

OPEN PEER REVIEW

Iran's Legislative Criminal Policy on Cyber Espionage

Seyed Amir. Hashemi^{1*}  Saeid. Atazadeh²  Mahmud. Ghayomzadeh³ 

¹ PhD Student, Department of Criminal Law and Criminology, Narag Branch, Islamic Azad University, Narag, Iran

² Associate Professor, Department of Criminal Law and Criminology, NAJA Institute of Law Enforcement Sciences and Social Studies, Tehran, Iran

³ Professor, Department of Education and Law, Saveh Branch, Islamic Azad University, Saveh, Iran

* Corresponding author email address: saeidbahjat@yahoo.com


Received: 2023-04-09

Revised: 2023-06-14

Accepted: 2023-06-24

Published: 2023-07-01


EDITOR:

Yuyu Zheng 

School of International Relations, University of St Andrews, St Andrews, London, United Kingdom

yuyuzheng@gmail.com


REVIEWER 1:

Nabeel Bani-Hani 

Faculty of Education Specialization, Wasit University, Wasit, Iraq

nabeelhani@uowasit.edu.iq

REVIEWER 2:

Vanessa Indama 

Public Administration Department, Basilan State College, Isabela City, Basilan, Philippines

vanesindama@gmail.com

1. Round 1

1.1. Reviewer 1

Reviewer:

The statement, "Cyber espionage is one of the most prevalent cyber activities." lacks supporting evidence. Providing statistical data or references to studies that quantify cyber espionage incidents would enhance the credibility of this claim.

The phrase, "Cyber espionage appears to be the same as traditional espionage, merely occurring in cyberspace." oversimplifies the issue. Consider elaborating on the key differences between traditional and cyber espionage beyond just their operational environment.

The statement, "Developing and coordinating countermeasures against cyber espionage require tools and expertise commensurate with the offenders operating in this domain." is a strong claim but lacks specific policy recommendations. Consider adding a brief mention of what types of tools and expertise are required.

The claim that "mere occurrence of a criminal act does not automatically imply the presence of mens rea." is legally sound, but it would be helpful to clarify the distinction between general intent (*dolus generalis*) and specific intent (*dolus specialis*) within espionage-related offenses.

The phrase, "The first category refers to unauthorized access to systems containing classified data, while the second category involves unauthorized access to the classified data itself." could be expanded by clarifying how Iranian law differentiates between these offenses in terms of penalties.

The statement, "Thus, if an individual mistakenly believes that the data is ordinary, they do not commit this crime." raises an important legal question—does Iranian law recognize a defense based on lack of knowledge about the classification of data? Clarifying this point would be helpful.

The explanation could be strengthened by discussing whether Iranian law applies different penalties for gross negligence versus simple negligence in cases of data mismanagement.

Authors revised the manuscript and uploaded the document.

1.2. Reviewer 2

Reviewer:

The phrase, "This process aims to identify a nation's strengths and weaknesses to block avenues for empowerment and exploit vulnerabilities for destructive purposes." is quite general. Clarify whether this applies exclusively to state-sponsored espionage or if it includes corporate espionage as well.

The proposed definition of cyber espionage could be refined by incorporating the element of intent more explicitly. For example, specifying whether unauthorized access must be performed with malicious intent or if accidental access also falls under this definition.

The reference to the Qur'an 17:15 to justify the principle of legality in criminal law is interesting but may not be universally applicable in a legal discussion. Consider integrating references to secular legal principles, such as those in international conventions on cybercrime.

The mention of "Articles 6, 7, and 8 of the Islamic Penal Code" should be followed by a brief description of their content to ensure clarity for readers unfamiliar with Iranian legal statutes.

The sentence, "The offender must have positively engaged in a material act, first by knowingly and deliberately acquiring secrets that were legally prohibited from their knowledge, and then by knowingly and deliberately transferring these classified secrets to others." could benefit from an example or case study illustrating such an act.

The explanation regarding "accessing, obtaining, or intercepting classified content in transit" would benefit from discussing whether merely attempting to access such data constitutes an offense, even if access is unsuccessful.

The sentence, "Making such data available to unauthorized persons shall be punishable by imprisonment ranging from two to ten years." lacks nuance regarding whether intent or negligence affects sentencing severity. Consider elaborating on whether intent must be proven.

The discussion on "disclosure" versus "making data available" would benefit from an illustrative example that distinguishes these terms in legal practice.

The phrase, "The most evident necessity is the requirement for proper legislation regarding cyber espionage." is valid, but consider adding a comparison with how other legal systems, such as the U.S. or EU, have adapted to cyber espionage threats.

The claim that "Many countries have explicitly criminalized economic espionage, recognizing its significance in the digital age." should be supported with specific examples of countries and relevant legislation, such as the U.S. Economic Espionage Act of 1996.

The question posed—"Should there still be a distinction between military and non-military personnel when committing cyber espionage?"—is an important legal issue. However, the article does not provide an argument supporting either position. Consider elaborating on potential legal or policy recommendations.

Authors revised the manuscript and uploaded the document.

2. Revised

Editor's decision: Accepted.

Editor in Chief's decision: Accepted.

