International Journal of Social Sciences

Caucasus International University
Volume 6, Issue 3

Journal homepage: http://journal.ciu.edu.ge/

DOI: https://doi.org/10.55367/EZBF7454



*Conference proceedings – **International scientific conference "Contemporary Challenges in International Relations, International Law and Media"** organised by Caucasus International University*
Held on March 12-13, 2026 in Tbilisi

When Cyber Operations Target Personal Data: A New Challenge for IHL?

Guram Gvinjilia [a1]

[a] PhD in Law, Associate Professor,
Caucasus International University

ARTICLE INFO

Keywords:

Rome Statute

Armed Conflict

Computer Data

Data Protection

ABSTRACT

International law, and international humanitarian law (IHL) in particular, continues to provide an uncertain and limited framework for the protection of personal data in the context of cyber operations conducted during armed conflict. This article examines the legal status of personal data in international cyber operations and evaluates whether cyber activities directed against civilian data may fall within existing IHL and international criminal law regimes. It argues that, at the time of the adoption of relevant international treaties and the formation of customary international law, electronically stored personal data were not envisaged as protected objects under IHL. Although contemporary legal scholarship increasingly supports the characterization of computer data as an "object" or "property," State practice and jurisprudence remain inconclusive. The article further assesses whether cyber operations against data may constitute war crimes under the Rome Statute of the International Criminal Court (International Criminal Court, 1998), highlighting interpretative challenges related to the scope of protected objects and the principle of legality. It concludes that while international law must adapt to the realities of cyber warfare, the unqualified application of peacetime data protection standards to armed conflict risks undermining the humanitarian logic of IHL, whose protective purpose must remain paramount.

[1] Corresponding author.
E-mail addresses: Guram.gvinjilia@ciu.edu.ge (G. Gvinjilia).
ORCID: https://orcid.org/0009-0002-7608-6683

Received: 10/04/2026 Revised: 29/06/2026 Accepted: 20/07/2026 Published: 26/11/2026
E-ISSN 2720-8036 / © 2026 The Author(s). Published in The International Journal of Social Sciences by Caucasus International University. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/)

როდის ხდება პერსონალური მონაცემები კიბეროპერაციების სამიზნე: ახალი გამოწვევა საერთაშორისო ჰუმანიტარული სამართლისთვის?

გურამ ღვინჯილია[a] [2]

[a] სამართლის დოქტორი, ასოცირებული პროფესორი,
კავკასიის საერთაშორისო უნივერსიტეტი

სტატიის შესახებ

საკვანძო სიტყვები:

რომის სტატუტი

შეიარაღებული კონფლიქტი

კომპიუტერული მონაცემები

მონაცემების დაცვა

აბსტრაქტი

საერთაშორისო სამართალი, განსაკუთრებით კი საერთაშორისო ჰუმანიტარული სამართალი, უზრუნველყოფს არამკაფიო და შეზღუდულ ჩარჩოს პირადი მონაცემების დაცვისათვის შეიარაღებული კონფლიქტის დროს განხორციელებული კიბეროპერაციების კონტექსტში. ნაშრომი განიხილავს პირადი მონაცემების სამართლებრივ სტატუსს საერთაშორისო კიბეროპერაციებში და აფასებს, შესაძლებელია თუ არა სამოქალაქო მონაცემების წინააღმდეგ მიმართული კიბერაქტივობები მოექცეს საერთაშორისო ჰუმანიტარული და საერთაშორისო სისხლის სამართლის მოქმედი რეჟიმების ფარგლებში. ნაშრომში არგუმენტირებულია, რომ საერთაშორისო ხელშეკრულებების მიღებისა და საერთაშორისო ჩვეულებითი სამართლის ჩამოყალიბების პერიოდში ელექტრონულად შენახული პირადი მონაცემები არ იყო მოაზრებული საერთაშორისო ჰუმანიტარული სამართლის მიერ დაცულ ობიექტებად. მიუხედავად იმისა, რომ თანამედროვე საერთაშორისო სამართლებრივი მიდგომები სულ უფრო მეტად უჭერს მხარს კომპიუტერული მონაცემების „ობიექტად“ ან „საკუთრებად“ დახასიათებას, სახელმწიფო პრაქტიკა კვლავაც არაერთგვაროვანია. ნაშრომი ასევე აფასებს, მონაცემების წინააღმდეგ მიმართული კიბეროპერაციების სამართლებრივ სტატუსს და მის განმარტებასთან დაკავშირებულ სირთულეებს. დასკვნის სახით აღნიშნულია, რომ მშვიდობიან პერიოდში მოქმედი მონაცემთა დაცვის სტანდარტების უპირობო გავრცელება შეიარაღებულ კონფლიქტზე შესაძლოა ეწინააღმდეგებოდეს საერთაშორისო ჰუმანიტარული სამართლის ჰუმანიტარულ მიზნებს.

[2] ავტორი კორესპონდენტი.
ელექტრონული ფოსტა: Guram.gvinjilia@ciu.edu.ge (გ. ღვინჯილია).
ORCID: https://orcid.org/0009-0002-7608-6683

1. Introduction

Cyber operations have become an increasingly prominent component of contemporary armed conflicts, generating complex legal questions regarding the interpretation and application of the Rome Statute of the International Criminal Court (International Criminal Court, 1998). One particularly significant issue concern whether cyber operations directed against data during armed conflict may fall within the scope of war crimes under international criminal law. This article examines that question by analysing whether cyber operations targeting computer data could, under certain circumstances, constitute conduct prohibited by the legal framework governing war crimes. Central to this analysis is the interpretation of International Humanitarian Law (IHL), which has been incorporated into international criminal law through Article 8 of the Rome Statute, the provision defining war crimes within the jurisdiction of the International Criminal Court (ICC).

The extent to which IHL regulates cyber operations affecting civilian data remains a contested issue in contemporary legal scholarship. Much of the existing debate has focused on whether data can be regarded as an "object" within the meaning of IHL targeting rules. The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Schmitt, 2017) reports that the majority of experts considered the intangible character of data to preclude its classification as an "object" independently protected under IHL. At the same time, a number of experts have argued in favour of a broader interpretation of the concept of "object," suggesting that such an interpretation could encompass computer data. In addition, cyber operations affecting data may fall within the protective scope of IHL if the affected data can be understood as a form of "property." Consequently, the ability of Article 8 of the Rome Statute to address cyber operations targeting civilian data, particularly in situations where no direct physical damage occurs, depends largely on whether the ICC interprets data as falling within the legal categories of object or property.

This article evaluates the soundness of including computer data within these categories as they appear in the Rome Statute. As a preliminary step, Section 4.1 examines the nature of computer data and explains why its classification within traditional legal notions of objects and property remains controversial. The section highlights the conceptual difficulties of applying legal categories developed for tangible entities to digital phenomena with predominantly intangible characteristics.

Section 4.2. provides an outline of the different types of cyber operations that may be conducted against or through computer data. While some cyber operations produce immediate kinetic consequences comparable to those caused by traditional military attacks, others generate effects that are more indirect and causally remote. Such effects may be difficult to measure or attribute, thereby complicating their legal assessment within the framework of international humanitarian law and international criminal law.

