The International Responsibility of States for Cyberattacks: A Comparative Study of International Practice and Iran's National Instruments

Roukhsare Vaziri Goodarzi

PhD student in International Law, Faculty of Law, Qom Branch, Islamic Azad University, Qom, Iran. (Corresponding Author)

Email: rokhsarehvazirig@gmail.com

Mohamad Arab Tat

PhD student in International Law, Faculty of Law, Damghan Branch, Islamic Azad University, Damghan, Iran.

Email: mohamadarabtat1997@gmail.com

Fatemeh Zibayienezhad

PhD student in International Law, Department of Law, Mofid University, Qom, Iran.

Email: Zibaeinejad@mofidu.ac.ir

DOI: https://doi.org/10.22096/law.2026.2089138.2374

Received Date: 14/07/2026

Accepted Date: 26/05/2026

Introduction

The rapid expansion of information and communication technologies and the growing dependence of states on cyber infrastructure have made cyber attacks an important concern for international law. Unlike traditional hostile conduct, cyber operations can be conducted across borders through concealed identities, intermediary servers, compromised networks, and infrastructure located in third states. These features create difficulties for applying traditional rules on state responsibility, particularly concerning sovereignty, non-intervention, the prohibition of the use of force, and attribution of wrongful conduct to states. Iran has also developed domestic strategic and legal approaches to cyber defense in response to cyber threats against critical infrastructure. Against this background, this study examines state responsibility for cyber attacks through a comparative analysis of international practice and Iranian national instruments.

Problem Statement

The central problem is the difficulty of establishing the international responsibility of a state for a cyber attack, particularly where the operation is carried out by non-state actors, hacker groups, or state-supported cyber proxies. Cyber attribution involves two distinct but related stages. Technical attribution seeks to identify the source or actor behind an operation, whereas legal attribution requires establishing a legally relevant connection between that conduct and a state. False identities, intermediary infrastructure, third-country servers, and false-flag operations make this connection difficult to establish. The study therefore asks whether existing rules of international law, especially the effective control standard and the duty of due diligence, are sufficient to address the characteristics of cyber operations, and how the Iranian legal framework responds to these challenges.

Main Argument

The study argues that the effective control standard remains an important basis for attributing the conduct of non-state cyber actors to a state. However, the concealed and transnational nature of cyber operations makes reliance on this standard alone difficult in practice. Complementary approaches, particularly the duty of due diligence, are therefore important where direct attribution cannot be established. The study further argues that, concerning the threshold of the use of force and the right of self-defense, the Iranian approach shows considerable convergence with an effects-based approach in international legal discourse. The scale and consequences of a cyber operation, rather than the technological means through which it is conducted, are therefore central to determining its legal significance.

Methodological Approach

This research adopts a descriptive-analytical method with a comparative approach. It first examines the legal characterization of cyber attacks and the two principal elements relevant to state responsibility: the existence of an internationally wrongful act and its attribution to a state. It then analyzes the difficulties of technical and legal attribution, focusing particularly on the effective control doctrine and the duty of due diligence. The study subsequently examines the international normative framework concerning cyber operations, including the Tallinn Manual, relevant United Nations documents, and approaches to sovereignty, non-intervention, the use of force, and self-defence. These principles are compared with Iranian strategic documents and legal instruments concerning cyber defence. The analysis also considers the Iranian criminal-law framework and its capacity to address transnational cyber attacks, before examining countermeasures and diplomatic responses.

Structure and Analytical Path of the Article

The article moves from the general legal characterization of cyber attacks to the specific question of state attribution. It first distinguishes cyber operations that may produce consequences comparable to conventional armed attacks from operations below the threshold of an armed attack.

It then examines the technical and legal obstacles to attribution and considers effective control in relation to non-state cyber actors. The following part places the international framework alongside Iranian national instruments, focusing on cyber sovereignty, due diligence, and the Iranian approach to self-defense. The

analysis then considers the criminal and deterrent dimensions of Iran's domestic framework, particularly its emphasis on individual criminal responsibility. Finally, it compares international and Iranian approaches to the threshold of the use of force and to countermeasures against cyber operations below that threshold. This structure connects attribution with the broader question of how states can respond lawfully to cyber attacks.

Conclusion

The comparative analysis demonstrates that cyberspace has created significant difficulties in applying traditional concepts of international responsibility to contemporary cyber operations. The most persistent difficulty lies in the gap between technical and legal attribution. Although effective control remains a significant legal standard, establishing direct state control over cyber proxies may be particularly difficult because of the concealed and decentralized nature of cyber operations. The duty of due diligence therefore assumes particular importance where a state fails to take reasonable measures to prevent its territory or cyber infrastructure from being used for internationally harmful activities. At the same time, the analysis identifies convergence between the Iranian position and an effects-based approach concerning the threshold of the use of force and self-defense, particularly where cyber operations cause serious human or material damage to critical infrastructure.

Findings and Recommendations

The study finds that the Iranian legal framework contains important capacities for addressing cyber threats, including mechanisms for protecting critical infrastructure and criminal-law provisions applicable to cyber offences. Nevertheless, its principal limitation is the absence of a clear and comprehensive framework specifically designed to establish the international responsibility of states for cyber operations. Iranian criminal legislation primarily focuses on individual offenders and does not provide an independent mechanism for attributing cyber conduct to states as subjects of international law. The study also finds that Iran lacks a sufficiently clear and specialized framework for non-military, state-oriented countermeasures against cyber operations below the threshold of an armed attack. International practice, by contrast, has developed legal and diplomatic responses to such operations. Accordingly, the study recommends further development of Iran's legal framework concerning state attribution, due diligence, and cyber countermeasures, together with more systematic use of legal and diplomatic mechanisms alongside technical and security measures. Such development would strengthen Iran's ability to respond to cyber attacks through a coherent legal framework and to address state-supported cyber operations.