

OPEN PEER REVIEW

Study of Opportunities and Challenges of Cyberspace and Its Impact on Cybercrimes in the Armed Forces of Iran

Mohammad. Amirmohammadi¹ , Saleh. Abdinejad^{2*} , Alireza. Shokrbeigi³ 

¹ PhD Student, Department of Criminal Law and Criminology, Kish International Branch, Islamic Azad University, Kish Island, Iran

² Assistant Professor, Department of Criminal Law and Criminology, Amin University of Law Enforcement Sciences, Tehran, Iran

³ Assistant Professor, Department of Criminal Law and Criminology, Payam Noor University, Kermanshah, Iran

* Corresponding author email address: silahlawyer29@gmail.com


Received: 2024-10-06

Revised: 2024-11-20

Accepted: 2024-11-27


Published: 2025-01-01

EDITOR:

Eman Shenouda 

Associate Professor, Department of Psychology, Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan, Iran
ens01@fayoum.edu.eg


REVIEWER 1:

Patrika Handique 

Patent Information Centre, Intellectual Property Facilitation Centre, Chhattisgarh Council of Science & Technology, Raipur, Chhattisgarh, India

Patriandique@gmail.com

REVIEWER 2:

Thanuja Kulasooriya 

Department Soil Science, Faculty of Agriculture, University of Ruhuna, Mapalana, Kamburupitiya, Sri Lanka

thkulasooriya@soil.ruh.ac.lk

1. Round 1

1.1. Reviewer 1

Reviewer:

The introduction provides a broad overview of cyberspace and cybercrimes but lacks clarity on the specific impact of these crimes within the armed forces. It would be beneficial to explicitly state why cybercrimes in military contexts differ from those in civilian domains.

The study's research question—"What are the most significant characteristics of cyberspace, and how do these characteristics influence cybercrimes within the armed forces?"—is too general. Consider refining it to specify whether the focus is on legal, operational, or strategic aspects of cybercrimes within military institutions.

The discussion on international cybercrime frameworks is informative but lacks an analysis of Iran's stance on these treaties. It would be beneficial to examine whether Iran has adopted or rejected specific international conventions and the implications of these choices.

The definition of military crimes should distinguish between offenses that have a direct impact on national security and those that primarily affect internal military discipline. A comparative approach with U.S. or EU military cybercrime laws would provide valuable insights.

The discussion on the Deep Web and anonymity lacks direct relevance to military cybercrimes. Instead, it would be more effective to discuss how military personnel might use encrypted communication tools and the associated risks.

The section highlights government control but lacks a discussion on how military institutions balance security concerns with digital freedoms. Including references to defense policies on cybersecurity training would be useful.

Authors revised the manuscript and uploaded the document.

1.2. Reviewer 2

Reviewer:

The argument regarding the need for revised criminal policy is compelling, but the paragraph lacks a direct connection to existing gaps in legislation. A comparison with international frameworks, such as NATO's cyber defense policies or the Budapest Convention, would strengthen the argument.

The section cites constitutional provisions but does not adequately contextualize how these legal frameworks shape cyber operations. Consider integrating an analysis of military digital infrastructure and its role in national cybersecurity.

While citing Gibson's literary origins of cyberspace is valuable, it would be more relevant to include an academic definition from cybersecurity literature, such as definitions provided by the National Institute of Standards and Technology (NIST) or the International Telecommunication Union (ITU).

The section provides multiple definitions of cybercrime but lacks a legal framework comparison. Consider including how Iranian military law defines cyber offenses in contrast to civilian cyber laws.

The classification of cyberspace is useful but should include more detail on military-specific cyber threats, such as cyber-espionage and cyber-warfare tactics.

The discussion on military identity security is valuable, but it does not sufficiently address countermeasures. Adding references to information security protocols and classified data management policies would be beneficial.

The section outlines Iranian cyber laws but does not compare them with international cyber espionage legislation. A brief comparison with U.S. laws such as the Computer Fraud and Abuse Act (CFAA) would enhance the discussion.

The discussion on extradition is important, but it does not address cybercriminals within the armed forces. How does Iran handle military personnel who commit cybercrimes while stationed abroad?

Authors revised the manuscript and uploaded the document.

2. Revised

Editor's decision: Accepted.

Editor in Chief's decision: Accepted.