INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner what sever for any consequences for any action taken by anyone on the basis of information in the Journal.

ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor
School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC-NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi. (2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN- 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

WHEN NOTHING BREAKS BUT EVERYTHING STOPS: LOSS OF FUNCTIONALITY AS "DAMAGE" UNDER INTERNATIONAL HUMANITARIAN LAW

AUTHORED BY - AASHI KAURA
O.P. Jindal Global University

ABSTRACT

Cyber operations in armed conflicts increasingly disable essential civilian services like healthcare, water, power, civil registration by corrupting or deleting data rather than physically damaging hardware. Whether such actions qualify as **"attacks"** depends on two linked questions under Additional Protocol I (AP I): can data be an **"object"**, and does loss of functionality count as **"damage"**? This article argues for a narrow, effects-based reading that fits the text, purpose and practice of International Humanitarian Law (IHL): where datasets are **essential to the continuity of civilian services**, foreseeable loss of functionality should be treated as **"damage"** to a protected object, thereby triggering the rules on distinction, proportionality, and precautions. To avoid overreach, this piece carves out **pure confidentiality breaches** without foreseeable service disruption and proposes a **feasibility-based precautions test** tailored to cyber means (alternative-means analysis, reversibility/rollback, timing, and limited operator notice). The conclusion offers a one-page **commander checklist** to operationalize the approach within existing doctrine, without creating new treaty categories.

KEYWORDS: International Humanitarian Law; Cyber Operations; Civilian Objects; Data; Loss of Functionality; proportionality; Precautions.

THE PROBLEM IN ONE PAGE

Modern public services are often data dependent. An electronic health-record index deleted at 2:00 a.m. can halt pharmacy dispensing by 2:05 a.m.; corrupting configuration files on a water utility's engineering workstation can desynchronize pumps and chemical dosing within minutes; scrambling civil-registry hashes can freeze humanitarian cash transfer for weeks. None of these outcomes require visible destruction. **Yet from a civilian's perspective, the service has stopped.**

ISSN: 2582-6433

IHL's conduct-of-hostilities rules were drafted with kinetic harm in mind. But AP I's framework is **technology-neutr**al and aimed at **protecting civilians** and the **services** they rely on. The central question is therefore not metaphysical "are bits 'things'?" but functional: when a cyber operation foreseeably disables an essential service by corrupting or deleting data, should IHL treat that as "damage" to a protected "object" and thus an "attack"? This article defends a carefully bounded **yes** and provides practical tools that operators and legal advisors can use ex ante.

THE BLACK-LETTER BASELINE

Under AP I, **"attacks"** are "acts of violence against the adversary",[1] **"civilian objects"** are all objects that are not military objectives,[2] and **"military objectives"** are those objects which, by their nature, location, purpose or use, make an effective contribution to military action and whose destruction, capture or neutralization offers a definite military advantage.[3] The rules of **distinction, proportionality, and precautions** then govern what may be attacked and how.[4]

Two terms to do the doctrinal work here: **"object"** and **"damage"**. AP I does not exhaustively define either. Text and commentary show that an object can be neutralized without permanent physical alteration (e.g., temporarily disabling a radar).[5] In other words, function has always mattered in targeting law. The question is whether, in cyber operations, **data integral to a system's civilian function** can be treated as the relevant "object", or whether only the tangible substrate (server, cable, terminal) counts.

Customary law adds texture: doubt is resolved in favour of civilian status; indiscriminate and disproportionate attacks are prohibited; and parties must take feasible precautions to spare civilians.[6] AP I art. 57's Feasibility standard is context-sensitive and technology-neutral; it demand choice of means and methods that minimize incidental harm when practicable, considering both humanitarian and military factors.[7]

[1] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) [hereinafter AP I] art. 49(1), June 8, 1977, 1125 U.N.T.S. 3.
[2] AP I, supra note 1, art. 52(1).
[3] Id. art. 52(2).
[4] Id. arts. 48, 51, 57; see also Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., **Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949** (ICRC 1987).
[5] U.S. Dep't of Def., **Law of War Manual** § 16.5 (June 2015, updated July 31, 2023); U.K. Ministry of Defence, **The Manual of the Law of Armed Conflict** ¶ 13.5(b), at 402 (Oxford Univ. Press 2004).
[6] Jean-Marie Henckaerts & Louise Doswald-Beck, **Customary International Humanitarian Law**, vol. I: **Rules** rr. 1, 7, 14, 15 (Cambridge Univ. Press 2005).
[7] AP I, supra note 1, art. 57(2)(a)(ii)–(iii).