Section 4.3. forms the core analytical component of the article and examines the circumstances when cyber operations targeting civilian computer data may be deemed war crimes under the Rome Statute. Bearing in mind the divergent views expressed by legal experts, this article argues that computer data should, if nothing else, be understood as a built-in element of digital networks and systems consisting of physical infrastructure, including hardware components, cables, and microprocessors, which clearly fall within the categories of "objects" and "property." In practice, it is difficult to establish a strict distinction

between data regarded as purely intangible and the physical technological systems within which such data is embedded and upon which these systems depend for their operation. Nevertheless, the current state of international law provides insufficient support for treating data itself as an independent category of object or property. Accordingly, establishing criminal responsibility would require demonstrating a connection between interference with computer data and a measurable impact on protected objects or property.

The final section explores the wider ramifications of this analysis for the interpretation of the Rome Statute. It explores whether the Statute can adequately respond to emerging forms of warfare in areas where legal norms remain underdeveloped, while simultaneously respecting the principle of legality that governs international criminal law. The section also examines whether a cyber operation resulting solely in the destruction of computer data, without additional physical or material consequences, could satisfy the gravity threshold required for admissibility before the ICC. The article concludes by examining future challenges that cyber operations pose for the Court and the need for continued legal clarification in this rapidly evolving area of armed conflict.

2. Literature Review

The existing literature on cyber operations and international humanitarian law demonstrates that the legal status of computer data remains one of the most unsettled issues in contemporary armed conflict. A first group of sources explains why data resists traditional legal classification. Daskal (2015) shows that digital data challenges territorially based legal frameworks because of its mobility, divisibility, location independence and reliance on third-party control. Ritter and Mayer (2017) similarly examine the difficulties of regulating data through property-based concepts, emphasizing that digital information may be controlled, transferred and economically exploited, while remaining conceptually distinct from tangible property.

A second body of literature concerns the application of IHL to cyber operations. The Tallinn Manual 2.0 reflects the dominant expert view that computer systems and networks may qualify as objects, whereas data itself generally does not, due to its intangible character (Schmitt, 2017). Schmitt (2019) further supports a cautious approach, warning that an overly broad interpretation of “object” may extend IHL targeting rules beyond their established legal foundation. At the same time, other scholars and institutions argue that strict tangibility requirements may create protection gaps. Mačák (2018, 2020) contends that computer data can be destroyed, captured or neutralized in ways that resemble the treatment of traditional military objectives. Horowitz (2022) likewise emphasizes that excluding civilian data from proportionality and targeting assessments may undermine the humanitarian purpose of IHL.

The ICRC has played a central role in framing the humanitarian implications of cyber operations. Its commentary to Additional Protocol I traditionally associates objects with material and tangible things (International Committee of the Red Cross, 1987), while its later work on cyber operations stresses that civilian societies increasingly depend on digital systems and data (International Committee of the Red Cross, 2021). Gisel, Rodenhäuser and Dörmann (2020) further underline the dependence of essential civilian services on information and communication technologies.

Finally, directly addressing international criminal law is particularly important for this article. McKenzie (2019, 2021) examines whether cyber operations against civilian data may fall within war crimes provisions concerning protected objects and property, while Harrison Dinniss (2012) distinguishes between content-level and operational-level data. Taken together, the literature reveals a central tension between legality, technological reality and humanitarian protection, which this article seeks to address through a functional interpretation of data within protected civilian systems.

3. Materials and Methods

The article is based primarily on the examination and critical assessment of documentary legal materials. The author studied a broad range of primary legal sources, including international treaties, instruments of international humanitarian law, international criminal law provisions, documents adopted by international organizations, official State positions, military manuals, and relevant case law. Particular attention was given to the Rome Statute of the International Criminal Court, the Geneva Conventions, Additional Protocol I, the Hague Regulations, the Convention on Cybercrime, and the General Data Protection Regulation. The research also examined jurisprudence of the International Criminal Court and the International Court of Justice, including decisions relevant to the interpretation of protected objects, property, gravity, and the treatment of documents and data. In addition, selected domestic judicial decisions were considered where they illustrate how courts have approached the legal characterization of digital data as movable property, intangible property, or information distinct from its physical medium.

The research also relies on secondary sources, especially academic literature and expert commentary concerning cyber operations, international humanitarian law, and international criminal law. The author examined the Tallinn Manual 2.0, ICRC materials, International Law Association documents, and scholarly works by Daskal, Schmitt, Mačák, McKenzie, Harrison Dinniss, Horowitz, Gisel, Rodenhäuser and Dörmann, Ritter and Mayer, and Dinstein. These materials were used to identify the principal doctrinal disagreements regarding whether computer data may be treated as an object or property under IHL, and whether cyber operations affecting data may fall within the Rome Statute's war crimes framework.

Several scientific research methodologies were used while preparing the article. First, the doctrinal legal method was applied to identify, interpret and systematize the relevant rules of international humanitarian law and international criminal law. This method made it possible to analyse the meaning of legal concepts such as “object,” “property,” “attack,” “destruction,” “seizure,” and “military objective” in their normative context. Second, the comparative legal method was used to assess different State positions, military manuals, scholarly approaches and domestic judicial interpretations concerning the legal nature of computer data. Third, the documentary research method was applied through the study of treaties, institutional reports, expert manuals, court decisions and academic writings. Fourth, qualitative case-law analysis was used to evaluate how international and domestic courts have interpreted concepts relevant to tangible and intangible property, protected objects and gravity. Fifth, systematic and teleological methods were used to interpret the relevant legal rules in light of the structure and humanitarian purpose of IHL. Finally, a normative analytical method was employed to assess whether existing legal categories can be adapted to cyber realities without violating the principle of legality. The research is limited by the

scarcity of consistent State practice and the absence of authoritative ICC jurisprudence directly addressing cyber operations against civilian data.

4. Discussion of Findings

The findings demonstrate that contemporary international humanitarian law remains unsettled regarding the legal status of computer data during armed conflict. The analysis confirms that neither the Rome Statute nor the principal IHL treaties expressly regulate cyber operations directed exclusively against data, thereby leaving considerable scope for legal interpretation. The comparative assessment of State practice and scholarly opinion reveals two competing approaches. The first, reflected in the majority position of the Tallinn Manual 2.0 and supported by several States, generally excludes data from the category of protected objects because of its intangible character. The second, represented in the writings of Mačák, McKenzie and the ICRC's more recent cyber-related work, favours a broader interpretation capable of preventing protection gaps in increasingly digitalized societies.

Against this background, the article advances a functional and system-oriented interpretation that differs from both extremes. It does not argue that computer data should automatically or invariably constitute an autonomous object or form of property under international humanitarian law. Rather, it proposes that data should ordinarily be understood as an integral component of protected civilian systems, networks and technological infrastructure. This approach better reflects the operational reality of modern digital environments, where the disruption, deletion or manipulation of data may disable hospitals, governmental institutions, financial networks, water systems, communication platforms or other civilian infrastructure, even when no immediate physical destruction occurs.

This interpretation also offers a more coherent balance between humanitarian protection and the principle of legality. It avoids the creation of entirely new criminal offences while allowing existing legal categories to respond to serious cyber operations that produce foreseeable functional harm. In this sense, the proposed approach remains more restrained than the claim that all data is independently protected as an object, but more protective than the view that only physically destructive cyber operations can fall within the scope of IHL and the Rome Statute.

