QUARTERLY, PEER REVIEWED
al-amir
ISSN(P): 2790-931X ISSN(E): 2790-9328
E-Mail: editor.alamir@gmail.com

اسرائیل-امریکہ اتحاد اور ایران کے خلاف اے آئی وسائبر جنگ: بین الاقوامی قانون اور علاقائی سلامتی کا تنقیدی جائزہ

The Israel–US Alliance and AI-Cyber Warfare against Iran: A Critical Analysis of International Law and Regional Security

Kanwar Muhammad Akif
Lecturer of Islamic Studies at Government Boys Degree College Ghotki, Sindh, Pakistan / Doctoral Candidate, Shah Abdul latif University Khairpur, Pakistan. Email: kanwarakif1@gmail.com

Dr. Zain-ul -Abdin Arijo
Associate Professor, Institute of Islamic Studies, Shah Abdul Latif University, Khairpur, Pakistan. Email: zain.arijo@salu.edu.pk

Submission Date: 02 June 2026
Review Date: 03 June 2026
Acceptance Date: 07 June 2026
Publication Date: 10 June 2026

Article Link: https://alamir.com.pk/index.php/ojs/article/view/319

Abstract:
This paper provides a comprehensive analysis of the joint military strikes on the Islamic Republic of Iran (IRI) conducted on February 28, 2026, comprising Operation Epic Fury (United States) and Operation Lion's Roar (Israel).

It critically examines the strategic integration of artificial intelligence (AI) and offensive cyber operations within high-intensity kinetic campaigns, assessing their profound implications for international humanitarian law (IHL), specifically jus ad bellum and jus in bello, and the broader regional security architecture of West Asia.

The study elucidates the operationalization of Israel's Lavender and The Gospel networks, which deployed real-time targeting systems in synergy with AI-driven platforms such as Palantir's Maven Smart System, augmented by Anthropic's Claude AI. Conversely, the analysis delves into Iran's asymmetrical "mosaic defense" doctrine and its "Electronic Operations Room" (EOR). This defensive framework was coordinated by the Iranian advanced persistent threat (APT) group Void Manticore (Handala), which executed a devastating "Living-off-the-Cloud" (LotC) cyberattack weaponizing Microsoft Intune against Stryker Corporation. Furthermore, the report critically evaluates a U.S. State Department legal memorandum authored by Reed Rubinstein, which challenges customary international law by rejecting the doctrine of 'ongoing armed conflict' and redefining the rigid parameters of 'imminence' and 'proportionality.' Ultimately, this research posits that the weaponization of the cyber-kinetic domain has fundamentally disrupted regional deterrence paradigms, thereby necessitating an urgent recalibration of international governance frameworks regarding autonomous military technologies.

Keywords: Operation Epic Fury, Artificial Intelligence, Cyber Warfare, Mosaic Defense, Living-off-the-Cloud, International Humanitarian Law, Stryker Corporation, Regional security complex.

تعارف(Introduction)

گذشتہ چند دہائیوں سے مشرقِ وسطیٰ (Middle East) کے کئی ممالک جغرافیائی و سیاسی کشیدگی کے باعث مسلسل جنگوں، اندرونی کشمکش اور امن و امان کے سنگین بحرانوں کا شکار رہے ہیں۔ تاہم، فروری 2026 میں ایک ایسی جنگ کا آغاز ہوا جو دنیا کی تاریخ میں بالکل نئی اور مختلف تھی، اس جنگ میں روایتی ہتھیاروں (جیسے بم اور گولیوں) کے ساتھ ساتھ کمپیوٹر ہیکنگ اور مصنوعی ذہانت (AI) کا بھی بھرپور استعمال کیا گیا۔

یہ بڑی جنگ اچانک شروع نہیں ہوئی، بلکہ یہ پرانے واقعات کا تسلسل تھی۔ ان واقعات میں اکتوبر 2023 میں حماس اور اسرائیل کی جنگ، یمن کے حوثی گروپ کی طرف سے بحیرہ احمر (سمندر) میں تجارتی جہازوں پر مسلسل حملے، اور جنوری 2026 میں ایران کے اندر حکومت کے خلاف ہونے والے عوامی مظاہروں کو ایرانی حکومت کی طرف سے طاقت کے ذریعے سختی سے کچلنا شامل تھے۔

جب ایرانی حکومت نے اپنے ہی شہریوں کے خلاف طاقت کا استعمال کیا، تو امریکی صدر ڈونلڈ ٹرمپ نے اس بات کو بہانہ بنا کر مشرقِ وسطیٰ میں اپنی فوجیں جمع کرنا شروع کر دیں۔ یہ سنہ 2003 کی عراق جنگ کے بعد مشرقِ وسطیٰ میں امریکہ کی سب سے بڑی فوجی تیاری تھی۔ اس فوجی تیاری کے ساتھ ساتھ، جنیوا اور عمان کے شہروں میں ایران کے ساتھ ایٹمی پروگرام پر خفیہ بات چیت کا ایک ڈرامہ بھی رچایا گیا، تاکہ ایران کا دھیان بٹایا جا سکے اور وہ جنگ کی تیاری نہ کر سکے۔[1]

آخر کار، 28 فروری 2026 کی صبح، امریکہ اور اسرائیل نے مل کر ایران پر فوجی حملہ کر دیا۔ اس مہم کو امریکہ نے 'آپریشن ایپک فیوری' (Operation Epic Fury) اور اسرائیل نے 'آپریشن لائنز رور' (Operation Lion's Roar) کا نام دیا۔[2]

حملے کے بالکل شروع میں ہی تہران پر ہوائی حملے کیے گئے اور ایران کے سب سے بڑے لیڈر آیت اللہ علی خامنہ ای اور سیکیورٹی کے نائب وزیر سید یحییٰ حسینی پاشاہی کو نشانہ بنا کر ہلاک کر دیا گیا۔ اس کا مقصد یہ تھا کہ ایرانی حکومت اور سیکیورٹی کا پورا نیٹ ورک ایک ہی جھٹکے میں مفلوج ہو جائے۔[3]

اس کے جواب میں ایران نے بھی بڑی تعداد میں ڈرونز اور گائیڈڈ میزائل فائر کیے۔ ان میزائلوں نے اسرائیل کے علاوہ بحرین، متحدہ عرب امارات اور عراق میں قائم امریکی فوجی اڈوں کو نشانہ بنایا۔ اس کے ساتھ ہی ایران نے تیل کی سپلائی کے اہم راستے یعنی 'آبنائے ہرمز' کو بھی بند کر دیا، جس سے دنیا بھر میں سامان اور تیل کی آمد و رفت شدید متاثر ہوئی اور عالمی مارکیٹ میں خام تیل کی قیمت بڑھ کر 118 ڈالر فی بیرل سے تجاوز کر گئی۔[4]

