Cour
Pénale
Internationale

International
Criminal
Court

BUREAU DU
PROCUREUR

OFFICE OF THE
PROSECUTOR

OFFICE OF THE PROSECUTOR

POLICY ON CYBER-ENABLED CRIMES UNDER THE ROME STATUTE

December 2025

COUR PÉNALE INTERNATIONALE
BUREAU DU PROCUREUR

INTERNATIONAL CRIMINAL COURT
OFFICE OF THE PROSECUTOR

OFFICE OF THE PROSECUTOR

POLICY ON CYBER-ENABLED CRIMES UNDER THE ROME STATUTE

December 2025

PREFACE

Justice must not be outpaced by the speed of global change. At the Office of the Prosecutor, this means ensuring that we adapt appropriately to the full range of circumstances in which Rome Statute crimes may be committed. This applies equally to our work in all situations where the International Criminal Court presently exercises its jurisdiction, for all types of crime.

In particular, new and emerging technologies bring new possibilities for humanity, and for human endeavour. We welcome them. But they also bring new risks and new challenges. New technologies may redraw the 'front lines', literally as well as figuratively, where human welfare and dignity are threatened with violence and oppression. On occasion, technology may even be exploited to try and obscure the fact that crimes are committed at all.

Even as our Office investigates and prosecutes current and past crimes, therefore, we have no lesser responsibility to ensure we are ready to address the crimes of tomorrow. This is vital if we are to continue our part in making the promise of the Rome Statute an equal reality for all. We will achieve this by careful interpretation and application of the law, further enhancing our ability to collect and analyse all forms of evidence, and deepening our cooperation with all partners who share our commitment to human rights and freedoms.

In this spirit, we are grateful to Prof. Marko Milanović for his support to the Office in developing this Policy, and the encouragement and partnership extended to us along the way by States Parties, civil society, private sector representatives, and other expert stakeholders. With the rapid pace of technological innovation, this Policy will—of course—not be the end of our increased efforts in this important area. But it sets a sure foundation for our beginning. We commend it to your attention, and we welcome the opportunities that it may bring to continue to work fruitfully together.

Nazhat Shameem Khan
Deputy Prosecutor

Mame Mandiaye Niang
Deputy Prosecutor

Table of Contents

EXECUTIVE SUMMARY

The *Policy on Cyber-enabled Crimes under the Rome Statute* sets out how the Office of the Prosecutor will use its mandate and powers to investigate and prosecute cyber-enabled crimes within the jurisdiction of the International Criminal Court. It also shows how the Office's work may support relevant national efforts to address unlawful and harmful uses of cyberspace more broadly where these amount to serious crimes under applicable national law, consistently with internationally recognised human rights.

This Policy uses the term 'cyber-enabled crimes' (as a factual description, and not as a distinct legal concept) simply to refer to the international crimes set out in the Rome Statute, which may be committed or facilitated by cyber means. It is important to underline that relevant crimes under the Statute include not only aggression, genocide, crimes against humanity, and war crimes, but also offences against the administration of justice at the Court. In addition, many considerations in this Policy apply equally to cyber conduct which provides legally required context, or correlates with, or is otherwise probative of Rome Statute crimes—even if they are not themselves committed or facilitated by cyber means. In this way, the issues addressed in this Policy may increasingly be relevant to *all* the Office's investigations.

The Court does not have jurisdiction over ordinary 'cybercrimes' that are punishable under domestic law, such as fraud or unauthorized access to a computer system. States may have assumed international obligations to punish such crimes under treaties to which they are parties, but as such these do not fall within the remit of the Court or the Office. National efforts to combat such crimes may, however, sometimes intersect with the Office's efforts to address crimes within the jurisdiction of the Court. Notably, this may apply where proceedings concern similar or related conduct, relevant both to the investigation of crimes within the jurisdiction of the Court and serious crimes under applicable national law. Similarly, many of the same investigative techniques may apply both to ordinary cybercrimes and to cyber-enabled crimes within the jurisdiction of the Court.

To date, the question of cyber-enabled crimes within the jurisdiction of the Court—and, indeed, cyber-specific issues more broadly—has only arisen at the margins of the Court's work and has not yet been addressed in any detail. The investigation and prosecution of such crimes therefore raises novel issues, legally and practically. This Policy sets out some of the key views of the Office where

these can usefully be communicated publicly, while maintaining prudential limits and avoiding pre-emption of certain issues before they become sufficiently ripe.

In principle, the commission of any crime within the jurisdiction of the Court—which is mandated to address the most serious crimes of international concern—warrants investigation and prosecution. This applies no less to crimes which are cyber-enabled. Consistently with the Statute, however, only cases of sufficient gravity will be admissible before the Court—assessed by reference to factors including the scale, nature, manner of commission, and impact of the alleged crime(s) attributed to the suspect(s) in question. This often means that cases before the Court relate to conduct which has caused serious harm to large numbers of people or placed them in significant danger of such harm. One exception concerns offences against the administration of justice, since such cases are not subject to any gravity requirement, but nonetheless merit action because they threaten the functioning of the Court itself.

Furthermore, in order to make the most effective use of its resources, the Office will be guided by the question of gravity, among other considerations, in determining *which* cases to investigate with a view to potential prosecution. Of particular importance here is the *relative* gravity of the potential case, that is, how it compares to other potential cases currently under consideration by the Office with a view to investigation or prosecution. The Office will approach cases concerning cyber-enabled crimes on an equal basis with other types of criminality. The Office is prepared to investigate and prosecute both the perpetrators and the facilitators of cyber-enabled crimes within the Court's jurisdiction.

This Policy was developed through an extensive consultative process involving multiple rounds of written input and direct discussion with internal Office staff and external experts, as well as a public consultation. The Office is grateful for the valuable participation in this consultation of a diverse range of States Parties, civil society organisations, and individual experts, as well as representatives of the private sector. The Office commits to continuing and extending this consultative approach as it works to implement the Policy.

INTRODUCTION

Addressing new technologies

1. In both national and international legal orders, the advent of new technologies frequently raises the question whether existing law is sufficient to address the challenges that these technologies pose, or whether substantial reform and new lawmaking is required. The development and use of information and communication technologies, including artificial intelligence, pose such a dilemma across international law as a whole. States have responded to this challenge through collaboration within UN working groups,[1] by formulating their official national positions on how international law applies in cyberspace,[2] through the adoption of certain soft law instruments,[3] and (more rarely) through the conclusion of new treaties, such as the Budapest Convention on Cybercrime, its two additional protocols and the new UN Convention against Cybercrime.[4] Some States have also supported independent academic studies.[5]

2. The core message that emerges from this ongoing multi-stakeholder process is that, while cyber-specific lawmaking can be helpful in certain areas, existing international law is largely adequate in covering cyber operations and

[1] These include the work of the Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG). For their reports, *see further below* fn. 6.

[2] Most of these national positions are usefully compiled here: https://cyberlaw.ccdcoe.org/wiki/List_of_articles#National_positions. These national positions have informed the analysis in this Policy, but in the interest of brevity will not be individually cited unless of particular relevance. In addition, in 2024, the African Union adopted its common position on the application of international law in cyberspace (AU Common Position), and the European Union adopted its declaration on a common understanding of the application of international law in cyberspace (EU Common Understanding).

[3] *See e.g.* UNHRC Res. 54/21; UN Global Digital Compact (2024).

[4] *See Convention on Cybercrime (Budapest Convention)*; *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (First Protocol to Budapest Convention)*; *Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence (Second Protocol to Budapest Convention)*; *United Nations Convention against Cybercrime (Hanoi Convention)*.

[5] *See e.g.* M.N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP, 2013); M.N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP, 2017) ("*Tallinn Manual 2.0*"). The Tallinn Manual process has been facilitated by the NATO Cooperative Cyber Defence Centre of Excellence, which has 32 "sponsoring nations" as well as the support of six other States as "contributing participants". The two *Manuals* set out the views of the international group of experts that drafted them, not those of any State: *see Tallinn Manual 2.0*, pp. 2-3.

other cyber-enabled conduct.[6] Notably, for example, the 34th International Conference of the Red Cross and the Red Crescent reiterated that, "in situations of armed conflict," established international humanitarian law rules and principles "serve to protect civilian populations and other protected persons and objects, including against the risks arising from ICT activities".[7] This resolution was passed by consensus of the 196 States Parties to the Geneva Conventions, as well as the 193 components of the International Movement of the Red Cross and Red Crescent. Likewise, the UN General Assembly and UN Human Rights Council have repeatedly affirmed that "the same rights that people have offline must also be protected online".[8]

3. International criminal law is no different. As set out in this Policy, the Office considers that the provisions of the Rome Statute, including those setting out the crimes within the Court's jurisdiction, clearly apply to the commission or facilitation of these crimes by cyber means.[9] The Statute is technology-neutral in the terms in which it is written. This is important in fulfilling its object and purpose to "put an end to impunity" and "contribute to the prevention" of core international

[6] *See e.g.* *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/68/98, 24 June 2013, para. 19 ("International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability"); *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/70/174, 22 July 2015, paras. 24-29; *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, UN Doc. A/76/135, 14 July 2021, paras. 69-71. *See also* *Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/75/816, 18 March 2021, Annex I, paras. 25, 34, Annex II, paras. 9-20; UNGA Res. 73/27 (confirming the conclusions of the Group of Governmental Experts); AU Common Position, para. 4; EU Common Understanding, Annex, p. 2.

[7] *Protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict*, October 2024, 34IC/24/R2, para. 4. *See also* paras. 5-8. *See further e.g.* AU Common Position, para. 47; EU Common Understanding, Annex, p. 7.

[8] *See e.g.* UNHRC Res. 20/8, para. 1; UNHRC Res. 26/13, para. 1; UNHRC Res. 32/13, para. 1; UNGA Res. 68/167, para. 3; UNGA Res. 69/166, para. 3. *See further e.g.* UN Global Digital Compact (2024), para. 8(c) (noting the general principle that the Compact is anchored in international law, including human rights law, and that human rights must be respected, protected and promoted online and offline); AU Common Position, para. 53; EU Common Understanding, Annex, p. 8. *See also below* para. 28.

[9] While States have infrequently made specific comment to date on international criminal law when setting out their national positions on the application of international law in cyberspace, exceptions include brief discussions in the 2024 national position of Austria and a 2023 speech by the President of Estonia. Likewise, in October 2024, the International Conference of the Red Cross and Red Crescent emphasised measures to prevent and suppress international humanitarian law violations "including through investigation and prosecution where appropriate, in accordance with their international legal obligations, including with regard to ICT activities": *Protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict*, October 2024, 34IC/24/R2, para. 9.

crimes.[10] New technologies cannot be exploited to side-step accountability for conduct which is otherwise clearly prohibited—a timely reminder when there is cause for concern that armed conflicts may otherwise see new and emerging technologies, including the use of cyber operations, "outpacing normative discussions and developments".[11]

4. Thus, as a matter of law, genocide, crimes against humanity, war crimes and aggression, as well as offences against the administration of justice, can be committed or facilitated by cyber means, consistent with the established framework of international law.[12] This is the key point that this Policy wishes to convey. This conclusion can be reached using ordinary, long-established means of interpretation,[13] without impermissibly stretching existing criminal law by analogy or otherwise violating the *nullum crimen sine lege* principle.[14]

5. By contrast, the Rome Statute is not addressed to 'cybercrimes' in the sense in which the term is often used—that is, criminal offences under *national law*, such as illegal access and interception of data, system interference, or fraud or theft committed by cyber means. Under treaties like the Budapest Convention, States (some of which may also be parties to the Rome Statute) may have assumed international obligations to penalize, investigate, prosecute and cooperate in the investigation of 'cybercrimes' of this kind. Such crimes remain crimes under national law only. Yet it is, of course, possible for the same underlying conduct simultaneously to be an ordinary cybercrime under national law *and* a crime within the jurisdiction of the Court, if all of the relevant legal requirements of each regime are met.

6. This Policy therefore emphasises that the Court has jurisdiction only over international crimes set out in article 5 of the Statute, as well as offences against the administration of justice set out in article 70 of the Statute—and this

---

[10] Rome Statute, Preamble.

[11] ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* (2024) ("ICRC *Challenges* Report (2024)"), p. 57.

[12] *See* Rome Statute, art. 21(1). *See also e.g.* arts. 8(2)(a), (b), (c), (e). *See further above e.g.* para. 2.

[13] *See also Prosecutor v. Ongwen*, Appeal Judgment, ICC-02/04-01/15-2022-Red A, 15 December 2022, para. 1061; *Prosecutor v. Bemba et al.*, Appeal Judgment, ICC-01/05-01/13-2275-Red A A2 A3 A4 A5, 8 March 2018 ("*Bemba et al.* Appeal Judgment"), para. 675; *Prosecutor v. Lubanga*, Appeal Judgment, ICC-01/04-01/06-3121-Red A5, 1 December 2014, para. 277.

[14] *See further e.g.* ICTY, *Prosecutor v. Hadžihasanović et al.*, IT-01-47-AR72, Decision on Interlocutory Appeal Challenging Jurisdiction in Relation to Command Responsibility, 16 July 2003, para. 12; *Prosecutor v. Stakić*, IT-97-24-A, Judgment, 22 March 2006, Partly Dissenting Opinion of Judge Shahabuddeen, para. 39 ("the question is not whether the law, as it stands, was ever applied concretely to a particular set of circumstances, but whether the law, as it stands, was reasonably capable of applying to those circumstances").

remains the case even if they are committed or facilitated by cyber means. Yet there may be synergies between States' efforts to build capacity to effectively investigate 'cybercrimes' under national law (and to enhance State cooperation in that regard) and capacity-building and cooperation efforts with regard to cyber-enabled international crimes within the Court's jurisdiction, in line with the principle of complementarity. In particular, circumstances may arise in which the same or linked conduct is relevant *both* to the Office's investigation of crimes under international law *and* investigations carried out by national authorities under national law.

7. Accordingly, to meet these challenges and opportunities, this Policy not only addresses the Office's understanding of the applicable international law, and its implications for the further development of its own internal processes, but also highlights the importance of external cooperation. Such cooperation is necessarily framed within the overall framework of the Office's mandate to act independently in conducting investigations and prosecutions before the Court,[15] and its obligation to act consistently with internationally recognised human rights.[16] Within this context, the Office will continue its efforts to build cooperation partnerships with States and civil society including the private sector.

8. In particular, with regard to conduct in cyberspace or exploiting related new technologies, corporations may have capabilities and information which could significantly assist the investigation and prosecution of international crimes within the jurisdiction of the Court. Corporations also have responsibilities to avoid infringing on the human rights of others and, if necessary, to address adverse consequences which may arise following from their actions.[17] Consequently, the Office may engage with corporations just as it may seek the cooperation of any State, organization, or person and enter into arrangements or agreements, consistent with the Rome Statute, which may be necessary to facilitate such cooperation.[18] This supports the Office in its duty to investigate objectively in order to establish the truth.[19]

[15] Rome Statute, art. 42(1).

[16] *See* Rome Statute, arts. 21(3), 54(1)(c). *See further below* paras. 118-122.

[17] *See e.g.* UN, *Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework*, 2011, principles 11, 13-14, 17. *See further* UNHRC Res. 17/4, para. 1 (endorsing these principles).

[18] *See* Rome Statute, art. 54(3)(c)-(d).

[19] Rome Statute, art. 54(1)(a).

Policy objectives

9. By issuing this Policy, the Office seeks to achieve the following objectives:

a. To affirm the Office's commitment to the rigorous investigation and prosecution of cyber-enabled crimes within the jurisdiction of the Court, including offences against the administration of justice;

b. To emphasise the Office's view that crimes under the Rome Statute may be committed or facilitated by cyber means, and that the Court's jurisdictional framework can apply to them;

c. To demonstrate that the Office's mandate will not be outpaced by technology, and that the Statute applies equally to all criminal conduct within the Court's jurisdiction, irrespective of the context in which it is carried out;

d. To emphasise the Office's commitment to establishing an institutional environment that facilitates effective investigation and prosecution of cyber-enabled crimes within the jurisdiction of the Court—including through recruitment, training, external collaboration, and meaningful implementation, monitoring, and evaluation measures;

e. To encourage and support national efforts to repress cyber-enabled crimes within the jurisdiction of the Court, including offences against the administration of justice, consistently with internationally recognised human rights;

f. To cooperate with and coordinate civil society organisations, corporations and other non-State actors, whose expertise or access to information enables them to support relevant law enforcement action at the international or, where appropriate, national level;

g. To contribute to the development at the Court and beyond of jurisprudence and best practices concerning the prosecution of genocide, crimes against humanity, war crimes, and the crime of aggression, when committed or facilitated by—or otherwise correlated with—the use of cyberspace.

10. The Policy presents the Office's understanding of its mandate in the context of the increasing relevance of cyberspace to all aspects of modern life. It will set out the views of the Office on the application of the Court's legal framework to conduct in cyberspace, and explain how crimes under the Statute—including not only article 5 crimes but also offences against the administration

of justice under article 70—can be committed and facilitated by cyber means.[20] Finally, it will articulate fundamental principles underlying the Office's approach to the investigation and prosecution of such crimes and provide guidance as to how these principles inform Office practice.

11. This Policy aligns with the Office's other policy documents. It draws on the experience of the Office, its existing good practices and lessons learned, as well as relevant jurisprudence, including that of the Court and other courts and tribunals. This Policy is subject to revision and does not give rise to legal rights.

