that deal with and to regulate issues related to cyberspace

Cyber Diplomacy is usually applied for managing the difficulties and obstacles presented by the cyber world and aims to promote responsible actions, preserve cybersecurity, and ensure stability in cyberspace

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

What is Cyber Diplomacy?

Cyber Diplomacy is a form of conflict resolution strategy that attempts to prevent conflicts in cyberspace from developing into bigger geopolitical problems

Cyber Diplomacy aims to address the problem of attribution, though building mechanisms that would make people accountable for hostile cyber operations

Concepts related to Cyber Diplomacy

Cyber Diplomacy is strongly related to Cybersecurity, but the two functions are fundamentally different

Cybersecurity is the activity of preventing unauthorised access, computer hacking, and information theft on computer systems, networks, and databases

While cybersecurity focuses on the technical and operational aspects of securing digital systems, cyber diplomacy deals with the diplomatic implications of managing cyber threats

Digital diplomacy, often referred to as e-Diplomacy or Diplomacy 2.0, is the practise of using social media, online platforms, and digital technology by governments and diplomats to interact with international audiences, promote communication, and carry out diplomatic outreach

Concepts related to Cyber Diplomacy

Digital diplomacy is a broader notion that includes the use of technology for diplomatic goals, whereas cyber diplomacy concentrates on cyberspace issues and security

Understanding the digital realm's impact on international relations

The widespread use of the internet and the quick development of technology have radically altered the way nations connect and carry out diplomacy

The importance of the online environment in influencing international relations has been demonstrated by several important factors , and Digital Diplomacy is just one of these factors

Digital technologies, social media, and online platforms are being used by governments and diplomats to interact with international audiences, share information, and carry out diplomatic outreach

Cyber diplomacy focuses on managing and negotiating cyber-related concerns in international relations

Understanding the digital realm's impact on international relations

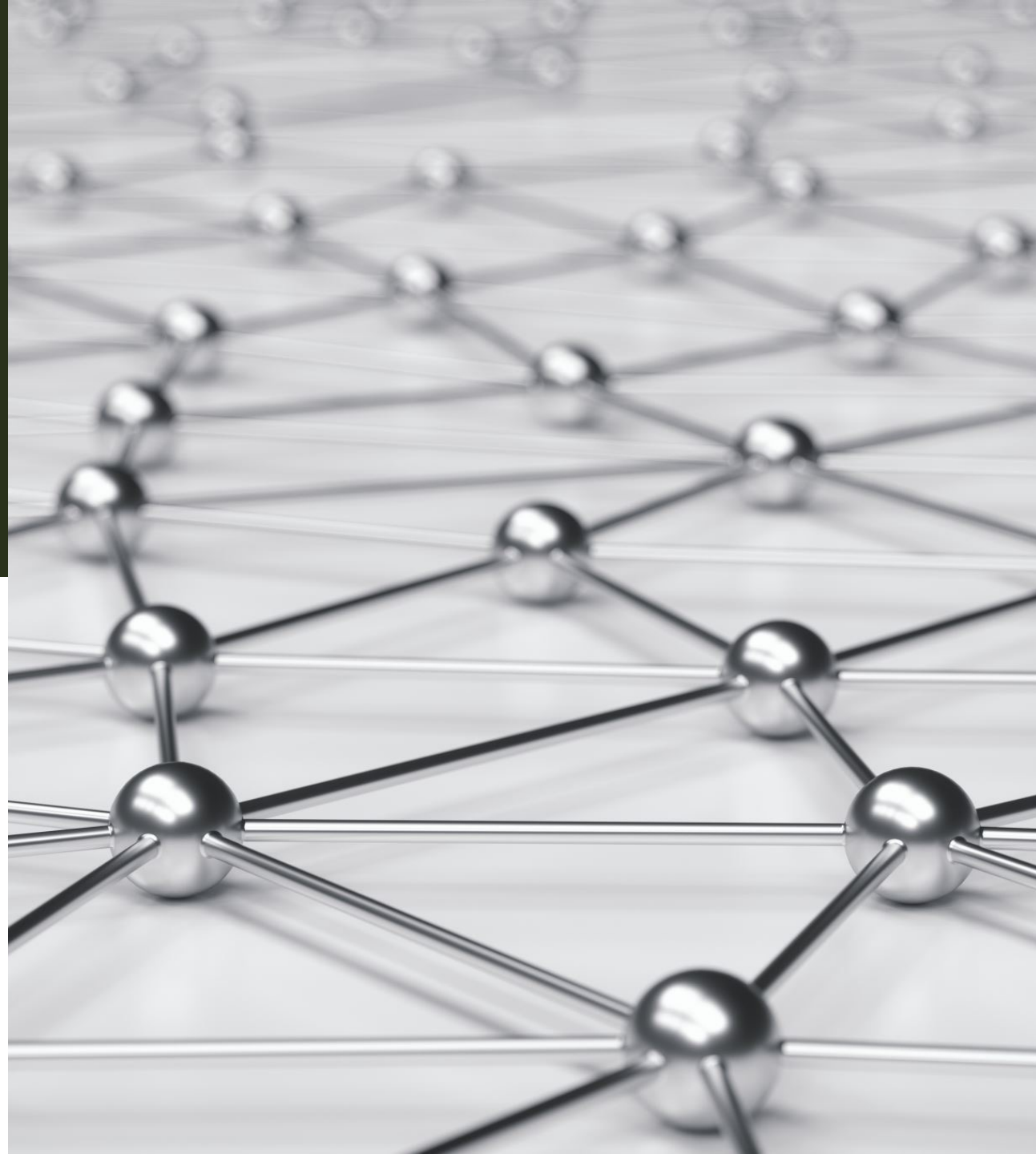
Information warfare has increased because of the advances in digital technologies, in which states and non-state actors utilise information and disinformation campaigns to impact public opinion and political outcomes in other nations

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 need to work together to handle the specific challenges that it brings

International collaboration allows for the exchange of best practises, information, and experience in the enhancement of cyber resilience

International cooperation is critical in developing policies addressing challenges related to internet governance, such as domain name systems, internet protocol allocations, and net neutrality



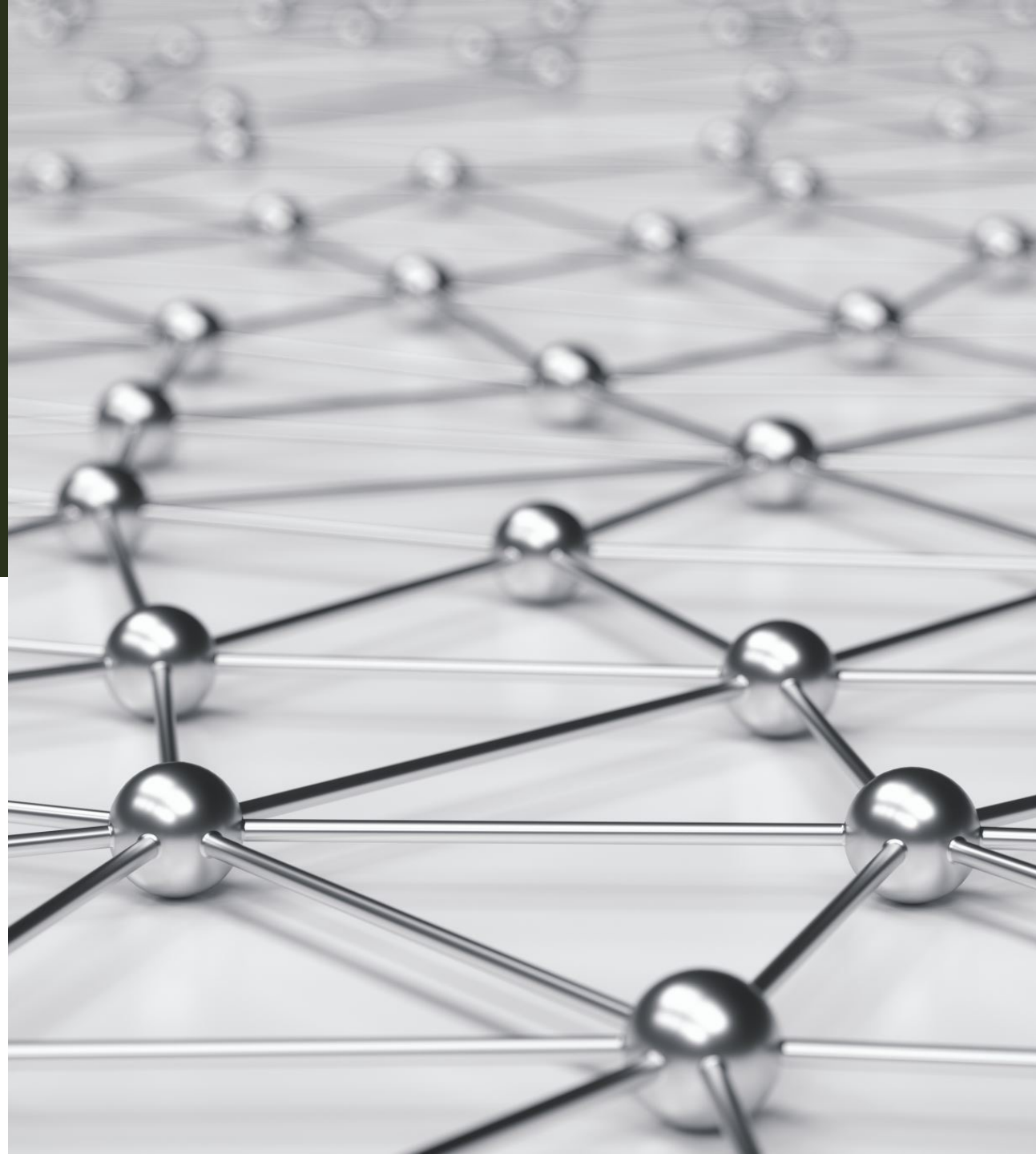
International Laws and Norms in Cyberspace