مقاصدِ تحقیق (Research Objectives)

اس تحقیقی مطالعے کا بنیادی مقصد فروری 2026 میں ایران کے خلاف شروع ہونے والے امریکہ-اسرائیل مشترکہ فوجی آپریشنز ('ایپک فیوری' اور 'رورنگ لائن') کے کثیر جہتی اثرات (Multidimensional impacts) کا علمی اور تنقیدی احاطہ کرنا ہے اس بنیادی ہدف کے حصول کے لیے درج ذیل مقاصد متعین کیے گئے ہیں۔

1. مصنوعی ذہانت (AI) کے جنگی استعمال کا آپریشنل تجزیہ: اس تحقیق کا پہلا مقصد یہ معلوم کرنا ہے کہ 'دی گوسپل (The Gospel)' اور 'لیونڈر (Lavender)' جیسے الگورتھمک سسٹمز نے روایتی ہدف سازی (Targeting) کے عمل کو کس طرح تبدیل کیا اور اس سے حملوں کی رفتار اور تباہی کی صلاحیت میں کتنا اضافہ ہوا۔

2. سائبر مفلوج کاری (Digital Sabotage) کے اثرات کی پیمائش: مہم کے دوران ایران کے انٹرنیٹ انفراسٹرکچر کو 4 فیصد تک گرانے والے ڈیجیٹل بلیک آؤٹ کی تکنیکی حکمتِ عملی کا جائزہ لینا اور یہ دیکھنا کہ اس نے ایران کے فضائی دفاعی اور کمانڈ سسٹمز کو کس حد تک کمزور کیا۔

3. بین الاقوامی قانون (Jus ad Bellum) کا تنقیدی جائزہ: اقوامِ متحدہ کے چارٹر کے آرٹیکل 51 کے تحت "پیشگی دفاع " (Anticipatory Self-Defense) کے امریکی و اسرائیلی دعوؤں کا قانونی تجزیہ کرنا اور یہ پرکھنا کہ کیا یہ اقدامات بین الاقوامی انسانی قانون (IHL) کے اصولوں پر پورا اترتے ہیں یا یہ قانونی انحطاط (Legal Erosion) کا باعث بن رہے ہیں۔

4. علاقائی سلامتی کے نئے ڈھانچے کا مطالعہ: اس تنازع کے نتیجے میں مشرقِ وسطیٰ میں ابھرنے والے نئے "سائبر سیکیورٹی کمپلیکس"، خلیجی ممالک اور اسرائیل کے مابین ڈیجیٹل تعاون، اور آبنائے ہرمز (Strait of Hormuz) جیسے اہم بحری راستوں پر پڑنے والے معاشی وتزویراتی (Strategic) اثرات کا تعین کرنا۔

مسئلہ تحقیق (Research Problem)

مشرقِ وسطیٰ میں روایتی جنگی طریقوں کی جگہ مصنوعی ذہانت (AI) اور سائبر وارفیر کے نظام کا اچانک شامل ہونا عالمی امن اور بین الاقوامی قانون کے لیے ایک بہت بڑا بحران بن کر ابھرا ہے۔ اصل مسئلہ یہ ہے کہ موجودہ بین الاقوامی قوانین اور اقوامِ متحدہ کا چارٹر (خاص طور پر آرٹیکل 51) اس دور میں لکھے گئے تھے جب جنگیں صرف روایتی ہتھیاروں، ٹینکوں اور فوجیوں سے لڑی جاتی تھیں۔[5]

جب فروری 2026 میں امریکہ اور اسرائیل نے مشترکہ طور پر ایران کے خلاف 'ایپک فیوری' اور 'رورنگ لائن' جیسے آپریشنز شروع کیے، تو انہوں نے الگورتھم کے ذریعے اہداف مقرر کیے اور پورے ملک کا انٹرنیٹ مواصلاتی نظام مفلوج کر دیا۔

اس نئی صورتِ حال نے دو بڑے اور سنگین مسائل کو جنم دیا ہے جن کا حل تلاش کرنا اس وقت کی سب سے بڑی ضرورت ہے۔

قانونی خلا اور انحطاط :(Legal Vacuum) پہلا بڑا مسئلہ یہ ہے کہ جب کوئی ریاست کسی دوسری ریاست پر ڈیجیٹل حملہ کر کے اس کا پورا نظامِ زندگی معطل کر دیتی ہے، تو بین الاقوامی قانون میں اس بات کی حدیں واضح نہیں ہیں کہ اسے باقاعدہ " مسلح حملہ " مانا جائے یا نہیں۔ "پیشگی دفاع (Anticipatory Self-Defense) " کے نام پر کیے جانے والے یہ اقدامات قانونِ جنگ کی روح کو شدید نقصان پہنچا رہے ہیں اور اس سے مستقبل میں کسی بھی ملک کے خلاف یکطرفہ کاروائی کا خطرناک راستہ کھل رہا ہے۔

علاقائی سلامتی کا بگاڑ :(Regional Instability) دوسرا مسئلہ یہ ہے کہ مصنوعی ذہانت کے خودکار سسٹمز (جیسے لیونڈر) انسانوں کے بجائے ڈیٹا کی بنیاد پر حملوں کے فیصلے کر رہے ہیں، جس سے عام شہریوں کے متاثر ہونے کا خطرہ بے پناہ بڑھ گیا ہے۔ اس ٹیکنولوجیکل (**Technological**) برتری نے مشرقِ وسطیٰ میں طاقت کا توازن بگاڑ دیا ہے، جس کے نتیجے میں پراکسی نیٹ ورکس کی فعالیت اور آبنائے ہرمز جیسے بین الاقوامی بحری راستوں میں معاشی عدم استحکام پیدا ہو رہا ہے۔

مختصراً یہ کہ ٹیکنالوجی کی رفتار اتنی تیز ہے کہ ہمارے بین الاقوامی قوانین اور سیکیورٹی کے پرانے فریم ورک اس کا ساتھ دینے میں ناکام ہو چکے ہیں، اور یہی اس تحقیق کا بنیادی مسئلہ ہے جس کا گہرا تجزیہ کرنا مقصود ہے۔

سابقہ تحقیق کا جائزہ(Literature Review)