At the same time, the findings must be assessed with caution. The absence of extensive State practice, the limited number of judicial decisions, and the rapidly evolving nature of cyber operations prevent definitive conclusions. Future research should therefore examine attribution, evidentiary standards, thresholds of functional harm, proportionality assessment in data-driven environments, and the emerging positions of States and international courts. These issues will be decisive in determining whether international criminal law can respond effectively to serious cyber operations while preserving legal certainty and doctrinal coherence.

4.1. Conceptualizing Computer Data in International Law

At its core, data may be understood as information. The Oxford English Dictionary defines data as "related items of (chiefly numerical) information considered collectively, typically obtained through scientific work and used for reference, analysis, or calculation." (Oxford English Dictionary Online, 2020). In the context of computing, the term refers to "quantities, characters, or symbols on which operations are performed by a computer" (Oxford English Dictionary Online, 2020) and more broadly to

information existing in digital form. Considering the pivotal role that data plays in modern social, economic, and governmental activities, it is unsurprising that states, international organizations and courts have increasingly confronted questions regarding how such information should be a subject to regulation.

This article focuses specifically on computer data, understood as information captured by electronic or digital means that can be retrieved, whether it is directly perceivable by humans or processed primarily by machines (Ritter, 2017). Determining whether and how such data should be addressed by current legal regimes presents considerable conceptual challenges. As Jennifer Daskal observes, computer data disrupts traditional legal frameworks, particularly those relying on territorial distinctions as a basis for legal regulation and jurisdiction (Daskal, 2015).

Many legal systems rely on geographically defined concepts to determine the applicability of legal rules. Jurisdictional frameworks, for example, rely on the capacity to distinguish between legally relevant spaces, often conceptualized as the boundaries between “here” and “there.” However, the characteristics of computer data complicate these assumptions. According to Daskal, several features of digital data undermine conventional territorial approaches, including its location independence, divisibility, mobility, intermingling with other data, and frequent reliance on third-party control. These characteristics make it difficult to apply legal categories originally designed for tangible property and geographically fixed objects.

Some of these features illustrate particularly clearly how computer data challenges traditional legal classifications. First, computer data is highly mobile and divisible. The speed with which digital information can move across networks complicates conventional understandings of movement and storage. For example, an email transmitted between individuals located in the same city may nevertheless pass-through servers or communication infrastructure located in another jurisdiction. Similarly, data stored through cloud-based services may be transferred automatically between servers situated in multiple countries.

In addition, digital information can be easily copied, divided into segments, and stored simultaneously in numerous locations, often without the knowledge of the user. Although physical documents may also exist in multiple copies, the simplicity and rapidity with which digital data can be replicated and transferred has led to a significant expansion of multisite, and frequently multinational, data storage practices.

Another defining characteristic is the separation between the location from which data is accessed and the physical infrastructure in which that data is stored. This phenomenon, described by Daskal as “location independence,” further complicates legal regulation. In practice, users frequently are unaware of the physical whereabouts of their data, nor is such information typically relevant to their interaction with digital services. At the same time, identifying the physical location of data does not unequivocally reveal the location of the individual accessing or controlling it.

Taken together, these characteristics demonstrate how computer data challenges traditional legal frameworks that rely on physical location, tangible property, and clearly identifiable jurisdictional

boundaries. Consequently, determining how existing legal regimes, including those applicable to armed conflict, should address cyber operations affecting computer data remains a complex and evolving issue.

The terms “object” and “property” are widely recognized in law to refer to tangible entities. Assessing whether these concepts may incorporate computer data therefore requires examining whether data can be regarded as possessing some form of tangibility. In certain respects, it can. Computer data is invariably integrated within physical hardware that enables its storage, processing, and retrieval. Although some data can be accessed through multiple devices and formats, in other situations the functioning of a particular device depends entirely on the data it processes in order to perform its intended tasks. From this perspective, computer data may be viewed as an integral component of a physical system. Depending on the method of storage, data may exist in the dyes of an optical disk, in the configuration of switches within a microchip, on magnetic storage media, or as light pulses transmitted through fibre-optic cables.

In each of these instances, data exists within a material structure. Furthermore, although digital information can be transferred between different forms of storage, any interaction with such data whether reading, modifying, copying, or removing it entails physical engagement with computer hardware. The close interrelationship between information and the physical infrastructure that enables its processing highlights the importance of clarifying the degree to which computer data is regulated by current legal frameworks.

Certain legal definitions of data reflect this relationship by referring not only to the informational content itself but also to the systems through which that information is processed. For instance, the Convention on Cybercrime defines computer data as any representation of facts, information, or concepts in a form suitable for processing within a computer system, including programs capable of causing such systems to perform specific functions (Convention on Cybercrime, 2001). The same instrument defines a computer system as a single device, or group of interconnected devices, that performs automated data processing pursuant to a program. This approach builds upon earlier work of the International Organization for Standardization, which defined data as information in electronic form capable of direct computer processing. Similarly, the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Schmitt, 2017) characterizes data as the fundamental element processed or generated by a computer to convey information.

Other legal regimes adopt wider and technology-neutral definitions that emphasize the informational nature of data rather than its technological context. For example, the European Union's General Data Protection Regulation defines personal data as any information relating to an identified or identifiable natural person. This definition encompasses both forms of information specific to digital environments, such as IP addresses, location data, or online identifiers, and information that exists independently of cyberspace, including a person’s name or address.

Conceptualizing data primarily as information allows it to be distinguished from the hardware through which it is stored or accessed. Cloud computing provides a clear illustration of this distinction. Governmental or private-sector data is frequently stored on infrastructure operated by third-party providers, such as Amazon Web Services. While such companies own and maintain the physical servers on which the data is stored, they do not necessarily possess ownership of the data itself. Consequently, a

cyber operation directed at such infrastructure might destroy or extract civilian data while leaving the physical systems supporting its storage and transmission largely intact.

Neither the ICC nor related instruments of international humanitarian law provide a specific definition of computer data. As a result, the extent to which these legal frameworks should treat data as analogous to physical objects or property remains contested. For international criminal law and IHL to be effectively applied to emerging technologies, it is essential to consider how the International Criminal Court may assess the relationship between digital data and its underlying physical systems that facilitate its use, particularly in relation to legal concepts such as attack, destruction, seizure, or appropriation.

4.2. Typology of Cyber Operations against Data in Armed Conflict

Obtaining reliable information about the scope and consequences of cyber operations remains difficult. The nature of cyberspace means that many operations are not publicly disclosed, and their full effects on governments, companies, and individuals are often challenging to measure. Nevertheless, certain cyber operations produce outcomes comparable to traditional military actions that generate kinetic effects (Zetter, 2014). A frequently cited example is the Stuxnet malware, which targeted Iranian nuclear centrifuges by manipulating the digital control systems responsible for their operation. Although the method employed was technologically novel, the outcome was conventional in nature: the centrifuges sustained physical damage.

