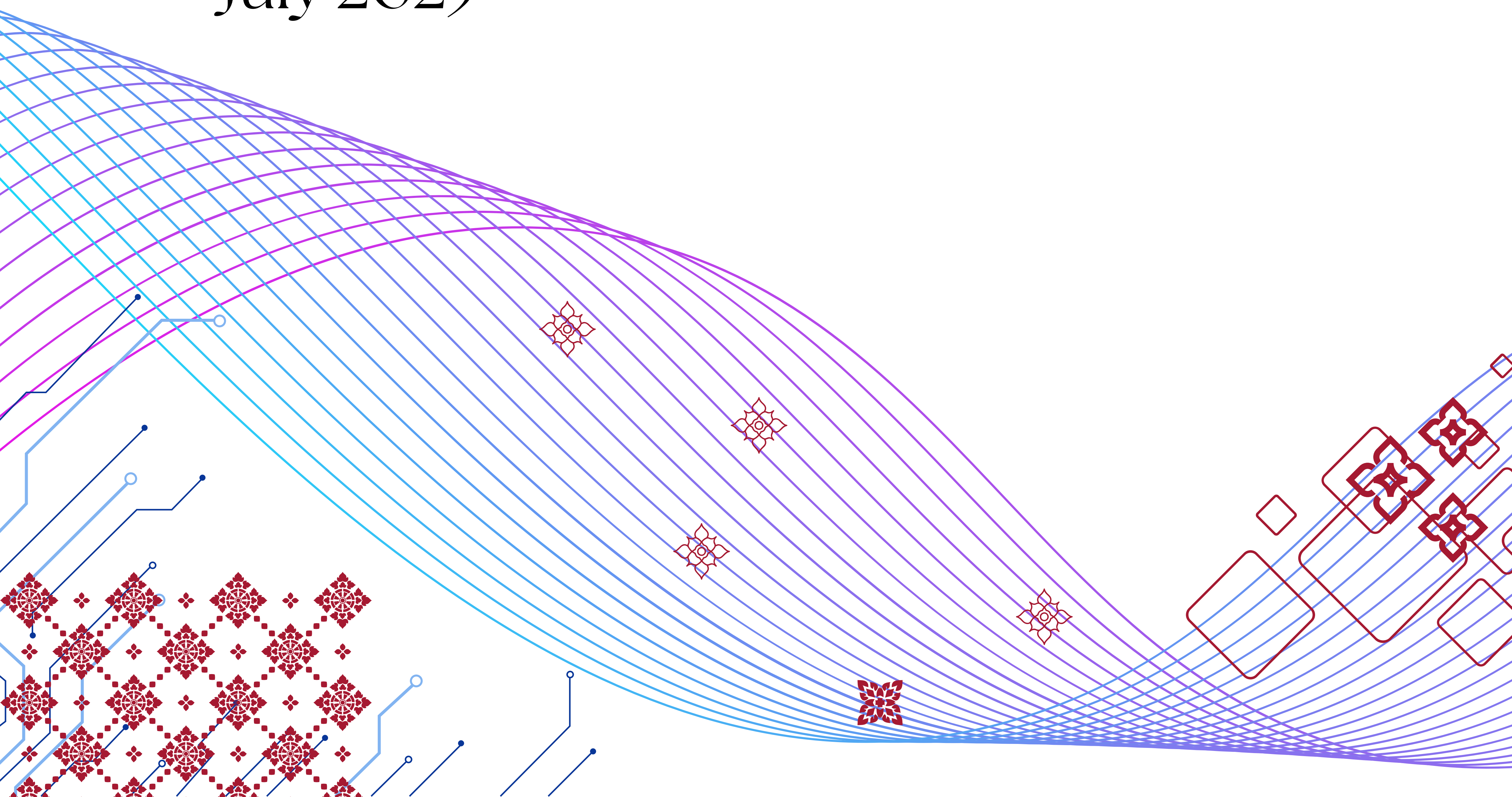


THAILAND'S

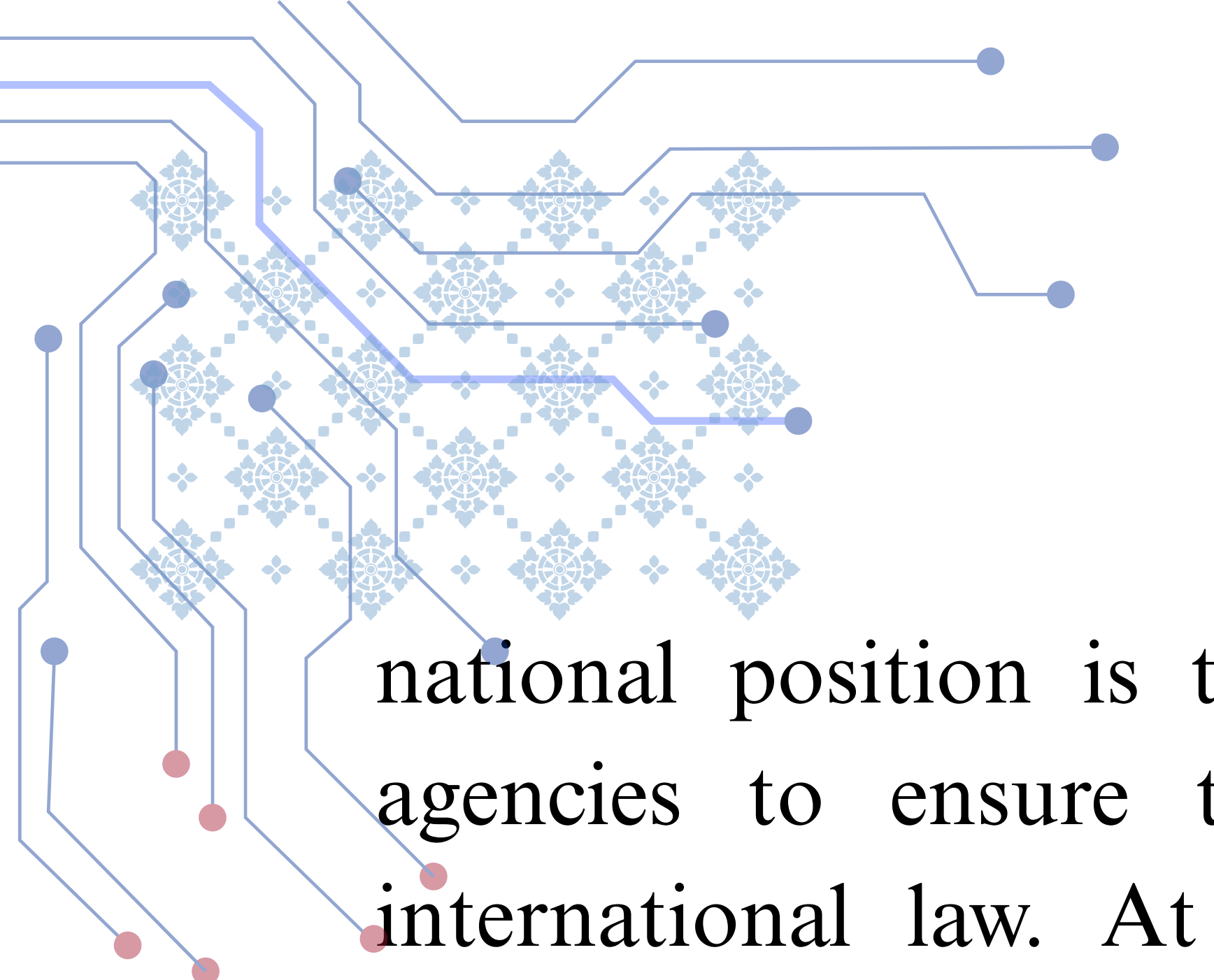


National Position on the
Application of International Law
in Cyberspace
July 2025



I. Introduction

1. Thailand recognizes the transformative potential of information and communication technologies (ICTs) and the increasing reliance on cyberspace across all sectors of society. At the same time, the expanding use of ICTs has introduced complex legal, policy, and security challenges that transcend borders and implicate the maintenance of international peace and security.
2. Against this backdrop, Thailand affirms its commitment to the rules-based international order and the vital role of international law in governing State behavior in cyberspace. Thailand supports the consensus among States that existing international law, including the Charter of the United Nations in its entirety, applies to conduct of States in cyberspace, which has been consistently reflected in the consensus reports of the United Nations Group of Governmental Experts (UNGGE) and the Open-ended Working Group (OEWG) on security of and in the use of information and communications technologies.
3. Thailand has actively participated in the OEWG and regional forums to support inclusive, transparent, and consensus-based efforts to develop common understandings of how international law applies to cyberspace. These processes have demonstrated the value of exchanging national views to foster legal clarity, build mutual trust, and reduce the risks of miscalculation, escalation, and conflict in the cyber domain.
4. Thailand has initiated a whole-of-government consultation process to develop Thailand's national position on the application of international law in cyberspace to serve two main objectives. At national level, this



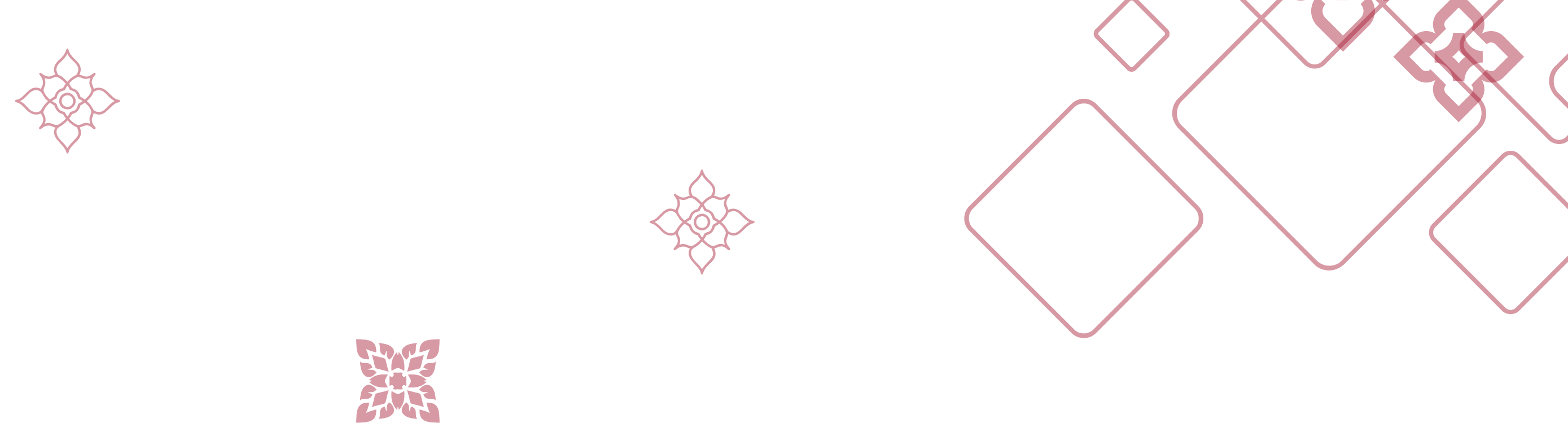
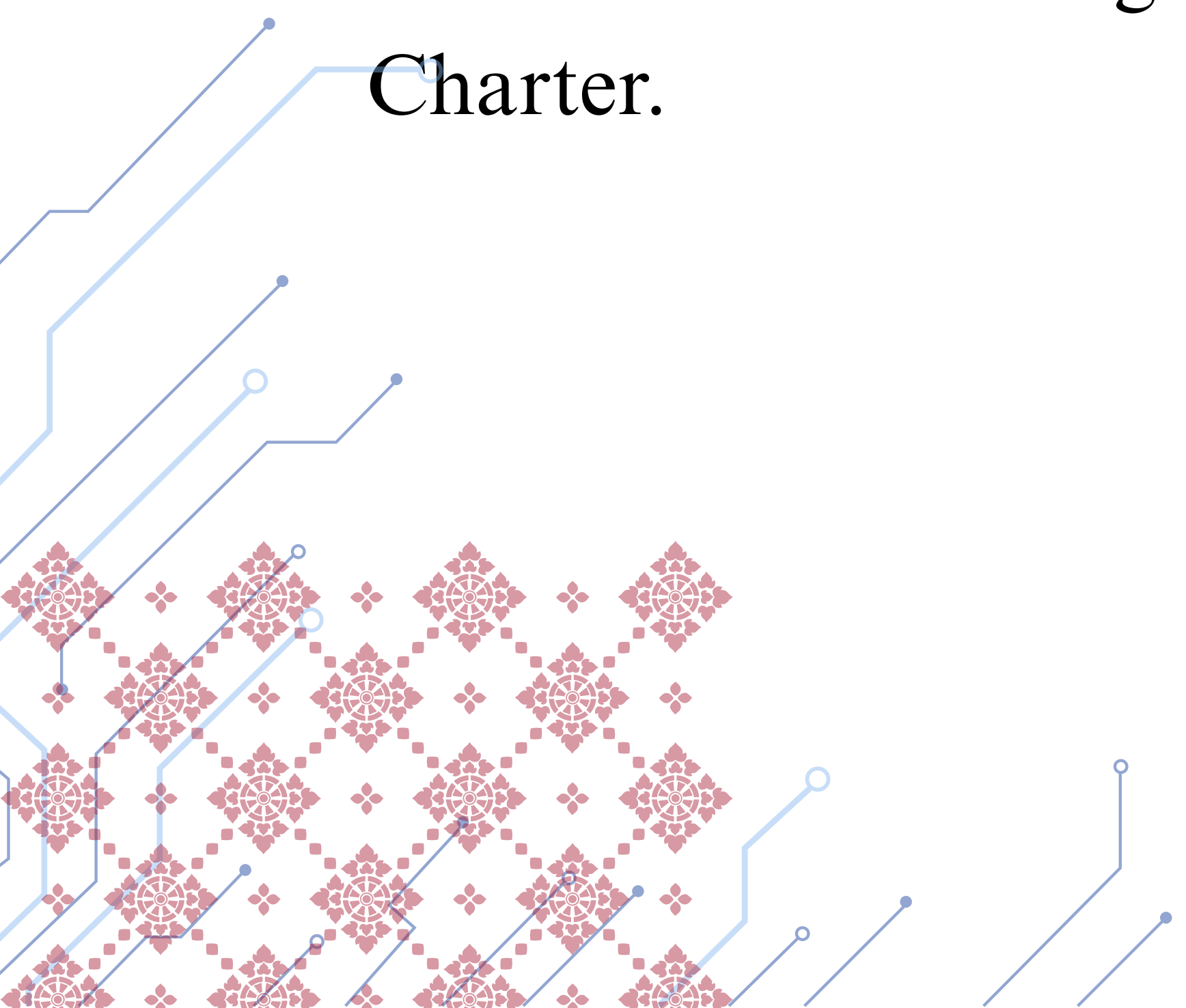
national position is to serve as a guideline for all Thai government agencies to ensure that their conduct in cyberspace comply with international law. At international level, it is hoped that Thailand's position contributes to the global discussion on how international law applies in cyberspace, and if further progressive development of international law is required in this field.