مشرقِ وسطیٰ میں آج کل جو کمپیوٹر اور انٹرنیٹ کی جنگ (سائبر وار) چل رہی ہے، اس کی ابتداء بنیادی طور پر 2010 میں 'سٹکس نیٹ ' (Stuxnet)نامی وائرس کے حملے سے ہوئی۔ احمد موہی نے اپنی تحقیق میں بتایا ہے کہ یہ تاریخ میں پہلی بار ہوا تھا جب کسی حکومت نے ایک ایسا وائرس بنایا جس کا مقصد دشمن کی مشینوں اور فیکٹریوں کو تباہ کرنے کے لیے اسے ایک باقاعدہ ہتھیار کے طور پر استعمال کرنا تھا۔[6]

موہی نے یہ بھی سمجھایا کہ ڈیجیٹل حملوں کی کوئی سرحد نہیں ہوتی۔ اسی وجہ سے عرب دنیا کو اب ایک نئے قسم کے سیکیورٹی خطرے کا سامنا ہے۔ انھی مشترکہ خطرات سے نمٹنے کے لیے اب سعودی عرب اور دیگر خلیجی ممالک (GCC) مل جل کر اپنے ڈیجیٹل دفاع کو مضبوط کر رہے ہیں۔[7]

دوسری طرف، بین الاقوامی قانون کے ماہر ایلن وینز کا کہنا ہے کہ کوئی بھی ملک صرف اسی وقت اپنے دفاع میں جوابی کاروائی کر سکتا ہے، جب اس پر حقیقت میں کوئی باقاعدہ مسلح حملہ ہو چکا ہو۔ محض اس شک یا ڈر کی بنیاد پر کسی پر پہلے سے حملہ کر دینا کہ "مستقبل میں اس سے ہمیں خطرہ ہو سکتا ہے"، بین الاقوامی قانون کے مطابق بالکل غیر قانونی ہے۔[8]

اس پیچیدہ موضوع کو گہرائی سے سمجھنے کے لیے دنیا کے معروف سیکیورٹی اور قانونی ماہرین کی حالیہ ابحاث کا جائزہ لینا ضروری ہے۔ درج ذیل میں ان اہم ترین ریسرچ آرٹیکلز کا تعارف اور ان کا خلاصہ پیش کیا جا رہا ہے۔

1۔ آرٹیکل:" Operation Epic Fury and the International Law on the Use of Force "

مصنف: فیڈریکا ڈی الیسنڈرا(Federica D'Alessandra)[9]

خلاصہ: اس اہم تحقیقی مقالے میں مصنف نے فروری 2026 میں امریکہ اور اسرائیل کی جانب سے ایران کے خلاف شروع کی جانے والی مہم کے قانونی پہلوؤں کا سخت تنقیدی جائزہ لیا ہے۔ الیسنڈرا کا استدلال ہے کہ "پیشگی دفاع (Anticipatory Self-Defense) " کے نام پر کیے جانے والے یہ حملے بین الاقوامی قوانین (Jus ad Bellum) کے روایتی ڈھانچے کو شدید نقصان پہنچا رہے ہیں، اور اس سے مستقبل میں قانونِ جنگ کے کمزور ہونے کا سنگین خطرہ پیدا ہو گیا ہے۔

2۔ آرٹیکل" Operation Epic Fury, Regime Change, and the Collapse of Legal Constraint "

مصنف: ڈیوٹ کھاچاتریان (Davit Khachatryan)[10]

خلاصہ: کھاچاتریان نے اپنے آرٹیکل میں اس بات پر توجہ مرکوز کی ہے کہ کس طرح یہ ڈیجیٹل اور براہ راست عسکری حملے (Kinetic Operation) طاقت کے استعمال پر موجود عالمی قانونی پابندیوں کو بالکل ختم کر رہا ہے۔ ان کا کہنا ہے کہ جنیوا مذاکرات کی ناکامی کے فوراً بعد ہونے والی یہ کاروائی دراصل بین الاقوامی قانون کی آڑ میں حکومت کی تبدیلی (Regime Change) کی ایک ایسی غیر قانونی کوشش ہے، جو عالمی نظام میں ایک خطرناک روایت قائم کر رہی ہے۔

3۔ آرٹیکل"Fog, Proxies and Uncertainty: Cyber in US-Israeli Operations in Iran"

مصنف: ڈاکٹر لوئیس میری ہوریل(Dr. Louise Marie Hurel)[11]

خلاصہ: یہ آرٹیکل اس مہم کے دوران سائبر وار فیئر کے آپریشنل اور تزویراتی (Strategic) کردار کا احاطہ کرتا ہے۔ ہوریل بتاتی ہیں کہ کس طرح امریکی اور اسرائیلی سائبر کاروائیوں نے ایران کی انٹرنیٹ تک رسائی (Connectivity) کو محض 4 فیصد تک محدود کر دیا۔ ان کا کہنا ہے کہ اس ڈیجیٹل بلیک آؤٹ نے نہ صرف ایران کے دفاعی نیٹ ورکس کو مفلوج کیا، بلکہ یہ ثابت کر دیا کہ جدید جنگوں میں سائبر ہتھیار اب محض ایک معاون ٹول نہیں بلکہ پہلے حملے کا بنیادی ہتھیار (First-Strike Enabler) بن چکے ہیں۔

4۔ آرٹیکل "The Impact of the Israeli-Iranian Cyberwar on Arab Regional Security"

مصنف: احمد موہی (Ahmad Mohee) [12]

خلاصہ: موہی نے اس تنازع کے عرب دنیا کی علاقائی سلامتی پر پڑنے والے اثرات کا جائزہ لیا ہے۔ بیوزان اور ویور کی 'علاقائی سیکیورٹی کمپلیکس تھیوری کا استعمال کرتے ہوئے وہ بتاتے ہیں کہ اس سائبر جنگ نے خلیجی ممالک (خصوصاً سعودی عرب) اور اسرائیل کے درمیان ڈیجیٹل دفاعی تعاون کو کس طرح بڑھا دیا ہے، جس سے پورے خطے کا روایتی توازنِ طاقت تبدیل ہو رہا ہے۔

جوازِ تحقیق

اگرچہ اسرائیل، امریکہ اور ایران کے مابین جاری سائبر کشمکش پر کافی کام ہو چکا ہے، تاہم موجودہ علمی ادب میں چند اہم اور کلیدی خلا (Gaps) پائے جاتے ہیں جنہیں اس تحقیق کے ذریعے پُر کرنے کی کوشش کی گئی ہے جو درج ذیل ہیں۔

1. اے آئی (AI) کے کردار پر تحقیق کا فقدان:

موجودہ ریسرچ کا زیادہ تر حصہ روایتی سائبر حملوں (جیسے سٹکس نیٹ) تک محدود ہے۔ اے آئی (AI) کے ذریعے خودکار حملوں (Autonomous Cyber-Attacks) کے عسکری، قانونی اور اسٹریٹجک اثرات کا تفصیلی تجزیہ ابھی تک بہت کم ہوا ہے۔