Cyber Diplomacy Actors: States and their roles 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 engage in cyber discussions with other countries

Cyber Diplomacy is facilitated by organisations such as the United Nations , the European Union , and the International Telecommunication Union



Cyber Diplomacy Actors: Non-state actors' influence on cyber international relations

They contribute to cyber diplomacy through 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

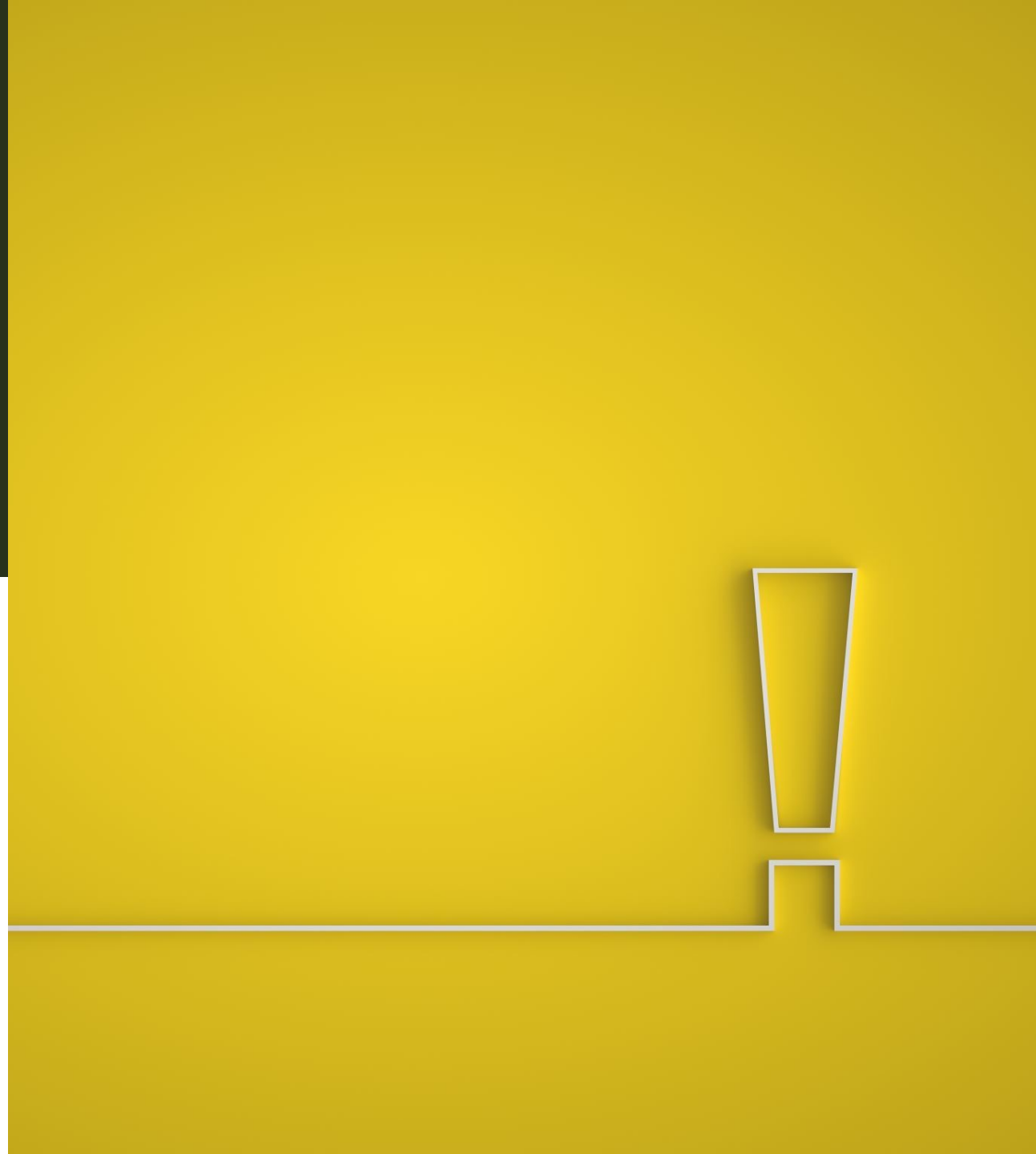
Non-governmental organisations and think tanks contribute to cyber diplomacy by conducting research, giving expert analysis, and advocating for safe cyber practises

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



Cyber Crisis Management and Response

Strategies for handling cyber incidents and crises

The United Nations Office on Drugs and Crime : addressing cybercrime

The United Nations Interregional Crime and Justice Research Institute : addressing cybercrime

The Council of Europe Convention on Cybercrime : international treaty on cybercrime

Organisation for Economic Co-operation and Development : Guidelines for the Security of Information Systems and Networks

International Telecommunication Union : the ITU Cybersecurity Framework

Building trust and cooperation during cyber emergencies

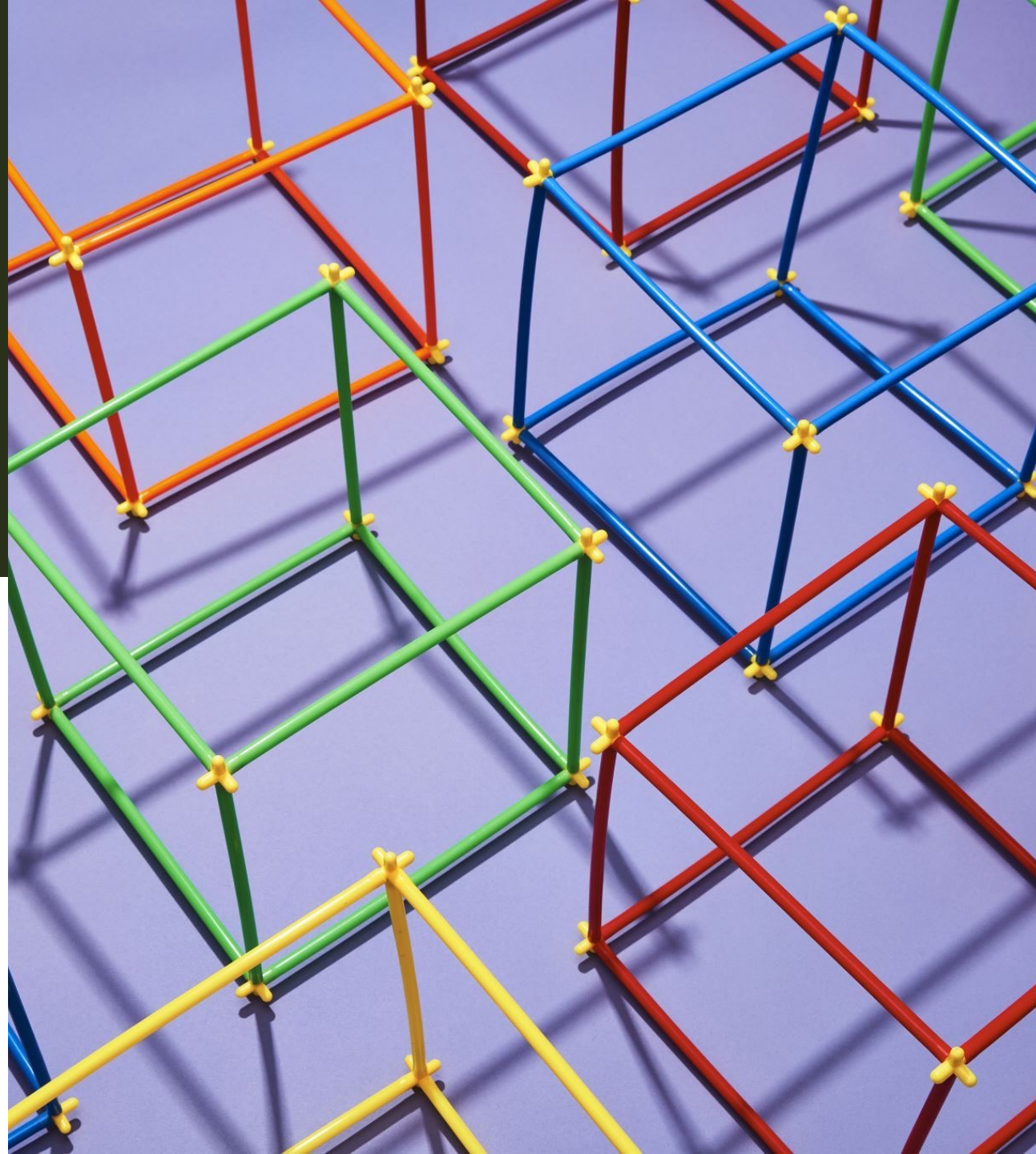
During cyber emergencies, trust and cooperation are critical for successful incident response and limiting the effects of cyber threats

Individual data breaches to large-scale cyberattacks on critical infrastructure can all result in cyber emergencies of varying scope and complexity

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

Communication must be clear and fast to share threat intelligence, incident updates, and coordinate response actions

Communication channels need to include information sharing and collaboration between national and international private and public sectors