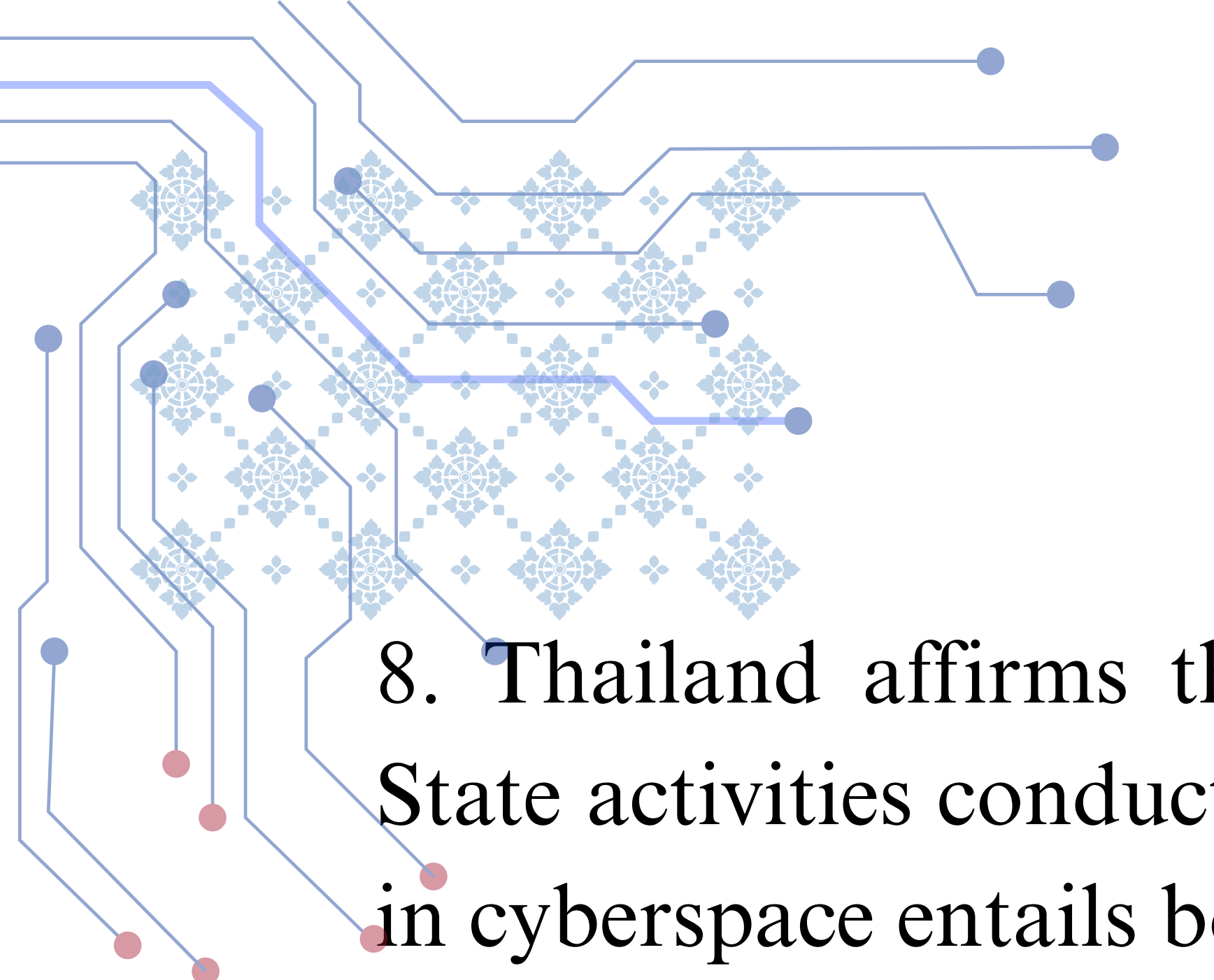
5. This national position represents the outcome of these consultations and reflects Thailand's current views on key principles and legal frameworks applicable to the use of ICTs by States. It is not intended to be exhaustive or definitive, but rather to serve as a foundation for future legal discourse both at home and with international partners. Thailand will review and refine its position in light of evolving international practice, and ongoing developments in the interpretation and application of international law in cyberspace.

6. Thailand reaffirms its commitment to promoting an open, secure, stable, accessible, and peaceful ICT environment, and stands ready to work with all States to uphold international law, strengthen responsible State behavior, and enhance international cooperation in cyberspace.

II. Sovereignty

7. The principle of state sovereignty is a fundamental rule of international law that underpins international relations. It is firmly established in customary international law and enshrined in international legal instruments including the Charter of the United Nations and the ASEAN Charter.





8. Thailand affirms that the principle of sovereignty applies in full to State activities conducted in cyberspace. As in other domains, sovereignty in cyberspace entails both rights and obligations for States.

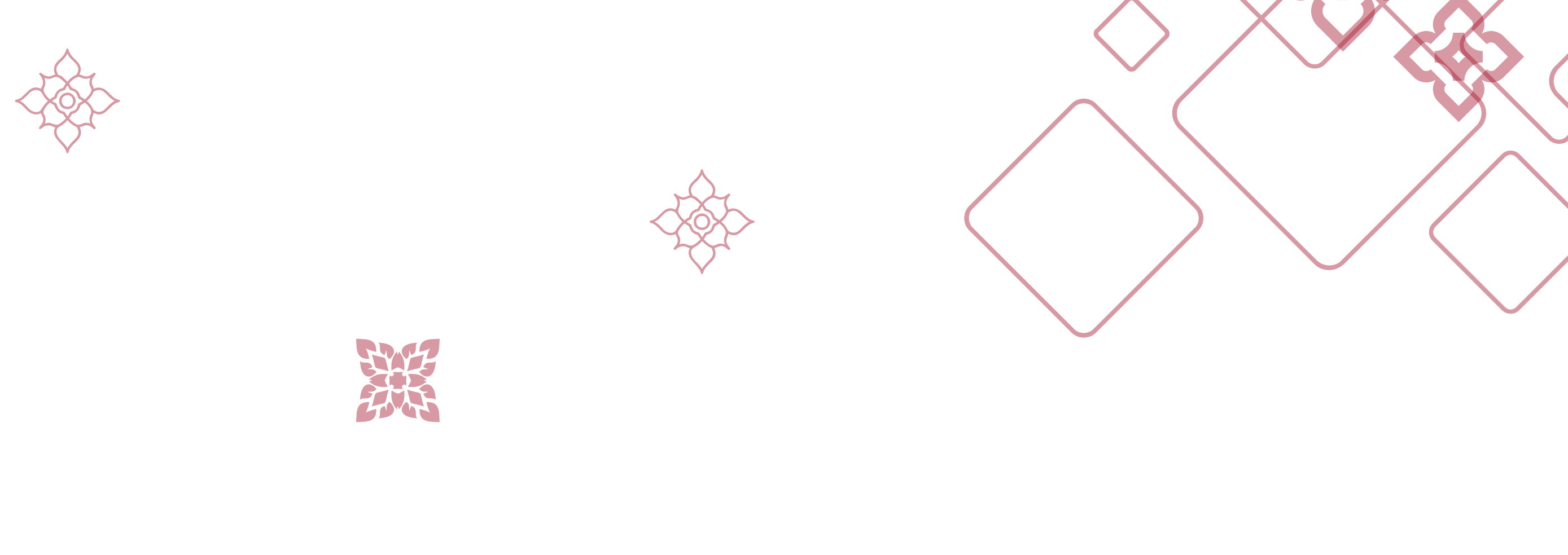
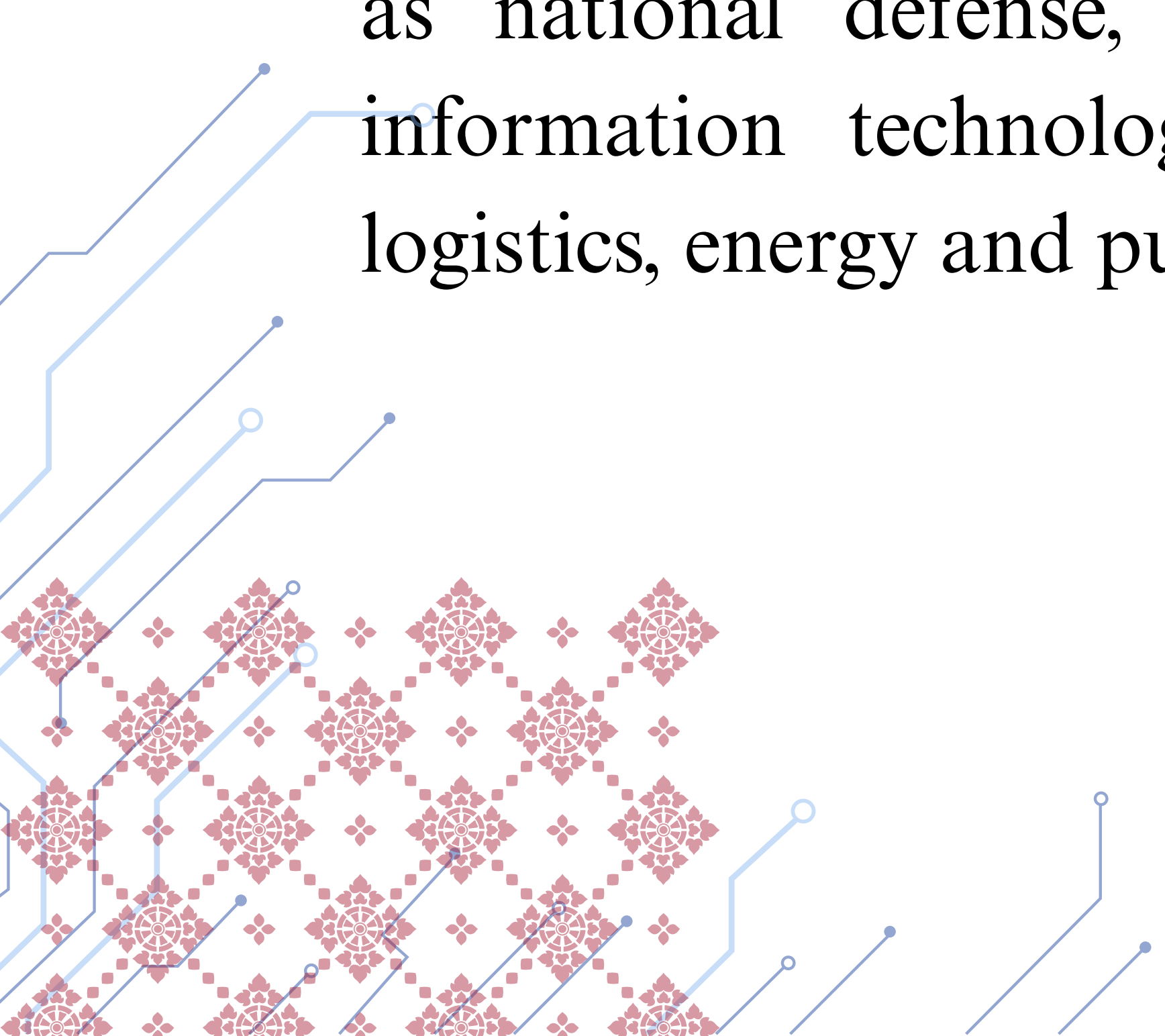
9. Under international law, every State exercises sovereignty over the ICT infrastructure, persons, and activities within its territory, subject to its international legal obligations. This includes the authority to prescribe and enforce laws and regulations governing cyberspace and to protect critical information infrastructure.