Background

12. In June 2023, in its *Strategic Plan 2023-2025*, the Office announced its intention to develop this Policy. January 2024 marked the commencement of a more intensive series of policy engagements by the Office in this area with a conference convened at the seat of the Court, in partnership with Microsoft. This conference brought together cybersecurity and technology experts, corporations, civil society, academics, State representatives, and members of the judiciary, to examine the practical implications of the misuse of cyberspace to commit or facilitate serious crimes under the Rome Statute.[21]

13. The drafting of this Policy was led by the Special Adviser on Cyber-Enabled Crimes, Prof. Marko Milanović, with support from key Office staff. An internal draft also received feedback from Office staff in various divisions, including international cooperation and complementarity, policy drafting and gender issues, preliminary examinations, investigations, and prosecutions. The team also consulted with relevant Special Advisers to ensure the Policy harmonised with other relevant Office policies and guidance documents.

14. While the application of existing international criminal law to cyber-enabled crimes within the jurisdiction of the Court is yet to be litigated,[22] it has nonetheless inspired a substantial body of academic scholarship. The Office acknowledges two expert-led initiatives in particular, which have particular

[20] Where appropriate, however, this Policy may refrain from taking a definitive position on a certain issue at the present time, and recognise diversity of opinion. This may not be taken to imply the Office's view of that diversity of opinion, or that the Office considers there is any necessary lacuna or ambiguity in the law.

[21] *See e.g.* ICC Office of the Prosecutor, *Statement by ICC Prosecutor Karim A.A. Khan KC on conference addressing cyber-enabled crimes through the Rome Statute system*, 22 January 2024.

[22] The Office has, however, received several communications pursuant to article 15 of the Statute dealing with cyber-enabled crimes.

relevance to the intersection of international criminal law and cyber operations.

- First, the process hosted by the Permanent Mission of Lichtenstein to the UN and co-organized by the Permanent Missions of Argentina, Austria, Belgium, Costa Rica, the Czech Republic, Estonia, Luxembourg, Portugal, Spain and Switzerland, which culminated in the 2021 *Council of Advisers' Report on the Application of the Rome Statute of the International Criminal Court to Cyberwarfare*.[23] The Office participated in this process as an observer, as did the International Committee of the Red Cross.

- Second, the ongoing work on the *Tallinn Manual 3.0* on the international law of cyber operations. While the third edition of the *Manual* is yet to be published, a new chapter on international criminal law and cyber operations was drafted, discussed and adopted by the *Manual's* International Group of Experts in 2024. The Office reviewed this draft, and provided its own feedback to the *Manual's* editors.

15. In drafting this Policy, the Office has not considered itself to be bound by the conclusions in either of these initiatives. It has simply taken due account of them as an aid to interpreting the content of relevant international law. The Office has also taken account of other scholarly projects looking at international law and cyber operations more broadly, such as the *Tallinn Manual 2.0* and the *Cyber Law Toolkit.*

16. An initial draft of the Policy was released for a round of public consultation on 7 March 2025. The Office is grateful for the valuable participation in this consultation of a diverse range of States Parties, civil society organisations, and individual experts, as well as representatives of the private sector.

17. The Office commits to continuing and extending this consultative approach as it works to implement the Policy itself, including by identifying victims and communities who may be disproportionately affected by conduct in cyberspace falling within the jurisdiction of the Court.

[23] Permanent Mission of Liechtenstein to the United Nations, *The Council of Advisers' Report on the Application of the Rome Statute of the International Criminal Court to Cyberwarfare*, August 2021 (report available from the Global Campaign for Ratification and Implementation of the Kampala Amendments on the Crime of Aggression) ("Council of Advisers' Report").

KEY TERMS AND CONCEPTS

Cyber

18. The term 'cyber' is used broadly in this Policy to denote the range of activities involving information and communications technologies (also known as ICT, or loosely as digital technologies) or networks, including artificial intelligence (AI). Such technologies or networks may very frequently be 'online' in some fashion, but need not necessarily be so. Relevant to the investigation and prosecution of crimes within the jurisdiction of the Court, conduct in cyberspace may typically encompass the use, manipulation or disabling of computer systems as a direct means of committing a crime, or to prepare, facilitate or target such crimes including by harvesting data to identify, locate, or track victims. Cyber conduct or means are in this context often contrasted with 'physical', 'kinetic', or 'traditional' means of carrying out or facilitating criminal activity.

Cyber-enabled crime under the Rome Statute

19. As explained in detail below, 'cyber-enabled crime' is used in this Policy as a factual term (rather than as a legal concept) to refer to crimes within the jurisdiction of the Court—that is, genocide, crimes against humanity, war crimes and aggression, as set out in article 5 of the Rome Statute, or offences against the administration of justice at the Court under article 70—when these crimes are *committed or facilitated* with the use of cyber means.

20. A crime is *committed* (perpetrated) by cyber means if the conduct element of the offence is satisfied by cyber conduct carried out by the perpetrator, or if the suspect makes an essential contribution to that conduct element by cyber means, consistent with the requirements of article 25(3)(a) of the Statute. The commission of Rome Statute crimes by cyber means can be direct or indirect.

21. A crime is *facilitated* by cyber means if a person engages in cyber conduct that satisfies the elements of a mode of responsibility listed in articles 25 or 28 of the Statute,[24] other than commission. These include ordering, inducing, soliciting, and aiding and abetting. It is irrelevant in this context whether the underlying crime of the principal is itself committed by cyber means (it could, but need not, be).

[24] But concerning article 28 of the Statute, and its proper legal characterisation, *see below* fn. 140.

22. Additionally, cyber conduct may also be *correlated* with the commission of a crime within the jurisdiction of the Court, even if it does not directly underpin the suspect's own conduct for the purpose of the relevant *actus reus*. Such conduct might, for example, be probative of the suspect's crime, including helping show the necessary intent and knowledge. For example, conduct in cyberspace might aim at concealing evidence of a crime which is being or has been committed (for example, by shutting down internet services in a given location), or might exploit such a crime for other purposes, such as propaganda, by means of social media. Cyber conduct may also provide relevant contextual evidence, for example to help establish the policy requirement for crimes against humanity, or to aggravate criminal responsibility for the purpose of sentencing.

23. The possibility that correlated conduct of this kind may be committed by cyber means is very significant, because it points to the increasing relevance of conduct in cyberspace to *all* of the Office's investigations, irrespective whether there is an obvious cyber dimension to the charged crime or form of responsibility. The pervasive nature of information technology means that, increasingly, many if not all criminal investigations will likely have a cyber component.

24. It is not required in any of these respects that the relevant cyber conduct necessarily violates applicable domestic law, although of course this may sometimes be the case. For example, intrusive surveillance potentially amounting to the *actus reus* of a crime under the Statute, such as persecution under article 7(1)(h), might be carried out either in accordance with a provision of domestic law, or in violation of it.

25. Likewise, it is not required in any of these respects that the relevant cyber conduct is a misuse of the hardware or software concerned, although again this may sometimes be the case. Thus, the use of destructive malware could amount to a crime under the Statute, or facilitate such a crime, but so too could the use of a computer system with the permission of its owner and in accordance with its planned functions—for example, the use of an artificial intelligence (AI) 'decision support system' to help choose (unlawful) targets for attack.

Cybercrime

26. 'Cybercrime' includes a range of offences (criminalised under domestic law, but not under the Statute) that are committed or otherwise enabled by cyber means, such as illegal access to a computer system, illegal interception, data interference, system interference, fraud, or the dissemination of child sexual abuse material. Such offences are the subject of treaties like the Budapest Convention or

the UN Convention against Cybercrime, which require States to criminalize them, prosecute them and cooperate in their investigation and prosecution. Cybercrimes so defined are not, as such, crimes within the jurisdiction of the Court.

27. Some of the types of conduct prohibited as 'cybercrimes' under national law, such as illegal access to a computer system, may also amount or otherwise be relevant to crimes within the Court's jurisdiction—for example, illegally accessing certain computer systems may be the first step in facilitating or even committing a war crime. For this reason, within the limits of its mandate under the Statute and consistent with internationally recognised human rights, the Office may in appropriate circumstances cooperate with national jurisdictions in investigating and prosecuting such conduct. There may be mutual benefit in pooling capabilities, techniques, skills, and procedures related to the investigation of conduct in cyberspace.

28. Both State and international efforts to address cybercrimes under national law must go hand-in-hand with respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments.[25]

Digital evidence

29. Evidence in electronic form (frequently described as 'digital evidence') is increasingly relevant to all investigations conducted by the Office, regardless of the means by which a crime might have been committed. Such evidence is also naturally inherent to the investigation and prosecution of cyber-enabled crimes within the jurisdiction of the Court. Yet detailed questions of its collection, analysis, management, and use are a topic of sufficient complexity and reach that they exceed the scope of this Policy and may merit consideration in their own right. Accordingly, such matters are only briefly addressed in this Policy as necessary. Likewise, and for similar reasons, this Policy does not address in any detail the use of digital technologies in forensic analysis or information management.

[25] *See* *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/68/98, 24 June 2013, para. 21; *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/70/174, 22 July 2015, para. 13(e). *See also* *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, UN Doc. A/76/135, 14 July 2021, paras. 36-41, 70; UNGA Res. 68/167, para. 4; UNGA Res. 69/166, para. 4.

Artificial intelligence

30. Artificial intelligence (AI) technologies are developing rapidly, and have obvious significance for any discussion of cyber-enabled crimes under the Rome Statute. It is thus appropriate to set out certain key principles in this Policy. At the same time, the very rapidity of the development of these technologies—and the wide variety of different applications and modalities for their use which may emerge—underlines the need for restraint in attempting to map the variety of possible implications at the present time. It is in this context that the wider dialogue concerning the sufficiency of the existing law may be at its most acute.[26]

31. What is already clear is that not all AI technologies are the same, nor put to the same use. Not all uses of AI will necessarily raise the same legal questions. At the very least, therefore, some of these critical distinctions can be usefully identified. It is also important to underline that, consistent with the approach of this Policy more generally, it is the view of the Office that the decision to deploy and use *any* AI technology must be consistent with the existing rules of IHL and international human rights law.[27] This is without prejudice to the question whether additional regulation may be useful to help ensure appropriate accountability at all relevant points throughout the development, distribution, and employment of an AI system (the so-called AI 'life cycle').

32. Thus, at one end of the spectrum, AI may simply be used *as a means* (like any other technology) to commit crimes in the jurisdiction of the Court or to facilitate them—but without necessarily affecting the criminal responsibility of a natural person using that technology and acting with intent and knowledge, as required under the Statute.[28] An example might be the use of AI-enhanced tools to support decision making, where a natural person (a so-called 'person in the loop') still makes all of the relevant decisions which lead to the commission of a crime. In these circumstances, the manner of operation of the AI system and the circumstances in which the user employed that system may be *evidentially* relevant[29]—but nothing changes as a matter of law. The core question remains the

[26] *See above* paras. 1-2.

[27] UNGA Res. 79/239, para. 1 ("Affirm[ing] that international law […], international humanitarian law and international human rights law, applies to matters governed by it that occur throughout all stages of the life cycle of artificial intelligence, including systems enabled by artificial intelligence, in the military domain"). *See also* ICRC, *Submission to the United Nations Secretary-General on Artificial Intelligence in the Military Domain* (2025), pp. 1-2.

[28] *See e.g.* Rome Statute, arts. 30, 32.

[29] *See also* ICRC, *Submission to the United Nations Secretary-General on Artificial Intelligence in the Military Domain* (2025), pp. 4-7, and Annex.

criminal responsibility of the individual making the relevant decisions, based on their own conduct (*actus reus*) and their mental state (*mens rea*).

33. At the other end of the spectrum may lie the potential development of AI technologies—including but not limited to so-called artificial *general* intelligence (AGI)—carrying out acts *autonomously* which, if committed by a natural person, would amount to crimes within the jurisdiction of the Court. Depending on the circumstances, the independent commission of such acts may be by design, or may be unintended and/or unforeseen.

34. In the latter scenario in particular, it may be more difficult to identify any natural person committing a relevant act with intent and knowledge, notwithstanding the harm caused. Obvious risks arise, for example, with regard to AI integrated into autonomous weapon systems.[30] Yet, formally, this still remains without prejudice to the potential application of the existing crimes within the jurisdiction of the Court, in the circumstances of a particular case, where a natural person, acting with intent and knowledge, may be proven to have caused or contributed to crimes resulting from the use of an AI system.

[30] *See e.g.* ICRC, *Submission to the United Nations Secretary-General on Artificial Intelligence in the Military Domain* (2025), p. 3 (noting that "[t]he integration of AI, particularly machine learning (ML) techniques, into autonomous weapon systems (AWS) exacerbates existing challenges posed by AWS in ensuring compliance with IHL", and reiterating "the joint call made by the ICRC President, with the UN secretary-general, for new, legally binding rules prohibiting certain AWS and constraining the use of others", including "a prohibition on unpredictable AWS—those that, due to their design or the circumstances and manner of use, do not allow a human user to understand, predict and explain the system's functioning and effects"). *See also* p. 7 (noting the use of AI to enhance cyber operations, including cyber attacks, with potentially increased "risks of indiscriminate attacks, incidental civilian harm, including damage to critical civilian infrastructure, as well as the uncontrolled escalation of conflict, particularly in complex and interconnected digital environments").

APPLICABLE LAW AND JURISDICTION

35. The investigation and prosecution of cyber-enabled crimes within the jurisdiction of the Court takes place within a prescribed legal framework, namely the Rome Statute, read together as appropriate with the Elements of Crimes ('Elements') and the Rules of Procedure and Evidence ('Rules').

36. Article 21(1) of the Statute sets out the applicable law before the Court. In the first place, the Court must apply the Statute, Elements, and Rules themselves. Second, where appropriate, the Court must also apply applicable treaties and the principles and rules of international law, including the established principles of the international law of armed conflict. Third, failing that, where necessary, the Court must apply general principles of law derived by the Court from national law of legal systems of the world, provided they are not inconsistent with the Statute, international law, and internationally recognised norms and standards.

37. Article 21(3) further mandates that both the application and interpretation of the Statute must be consistent with internationally recognised human rights, without any adverse distinction. Rights particularly relevant to the investigation and prosecution of cyber-enabled crimes may include, *inter alia*, the right to life, the right to physical and mental health, the right to freedom of expression, the right to privacy and family life, the right to participate in public affairs, and the right to freedom from discrimination, including on grounds of gender.[31]

38. Any case investigated by the Office—including with regard to cyber-enabled crimes—must form part of a situation fulfilling the statutory preconditions to the exercise of the Court's jurisdiction: temporal jurisdiction; either territorial or personal jurisdiction; and subject-matter jurisdiction.[32] The Court may only exercise jurisdiction over natural persons, of 18 years of age or more.[33]

39. Additionally, the *exercise* of the Court's jurisdiction must also be triggered in accordance with the Statute, either by a referral to the Court by a State Party or by the UN Security Council or the action of the Prosecutor at their own motion, *and* is subject to a showing that the legal thresholds for the Court's intervention are

[31] *See also below* paras. 118-122.

[32] Rome Statute, arts. 5, 11-12.

[33] Rome Statute, arts. 25(1), 26.

satisfied.[34] Just because cyber-enabled crimes under the Statute *can* be addressed by the Court does not mean that they always will be. In this regard, as set out further below, a key consideration may be the gravity of the relevant conduct—relevant not only in determining whether an investigation may be opened, but also which potential cases in that situation might ultimately be investigated with a view to prosecution before the Court.

40. Under article 12(2) of the Statute, the Court has jurisdiction over a crime:

> if one or more of the following States are Parties to this Statute or have accepted the jurisdiction of the Court in accordance with paragraph 3:
>
> (a) The State on the territory of which the conduct in question occurred or, if the crime was committed on board a vessel or aircraft, the State of registration of that vessel or aircraft;
>
> (b) The State of which the person accused of the crime is a national.

41. Cyber-enabled crimes may be seen as posing certain challenges to the application of this jurisdictional framework. Nevertheless, the Office considers that the Court's jurisdiction over conduct in cyberspace is regulated by the same jurisdictional principles applicable to other kinds of conduct under the Statute. This is based on the classical principles of territoriality and personality that are universally accepted under general international law. Notably, States rely on such principles to exercise their own national jurisdiction over conduct in cyberspace. When interpreting the pre-conditions to the Court's exercise of jurisdiction set out in article 12(2), such as the understanding of when conduct is to be regarded as taking place "on the territory" of a State, the Office may therefore also take into account as appropriate the general practice of States in such situations.[35]

42. With regard to the territoriality principle under article 12(2)(a) of the Statute, the key question is where 'the conduct in question occurred,' and how precisely to define the scope of the relevant conduct. The Court has already addressed these matters, holding that territorial jurisdiction will exist even if "at least one element […] or part of" a crime within the jurisdiction of the Court occurred on a State Party's territory.[36] With respect to the term 'conduct' in

---

[34] Rome Statute, arts. 13-15, 53. *See also* ICC RPE, rule 48. For the crime of aggression, which has a distinct jurisdictional regime, *see further* Rome Statute, arts. 15*bis*, 15*ter*. *See below* paras. 146-150.

[35] *See also above* para. 36.

[36] *Situation in Bangladesh/Myanmar*, Decision pursuant to article 15 of the Rome Statute on the authorisation of an investigation, ICC-01/19-27, 14 November 2019 ("*Bangladesh/Myanmar* Article 15 Decision"), para. 43. *See also Request under Regulation 46(3)*, Decision on the 'Prosecution's request for a ruling on jurisdiction under article 19(3) of the Statute', ICC-RoC46(3)-01/18-37, 6 September 2018, paras. 64, 70, 72.

article 12(2), the Court further held that "the word is used in a factual sense, capturing the *actus reus* element underlying a crime"[37] and that "depending on the nature of the crime alleged, the *actus reus* element of conduct may encompass within its scope, the consequences of such conduct."[38]

43. Bearing these principles in mind, the Office is of the view that the Court's territorial jurisdiction would cover both subjective and objective territoriality when it comes to the commission of crimes by cyber means. That is, it would extend to both the territory of the State (or States) in which the criminal conduct began (subjective territoriality), and to that of the State (or States) in which it is completed (objective territoriality).[39] The same applies, *mutatis mutandis*, to crimes committed by cyber means on board a vessel or aircraft registered with a State Party (*i.e.*, flag jurisdiction, which is another application of the territoriality principle).

