

Cyber-Enabled Crimes under the Rome Statute: Jurisdictional, Substantive and Evidentiary Challenges

Mahbuba Kamal*

Abstract

Cyber operations can cause or facilitate harm of a scale traditionally associated with kinetic violence, but their use does not create a fifth international crime. The International Criminal Court's Office of the Prosecutor now treats 'cyber-enabled crimes' as a factual description of genocide, crimes against humanity, war crimes, aggression and offences against the administration of justice when committed or facilitated through cyber means. This article examines how the technology-neutral Rome Statute can apply to such conduct and where its application remains difficult. It distinguishes ordinary cybercrime, State responsibility and the prohibition of force, international humanitarian law governing cyber operations during armed conflict, and individual criminal responsibility under the Rome Statute. Using a doctrinal, qualitative and analytical method, it reassesses Stuxnet, the 2015 Ukrainian power-grid incident, cyber operations linked to aggression and attacks affecting medical services without presuming that any incident automatically satisfies a Rome Statute offence. The article then analyses subject-matter and territorial jurisdiction, attribution to natural persons, modes of liability, digital evidence, presence at trial and the gravity threshold. It argues that existing international criminal law is capable of addressing cyber-enabled conduct, but effective accountability depends on an elements-based analysis, reliable attribution, specialist technical capacity, preservation and authentication of digital evidence, and cooperation between the ICC, States and private technology providers. Remaining uncertainty concerns non-physical loss of functionality, the legal status of civilian data, civilian hackers, private infrastructure and cross-border evidence. The appropriate immediate response is therefore not a new cyber-war offence, but clearer prosecutorial practice, stronger cooperation and disciplined application of existing law.

Keywords: Cyber-Enabled Crimes, International Criminal Court, Rome Statute, International Criminal Law, Digital Evidence.

1. Introduction

The digitalisation of military and civilian infrastructure has expanded the means through which serious harm may be inflicted. The International Committee of the Red Cross (ICRC) describes

* Founder, Bangladesh Society of International Law; LLM in Human Rights, University of Birmingham; Research Assistant, Birmingham Law School; LLB (Hons.), BRAC University.

cyber operations during armed conflict as operations against or through computers, computer systems and networks, and stresses that international humanitarian law (IHL) limits them in the same manner as other means and methods of warfare.¹ Cyber means may disable power, water, communications or medical services, manipulate information, collect intelligence or facilitate physical operations. They may also be used outside armed conflict, where ordinary cybercrime rules, the law of State responsibility and the prohibition of force may be more immediately relevant.

The legal problem is therefore one of classification rather than technological exceptionalism. Harmful cyber activity can constitute domestic cybercrime, an internationally wrongful act of a State, a breach of IHL, or conduct attributable to an individual that satisfies a Rome Statute crime. The same operation may engage more than one regime, but the elements and consequences of each remain distinct.² Conflating these regimes produces categorical conclusions unsupported by jurisdiction, context, intent or individual attribution.

In December 2025, the Office of the Prosecutor (OTP) of the International Criminal Court (ICC) issued its *Policy on Cyber-Enabled Crimes under the Rome Statute*. The Policy treats the Rome Statute as technology-neutral and uses ‘cyber-enabled crime’ as a factual expression for existing crimes committed or facilitated through cyber means, not as an additional legal category.³ The Court’s subject-matter jurisdiction remains confined to genocide, crimes against humanity, war crimes and aggression, together with offences against the administration of justice.⁴

The Policy is a prosecutorial framework rather than a judicial holding. It records the OTP’s present approach, remains open to revision and does not create legal rights.⁵ Nevertheless, it materially alters the appropriate research question. The issue is no longer whether ‘cyber warfare’ should be declared an autonomous international crime, but how cyber conduct may satisfy the jurisdictional, contextual, material and mental elements of crimes already recognised by the Statute. Chatham House similarly concludes that no new substantive

¹ International Committee of the Red Cross, *International Humanitarian Law and Cyber Operations during Armed Conflicts: ICRC Position Paper* (November 2019) 3–5.