یہ تحقیق اس خلا کو پُر کرتی ہے کہ کس طرح اے آئی نے ڈیجیٹل جنگ کی رفتار اور تباہی کی صلاحیت کو تبدیل کر دیا ہے۔

2. بین الاقوامی قانون کی ناکافی مطابقت:

موجودہ قانونی تحقیقات اکثر اس بات پر متفق ہیں کہ بین الاقوامی قانون سائبر اسپیس میں مبہم ہے۔

تاہم، اس بات پر بہت کم بحث ہوئی ہے کہ "مصنوعی ذہانت" کے استعمال کے بعد بین الاقوامی قانون کے تحت ریاستی ذمہ داری (State Responsibility) کا تعین کیسے کیا جائے۔ یہ تحقیق اس بات کا جائزہ لیتی ہے کہ آیا موجودہ قوانین (جیسے ٹیلن مینول 2.0) اے آئی دور کے چیلنجوں کو نمٹنے کے لیے کافی ہیں یا نہیں۔

3. علاقائی سلامتی پر کثیر جہتی اثرات:

زیادہ تر تحقیقی کام یا تو صرف تکنیکی پہلوؤں پر مرکوز ہے یا پھر سیاسی تجزیوں تک محدود ہے۔ اس مقالے کا جواز یہ ہے کہ یہ تکنیکی پیش رفت (اے آئی)، قانونی ابہام اور علاقائی سیکیورٹی کو ایک ہی فریم ورک میں اکٹھا کرتا ہے، تاکہ یہ سمجھا جا سکے کہ ٹیکنالوجی کس طرح مشرقِ وسطیٰ میں بغیر اعلان شدہ جنگ (Undeclared War) کو فروغ دے رہی ہے۔

جنگوں میں مصنوعی ذہانت (AI) اور جدید ٹیکنالوجی کا استعمال

"آپریشن ایپک فیوری" (Operation Epic Fury) نے ثابت کر دیا ہے کہ اب جنگوں میں فوجی کمانڈروں کے بجائے کمپیوٹر اور مصنوعی ذہانت (AI) کا راج ہے۔ اس جنگ میں امریکہ نے اپنے اسمارٹ فوجی سسٹم کے اندر 'کلاڈ اے آئی (Claude AI) 'نامی ٹیکنالوجی کو شامل کیا۔

اس ٹیکنالوجی کا کمال یہ تھا کہ اس نے سیٹلائٹ کیمروں اور ڈرونز سے ملنے والی معلومات کو فوراً اکٹھا کیا اور پہلے ہی 24 گھنٹوں کے اندر دشمن کے ایک ہزار سے زیادہ اہم ٹھکانوں کا پتہ لگا لیا۔ اس سے حملے کے فیصلے کرنے کی رفتار بہت تیز ہو گئی۔ یہ نظام براہ راست میزائلوں، بمبار طیاروں اور خودکار ڈرونز کے ساتھ جڑا ہوا تھا، جس نے انسانوں کی مداخلت کے بغیر ہی خود بخود مقررہ نشانے پر بمباری کی۔

اسرائیل نے بھی 'لیونڈر' (Lavender) اور 'دی گاسپل' (The Gospel) نامی اے آئی پروگرام استعمال کیے، جن کی مدد سے حملے کے لیے ہدف چننے کا کام بہت تیز ہو گیا۔ ان پروگراموں نے ہزاروں مشتبہ افراد کی فہرستیں تیار کیں (اگرچہ ان میں 10 فیصد غلطیوں کی گنجائش بھی تسلیم کی گئی)۔

دسمبر 2025 میں، دفاعی صلاحیتوں کو مزید مستحکم کرنے کے لیے 'آئرن بیم' (Iron Beam) لیزر سسٹم متعارف کرایا گیا۔ اس نظام میں موجود جدید مصنوعی ذہانت (AI) نے دشمن کے حملوں کی بروقت نشاندہی کر کے انہیں ناکام بنانے میں انتہائی موثر اور درست کردار ادا کیا۔ اس ٹیکنالوجی کا سب سے نمایاں پہلو اس کی فعالیت اور کم لاگت ہے؛ روایتی ہتھیاروں کے مقابلے میں یہ سسٹم 90 فیصد کم خرچ پر کام کرتا ہے۔ مختصر یہ کہ، آئرن بیم جدید دفاعی طریقہ کار میں ایک انتہائی موثر، برق رفتار اور جدید ترین اضافہ ہے۔[13]

بمباری شروع کرنے سے پہلے امریکہ اور اسرائیل نے انٹرنیٹ اور سائبر حملوں کے ذریعے ایران کے ریڈار اور دفاعی نظام کو بالکل اندھا کر دیا تھا۔ اس کے ساتھ ہی، ایران میں نماز اور کیلنڈر کی ایک مشہور موبائل ایپ "بادِ صبا" کو ہیک کر لیا گیا۔ اس ایپ کے ذریعے لاکھوں عام صارفین کے موبائل پر حکومت کے خلاف بغاوت کرنے کے پیغامات بھیجے گئے۔ یہی نہیں، تہران کے ٹریفک کیمروں اور موبائل نیٹ ورکس کی طویل عرصے سے جاری جاسوسی نے اہم فوجی رہنماؤں کو نشانہ بنانے میں بڑا کردار ادا کیا۔[14]

یہ سائبر جنگ صرف ایران تک محدود نہیں رہی بلکہ پڑوسی ملکوں کو بھی اپنی لپیٹ میں لے لیا۔ مارچ 2026 میں پاکستان کے بڑے نیوز چینلز (جیو، اے آر وائی، اور سماء) کو اسرائیل کے حامی ہیکرز نے ہیک کر کے اپنی مرضی کے پیغامات چلائے، اور گوگل اشتہارات کے ذریعے بھی ایسا ہی پروپیگنڈا پھیلایا گیا۔ اس کے جواب میں 2 مارچ کو "پاکستان سائبر فورس" نامی ایک آزاد ہیکر گروپ نے بھارتی نیوز چینل اے بی پی (ABP) نیوز کو ہیک کر کے جوابی کاروائی کی۔ اس واقعے سے یہ بات واضح ہوتی ہے کہ ڈیجیٹل دور کی جنگوں میں اب صرف حکومتیں نہیں لڑ رہیں، بلکہ آزاد ہیکر گروپس اور عام لوگ بھی ایک بڑی طاقت بن کر ابھر رہے ہیں۔[15]