Building trust and cooperation during cyber emergencies

Incident response mechanisms need to encourage openness in incident reporting and response efforts, while holding individuals responsible for malicious cyber activity accountable

National Cyber Strategies

Development and implementation of effective national cyber policies

National Cyber Strategies

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

National Cyber Strategies

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

National Cyber Strategies

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 to achieve cybersecurity goals

Focus on the importance of international cooperation in addressing cyber threats

Commitment to working with other countries to share information, investigate cybercrimes

Key components of a comprehensive cyber strategy

A comprehensive cyber strategy includes several key elements that work collectively to effectively confront dynamic and emerging cyber threats

Comprehensive cyber strategy also requires capacity building and training initiatives provide government employees, law enforcement, and the commercial sector with the information and skills needed to tackle cyber threats

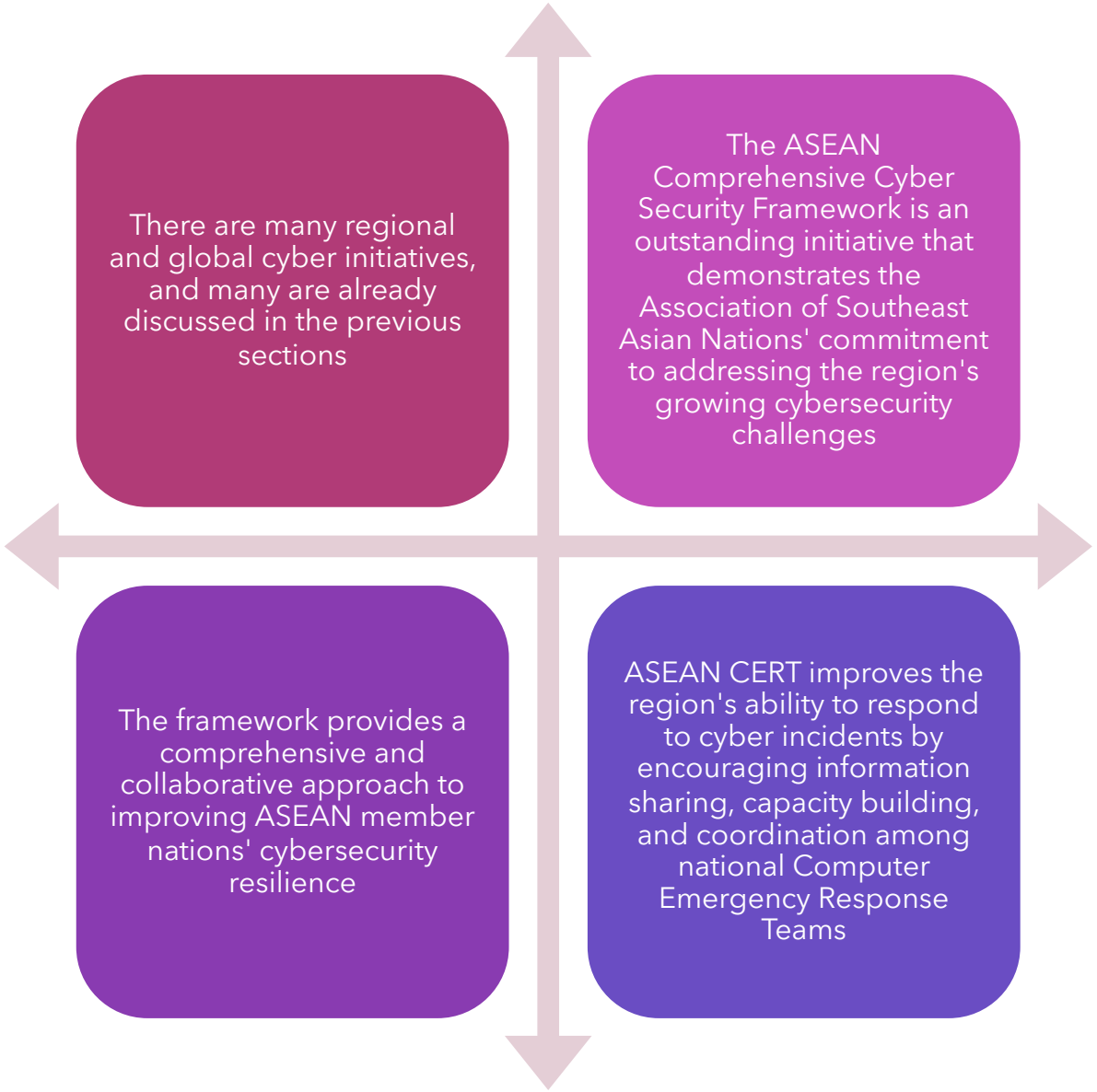
Comprehensive cyber strategy is grounded on a comprehensive legal and regulatory framework that addresses cybercrime, data protection, and privacy concerns, establishing a legal foundation for punishing cyber offenders and protecting personal data

Key components of a comprehensive cyber strategy

The elements are also compared and related to the U.S

Regional and Global Cyber Initiatives

Collaborative efforts to address cyber threats at regional and global levels



Collaborative efforts to address cyber threats at regional and global levels

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

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 , is a critical component of the EU's cybersecurity infrastructure

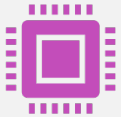
Collaborative efforts to address cyber threats at regional and global levels

ENISA, as the designated agency for network and information security, plays a critical role in assisting both the European Commission and Member States in addressing various cyber security concerns

ENISA's resolute commitment to developing cybersecurity resilience and collaboration makes it a vital tool in protecting Europe's digital infrastructure and data from ever-changing cyber threats

Case studies of successful cyber initiatives

The Multi-State Information Sharing and Analysis Centre is the first case study

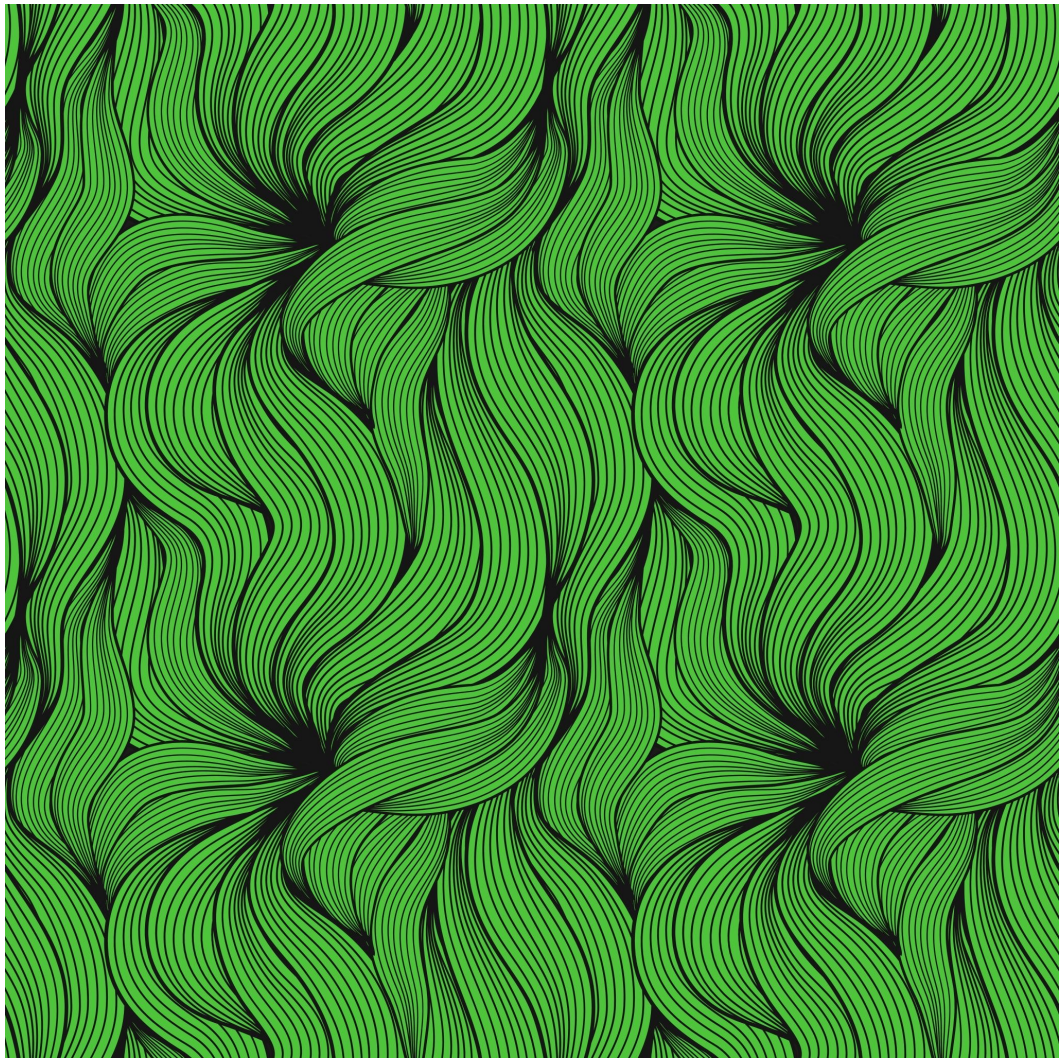


The Multi-State Information Sharing and Analysis Centre is a successful cyber initiative in the United States that focuses on improving cybersecurity resilience across state, local, tribal, and territorial administrations

MS-ISAC, which was founded in 2003, serves as a central centre for its members to share essential cybersecurity information, threat intelligence, and best practises