² Elizabeth Wilmschurst, Harriet Moynihan and Tsvetelina van Benthem, *Securing Justice for Cyber-Enabled International Crimes: Legal Foundations and Practical Routes to Prosecution* (Chatham House 2026) 4–7.

³ Office of the Prosecutor, International Criminal Court, *Policy on Cyber-Enabled Crimes under the Rome Statute* (December 2025) paras 3–6, 19.

⁴ Rome Statute of the International Criminal Court (adopted 17 July 1998, entered into force 1 July 2002) 2187 UNTS 3 (Rome Statute) arts 5 and 70.

⁵ ICC OTP, *Policy on Cyber-Enabled Crimes* (n 3) para 11.

offence is required to capture core international crimes committed by cyber means, while emphasising substantial investigative and prosecutorial obstacles.⁶ This article therefore asks under what jurisdictional, contextual, material and mental conditions cyber-enabled conduct may constitute an existing Rome Statute crime, and what evidentiary and institutional obstacles continue to impede its effective investigation and prosecution.

Accordingly, this article analyses the application of existing international criminal law to cyber-enabled conduct. It first separates the relevant legal regimes and identifies unresolved substantive questions. It then examines jurisdiction, individual responsibility, evidence, trial and admissibility before proposing practical reforms. National cybercrime policy, general human-rights analysis and broader criticism of the ICC fall outside its scope except where necessary to clarify the boundaries of individual criminal responsibility.

This separation has practical consequences throughout the analysis. A finding that a State has breached the Charter or IHL does not automatically establish that a natural person committed a Rome Statute crime. Conversely, the absence of a sufficiently attributable State act does not necessarily preclude individual liability for genocide, crimes against humanity or war crimes committed through a non-State organisation. The governing question at each stage is therefore who is responsible, under which legal regime, for which precisely defined conduct. Maintaining that sequence prevents the language of cyber warfare from obscuring the Court's limited subject-matter jurisdiction and the principle of legality.

2. Cyber-Enabled Conduct under International Criminal Law

2.1 Conceptual and Regulatory Framework

International criminal law imposes responsibility on natural persons for conduct recognised as crimes under international law. The Nuremberg judgment stated that crimes against international law are committed by individuals rather than abstract entities and that international law is enforced by punishing those individuals.⁷ The Rome Statute institutionalises that principle through the jurisdiction and applicable-law provisions of the ICC.⁸

The Statute defines the four core crimes, while the Elements of Crimes assist the Court in interpreting and applying their legal requirements.⁹ Cyber means do not displace those

⁶ Wilmshurst, Moynihan and van Benthem (n 2) 2–5.

⁷ Judgment of the International Military Tribunal (1947) 41 AJIL 172, 221.

⁸ Rome Statute (n 4) arts 5, 21 and 25.

⁹ International Criminal Court, *Elements of Crimes* (2013) general introduction and arts 6–8 bis.

requirements. A digital operation must still be connected to the relevant protected interest, prohibited conduct, context, consequence and mental element. Technology may change how harm is caused and proved, but it does not lower the threshold of criminality.

IHL governs cyber operations only when an armed conflict exists and the operation is sufficiently connected with it. In that setting, the principles of distinction, proportionality and precautions remain applicable. Parties must distinguish civilians and civilian objects from military objectives, refrain from indiscriminate or disproportionate attacks and take feasible precautions.¹⁰ The ICRC's 2024 Challenges Report confirms both the applicability of IHL to cyber operations and the continuing disagreement over how established rules apply to data, network functionality and digitally dependent civilian services.¹¹

The Tallinn Manual 2.0 is an influential expert restatement of how international law may apply to cyber operations, but it is not a binding treaty, judgment or official NATO position.¹² Its value lies in exposing areas of consensus and disagreement. The Tallinn Manual 3.0 project should also be acknowledged as a continuing revision designed to reflect later practice and technological developments, not as law already adopted.¹³

2.2 Existing International Crimes and Cyber Means

The Court's subject-matter jurisdiction remains confined to genocide, crimes against humanity, war crimes and aggression.¹⁴ The expression 'cyber-enabled crime' does not create another category; the OTP uses it for existing crimes committed or facilitated by cyber means.¹⁵ In the OTP's view, the Statute is technology-neutral.¹⁶ Accordingly, cyber-enabled conduct is prosecutable only when the same *actus reus*, causation, *mens rea* and standard of proof applicable to conduct by other means are established.¹⁷

¹⁰ Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (Additional Protocol I) arts 48, 51, 52 and 57.