Other cyber operations produce effects that are somewhat further removed from direct physical destruction but still result in observable consequences in the physical world. For instance, in May 2020 reports indicated that a cyber operation attributed to Israel disrupted the functioning of an Iranian port for several days, resulting in substantial operational disruptions. The operation was presumably undertaken in response to a failed Iranian cyber attempt targeting the command-and-control systems of Israel's water distribution infrastructure (Bergman, 2020). In such cases, the cyber activity does not directly destroy physical infrastructure but interferes with the functioning of systems in ways that produce tangible real-world consequences.

A third category involves operations whose effects are visible but more difficult to quantify. These may include situations in which individuals or organizations temporarily lose access to important digital services or stored information. In February 2020, several states accused Russia of carrying out a cyber operation against Georgia that disabled thousands of governmental, private, and media websites, rendering them inaccessible for a period of time (Corera, 2020). Although such incidents may not involve physical destruction, they can significantly disrupt essential communication and administrative functions.

Each of these examples can, in a broad sense, be understood as an operation conducted through or against computer data. Cyber actors manipulate data and software within digital systems in order to alter or disrupt their operation. However, these incidents are often more accurately conceptualized as attacks on the broader systems within which the data operates rather than as attacks on data itself. The Stuxnet operation is commonly described as a kinetic attack conducted via cyber means against physical centrifuges. Similarly, the interruption of the Iranian port may be interpreted as an assault on port infrastructure because of its operational consequences. The operation affecting Georgian websites can

likewise be viewed as an attack directed against governmental, commercial, and private institutions via the digital systems they rely upon.

In the setting of military conflict, some academics of IHL advocate a cautious approach, suggesting that cyber operations should only be under the umbrella of IHL targeting rules where they produce measurable kinetic effects (Schmitt, 2017). Under such an interpretation, only the Stuxnet example among those discussed would clearly satisfy the relevant threshold. However, adopting such a restrictive view risks leaving significant aspects of civilian digital infrastructure outside the protective scope of IHL and may fail to reflect the realities of modern warfare.

This limitation is particularly significant given the central role those digital technologies now play in civilian life. As noted by Laurent Gisel, Tilman Rodenhäuser, and Knut Dörmann, data constitutes a fundamental component of the digital environment and is essential to the functioning of many contemporary societies (Gisel et al., 2020). The widespread dependence on information and communication technologies amplifies the vulnerability of numerous real-world systems to disruption or manipulation through cyber means. Such vulnerabilities extend across a wide range of sectors, including industry, telecommunications, transport networks, financial systems, and governmental infrastructure, as well as critical civilian services.

Particularly sensitive sectors include healthcare, electricity supply, and water and sanitation systems. An illustrative example occurred in February 2021 when hackers gained remote access to the control software of a water facility in Oldsmar, Florida. The attackers tried to raise the concentration of sodium hydroxide in the water supply to hazardous levels. Fortunately, the intrusion was detected before the alteration took effect, preventing potentially serious harm.

4.3. Cyber Operations against Data and the Threshold of War Crimes under the Rome Statute

The widespread use of the internet means that conduct falling within the scope of crimes defined in the Rome Statute of the International Criminal Court may, at least in part, occur in the digital environment. For instance, the crime of direct and public incitement to commit genocide may be carried out through online platforms, including social media. In a similar manner, cyber operations directed against data could, under certain circumstances, constitute war crimes within the meaning of the Statute.

This possibility arises because several provisions defining war crimes refer explicitly to “objects” (ICC Statute). Computer data could potentially fall within this category if it is interpreted as an object in its own right. Alternatively, data may be regarded as embedded within a physical object, such that an operation targeting data also affects the object of which it forms a part. In addition, a number of provisions concerning war crimes refer to “property” (ICC Statute). Within this framework, either computer data itself, or the technological systems in which it is stored and processed, may be regarded as forms of property.

A central issue therefore concerns how the terms “object” and “property” should be interpreted in the relevant provisions of the Rome Statute, as well as in the corresponding rules of IHL. The link among these two concepts is not entirely clear. It is possible that the phrase “objects which are not military objectives,” contained in Article 8(2)(b)(ii) of the Rome Statute, encompasses the full range of civilian

property. However, it could also be interpreted as protecting either a narrower or a broader category of material entities.

Before examining these concepts in greater detail, it is necessary to acknowledge an additional legal debate concerning the meaning of the term “attack.” Under IHL, an attack is generally defined as an act of violence, whether offensive or defensive, directed against an adversary. This notion is central to the regulation of the conduct of hostilities and to the definition of several war crimes involving protected objects and property. However, scholars continue to debate what precisely constitutes an “act of violence” in the cyber context and how cyber operations that qualify as attacks can be distinguished from those that do not.

Further complexity arises from the fact that, for the purposes of IHL, an attack must occur within the context of an armed conflict. Questions therefore arise regarding the circumstances in which cyber activities may be considered part of hostilities and whether particular intent or motivation is required for such operations to qualify as attacks under international law.

Although a comprehensive examination of these issues lies beyond the scope of this article, the argument developed here remains relevant to them. If computer data is understood as embedded within and forming part of physical technological systems, then actions directed at data, such as its appropriation, deletion, destruction, or seizure, may also affect the physical objects that contain it. Where cyber operations against data result in direct physical damage to tangible objects, they can clearly be characterized as attacks and therefore fall within the scope of IHL.

More difficult questions arise in situations where cyber operations do not produce immediate physical consequences. In such cases, the legal assessment must consider whether actions that degrade the functioning of a computer system or cause the temporary or permanent loss of access to digital information may nevertheless amount to an attack on an object or the appropriation, destruction, or seizure of property. The following sections address these questions in greater detail.

4.3.1. Can Computer Data Qualify as an “Object” under IHL?

The central issue is whether computer data can itself qualify as an “object” under International Humanitarian Law and therefore receive protection under the war crimes provisions of the Rome Statute of the International Criminal Court. State practice on the categorization of data remains limited and inconsistent, and scholarly opinion is similarly divided. The most commonly expressed view maintains that only cyber operations producing kinetic damage to a tangible civilian object satisfy the requirements to be qualified as war crimes. Under this approach, reversible operations that merely impair the functioning of a system would fall outside the scope of these crimes. Pursuant to this interpretation, the relevant object is not the data itself but the physical item that has sustained damage.

A more versatile approach considers data as embedded within and integral to physical computer systems understood as objects. From this perspective, a cyber operation targeting data that significantly detracts from the functionality of a system could potentially be characterized as an assault on that system. Conversely, the most far-reaching interpretation treats data as an “object,” capable of being attacked through its destruction or through interference that prevents its use.

The relevant war crimes provisions aim to protect “civilian objects”, defined negatively as objects that do not constitute military objectives. However, neither the Rome Statute nor the Elements of Crimes provide a detailed definition of these concepts. Because these terms derive from IHL, their interpretation requires reference to the treaty and customary law foundations underlying these crimes. Article 52 of Additional Protocol I (United Nations, 1977) to the Geneva Conventions (United Nations, 1949) provides that attacks must be strictly limited to military objectives, defined as objects which, by their nature, location, purpose, or use, effectively contribute to military action and whose destruction, capture, or neutralization offers a definite military advantage (Dinstein, 2016).