Cyber Green is a successful global initiative that addresses the growing concern about the sustainability of cyberspace

Public-Private Partnerships in Cyber Diplomacy



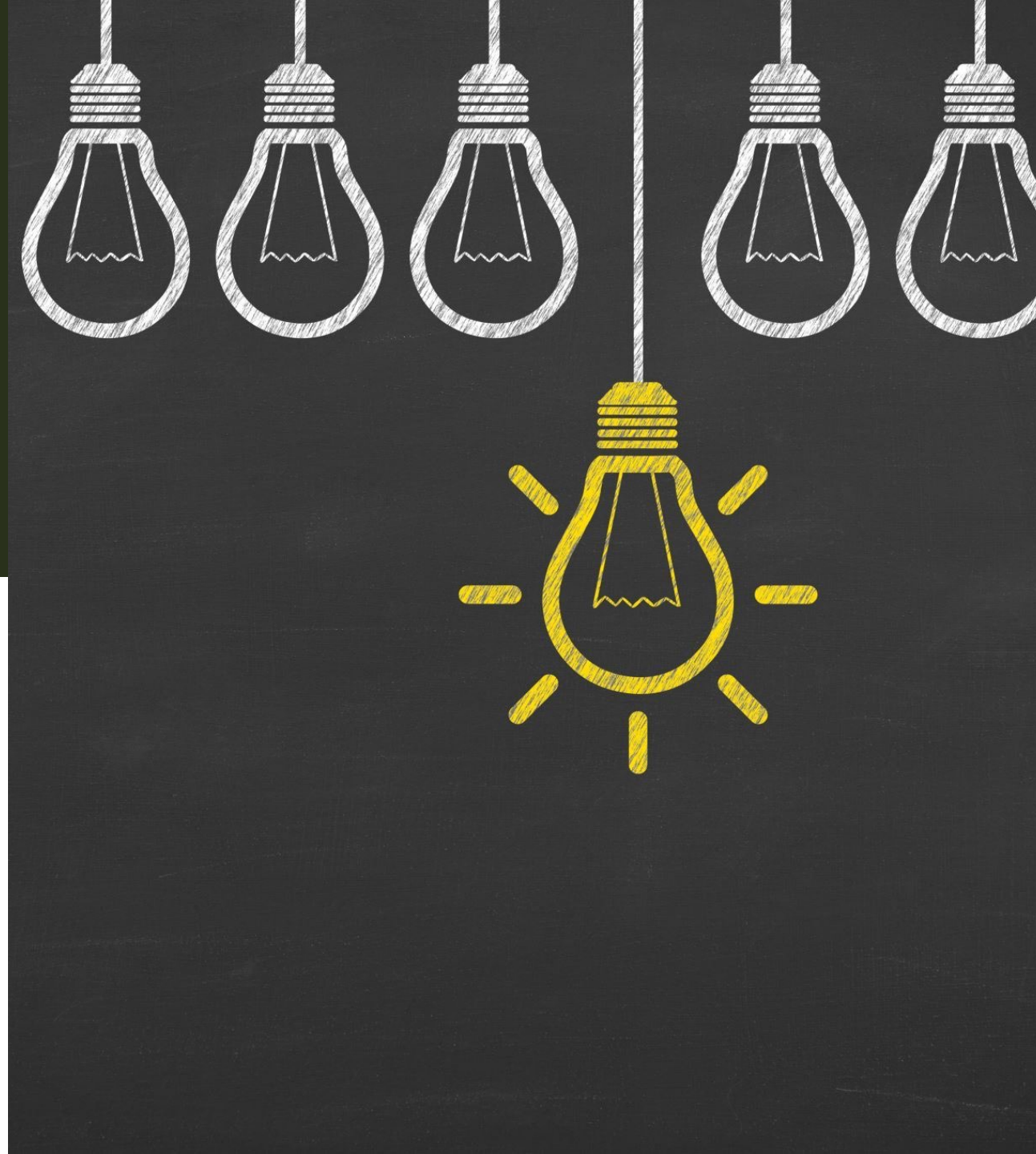
The role of private sector entities in cyber diplomacy

Private sector organisations play an important role in cyber diplomacy, helping to shape international cybersecurity policies and practises

Private sector organisations frequently have significant threat intelligence and data on cyber occurrences that they can share with governments and international organisations

The private sector actively contributes to the creation of cybersecurity standards and best practises

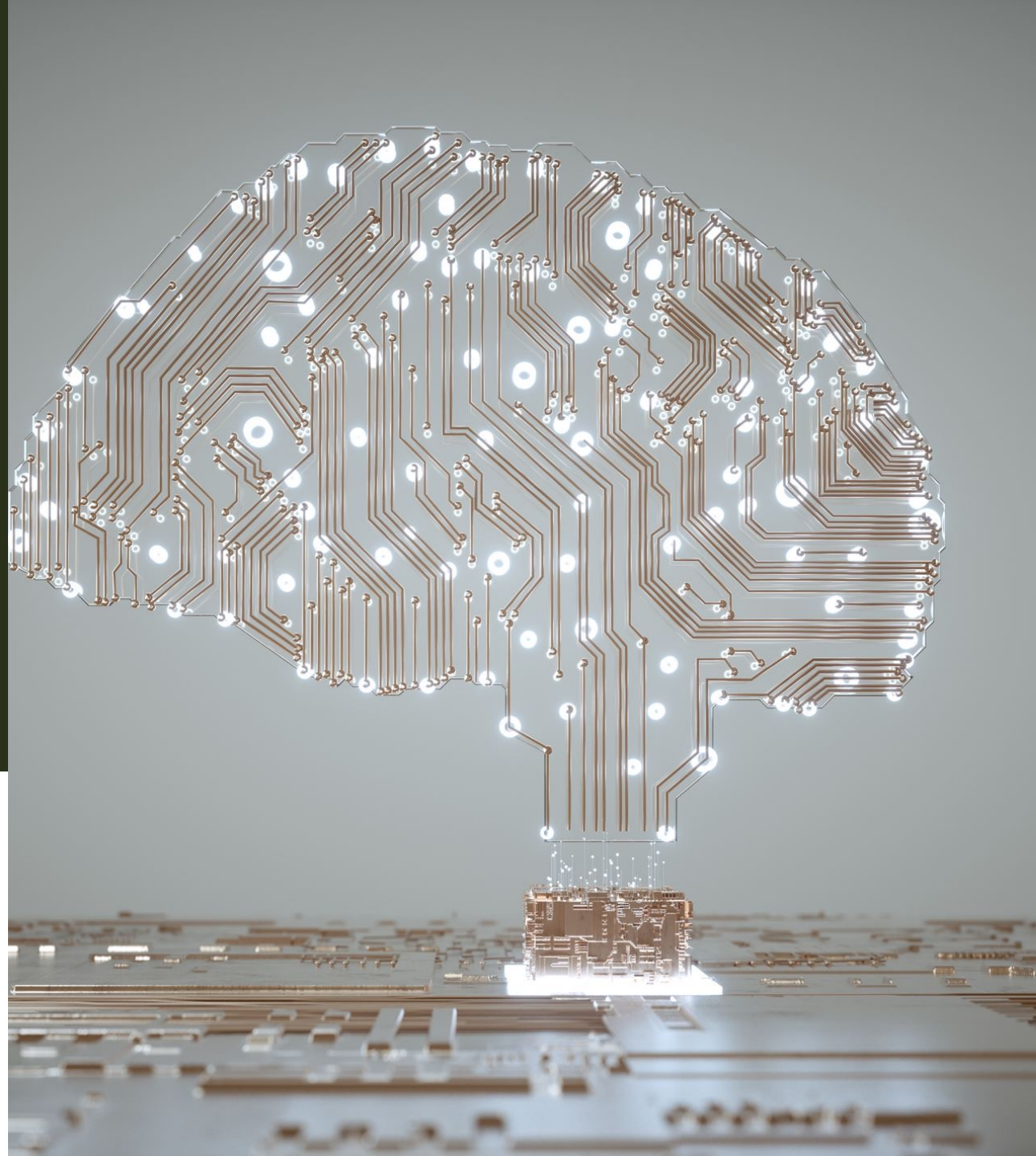
Private-sector firms drive cybersecurity technology innovation, developing new tools and solutions to combat increasing cyber threats