¹¹ International Committee of the Red Cross, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts: Building a Culture of Compliance for IHL to Protect Humanity in Today's and Future Conflicts* (ICRC 2024) 57–60.

¹² Michael N Schmitt (gen ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, CUP 2017) 2–3.

¹³ NATO Cooperative Cyber Defence Centre of Excellence, *2022 Training Catalogue* (CCDCOE 2021) 83.

¹⁴ Rome Statute (n 4) art 5.

¹⁵ ICC OTP, *Policy on Cyber-Enabled Crimes* (n 3) para 19.

¹⁶ *ibid* para 3.

¹⁷ *ibid* paras 4 and 49–51.

Ordinary cybercrimes such as unauthorised access, fraud or interference with computer systems remain outside the ICC's jurisdiction unless the conduct independently fulfils a Rome Statute crime.¹⁸ This distinction prevents gravity, novelty or cross-border effects from being treated as substitutes for the legal elements. It also avoids treating State responsibility for an internationally wrongful cyber operation as equivalent to the criminal responsibility of a particular natural person.

2.3 Illustrative Incidents and Legal Qualification

Stuxnet illustrates the need for a fact-specific assessment. A technical report found that Iran decommissioned and replaced approximately 1,000 IR-1 centrifuges at the Natanz Fuel Enrichment Plant and regarded Stuxnet as a reasonable explanation for the apparent damage, while stressing uncertainty about its precise effects.¹⁹ Those facts do not by themselves establish a Rome Statute violation. A war-crime finding would require proof of a qualifying armed conflict and nexus, a protected object or other prohibited target, the relevant consequence and the accused's intent and knowledge.²⁰ Any ICC case would additionally require a statutory jurisdictional basis and an identifiable mode of individual responsibility.²¹

The 2015 Ukrainian power-grid incident is also significant but cannot automatically be labelled a crime against humanity. The cyber operation interrupted electricity for approximately 225,000 customers, and affected several distribution companies.²² Article 7 requires one of the listed acts to form part of a widespread or systematic attack directed against a civilian population, pursuant to or in furtherance of a State or organisational policy, with the accused's knowledge of the attack.²³ The outage is evidence of potentially serious civilian harm, but the scale of one incident, its attribution and its relationship to a broader attack must

¹⁸ *ibid* paras 5–6.

¹⁹ David Albright, Paul Brannan and Christina Walrond, 'Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment' (Institute for Science and International Security, 22 December 2010) 1, 7.

²⁰ Rome Statute (n 4) art 8(2)(b)(ii); International Criminal Court, *Elements of Crimes* (n 9) art 8(2)(b)(ii), elements 1–5.

²¹ Rome Statute (n 4) arts 12–13, 25 and 30.

²² Cybersecurity and Infrastructure Security Agency, 'Cyber-Attack Against Ukrainian Critical Infrastructure' (ICS Alert IR-ALERT-H-16-056-01, 25 February 2016).