A key question in the debate is whether objects must be tangible. The International Committee of the Red Cross Commentary (ICRC, 1987) to Additional Protocol I (United Nations, 1977) suggests that objects are limited to material and tangible things. Relying on this interpretation, the majority of experts involved in the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Schmitt, 2017) concluded that computers, networks, and cyber infrastructure may qualify as objects, whereas computer data itself does not.

State positions remain inconsistent. Israel has excluded data from the category of objects on the basis that tangibility is required. On the contrary, France has stated that civilian data should be protected as an object under IHL, arguing that excluding it would undermine the humanitarian purpose of the law. The Norwegian military manual similarly recognizes that data may constitute an object when lawfully targeted. Other states adopt more cautious approaches. Denmark acknowledges that although data is not generally considered an object, damage to or deletion of certain irreplaceable data may produce effects comparable to physical destruction and should therefore be treated as collateral damage. Peru, Chile, and Guyana emphasize the potentially significant consequences of data manipulation. Meanwhile, Australia appears to favour a requirement for tangible effects, while Iran has suggested that cyber operations resulting in material damage to persons or property may amount to a use of force. A legal advisor of the United States Department of State has likewise left open the possibility that data could qualify as an object where a cyber operation constitutes an attack under IHL.

The International Committee of the Red Cross acknowledges that the question of whether and to what extent civilian data constitutes a civilian object remains unresolved, although it expresses support for an expansive interpretation. It argues that data within the category of objects aligns with the humanitarian purpose of IHL, particularly given the potential harm to civilians if cyber operations disrupt governmental services or private activity.

By contrast, Michael N. Schmitt supports a narrower interpretation, excluding data from the definition of object. He contends that treating data as an object risks overextension, as many cyber operations targeting data resemble psychological operations rather than physical attacks (Schmitt, 2019).

Nevertheless, the term “object” denotes a broad and adaptable category capable of evolution. On this basis, Dávid Mačák argues that, interpreted in light of contemporary conditions, particularly given that the relevant treaty was concluded for long-term application, the concept of object does not necessarily require tangibility (Mačák, 2018). Moreover, the French and Spanish authentic versions of Additional

Protocol I (United Nations, 1977) employ the term “bien,” which is not limited to physically tangible entities, further supporting a non-restrictive interpretation.

Dávid Mačák further argues that computer data can be destroyed, captured, or neutralized and, in this respect, more closely resembles tangible objects, such as bridges, than abstract concepts like morale (Mačák, 2018). While morale is inherently subjective and cannot be objectively verified, a bridge either remains intact, is damaged, or ceases to exist; its condition is determinable independently of perception. On this basis, data may similarly be treated as an entity whose existence and condition can be objectively assessed.

A significant justification for this broader interpretation is teleological. Proponents argue that including data within the notion of “object” better serves the protective purpose of International Humanitarian Law. As Hadar Horowitz notes, a narrow interpretation of “civilian objects” risks creating a protection gap and may encourage cyber operators to exclude the destruction of civilian data from proportionality assessments. Likewise, a minority within the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Schmitt, 2017) contended that the majority approach is overly restrictive and could allow the deletion of essential civilian datasets, such as social security records, tax files, or banking information, to fall beyond the scope of IHL, contrary to the principle that civilians enjoy general protection from the effects of hostile acts.

Omitting data from the category of object could result in situations where targets whose physical counterparts are clearly protected under IHL would be deemed lawful so long as the effects remain confined to cyberspace, a consequence some scholars describe as manifestly unreasonable. Given the capacity of cyber operations to aim civilian networks and infrastructure, the implications of such exclusion may be substantial. Accordingly, some commentators question whether the concept of “object” within targeting rules necessarily requires corporeal existence.

These normative considerations provide strong arguments in favour of a broader interpretation. It is generally accepted that destruction of data may produce harmful consequences even where the underlying system continues to function and physical replacement is unnecessary.

However, scholars also emphasize that not every interference with data amounts to an attack on an object. Mačák sets apart the susceptibility of data to harm and the intensity of harm required to trigger legal consequences. While all data may be capable of being harmed, only certain forms of interference, such as deletion or alteration, are likely to meet the requisite threshold; mere misappropriation or misuse may not. Although assessing intensity may prove challenging, such gradations are familiar within legal doctrine. The possibility that data can sometimes be recoverable does not negate its susceptibility to destruction. Because data destruction can be objectively verified, despite potential evidentiary difficulties, the analogy with purely psychological operations should not be extended to exclude data categorically.

Heather Harrison Dinniss proposes a narrower distinction between content-level and operational-level data. Content-level data (e.g., text or database information) would generally be protected only where specific IHL provisions apply, while operational-level data, responsible for system functionality, may,

when destroyed, cause loss of functionality. Although state practice is limited, she suggests that states tend to treat disruptions affecting system functionality differently from those merely involving content data. She therefore argues that the two categories should be analysed separately (Dinniss, 2012).

By contrast, Michael N. Schmitt contends that approaches based primarily on consequences lack firm legal grounding beyond general appeals to object and purpose (Schmitt, 2015). In his view, insufficient state practice and *opinio juris* currently support treating data as an object. While this may represent the prevailing interpretation, the novelty of cyber operations means that the absence of extensive practice is neither unexpected nor necessarily determinative.

4.3.2. Identifying the Target: Data, Systems, and the Object of Attack

The war crimes discussed apply exclusively to attacks against "objects," making it essential to determine which object is targeted. If the data itself is not the relevant object, its legal status may not dictate the applicability of IHL. Divergences in the literature partly arise from differing approaches to identifying the object under attack. As previously noted, assessing data in isolation risks abstraction, obscuring the reality that data is invariably embedded in systems, processes, and physical objects, many of which may already enjoy protection under IHL.

This concern underlies the use of illustrative scenarios to examine whether data should be regarded as an object. Dávid Mačák considers critical military data, such as air traffic control information or weapons logs, to demonstrate circumstances in which data might constitute a military objective (Mačák, 2018). Civilian data, however, presents the most complex scenario. Hospital records, frequently cited in scholarship, illustrate the potential consequences of data interference: clandestine deletion or alteration of such data could endanger patient lives, compromising both the soundness of civilian data and the security of the civilian population.

Michael N. Schmitt cautions that the hospital example may be misleading, as an attack on the hospital itself would be unlawful regardless of whether the data were directly targeted, due to the foreseeability of harm to patients (Schmitt, 2019). This interpretation aligns with widely accepted IHL principles: belligerents are required to respect and safeguard medical facilities and personnel in any circumstance, and ensure the protection of objects indispensable to civilian survival. This protection extends beyond direct attacks; interference that obstructs medical operations, for instance, by impeding the delivery of supplies or preventing the continuation of treatment, is prohibited.

Similarly, the International Law Association, while not definitively classifying data as an object, recognized that certain protected categories, such as water systems, medical units and cultural property, ought to be understood to extend to associated data. Operations aimed at deleting, damaging, or manipulating such data are therefore prohibited under IHL.

The law must also account for cyber operations that leave physical systems intact yet cause significant indirect harm. The hospital scenario exemplifies this: lack of access to critical data may prevent doctors and nurses from making informed decisions or disrupt patient flow management. For instance, in September 2020, in Germany woman became victim of a ransomware attack which delayed hospital admission by one hour. Prosecutors deemed charging the hackers with negligent homicide but ultimately

did not, due to the patient's underlying condition. Nonetheless, the case illustrates that foreseeable cyber-induced disruptions to civilian services may imminently cause harm or death, highlighting the importance of including such indirect effects in the IHL assessment.