44. In the view of the Office, the above analysis equally covers situations in which the cyber conduct in question took place in the territory of more than two States simultaneously.[40] The use of cloud computing technology to commit or facilitate crimes under the Rome Statute may pose one such example. Nothing in the jurisdictional framework of the Rome Statute precludes the possibility of concurrent territorial jurisdiction by multiple States and the Court.[41] Instead, the Statute provides for the principle of complementarity as a means to resolve

---

[37] *Bangladesh/Myanmar* Article 15 Decision, para. 49. *But see also* para. 61 (referring to "at least part of the conduct (*i.e.* the *actus reus* of the crime)" and "part of the *actus reus*").

[38] *Bangladesh/Myanmar* Article 15 Decision, para. 50. *See also* ICC OTP, *Situation in the Republic of Korea: Article 5 Report* (June 2014), para. 39.

[39] *See also Tallinn Manual 2.0*, pp. 55-57. The *Manual* discusses the jurisdiction of States, rather than the jurisdiction of the Court specifically. However, because the jurisdiction of the Court is grounded in the territoriality and nationality principles that have long guided the boundaries of State jurisdiction, the *Manual*'s analysis of these principles in the cyber context is helpful in examining the jurisdiction of the Court. *See also e.g.* England and Wales, *Shehabi & Anor v Kingdom of Bahrain* [2024] EWCA Civ 1158, para. 34 (the Court of Appeal of England and Wales holding unanimously that "as a straightforward use of language, the remote manipulation from abroad of a computer located in the United Kingdom is an act within the United Kingdom. The true position in such a case is that the agents of the foreign state commit acts both in this country and abroad"). Additionally, some commentators treat the 'effects doctrine' as a further dimension of territorial jurisdiction, with particular utility concerning cyber-enabled crimes: *see e.g. Tallinn Manual 2.0*, pp. 57-59; W. Schabas and G. Pecorella, 'Article 12: preconditions to the exercise of jurisdiction,' in K. Ambos (ed.), *Rome Statute of the International Criminal Court: Article-by-Article Commentary*, 4th Ed. (Beck/Hart/Nomos, 2022), p. 820. *See further* K. Ambos, *Treatise on International Criminal Law, Volume III: International Criminal Procedure* (OUP, 2016), pp. 213-216.

[40] *See Tallinn Manual 2.0*, p. 57.

[41] Indeed, as a matter of general international law, there is no indication in State practice that only the State with the 'best' jurisdictional claim (for example, because most of the harm occurred there) can exercise exclusive territorial jurisdiction: *see e.g. Tallinn Manual 2.0*, p. 54.

any conflict of jurisdictions which may actually arise.[42] This is consistent with the nature of the crimes under the jurisdiction of the Court, which are the most serious crimes of international concern, and ensures that there is no risk of impunity resulting from a mere failure by States to exercise the jurisdiction that they possess.[43]

45. The Office notes that there is some disagreement among States and experts on the question of whether the territoriality principle could apply to situations where there is only a minimal connection with cyber infrastructure on a State's territory, for instance, if data packets through which a piece of malware was transmitted simply transited through cables or servers on the territory of a State Party.[44] Bearing in mind the carefully calibrated jurisdictional regime of the Rome Statute, and in the specific context of cyberspace, the Office would not regard the mere transit of data through a State Party's territory as a sufficient basis to assert the Court's territorial jurisdiction.[45]

46. Even if there is no basis to establish the jurisdiction of the Court on the basis of territoriality under article 12(2)(a), the Court may still exercise jurisdiction under article 12(2)(b) on the basis of the nationality (active personality) principle if the perpetrator is a national of a State which is a Party to the Statute or accepts the jurisdiction of the Court. By contrast, the nationality of the offender is irrelevant if the Court already has jurisdiction on the basis of the territoriality principle.[46]

47. Finally, while crimes within the Court's jurisdiction can be committed by cyber means, the *facilitation* by cyber means of crimes under the Statute (however carried out) may be particularly likely. This raises the question of how the Court's territorial and personal jurisdiction framework would apply to accessorial conduct or to forms of responsibility other than direct perpetration. This is a matter of some complexity. It is not cyber-specific, and has not been addressed in the Court's jurisprudence so far. The Office is of the view that, *at a minimum*, the Court would have jurisdiction in a scenario in which a person facilitates a crime

---

[42] *See* Rome Statute, arts. 17-19. *See also* art. 53(1)(b); ICC RPE, rule 48. *See also below* para. 180.

[43] *See* Rome Statute, Preamble.

[44] *Tallinn Manual 2.0*, p. 55.

[45] *But see Tallinn Manual 2.0*, p. 55 (considering that, "if cyber infrastructure in an intermediary State constitutes an integral facet of an operation, that State will enjoy jurisdiction based on the territorial principle", considering that "the use of such compromised infrastructure was not of *de minimis* character").

[46] *See e.g. Situation in the State of Palestine*, Decision on Israel's challenge to the jurisdiction of the Court pursuant to article 19(2) of the Rome Statute, ICC-01/18-374, 21 November 2024, para. 13; *Situation in Afghanistan*, Decision pursuant to article 15 of the Rome Statute on the authorisation of an investigation, ICC-02/17-33, 12 April 2019, para. 58.

that is committed on the territory of a State Party, by kinetic or cyber means, regardless of whether the accomplice is himself or herself acting on the territory of a State Party.[47]

48. The Office concludes this discussion of jurisdiction by noting that the application of the Court's jurisdictional framework to cyber-enabled crimes may inevitably lead to complex scenarios. For obvious reasons, this Policy cannot anticipate all possible permutations, and should not be taken as a complete statement of the views of the Office on these jurisdictional questions. The Office reserves its position on all issues not expressly addressed above, and in any event underlines the importance of considering each scenario on its own merits if and when it may arise in the work of the Office and the Court.

[47] *See* *Situation in Afghanistan*, Public redacted version of 'Request for authorisation of an investigation pursuant to article 15', ICC-02/17-7-Red, 20 November 2017, para. 47.

COMMITTING ROME STATUTE CRIMES BY CYBER MEANS

49. As noted above, the position of the Office is that crimes within the jurisdiction of the Court can, in principle, be committed by cyber means. Obviously, this is more straightforwardly the case with some crimes than with others. Questions may arise in litigation, for example, concerning causation—how the perpetrator's conduct actually caused certain consequences. Such questions will be resolved on the basis of the same fundamental principles as for crimes within the jurisdiction of the Court which are committed by other means. But this does not change the essential fact that the crimes under the Statute are generally framed in a technology-neutral way.[48]

50. The following discussion will necessarily focus on particular *actus reus* elements of relevant crimes, in order to illustrate aspects which may be especially salient when considering the use of cyberspace. However, the Office emphasizes that it would in each case also be necessary to establish the corresponding *mens rea* as required by the Statute. Notably, and unless otherwise required by the terms of the Rome Statute, this requires the *actus reus* elements to be committed with intent and knowledge as defined in article 30 of the Statute.[49] Again, the mental elements apply in the same way for cyber-enabled crimes within the jurisdiction of the Court as to such crimes committed by other means. Some aspects of the use of cyber means may assist the Office in showing the necessary intent and knowledge, while other aspects may pose unique challenges. Such issues are, however, evidentiary rather than legal in nature.

51. Consistent with the requirements of the Rome Statute, the Office will seek to establish cyber-enabled crimes within the jurisdiction of the Court to the same standard of proof that would apply to such crimes committed by other means. Ultimately, at trial, this requires that "the Court must be convinced of the guilt of the accused beyond reasonable doubt."[50]

52. The examples given in this section are illustrative of some typical scenarios, but are not intended to be comprehensive. Silence on a particular crime in this section does not mean that it cannot be committed by cyber means.

---

[48] *See above* paras. 3-4.

[49] Rome Statute, art. 30.

[50] Rome Statute, art. 66(3). *See further below* para. 175.

Genocide (including direct and public incitement to genocide)

53. The crime of genocide, as defined in article 6 of the Statute and article II of the Genocide Convention, is concerned with the protection of certain human groups from proscribed forms of harm which could cause their destruction, at least in part. Since such conduct may occur in a wide variety of potential contexts and circumstances, there is no reason to consider that the means by which the prohibited conduct is carried out excludes any form of technology. Consequently, genocide can undoubtedly be committed by cyber means.

54. The main distinguishing feature of genocide—genocidal intent—is a mental element, which can be proven by any means. There is nothing special about it in the cyber context. Conduct in cyberspace may well be relevant to proving genocidal intent; for example, an individual's activity on social media may provide clear insights into their state of mind. Likewise, while the genocidal intent itself (to destroy a protected group) is generally understood to entail physical or biological destruction, this does not mean that the *means* used to cause such destruction must themselves be physical or tangible.[51]

55. As for the *actus reus* of genocide, the five forms of genocide are all susceptible to commission by cyber means. Killing members of a group, causing them serious bodily or mental harm, or inflicting on a group conditions of life calculated to bring about its physical destruction, in whole or in part, can be done, for instance, through cyber attacks against services essential to human life and wellbeing such as water and electricity supply, heating, medical facilities, or food production.[52] There is no meaningful legal difference between killings caused by bullets or those caused by cyber operations, so long as the requisite degree of causation can be proven.[53]

56. Similarly, cyberspace and digital technologies can be used as part of a programme of measures intended to prevent births within the group, or to forcibly transfer children from the group to another group.[54] Such technologies can also be used as a means to create and publish online material which may itself inflict serious mental harm (including depictions of the commission of serious crimes).[55] The Office does not consider that there is any reason in principle why this would be incompatible with proof of the required specific intent to destroy the group in whole or in part.[56]

---

[51] *See* Council of Advisers' Report, p. 74.

[52] *See* Council of Advisers' Report, pp. 77-84. *See also below* paras. 72-73, 86, 93.

[53] *See above* para. 49.

[54] *See* Council of Advisers' Report, pp. 84-85.

[55] *See further below* paras. 75-78, 95.

[56] *Cf.* Council of Advisers' Report, pp. 79-83. *See also above* para. 54.

57. Practically speaking, at least at present, the Office considers it unlikely that a real-world scenario of genocide would be committed solely or primarily by cyber means—but this does not preclude the possibility that individual offenders within the context of a genocide may act by such means.[57] Indeed, future instances of genocide may be committed through a combination of various means, some of them cyber. In such cases, perpetrators of cyber-enabled genocide will be investigated and prosecuted equally with those who employed conventional, physical means.

58. Another scenario for the prosecution of cyber operators arises from article 25(3)(e) of the Statute, addressing direct and public incitement to commit genocide. Consistent with the duty of States under the Genocide Convention to prevent genocide, this conduct may be of particular concern because it creates a grave and unacceptable risk that genocide will occur.

59. In the view of the Office, there is no doubt that direct and public incitement of genocide can be committed by cyber means, for example, through postings on social media platforms. When made with the requisite intent, such postings could satisfy the relevant *actus reus* requirements and be prosecuted as such, having regard to the context in which such statements were made, and provided that they were sufficiently direct in calling for genocide to be carried out.[58] This latter criterion may be especially significant in determining the criminal nature of the relevant conduct.[59]

60. The use of cyber means, including social media, to carry out an act of incitement may afford it much greater reach, and have impact more quickly, than other forms of speech. The Office considers that, in at least some cases of particular gravity, relevant conduct may also include sharing or otherwise disseminating utterances originating from others. Further, while it is not the business of the Office or the Court to supervise the day-to-day operation of online service providers (including with regard to algorithmic content promotion, curation or moderation), this does not exclude the potential responsibility under the Statute of any natural person—acting with the required intent and knowledge—even for conduct carried out in the context of commercial activity.[60]

61. With particular relevance to the scenarios described above, the Office recalls that the Rome Statute provides only for cases of "sufficient gravity" to

[57] *See also e.g.* Elements of Crimes, art. 6(a), Element 4.

[58] *See also* Council of Advisers' Report, pp. 86-88.

[59] *See further below* para. 122.

[60] *See further below* para. 170.

be admissible before the Court.[61] This filters out "those rather unusual cases when conduct that technically fulfils all the elements of a crime under the Court's jurisdiction is nevertheless of marginal gravity only."[62] Likewise, the Office also bears in mind the potential need to apply relevant principles of international human rights law in determining whether speech acts themselves merit criminal responsibility.[63]

Crimes against humanity

62. Crimes against humanity aim to ensure broad protection to the civilian population from the widespread or systematic infliction of certain serious harms set out in article 7(1) of the Statute, committed according to a State or organisational policy.[64] Like genocide, crimes against humanity can be committed both in peacetime and during armed conflict. They do not require a nexus to an armed conflict, and the notion of 'attack' which is part of their contextual element is not equivalent to the notion of 'attack' in international humanitarian law (IHL, the law of armed conflict).[65] Crimes against humanity thus have a close relationship to international human rights law. While not all human rights violations amount to a crime against humanity, the specific prohibitions which do amount to crimes against humanity are informed by corresponding human rights.

63. Cyberspace can be a medium to implement or facilitate potential human rights violations but also a medium to combat or remedy certain violations. Consequently, conduct in cyberspace may be relevant not only as a means of committing or facilitating crimes against humanity, but also as a means of proving or obtaining evidence about them.

---

[61] *See* Rome Statute, art. 17(1)(d). *See also below* paras. 131-132.

[62] *See e.g.* *Prosecutor v. Al Hassan*, Judgment on the appeal of Mr Al Hassan against the decision of Pre-Trial Chamber I entitled 'Décision relative à l'exception d'irrecevabilité pour insuffisance de gravité de l'affaire soulevée par la défense', ICC-01/12-01/18-601-Red OA, 19 February 2020, paras. 53-59.

[63] *See further below* para. 122.

[64] *See further* K. Ambos, 'Article 7: crimes against humanity,' in K. Ambos (ed.), *Rome Statute of the International Criminal Court: Article-by-Article Commentary*, 4th Ed. (Beck/Hart/Nomos, 2022), p. 146 (mn. 3). *See also* Rome Statute, arts. 7(1)(k) (referring to other "inhumane acts" similar to those enumerated in article 7(1), 7(2)(h) (characterising article 7(1) acts as "inhumane acts"). This does not mean that article 7(1) acts must invariably be directed against "the physical integrity or liberty of persons": *contra* *Prosecutor v. Bemba*, Appeal Judgment (Separate Opinion of Judges Van den Wyngaert and Morrison), ICC-01/05-01/08-3636-Anx2, 8 June 2018, para. 63.

[65] These acts "need not constitute a military attack": Elements of Crimes, Introduction to Article 7, para. 3.

64. One clearly observable phenomenon in the course of the Office's work to date has been the rise in victims, affected communities, and civil society organisations using cyber means to monitor, document, and report crimes within the jurisdiction of the Court.[66] At the same time, there is also a clear rise in attempts to impede such activities, including on occasion by the use of more or less targeted 'internet shutdowns', which may serve the aim of attempting to conceal evidence of the commission of crimes. Irrespective of whether such conduct itself amounts to a crime within the jurisdiction of the Court,[67] such conduct may be relevant to matters such as establishing the perpetrators' intent and/or the existence of a relevant State or organisational policy.

65. Likewise, cyberspace may afford a means for the targeting of certain communities, either as a whole or through prominent representatives (such as leadership figures, human rights defenders, journalists, etc.). This can be achieved through means which either themselves amount to a crime in the jurisdiction of the Court or, perhaps more commonly, which serve as a precursor to such crimes (whether committed by cyber means or otherwise). Typical examples may include the use of intrusive surveillance, and information operations (such as disinformation campaigns) exploiting social media.

CONTEXTUAL ELEMENTS

66. For the purpose of the contextual element of crimes against humanity, it is necessary to prove the existence of a qualifying 'attack' against any civilian population, pursuant to or in furtherance of a State or organizational policy. An 'attack' is a course of conduct involving the multiple commission of acts referred to in article 7(1) of the Statute.[68] It must additionally be shown either to be 'widespread' or 'systematic'.

67. Conduct in cyberspace that amounts to one of the acts defined in article 7(1) of the Statute—such as murder, persecution, or other inhumane acts—may be charged as a crime against humanity if it is committed as part of such an attack. It is important to underline that cyber operations conducted as part of such a context need not themselves, when assessed in isolation, satisfy the threshold criterion. For example, a cyber operation that resulted even in a small number of deaths could nonetheless qualify as the crime against humanity of murder,

[66] *See also* ICC OTP, *Documenting international crimes and human rights violations for accountability purposes: guidelines for civil society organisations* (2022). Information concerning alleged crimes within the jurisdiction of the Court can be directly reported to the Office using OTPLink.

[67] *See also below* para. 78.

[68] Rome Statute, art. 7(2)(a).

if it was done as part of a wider attack meeting the threshold 'widespread' or 'systematic' criterion and other requirements.