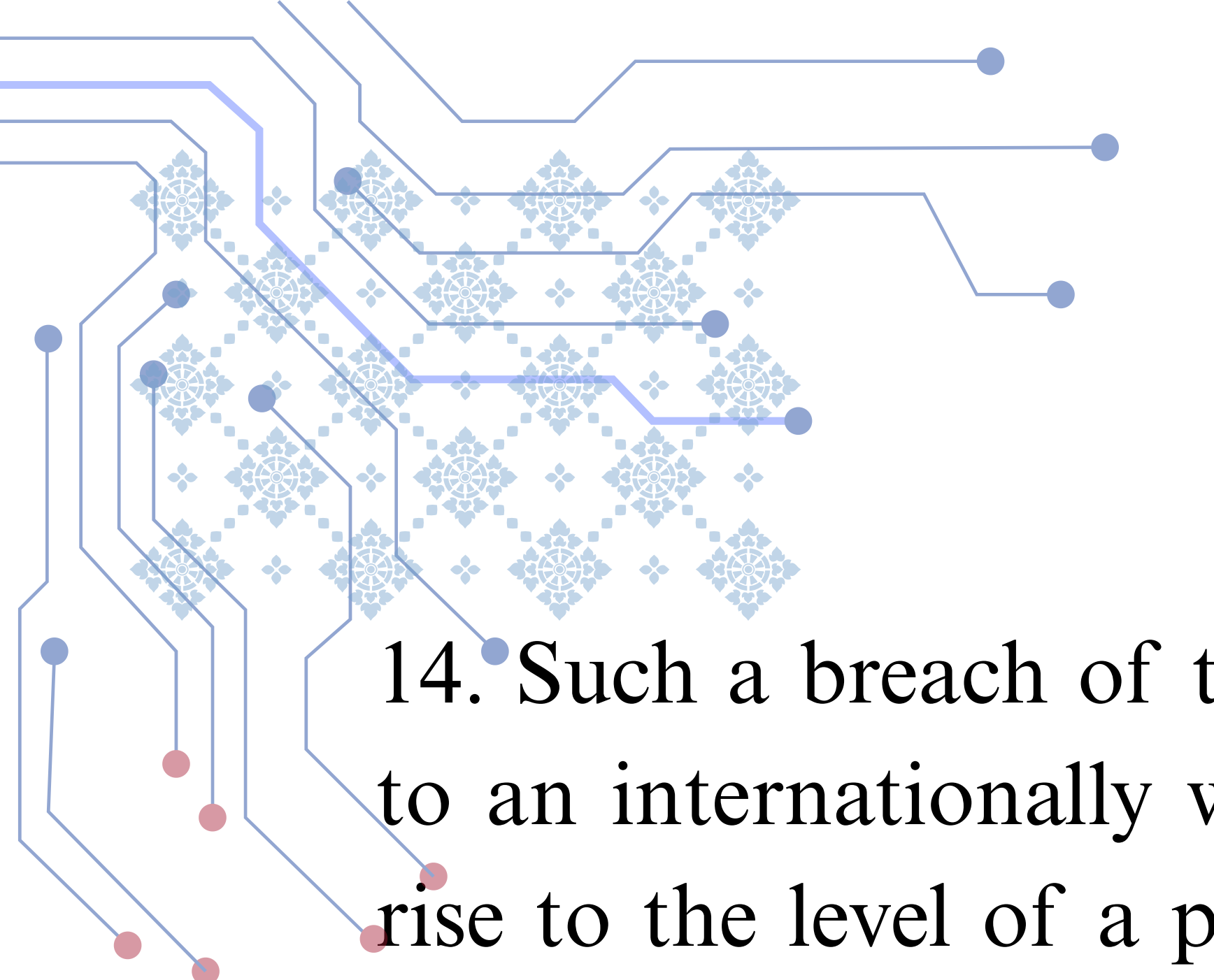
10. At the same time, the principle of sovereignty entails a corresponding obligation for States to respect the sovereignty of other States and to refrain from conducting cyber operations that infringe upon it.

11. Therefore, a cyber activity attributable to a State that causes, or is reasonably expected to cause, harmful effects on ICT systems or infrastructure located within another State's territory constitutes a violation of that State's territorial sovereignty.

12. State cyber operations targeting another State's critical infrastructure constitute a violation of sovereignty where they interfere with the State's sovereign control over the critical infrastructure; cause harm or compromise essential functions of the critical infrastructure.

13. For the purposes of this national position, critical infrastructure includes key sectors essential to national security and public welfare, such as national defense, essential public services, banking and finance, information technology and telecommunications, transportation and logistics, energy and public utilities, and public health systems.



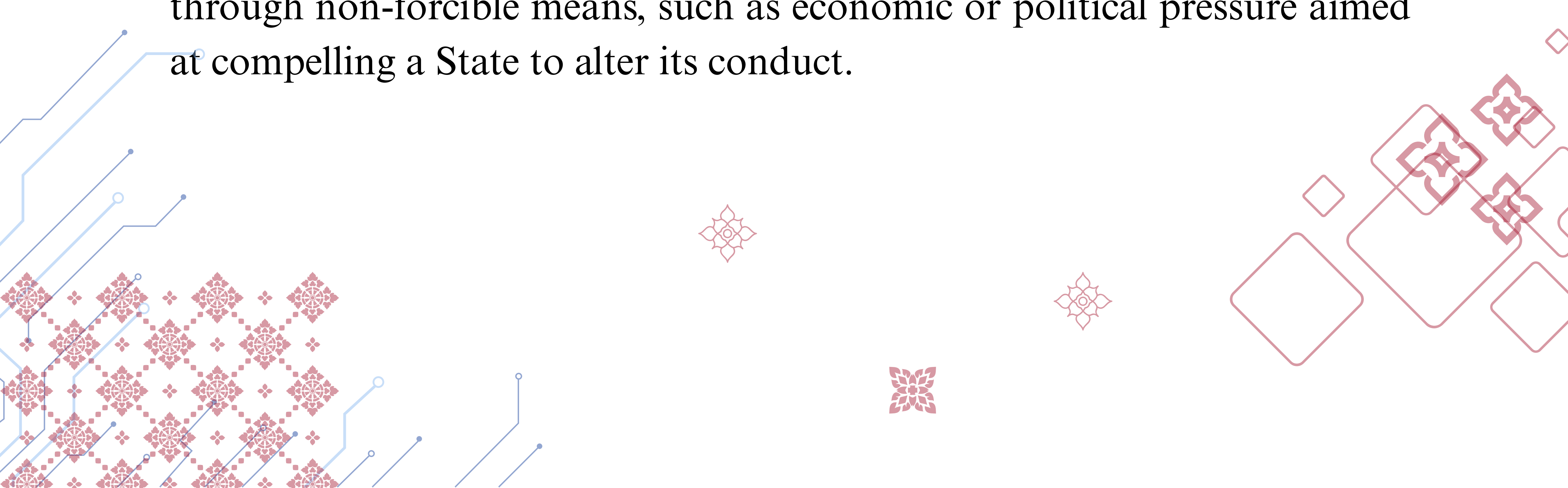


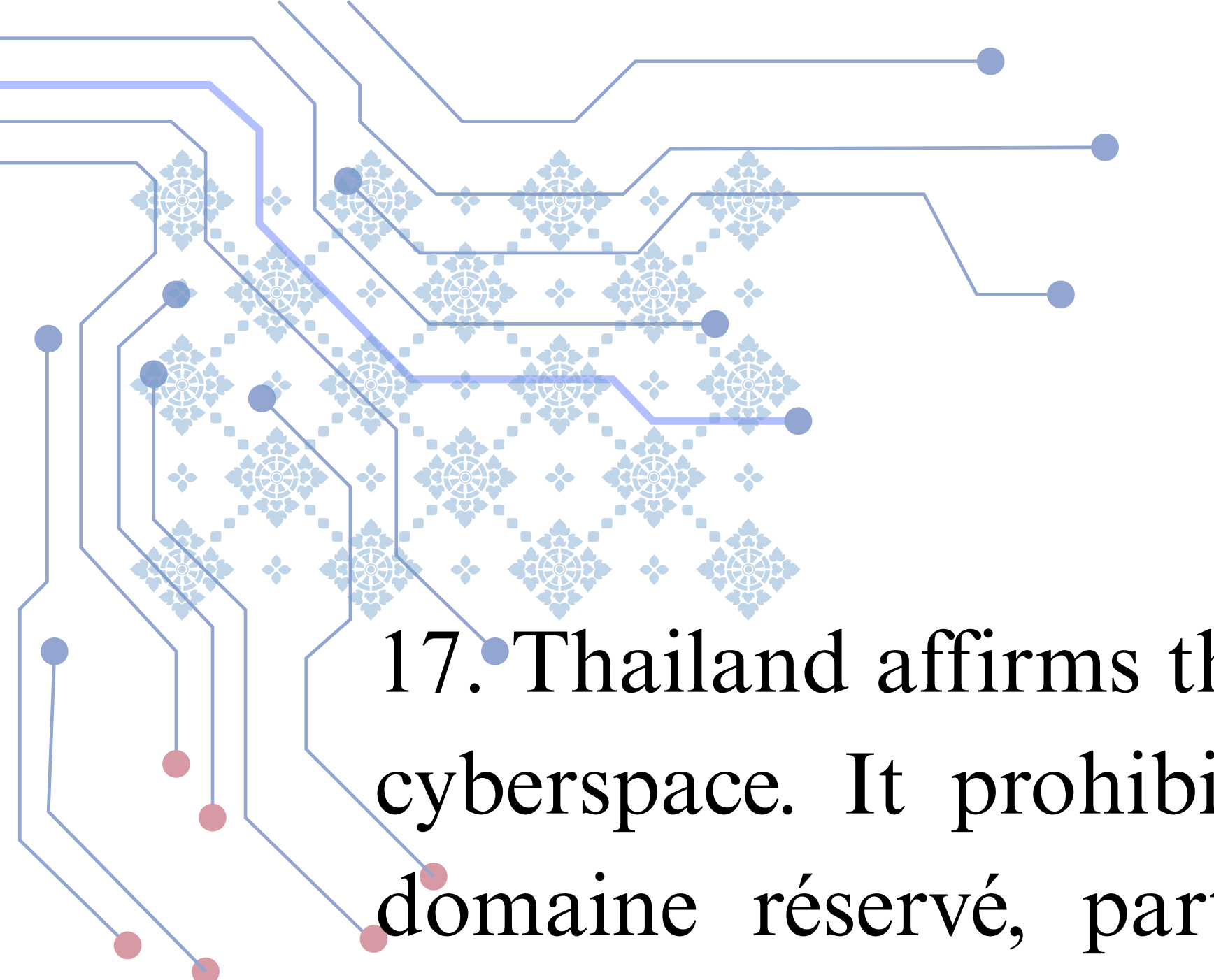
14. Such a breach of the obligation to respect State sovereignty amounts to an internationally wrongful act, even if the cyber operation does not rise to the level of a prohibited intervention or a prohibited use of force under international law.

III. Prohibition of Intervention

15. The prohibition of intervention is a fundamental principle of international law, firmly established in customary international law, and a direct corollary of the principle of sovereignty. It is reflected in international treaties, in particular Articles 2(1) and 2(7) of the Charter of the United Nations and Article 2(2) of the ASEAN Charter, which obligate States to respect the sovereign rights of other States in matters within their exclusive jurisdiction, including political, economic, social, and foreign policy affairs.

16. The International Court of Justice (ICJ) affirmed this principle in the *Case Concerning Military and Paramilitary Activities in and Against Nicaragua* (Nicaragua v. United States of America), emphasizing that coercion constitutes the essence of an unlawful intervention. While the precise meaning of "coercion" remains under discussion among States, the ICJ clarified that direct or indirect coercive measures, including the threat or use of force, may constitute unlawful intervention. The 1970 Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations further recognizes that coercion can also arise through non-forcible means, such as economic or political pressure aimed at compelling a State to alter its conduct.