ایرانی ڈیجیٹل ردعمل، موزیک مدافعت اور ہنڈالا ہیک (Iranian Response, Mosaic Defense & Stryker Breach)

ایرانی فوج کا موزیک ڈیفنس حربہ اور کمال حکمتِ عملی

اگرچہ ایران میں انٹرنیٹ سروسز کو تقریباً بند کر دیا گیا تھا (وہاں انٹرنیٹ کی رفتار معمول سے گر کر صرف 1 سے 4 فیصد رہ گئی تھی) اور ان کا مرکزی کمانڈ روم بھی تباہ ہو چکا تھا، لیکن ایرانی فوج (پاسدارانِ انقلاب) نے ہمت نہیں ہاری۔ انہوں نے اپنے خاص دفاعی منصوبے، جسے 'موزیک ڈیفنس' کہا جاتا ہے، کے تحت ان حملوں کا انتہائی لچکدار اور مضبوط جواب دیا۔[16] ایران نے یہ جنگی منصوبہ سال 2005 میں تیار کیا تھا۔ اس کا بنیادی اصول یہ تھا کہ پوری فوج کے کنٹرول کو کسی ایک مرکز میں رکھنے کے بجائے اسے 31 الگ الگ اور خود مختار صوبائی حصوں میں بانٹ دیا جائے۔ اس کا سب سے بڑا فائدہ یہ ہوا کہ

جب ملک میں انٹرنیٹ تقریباً مکمل بند ہو گیا اور مرکزی کمانڈ سے رابطہ کٹ گیا، تب بھی بیرونِ ملک سرگرم ایرانی انٹیلی جنس ایجنسی (MOIS) اور پاسداران کے سائبر سیلز نے اپنے طور خود فیصلے کیے اور جوابی کاروائی جاری رکھی۔

دشمن کے حملے کے محض 24 گھنٹوں کے اندر، ایران کے کمپیوٹر آپریشنز روم نے بڑی مستعدی دکھائی اور دنیا بھر کے 60 سے زیادہ ہیکر گروپس کو ایک جگہ اکٹھا کر دیا، جس کے بعد امریکی اور اسرائیلی کمپنیوں پر انتقامی سائبر کاروائیوں کا ایک طوفان کھڑا ہو گیا۔[17]

امریکی کمپنی پر تباہ کن سائبر حملہ

جوابی کاروائی کے طور پر 11 مارچ 2026 کو ایران سے جڑے ہیکرز کے ایک گروپ نے 'اسٹرائیکر' نامی ایک بڑی امریکی میڈیکل کمپنی کو نشانہ بنایا۔

اس حملے کا طریقہ بہت انوکھا تھا۔ ہیکرز نے کمپنی کے کمپیوٹرز میں کوئی روایتی وائرس یا خطرناک سافٹ ویئر نہیں ڈالا، بلکہ بڑی ہوشیاری سے کمپنی کے اپنے ہی آفیشل اور جائز سسٹمز کا کنٹرول چھین لیا۔ انہوں نے پاسورڈ اور سیکیورٹی کے دیگر سخت پہروں کو دھوکہ دے کر کمپنی کے مرکزی سسٹم تک رسائی حاصل کر لی۔

کنٹرول ملنے کے بعد، انہوں نے ایک ہی کمانڈ بھیج کر 61 ممالک میں موجود اس کمپنی کے تقریباً 2 لاکھ لیپ ٹاپس، موبائل فونز اور مین سرورز کا سارا ڈیٹا مکمل طور پر اڑا دیا (یعنی سب کچھ ڈیلیٹ کر کے فارمیٹ کر دیا)۔ اس ایک کاروائی سے امریکی کمپنی کو 6 سے 8 ارب ڈالر کا شدید مالی نقصان پہنچا۔

ثبوت مٹانا اور حساس معلومات کی چوری

اس تباہ کن حملے میں ہیکرز نے صرف سسٹمز کو تباہ ہی نہیں کیا، بلکہ بہت ہوشیاری سے کام لیا۔ حملے سے ٹھیک پہلے، ہیکرز کی ایک اور ٹیم نے خاموشی سے 50 ٹیرابائٹ (یعنی کئی ہزار لیپ ٹاپس کے برابر) ڈیٹا چوری کر لیا تاکہ پیچھے کوئی ایسا ثبوت نہ بچے جس سے ان کا سراغ لگایا جا سکے۔

اس کے ساتھ ہی، انہوں نے دو اور بڑے محاذوں پر حملے کیے:

- **تیل کے نقشوں کی چوری**: ایک اور ہیکر گروپ نے متحدہ عرب امارات کی سرکاری تیل کمپنی کا نظام ہیک کیا۔ وہاں سے انہوں نے تیل کی پائپ لائنز کے انتہائی حساس نقشے اور تکنیکی معلومات چرائیں اور انٹرنیٹ کی اس تاریک دنیا (ڈیپ ویب) پر ڈال دیں جہاں عام لوگ نہیں پہنچ سکتے۔

- **خفیہ دستاویزات کا انکشاف**: ہیکرز نے اسرائیلی خفیہ ایجنسی 'موساد' کے ایک سابق اعلیٰ افسر کی ذاتی ای میلز کو نشانہ بنایا۔ وہاں سے انہوں نے فوج اور انٹیلیجنس کی ڈیڑھ لاکھ (150,000) سے زیادہ انتہائی خفیہ دستاویزات نکال کر پوری دنیا کے سامنے انٹرنیٹ پر پھیلا دیں۔

ان سب کاروائیوں کا ایک ہی وقت میں مل کر ہونا اس بات کا واضح ثبوت ہے کہ سائبر دنیا کی جنگ میں ایران اور اس کے ساتھیوں کی جوابی کاروائی کی صلاحیت کتنی خطرناک اور مربوط ہے۔[18]

بین الاقوامی قانون اور آئینی سوالات کا تنقیدی محاکمہ (International Law & Constitutional Critiques)

بین الاقوامی قوانین پر اٹھنے والے اعتراضات

جب امریکہ اور اسرائیل کی فضائی افواج نے ایران کی جغرافیائی یا سلیمانی حدود کے اندر داخل ہو کر بڑے پیمانے پر بمباری کی، تو اس کاروائی کو جنگ شروع کرنے کے روایتی بین الاقوامی قوانین (Jus ad Bellum) کے خلاف قرار دیا گیا۔[19] دنیا میں جنگ شروع کرنے کے لیے کچھ مسلّمہ اور پرانے اصول طے ہیں جن کی کھلی خلاف ورزی اس حملے میں دیکھی گئی۔