68. A group may qualify as an 'organization' for the purpose of article 7 if it has "sufficient resources, means and capacity to bring about the course of conduct or the operation involving the multiple commission of acts referred to in article 7(2)(a) of the Statute."[69] As such, cyber-enabled crimes against humanity can thus be committed not only by individuals acting on the behalf of States, but also by non-state actors, such as members of organised armed groups. The Office recalls that it will always determine whether this test is met on the basis of a fact-specific, contextual assessment—but notes that there is no reason in principle why such organizations cannot, in appropriate cases, also include hacker groups, especially if part of a wider entity such as an armed group, or a corporation.[70]

69. In principle, since a widespread or systematic attack is established by the multiple commission of article 7(1) acts (and these may be carried out by cyber means), it is possible that conduct carried out *exclusively* by cyber means could amount to a widespread or a systematic attack.[71] However, in practice, it may be more likely for this threshold to be satisfied when cyber acts are mixed with physical or kinetic conduct also amounting to article 7(1) acts against the civilian population.

70. The Office further notes that conduct in cyberspace may well be relevant in establishing the required policy to commit an article 7 attack. This requirement aims to show that "the multiple acts forming the course of conduct are linked", and "ensures that acts which are unrelated or perpetrated by individuals acting randomly on their own are excluded."[72]

EXAMPLES OF UNDERLYING CRIMES

71. Assuming the contextual elements are satisfied (whether by cyber or kinetic means), many crimes against humanity in the Statute have obvious potential to be committed by cyber means.[73] The following examples, therefore, are merely illustrative. In practice, the Office anticipates that most situations of crimes against humanity will increasingly see relevant conduct in cyberspace taking place alongside physical or kinetic conduct.

---

[69] *See e.g.* *Prosecutor v. Ongwen*, Trial Judgment, ICC-02/04-01/15-1762-Red, 4 February 2021 ("*Ongwen* Trial Judgment"), para. 2677.

[70] *See also* Council of Advisers' Report, pp. 56-60.

[71] *See also* Council of Advisers' Report, pp. 53-56, 60-63.

[72] *See e.g.* *Ongwen* Trial Judgment, para. 2678.

[73] *See* Council of Advisers' Report, pp. 65-70.

72. Article 7(1)(a) of the Statute criminalises murder. This includes the intentional causing of death through indirect but sufficiently proximate means. For example, a person may commit murder by cyber means by hacking power plants or grids, water supply or hospitals, with this conduct amounting to a sufficiently proximate cause of death, and the perpetrator either intending to kill or being aware that death would occur in the ordinary course of events.

73. Article 7(1)(b) of the Statute criminalises extermination, which is simply mass killing. Extermination can be committed "by different methods of killing, either directly or indirectly,"[74] and includes "the intentional infliction of conditions of life, *inter alia*, the deprivation of access to food and medicine, calculated to bring about the destruction of part of a population."[75] It thus differs from the crime of murder by its 'mass' context. Large-scale killing perpetrated by cyber means, such as the hacking of airplane navigation systems or air traffic control, which results in plane crashes and many victims, could count as extermination.

74. Article 7(1)(c) of the Statute criminalises enslavement, which entails the exercise by the perpetrator of any or all of the powers attaching to the right of ownership over a person,[76] including "in the course of trafficking in persons, in particular women and children."[77] Notwithstanding the clear legal prohibition of this conduct, "odious slavery crimes continue to be committed in various ways today" including by "transnational trafficking in persons"—which may in particular target "individuals from economically depressed geographies who are reduced to sexualised commodities" and "minority group members disproportionately imprisoned and forced to labour in detention".[78] The relationship between enslavement and the use of cyberspace may be complex. On the one hand, persons may potentially be enslaved in order to exploit their labour in support of (legitimate or illegitimate) commercial activity carried out online.[79] On the other hand, cyberspace may be used as a means to facilitate activities relevant to enslavement, including trafficking in persons,[80] forced marriage, sexual slavery, and other forms of unlawful exploitation.[81]

---

[74] Elements of Crimes, art. 7(1)(b), Element 1, n. 8.

[75] Rome Statute, art. 7(2)(b).

[76] Elements of Crimes, art. 7(1)(c), Element 1.

[77] Rome Statute, art. 7(2)(c).

[78] *See e.g.* ICC OTP, *Policy on Slavery Crimes* (2024), Preface, and paras. 1, 6, 25-26, 55, 58, 61.

[79] *See e.g. Report of the Special Rapporteur on contemporary forms of slavery, including its causes and consequences*, UN Doc. A/78/161, 12 July 2023, para. 7. *See also* ICC OTP, *Policy on Slavery Crimes* (2024), para. 47.

[80] On the relationship between human trafficking and enslavement, *see further* ICC OTP, *Policy on Slavery Crimes* (2024), paras. 55-59.

[81] *See e.g. Report of the Special Rapporteur on contemporary forms of slavery, including its causes and consequences*, UN Doc. A/78/161, 12 July 2023, paras. 3-8.

75. Article 7(1)(f) prohibits torture, which is defined relevantly in this context as the infliction of severe physical or mental pain or suffering upon a person in the custody or control of the perpetrator.[82] Relatedly, article 7(1)(k) of the Statute criminalises "[o]ther inhumane acts of a similar character" to the acts expressly set out in article 7(1), and which "intentionally caus[e] great suffering, or serious injury to body or to mental or physical health." The provision is a residual clause intended to capture conduct that is similar in *nature* and *gravity* to the other crimes listed in article 7(1), but does not fall within their particular elements.[83]

76. Reading articles 7(1)(f) and (k) in combination, it is clear that intentional conduct in cyberspace causing serious harm to mental health may amount to a crime against humanity, irrespective whether the victim is under the perpetrator's control (such as a detainee) or in the population at large. Various forms of conduct—including through the creation, appropriation, or dissemination of certain content sufficiently affecting core interests of victims under international law (such as imagery showing the commission of serious crimes)[84]—may potentially meet the required threshold, which will be assessed on a case-by-case basis. Among other relevant considerations, the Office will take into account: the duration, intensity, and context of the relevant conduct, including any repetition; the potential traumatic effects associated with any exercise of control over the victim through the relevant conduct, and; the degree to which the relevant conduct forms part of an overall environment of coercion affecting the victim, including by linked conduct such as surveillance, 'doxxing',[85] and so on.

77. Article 7(1)(h) of the Statute criminalises "[p]ersecution against any identifiable group or collectivity" on political, racial, national, ethnic, cultural, religious, gender, or other impermissible grounds, and in connection with any

[82] Torture as a crime against humanity and torture as a war crime have some "notable differences" in their elements: *see e.g.* *Prosecutor v. Yekatom and Ngaïssona*, Trial Judgment, ICC-01/14-01/18-2784-Red, 24 July 2025 ("*Yekatom and Ngaïssona* Trial Judgment"), paras. 3817-3820.

[83] *See* *Yekatom and Ngaïssona* Trial Judgment, paras. 3825-3828.

[84] *See also* Council of Advisers' Report, pp. 65-66, 68; S. Zarmsky, 'Is international criminal law ready to accommodate online harm: challenges and opportunities,' [2024] 22 *Journal of International Criminal Justice* 169, pp. 176-180; Cyber Law Toolkit, "Scenario 31: Sharing degrading content". *See also below* para. 95 (concerning outrages upon personal dignity as a war crime).

[85] In other words, publishing online private or identifying information about another person, without their consent, and typically with malicious intent.

act referred to in this paragraph or any crime within the jurisdiction of the Court.[86] Within this context, the core conduct element of persecution is "the intentional and severe deprivation of fundamental rights contrary to international law by reason of the identity of the group or collectivity."[87] This can occur either by means of committing one or more of the other article 7(1) acts with the necessary discriminatory intent,[88] or by means of otherwise depriving one or more individuals of fundamental rights (with the minimum level of severity required) and with the necessary discriminatory intent.[89]

78. Conduct in cyberspace may be used to seriously deprive persons or groups of various fundamental rights, including but not limited to the right to life, the right to physical and mental health, the right to adequate food and water, the right to freedom of expression, the right to privacy and family life, and the right to participate in public affairs.[90] For example, a particular ethnic or religious group may be subjected to a campaign of persecution, which may be facilitated or even partly constituted by the use of various intrusive surveillance techniques (including biometric and AI-enabled surveillance).[91] Likewise, the creation and sharing of certain content online—including by social media—may also be relevant in establishing that the alleged perpetrator acted with the necessary discriminatory intent, or in certain circumstances itself amount to conduct which severely violates the rights of others (for example, if the content causes serious harm to a person's mental health, such as imagery showing the commission of serious crimes).[92] Members of the targeted group could potentially be severely deprived of their freedom of expression by means, *inter alia*, of preventing their access, over a sustained period, to communication technologies such as the internet.

---

[86] The prohibited grounds forming the persecutory intent may be single or multiple and intersecting: *see e.g.* ICC OTP *Policy on the Crime of Gender Persecution* (2022), para. 55. The 'connected crimes' requirement entails only that the alleged persecution as a whole is linked, as a matter of fact, with at least one article 7(1) act or crime under the Statute: *see e.g. Prosecutor v. Al Hassan*, Trial Judgment, ICC-01/12-01/18-2594-Red, 26 June 2024 ("Al Hassan Trial Judgment"), paras. 1208-1211; ICC OTP *Policy on the Crime of Gender Persecution* (2022), paras. 56-58.

[87] Rome Statute, art. 7(2)(g).

[88] *See e.g. Al Hassan* Trial Judgment, paras. 1202, 1204. Somewhat similar to persecution, the crime of apartheid under article 7(1)(j), can also be committed by means of carrying out "inhumane acts of a character similar to those" in article 7(1), within the context of an institutionalized regime of systematic oppression and domination by one racial group over any other racial group or groups, with the intention of maintaining that regime: Rome Statute, art. 7(2)(h).

[89] *See e.g. Al Hassan* Trial Judgment, paras. 1202-1203, 1205.

[90] *See also e.g. Al Hassan* Trial Judgment, para. 1201 (referring, non-exhaustively, to various fundamental rights which may be relevant to establishing the crime of persecution).

[91] *See also* Council of Advisers' Report, pp. 66-68.

[92] *See above* para. 76.

War crimes

79. The centrality of information and communication technologies to modern life is also evident in armed conflict. In this context, the civilian population may not only suffer serious incidental harms from disruption of such technologies in the course of combat operations, but may also be specifically targeted by means of such technologies—often mediated through cyberspace. This includes the intentional use of cyber operations to cause various kinds of actual harm to the civilian population (including by disabling or impeding the provision of essential services). It also includes the intentional use of cyberspace more generally to conduct or facilitate information operations which endanger the civilian population or other protected persons, or cause serious mental harms or outrages upon personal dignity.[93] Such cyber conduct may not only violate IHL, but also incur individual criminal responsibility as a potential war crime.

CONTEXTUAL ELEMENTS

80. War crimes can only be committed in the context of an armed conflict. In the view of the Office, an armed conflict can, in principle, commence and be fought exclusively by cyber means.[94] Whether an international armed conflict (IAC) commences by cyber means depends on whether the cyber operation amounted to a use of 'armed force' by one State against another.[95] For a non-international armed conflict (NIAC), the test may be more demanding since the cyber operation(s) amounting to the hostilities between the parties (that is, between a State and an organised armed group, or between such groups) would need to meet a certain threshold of intensity.[96] In practice, since both IACs and NIACs are more likely to be fought using a combination of kinetic and cyber means, establishing the existence of a relevant conflict may be unlikely in the near term to turn simply on conduct in cyberspace. Cyber means may also frequently be used in the context of a pre-existing armed conflict whose constitutive requirements are established purely kinetically.

---

[93] *See also* ICRC *Challenges* Report (2024), p. 57.

[94] *See also* *Tallinn Manual 2.0*, pp. 375-391; Council of Advisers' Report, pp. 30-36.

[95] *See e.g.* ICC OTP, *Situation in the Republic of Korea: Article 5 Report* (June 2014), paras. 44-45; ICRC, *How is the term 'Armed Conflict' defined in international humanitarian law* (2024), pp. 9-10. Considering this framework specifically with regard to cyber operations, *see e.g.* *Convention (III) relative to the Treatment of Prisoners of War: Commentary of 2020*, art. 2, paras. 286-289; AU Common Position, paras. 39-40; EU Common Understanding, Annex, p. 6. *See also below* para. 99.

[96] Rome Statute, art. 8(2)(c), (f). *See further e.g.* *Yekatom and Ngaïssona* Trial Judgment, para. 3766; *Al Hassan* Trial Judgment, para. 1097; *Ongwen* Trial Judgment, para. 2684; *Prosecutor v. Ntaganda*, Trial Judgment, ICC-01/04-02/06-2359, 8 July 2019 ("*Ntaganda* Trial Judgment"), para. 716; *Prosecutor v. Katanga*, Trial Judgment, ICC-01/04-01/07-3436-tENG, 7 March 2014 ("*Katanga* Trial Judgment"), para. 1187.

81. Conduct in cyberspace that satisfies the elements of offences defined in article 8(2) of the Statute may be charged as a war crime as long as the act "took place in the context of and was associated with" an armed conflict, whether international or non-international.[97] For example, it may suffice that the conflict "played a substantial part in the perpetrator's ability to commit the crime, the decision to commit it, the purpose of the commission, or the manner in which the crime was committed."[98] Provided this 'nexus' test is met, any person may be the perpetrator of a cyber-enabled war crime, irrespective of whether they act on behalf of a party to the armed conflict. Likewise, if the nexus test is met, the relevant conduct of the perpetrator need not necessarily take place in geographic proximity to the combat area, even extending in certain circumstances to the territory of other States where the Court has a legal basis to exercise jurisdiction.[99] There is no requirement that the perpetrator intended the act in question to further the armed conflict; there is only a requirement for the awareness of the factual circumstances that established the existence of an armed conflict.

EXAMPLES OF UNDERLYING CRIMES

82. War crimes under the Statute may be committed by cyber means. As noted above, the examples given are illustrative, and failing to mention a particular war crime does not preclude the possibility of its commission by cyber means.

83. The applicable underlying rules of IHL, and the applicable war crimes provisions in the Statute, vary depending on the classification of the armed conflict as an IAC or a NIAC (although with significant overlaps). The applicable rules of IHL and corresponding war crimes also broadly divide between those which govern behaviour in combat (often termed as the 'conduct of hostilities') and those which govern behaviour with regard to persons and objects under the control of the perpetrator.[100] In principle, both types of war crimes can be committed by cyber means, provided as always that the nexus requirement is met.[101]

---

[97] Elements of Crimes, art. 8. This requirement is reproduced for each war crime.

[98] *See e.g.* *Situation in Afghanistan*, Judgment on the appeal against the decision on the authorisation of an investigation into the Situation in the Islamic Republic of Afghanistan,' ICC-02/17-138 OA4, 5 March 2020 ("*Afghanistan* Article 15 Appeal Judgment"), para. 69; *Prosecutor v. Ntaganda*, Judgment on the appeal of Mr Ntaganda against the 'Second decision on the Defence's challenge to the jurisdiction of the Court in respect of Counts 6 and 9', ICC-01/04-02/06-1962 OA5, 15 June 2017 ("*Ntaganda* Jurisdiction Appeal Judgment"), para. 68. *See further* ICTY, *Prosecutor v. Kunarac et al.*, Appeal Judgment, IT-96-23 & IT-96-23/1-A, 12 June 2002, paras. 57-60.

[99] *See e.g.* *Afghanistan* Article 15 Appeal Judgment, paras. 73-77 (in the context of a NIAC).

[100] Certain war crimes, however, may apply equally in both contexts, consistent with the established framework of international law.

[101] *See above* para. 81.

84. Several war crimes relating to the conduct of hostilities require the existence of an 'attack' as defined in IHL.[102] These include:

- articles 8(2)(b)(i) and 8(2)(e)(i) (intentionally directing attacks against the civilian population as such or against individual civilians);
- article 8(2)(b)(ii) (intentionally directing attacks in IAC against civilian objects);
- article 8(2)(b)(iv) (intentionally launching an attack in IAC knowing that it will cause incidental harm to civilians or widespread, long-term and severe damage to the natural environment that is clearly excessive in relation to the concrete and direct overall military advantage anticipated);
- articles 8(2)(b)(iii) and 8(2)(e)(iii) (intentionally directing attacks against humanitarian assistance or peacekeeping missions); and
- articles 8(2)(b)(xxiv) and 8(2)(e)(ii) (intentionally directing attacks against objects or persons lawfully using the distinctive emblems of the Geneva Conventions).

85. Likewise, while articles 8(2)(b)(ix) and 8(2)(e)(iv) (intentionally directing attacks against other specially protected objects such as buildings dedicated to religion, education, art, science or charitable purposes, historic monuments, and hospitals) certainly prohibit such 'attacks', they may also prohibit acts of violence even to objects under the control of the relevant party, to the extent such conduct falls within the scope of the underlying prohibitions in IHL.[103]

---

[102] *See e.g.* *Yekatom and Ngaïssona* Trial Judgment, para. 3788; *Ongwen* Trial Judgment, para. 2758; *Ntaganda* Trial Judgment, para. 916; *Katanga* Trial Judgment, para. 798. *See further* Rome Statute, arts. 8(2)(b), 8(2)(e), 21(1)(b); *Ntaganda* Jurisdiction Appeal Judgment, paras. 52-53; Protocol Additional to the Geneva Conventions of 19 August 1949, and relating to the Protection of Victims of International Armed Conflicts ("Additional Protocol I"), art. 49(1); *Protocol Additional to the Geneva Conventions of 19 August 1949, and relating to the Protection of Victims of International Armed Conflicts: Commentary of 1987*, art. 49(1), para. 1880.