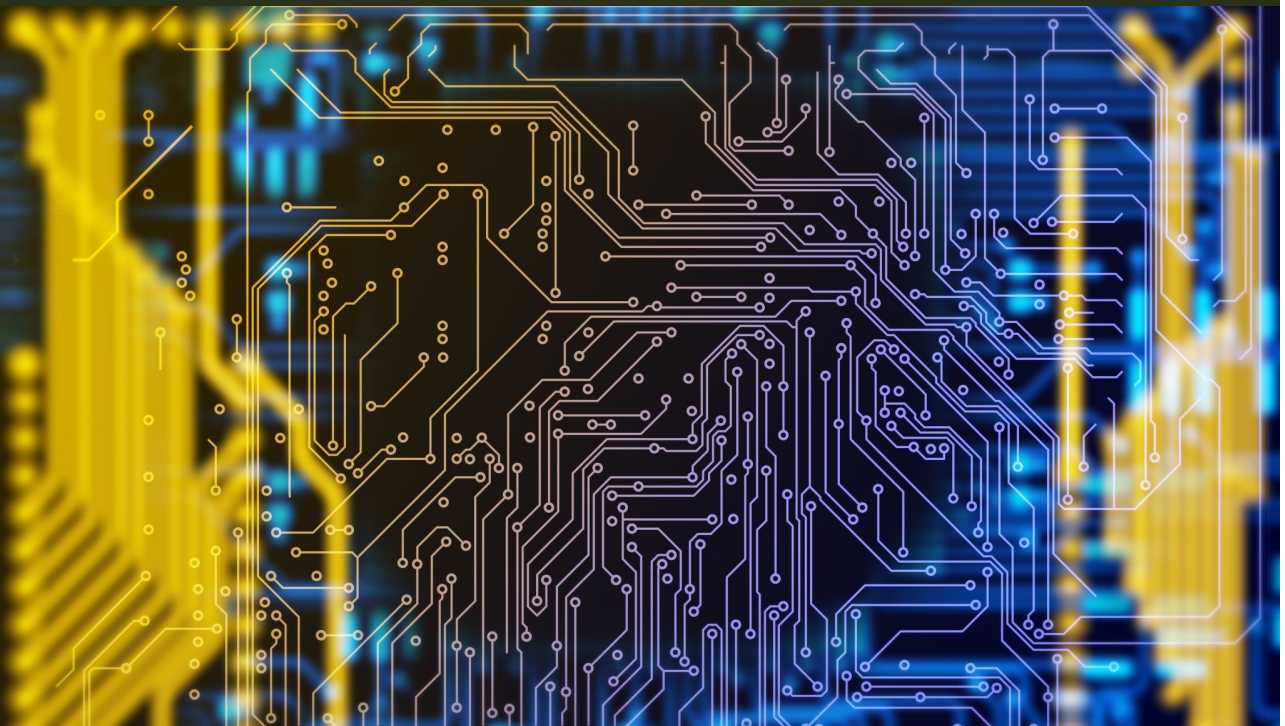
The role of private sector entities in cyber diplomacy

Their partnership with governments and international organisations is critical to improving global cyber resilience, establishing trust, and protecting the digital world for both public and commercial interests

Cyber Intelligence Sharing



Challenges and benefits of sharing cyber threat intelligence



One of the main benefits of cyber intelligence sharing is the access to shared threat intelligence

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

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 effectively tackle cyber threats

Challenges and benefits of sharing cyber threat intelligence

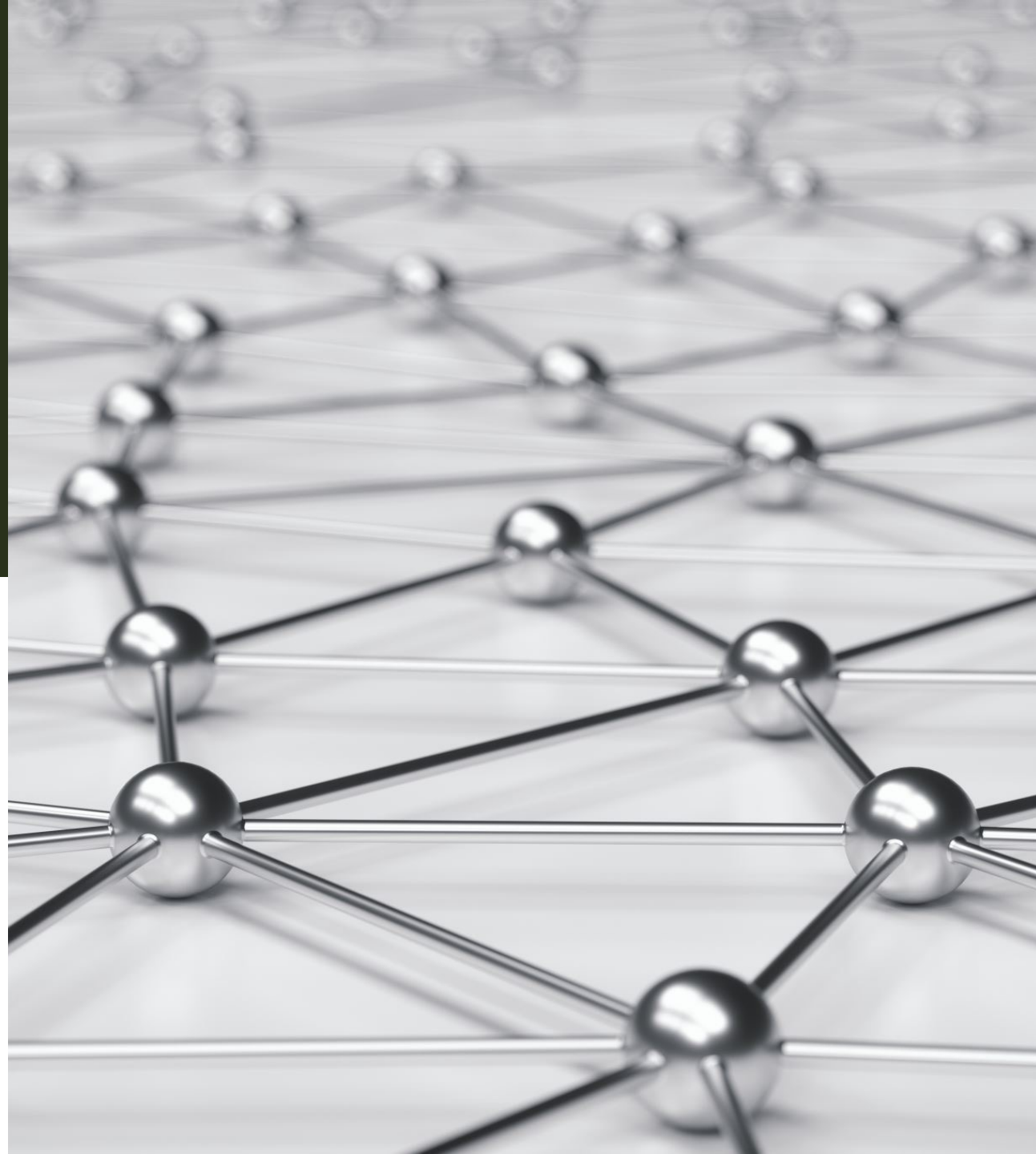
Cyber threat intelligence frequently originates in a variety of formats and patterns, making it challenging to consolidate and analyse data across several organisations efficiently

International efforts to promote intelligence cooperation

CISCP is a United States government effort that promotes information sharing between federal agencies and private-sector organisations in order to improve cybersecurity

One ongoing academic effort is the Global Cyber Security Capacity Centre at the University of Oxford

GCSCC is a cybersecurity capacity-building centre, advocating an increase in the global scale, pace, quality, and impact of cybersecurity capacity-building activities



Cyber Diplomacy Challenges and Roadblocks

Attribution issues in cyberspace

Cyber diplomacy is confronted with several challenges and barriers capable of impede successful international collaboration and the development of a secure and stable cyberspace

Cyber diplomacy is a difficult and challenging field due to the a number of factors

One factor is the international character of cyber threats

Given that cyber-attacks can originate anywhere in the globe, it is difficult to trace down and prosecute hackers

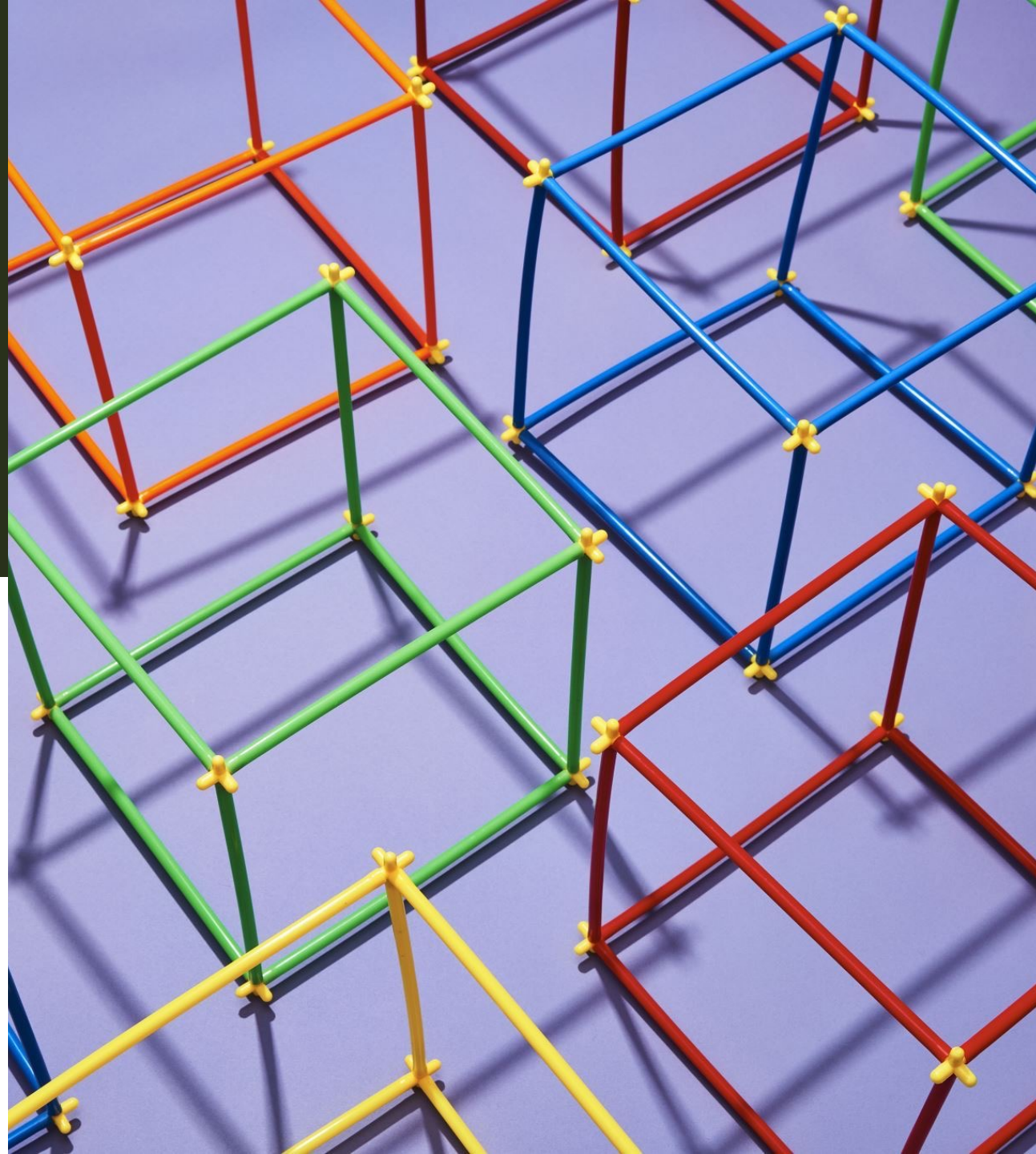
Second factor is lack of a unified international agreement that defines what constitutes a cyber-attack or how to respond to one