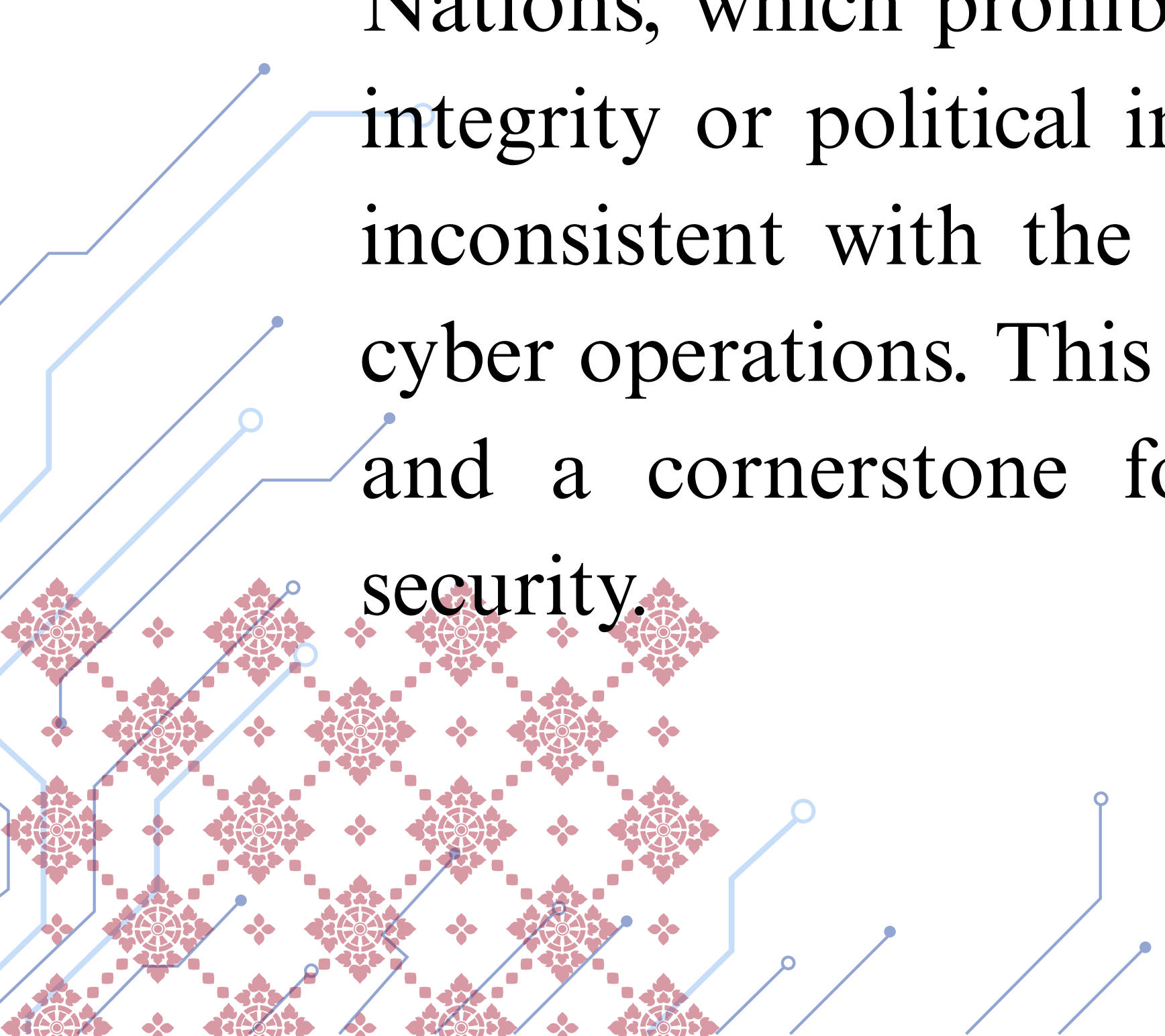


17. Thailand affirms that the prohibition of intervention applies in full to cyberspace. It prohibits cyber operations that intervene with a State's *domaine réservé*, particularly where such operations target sovereign governmental functions or essential public services. As non-exhaustive examples, coercive cyber operations that significantly impair Thailand's capacity to conduct elections, maintain public administration, deliver essential services, or uphold internal security will constitute unlawful intervention under international law.

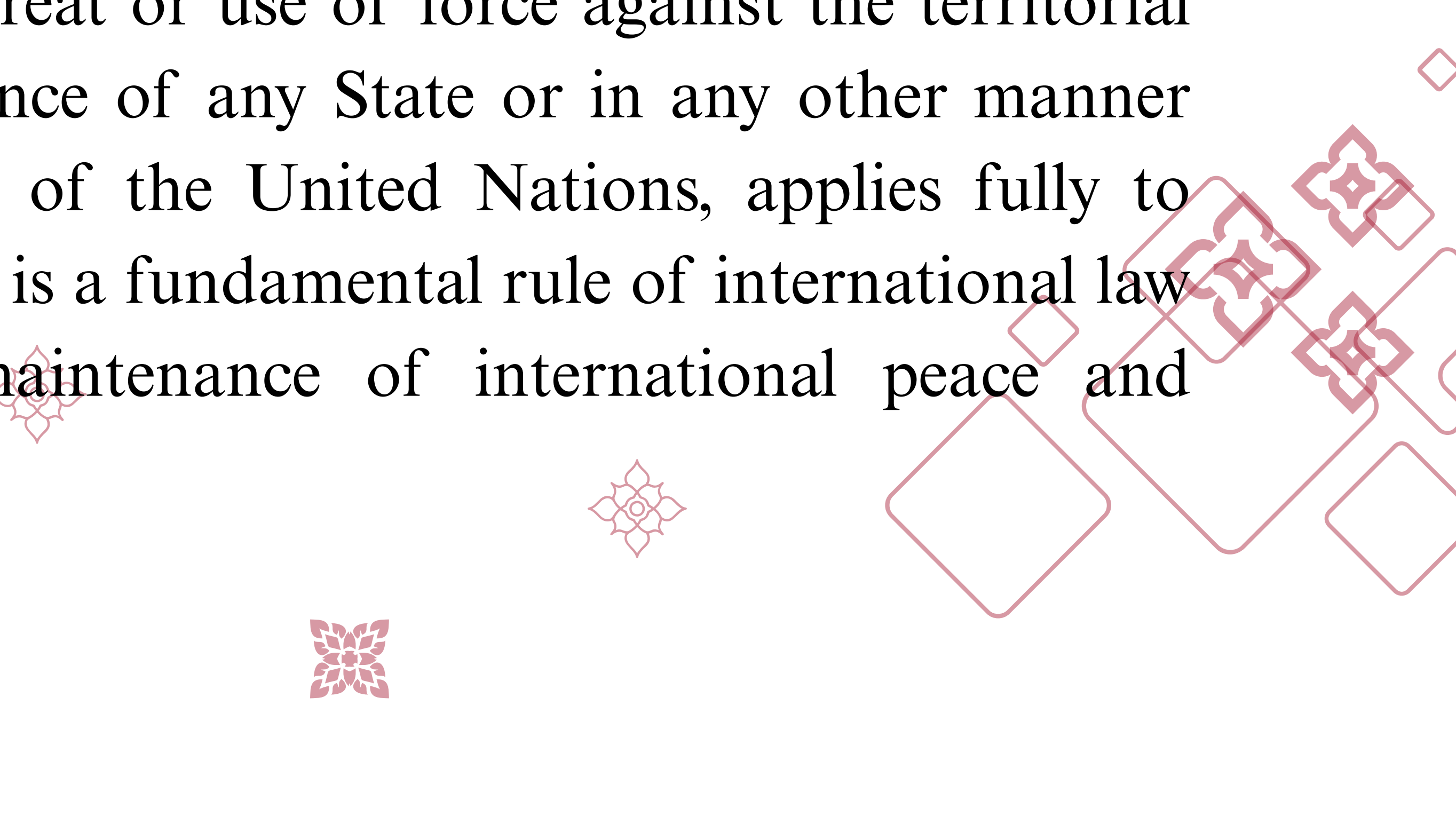
18. Thailand affirms that coercion must be assessed on a case-by-case basis, taking into account the nature, scale, consequences, and context of a cyber operation. Coercion may arise where a cyber operation undermines a State's sovereign functions or impairs its ability to exercise its reserved domain (*domaine réservé*) freely, even without an explicit demand, demonstrable motive, or intention to compel. The assessment should focus primarily on the practical effects and severity of the interference.

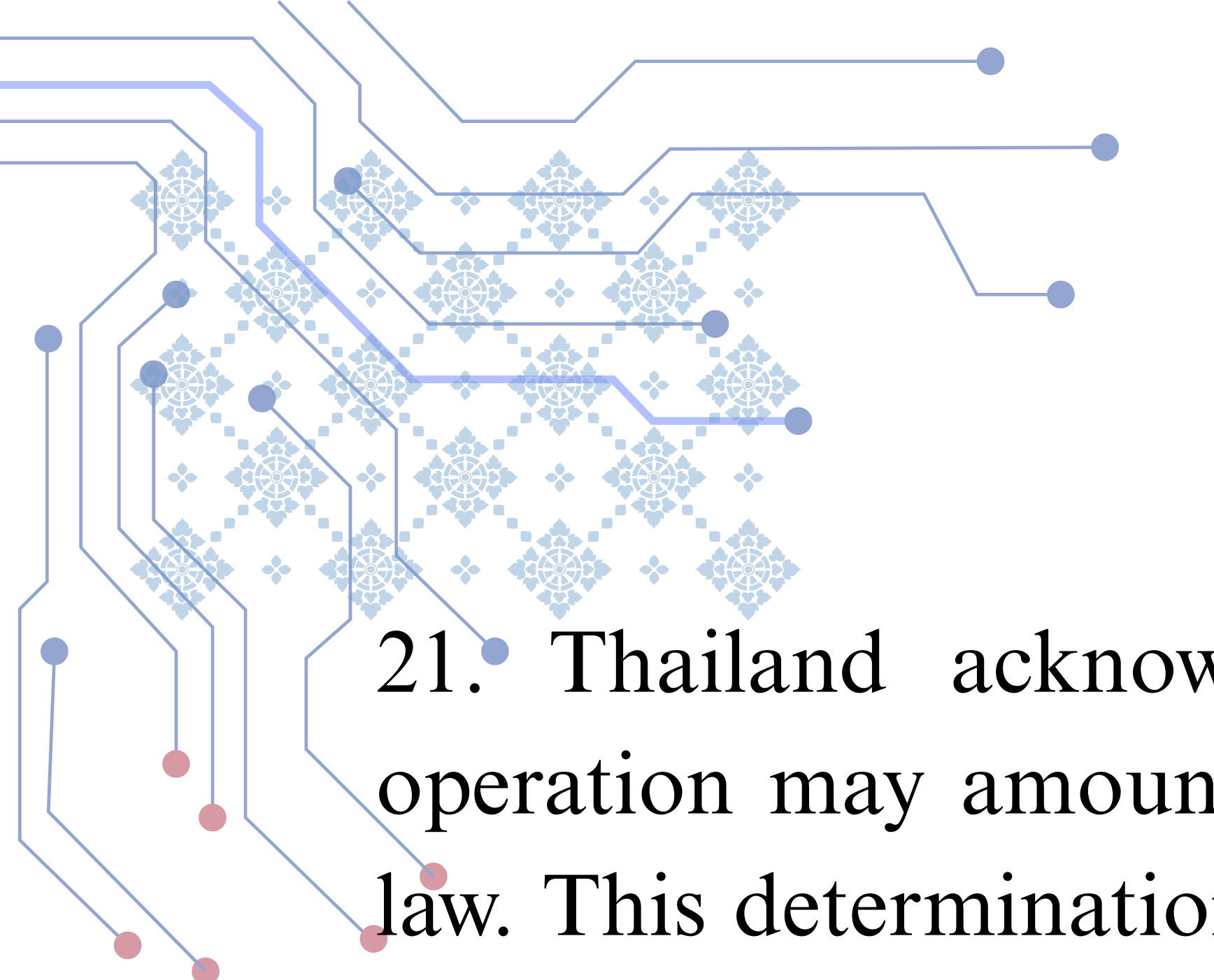
19. Cyber operations that do not meet the threshold to constitute a breach of the prohibition of intervention may nonetheless breach other obligations under international law, including the principles of sovereignty and the prohibition of the use of force.

IV. Prohibition of Use of Force



20. Thailand reaffirms that Article 2(4) of the Charter of the United Nations, which prohibits the threat or use of force against the territorial integrity or political independence of any State or in any other manner inconsistent with the Purposes of the United Nations, applies fully to cyber operations. This principle is a fundamental rule of international law and a cornerstone for the maintenance of international peace and security.