[103] In this respect, the "jurisprudence of the Court is not settled": *Yekatom and Ngaïssona* Trial Judgment, paras. 3812-3814. For authority that article 8(2)(e)(iv) prohibits violent acts against at least some types of specially protected objects not only in the conduct of hostilities but also when they have fallen under the control of the party carrying out the relevant act: *compare e.g.* *Prosecutor v. Al Mahdi*, Judgment and Sentence, ICC-01/12-01/15-171, 27 September 2016, para. 15, *with* *Ntaganda* Trial Judgment, paras. 1136 (fn. 3147: endorsing the principle in *Al Mahdi* with regard to certain types of cultural objects only), 1142 (not following the principle in *Al Mahdi* with regard to religious buildings). For a range of views on this issue, but reaching "no consensus" (*Yekatom and Ngaïssona* Trial Judgment, para. 3813), *see* *Prosecutor v. Ntaganda*, Appeal Judgment, ICC-01/04-02/06-2666-Red A A2, 30 March 2021, paras. 1163-1169. *Cf.* *Al Hassan* Trial Judgment, para. 1099 (fn. 3770: suggesting that the conduct in article 8(2)(e)(i) to (iv) must "take place as part of hostilities"), *but see* para. 1181 (considering it unnecessary to set out the legal requirements of article 8(2)(e)(iv)). In any event, the actual destruction of objects under the control of the relevant party falls within the general prohibitions of destruction in articles 8(2)(b)(xiii) and 8(2)(e)(xii): *see below* para. 92.

86. In the view of the Office, cyber operations can qualify as an 'attack' for all of the above purposes.[104] This is certainly the case for those cyber operations whose (actual or potential) direct and indirect effects include death or injury to persons, such as cyber operations against hospitals or other medical facilities. If civilians or the civilian population were the "*primary* object" of such attacks,[105] with the requisite *mens rea*, the requirements of the war crime of intentionally directing attacks against civilians would be met. The Office likewise considers that cyber operations whose (actual or potential) direct and indirect effects include physical damage to civilian objects qualify as an 'attack' for the purpose of article 8(2)(b)(ii) (intentionally directing attacks against civilian objects).

87. The Office also recalls that "indiscriminate attacks […] may qualify as intentional attacks against the civilian population or individual civilians, especially where the damage caused to civilians is so great that it appears […] that the perpetrator meant to target civilian[s]" alongside military objectives, rather than as a mere incidental harm.[106] Similar reasoning may apply with regard to civilian objects. In this regard, one relevant consideration may be evidence of the "[u]se of weaponry that has indiscriminate effects" within the context of the relevant circumstances.[107] Accordingly, the Office considers that certain attacks carried out by cyber means may be indiscriminate, and takes the position that such attacks may amount to intentional attacks directed against the civilian population, individual civilians, or (where applicable) civilian objects. One example might be the intentional use of destructive malware that can automatically self-replicate and proliferate (such as a worm), and which is capable of causing the requisite degree of harm through its effects on a wide variety of military and civilian computer systems, without discrimination.[108]

---

[104] See *Tallinn Manual 2.0*, pp. 415-420; Council of Advisers' Report, pp. 37-39. *See also* AU Common Position, paras. 50-52; EU Common Understanding, Annex, p. 7; Cyber Law Toolkit, summary of national positions on "attack (international humanitarian law)".

[105] *See e.g.* *Yekatom and Ngaïssona* Trial Judgment, para. 3790 (emphasis supplied); *Ongwen* Trial Judgment, para. 2760; *Katanga* Trial Judgment, para. 802.

[106] *Katanga* Trial Judgment, para. 802. *See also* *Ntaganda* Trial Judgment, para. 921. *See further* *Yekatom and Ngaïssona* Trial Judgment, para. 3790; *Ongwen* Trial Judgment, para. 2760 ("Depending on the circumstances, the civilian population can still qualify as the primary object of an attack in a situation where everyone is targeted at a mixed military-civilian position"). Circumstances where civilians or the civilian population are incidentally harmed in the course of an attack on a military objective may fall under article 8(2)(b)(iv) of the Statute: *see also below* para. 89.

[107] *See* *Ntaganda* Trial Judgment, para. 921; *Katanga* Trial Judgment, para. 802.

[108] The Office takes this position notwithstanding the separate issue that States have not yet acted to schedule any specific weapon or method of warfare which they consider to be of a nature to cause superfluous injury or unnecessary suffering or which are inherently indiscriminate, and which are the subject of a comprehensive prohibition, as anticipated in article 8(2)(b)(xx) of the Statute. *See further* Council of Advisers' Report, p. 43.

88. There continues to be much contemporary discussion, both in and outside the cyber context, about the appropriate assessment of attacks on objects which, even if they may qualify as a military objective,[109] also continue to serve an important civilian use—sometimes described in a non-technical sense as 'dual use' objects.[110] This is especially challenging with regard to complex objects in which distinct components comprise an integral whole, such as a tower block containing multiple apartments, or a computer network, a cloud platform or other cyber infrastructure.[111] In the view of the Office, the proper assessment of attacks on such complex objects will be highly fact-sensitive, including being informed by evidence of compliance or otherwise with other relevant rules of IHL.[112] However, it is clear that attacks (whether committed by cyber means or otherwise) that treat *as a single target* civilian infrastructure *and* objects which qualify as a military objective may amount to the war crime of intentionally directing attacks against civilian objects, at least in circumstances when it is technically possible to isolate and target only the military objective and the perpetrator intentionally declined to do so.[113]

89. Likewise, the IHL rule on proportionality may also be particularly relevant in such contexts—and it is a war crime at least under article 8(2)(b)(iv) of the Statute (applicable in IACs) to intentionally launch an attack in the knowledge that it will cause injury or damage which would be "clearly excessive in relation to the concrete and direct overall military advantage anticipated". In this context, the collateral harms to be assessed by the person launching the attack are not necessarily limited to direct harms and may encompass harms which were sufficiently foreseeable in the circumstances.[114] In the particular context of cyber operations, the networked nature of computer systems and their integration into civilian life may be taken into account alongside other relevant circumstances in assessing the foreseeability of cascading harmful effects on the civilian population and civilian objects.

---

[109] *See* Additional Protocol I, art. 52(2) (referring to "objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or netrualization, in the circumstances ruling at the time, offers a definite military advantage").

[110] This is not a discrete category in IHL, however, since civilian objects are defined negatively as "all objects which are not military objectives": Additional Protocol I, art. 52(1).

[111] *See further e.g.* Council of Advisers' Report, pp. 41-42; ICRC, *Cyber Operations during Armed Conflict: the Principle of Distinction* (2023), pp. 1-2; C. Droege, 'Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians,' Vol. 94, No. 886, *International Review of the Red Cross* (Summer 2012) 533, pp. 562-566; M.N. Schmitt, 'Targeting dual-use structures: an alternative interpretation,' *Articles of War*, 28 June 2021.

[112] *See e.g.* Additional Protocol I, arts. 52(3), 57(1), 57(3).

[113] *See Tallinn Manual 2.0*, p. 470; Council of Advisers' Report, pp. 43-44.

[114] *See e.g.* Council of Advisers' Report, pp. 44-46; ICRC, *International Humanitarian Law and Cyber Operations During Armed Conflicts* (2019), p. 7; L. Gisel (ed.), *The Principle of Proportionality in the Rules Governing the Conduct of Hostilities under International Humanitarian Law* (2018), p. 45.

90. There is some debate as to whether cyber operations that only cause loss of functionality to computer systems can qualify as 'attacks.'[115] In the view of the Office, if a loss of functionality led, or could have led, to death, injury or damage, the situation would be no different than in the scenarios above. It is only when losses of functionality do not cause, or are incapable of causing, such harms that the qualification question arises. The Office does not, at this time, need to take a further position, although it will continue to monitor and evaluate the evolving practice and positions of States on this matter.[116]

91. The same goes for the related question of whether data alone can qualify as an object. By way of example, the issue is whether cyber operations that, say, delete the database of the recipients of state pensions or other social benefits in a State, qualify as an attack against a civilian object. Views on this question differ.[117] Again, this is not a matter on which the Office presently regards it as necessary to take a position. The Office is mindful of the evolving practice and positions of States, which it will monitor and evaluate carefully. However, it is clear that if cyber operations are designed to delete data, and that deletion leads, or could have led, to death or injury—for example, a power plant is unable to function because indispensable data on its systems was deleted, and this then leads to a prolonged disruption in power supply that causes the death of civilians—the Office could potentially charge this act as the war crime of intentionally directing attacks against civilians or the civilian population. Likewise, if such a cyber operation deletes data that leads, or could have led, to damage of a civilian object, the Office could potentially charge this as the war crime of intentionally directing attacks against civilian objects.

92. Articles 8(2)(b)(xiii) and 8(2)(e)(xii) of the Statute prohibit destroying or seizing the enemy's (or adversary's) property unless such destruction or seizure be imperatively demanded by the necessities of war. In the view of the Office, an act of destruction or seizure can be committed by cyber means. Similarly, it is also possible for digital assets, including data, to qualify as 'property' within the meaning of these rules.[118]

---

[115] *See* *Tallinn Manual 2.0*, pp. 417-418. *See also* ICRC *Challenges* Report (2024), pp. 57 (expressing the view that "interpretations of IHL that focus on the protection of civilian objects only against physical damage are […] inadequate"), 58.

[116] *See* Cyber Law Toolkit, summary of national positions on "attack (international humanitarian law)". *See also* Council of Advisers' Report, p. 38.

[117] *See* *Tallinn Manual 2.0*, pp. 436-437; Council of Advisers' Report, p. 39.

[118] *See e.g.* *Convention (IV) relative to the Protection of Civilian Persons in Time of War: Commentary of 2025*, art. 53, para. 3362; *Convention (IV) relative to the Protection of Civilian Persons in Time of War: Commentary of 2025*, art. 147, para. 6784.

93. Article 8(2)(b)(xxv) of the Statute criminalises in IACs "[i]ntentionally using starvation of civilians as a method of warfare by depriving them of objects indispensable to their survival, including wilfully impeding relief supplies as provided for under the Geneva Conventions." Article 8(2)(e)(xix) of the Statute criminalises the same acts in NIACs, pursuant to an amendment adopted in 2019.[119] Objects indispensable to survival include "foodstuffs, agricultural areas for the production of foodstuffs, crops, livestock, drinking water installations and supplies and irrigation works."[120] Cyber operations intended to disrupt the production or supply of such objects, or those targeting relief supplies to the civilian population, may thus qualify as the war crime of starvation.[121] Importantly, there is no requirement that the deprivation actually results in starvation; the intent to starve as a method of warfare is sufficient for criminal responsibility, if coupled with conduct which actually deprives civilians of objects indispensable to survival.

94. War crimes can also be committed by cyber means beyond the immediate conduct of hostilities, but with regard to persons and objects under the control of the perpetrator, where there is a sufficient nexus to the conflict.[122] Some of these offences directly cause harm to protected persons; others create an unacceptable risk of harm to such persons ('endangerment' offences).

95. Notably, the war crime in articles 8(2)(b)(xxi) and 8(2)(c)(ii) prohibits the commission of outrages upon personal dignity, in particular humiliating and degrading treatment. This includes the production and publication of humiliating images of persons in captivity, or deceased persons, which can be carried out online and exploit existing platforms and channels such as popular social media. While mindful of the importance of free expression, and the public interest in fair and accurate journalistic reporting (especially in circumstances of armed conflict),[123] the Office considers that these interests will rarely conflict in practice with the conduct which amounts to an outrage upon personal dignity. Typical examples may include graphic depictions of criminal conduct, especially violence

[119] The amendment was adopted pursuant to article 121(5) of the Rome Statute. To date, it has been ratified by 23 States.

[120] *See* Additional Protocol I, art. 54; *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts* ("Additional Protocol II"), art. 14.

[121] *See* ICRC *Challenges* Report (2024), p. 46. *See further* pp. 45, 47-48. *See also* AU Common Position, para. 52; Cyber Law Toolkit, summary of national positions on "Specially protected persons, objects, and activities (international humanitarian law)".

[122] *See above* paras. 81, 83.

[123] *See also below* paras. 118-122.

to the person, including gender based crimes.[124] The production and publication of such images not only reflects a further dimension of the victimisation of the person depicted, but also frequently serves or is intended to serve the interests of the perpetrator, including potentially calling for or encouraging the commission of further crimes and thereby endangering others.

96. Likewise, it is a war crime in articles 8(2)(b)(xii) and 8(2)(e)(x) to declare that "no quarter will be given"—in other words, for a person "in a position of effective command or control" over relevant subordinate forces to declare or order that there shall be no survivors as a consequence of those forces' combat operations, or in order to threaten an adversary.[125] It is immaterial that such a declaration is made publicly. Accordingly, statements to this effect made in social media, or otherwise transmitted or disseminated via the intent, could potentially qualify in appropriate circumstances. Similar logic could apply where a person in control of detained persons held hostage makes public threats to kill, injure, or continue to detain them, with the intent to compel a third party to undertake an act or to refrain from an act, amounting to the war crime in articles 8(2)(a)(viii) and 8(2)(c)(iii).[126]

Aggression

97. Article 8*bis* of the Rome Statute, concerning the crime of aggression, builds *inter alia* on the definition of aggression adopted by the UN General Assembly in 1974.[127] The amendment to the Statute introducing this provision was activated in 2018. However, given the particular jurisdictional limitations pertaining to this crime,[128] it has not yet been subject to the Court's exercise of jurisdiction in any situation. Accordingly, for the purpose of the present Policy, the Office will only provide limited comment on the crime's requirements. This should not be misinterpreted, however, as diminishing the importance of this crime or the Office's commitment to its investigation and prosecution in appropriate circumstances.

---

[124] *See also above* para. 76. In the *Sneidel* case, in an arrest warrant issued in 2020 but recently unsealed by the Court, the Pre-Trial Chamber found reasonable grounds to believe that the suspect was responsible, *inter alia*, for the war crime of outrages upon personal dignity based on his participation in executions which appeared to be "exceptionally cruel, humiliating, dehumanising and degrading", and which "were all filmed and the videos posted on social media" as well as "photographs [having been] taken with the corpse of one […] victim": *Prosecutor v. Sneidel*, Warrant of Arrest, ICC-01/11-01/20-26-Anx-Red, 10 November 2020 (public redacted version 8 August 2025), para. 13.

[125] *See e.g.* Elements of Crimes, art. 8(2)(b)(xii), Elements 1-3; art. 8(2)(e)(x), Elements 1-3.

[126] *See e.g.* Elements of Crimes, art. 8(2)(a)(viii), Elements 1-3; art. 8(2)(c)(iii), Elements 1-3.

[127] *See* UNGA Res. 3314 (XXIX).

[128] *See* Rome Statute, arts. 15*bis*, 15*ter*. To date, 49 States Parties to the Rome Statute have ratified the amendment accepting the Court's jurisdiction over the crime of aggression.

98. Article 8*bis*(1) of the Statute criminalises aggression, defined as "the planning, preparation, initiation or execution, by a person in a position effectively to exercise control over or to direct the political or military action of a State, of an act of aggression which, by its character, gravity and scale, constitutes a manifest violation of the Charter of the United Nations." An act of aggression is defined by article 8*bis*(2) as "the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations." Examples of such acts listed in article 8*bis*(2) include invasion, military occupation, bombardment, and attack by the armed forces of one State against the armed forces of another.

99. In the view of the Office, a cyber operation can qualify as a use of force prohibited by article 2(4) of the Charter and as an act of aggression.[129] It is not the technological means used, but the effects produced, that matter for establishing whether certain conduct constitutes a use of force. This may be the case if the operators of one State launch cyber operations against the armed forces of another State, for example by hacking the navigational systems of aircraft or naval vessels, thereby causing death, injury or physical damage. It may be less straightforward if the alleged cyber use of force does not cause such consequences. However, the Office is mindful of the potentially evolving practice and positions of States on these issues, which it will carefully monitor and consider. This includes the question whether a concerted series of cyber operations, none of which would individually qualify as a prohibited use of force, could nonetheless pass this threshold when considered cumulatively.[130]

100. Whether an act of aggression constitutes "a manifest violation of the Charter of the United Nations" is determined by its "character, gravity, and scale."[131] In assessing those factors, the Office will take into account, *inter alia*, the physical damage caused by the aggressive act, including damage to the natural environment, and the number and kind of the act's victims. While it is possible for the crime of aggression to be committed by cyber means alone, as a practical matter it presently may be more likely that cyber operations will be used by the aggressor State as part of a wider course of conduct, also including acts entailing physical or kinetic force. The Office would holistically address the character, gravity and scale of all elements of a campaign of aggression, and would not examine conduct in cyberspace in isolation.

---

[129] *See* *Tallinn Manual 2.0*, pp. 330-337; Council of Advisers' Report, pp. 9-18.

[130] *See e.g.* Council of Advisers' Report, p. 15.

[131] Rome Statute, art. 8*bis*(1).

101. The crime of aggression differs from other crimes in the Statute in that it is a leadership crime, and that the political or military leader in question must be able to control or direct State action. However, any questions posed by the leadership requirement are not unique to the cyber context.

102. Similarly, the requirement that force is used between States is also resolved on similar principles both for kinetic and cyber operations. For example, relevant cyber conduct of a non-State actor targeting a State, such as a hacking group, may constitute a use of force between States if the conduct of the non-State actor was attributable to another State, in accordance with applicable rules of international law. In other words, an act of aggression, by cyber means or otherwise, can potentially be committed through the use of a non-State actor acting as a proxy on behalf of a State. In any event, such a requirement is cumulative to the required showing that the suspect—who must be in a position of leadership of a State[132]—"planned, prepared, initiated or executed" the relevant act of aggression carried out by the non-State actor, with the required intent and knowledge.[133]

Offences against the administration of justice

103. Finally, in addition to the core international crimes of genocide, crimes against humanity, war crimes, and aggression, the Court also exercises jurisdiction over offences against the administration of justice affecting its own proceedings. The Office has previously demonstrated that, where necessary, it will investigate, prosecute, and obtain convictions of those responsible for such conduct.[134]

104. The malicious use of cyber operations against the Court are more than a mere theoretical possibility. It is a real and present danger, and the Court has already been subjected to such activity. For example, in September 2023, the Court detected a "serious cyber security incident," which was publicly described as a "targeted and sophisticated attack with the objective of espionage." The Registrar of the Court expressed the view that this could "therefore be interpreted as a serious attempt to undermine the Court's mandate," and noted that the Dutch authorities had opened a criminal investigation.[135] Likewise, on 30 June 2025,

---

[132] *See above* para. 101.