Cyber-attacks can be used to achieve political objectives such as disrupting elections or inciting discontent in a society

Attribution issues in cyberspace

Balancing national security concerns with global cooperation can be difficult, resulting in various approaches to cyber diplomacy

The international legal framework for cyber operations is continually changing, and gaps and inconsistencies exist in how existing rules apply to cyberspace



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

IN FIGURE 8, WE SUMMARISE STRATEGIES AND APPROACHES FOR OVERCOMING GEOPOLITICAL TENSIONS IN CYBER NEGOTIATIONS

AS OUTLINED IN FIGURE 8, 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

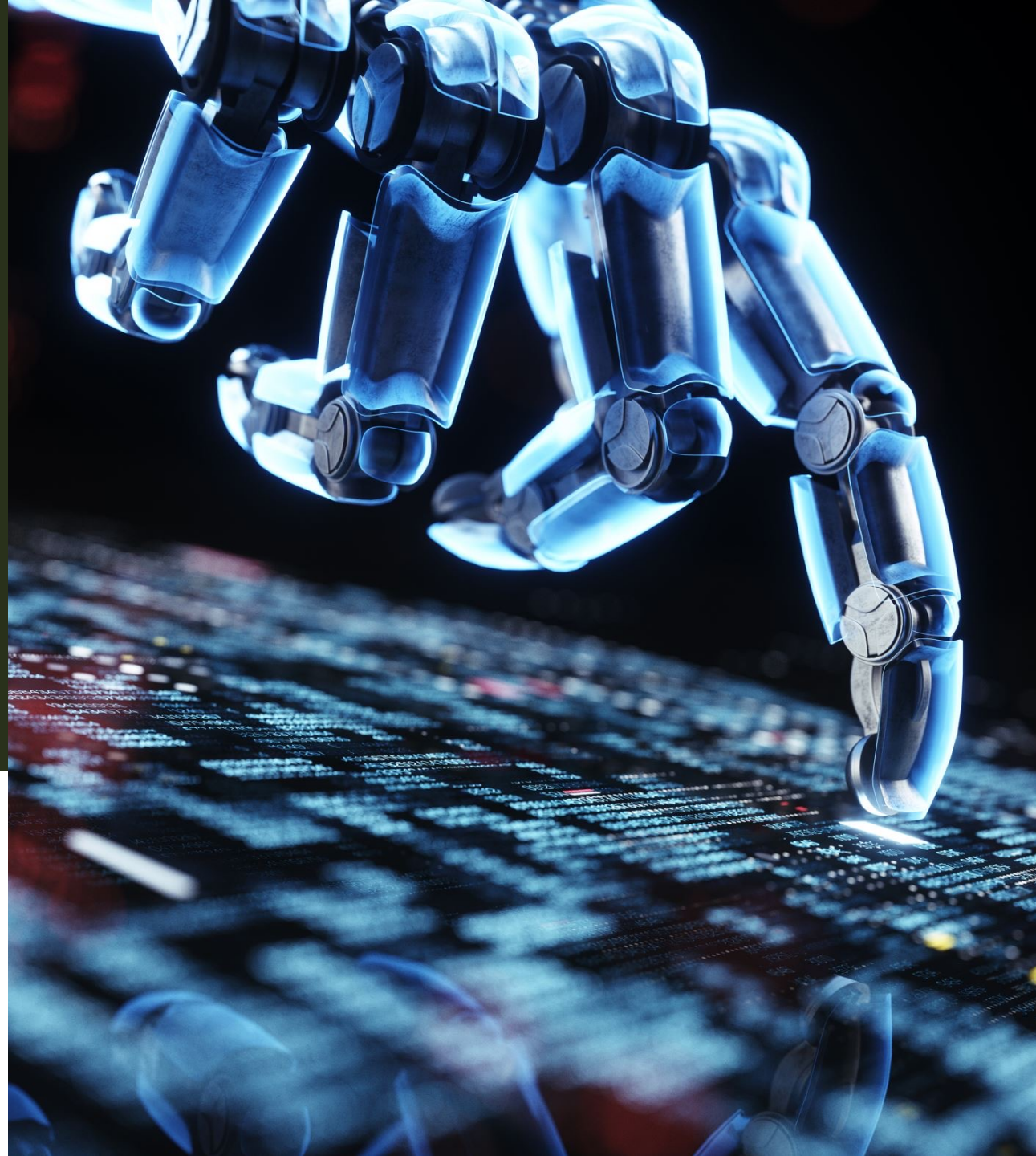
CREATING AVENUES FOR REGULAR COMMUNICATION AND DISCUSSION CAN HELP NATIONS CREATE TRUST AND UNDERSTANDING

Overcoming geopolitical tensions in cyber negotiations

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

Nations can collaborate to develop rules that improve cybersecurity while discouraging malevolent behaviour

Future Trends in Cyber Diplomacy



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 have a substantial impact on international cooperation, policy, and responses to growing cyber threats

One of the anticipated future trends is the emergence of international cyber norms

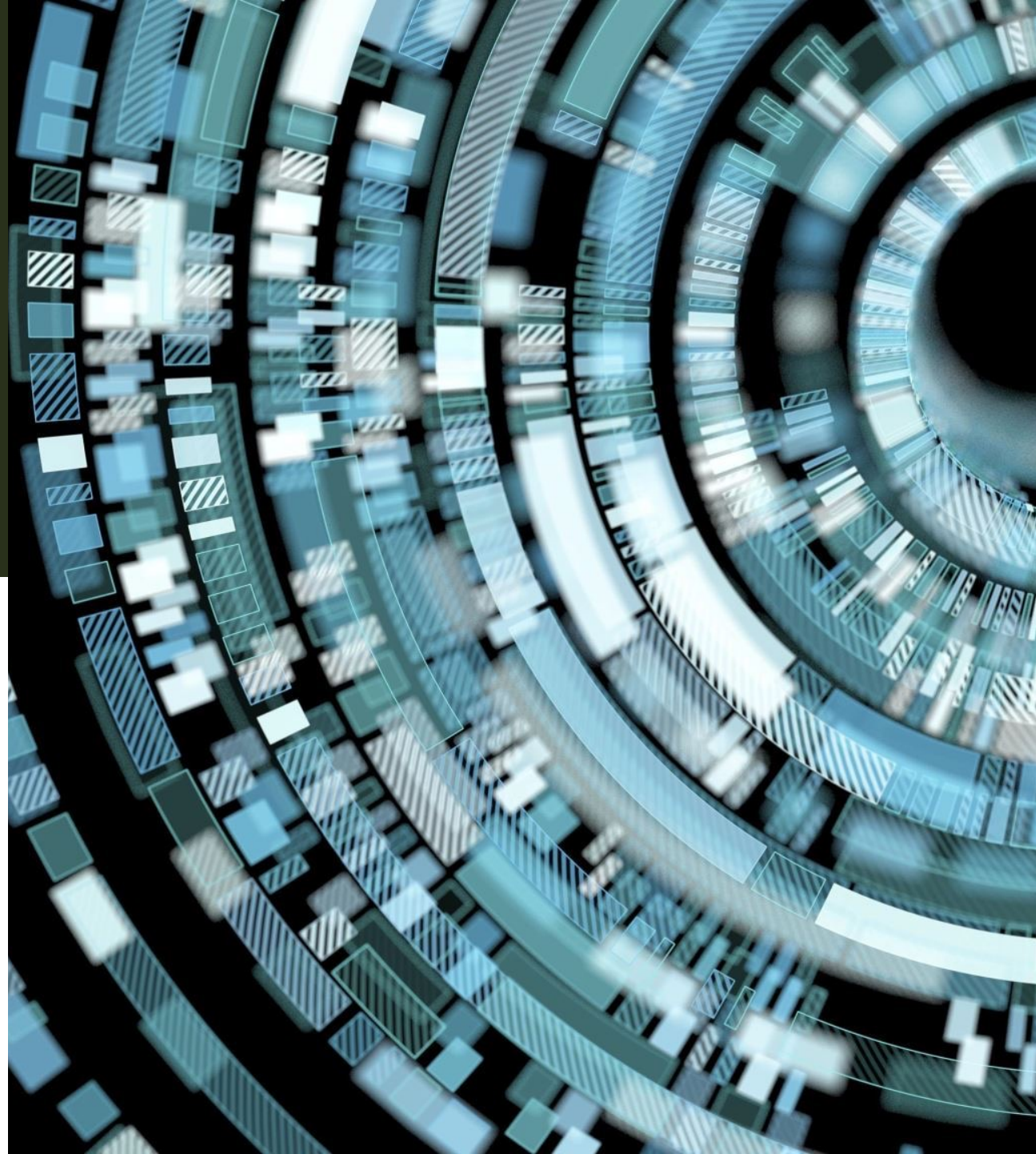
The creation of internationally recognised cyber norms will gain traction