ISSN: 2582-6433

TWO VIEWS

View A (tangibility-only)

On a strict view, "object" means *material things*; **data** which is an arrangement of bits, cannot be the object of attack. "Damage," in turn, requires **physical alteration**. Under this approach, deleting a hospital database without altering hardware is not an attack (it might still be unlawful on other grounds), and AP I's attack rules do not apply. Proponents warn that broadening "object" risks pulling espionage, psychological operations, and routine intrusions into targeting law and collapsing useful distinctions.[8]

View B (effects-based within limits)

A rival view looks to **IHL's protective purpose**. If the foreseeable effect of corrupting or erasing essential services data is to neutralize the operation of a hospital, water plant, or civil-registry system, then the operation causes **"damage"** to an **object** for AP I purposes, even if no chassis is dented. This need not make all data "**objects"**, nor all intrusions "attacks". The key is **foreseeability** and **service continuity**.

This article defends view B with two guardrails:

- **Guardrail 1 (scope):** It concerns **Essential Civilian Data (ECD)** only datasets whose availability or integrity is reasonably forceable to be necessary for the continuity of healthcare, water and sanitation, electricity, emergency response, social protection, or civil status administration.
- **Guardrail 2 (carve-out): Confidentiality-only** breaches that do not foreseeably degrade service continuity are not "damage" for attack analysis.
  This framing preserves the attack/other-operations line while honouring the humanitarian logic of the rules.

DEFINING ESSENTIAL CIVILIAN DATA (ECD)

Definition. **ECD** *Means data whose availability or integrity is reasonably foreseeable to be necessary for the continuity of essential civilian services,* including healthcare, water and sanitation, electricity, emergency responses, social protection, and civil status administration. This category is deliberately narrow: it is service facing, not "all data on a civilian owned

[8] See **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations** rr. 92–95 C cmts. (Michael N. Schmitt gen. ed., 2d ed. 2017).

ISSN: 2582-6433

system."

Three cumulative Indicia guide planners and operators:

- **Criticality** - How directly does the data set condition service continuity at a minimally acceptable level? (Compare a hospital's medication-allergy tables with a public relations image archive.)
- **Substitutability** - Are there timely workarounds or hot backups? How long would restoration take under *war time constraints* (staffing, curfew, fuel)?
- **Foreseeability** – Would a reasonably informed attacker (using public documentation, sector norms, or prior reconnaissance) understand that manipulating this data set risks disabling an essential service?

Why ECD is not a new treaty category. The point is not to create a novel protected class akin to "objects indispensable to survival." Rather, ECD operationalizes the **civilian-object presumption** for data whose loss predictably causes **civilian-facing service degradation**. It fits the existing architecture: if an object neutralization offers a definite military advantage, it may be a military objective, but incidental harm to civilian objects (including ECD) must still be assessed for proportionality and mitigated via precautions.[9]

Dual use and rebuttal. The presumption is rebuttable. If the same data set directly enables enemy fire control, or if reliable evidence shows **high substitutability** (e.g., an air-gapped read-only mirror updated hourly), the ECD presumption can fall away. The key is documented, good-faith assessment in the circumstances ruling at the time.

WHY "LOSS OF FUNCTIONALITY" IS "DAMAGE" (text, purpose, analogies, practice)

Text and context. AP I art. 52(2) lists "neutralization" alongside "destruction" and "capture". Neutralization is an **effects term**: an object is unusable for its intended function. If a bridge's bolts are removed, the bridge is neutralized though not pulverized. Likewise, if a server's filesystem keys are encrypted or its essential datasets erased, the system is neutralized, the server halts, even if the rack hums along. Reading "damage" to require **molecular**

[9] AP I, supra note 1, art. 52(2).