21. Thailand acknowledges that, in certain circumstances, a cyber operation may amount to a prohibited use of force under international law. This determination must be based on an assessment of the scale and effects of the cyber operation, including its foreseeable consequences on human life, property, or loss of functionality of critical infrastructure.

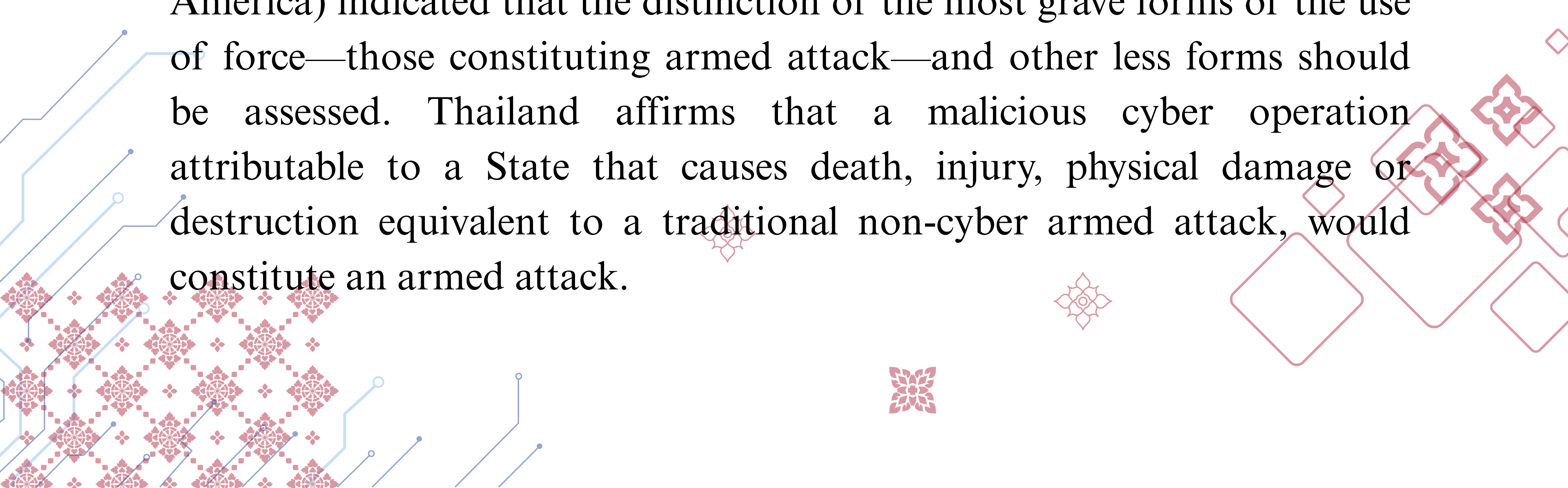
22. Cyber operations may amount to a use of force if they cause, or are reasonably expected to cause, physical destruction or injury equivalent in gravity to a kinetic attack. For instance, a cyberattack that disables critical infrastructure—such as power grids, air traffic control systems, or hospital networks—resulting in loss of life, injury, or significant material damage, may meet this threshold.

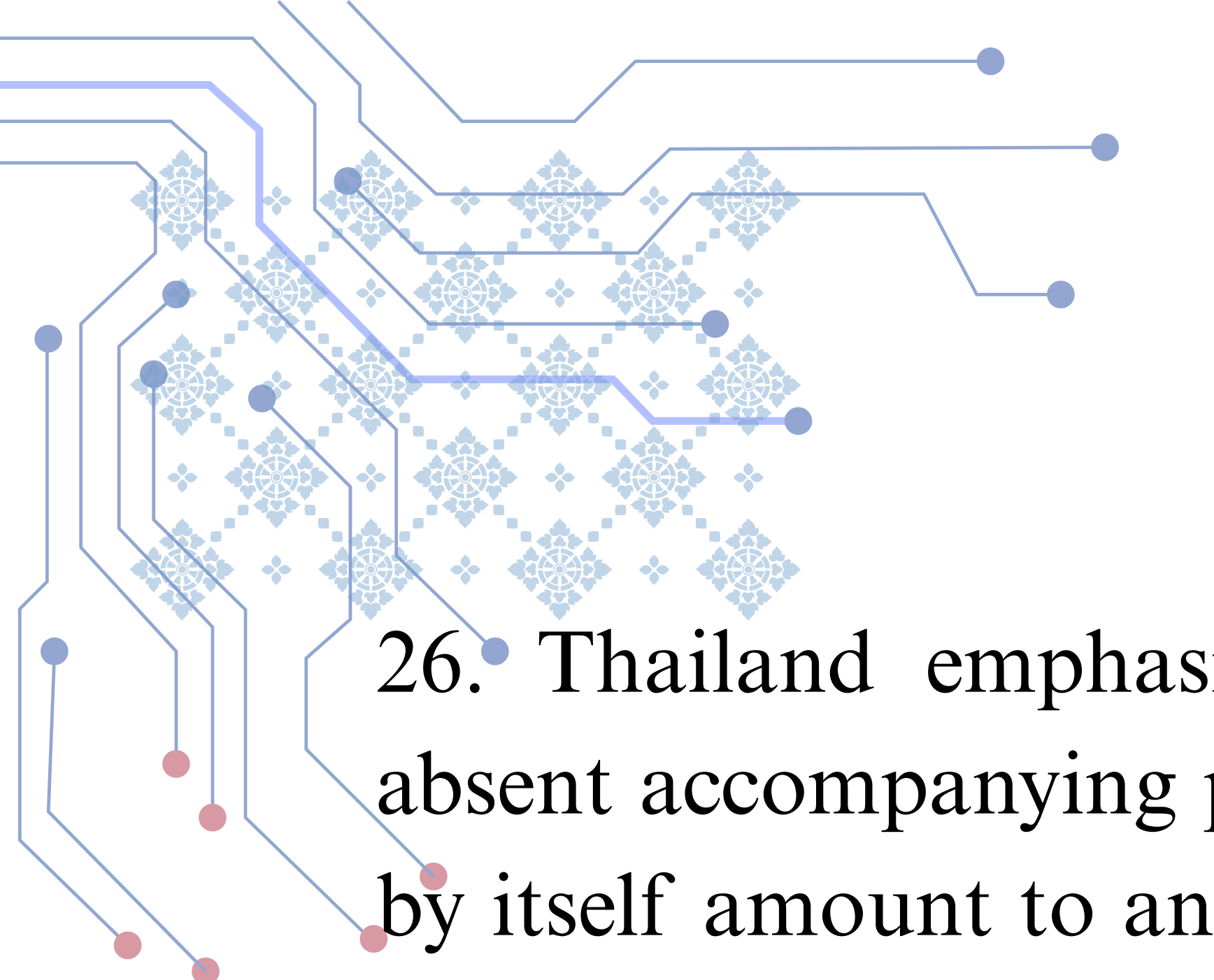
23. Thailand further notes that cyber operations falling below the threshold of the use of force may nonetheless breach other obligations under international law, including the principles of sovereignty and non-intervention.

V. Self-Defence

24. Thailand affirms that the inherent right of self-defence under international law including Article 51 of the Charter of the United Nations applies fully in cyberspace.

25. The ICJ judgment in *Case Concerning Military and Paramilitary Activities in and Against Nicaragua* (Nicaragua v. United States of America) indicated that the distinction of the most grave forms of the use of force—those constituting armed attack—and other less forms should be assessed. Thailand affirms that a malicious cyber operation attributable to a State that causes death, injury, physical damage or destruction equivalent to a traditional non-cyber armed attack, would constitute an armed attack.





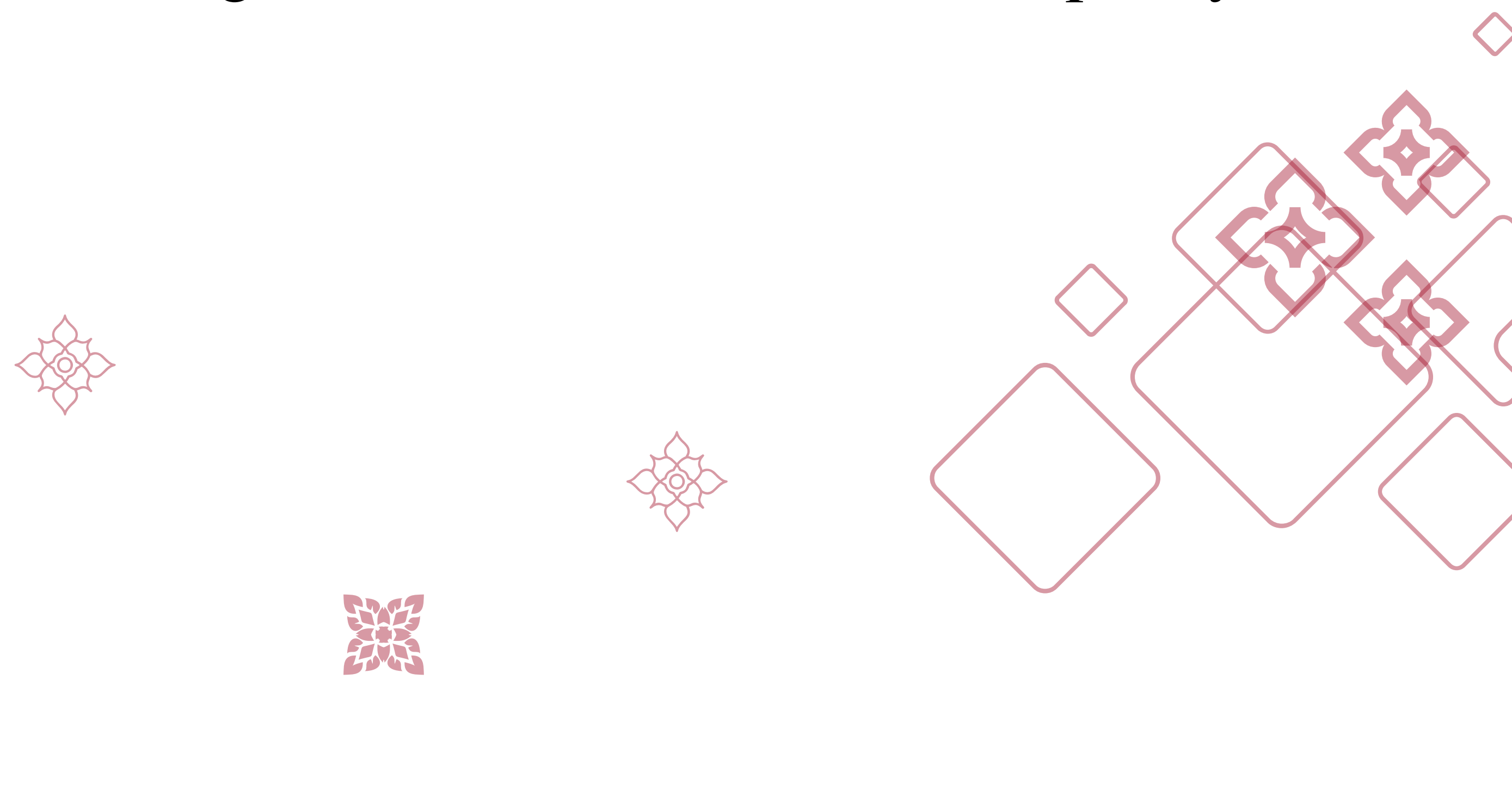
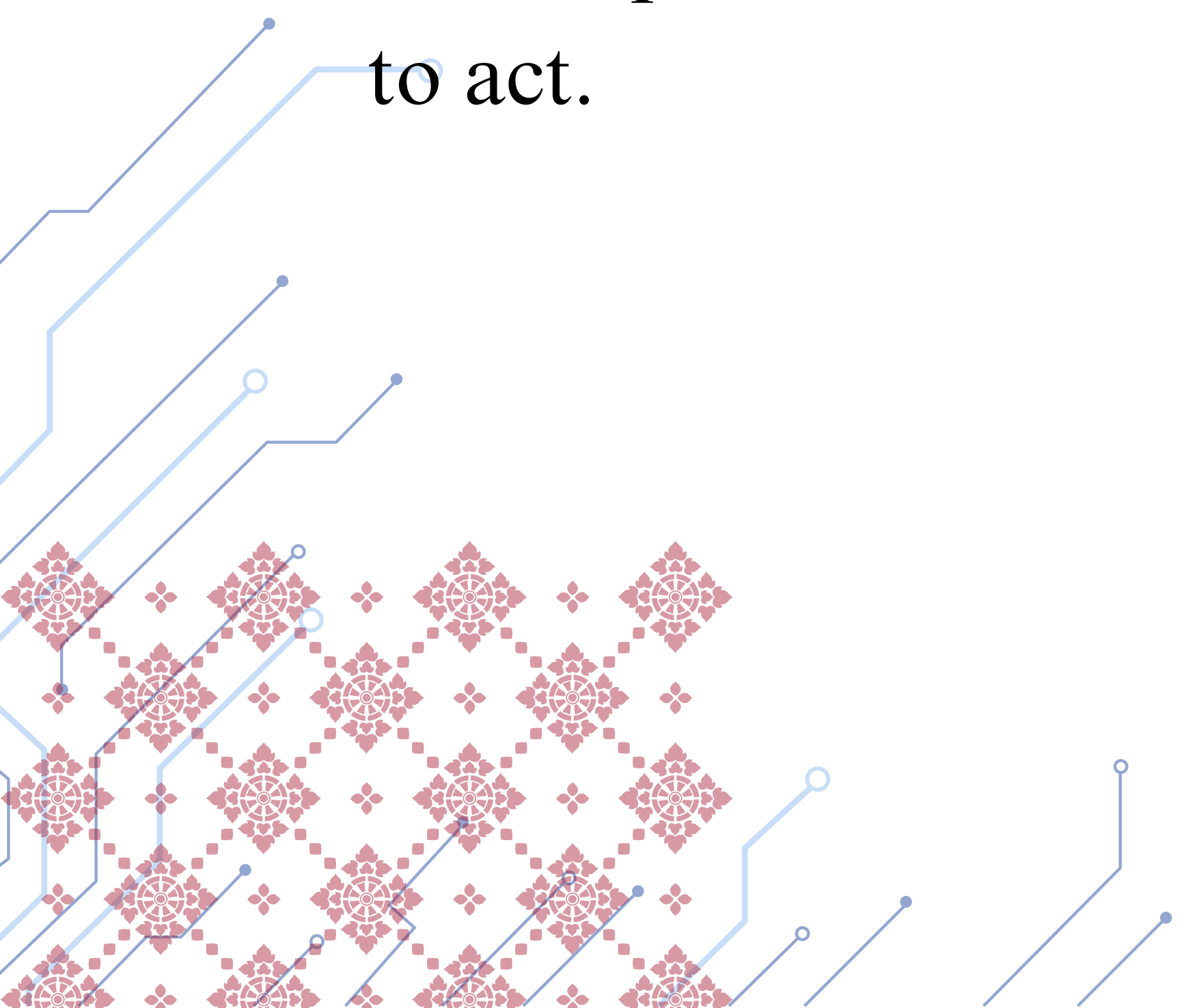
26. Thailand emphasizes that disruption to essential State functions, absent accompanying physical destruction, injury, or loss of life, does not by itself amount to an armed attack. The invocation of self-defence must strictly comply with the principles of necessity, proportionality, and immediacy, and must be based on responsible and reasonably certain attribution to a State.