²³ Rome Statute (n 4) art 7(1) and (2)(a); International Criminal Court, *Elements of Crimes* (n 9) art 7, introduction, paras 1–3.

be proved before Article 7 can apply. The OTP likewise treats the contextual elements and the possible role of organised hacker groups as questions requiring evidence, not presumptions.²⁴ The prohibition of force under Article 2(4) of the UN Charter belongs primarily to the law governing interstate conduct.²⁵ It does not convert every harmful cyber operation into the individual crime of aggression. Article 8 bis requires an act of aggression by a State that, by character, gravity and scale, constitutes a manifest Charter violation, together with planning, preparation, initiation or execution by a person effectively controlling or directing the State's political or military action.²⁶ Cyber activity therefore amounts to aggression only in exceptional circumstances and only where State attribution, the armed-force threshold, manifest violation and leadership requirements are satisfied.²⁷

Medical units require a similarly careful analysis. The Second Geneva Convention principally concerns wounded, sick and shipwrecked members of armed forces at sea; it is not the general source of protection for civilian hospitals. Civilian hospitals are protected by the Fourth Geneva Convention, and medical units receive specific protection under Additional Protocol I.²⁸ A cyber operation that disrupts medical services may be unlawful under IHL and may, where the elements and armed-conflict nexus are established, support a war-crime charge. It cannot be classified solely from the identity of the affected institution or the seriousness of disruption.²⁹

Two substantive uncertainties remain especially important. First, experts disagree about whether a cyber operation causing loss of functionality without physical damage constitutes an 'attack' for IHL and Rome Statute purposes. Secondly, there is no settled answer on whether civilian data, as distinct from the physical infrastructure storing them, qualify as protected objects.³⁰ The ICRC identifies these issues as operationally significant because modern civilian life depends on the availability and integrity of digital infrastructure and data.³¹

²⁴ ICC OTP, *Policy on Cyber-Enabled Crimes* (n 3) paras 62 and 66–70.

²⁵ Charter of the United Nations art 2(4).

²⁶ Rome Statute (n 4) arts 8 bis(1)–(2) and 25(3) bis.

²⁷ ICC OTP, *Policy on Cyber-Enabled Crimes* (n 3) paras 97–102.

²⁸ Geneva Convention relative to the Protection of Civilian Persons in Time of War (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 287 art 18; Additional Protocol I (n 10) arts 12 and 15.

²⁹ International Committee of the Red Cross, *International Humanitarian Law and Cyber Operations during Armed Conflicts* (n 1) 4–5.

³⁰ ICC OTP, *Policy on Cyber-Enabled Crimes* (n 3) paras 90–91.

³¹ ICRC, *2024 Challenges Report* (n 11) 57–60.

3. Cyber-Enabled Crimes before the International Criminal Court

3.1 Jurisdiction

Article 5 limits the Court's subject-matter jurisdiction to the four core crimes, while Articles 11-13 regulate temporal jurisdiction, territorial or personal preconditions and the mechanisms by which jurisdiction is exercised.³² The absence of an express reference to cyberspace does not create a jurisdictional gap because the OTP applies those ordinary provisions to cyber-enabled conduct.³³

Cyber operations nevertheless complicate territorial analysis. The operator, command infrastructure, compromised servers, targeted systems and legally relevant consequences may be distributed across several States. The decisive question is whether conduct or a consequence forming part of the crime establishes the nexus required by Article 12, not whether data happened to transit a server in a State Party. The OTP regards both subjective and objective territoriality as potentially relevant while rejecting mere data transit as a sufficient basis.³⁴ Chatham House similarly notes that concealed locations and distributed effects can create multiple plausible jurisdictions and substantial coordination problems.³⁵

The ICC may also rely on the nationality of an accused who is a national of a State Party or a State accepting jurisdiction, or on a Security Council referral. Aggression remains subject to the distinct jurisdictional conditions in Articles 15 bis and 15 ter. The relevant inquiry is therefore whether the facts satisfy an existing crime and a statutory jurisdictional route, rather than where 'cyber warfare' belongs as a separate offence.³⁶

3.2 Individual Criminal Responsibility

The Rome Statute imposes responsibility on natural persons who commit, order, solicit, induce, aid, abet or otherwise contribute to crimes, and it separately regulates superior responsibility. Intent and knowledge are generally required unless the Statute provides otherwise.³⁷ Cyber operations complicate these rules because technical execution may be divided among commanders, intelligence personnel, malware developers, infrastructure providers and operators who know only part of the overall plan. The OTP therefore emphasises the ordinary

³² Rome Statute (n 4) arts 5 and 11–13.