اقوام متحدہ کے چارٹر کی شق نمبر 2(4) واضح طور پر کہتی ہے کہ کوئی بھی ملک کسی دوسرے آزاد ملک کے خلاف نہ تو طاقت استعمال کر سکتا ہے اور نہ ہی اسے فوجی حملے کی دھمکی دے سکتا ہے۔ دوسری طرف، اسی قانون کی شق نمبر 51 یہ بتاتی ہے کہ کوئی ملک اپنے دفاع میں جوابی کاروائی صرف اسی وقت کر سکتا ہے جب اس پر باقاعدہ اور عملی طور پر کوئی مسلح حملہ ہو چکا ہو۔[20] چونکہ ایران کی طرف سے امریکہ یا اسرائیل پر اس نوعیت کا کوئی فوری اور بڑا حملہ نہیں ہوا تھا، اس لیے ایران کی سرزمین پر 900 فضائی بم گرانے کے عمل کو کسی بھی طرح قانونی یا جائز نہیں مانا جا سکتا۔[21]

امریکہ کا قانونی دفاع اور مسلسل لڑائی کا نظریہ

اس فوجی مہم کے حق میں امریکی اسٹیٹ ڈیپارٹمنٹ (محکمہ خارجہ) کے قانونی مشیر "رئیڈی رابنسٹائن" نے 21 اپریل 2026 کو ایک طویل قانونی تحریر پیش کی۔ انہوں نے اس حملے کو درست ثابت کرنے کے لیے جاری مسلح تنازعے کے نظریے (Ongoing Armed Conflict Theory) کا سہارا لیا۔[22]

ان کا دعویٰ تھا کہ امریکہ اور اسرائیل سال 1979 یا 2019 سے ایران کے ساتھ ایک مسلسل جنگ اور کشیدگی کی حالت میں ہیں۔ رابنسٹائن کے مطابق، جب دو ممالک کے مابین پہلے سے ہی ایک طویل لڑائی چل رہی ہو، تو ہر نئے حملے سے پہلے یہ ثابت کرنا لازمی نہیں رہتا کہ دشمن ہمارے اوپر بالکل ابھی اور اسی وقت حملہ کرنے والا ہے، جسے قانون کی اصطلاح میں "کیرولین فوری خطرے کا معیار" (Caroline Imminence Standard) کہا جاتا ہے۔[23] انہوں نے یہ مؤقف بھی اپنایا کہ ماضی میں عارضی طور پر ہونے والی جنگ بندیاں یا ناکام سفارتی کوششیں اپنے دفاع میں طاقت استعمال کرنے کے حق کو ختم نہیں کر سکتیں۔

عالمی قانون دانوں کا ردِ عمل اور معصوم شہریوں کا نقصان

دنیا بھر کے قانون دانوں نے امریکی حکومت کی اس تشریح پر شدید تنقید کی اور خبردار کیا کہ یہ ایک خطرناک سوچ ہے۔ اگر اس مبہم اور کمزور دلیل کو تسلیم کر لیا جائے، تو مستقبل میں کوئی بھی طاقتور ملک پرانی دشمنیوں کا بہانہ بنا کر جب چاہے گا کسی دوسرے ملک پر اکیلے ہی بمباری شروع کر دے گا اور دنیا کا امن و امان تباہ ہو جائے گا۔

اس کاروائی میں ایک اور سنگین خلاف ورزی خود کار سسٹمز یعنی مصنوعی ذہانت (AI) کے ذریعے بمباری کرنا تھی۔ انسانی بستیوں اور دیگر تنصیبات پر بغیر سوچے سمجھے بم گرانا جنگی قوانین (Jus in Bello) کے تحت امتیاز اور تناسب کے اصول (Necessity and Proportionality) کی صریح خلاف ورزی تھی۔ ان قوانین کے تحت جنگ کے دوران معصوم شہریوں اور عسکری اہداف میں فرق کرنا (امتیاز کا اصول) اور صرف اتنی طاقت استعمال کرنا جتنی ضرورت ہو (تناسب کا اصول) لازمی ہوتا ہے، اس لاپرواہی کی وجہ سے ایران کے شہر "بندر عباس" کے قریب کئی معصوم شہریوں کو اپنی جانیں گنوانی پڑیں۔

امریکہ کا اندرونی سیاسی اور آئینی جھگڑا

امریکہ کے اپنے ملک کے اندر بھی صدر ٹرمپ کی جانب سے پارلیمنٹ (کانگریس) کی پیشگی منظوری کے بغیر اتنے بڑے پیمانے پر جنگ چھیڑنے پر ایک بڑا آئینی بحران پیدا ہوگیا۔ امریکی آئین کی شق نمبر 1، سیکشن 8 کے مطابق، جنگ کا فیصلہ کرنے اور اس کا اعلان کرنے کا پورا اختیار صرف پارلیمنٹ کے پاس ہے، صدر کے پاس نہیں۔ اس کے علاوہ، امریکی محکمہ انصاف کا ایک ذیلی ادارہ "آفس آف لیگل کونسل (OLC) " بھی یہ کہتا ہے کہ صدر صرف چھوٹی موٹی اور عارضی عسکری کاروائیاں خود کر سکتا ہے، ایسی مہمات نہیں جو باقاعدہ اور طویل جنگ کی شکل اختیار کر لیں۔

چونکہ یہ فضائی مہم جسے آپریشن ایپک فیوری(Operation Epic Fury)کا نام دیا گیا، مسلسل 38 دنوں تک جاری رہی اور اس میں زمینی فوج بھیجنے کا شدید خطرہ موجود تھا، اس لیے سال 1973 کے "جنگی اختیارات کے قانون"(War Powers Resolution) کے تحت صدر ٹرمپ پر پابندی لگانا ضروری ہو گیا تھا۔ لیکن سینیٹ اور اسمبلی دونوں ایوانوں میں ٹرمپ کی اپنی سیاسی جماعت (ریپبلکن پارٹی) کی اکثریت ہونے کی وجہ سے صدر کو حاصل فنڈز روکنا ممکن نہ رہا اور کانگریس کی تمام کوششیں ناکام ہو گئیں۔[24]

نتائج(Findings)

تحقیق کے تنقیدی تجزیے سے مندرجہ ذیل اہم نتائج حاصل ہوئے ہیں:

فروری 2026 میں ایران کے خلاف امریکہ اور اسرائیل کے مشترکہ آپریشنز (ایپک فیوری' اور 'رورنگ لائن) کا قانونی اور تزویراتی تجزیہ کرنے کے بعد درج ذیل اہم اور ٹھوس نتائج حاصل ہوئے ہیں۔