ISSN: 2582-6433

rearrangement ignores this functional vocabulary.[10]

Object and purpose. The conduct-of-hostilities rules are designed to **protect civilians and essential services** from the effects of attack. If foreseeable loss of functionality predictably deprives civilians of medical care or safe water, treating that outcome as legally invisible merely because it was achieved by corrupting data, not smashing metal, defeats the rules' protective function.[11]

Analogies already accepted in LOAC. Several accepted practices show that function matters: electronic warfare that temporarily **blinds** sensors; non-kinetic means that jam weapon systems; disabling vehicles by removing key components. None of these depends on shrapnel. The law looks to the **operational effect** that whether the object has been rendered **unusable** and subjects that affect to the attack rules.[12] Cyber operations that foreseeably render essential services unusable via data corruption are of the same genus.

Thresholds and limits. To avoid overbreadth, this article proposes:

- **Availability/integrity focus.** Only availability or integrity losses that foreseeably impair services continuity qualify; confidentiality-only compromises do not.
- **Temporality matters.** Longer, wider, or harder-to-reverse functionality loss weighs more heavily in proportionality; brief, well controlled effects with rollback weigh less.
- **Causation and knowledge.** The attackers means of knowledge is a part of foreseeability: widely known system dependencies (e.g., a nation's immunization registry) are different from obscure, non-public datasets.[13]

Method (VCLT arts. 31-32). Interpreting AP I's terms **"object"** and **"damage"** follows the Vienna Convention's general rule: ordinary meaning in context and in light of the treaty's object and purpose, taking into account any subsequent agreement or subsequent practice showing the parties' understanding. Read alongside AP I art. 52(2)'s reference to "neutralization", this supports a **functional** lens rather than a purely material one. Recent **State**

[10] Id.; see also Program on Humanitarian Policy & Conflict Research (HPCR), **Manual on International Law Applicable to Air and Missile Warfare** ¶ 21 (2009).
[11] Int'l Comm. of the Red Cross (ICRC), **International Humanitarian Law and the Challenges of Contemporary Armed Conflicts** ch. V.1(A) at 57–60 (Oct. 2024).
[12] U.S. Dep't of Def., **Law of War Manual** § 16.5; U.K. **LOAC Manual**, supra note 5, ¶¶ 13.4–13.5.
[13] **Tallinn Manual 2.0**, supra note 8, cmts. on knowledge and foreseeability.

ISSN: 2582-6433

positions for example **France** (treating a cyber operation as an attack where systems can no longer provide their service even temporarily)[14], **Germany** (defining cyber-attacks to include harmful effects on information that is stored/processed/transmitted),[15] and **New Zealand** (including loss of functionality within IHL's notion of attack) are pertinent subsequent practice confirming an effects based interpretation within limits[16]. See also **Switzerland** noting incidents in which functionality is damaged or data altered/deleted interfering with governmental functions.[17] Where ambiguity persists, Article 32 permits recourse to supplementary means to confirm this bounded reading: confidentiality-only operations remain outside the attack rules; foreseeable **loss of functionality** of **essential services** counts as **"damage."[18]**

Not every cyber intrusion that concerns "data" engages the attack rules. Intelligence collection, even if unlawful under domestic law, is not, without more, an attack. This article therefore carves out incidents where the only foreseeable effect is loss of confidentiality (e.g., exfiltration of emails) and there is no reasonable prospect of service degradation. This preserves a stable **attack/other operations** boundary while still catching operations that predictably stop the service.