³³ ICC OTP, *Policy on Cyber-Enabled Crimes* (n 3) paras 38–48.

³⁴ *ibid* paras 43–46.

³⁵ Wilmshurst, Moynihan and van Benthem (n 2) 30–36.

³⁶ Rome Statute (n 4) arts 12(2)–(3), 13, 15 bis and 15 ter.

³⁷ Rome Statute (n 4) arts 25, 28 and 30.

modes of liability and the need to connect each person's contribution and mental state to the relevant crime.³⁸

State attribution and individual criminal responsibility must not be collapsed. Proof that an operation is attributable to a State does not establish which natural person bears criminal responsibility, while failure to attribute conduct to a State does not necessarily prevent prosecution of members of a non-State group. The crime of aggression is exceptional because it requires a State act and leadership status. Other crimes may be committed by State agents, organised armed groups or private individuals if the statutory elements and modes of liability are met.

The expanding involvement of civilian hackers and private technology companies makes this distinction practically important. The ICRC's 2025 report focuses on individuals, hacker groups and technology companies whose activities may blur the civilian-military distinction and expose civilian people and infrastructure to risk.³⁹ Under the Rome Statute, their liability cannot rest on association alone. A prosecutor must prove the contribution required by the relevant mode of liability and the corresponding knowledge or purpose. Chatham House identifies assistance through infrastructure, cloud services or platforms as a possible complicity issue but cautions that ordinary commercial provision and criminal participation are not equivalent.⁴⁰

3.3 Evidence and Trial

Cyber-enabled cases depend heavily on digital evidence. Logs, malware samples, server images, subscriber information, communications, command records and open-source material may establish conduct, attribution, causation and mental elements. Yet such evidence is volatile, distributed, encrypted and vulnerable to manipulation. Investigators must preserve provenance, document the chain of custody, validate forensic methods and distinguish technical indicators from proof of individual criminal responsibility.⁴¹

The Rome Statute requires the Prosecutor to investigate incriminating and exonerating circumstances equally and permits the Court to assess relevance, probative value and

³⁸ ICC OTP, *Policy on Cyber-Enabled Crimes* (n 3) paras 109–116.

³⁹ International Committee of the Red Cross and Geneva Academy of International Humanitarian Law and Human Rights, *IHL and the Growing Involvement of Civilians in Cyber Operations and Other Digital Activities During Armed Conflict* (ICRC 2025) 2–4.

⁴⁰ Wilmschurst, Moynihan and van Benthem (n 2) 23–29.

⁴¹ ICC OTP, *Policy on Cyber-Enabled Crimes* (n 3) paras 149–165.

prejudicial effect.⁴² Cyber evidence may require urgent preservation orders and cooperation from States and private providers before data are deleted or altered. Chatham House consequently recommends specialist cyber expertise, secure facilities for storing and analysing large evidentiary datasets and cooperation across investigative bodies.⁴³

The burden of proof remains unchanged. At confirmation of charges, the Chamber must find substantial grounds to believe that the person committed each charged crime; at trial, guilt must be established beyond reasonable doubt.⁴⁴ Technical sophistication may explain why specialist evidence is necessary, but it does not justify inferential shortcuts on attribution, intent or causation.

The accused's presence must also be described accurately. Article 63(1) requires the accused to be present during trial, but Article 61(2) permits confirmation-of-charges proceedings in the accused's absence in specified circumstances, including waiver or flight where reasonable steps have been taken to secure appearance and provide notice.⁴⁵ The difficulty of identifying or apprehending a cyber operator may therefore impede proceedings, but the Statute does not impose an absolute presence requirement at every pre-trial stage.

Institutional capacity remains a serious constraint. The OTP's approach requires trained investigators, forensic tools, secure data management and continuing cooperation with cybercrime units, international organisations and private entities.⁴⁶ These needs create resource demands, but they are a challenge of implementation rather than proof that the Rome Statute is legally obsolete.