[133] *See* Elements of Crimes, art. 8*bis*, Element 1; Rome Statute, art. 30.

[134] *See e.g.* *Bemba et al.* Appeal Judgment. *See also e.g.* *Prosecutor v. Barasa*, Warrant of Arrest, ICC-01/09-01/13-1-Red2, 2 August 2013 (redacted version 2 October 2013); *Prosecutor v. Bett*, Warrant of Arrest, ICC-01/09-01/15-1-Red, 10 March 2015 (redacted version 10 September 2015); *Prosecutor v. Gicheru*, Decision terminating the proceedings against Paul Gicheru, ICC-01/09-01/20-337, 14 October 2022.

[135] *See e.g.* ICC, 'Measures taken following the unprecedented cyber-attack on the ICC,' 20 October 2023.

the Court announced that it had detected and contained "a new, sophisticated and targeted cyber security incident".[136] Accordingly, the Office will rigorously investigate and prosecute attempts to undermine the Court's mission, by cyber means or otherwise, where they amount to offences against the administration of justice.

105. Article 70(1) of the Statute provides for six different offences against the administration of justice at the Court:

> (a) Giving false testimony when under an obligation pursuant to article 69, paragraph 1, to tell the truth;
>
> (b) Presenting evidence that the party knows is false or forged;
>
> (c) Corruptly influencing a witness, obstructing or interfering with the attendance or testimony of a witness, retaliating against a witness for giving testimony or destroying, tampering with or interfering with the collection of evidence;
>
> (d) Impeding, intimidating or corruptly influencing an official of the Court for the purpose of forcing or persuading the official not to perform, or to perform improperly, his or her duties;
>
> (e) Retaliating against an official of the Court on account of duties performed by that or another official;
>
> (f) Soliciting or accepting a bribe as an official of the Court in connection with his or her official duties.

106. As a general matter, in the view of the Office, all of these offences can be committed by cyber means. For example, a person can give false testimony online, such as by video link when they have made a solemn affirmation that they will tell the truth. Likewise, a party to the Court's proceedings can appear before a Chamber online, and by that means present evidence that is false or forged. A person can also falsify or forge the relevant evidence by using cyber tools, and thus at least facilitate the commission of this offence and potentially be a co-perpetrator—for example, by manipulating a video with the intent and knowledge that it will be presented to the Court as evidence.

107. Witness interference under article 70(1)(c) can be committed by cyber means in multiple ways—a witness can be intimidated or retaliated against by means such as circulating death threats against them on social media, or by disseminating an AI-generated deep fake video harmful to their reputation. Evidence may be tampered or interfered with by, for instance, altering or deleting digital records. Similarly, an official of the Court may be subjected to blackmail,

[136] *See e.g.* ICC, 'ICC detects and contains new sophisticated cyber security incident,' 30 June 2025.

intimidation, or retaliation through the use of social media, the digital fabrication of evidence of their supposed wrongdoing, or the dissemination or threatened dissemination of reputationally harmful 'deepfakes'. The solicitation or acceptance of a bribe, as well as the transfer of any funds, can all be done by cyber means—for instance, through the use of encrypted messaging apps or cryptocurrencies.

108. The Office underlines that conduct relevant to these offences may occur not only at the seat of the Court in the Netherlands, but also in various locations relevant to the situations and cases under the Court's jurisdiction.[137] Likewise, such conduct may be criminal not only when trial proceedings at the Court are underway, but also before such proceedings commence or after they have been completed. In addressing such conduct, the Office will seek to work in coordination with relevant States Parties to the Statute.[138] It will at all times remain mindful that mere expressions of disagreement with the Court or its officials, or its work, do not amount to crimes whether done online or offline, but rather fall within the right of free expression which is to be respected.[139]

[137] *See* Rome Statute, art. 70(2); ICC RPE, rule 162.

[138] *See further below* paras. 172-174.

[139] *See further below* paras. 118-122.

FACILITATING ROME STATUTE CRIMES BY CYBER MEANS

109. Under the Statute, criminal responsibility attaches not only to the commission (perpetration) of the crimes within the jurisdiction of the Court, but also to other forms of participation. For the sake of convenience, this Policy will use the term 'facilitation,' in a non-technical sense, to cover the different forms of responsibility set out in articles 25 and 28 of the Statute other than individual or joint perpetration.[140]

110. The Office emphasizes its view that cyber conduct has *already* facilitated the commission of physical or kinetic crimes under the Statute with substantial numbers of victims. The Office is prepared to prosecute cyber accomplices, irrespective of the means by which the principal committed the underlying crime.

111. Under article 25 of the Statute, an individual who is not a perpetrator can be held responsible for ordering, soliciting or inducing a crime; for aiding and abetting, or otherwise assisting a crime; and for contributing to a crime committed by a group of persons acting with a common purpose.[141] Thus, an individual can use cyber means to engage in conduct that could render them responsible on one of the bases above.

112. Notably, an order can be communicated by means of digital communications technology, as can statements that amount to inducing, soliciting, or providing moral encouragement for (abetting) a crime.

113. Likewise, particularly relevant to article 25(3)(c) and (d) of the Statute, a crime within the jurisdiction of the Court—whether physical or cyber in character—can be practically facilitated by a wide variety of cyber means. For example, a military unit engaged in the killing of civilians can be assisted by cyber operators, who use methods of surveillance or cyber intrusion to locate or extract information about intended victims, or who manipulate computer systems to

[140] Accordingly, this is without prejudice to the proper technical characterisation of article 28 (superior responsibility), which as a matter of law does not require the superior to facilitate or participate in the crime(s) of their subordinate(s). *See below* para. 115.

[141] In addition, article 25(3)(f) also provides for criminal responsibility for attempting to commit a crime within the jurisdiction of the Court, although this is an inchoate offence rather than a form of responsibility.

delete records about the victims or otherwise destroy evidence after the fact.[142] It is equally possible for crimes under the Statute which have been committed by cyber means to be facilitated by non-cyber means, such as the provision of money to purchase malware that is later used to commit a crime.

114. There is no requirement that conduct facilitating a crime within the jurisdiction of the Court need be criminal in and of itself, either as a matter of international law or national law.[143] For example, an individual may facilitate such a crime in the course of ordinary commercial activity.[144] What determines and delimits criminal responsibility in such circumstances is the *mens rea* with which a person acts—for example, under article 25(3)(c) of the Statute, they must act "[f]or the purpose of facilitating the commission of such a crime" as that committed by the perpetrator; under article 25(3)(d), they must either act "with the aim of furthering the criminal activity or criminal purpose" of a group or otherwise at least know "of the intention of the group to commit the crime".

115. Under article 28 of the Statute, both civilian and military superiors can bear criminal responsibility for the crimes of their subordinates that they failed to prevent or punish, with the requisite *mens rea*.[145] For civilian superiors (that is, those who are not military or paramilitary in the sense of article 28(1)(a)), this principle is limited to crimes which "concerned activities that were within the effective responsibility and control of the superior"[146]—for example, if the civilian superior is a corporate officer or employer,[147] for activities carried out by their employees in the course of their employment.

116. In the view of the Office, consistent with the principles above, a superior can be responsible for crimes either committed or facilitated by their subordinates using cyber means.[148] Subject to showing the required *mens rea* and effective

[142] An individual may be held responsible for facilitating a crime within the jurisdiction of the Court even after it has been committed, provided that at the time the perpetrator committed the relevant crime they understood that such *ex post facto* assistance would occur: *see e.g.* *Bemba et al.* Appeal Judgment, para. 1399; *Yekatom and Ngaïssona* Trial Judgment, para. 3881.

[143] *See also above* para. 24.

[144] *See also below* paras. 170-171.

[145] *See* Rome Statute, arts. 28(1)(a) (requiring that a military commander or person effectively acting as a military commander "either knew or, owing to the circumstances at the time, should have known" that their subordinates were committing or about to commit relevant crimes), 28(2)(a) (requiring that any other person "either knew, or consciously disregarded information which clearly indicated," that their subordinates were committing or about to commit relevant crimes).

[146] Rome Statute, art. 28(2)(b).

[147] *See also below* paras. 170-171.

[148] *See* *Tallinn Manual 2.0*, pp. 396-400.

control over the relevant subordinates, this principle extends both to superiors with technical and non-technical expertise. For example, the commander of a military cyber unit can be held responsible as a superior for cyber-enabled crimes committed by their subordinates. But so too can the military superior of that commander (who may not be a cyber specialist), as can the civilian leadership who may have ultimate responsibility (such as a head of state or minister of defence).[149] Similarly, as modern command and control systems may become increasingly dependent upon the use of computers and digital communications, the use of such systems may be relevant in establishing superior responsibility even for physical or kinetic crimes.

[149] *See e.g.* ICTY, *Prosecutor v. Strugar*, Trial Judgment, IT-01-42-T, 31 January 2005, paras. 361-366 (concluding that "there is no legal requirement that the superior-subordinate relationship be a direct or immediate one for a superior to be found liable for a crime committed by a subordinate, provided that the former had effective control over the acts of the latter").

PRINCIPLES GUIDING THE WORK OF THE OFFICE

117. The Office's approach to cyber-enabled crimes under the Rome Statute will be informed by the same fundamental principles that apply to all its work. However, those of particular application to the context of cyberspace include the Office's commitments to: acting in accordance with internationally recognised human rights; working consistently; prioritising cases in accordance primarily with their gravity; investigating independently, objectively, and diligently; and cooperating effectively to build partnerships for accountability. This section briefly explains the particular relevance of these principles, and their application to the investigation and prosecution of cyber-enabled crimes within the jurisdiction of the Court.

Conformity with internationally recognised human rights

118. Article 21(3) requires the interpretation and application of the Rome Statute to be "consistent with internationally recognised human rights".[150] Furthermore, article 54(3) requires the Prosecutor to "[f]ully respect the rights of persons" arising under the Statute when carrying out investigations. This naturally includes, but is not limited to, respect for the interests and personal circumstances of victims and witnesses.[151]

119. The Office adheres to these principles and ensures that its investigations are consistent with internationally recognised human rights, within the framework of the Statute. This applies to all investigative activities carried out by the Office, including when seeking the cooperation of a State through the mechanisms in Part 9 of the Statute, but also when entering into other "arrangements or agreements, not inconsistent with [the] Statute, as may be necessary to facilitate the cooperation of a State, intergovernmental organization or person."[152] The Office will thus act consistently with internationally recognised human rights both when participating in joint investigations,[153] and when otherwise deciding

[150] *See also* *Prosecutor v. Lubanga*, Judgment on the Appeal of Mr Thomas Lubanga Dyilo against the Decision on the Defence Challenge to the Jurisdiction of the Court pursuant to article 19(2)(a) of the Statute of 3 October 2006, ICC-01/04-01/06-772 OA4, 14 December 2006, para. 37 ("Human rights underpin the Statute").

[151] Rome Statute, art. 54(1)(b). *See also* art. 68(1).

[152] Rome Statute, art. 54(3)(d).

[153] *See further below* paras. 167-169.

whether to provide assistance to a State investigating conduct which "constitutes a crime within the jurisdiction of the Court or which constitutes a serious crime under […] national law".[154] The Office will also expect partners cooperating with it, including States, international organizations and businesses, to likewise act in conformity with their international obligations.

120. For the purpose of this Policy, it is not necessary to list all of the rights which may be relevant to the work of the Office or the crimes under the Rome Statute. However, given their particular relevance to conduct in cyberspace, it is appropriate to refer briefly to two key rights: privacy[155] and freedom of expression.[156] Focusing on these two rights is, of course, without prejudice to the rights to which suspects or accused before the Court are always entitled under the Statute.[157]

121. Consistent with its established practice, the Office will seek access to private information in accordance with the applicable law,[158] and when necessary in the interest of discharging its statutory mandate to detect and establish the occurrence of crimes within the jurisdiction of the Court, whether cyber-enabled or otherwise, and thereby protect human rights and freedoms.

122. The Office recognises that certain speech acts potentially subject to investigation and prosecution may raise questions about the interplay with the right to freedom of expression. However, as a general matter, acts for which there is individual criminal responsibility under the Rome Statute fall within the recognised qualifications to this right—notably as provisions of law which are necessary to ensure respect for the fundamental rights of others, and to maintain public order.[159] Moreover, to any extent it is necessary and appropriate to apply

---

[154] Rome Statute, art. 93(10). *See further below* paras. 189-190.

[155] *See e.g.* Universal Declaration of Human Rights ("UDHR"), art. 12; International Covenant on Civil and Political Rights ("ICCPR"), art. 17. *See also* UNGA Res. 68/167, Preamble and para. 1; UNGA Res. 69/166, Preamble and para. 1; UNHRC 54/21, Preamble and para. 1.

[156] *See e.g.* UDHR, art. 19; ICCPR, art. 19.

[157] In particular, once a prosecution is initiated before the Court, the Office not only acts consistently with internationally recognised rights but also in light of the rights of the accused: *see* Rome Statute, art. 67. The Office also conducts investigations on an objective basis: *see e.g.* Rome Statute, art. 54(1)(a). *See also below* para. 125.

[158] In the context of Part 9 requests to States Parties, *see e.g.* Rome Statute, arts. 54(2), 88, 93, 96.

[159] *See e.g.* ICCPR, arts. 19-20. *See also* UN Human Rights Committee, *General Comment No. 34 (Article 19: Freedoms of opinion and expression)*, UN Doc. CCPR/C/GC/34, 12 September 2011 ("UN HRCttee General Comment No. 34"), para. 50.

relevant principles of human rights law in the course of exercising its jurisdiction under the Statute, the Court is mandated and equipped to do so.[160]

Consistency

123. In the interests of transparency, accountability, and greater efficiency, the Office has produced (and continues to produce) a wide range of policy papers outlining different facets of its work to further the mandate in the Rome Statute. Policy papers addressing specific types of crime—such as gender-based crimes, crimes against and affecting children, slavery crimes, and crimes associated with environmental damage[161]—reflect the Office's efforts to ensure that its investigations are informed by the best contemporary practice. Such policies also serve to make sure that the Office adopts concrete measures to eliminate factors which may tend to impede the Office in correctly identifying and acting upon the full range of crimes within its jurisdiction, when established on the evidence.

124. It follows from this that the conduct addressed in this policy—cyber-enabled crimes within the jurisdiction of the Court—will be addressed in full conformity with the principles set out in the other thematic policies issued by the Office. Correspondingly, the considerations in this policy will likewise be of potentially general application in ensuring best practice for all crimes within the Court's jurisdiction that have a cyber dimension.

Independence, objectivity and diligence

125. In all cases, the Office seeks to establish the truth, to investigate objectively, and to take appropriate measures to ensure the effective investigation and prosecution of crimes within the jurisdiction of the Court, while fully respecting the rights of persons arising under the Statute.[162]

126. The Office will ensure that it is in a position to recognise and exploit the relevance of conduct in cyberspace in support of its investigations of crimes

---

[160] *See* Rome Statute, arts. 5-8*bis*, 21, 70. *See also e.g.* UN HRCttee General Comment No. 34, paras. 21-35, 38-49; UN HRC, *Report of the United Nations High Commissioner for Human Rights on the expert workshops on the prohibition of incitement to national, racial, or religious hatred*, UN Doc. A/HRC/22/17/Add.4, 11 January 2013, Appendix (Rabat Plan of Action), para. 29.

[161] *See e.g.* ICC OTP *Policy on Gender-Based Crimes* (2023); *Policy on Children* (2023); *Policy on Slavery Crimes* (2024). The Office will also launch its *Policy on Addressing Environmental Damage Through the Rome Statute* in 2025.

[162] Rome Statute, art. 54. *See also above* paras. 118-122.

within the jurisdiction of the Court. It will seek to charge cyber-enabled conduct as a crime under the Statute when appropriate.

127. While the Office will engage with relevant partners as necessary to achieve these aims—including with States, civil society and affected communities, and the private sector—this will always be subject to compliance with its mandate and obligations under the Rome Statute.[163] This will not only shape the nature and extent of the Office's external engagements, but also reflects and underpins the statutory independence of the Prosecutor, Deputy Prosecutor(s), and the staff of the Office.[164]

Gravity, impact, and practicality

128. One premise underlying this Policy is that, at least in the near- to medium-term, cyber-enabled crimes within the jurisdiction of the Court will rarely be committed in isolation. Typically, they will be committed within a broader context of relevant criminality, in which the Office will be required to make choices as to *which* cases to pursue in order to deliver its mandate within the limits of its capabilities.

129. The Office has previously explained how it selects and prioritises cases for investigation and, where appropriate, prosecution.[165] In this regard, one key consideration is the gravity of the alleged conduct, having regard to all the relevant circumstances.[166] Another is the degree of responsibility of the alleged perpetrators, bearing in mind that this does not necessarily equate with *de jure* hierarchical status within a structure but rather is to be assessed on a case-by-case basis depending on the evidence. Other relevant considerations in prioritising cases include the anticipated impact of the Office's action on victims, affected communities, and potential perpetrator groups (for example, disrupting or deterring further crimes), as well as certain issues of practicality.

[163] *See below* paras. 133-135.

[164] *See* Rome Statute, art. 42.