Nations will work more closely together to develop common principles and standards guiding responsible state behaviour in cyberspace

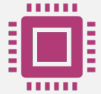
Nations will need to address concerns such as AI ethics, the possible threats of autonomous cyber systems, and the development of rules for the appropriate use of AI in cyber operations

Artificial Intelligence and its impact on cyber diplomacy

Cyber diplomacy will increasingly address issues such as digital governance, data protection, and privacy



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

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 practises that account for the impact of quantum computing

Diplomacy may foster public-private partnerships for solving quantum computing's problems

Diplomacy has the capacity to raise worldwide awareness about the risks of quantum computing to cybersecurity

Preparing for the challenges of quantum computing

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

Internet of Things and its impact on cyber diplomacy

The Internet of Things is a network of physical devices, automobiles, appliances, and other objects that are integrated with sensors, software, and connection 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

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

Internet of Things and its impact on cyber diplomacy

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 the sharing of experience and best practises to improve IoT security and effectively confront emerging cyber threats

IoT devices vastly increase the attack surface for cyber threats

Cyber diplomacy is critical in negotiating international agreements and legislation to safeguard user data and set cross-border data privacy standards

Blockchain technology and its impact on cyber diplomacy

Blockchain technology is a distributed ledger system that allows for secure and transparent transactions without the need for a central authority

Blockchain technology has numerous applications and has the potential to significantly alter cyber diplomacy

Because of its decentralised design and cryptographic procedures, blockchain is extremely resistant to tampering and hacking

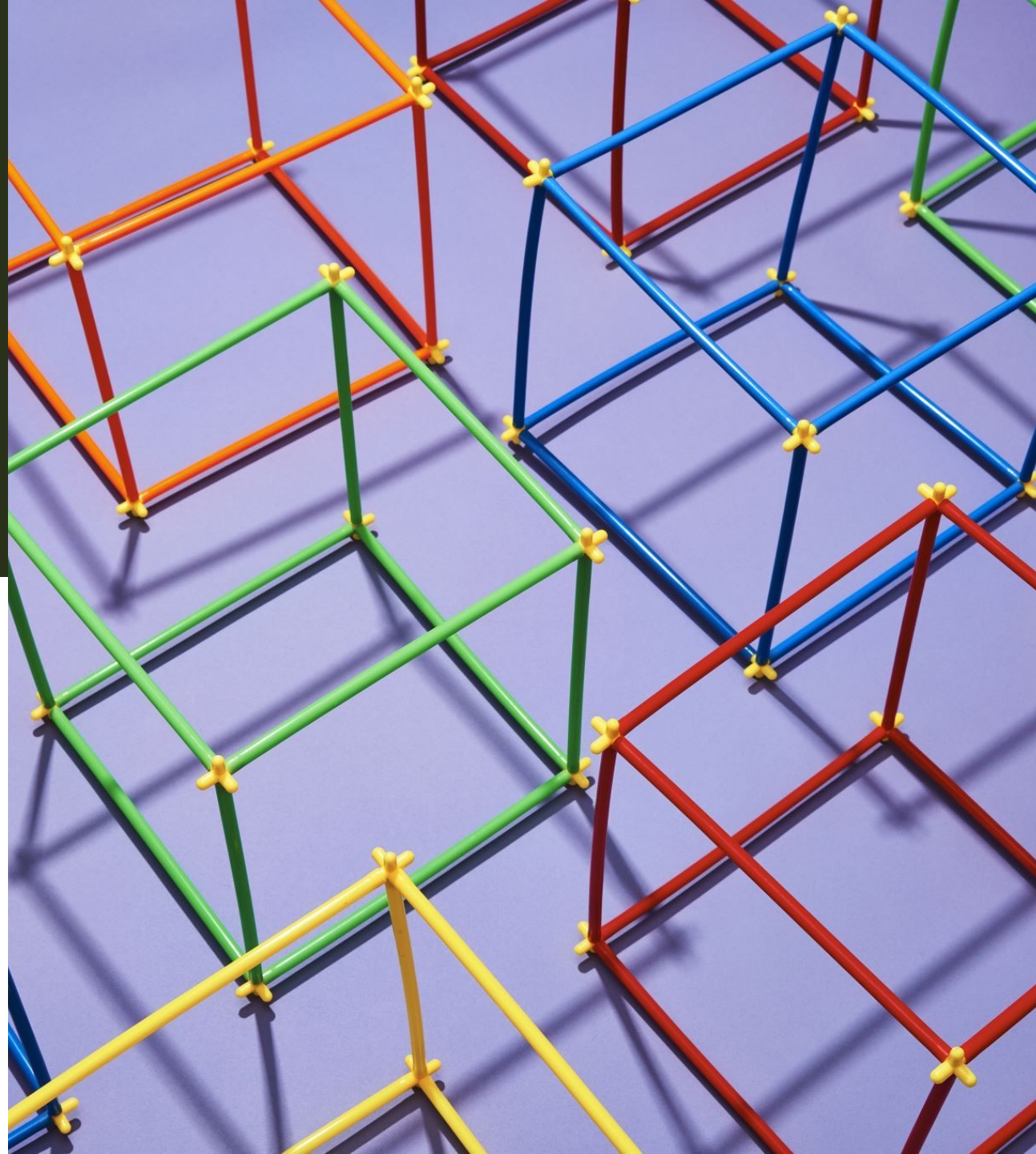
Blockchain-based identity management systems have the potential to provide a more secure and tamper-proof method of confirming identities and restricting access to classified material, lowering the risk of identity-related cyber breaches

Blockchain technology and its impact on cyber diplomacy

Blockchain technology can be used to create a tamper-proof record of these papers, assuring their legitimacy, and giving a trustworthy audit trail for checking their origin and integrity

Blockchain, at its heart, is a decentralised and distributed ledger system that enables secure and transparent transactions in the absence of a central authority

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



Building Cyber Trust

Strategies for fostering trust in cyberspace

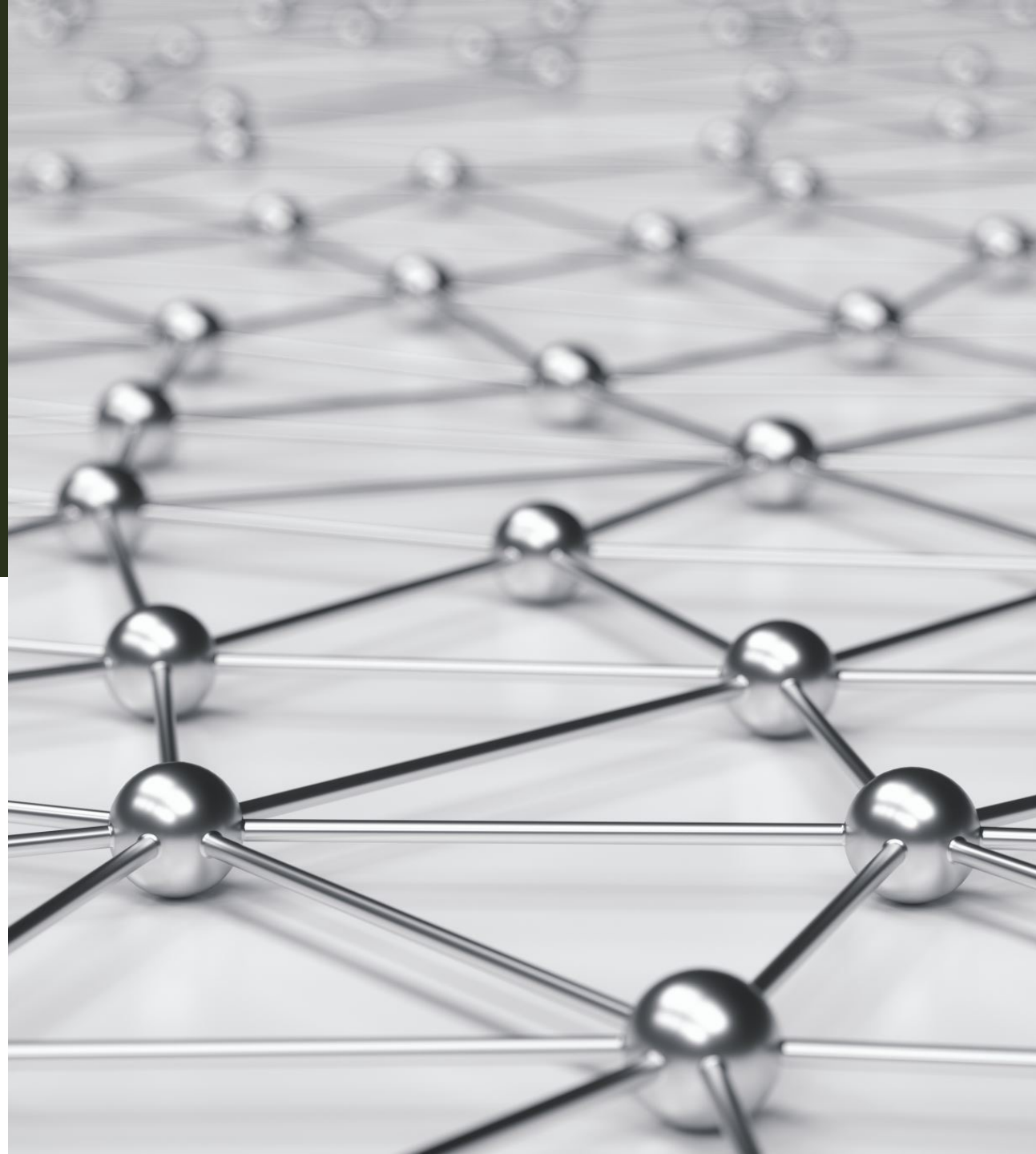
Building cyber trust among consumers, businesses, and governments is critical in today's connected world for encouraging collaboration, cooperation, and effective cybersecurity measures