3.4 Admissibility and Gravity

Jurisdiction does not by itself make a case admissible. Under Article 17, a case may be inadmissible because of genuine national proceedings, prior disposition, or insufficient gravity.⁴⁷ Gravity is assessed through the scale, nature, manner of commission and impact of the potential crimes. The cyber character of conduct neither automatically satisfies nor defeats that threshold.

A cyber operation may have exceptional gravity where it causes deaths, serious injury, prolonged denial of essential services, large-scale displacement or forms part of a broader

⁴² Rome Statute (n 4) arts 54(1)(a) and 69(4).

⁴³ Wilmschurst, Moynihan and van Benthem (n 2) 37–57.

⁴⁴ Rome Statute (n 4) arts 61(7) and 66(3).

⁴⁵ Rome Statute (n 4) arts 61(2) and 63(1).

⁴⁶ ICC OTP, *Policy on Cyber-Enabled Crimes* (n 3) paras 143–145 and 158–165.

⁴⁷ Rome Statute (n 4) art 17(1).

campaign against civilians. Conversely, many intrusions, disruptions and data compromises, though unlawful under domestic law or State-responsibility rules, will not meet the ICC threshold. The OTP treats gravity as a holistic assessment and recognises that digital effects must be evaluated together with physical, psychological and societal consequences.⁴⁸

The assessment must remain case-specific. It would be equally mistaken to exclude non-physical cyber harm categorically or to assume that disruption of critical infrastructure is necessarily sufficiently grave. The proper approach links documented consequences to the elements of the alleged crime and to the Court's limited institutional mandate.

This approach also preserves proportionality in prosecutorial selection. Cyber operations vary from brief and reversible interference to conduct that disables essential services for prolonged periods or forms part of a coordinated campaign of violence. Treating all of them as one category would weaken both the gravity inquiry and the distinction between international crimes and ordinary cyber offences. The Prosecutor should identify the protected population or object, the legally relevant consequence, the scale and duration of harm, the broader criminal context and the accused's contribution before deciding that the Court's exceptional jurisdiction is warranted.

4. Recommendations

First, the ICC should implement the 2025 Policy through offence-specific guidance rather than seek an immediate amendment creating a cyber-war offence. Existing international criminal law applies to cyber-enabled conduct; the priority is to clarify how the elements of Article 5 crimes operate in recurring digital scenarios.⁴⁹ Guidance should address loss of functionality, civilian data, causation through interdependent systems, the evidential distinction between technical and legal attribution, and the relationship between State attribution and individual liability.

Secondly, the OTP should maintain permanent cyber expertise within multidisciplinary investigation teams. Cyber specialists should participate from the earliest stage in preservation, collection and analysis, while lawyers define the legal propositions that technical evidence must prove. Standard operating procedures should cover forensic imaging, hashing, chain of custody, metadata preservation, validation of tools and disclosure of technical limitations.⁵⁰

⁴⁸ ICC OTP, *Policy on Cyber-Enabled Crimes* (n 3) paras 128–132.

⁴⁹ Wilmschurst, Moynihan and van Benthem (n 2) 58–63.

⁵⁰ ICC OTP, *Policy on Cyber-Enabled Crimes* (n 3) paras 149–169.

Thirdly, cooperation arrangements should be strengthened before incidents occur. States should designate contact points capable of responding rapidly to preservation and assistance requests; private technology providers should maintain lawful and transparent processes for preserving and producing evidence; and international organisations should facilitate joint investigation, deconfliction and technical assistance. The Statute already requires general cooperation and authorises assistance in identifying persons, collecting evidence and preserving records.⁵¹ The OTP's Policy and Chatham House both regard sustained cooperation with private entities as indispensable to effective cases.⁵²

Fourthly, complementarity should remain central. States should ensure that domestic legislation covers Rome Statute crimes when committed or facilitated by cyber means and that investigators can lawfully obtain and authenticate cross-border digital evidence. National proceedings will often be better placed to access suspects, infrastructure and service providers. ICC engagement should support rather than displace capable national investigations.