A FEASIBILITY-BASED PRECAUTIONS TEST (tailored to cyber)

AP I art. 57 constant care and feasible precautions to spare civilians. "Feasible" is contextual to what is practicable in the circumstances, balancing humanitarian and military considerations.[19] In cyber operations with plausible ECD impacts, planners/operators should document:

- **ECD screen.** Has their dataset (or dataset class) been assessed against critically (to service continuity), substitutability (backups/workarounds/time to restore under wartime conditions), and foreseeability (what a reasonably informed attacker

[14] Ministère des Armées (France), **International Law Applied to Operations in Cyberspace** 10–11 (2019) (sections 2.2.1–2.2.2) (treating a cyber operation as an attack where targeted systems can no longer provide their service, even temporarily).
[15] Federal Republic of Germany, **On the Application of International Law in Cyberspace** 7 (2021) (defining a cyber attack, for IHL, to include harmful effects on information stored, processed, or transmitted on systems).
[16] New Zealand, **OEWG Intersessional Statement on International Law** 2 (May 24, 2023) (an IHL "attack" may include "loss of functionality" equivalent to kinetic effects).
[17] Switzerland, **Position Paper on the Application of International Law in Cyberspace** 2 (May 27, 2021) (noting incidents where functionality is damaged/limited or data altered/deleted interfering with governmental functions).
[18] Vienna Convention on the Law of Treaties, May 23, 1969, 1155 U.N.T.S. 331, arts. 31–32.
[19] AP I, supra note 1, art. 57; ICRC Commentary thereto.

ISSN: 2582-6433

knew/should have known.)?[20]

- **Alternative-means analysis.** Can the military objective be achieved using functionality-preserving means? Examples:
  - Isolate/segment the target network rather than erasing data;
  - Throttle or rate-limit a service rather than corrupting configuration files;
  - Sandbox processes rather than encrypting entire volumes;
  - Use time limited locks that auto-revert;
  - Target non-essential replicas rather than primaries;
- **Reversibility and rollback**. Are tools configured and tested (in a representative environment) for a rollback or auto-expiry? Is there a plan to lift effects once the military advantage is achieved? Document lab results and limitations so commanders can weigh them.[21]
- **Timing and operator notice (where feasible).** Can execution be aligned with maintenance windows or accompanied by a limited, non-attributive notice that enables operators to create fresh backups, without compromising the mission? In some contexts, even hours matter for reducing civilian harm.[22]
- **Proportionality with functionality metrics.** Does the proportionality assessment explicitly weigh the **anticipated incidental loss of functionality** to essential services (duration, geographic spread, number of affected civilians, critical dependencies) against the concrete and direct military advantage? Legal advisors should require recent estimates, even if rough, rather than generic statements.[23]
- **After action review and learning.** Post-operation, records actual effects (including unexpected cascades). Feedback loop improve **future feasibility judgements** and enable **remedial measures** (e.g., providing technical indicators to speed restoration). The test dovetails with (where applicable) **Article 36** legal reviews of means and methods, which can pre-validate tools that incorporate rollback and fail-safe features.[24]

[20] Id.
[21] See, e.g., practice on reversibility and time-limited effects in electronic warfare/information operations manuals (collecting examples).
[22] AP I, supra note 1, art. 57(2).
[23] Id. art. 51(5)(b).
[24] AP I, supra note 1, art. 36; ICRC, **A Guide to the Legal Review of New Weapons, Means and Methods of Warfare** 3–6 (2006); U.S. Dep't of Def., **Law of War Manual** § 16.6.

ISSN: 2582-6433

ANSWERS TO THE HARD OBJECTIONS

"You're turning espionage into attack." No. The test explicitly excludes confidentiality-only breaches that do not foreseeably degrade essential services. It focuses on availability/integrity impacts with service-continuity effects.

"Everything will become ECD." No. The ECD screen uses three cumulative Indicia; many data sets will fail criticality or be easily substitutable (e.g., hot standbys, printed fallbacks). The presumption is rebuttable by showing low criticality, high substitutability, or lack of foreseeability.

"Commanders can't know all this." Feasibility is contextual, not omniscient. Many militaries already maintained **target intelligence packages**; adding a short ECD screen and documenting alternative means is incremental and implementable.