- طرزِ جنگ میں انقلابی تبدیلی :(Operational Paradigm Shift) اس تحقیق سے یہ بات سامنے آئی ہے کہ اب مصنوعی ذہانت (AI) اور سائبر ہتھیار محض روایتی فوج کی مدد کرنے والے اوزار (Auxiliary Tools) نہیں رہے۔ فروری 2026 کا تنازع تاریخ کا وہ پہلا موڑ ہے جہاں 'دی گوسپل' اور 'لیونڈر' جیسے الگورتھمک سسٹمز نے انسانی مداخلت کے بغیر، سیکنڈوں میں ہزاروں اہداف خودکار طریقے سے متعین کیے۔ اس پیشرفت نے جنگ کی رفتار کو انسانوں کے کنٹرول اور سوچنے کی صلاحیت سے زیادہ تیز کر دیا ہے۔
- ڈیجیٹل بلیک آؤٹ کی ہولناکی :(Strategic Impact of Digital Sabotage) مہم کے آغاز میں ایران کے انٹرنیٹ انفراسٹرکچر پر ہونے والے مربوط سائبر حملوں نے ملکی رسائی (Connectivity) کو اچانک 4 فیصد تک گرا دیا۔ اس کا سب سے بڑا نتیجہ یہ نکلا کہ ایران کا فضائی دفاعی نظام (Air Defense) اور کمانڈ اینڈ کنٹرول نیٹ ورکس اپنے مقامی سینسرز سے کٹ کر رہ گئے، جس نے ثابت کیا کہ جدید دور میں کسی ملک کو مروجہ ہتھیاروں سے پہلے ڈیجیٹل طور پر مفلوج کرنا سب سے مہلک ہتھیار بن چکا ہے۔
- بین الاقوامی قانون کا انحطاط :(Legal Erosion of Jus ad Bellum) قانونی لحاظ سے یہ تحقیق اس نتیجے پر پہنچی ہے کہ اقوام متحدہ کے چارٹر کے آرٹیکل 51 کے تحت "پیشگی دفاع (Anticipatory Self-Defense) "کا جو جواز امریکہ اور اسرائیل نے اپنایا، وہ عالمی قوانین کو شدید نقصان پہنچا رہا ہے۔ جنیوا مذاکرات کی ناکامی کے فوراً بعد کیا جانے والا

یہ حملہ دراصل بین الاقوامی قانون کی آڑ میں حکومت کی تبدیلی (Regime Change) کی ایک ایسی کوشش ہے، جو مستقبل میں دیگر طاقتور ممالک کے لیے بھی یکطرفہ جنگیں شروع کرنے کا ایک خطرناک قانونی راستہ کھول رہی ہے۔

- علاقائی سلامتی کا نیا سیکیورٹی کمپلیکس :(Emergence of Regional Cyber Complex) سلامتی کے میدان میں یہ نتیجہ ملا ہے کہ اس جنگ نے مشرقِ وسطیٰ کے روایتی توازنِ طاقت (Power Balance) کو یکسر بدل دیا ہے۔ ایران کے خطرے سے نمٹنے کے لیے خلیجی ممالک (خصوصاً سعودی عرب) اور اسرائیل کے مابین ایک غیر علانیہ "ڈیجیٹل اور سائبر سیکیورٹی تعاون" مضبوط ہوا ہے، جس کے جواب میں ایران کی جانب سے پراکسی نیٹ ورکس کی متحرک کاری اور آبنائے ہرمز جیسے حساس بحری راستوں میں معاشی عدم استحکام پیدا کیا جا رہا ہے۔

سفارشات(Recommendations)

فروری 2026 کے تنازع (آپریشن ایپک فیوری اور رورنگ لائن) سے حاصل ہونے والے نتائج کی روشنی میں، عالمی برادری، قانونی اداروں اور علاقائی ممالک کے لیے درج ذیل سفارشات پیش کی جاتی ہیں:

1. نئے عالمی سائبر قوانین کی تشکیل :(Formulation of a New Cyber Legal Framework) موجودہ بین الاقوامی قوانین (جیسے اقوامِ متحدہ کا چارٹر) ڈیجیٹل دور کے تقاضوں کو پورا کرنے میں ناکام ہو رہے ہیں۔ سفارش کی جاتی ہے کہ جنیوا کنونشن کی طرز پر ایک نیا عالمی معاہدہ تیار کیا جائے، جسے "ڈیجیٹل جنیوا کنونشن" کہا جا سکے۔ اس معاہدے کے تحت کسی خود مختار ملک کے انٹرنیٹ انفراسٹرکچر کو مکمل مفلوج کرنے (ڈیجیٹل بلیک آؤٹ) کو باقاعدہ جنگی جرم (War Crime) قرار دیا جانا چاہیے۔
2. مصنوعی ذہانت کے جنگی استعمال پر پابندیاں:(Regulation of Military AI Systems) لیونڈر اور دی گوسپل جیسے اے آئی sسسٹمز نے ثابت کیا ہے کہ خودکار ہدف سازی عام شہریوں کے لیے کتنی مہلک ہو سکتی ہے۔ بین الاقوامی قانون میں یہ لازمی قرار دیا جائے کہ فوجی فیصلوں میں انسانی کنٹرول (Human-in-the-loop) کو برقرار رکھا جائے، تاکہ الگورتھم کو تنہا انسانی جانوں کے فیصلے کرنے کا اختیار نہ ہو۔
3. علاقائی سائبر سیکیورٹی ڈائیلاگ کا آغاز :(Regional Cyber Diplomacy) مشرقِ وسطیٰ میں پیدا ہونے والے نئے سیکیورٹی تناؤ کو کم کرنے کے لیے خلیجی ممالک، ایران اور دیگر اسٹیک ہولڈرز کے مابین ایک مشترکہ "سائبر ہاٹ لائن" قائم کی جانی چاہیے۔ اس کا مقصد کسی بھی سائبر حملے کی صورت میں غلط فہمیوں کو دور کرنا اور کشیدگی کو کھلی جنگ میں تبدیل ہونے سے روکنا ہے۔
4. بحری اور معاشی گزرگاہوں کا تحفظ :(Protection of Critical Maritime Corridors) آبنائے ہرمز جیسے اہم بین الاقوامی بحری راستوں کو سائبر اور روایتی جنگ کے اثرات سے محفوظ رکھنے کے لیے اقوامِ متحدہ کے زیرِ نگرانی ایک مستقل سیکیورٹی فریم ورک بنایا جائے، تاکہ عالمی معیشت کو بڑے بحرانوں سے بچایا جا سکے۔

References

1.Edwards, Chuck. “Operation Epic Fury Is Long Overdue for US Self-Defense.” Congressman Chuck Edwards, March 17, 2026. https://edwards.house.gov/media/opinion-editorials/operation-epic-fury-long-overdue-us-self-defense

Wikipedia, s.v. "2026 Iran war," last modified May 16, 2026, https://en.wikipedia.org/wiki/2026 Iran war.