Ultimately, these scenarios underscore that the law must consider not only the physicality of objects but also the functional and protective role of data embedded within them, particularly where interference may foreseeably jeopardize civilian life.

If this reasoning applies to hospital systems, it raises the question of why it should not equally apply to other governmental infrastructures. For example, a cyber operation targeting governmental computer systems could disrupt the distribution of welfare payments, potentially contributing to increased poverty or related social harms. Similarly, interference with justice-sector networks, used to administer courts, manage detention facilities, and coordinate law enforcement, could result in prolonged detention, impede judicial processes, or prevent police responses to criminal activity. Such consequences are tangible and measurable, and they carry a clear potential to affect human life and well-being. Although the chain of causation connecting the cyber operation and the resulting harm may be more complex than in traditional kinetic scenarios, the effects may nonetheless be foreseeable: by denying access to essential information, the operation may cause systemic failure and consequent civilian harm. From this perspective, such conduct may be conceptualized not as an attack on data per se, but rather as an attack directed against the system or infrastructure with data incorporated in it.

This highlights the limitations of treating data purely as abstract information, detached from the computer code, electrical signals, hardware components, and broader systems that enable its storage and operational use. Data exists within a technologically and physically grounded environment. An analogy may be drawn to paper files stored in a physical filing cabinet. From the standpoint of IHL, it would be artificial to separate the informational content of documents from the material objects in which they are contained. If a filing cabinet qualified as a military objective because it held operationally significant plans, the determining factor would be the information it contains; however, the physical medium would remain integral to the analysis. Conversely, where the contents relate solely to civilian matters, such as social security administration, the object would remain protected from attack.

Distinguishing when harmful consequences arising from operations affecting data are closely linked to tangible effects to fall within IHL regulation will inevitably require careful assessment. Introducing a severity threshold for harm, as well as limiting consideration to consequences that are reasonably foreseeable, would provide principled constraints. Although such evaluations involve complex value judgments, they are consistent with established methods in international criminal law.

A more direct and protective interpretative approach would consider data as an integral component of a physical system that may be targeted. Under this framework, the relevant object would be the system and infrastructure within which data is embedded, rather than the data in isolation. While not all operations against data will meet the threshold of an "attack," some will, particularly where significant and foreseeable consequences arise. Should the International Criminal Court adopt this interpretation, it could enhance civilian protection and contribute to the gradual evolution of international criminal law and IHL.

Nonetheless, the Court may also adopt a more cautious interpretation, declining to treat computer data as part of an "object" for war crimes purposes. Currently, there is no clear consensus among states or scholars on this issue. The ultimate resolution will depend largely on the interpretative approach used by the Court, a matter addressed in the following section.

4.3.3. Computer Data as Property under IHL

War crimes concerning the appropriation, destruction, or seizure of property, rooted in the Geneva Conventions (United Nations, 1949) and the Hague Regulations of 1907, may provide an additional legal basis for establishing criminal responsibility for cyber operations directed against civilian data. Within this framework, data itself, or the technological systems in which it is stored and processed, could potentially be regarded as a form of property. However, the question of whether the notion of "property" encompasses digital data was not addressed during the drafting of the Rome Statute of the International Criminal Court, nor in earlier foundational instruments of IHL.

Clarifying this issue is particularly significant given the continuing debate regarding the temporal scope of the rules governing attacks under Additional Protocol I (United Nations, 1977) to the Geneva Conventions (United Nations, 1949). While disagreement persists concerning the precise limits of these rules, it is possible that the broader protections afforded to property under international humanitarian law extend beyond conduct that qualifies as an "attack" in the strict legal sense. As a result, certain cyber operations affecting civilian data systems—although not meeting the legal threshold of an attack—may still fall within the scope of prohibitions against the destruction, appropriation, or seizure of protected civilian property (McKenzie, 2021).

4.3.3.1. Defining Property: Can Digital Data be Owned?

The common meaning of the term "property" generally refers to a thing, typically material, that belongs to an individual or a group. Because the relevant war crimes provisions do not expressly restrict this concept through additional qualifiers, it is plausible to adopt a broad interpretation under which property encompasses anything capable of ownership. From this perspective, digital data could potentially fall within the notion of property. In the language of the applicable provisions, data may be destroyed or appropriated. A related issue has emerged in discussions concerning the seizure of land, namely whether appropriation requires a formal legal transfer, such as a change in title. A broader interpretation suggests that de facto control may be sufficient, with emphasis placed on those who actually control, manage, or utilize the asset in practice. Although the application of this reasoning to digital data may be more complex than with traditional forms of property, it remains conceptually possible (McKenzie, 2019).

The notion of property also plays a central role in numerous legal systems beyond International Humanitarian Law. Policymakers and courts at both international and domestic levels have therefore examined whether data should fall within legal frameworks designed to protect property rights, adopting a variety of approaches. Although the following overview is not exhaustive, it illustrates several models that may inform interpretation within international humanitarian and criminal law.

International jurisprudence on the property status of digital data remains limited. In Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v Australia) before the

International Court of Justice (ICJ), Timor-Leste implicitly treated data as movable property for the purpose of determining the applicable legal rules. While the Court did not explicitly determine whether data constitutes property, it did not dismiss this characterization.

Domestic courts have addressed the issue more extensively. In 2020, the Italian Court of Cassation concluded that data could be regarded as movable property, reasoning that it can be appropriated, possessed, and transferred between digital media while retaining its structural characteristics. Some United States courts have similarly accepted that electronic documents and digital information may qualify as property. For instance, the New York Court of Appeals held that, for the purposes of the tort of conversion, a digital document possesses the same value as a physical document because its value derives from the information it embodies rather than in its physical medium. In Kremen v. Cohen, the United States Court of Appeals for the Ninth Circuit recognized an internet domain name as a form of intangible property, emphasizing that legal protection ought not to rely solely on the existence of a physical document.

Common law systems often rely on the definition of property articulated in National Provincial Bank Ltd v. Ainsworth, according to which property must be identifiable, definable, capable of assumption by third parties, and exhibit some degree of permanence. Some jurisdictions conclude that data fails to meet this test because it is essentially information accessible to others. For example, the Court of Appeal of England and Wales distinguished between the physical medium storing a database, which constitutes property, and the information itself, which does not.

Conversely, courts in New Zealand have taken a broader approach. In Dixon v R, the court accepted that data, although intangible, could still constitute property, noting that digital information possesses a form of physical existence and may be controlled, excluded, or deleted. Similar reasoning appeared in Henderson v Walker, where the court emphasized that data may be both excludable, through password protection or control over storage devices, and exhaustible, as it can be modified or erased.

Policy discussions have likewise produced divergent conclusions. The Japanese Ministry of Economy, Trade and Industry has suggested that data cannot be owned under the Japanese Civil Code due to its intangible nature. By contrast, in 2017 the German Federal Ministry of Transport and Digital Infrastructure proposed modifying the legal definition of data to allow clearer attribution of ownership rights.