[165] *See* ICC OTP, *Policy on Case Selection and Prioritisation* (2016). It should be noted, however, that the Office is presently reviewing this policy, as well as policies on related procedural matters, as part of its renewed policy framework: *see* ICC OTP, 'Policies and strategies'.

[166] While gravity is conceptualised as a *threshold* for the purpose of admissibility under article 17(1)(d) of the Statute, it may nonetheless be assessed *relatively* by the Office for the purpose of case selection and prioritisation, which has a distinct statutory basis as part of the Prosecutor's independent exercise of investigative discretion under articles 42, 54, and 58 of the Statute.

130. Cyber-enabled crimes under the Statute will be investigated and, where appropriate, prosecuted, according to the same principles. In the near-to-medium-term, conduct in cyberspace may be more frequently relevant to the Office's investigations either to the extent it facilitates kinetic crimes or helps to prove these crimes under the Statute.

131. The Office will assess the gravity of cases concerning cyber-enabled crimes within the jurisdiction of the Court in accordance with the standard criteria used by the Office, including the scale, impact, factual nature, and manner of commission of the relevant criminal acts. While the Office welcomes further engagement with relevant stakeholders in identifying metrics which may be particularly relevant to these criteria in the specific context of cyber operations, relevant considerations may include: the variety and extent of systems affected; the manner in which systems are affected; the geographic spread of systems affected; the temporal duration in which systems are affected; the degree to which affected systems are relevant to services and infrastructure essential to the civilian population; the degree to which affected systems are otherwise relevant to humanitarian services; the degree to which it can be determined that the effects caused were planned and/or premeditated; the technical sophistication of the means and methods used to cause the relevant effects, and, most importantly; the extent of harms actually caused as a result of the relevant effects including death or serious injury to persons and damage to property.

132. The Office will also take account of the potential for some categories of victims to be disproportionately affected by such crimes.[167] However, the mere fact that cyber means have been used, in isolation, will not be taken either to aggravate or mitigate the seriousness of the conduct at issue.

Partnership and vigilance

133. The Office has recently re-emphasised the importance not only of the principle of complementarity but also of the potential for wider cooperation in support of the objectives of the Statute.[168] This demands effective partnerships, and vigilance to ensure that the Office and its partners remain faithful to the requirements of the Statute. The Office will deepen its engagement with national authorities by its efforts to develop and consolidate a community of practice, to leverage appropriate technology, to bring justice closer to affected communities, and to harness the full range of cooperation mechanisms which may be available.

[167] *See also below* para. 166.

[168] *See* ICC OTP, *Policy on Complementarity and Cooperation* (2024).

134. As set out in more detail below, further improving partnerships towards accountability will be essential in addressing cyber-enabled crimes under the Rome Statute. In particular, the transnational character of cyberspace means that relevant evidence may often be held in multiple different jurisdictions, and the effects of criminal conduct may be similarly distributed across international borders. The fast-changing nature of cyberspace means that expertise must be tapped wherever it may be found, whether in the public or private sector. And the wide contemporary relevance of cyberspace makes it essential to reinforce that the prohibition of the crimes in the Rome Statute—which are the most serious crimes of international concern—applies equally in this domain, as in any other.

135. The Office will maintain and develop existing partnerships, and build new partnerships, to meet these requirements. Where appropriate, the Office will work collaboratively with States to investigate cyber-enabled crimes under the Statute, and to disrupt such activities where they may be ongoing. Within the framework of their respective legal obligations and interests, the Office will seek to enhance cooperation with the private sector. The Office will also benefit, as appropriate within the context of its independent mandate, from the support of external experts and policy advice in meeting the new opportunities and challenges presented by cyberspace and the information revolution.

PRACTICAL CONSIDERATIONS

136. The Office will integrate the insights and principles set out in this Policy into its practical operations and procedures, in order to ensure that it is equipped to investigate and, where appropriate, prosecute cyber-enabled crimes under the Rome Statute on an equal basis with such crimes committed by more traditional means.

137. The Office will develop and adapt its institutional structures as necessary and feasible for this purpose. It will take into account considerations particular to cyber-enabled criminality at all phases of its work, including preliminary examination, investigation, and prosecution. Mindful of the particular relevance of cooperation and complementarity in addressing conduct in cyberspace, it will adopt specific measures in this area.

138. Consistent with its standing commitment to best practice, including where appropriate by use of a standardised 'lessons learned' process, the Office will review, identify, and document key aspects of its past performance in addressing cyber-enabled crimes in order to facilitate continuous learning, to preserve institutional knowledge, and to build upon successful innovations.

Institutional structures and strategic advice

139. The primary expertise of the Office lies in carrying out complex investigations and prosecutions concerning alleged crimes within the jurisdiction of the Court. While conduct in cyberspace intersects with the Office's mandate in this respect, as described above, it has distinct features requiring that the Office is supported with the necessary strategic advice, structures and expertise. All such measures described in this Policy are without prejudice to, and shall not compromise, the Prosecutor's independence as guaranteed and required by article 42 of the Statute.[169]

140. The Office has already appointed a Special Adviser on Cyber-Enabled Crimes within the jurisdiction of the Court, to assist the Office in developing and implementing the present Policy. Recognising the broad spectrum of experience and expertise which may be relevant to the investigation and prosecution of cyber-enabled crimes in practice, the Office will take further steps to ensure access to

[169] *See also above* paras. 125-127.

strategic advice in this area from leading experts, including from the private sector. This will include a standing mechanism to ensure that the Office can benefit from expert dialogue with relevant stakeholders, including but not necessarily limited to civil society and industry experts. On a case-by-case basis, the Office may also commission specific advice from approved third party providers, including on a *pro bono* or commercial basis as necessary.

141. The primary structure for carrying out the Office's investigative and prosecutorial activities in a situation is the 'Unified Team,' as described further below. This is supported by dedicated units for information handling (the Evidence and Discovery Management Unit), forensic scientific processing (the Cyber Unit), all-source analysis (the Information Fusion Centre), and financial investigations (the Financial Investigations Unit). Specific expertise in the investigation and prosecution of cyber-enabled crimes will be developed and integrated within these existing structures as required.

142. The Office's regular programme budget remains the primary source of funding with respect to its investigative and prosecutorial activities, and related functions, under this Policy.[170]

Strengthening expertise and training

143. The Office recognises the need to further strengthen its in-house expertise on cyber-enabled crimes under the Statute. It will provide training to appropriate staff members in Unified Teams and relevant support units, aimed at enhancing their capacity to identify and investigate such conduct. Such training will be legal and/or technical in nature, as required. The Office will continue to recruit staff members with the required breadth and depth of experience relevant to the work of the Office, including facility with technical and digital evidence. It will seek to build and maintain broad structures for knowledge exchange and professional

[170] The Office has also created a Trust Fund for Complementarity and Cooperation that allows it to promote the Office's dynamic complementarity approach by increasing its engagement with and support to specific programmatic activities in selected situations and thematic areas of work. Any voluntary contributions to this Trust Fund by governments, international organisations, individuals, corporations, and other entities in accordance with article 116 of the Statute will enable the Office to further strengthen its capacity to implement this Policy. *See* Financial Regulations and Rules, paras. 7.2-7.4. As the Prosecutor informed the States Parties in his Note Verbale of 7 March 2022, donations from States Parties are to be used to enhance the capacity of the OTP across all situations. Earmarking donations for certain situations is not possible, but donors may direct the funds to one of the specific priority areas, which were stated in the Note Verbale and repeated in several documents thereafter. *See* Report of the Committee on Budget and Finance on the Work of Its Thirty-Ninth Session (29 November 2022), paras. 248-252.

updating, mindful of the potential overlap in the skills required to investigate cyber-enabled crimes under the Statute and other types of investigative and similar activity carried out by States (for example, with regard to ordinary cybercrimes).

144. The Office will include expertise in cyber-enabled criminality as a recruitment profile within its secondment programme. It will also explore avenues for requesting secondments of this kind as short notice 'surge capacity,' including from the private sector.

145. The Office recognises that addressing cyber-enabled criminality under the Statute is also likely to require increased engagement with professional communities who may not be well acquainted with the Statute or the work of the Court. Accordingly, and where necessary, the Office will offer briefings and training to appropriate external partners, including in the private sector, to explain the potential relevance of the Statute and the Court to their work, and to facilitate future mutual cooperation.

Preliminary examinations

146. The preliminary examination is the process by which the Office determines whether it has a legal basis to open an investigation in a situation, once the Court's exercise of jurisdiction has been triggered either by a referral to the Court (from a State Party or the UN Security Council) or by the Prosecutor acting of their own motion.[171] Where there is a 'reasonable basis to proceed', the preliminary examination will be resolved in favour of investigation.[172]

147. While it is legally possible for an investigation to be opened with regard to a single incident of alleged crimes under the Statute, in practice it is more common for a situation to be defined by broader geographic, temporal, or other parameters containing multiple potential cases of alleged crimes under the Statute.

---

[171] *See above* paras. 35-39.

[172] Specifically, for referred situations, this is established where there is a reasonable basis to believe that at least one crime under the Statute has been committed, and that at least one case arising from such allegations would be admissible under the Statute, and there are not substantial reasons to believe that an investigation would be contrary to the interests of justice. *See* Rome Statute, art. 53(1). For situations where the Prosecutor acts on their own motion, these same factors will be taken into account but within the broader framework of the Prosecutor's exercise of discretion: Rome Statute, art. 15(3); ICC RPE, rule 48. For the Office's position in this respect, *see* ***Request under Regulation 46(3) of the Regulations of the Court***, Prosecution's response to the 'Victims' request for clarification and an order to compel the Prosecutor to act on their legal obligations under article 15(3)', ICC-RoC46(3)-01/24-3, 13 December 2024, paras. 15-19. *See also below* para. 149.

148. In carrying out preliminary examinations, and in assessing whether there is a reasonable basis to believe that one or more crimes under the Statute have been committed, the Office will duly consider the possible commission of cyber-enabled crimes.

149. Furthermore, while the Prosecutor's decision to initiate a preliminary examination of their own motion (*i.e.*, in the absence of a referral) is discretionary, due consideration will be given in that regard to allegations of cyber-enabled crimes. In at least some circumstances, it is acknowledged that even detecting the possible commission of cyber-enabled crimes under the Statute may be more difficult than for such crimes committed by physical means. For this purpose, therefore, the Office may rely, in particular, on communications submitted by reputable external partners under article 15(1) of the Statute, including from competent State authorities (such as computer emergency and computer security incident response teams (CERTs and CSIRTs)) and the private sector.[173]

150. In carrying out preliminary examinations in which cyber-enabled crimes under the Statute may allegedly have occurred, the Office may as appropriate "seek additional information from States, organs of the United Nations, intergovernmental or non-governmental organisations, or other reliable sources", including from the private sector.[174] Mindful of the possible degradation or loss of relevant evidence, especially where it is technical or digital in nature, the Office may also request voluntary measures to preserve evidence of such crimes pending the opening of a full investigation.[175] The Office will work with relevant stakeholders to explore the desirability of clear guidelines for cooperation on data preservation requests.

Investigations

151. For each situation under active investigation by the Office, the investigation is carried out by a dedicated multi-disciplinary team (the 'Unified Team'). This team has the primary responsibility for investigating cases with a

[173] Under this provision, the Office recalls that any person may submit to the Prosecutor "information on crimes within the jurisdiction of the Court".

[174] ICC RPE, rule 104(2). *See also* Rome Statute, art. 15(2).

[175] *See e.g.* *Situation in Burundi*, Public Redacted Version of 'Decision pursuant to Article 15 of the Rome Statute on the Authorization of an Investigation into the Situation in the Republic of Burundi […],' ICC-01/17-9-Red, 9 November 2017, para. 15 (noting that "the fact that States Parties are not obliged to cooperate with the Court prior to the initiation of an investigation does not prevent the Prosecutor from seeking their voluntary cooperation […] The same would apply to States not Parties to the Statute and non-state entities"). *See also below* paras. 162-163.

view to potential prosecution, consistent with the law applicable before the Court and the Office's internal policies and practices. The final decision to prosecute is taken by the Prosecutor, with the advice of Office staff members.[176]

152. Consistent with the principles described above, the investigation of cyber-enabled crimes is simply a novel application of the Office's existing mandate under the Statute.[177] As such, cyber-enabled crimes will be addressed as an integral part of the broader investigation within the relevant situation, rather than in a 'silo' or as a special case in isolation from other considerations.

153. In every investigation, the Office will take due account of the possibility of cyber-related crimes. In this regard, it will pursue relevant lines of inquiry according to the same principles and on an equal basis with crimes committed by other means. Where possible, it will seek to identify such lines of inquiry concerning cyber-enabled crimes early in the investigation, in order to facilitate appropriate planning and the optimal use of resources.

154. The Office's commitment to addressing cyber-enabled crimes on an equal footing to crimes committed by other means does not imply that all allegations will necessarily result in a prosecution for such crimes before the Court, particularly bearing in mind considerations of relative gravity.[178] The Office will, however, have due regard to the expressive value of addressing such allegations in determining the programme of cases to be prosecuted—serving the overall goal of representing the true extent of the criminality in a situation, to ensure, jointly with the relevant national jurisdictions, that the most serious crimes do not go unpunished.

155. Importantly, while the Office investigates each situation within its jurisdiction with a view to prosecuting at least one case before the Court, this is not to the exclusion of other prosecutorial and non-prosecutorial outcomes which may serve to deter or to disrupt crimes under the Statute, or to mitigate the harm caused.[179] Such outcomes may be particularly significant for some forms of cyber-enabled crime under the Statute, such as those based on the dissemination of material calling for the commission of genocide, crimes against humanity, war crimes, or aggression.

156. To carry out effective investigations into cyber-enabled crimes, the Office will actively cooperate with external partners, including those with access to

[176] *See further below* paras. 175-177.

[177] *See above* paras. 3, 19-25, 49-52.

[178] *See above e.g.* paras. 39, 128-132.

[179] *See further below* paras. 177-178.

relevant evidence or expertise. The Office may also support the investigative activities of States Parties—with regard not only to crimes under the Statute, but also other serious crimes under national law—by providing information or suitable other assistance at their request.[180]

157. Anticipating that the cyber dimension of all its investigations will continue to expand in the coming years, the Office will ensure that it is equipped with the skills, expertise, facilities, and procedures necessary to determine the truth, and to prosecute cases successfully. To this end, the Office will in particular take measures to facilitate its access to the requisite technical expertise, its access to relevant evidence, and its ability to interpret and analyse such evidence. The Office will seek to participate in joint investigations, where appropriate. The Office will also pay particular attention to the investigation of cyber-enabled offences against the administration of justice at the Court.

ACCESSING SPECIALISED TECHNICAL EXPERTISE

158. The Office recognises that investigating cyber-enabled crimes will on occasion require technical expertise that is not otherwise required in carrying out its mandate, and which is unlikely to be routinely funded as part of its core budget. For example, this may apply for crimes under the Statute which are carried out by the use of malicious computer code, where analysis of the functioning of that code and attributing its design or use to particular computer systems or even individuals is a highly specialised form of investigative activity.

159. The Office will ensure that it can access such expertise if and when required for the purpose of its investigation through a range of suitable means, including but not limited to: secondments of personnel by national authorities, including persons from both the public and private sectors who may be previously identified as a part of a standing roster; the short-term appointment of external consultants; requests for assistance from States Parties under article 93(1) of the Statute; and the commissioning of reputable external institutions to carry out forensic and technical analysis.[181] This is without prejudice to the normal process by which the Office seeks to ensure that activities necessary to its mandate are funded within the regular programme budget approved by the Assembly of States Parties.[182]

[180] Rome Statute, art. 93(10).

[181] *See also above* paras. 143-144.

[182] *See above* para. 142.

160. In evaluating its existing capabilities, and putting any necessary additional modalities in place, the Office will take into account strategic advice from relevant stakeholders, including but not necessarily limited to civil society and industry experts.[183]

ACCESSING RELEVANT EVIDENCE

161. The Office will seek to rely on the full spectrum of relevant and probative evidence to investigate whether cyber-enabled crimes under the Statute have been committed, to assess the cause and impact of such crimes, and to determine individual criminal responsibility. Technical digital evidence may be of particular importance in establishing how some such crimes were committed and in attributing conduct to certain direct perpetrators. Other types of evidence, broadly conceived, will likely remain relevant in establishing individual criminal responsibility more broadly.

162. The Office will make appropriate and diligent use of all its investigative powers under the Statute. These include powers to request the assistance of States, including but not limited to the production of evidence, the examination of places and sites, the execution of searches and seizures, and the provision of records and documents.[184] In accordance with the provisions of their national law, States Parties are required to provide such assistance, including by executing measures to compel corporations, individuals, and other entities within their jurisdiction. In addition, the Office may also request the voluntary cooperation of private entities, within the framework of their applicable legal obligations.

163. Evidence relevant to the investigation of cyber-enabled crimes, especially certain kinds of digital evidence, may be at particular risk of degradation or deletion over time.[185] Accordingly, the Office will not only consider requests for voluntary measures to preserve evidence during the preliminary examination,[186] but will also take such measures when warranted during its investigation—including where permitted on a compulsory basis.[187] In this context, as necessary, the Office will also seek the assistance of the Court in relation to unique investigative opportunities.[188] Intentional measures to destroy, tamper with, or interfere with the collection of evidence by the Court constitute an offence

[183] *See above* para. 140.

[184] Rome Statute, art. 93(1).

[185] *See also above* para. 150.

[186] *See above* para. 150.

[187] Rome Statute, art. 93(1)(j).