Domestic implementation should not be limited to inserting the word 'cyber' into criminal codes. Prosecutors need authority and technical capacity to preserve remote data, obtain evidence across borders, protect sensitive intelligence, disclose material fairly and present complex technical conclusions in an intelligible form. States should also ensure that ordinary cybercrime investigations can be escalated when evidence reveals a connection to a broader campaign of international crimes. Clear referral pathways between cybercrime units, war-crimes units and national points of contact for ICC cooperation would make complementarity operational rather than merely formal.

Fifthly, policy development must protect the civilian character of digital infrastructure. States should avoid drawing civilians into hostile cyber activity where feasible, communicate IHL obligations to civilian hacker groups and assess the risks created when private technology services are integrated into military operations.⁵³ These preventive measures do not determine criminal liability, but they reduce ambiguity, preserve evidence and limit foreseeable civilian harm.

Finally, the Tallinn Manual 2.0 may continue to inform legal analysis, while the Tallinn Manual 3.0 process should be monitored as an expert project. Neither should be treated as binding law. Courts and prosecutors should prioritise the Rome Statute, Elements of Crimes,

⁵¹ Rome Statute (n 4) arts 86 and 93(1).

⁵² ICC OTP, *Policy on Cyber-Enabled Crimes* (n 3) paras 180–194; Wilmshurst, Moynihan and van Benthem (n 2) 54–63.

⁵³ ICRC and Geneva Academy, *IHL and the Growing Involvement of Civilians* (n 39) 2–4.

applicable treaties and judicial decisions, using manuals and institutional reports as persuasive aids where genuine interpretative uncertainty remains.⁵⁴

5. Conclusion

Cyber-enabled crimes do not require recognition of a fifth crime under the Rome Statute. The Statute's technology-neutral offences can apply when cyber conduct satisfies their jurisdictional, contextual, material and mental elements. The gravity or novelty of a cyber operation does not, by itself, establish international criminality, and cybercrime, State responsibility, IHL and individual criminal responsibility must each be assessed under their distinct legal tests.

A disciplined elements-based approach changes the assessment of prominent incidents. Stuxnet cannot be declared a Rome Statute violation without proving jurisdiction, armed-conflict nexus, object status, consequences, attribution and mens rea. The Ukrainian power-grid outage affected about 225,000 customers, but Article 7 still requires proof of a widespread or systematic attack, policy and knowledge. Cyber operations amount to aggression only where the stringent State-act, manifest-violation and leadership requirements are met. Civilian hospitals are protected under the Fourth Geneva Convention and Additional Protocol I, not generally by the Second Geneva Convention, and the Charter prohibition of force is Article 2(4).

Existing law is therefore applicable but not frictionless. Uncertainty persists over non-physical loss of functionality, whether civilian data are protected objects, how technical indicators support legal attribution, and when assistance by civilian hackers or private technology providers satisfies a mode of liability.⁵⁵ Digital evidence also requires rapid preservation, specialist validation and cooperation across States and private networks. The ICRC identifies the dependence of civilians on digital systems and the growing involvement of civilian actors as continuing interpretative and operational concerns.⁵⁶

The appropriate response is not to presume the inadequacy of the Rome Statute or to make a new convention the immediate condition of accountability. It is to apply existing crimes rigorously, develop focused guidance, invest in technical capacity, strengthen complementarity and secure cooperation from those who hold digital evidence. This approach preserves legality

⁵⁴ Schmitt (n 12) 2–3; NATO CCDCOE, *2022 Training Catalogue* (n 13) 83.

⁵⁵ ICC OTP, *Policy on Cyber-Enabled Crimes* (n 3) paras 90–91 and 109–116.

⁵⁶ ICRC, *2024 Challenges Report* (n 11) 57–60; ICRC and Geneva Academy, *IHL and the Growing Involvement of Civilians* (n 39) 2–9.

while making international criminal justice responsive to the means through which contemporary atrocities may be committed or facilitated.