As mentioned in the commentary to the Tallinn Manual 2.0, one widely accepted category of property already centers on information rather than physical objects: intellectual property. Such rights relate directly to informational content and may be owned, transferred, or misappropriated. If the sole record of information were destroyed, eliminating the medium that stored it could effectively result in the disappearance of the information itself.

Overall, this brief survey demonstrates that legal systems adopt inconsistent approaches to the treatment of data within property regimes. Ultimately, the issue returns to the broader question of how the ICC might conceptualize the relationship between information and the technological infrastructure through which it is stored or transmitted. Whether the Court would maintain a strict distinction between data and

hardware, or interpret the relevant provisions as encompassing data itself as property, remains uncertain. The diversity of existing approaches provides no definitive answer.

4.3.3.2. Unlawful Interference with Data: Destruction, Seizure, and Military Necessity

Even if one were to accept, and the ICC were to conclude, that digital data may qualify as a form of property, an additional issue arises: whether its appropriation, destruction, or seizure would be considered "unlawful" under IHL and, consequently, under the Rome Statute of the International Criminal Court. The prohibition on the destruction or seizure of property has deep historical roots in IHL. Article 23(g) of the Hague Regulations of 1907, as well as the earlier 1899 version, forbade belligerents from seizing or destroying enemy property unless such measures were imperatively required by military necessity.

The Geneva Conventions (United Nations, 1949) further developed these protections by establishing distinct standards for particular categories of protected property. For instance, they provide differentiated safeguards for civilian private property and hospitals in occupied territories and classify certain acts of destruction as grave breaches. Protection of property in occupied territories is particularly comprehensive. Article 53 of the Fourth Geneva Convention prohibits the destruction of real or personal property belonging to private individuals, the state, or public institutions, except where such destruction is imperatively required by military operations.

A key unresolved question is whether digital data could be considered protected property under IHL even if it is not categorized as an "object" within the meaning of Article 52 of Additional Protocol I (United Nations, 1977) to the Geneva Conventions (United Nations, 1949). Some support for including intangible assets within the concept of property can be found in post–Second World War jurisprudence. In the IG Farben Trial and the Krupp Trial, defendants were convicted of property-related offences despite the assets involved being largely intangible corporate shares and related rights.

More recent ICC jurisprudence suggests a narrower interpretation. In the Prosecutor v. Katanga and Ngudjolo Chui decision, the ICC Pre-Trial Chamber linked the notion of civilian property directly to the concept of "objects," indicating that civilian property comprises those objects that do not qualify as military objectives under Article 52(2) of Additional Protocol I (United Nations, 1977). Although restrictive, this approach promotes doctrinal coherence by aligning the definitions of "property" and "objects" across different war crimes provisions.

The issue has also been examined in the Tallinn Manual 2.0. Rule 149 addresses confiscation and requisition of property during occupation and, similar to the Manual's treatment of "objects," distinguishes between computer hardware and the data stored within it. The commentary indicates that a majority of experts considered computer hardware, such as computers and storage devices, to constitute movable state property, whereas data itself was generally not regarded as property. Nevertheless, the majority acknowledged that an occupying power might still use state data for military purposes and recognized that forms of "virtual" confiscation could occur when the occupier effectively gains control of property and denies its use to the original owner. A minority of experts, however, maintained that digital data could itself qualify as property.

An alternative analytical approach focuses on particular categories of data. Debates regarding the protection of cultural property suggest a greater willingness to recognize that, in certain circumstances, the destruction of digital information may amount to the destruction of protected cultural property. According to the commentary to Rule 142 of the Tallinn Manual 2.0, some experts argued that the concept of property need not be limited to tangible objects. Digital cultural materials, such as electronic archives, musical compositions, films, governmental records, or scientific data, may therefore qualify as protected property, particularly when the original works are inaccessible or destroyed, and reproduction is difficult or limited.

The commentary further clarifies that only serious forms of interference, such as alteration, damage, deletion, destruction, or military exploitation of such data, would fall within the prohibition. Temporary disruption of access, for example through interference with electronic systems, would generally fall outside the scope of cultural property protection. From a normative perspective, this approach resembles a severity-based model, in which protection depends less on the formal classification of data as property and more on the gravity of the consequences of its destruction.

Overall, there remains no clear consensus that digital data itself constitutes property. The absence of explicit guidance in foundational IHL instruments, combined with divergent approaches among states, makes the broadest interpretation, treating all data as property, difficult to sustain. A more balanced approach may therefore resemble that proposed in relation to "objects": although data itself may not constitute property, it can be understood as integrated within systems, computer networks, and infrastructure that clearly qualify as property under IHL.

4.4. Interpreting the Rome Statute in Light of Emerging Cyber Realities

As previously discussed, certain interpretations suggest that the terms "objects" and "property" appearing in certain provisions of International Humanitarian Law and in the definitions of related war crimes could encompass civilian data. The question, however, is whether adopting such a progressive interpretation would be appropriate when interpreting the Rome Statute of the International Criminal Court. A principal challenge lies in the limited evidence of supporting state practice, military doctrine, or international jurisprudence endorsing this position.

At the same time, it must be acknowledged that the legal status of digital data within computer networks has just lately emerged as relevant in the context of IHL. When addressing emerging technologies, an approach relying exclusively on established state practice and *opinio juris* may prove overly restrictive. As noted in scholarship on cyber operations, technological innovation inevitably introduces new concepts and categories for which consistent legal practice has not yet fully developed. In such circumstances, the application of widely recognized methods of treaty interpretation may assist in clarifying the scope of existing legal terminology, although some commentators caution that such exercises may remain partly speculative.

Recent developments suggest that the broadest interpretation—treating all data as falling within the protective regimes applicable to civilian objects or property—has become more difficult to sustain. Most states that have formally articulated their views have refrained from endorsing the inclusion of all data within these categories. Nevertheless, the issue remains unsettled. Against this background, an important

question arises: whether the ICC should contribute to the development of the law by interpreting the terms “objects” and “property” expansively in the applicable war crimes provisions.

This matter is highly sensitive in the light of the prominence of the principle of legality in the Rome Statute. The interpretative framework applicable to the Statute differs in certain respects from that governing general international law. Article 22(2) of the Statute requires that definitions of crimes be interpreted strictly and not extended through analogy, and that ambiguity be resolved in favour of the accused. The provision reflects the principle that criminal norms must be accessible and foreseeable, enabling individuals to anticipate whether particular conduct constitutes an international crime. Judicial interpretation may clarify the contours of offences, but such clarification should remain limited to modest, incremental developments rather than to broad judicial law-making.

Existing debates regarding the legal status of data indicate that, if anything, a more restrictive understanding currently predominates. The most expansive view, that information alone can constitute an object or property, may therefore fall outside the plausible interpretative range of the relevant war crimes provisions (McKenzie, 2019). Were the Court to adopt such a position without broader support in state practice, it might risk undermining its institutional legitimacy. At the same time, a complete failure to address harm inflicted on civilian systems through cyber operations would also be problematic, particularly given the central role of digital infrastructure in contemporary society.