27. Thailand stresses that the right of self-defence must not be used to justify preemptive or preventive use of force in cyberspace. Measures taken in self-defence must be exercised with the utmost caution to avoid escalation, miscalculation, and unintended consequences.

VI. Due Diligence

28. The principle of due diligence is firmly established in international law, as recognized by the International Court of Justice (ICJ) in the *Corfu Channel* case (1949), where the Court confirmed that a State must not knowingly allow its territory to be used for acts contrary to the rights of other States.

29. Accordingly, Thailand recognizes that due diligence applies to State conduct in cyberspace. Under this principle, States must take reasonable and proportionate measures, based on their knowledge and capacity, to prevent, mitigate, or terminate cyber activities emanating from their territory that cause significant adverse consequences for other States. This obligation applies when such cyber activities are conducted by non-State actors, provided the State has knowledge of the activities and the capacity to act.





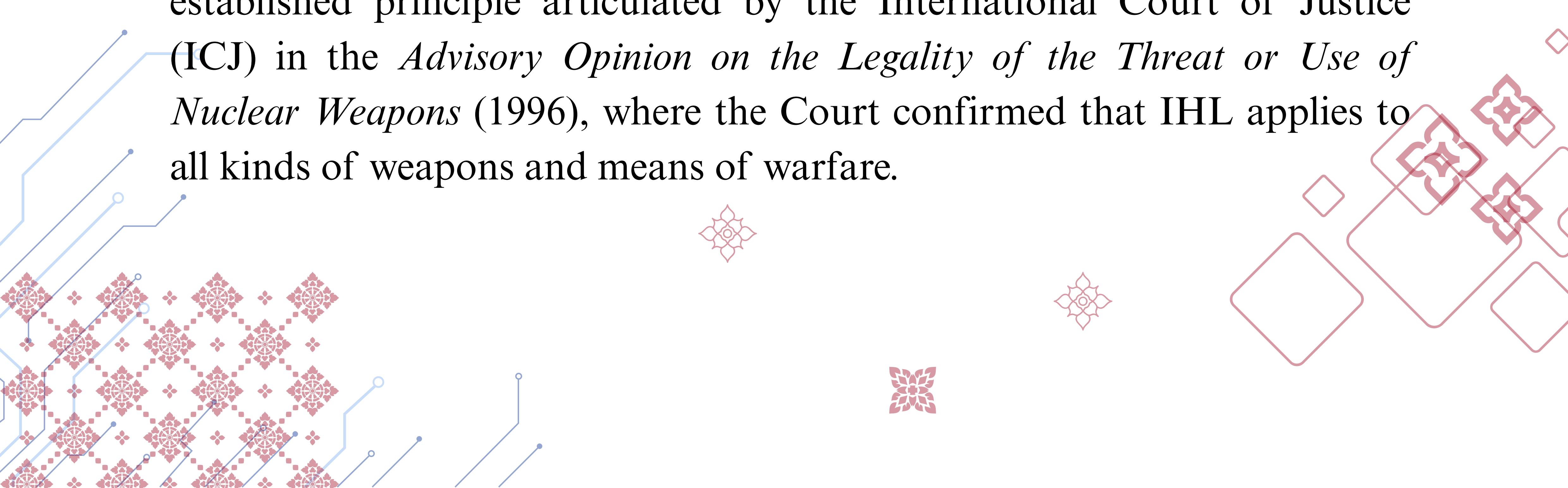
30. Thailand emphasizes that due diligence is an obligation of conduct, not of result. A State is not automatically responsible merely because a malicious cyber operation originates from its territory. Responsibility arises where a State, with knowledge and reasonable capacity to act, fails to take appropriate measures to prevent, mitigate or terminate such wrongful acts.

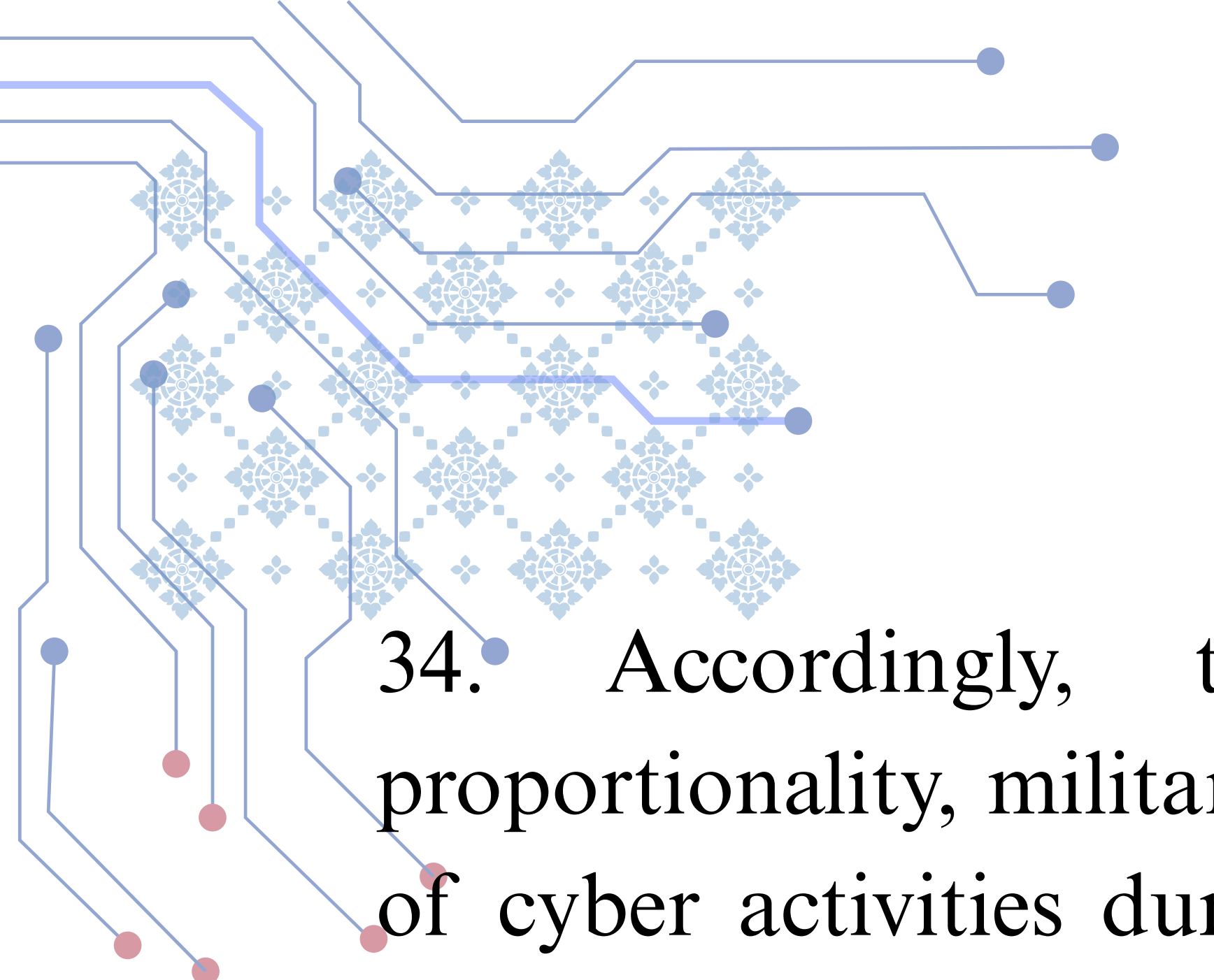
31. Thailand acknowledges the particular technical and operational challenges that cyberspace poses for the implementation of due diligence. These challenges include difficulties in detecting, attributing, and responding to malicious activities, particularly when operations are conducted anonymously or across multiple jurisdictions. Therefore, the scope and content of due diligence obligations must be interpreted contextually, taking into account each State's legal, technical, and institutional capacities.

VII. International Humanitarian Law

32. Thailand reaffirms its strong commitment to the fundamental principles and rules of International Humanitarian Law (IHL), which regulate the conduct of hostilities and seek to limit the effects of armed conflict for humanitarian reasons.

33. Thailand affirms that IHL applies to cyber operations conducted in the context of armed conflicts. Thailand's position is that IHL applies to all forms of warfare, including cyber warfare, consistent with the well-established principle articulated by the International Court of Justice (ICJ) in the *Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons* (1996), where the Court confirmed that IHL applies to all kinds of weapons and means of warfare.

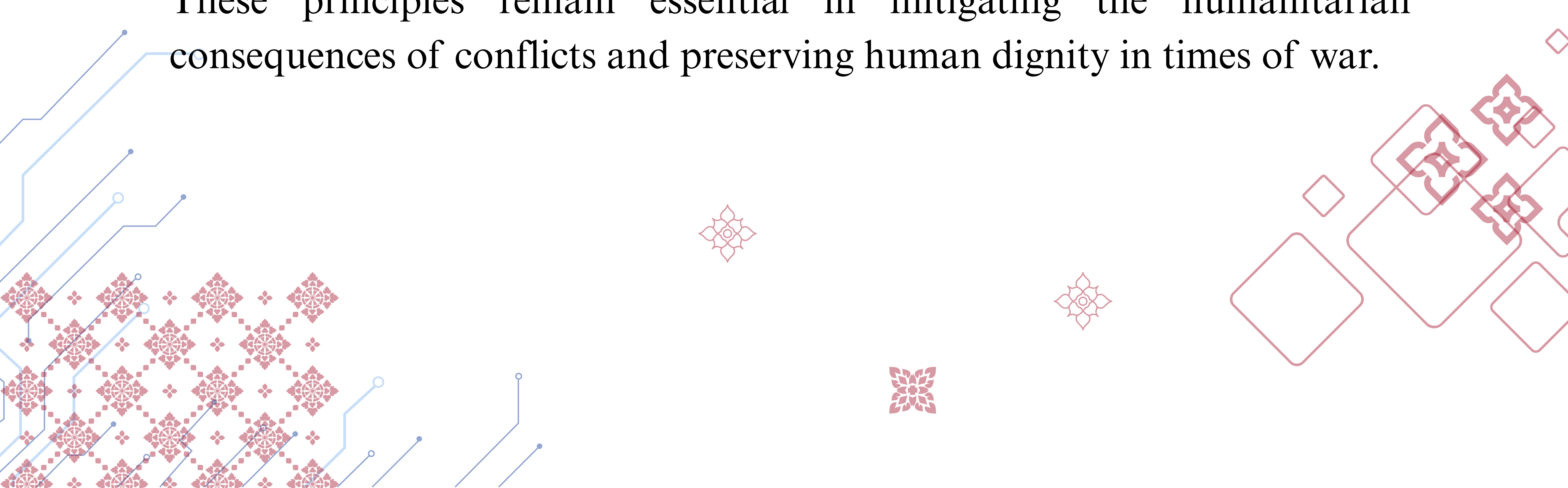




34. Accordingly, the foundational principles of distinction, proportionality, military necessity, and humanity must guide the conduct of cyber activities during armed conflicts, as they do for operations in other domains. These principles serve to protect civilian populations, civilian objects, and essential public services from the effects of hostilities.