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 their cybersecurity measures and swiftly disclose any breaches or events

Governments and corporations can collaborate to exchange threat intelligence, best practises, and resources, thereby enhancing overall cybersecurity efforts



Confidence-building measures among states

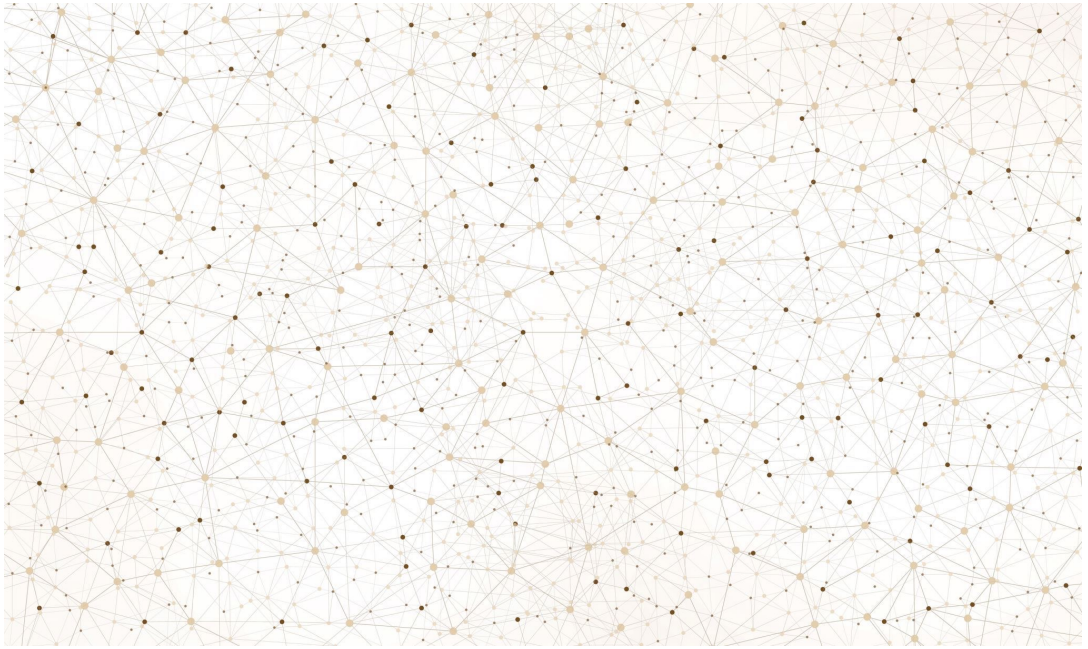
National confidence-building measures are critical in decreasing tensions and boosting cooperation in cyberspace

Confidence-building measures are agreements and acts that try to increase mutual trust, transparency, and communication between different governments in order to avoid misunderstandings and miscalculations in cyber activities

Government can communicate information on cybersecurity policies, plans, and threat assessments on a voluntary basis

States can sign agreements defining areas of engagement, such as joint cybersecurity exercises, capacity-building efforts, and technical cooperation, for cybersecurity cooperation

Cyber Diplomacy and Traditional Diplomacy



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 a wide range of global concerns, cyber diplomacy focuses particularly on cyberspace and cybersecurity

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

Cyber-power as a new dimension of state influence

In today's interconnected world, cyber-power provides a new dimension of state influence

It refers to a country's ability to wield influence, project strength, and achieve strategic goals by utilising cyberspace and cyber capabilities

Cyber-powerful states can use their technological prowess to acquire strategic advantages in a variety of disciplines, including the military, economic, political, and social realms

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 as a new dimension of state influence

Cyber-power improves a country's intelligence gathering capabilities by allowing for the targeted collection of sensitive information from foreign governments, entities, and individuals

Conclusion: Shaping a Secure Digital Future

Cyber diplomacy is critical in dealing with the complexity of the digital environment in international relations

It focuses on encouraging responsible behaviour, safeguarding cybersecurity, and assuring cyberspace stability

International cooperation, conflict resolution, cybersecurity governance, confidence-building measures, attribution, public-private partnerships, capacity building, and defending digital rights and freedoms are all important components

As the internet connects the world, international collaboration in cyberspace is critical for detecting, preventing, and responding to cyber threats

Conclusion: Shaping a Secure Digital Future

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

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

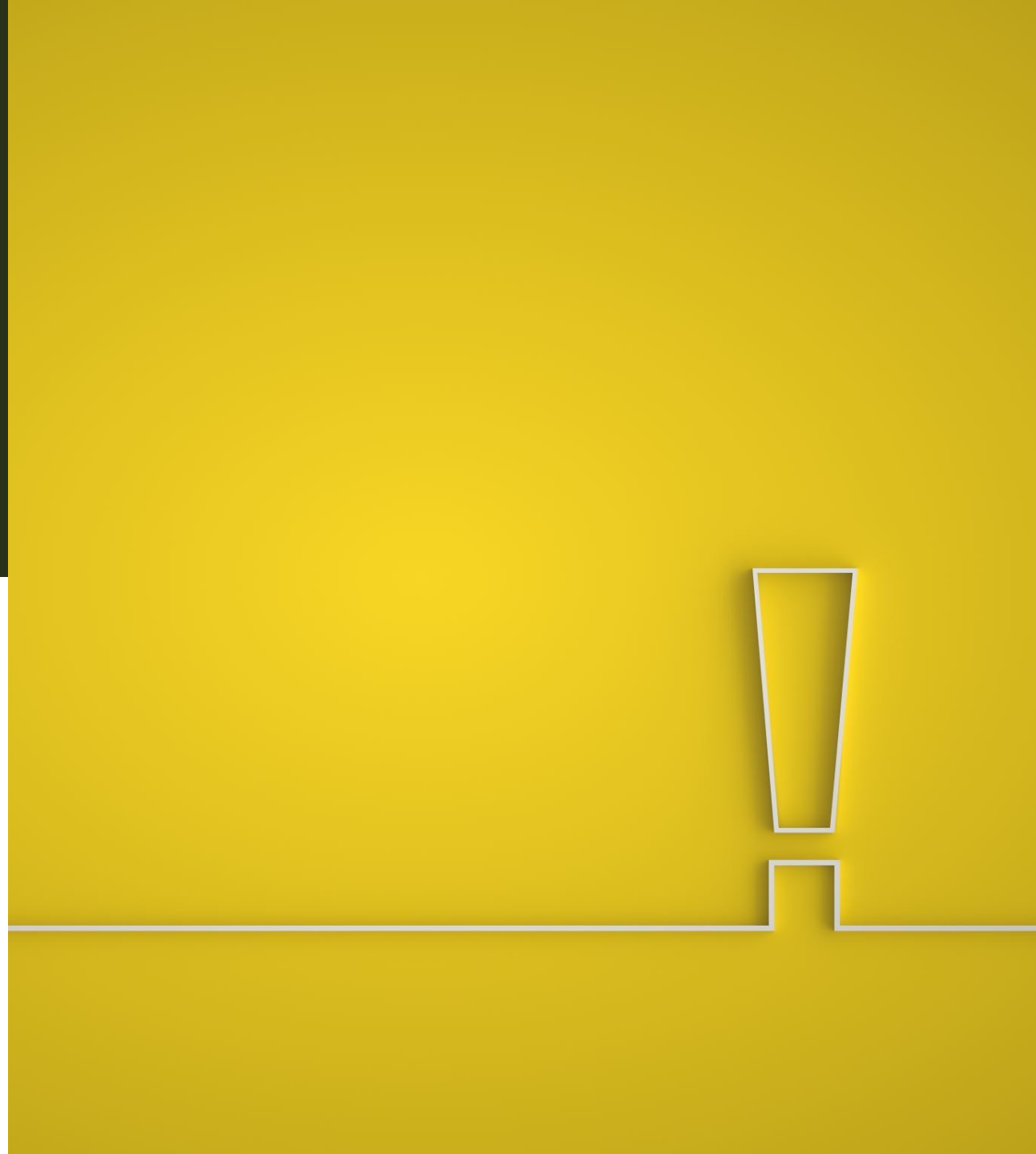
Existing international cyber laws and conventions seek to address cyber problems while also encouraging responsible internet behaviour

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

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



References

US Department of State, “Bureau of Cyberspace and Digital Policy - United States Department of State,”

https://www.state.gov/bureaus-offices/deputy-secretary-of-state/bureau-of-cyberspace-and-digital-policy/

ICANN, “ICANN Computer Incident Response Team - ICANN,”