"The law doesn't say 'data' is an object." True. The treaties are silent. But the neutralization language, the protective object-and-purpose, and accepted analogies on temporary disabling support treating foreseeable loss of functionality as damage in the narrow ECD context. The alternative is declaring such harm legally invisible which undermines civilian protection.

"Won't this shield enemy dual-use data?" No. If data directly and effectively contributes to enemy military action (e.g., fire-control tables), it may be a military objective. The proportionality and precautions rules still apply, but the ECD presumption can be rebutted on evidentiary grounds.

RESPONSIBILITY AND REMEDIES IN BRIEF

If an operation foreseeably degrades ECD And thereby neutralizes an essential civilian service, **state responsibility** follows where the conduct is attributable and breaches IHL. **Attribution rules** (organ, direction or control, acknowledgement/adoption) apply as usual.[25] **Remedies** include cessation, assurances of non-repetition, and reparation (which may involve funding data restoration, backups, network segmentation, and surge staffing to restore services).[26] Cooperative incident-assessment mechanisms including technical fact-finding with

[25] Draft Articles on Responsibility of States for Internationally Wrongful Acts, G.A. Res. 56/83, annex, arts. 4, 8, 11 (Dec. 12, 2001)
[26] Id. arts. 30–31, 34–39.

ISSN: 2582-6433

humanitarian participation can speed restoration without prejudicing legal positions.

IMPLEMENTATION: A SHORT MANUAL-STYLE INTERPRETIVE NOTE (for annexes and SOPs)

The following text is drafted to be dropped, verbatim, into a targeting manual or operations SOP.

A. **Essential Civilian Data (ECD).** For targeting and collateral-damage estimation, treat as civilian objects any data sets whose availability or integrity is reasonably foreseeable to be necessary for the continuity of essential civilian services (including healthcare; water and sanitation; electricity; emergency responses; social protection; civil status). The ECD presumption is rebuttable by reliable evidence of low criticality, high substitutability, or lack of foreseeability at the time of decision.

B. **Loss of functionality as damage.** When an operation foreseeably causes loss of functionality of ECD (e.g., by erasing indexes or corrupting configuration files), treat this as "damage" for attack analysis. Confidentiality-only breaches with no reasonably foreseeable service degradation are not "attacks."

C. **Precautions.** Where ECD may be affected, take **feasible precautions**, including alternative-means analysis favouring functionality-preserving methods, reversibility rollback planning, timing to reduce civilian impact, and explicit proportionality assessments that account for foreseeable duration and scale of service disruption.

D. **Documentation.** Target folder shall include a short ECD screen (criticality, substitutability, foreseeability), the means analysis, and functionality-aware proportionality worksheet

ANNEX – COMMANDER CHECKLIST

ECD Precautions checklist (Operations Potentially Affecting Data)

- **Screen:** Is the target data set plausibly essential to healthcare, water, power, emergency response, social protection, or civil status?
  - Criticality? Substitutability? Foreseeability?
- **Means:** Have functionality-preserving alternatives been considered and documented?
- **Effects:** What is the anticipated duration/scale of incidental functionality loss to civilians?
- **Reversibility:** Are rollback/expiry features enabled and tested?

ISSN: 2582-6433

- **Timing/Notice:** Can execution coincide with maintenance windows or include limited operator notice compatible with mission needs?
- **Proportionality:** Do targeting files record a functionality-aware proportionality analysis?
- **After-Action:** Plan to monitor and, if feasible, lift effects once the military advantage is achieved.

CONCLUSION

When nothing breaks but everything stops, law should care. Reading "damage" to include foreseeable loss of functionality but only where essential civilian services are at stake keeps IHL's promise to civilians without collapsing doctrinal boundaries or converting espionage into attack. The proposed **ECD screen**, **confidentiality carve-out**, and **feasibility-based precautions test** give planners a lawful, practical way to reduce harm before an operation, and a reviewable record after it. No treaty amendment is needed; only a disciplined, functionality-sensitive applications of rules we already have. If adopted in manuals and SOPs, these tools would make cyber operations more **predictable, reviewable, and humane**. In short, more consistent with the law's protective purpose.