35. Thailand acknowledges that the application of IHL to cyber operations presents specific technical and operational challenges. In particular, the fact that digital infrastructure is often used for both civilian and military purposes complicates the application of the principles of distinction and proportionality, requiring rigorous legal review and operational caution, especially regarding the identification of military objectives and the assessment of collateral damage. Cyber operations may only be directed against military objects and must not be conducted with indiscriminate effects on civilian populations and infrastructure. Further, the principle of proportionality prohibits cyber operations that may be expected to cause incidental civilian harm excessive in relation to the direct anticipated military advantage, and the principle of military necessity permits only those operations indispensable for achieving legitimate military objectives, without justifying violations of other IHL obligations.

36. Thailand stresses its commitment to applying IHL principles in cyberspace, including the prohibition of indiscriminate attacks, the necessity of distinguishing between combatants and civilians, and the obligation to minimize harm to civilian populations and infrastructure. These principles remain essential in mitigating the humanitarian consequences of conflicts and preserving human dignity in times of war.



37. Thailand further stresses that applying International Humanitarian Law to the use of ICTs in the context of armed conflicts does not in any way encourage or legitimize conflict. IHL regulates the conduct of hostilities with the sole aim of limiting human suffering and protecting those not participating in hostilities, without affecting the legality of the use of force under the Charter of the United Nations.

38. Recognizing the evolving nature of conflict and the reliance of modern societies on digital infrastructure, Thailand supports continued dialogue among States and relevant stakeholders, including the International Committee of the Red Cross (ICRC), to reach conclusion on and promote common understandings on the application of IHL in cyberspace.

VIII. International Human Rights Law

39. Thailand reaffirms that international human rights law (IHRL) applies in cyberspace, as it does in the physical world. States' activities in cyberspace must be conducted in accordance with their international human rights obligations, as expressed in the international human rights treaties to which they are a party, and in customary international law. This position is grounded in the Charter of the United Nations, the Universal Declaration of Human Rights, and the International Covenant on Civil and Political Rights (ICCPR), and is highlighted, among others, in United Nations Human Rights Council resolutions 53/29 (2023), 54/21 (2023), 20/8 (2012), which recognize that the same rights people have offline must also be protected online.

40. Thailand emphasizes that the protection of human rights in the digital environment is essential to the responsible use of ICTs and to preserving the openness, accessibility, and inclusivity of cyberspace, thereby fostering trust, innovation, and inclusive development in the digital domain, and promoting a secure, stable, and rights-respecting cyberspace. Thailand also welcomes the adoption of the UN Convention against Cybercrime which includes the elements related to human rights protection.

41. Thailand affirms that, in accordance with Article 2(1) of the ICCPR, each State Party must respect and ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the Covenant, without discrimination of any kind, such as the right to freedom of expression, the right to privacy, the right to freedom of association and peaceful assembly, and the right to access to information. At the same time, it must be taken into account that certain rights may be subject to restrictions, which are provided by the law and are necessary, in particular due to public security interest, protection of public order, health and morality or the protection of rights and freedoms of other persons.

IX. State Responsibility, Attribution, and Countermeasures

A. State Responsibility

42. Thailand affirms that the general rules of State responsibility under customary international law apply fully to State conduct in cyberspace. These rules are reflected in the Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA), adopted by the International Law Commission in 2001, and widely accepted by the international community.

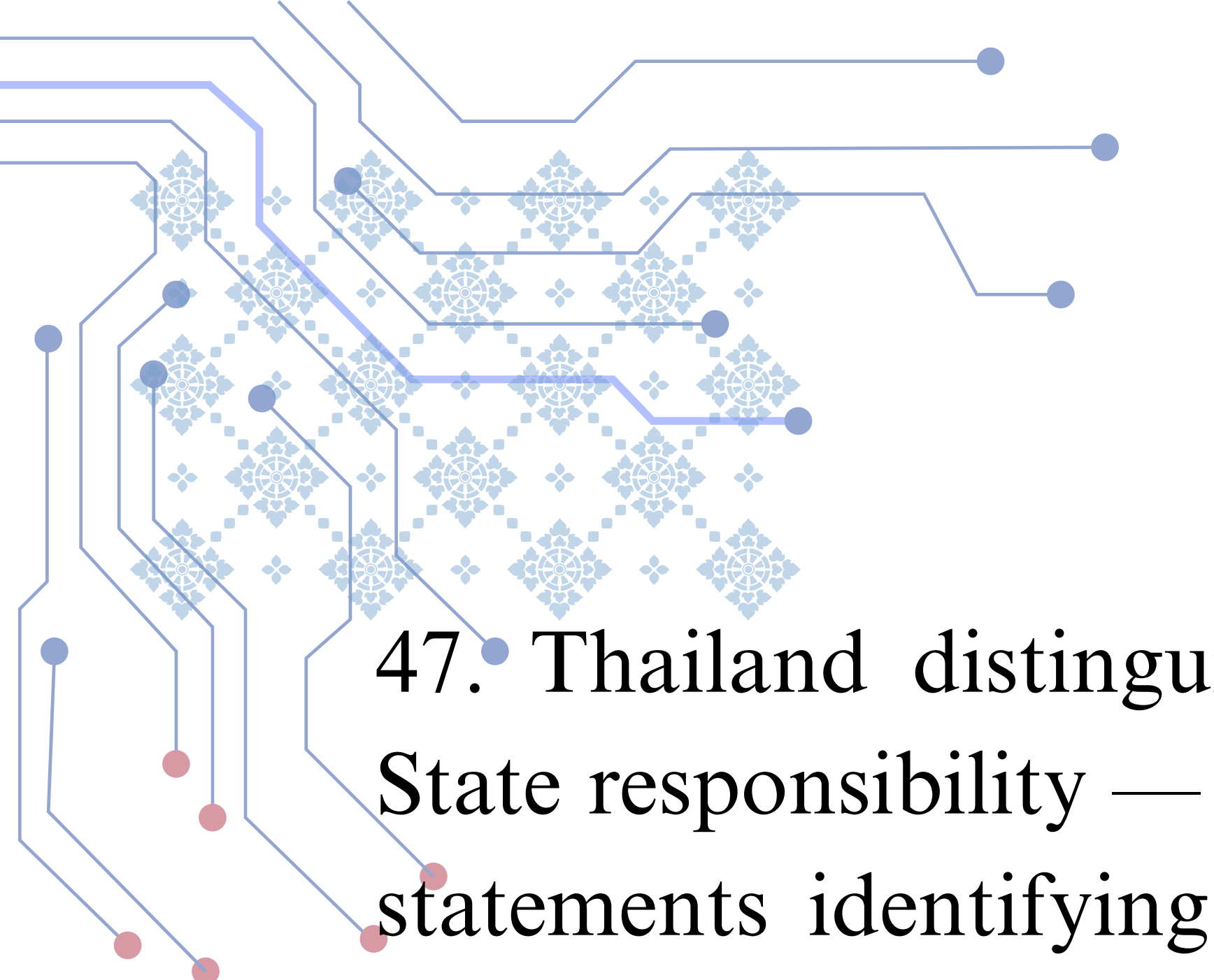
43. In particular, the principles governing attribution, breach of an international obligation, defenses such as force majeure or necessity, and the legal consequences of internationally wrongful acts apply equally in the cyber domain as in the physical world.

44. Thailand emphasizes that a State bears international responsibility if a cyber activity is attributable to it and constitutes a breach of an international obligation of the State. The fact that a State cyber activity is lawful under the domestic law of that State does not preclude it from being an international wrongful act under international law.

B. Attribution

45. Thailand affirms that attribution of cyber activities to a State must be consistent with the established principles of international law. A cyber operation is attributable to a State if it is carried out by its organs, or by persons or groups acting on its instructions, or under its direction or control, among other forms of attribution, in accordance with Articles 4 to 11 of ARSIWA.

46. Thailand acknowledges the significant technical and operational challenges involved in cyber attribution, including difficulties in identifying perpetrators, disguising operations, and investigating across jurisdictions. While recognizing that definitive evidence may not always be available due to these complexities, Thailand stresses that any attribution made for the purpose of invoking international responsibility should be undertaken carefully, based on the available information and surrounding circumstances.