Operation Epic Fury: Hybrid Warfare and Legal Erosion in the 2026 US-Israel-Iran Conflict." Education Genius Solutions, 2026. https://www.researchgate.net/publication/403947089 Publisher EDUCATION GENIUS SOLUTIONS Review Type Double Blind Peer Review Operation Epic Fury Hybrid Warfare and Legal Erosion in the 2026 US-Israel-Iran Conflict.

2.Rubinstein, Reed D. "Operation Epic Fury and International Law." Office of the Legal Adviser,(U.S. Department of State, April 2026), 1–12.

Edwards, Donna. "Operation Epic Fury: Long Overdue U.S. Self-Defense." Opinion/Editorials. Donna Edwards, U.S. House of Representatives. https://edwards.house.gov/media/opinion-editorials/operation-epic-fury-long-overdue-us-self-defense.

The Asymmetric Frontier: A Strategic Analysis of Iranian Cyber Operations and Geopolitical Resilience in the 2026 Conflict." ResearchGate, 2026. https://www.researchgate.net/publication/402998854

The Asymmetric Frontier A Strategic Analysis of Iranian Cyber Operations and Geopolitical Resilience in the 2026 Conflict.

3. "2026 Iran war." Britannica. Accessed May 21, 2026. https://www.britannica.com/event/2026-Iran-war.

4.Weiner, Allen. "Stanford’s Allen Weiner on the Constitutional and International Law Questions Raised by the Iran Attack.(Stanford Law School, March 3, 2026), 1–5.

ResearchGate. "The 2026 US-Israel-Iran War: Divergent Strategies, Information Warfare, and a Fractured West Asia." 2026. https://www.researchgate.net/publication/403704920 The 2026 US-Israel-Iran War Divergent Strategies Information Warfare anda Fractured West Asia.

5. Michael N. Schmitt, “Cyber Operations and the Jus Ad Bellum Revisited,” Villanova Law Review 56, no. 3 (2011): 569–606, SSRN Electronic Journal

6. Mohee, Ahmad. “The Impact of the Israeli-Iranian Cyberwar on Arab Regional Security.”(APSA Preprints, March 27, 2023),1–15.

7.MacVaugh, Kimberly. “Fostering Critical Thinking in the Age of AI: Why Information Literacy Still Matters.”(APSA Preprints, January 27, 2025), 1–12

Al-Marashi, Ibrahim. "The Impact of the Israeli-Iranian Cyberwar on Arab Regional Security." APSA Preprints, 2023. https://preprints.apsanet.org/engage/api-gateway/apsa/assets/orp/resource/item/6420d528647e3dca998d3122/original/the-impact-of-the-israeli-iranian-cyberwar-on-arab-regional-security.pdf

8.Weiner, Allen. "Stanford’s Allen Weiner on the Constitutional and International Law Questions Raised by the Iran Attack."(Stanford Law School, March 3, 2026),1–5.

9.D'Alessandra, Federica. "Operation Epic Fury and the International Law on the Use of Force." (Carnegie Endowment for International Peace, March 31, 2026),1–25.

10.Khachatryan, Davit. "Operation Epic Fury, Regime Change, and the Collapse of Legal Constraint." (Center for International Policy (CIP), March 4, 2026), 1–10.

11.Hurel, Louise Marie. "Fog, Proxies and Uncertainty: Cyber in US-Israeli Operations in Iran."(Royal United Services Institute (RUSI), March 5, 2026), 1–8.

12.Ahmad Mohee, "The Impact of the Israeli-Iranian Cyberwar on Arab Regional Security," APSA Preprints, 2023, https://preprints.apsanet.org.

13.Al Mazrouei, Noor Saif Fares. "Comparative Report: AI Utilization in the Israel-USA-Iran Conflict."(TRENDS Research & Advisory, 2026), 1–30.

14.Badgi, Kuhu, and Lauryn Williams. "How Will Cyber Warfare Shape the U.S.-Israel Conflict with Iran?"(Center for Strategic & International Studies (CSIS), March 3, 2026), 1–15.

15. Wikipedia. "Cyberwarfare during the 2026 Iran war." Accessed May 21, 2026. https://en.wikipedia.org/wiki/Cyberwarfare during the 2026_Iran_war.

16.Nocturnal Knight. "The Asymmetric Frontier: A Strategic Analysis of Iranian Cyber Operations and Geopolitical Resilience in the 2026 Conflict.

https://nocturnalknight.co/the-asymmetric-frontier-a-strategic-analysis-of-firanian-cyber-operations-and-geopolitical-resilience-in-the-2026-conflict.

17.Kean Miller LLP. "Iran Conflict Adds New Motivations to Cyber Threats."(Kean Miller Insights, May 21, 2026), 1–5.

18.S2W Inc. "Detailed Analysis of Iran-Israel/USA Cyberwarfare: Multi-Domain Escalation."(S2W Insights, 2026), 1–20.

19. Carnegie Endowment for International Peace. "Operation Epic Fury and International Law." March 2026. https://carnegieendowment.org/research/2026/03/operation-epic-fury-and-the-international-law.

Weiner, Allen. "Stanford's Allen Weiner on the Constitutional and International Law Questions Raised by the Iran Attack." Stanford Law School, March 3, 2026. https://law.stanford.edu/2026/03/03/stanfords-allen-weiner-on-the-constitutional-and-international-law-questions-raised-by-the-iran-attack

20.Just Security. "On the State Department Memorandum '(Operation Epic Fury and International Law'." May 21, 2026),1–12.

21.Britannica, T. Editors of Encyclopaedia. "2026 Iran War." Encyclopedia Britannica, May 21, 2026. https://www.britannica.com/event/2026-Iran-war.

22.U.S. Department of State. "Operation Epic Fury and International Law." Office of the Legal Adviser, April 2026. https://www.state.gov/releases/office-of-the-legal-adviser/2026/04/operation-epic-fury-and-international-law

23.Iran War: Criminal Aggression." The Guardian, May 14, 2026. https://www.theguardian.com/commentisfree/2026/may/14/iran-war-criminal-aggression

24.The White House. "Peace Through Strength: Operation Epic Fury Crushes Iranian Threat as Ceasefire Takes Hold." White House Releases, April 2026. https://www.whitehouse.gov/releases/2026/04/peace-through-strength.