[188] Rome Statute, art. 56.

against the administration of justice, regardless of motive, and may be prosecuted as such.[189]

164. Certain information relevant to the Office's investigations may be of a sensitive nature, and require special handling or protection. The Office already has in place the necessary procedures and tools to accommodate such concerns.[190] While recognising legitimate interests of national security, the Office will seek to resolve any such issues arising in cooperation with concerned States.[191]

165. The Office recognises that some forms of technical digital evidence relevant to proving cyber-enabled crimes may be of substantial volume. It has already put in place measures to upgrade and invest in its systems to store, manage, and review evidence. These are sustainable, resilient, and have the potential for appropriate growth as required. Specific demands beyond the typical requirements of the Office may be assessed on a case-by-case basis.

166. In assessing the impact of cyber-enabled crimes, consistent with its general policy, the Office will take into account a comprehensive array of perspectives. These will include, as appropriate, those of women, men, children and youth, persons with disabilities, and persons who are vulnerable or marginalised either for reasons associated with the alleged crimes themselves, or for other discernible reasons.

JOINT INVESTIGATIONS

167. The Office has already stated its intention to seek to expand its participation, where appropriate, in joint investigations.[192] Such activities allow two or more investigative, prosecutorial, or judicial bodies to coordinate common lines of inquiry and/or work alongside each other in specific operations. This can be done under the auspices of several institutions and treaties[193]—now also including the Ljubljana-Hague Convention on International Cooperation

[189] Rome Statute, art. 70(1)(c). *See also* art. 30; *Bemba et al.* Appeal Judgment, para. 738 (affirming that the mental element is satisfied where the perpetrator "meant" to engage in the relevant conduct).

[190] *See also* Rome Statute, art. 54(3)(e), (f).

[191] *See also* Rome Statute, arts. 72-73, 93, 97, 99.

[192] *See* ICC OTP, *Policy on Complementarity and Cooperation* (2024) (further noting that such measures can serve to maximise and enhance potentially overlapping efforts, while respecting the independence, impartiality, and legal regime applicable to each participating entity).

[193] For example, the Office is already participating in a Joint Investigation Team under the auspices of EUROJUST, in the *Situation in Ukraine*, and a Joint Team supported by EUROPOL, in the *Situation in Libya*. *See* ICC OTP, *Policy on Complementarity and Cooperation* (2024), paras. 103-109.

in Investigating International Crimes,[194] the Second Additional Protocol to the Budapest Convention on Cybercrime,[195] and the UN Convention against Cybercrime.[196]

168. The Office recognises that cyber-enabled crimes within the jurisdiction of the Court may be likely in practice also to implicate various offences under national law, including ordinary 'cybercrimes', such as illegally accessing a computer system. Such conduct may also take place within or have spill-over effects in multiple jurisdictions.

169. By participating in joint investigations where appropriate, addressing serious crimes under national law and acting consistently with internationally recognised rights,[197] the Office may in particular help secure tangible results in disrupting ongoing cyber-enabled crimes within the jurisdiction of the Court, and reduce their harmful consequences.

CRIMES COMMITTED WITHIN THE CONTEXT OF COMMERCIAL ACTIVITY

170. While the Court may only exercise jurisdiction under the Rome Statute over "natural persons" (and therefore not over purely legal persons such as corporations), the Statute is to be applied "equally to all persons without any distinction" based on official capacity or other role or status.[198] Accordingly, within the framework of the overall discretion afforded to the Prosecutor under the Rome Statute to select and prioritise cases for the investigation, the Office will investigate alleged crimes within the jurisdiction of the Court equally, irrespective whether they are committed within the context of commercial activity.

171. Notwithstanding any investigative steps that the Office might take, if the Office has reason to believe that a corporation or corporate officer, employee, or similar person is involved in the commission or facilitation of cyber-enabled crimes within the jurisdiction of the Court, the Office may directly engage with that corporation or person, or other relevant corporations or persons, if appropriate,

---

[194] *Ljubljana-The Hague Convention on International Cooperation in the investigation and prosecution of the crime of genocide, crimes against humanity, war crimes, and other international crimes*, art. 41.

[195] *Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence (Second Protocol to Budapest Convention)*, art. 12.

[196] *United Nations Convention against Cybercrime (Hanoi Convention)*, art. 48.

[197] *See further above* paras. 118-122; *below* paras. 189-190. *See also e.g.* Rome Statute, art. 93(10) (referring to "a serious crime under the national law of the requesting State").

[198] *See* Rome Statute, arts. 25(1), 27(1). *See also* art. 21(3). *See also above* para. 38.

consistent with its powers under the Rome Statute. Such engagement may seek, among other objectives, to:

a. Affirm that relevant person(s) are aware of their alleged involvement in cyber-enabled crimes within the jurisdiction of the Court ("putting them on notice");

b. Ensure that corporations or persons who possess or may come into possession of proceeds, property, assets, or instrumentalities of crimes, are not to be regarded as *bona fide* third parties who may be protected from identification, tracing, freezing, or seizure of the same for the purpose of eventual forfeiture;

c. Prompt a relevant corporation to take appropriate lawful action, including conducting its own internal inquiries not inconsistent with the Office's investigation or applicable national law, pursuant to its due diligence obligations, and/or;

d. Inform relevant corporations or persons of the legal, financial, and reputational risks associated with the alleged activities, and thereby encourage them to cease and desist from such activities and/or to terminate their cooperation with others allegedly engaged in such activities.

SUSPECTED OFFENCES AGAINST THE ADMINISTRATION OF JUSTICE AT THE COURT

172. The Office will take rigorous action to disrupt, deter, and punish cyber-enabled offences against the administration of justice at the Court. The Prosecutor may initiate such investigations on his or her own initiative.[199] The Office will prioritise such investigations especially in circumstances where the IT infrastructure of the Court itself has been materially affected.

173. The Office recalls that "[t]he conditions for providing international cooperation to the Court" with respect to investigations into suspected offences against the administration of justice "shall be governed by the domestic laws of the requested State."[200] The Office will work with States, and especially as relevant the Host State, to ensure that the necessary cooperation modalities are available to facilitate such investigations. The Office will also ensure that the necessary modalities exist to facilitate the cooperation of relevant organs of the Court, such as the Registry, in circumstances where they may hold relevant evidence.

[199] ICC RPE, rule 165(1).

[200] Rome Statute, art. 70(2). *See also* ICC RPE, rule 167.

174. Where possible, the Office will seek to cooperate with States Parties, and especially as relevant the Host State, in determining the most appropriate and effective venue to conduct a prosecution if warranted.[201] It recalls that States Parties are obliged to ensure that their criminal laws penalizing offences against the integrity of their own investigative and judicial proceedings extend to similar conduct directed against the Court,[202] and that this should therefore apply equally to conduct in the cyber domain. The Office will engage in a constructive dialogue with States to enhance cooperation in investigating and prosecuting offences against the administration of justice before the Court.

Prosecutions

175. The Prosecutor will decide to prosecute a case before the Court if there is a sufficient basis to proceed under the Statute and a reasonable prospect of securing a conviction.

176. In applying to the Court for the issue of an arrest warrant, or summons to appear, the Prosecutor may be selective in the crimes and forms of responsibility which are initially alleged. This is without prejudice to the Prosecutor's discretion to present further allegations at a later stage, including after the suspect has made their initial appearance before the Court.[203]

177. In appropriate circumstances, the Office will also pursue alternative outcomes to prosecution before the Court, including cooperating in prosecutions before other jurisdictions. Where cyber-enabled crimes are ongoing, and where practicable and appropriate, the Office will also consider adopting lawful measures to disrupt or mitigate such conduct.

178. As appropriate, the Office may seek the assistance of States Parties in identifying, tracing, freezing, and/or seizing the means used to carry out cyber-enabled crimes under the Statute (so-called 'instrumentalities of crimes').[204] This may potentially include not only physical objects but also virtual objects, such as web domains. Additionally, the Office may also request the freezing and seizure

[201] Rome Statute, art. 70(4); ICC RPE, rule 162.

[202] Rome Statute, art. 70(4).

[203] Where necessary in such circumstances, a waiver of the rule of speciality may be requested from a surrendering State: Rome Statute, art. 101.

[204] Rome Statute, art. 93(1)(k).

of the proceeds of crimes, and all property and assets of suspects, for the purpose of eventual forfeiture.[205]

179. In presenting cases at trial of cyber-enabled crimes within the jurisdiction of the Court, the Office will make appropriate use of expert witnesses and other means of proof adapted to the clear and concise presentation of technical information.

Cooperation and Complementarity

180. The Office incorporates considerations of cooperation and complementarity into each stage of its activities as described above. Effective cooperation is essential to the Office's ability to discharge all facets of its mandate. Complementarity—which reflects the principle that the Court should defer to genuine and effective national proceedings where they actually exist[206]—is not simply a legal means of resolving conflicts of jurisdiction by rendering certain cases inadmissible before the Court,[207] but also an animating principle which may favour cooperation, including appropriate burden-sharing, in delivering accountability for victims and affected communities.[208]

181. The Office recalls that cases which are or have been investigated or prosecuted by a State with jurisdiction, genuinely and effectively, are inadmissible before the Court.[209] Such cases are assessed on the basis that they concern both the "same person" and substantially the "same conduct" as the proceedings before the Court.[210] This does not necessarily require that the charge under applicable

[205] Rome Statute, art. 93(1)(k). *See also* *Prosecutor v. [Redacted]*, Judgment on the appeal of the Prosecutor against the decision of [Redacted], ICC-ACRed-01/16, 15 February 2016, paras. 1, 63 (finding that there is no requirement that such property or assets are limited to that which is derived from, or otherwise linked to, the commission of alleged crimes under the Statute).

[206] *See e.g.* *Prosecutor v. Gaddafi and Al-Senussi*, Judgment on the appeal of Libya against the decision of Pre-Trial Chamber I of 31 May 2013 entitled "Decision on the admissibility of the case against Saif Al-Islam Gaddafi", ICC-01/11-01/11-547-Red OA4, 21 May 2014, para. 78.

[207] *See also above* para. 44.

[208] *See* ICC OTP, *Policy on Complementarity and Cooperation* (2024).

[209] *See* Rome Statute, arts. 17-20.

[210] *See e.g.* *Situation in the Republic of the Philippines*, Judgment on the appeal of the Republic of the Philippines against Pre-Trial Chamber I's "Authorisation pursuant to article 18(2) of the Statute to resume the investigation", ICC-01/21-77 OA, 18 July 2023, paras. 101-103.

national law is identical to the applicable charge under the Rome Statute.[211] It follows that, at least in certain circumstances, a prosecution for a cybercrime under national law could satisfy the "same person" and "same conduct" tests and thus overlap with a prosecution at the Court alleging the commission or facilitation of a cyber-enabled crime under the Statute.

182. Given the particular significance of cooperation in responding effectively to cyber-enabled crimes under the Statute, some further general matters are set out with regard to: cooperation with States Parties under the Statute; the possibility of enhanced cooperation by States; cooperation with the private sector, and; responding to requests for assistance from States.

COOPERATION WITH STATES PARTIES UNDER THE STATUTE

183. Consistent with its *Policy on Complementarity and Cooperation*, the Office will adopt a two-track approach in addressing cyber-enabled crimes under the Statute: namely, coordinating with national authorities to promote cooperation and complementarity while remaining committed to its mandate to independently and impartially investigate and prosecute Rome Statute crimes when national authorities are unwilling or unable to act.

184. As appropriate, and consistent with internationally recognised human rights, the Office's assistance to national authorities in their efforts to investigate and prosecute cyber-enabled crimes may include the sharing of intelligence, evidence, or situation briefs; offering expertise and support to enhance the capacity of national authorities; undertaking joint investigative activities; and holding strategic consultations on case selection and prioritisation to share the burden of investigating and prosecuting Rome Statute crimes.

185. The Office will cooperate with national authorities either bilaterally or through the Cooperation and Complementarity Forum. The Forum serves as a platform for the two-way sharing of information and expertise between the Office and national authorities, aiming to enhance coordination, harmonisation, and cohesion, and will identify areas where mutual support can be provided.

[211] *Prosecutor v. Gaddafi and Al-Senussi*, Judgment on the appeal of Mr Abdullah Al-Senussi against the decision of Pre-Trial Chamber I of 11 October 2013 entitled "Decision on the admissibility of the case against Abdullah Al-Senussi", ICC-01/11-01/11-565 OA6, 24 July 2014, para. 119. *But see further Situation in the Bolivarian Republic of Venezuela I*, Judgment on the appeal of the Bolivarian Republic of Venezuela against Pre-Trial Chamber I's "Decision authorising the resumption of the investigation pursuant to article 18(2) of the Statute", ICC-02/18-89 OA, 1 March 2024, paras. 326-332.

ENHANCED COOPERATION BY STATES IN PROVIDING ACCESS TO EVIDENCE

186. States may agree to enhance the modalities by which they will cooperate with the Court, and the Prosecutor may enter into such arrangements or agreements for this purpose, provided they are not inconsistent with the Statute.[212] Likewise, non-States Parties may also agree to cooperate with the Court on an *ad hoc* basis.

187. Recent treaty law developments relevant to the investigation and prosecution of cybercrimes, including under the Second Additional Protocol to the Budapest Convention on Cybercrime and the UN Convention against Cybercrime will require States Parties to amend their domestic law in order to provide for mutual legal assistance under those regimes. While, as explained above, the Court does not have jurisdiction over ordinary cybercrimes, there are substantial similarities in the modalities of effective cooperation that are required for the prosecution of these crimes and cyber-enabled crimes within the jurisdiction of the Court. The Office will seek the support of ICC States Parties and any other interested States to conclude voluntary agreements extending similar assistance to the Office for the purpose of investigating and prosecuting cyber-enabled crimes under the Statute, including both article 5 crimes and article 70 offences.

188. The Office will also engage in a constructive dialogue in particular with relevant States Parties to raise awareness of the need to cooperate with the Court at the time these States will be amending their legislation to ensure effective international cooperation in the prosecution of cybercrimes.

RESPONDING TO REQUESTS FOR ASSISTANCE FROM STATES

189. The Office "may, upon request, cooperate with and provide assistance to" a State Party or other States "conducting an investigation into or trial in respect of conduct which constitutes a crime within the jurisdiction of the Court or which constitutes a serious crime under the national law of the requesting State",[213] including by sharing evidence obtained in the course of an investigation conducted by the Office.[214] The Office exercises its discretion in responding to such requests based, among other considerations, on its duty to act consistently with internationally recognised human rights.[215]

---

[212] Rome Statute, art. 54(3)(c), (d).

[213] Rome Statute, art. 93(10)(a) (applying to States Parties). *See also* art. 93(10)(c) (applying to non-States Parties).

[214] *See* Rome Statute, art. 93(10)(b)(i).

[215] *See above* paras. 7, 37, 118-122.

190. In principle, as stated above, the Office recognises the potential intersection between cyber-enabled crimes within the jurisdiction of the Court and conduct amounting to serious crimes under national law, and is committed to working with States in that respect.[216] At the same time, it notes that not all cybercrimes under national law necessarily fall into these categories. It will also remain mindful of the diversity of national legislation concerning cybercrimes, and the possibility of variations in the degree to which internationally recognised human rights may be incorporated into and compatible with national law in this respect.

COOPERATION WITH CIVIL SOCIETY ORGANISATIONS AND CORPORATIONS

191. The Office may seek the cooperation of any entity in accordance with its competence and mandate, and the Prosecutor may enter into arrangements or agreements as may be necessary to facilitate the cooperation of any person, provided they are not inconsistent with the Statute.[217] This includes, among others, both civil society organisations and corporations. The Office notes that, in the intersection of law and emerging technologies, effective cooperation and dialogue between States, civil society, and the private sector is key. To this end, as noted above, it will ensure that it can benefit from strategic advice from relevant stakeholders.[218]

192. The Office has long been committed to collaborating effectively with civil society in all facets of its work.[219] Leading to the development and publication of this Policy, the Office has benefited from and appreciated new opportunities to work with civil society organisations playing a critical role in the protection of digital rights, privacy, and freedom of expression, and helping work towards accountability for violations. It will seek both to broaden and deepen this engagement relevant to cyberspace and the crimes within the jurisdiction of the Court.

193. Recognising the particular role that the private sector plays in the management and development of cyberspace, and related technologies, the Office will also seek to enhance direct cooperation with private corporations on matters relevant to the investigation and prosecution of cyber-enabled crimes within the jurisdiction of the Court. The Office is grateful for the positive engagement it has already received, including in the development and publication of this Policy.

---

[216] *See above* paras. 167-169, 183-185.

[217] Rome Statute, art. 54(3)(c), (d).

[218] *See above* para. 140.

[219] *See* ICC OTP, *Policy on Complementarity and Cooperation* (2024), paras. 82-85.

194. Concretely, working with civil society and the private sector, the Office will seek to enhance and clarify voluntary frameworks for the sharing of relevant information and expertise, facilitating effective cooperation and developing best practices in addressing the misuse of cyberspace leading to crimes within the jurisdiction of the Court. This will be based on a shared commitment to compliance with internationally recognised human rights,[220] in the pursuit of justice for cyber-enabled crimes within the jurisdiction of the Court.

[220] *See e.g.* UN, *Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework,* 2011, principles 11, 13-14, 17. *See further* UNHRC Res. 17/4, para. 1 (endorsing these principles).

WAY FORWARD

195. With this policy, the Office seeks to ensure that it will remain equipped to address the full spectrum of means by which crimes within the jurisdiction of the Court may be committed. This is important to ensure that the Office can fulfil its mandate to investigate and, where appropriate, prosecute cases in which the most serious crimes of international concern have been committed—regardless of the technology which might have been used to carry them out. What matters, rather, is the impact upon victims and affected communities.

www.icc-cpi.int

InternationalCriminalCourt

IntlCrimCourt

flickr icc-cpi

IntlCriminalCourt

InternationalCriminalCourt