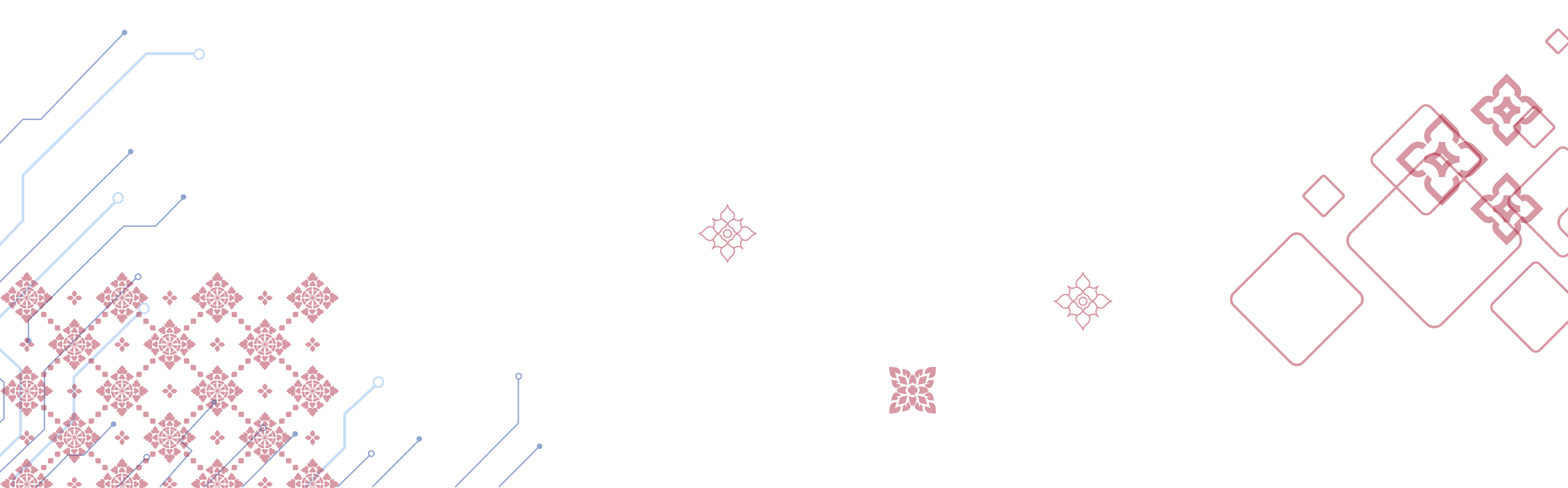


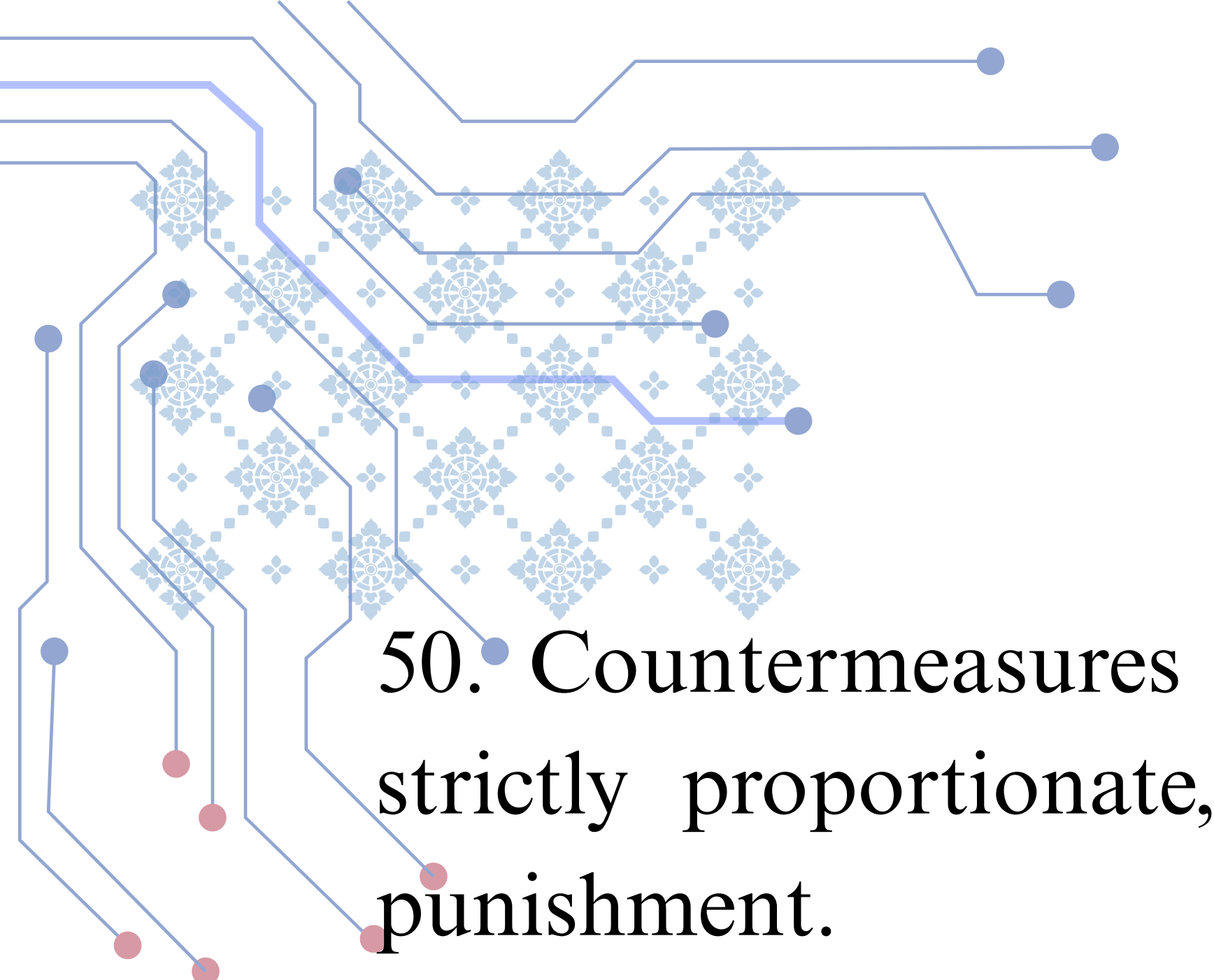
47. Thailand distinguishes between legal attribution — which engages State responsibility — and political attribution, such as public attribution statements identifying cyber operations or responsible actors. Thailand underscores the importance of cautious consideration of all relevant information in making any legal attribution to avoid escalation and preserve credibility.

48. Thailand further emphasizes that the mere fact that a cyber operation originates from a State's territory is not in itself sufficient under international law to attribute that operation to the State.

C. Countermeasures

49. Thailand acknowledges that, under customary international law, a State injured by an internationally wrongful act attributable to another State may resort to countermeasures to induce compliance with international obligations. This right is subject to strict conditions, including that countermeasures:

- must be proportionate to the injury suffered;
 - must be intended to induce the responsible State to comply with its obligations;
 - must not involve the threat or use of force, in accordance with Article 2(4) of the Charter of the United Nations;
 - must respect obligations relating to the protection of fundamental human rights and humanitarian obligations;
 - and, in principle, must be preceded by prior notification and an opportunity for the responsible State to cease its wrongful conduct.
- 



50. Countermeasures must be temporary, as far as possible reversible, strictly proportionate, and aimed solely at inducing compliance, not punishment.

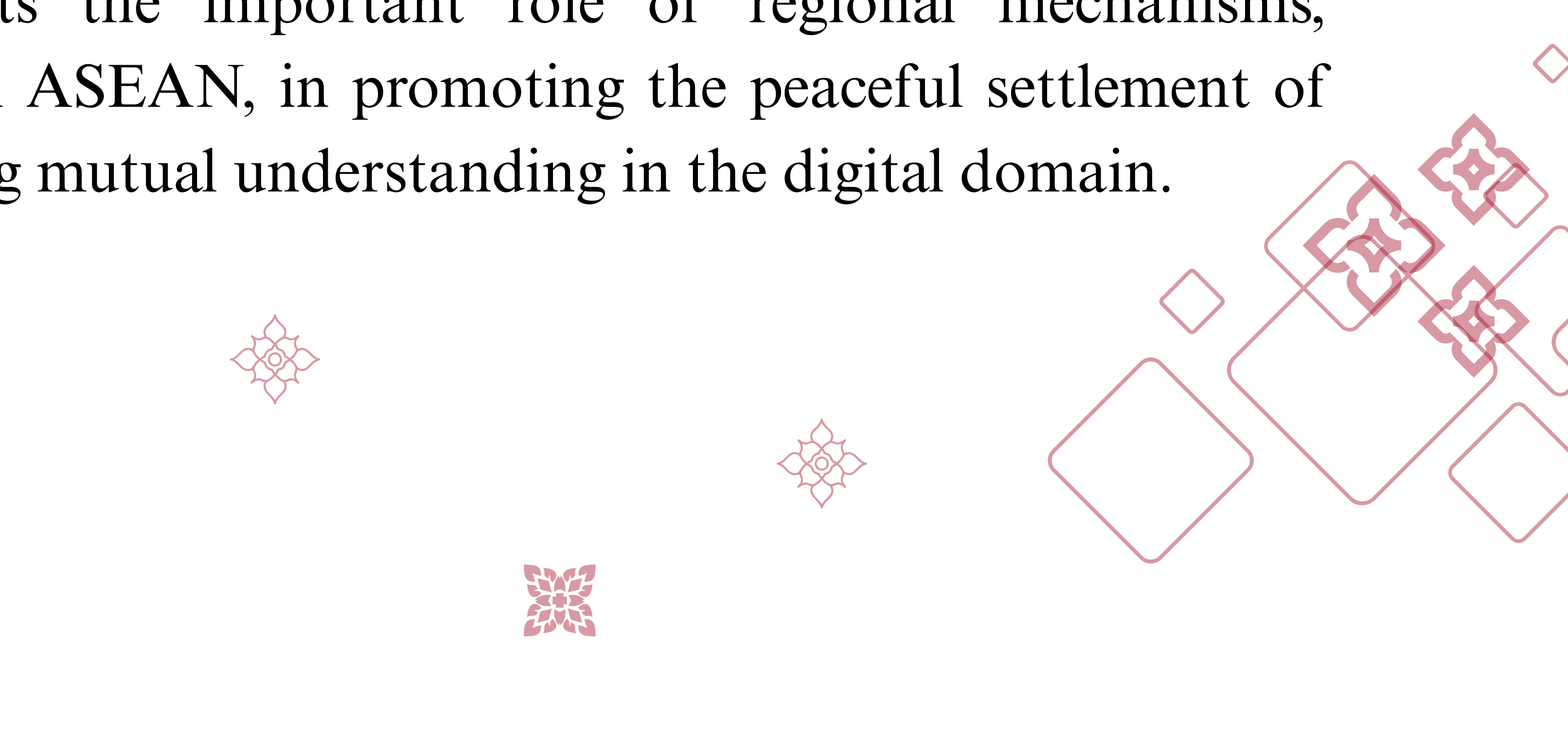
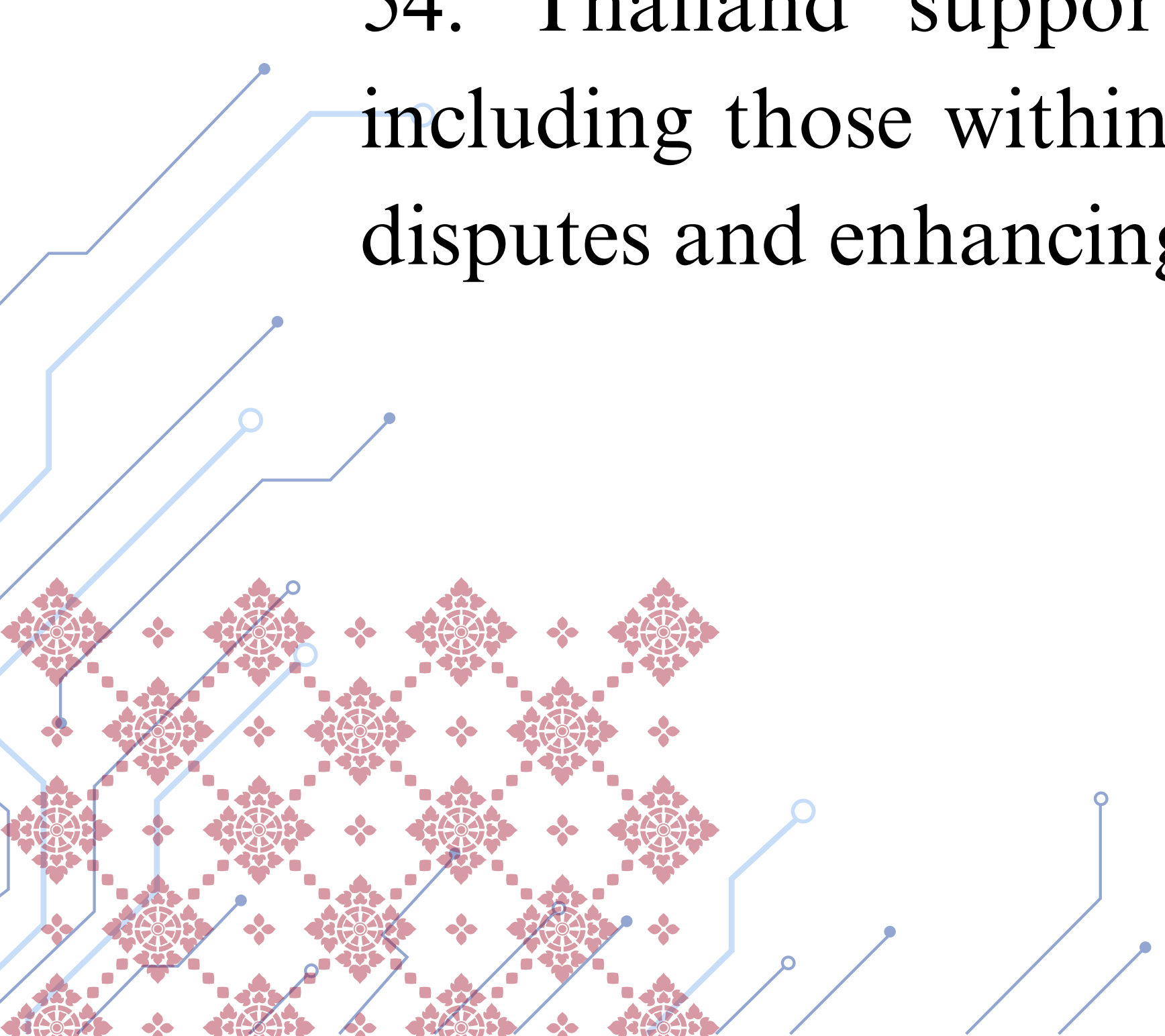
51. Thailand emphasizes that countermeasures should only be adopted as a measure of last resort, after efforts to resolve the dispute peacefully have been exhausted. Thailand encourages States to prioritize dialogue, transparency, mutual assistance, and confidence-building measures to address incidents in cyberspace, and to work through regional and international frameworks to prevent escalation and maintain international peace and security.

X. Peaceful Settlement of Disputes

52. Thailand reaffirms that, in accordance with Article 2(3) and Chapter VI of the Charter of the United Nations, States must settle their international disputes through peaceful means in a manner that does not endanger international peace, security, or justice.

53. Thailand emphasizes that a wide range of peaceful means is available to States, including negotiation, inquiry, mediation, conciliation, arbitration, judicial settlement, and recourse to regional agencies or arrangements. Thailand encourages States to prioritize dialogue, cooperation to prevent escalation and to address incidents in cyberspace in a peaceful, transparent, and constructive manner.

54. Thailand supports the important role of regional mechanisms, including those within ASEAN, in promoting the peaceful settlement of disputes and enhancing mutual understanding in the digital domain.



XI. Conclusion

55. This position reflects Thailand's current views on the key principles of international law as they apply to State activities in cyberspace. This position constitutes an exercise of legal interpretation and does not create new obligations for Thailand.

56. Thailand recognizes that the evolving nature of the digital domain may raise new challenges and reaffirms its openness to continuing dialogue, exchange of views, and cooperation with other States and stakeholders. Thailand remains committed to adapting legal interpretations where necessary while preserving fundamental legal principles.

57. Thailand emphasizes the importance of international cooperation, confidence-building measures, and capacity-building initiatives to bridge gaps among States, enhance mutual understanding, and strengthen collective resilience against emerging threats. Thailand stands ready to engage actively and contribute positively to international discussions on these matters to ensure that cyberspace remains open, secure, stable, peaceful, and accessible to all.

* * * * *