A more balanced approach would therefore recognize that digital data forms part of objects or property capable of protection under IHL. This perspective reflects the reality that data is inseparable from the physical systems and infrastructure that store, process, and transmit it. By interpreting existing provisions in this manner, rather than creating entirely new legal categories, the Court could remain consistent with the principle of legality while acknowledging the real-world consequences of cyber operations. For example, a cyber operation that disables computer systems and prevents them from functioning as intended could potentially be considered an attack on protected objects even in the absence of immediate physical destruction.

Such an interpretation acknowledges that data is embedded within tangible technological infrastructures, including servers, computers, and communication networks. Consider, for instance, a cyber operation targeting financial infrastructure that prevents individuals and businesses from conducting transactions for an extended period. Even if the immediate technical effects were reversible, prolonged disruption could cause supply chains to collapse and potentially lead to severe economic and humanitarian consequences. In this context, data ought to be deemed as an integral component of the banking systems and digital networks that clearly qualify as objects and property under IHL (McKenzie, 2021).

Admittedly, determining whether such an interpretation constitutes a moderate or excessive development of the law ultimately involves a matter of legal judgment. Critics may argue that recognizing data as part of protected objects or property effectively extends these categories to intangible information. Nevertheless, it is also possible that the Court may never face a case in which the distinction between these competing interpretations proves decisive. Cyber operations producing only minimal or purely virtual effects are unlikely to satisfy the gravity requirement for admissibility under Article 17(1)(d) of the Rome Statute.

In decisions such as Prosecutor v. Lubanga, the Court emphasized that conduct must generally be large-scale or systematic and generate significant social alarm within the international community. Similar considerations have been applied when assessing the scale, nature, and impact of alleged crimes. These standards suggest that cases involving cyber operations without significant tangible consequences would rarely reach the threshold necessary for proceedings before the ICC.

5. Conclusion

Under IHL and the corresponding war crimes provisions in the Rome Statute of the International Criminal Court, civilian data should be understood as part of protected objects and property. If the International Criminal Court were required to assess such crimes, it would be preferable not to require evidence of direct kinetic or physical destruction emanating from the pertinent cyber operation. Instead, the Court could interpret the applicable offences as being committed where a cyber operation directed against or through data foreseeably disrupts or disables civilian systems or infrastructure. In such circumstances, the loss of functionality or operational capacity of those systems would constitute the relevant harm.

Digital data is invariably embedded within tangible technological infrastructures, such as servers, networks, and computer systems, that clearly qualify as protected objects and property under international law. Adopting an unduly restrictive interpretation would risk creating a significant gap in the protection afforded to civilians against a broad range of cyber operations. By contrast, recognizing data as an integral component of protected systems offers a more coherent and realistic understanding of how modern digital infrastructures function. Although this interpretation may not represent the most conservative reading of the Statute, it remains consistent with the interpretative framework governing the Rome Statute.

Importantly, this approach would not imply that every cyber operation could give rise to proceedings before the Court. The admissibility requirements contained in Article 17(1)(d) of the Rome Statute establish a gravity threshold, ensuring that only cyber operations producing consequences of significant severity would be subject to investigation or prosecution. While applying this threshold in the cyber context may present practical challenges, particularly with regard to attribution and the assessment of broader effects, certain operations may nonetheless reach the level of gravity required for the Court's jurisdiction. Interpreting the concepts of "object" and "property" in a manner that accommodates such cases would therefore allow the existing legal framework to respond meaningfully to serious harms caused by cyber operations.

The statement regarding the usage of AI: Artificial intelligence (AI) tools were used solely for language editing and stylistic refinement of the manuscript. Specifically, Claude AI was utilized to assist with grammar correction sentence and structure improvement. The author reviewed, verified, and takes full responsibility for all content, interpretations, analyses, and conclusions presented in this article.

Funding: This research received no external funding.

Conflict of Interests: The author has declared no conflict of interest regarding this study.

References

1. Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review, 84*(2), 191–215. https://doi.org/10.1037/0033-295X.84.2.191
2. Bergman, R., & Halbfinger, D. M. (2020, May 19). *Israel hack of Iran port is latest salvo in exchange of cyberattacks*. The New York Times. Retrieved from www.nytimes.com
3. Corera, G. (2020, February 20). *UK says Russia's GRU behind massive Georgia cyber-attack*. BBC News. Retrieved from www.bbc.com
4. Council of Europe. (2001). *Convention on Cybercrime*.
5. Daskal, J. (2015). The un-territoriality of data. *Yale Law Journal, 125*(2), 326–398.
6. Dinstein, Y. (2016). *The conduct of hostilities under the law of international armed conflict* (3rd ed.). Cambridge University Press.
7. European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)*.
8. Gisel, L., Rodenhäuser, T., & Dörmann, K. (2020). Twenty years of the ICRC's study on customary international humanitarian law. *International Review of the Red Cross, 102*(913), 1–22. https://doi.org/10.1017/S1816383120000375
9. Harrison Dinniss, H. (2012). *Cyber warfare and the laws of war*. Cambridge: Cambridge University Press.
10. Horowitz, H. (2022). The concept of "attack" in cyber operations: Bridging the gap in international humanitarian law. *Journal of Conflict and Security Law, 27*(1), 1–30. https://doi.org/10.1093/jcsl/krac001
11. International Committee of the Red Cross. (1987). *Commentary on the Additional Protocols of 8 June 1977*. Geneva: ICRC.
12. International Committee of the Red Cross. (2021). *International humanitarian law and cyber operations during armed conflicts*. Retrieved from www.icrc.org
13. International Court of Justice. (2015). *Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia)*.
14. International Criminal Court. (1998). *Rome Statute of the International Criminal Court*.
15. International Criminal Court. (2012). *Prosecutor v. Lubanga*.
16. International Criminal Court. (2014). Prosecutor v. Katanga and Ngudjolo Chui.
17. International Law Association. (2020). *Report of the ILA Study Group on the Conduct of Hostilities in the 21st Century*.
18. Ma□ák, D. (2018). *Internationalized armed conflicts in international law*. Oxford: Oxford University Press.
19. Ma□ák, D. (2020). Military objectives 2.0: The case for interpreting computer data as objects under international humanitarian law. *Israel Law Review, 53*(1), 55–80. https://doi.org/10.1017/S0021223720000016
20. McKenzie, S. (2019). *Disputed territories and international criminal law: Israeli settlements and the International Criminal Court*. Routledge.
21. McKenzie, S. (2021). Cyber operations against civilian data: Revisiting war crimes against protected objects and property in the Rome Statute. *Journal of International Criminal Justice, 19*(5), 1165–1192. https://doi.org/10.1093/jicj/mqab067

22. Ritter, J., & Mayer, A. (2017). Regulating data as property: A new construct for moving forward. *Duke Law and Technology Review*, 220–224.
23. Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations*. Cambridge: Cambridge University Press.
24. Schmitt, M. N. (2019). The law of cyber warfare: Quo vadis? *International Law Studies*, *95*, 1–30.
25. United Nations. (1907). *Hague Regulations Respecting the Laws and Customs of War on Land*.
26. United Nations. (1949). *Geneva Conventions of 12 August 1949*.
27. United Nations. (1977). *Additional Protocol I to the Geneva Conventions*.
28. Zetter, K. (2014). *An unprecedented look at Stuxnet, the world's first digital weapon*. Wired. Retrieved from www.wired.com