COUR PÉNALE INTERNATIONALE

BUREAU
DU PROCUREUR

INTERNATIONAL CRIMINAL COURT

OFFICE OF
THE PROSECUTOR

OFFICE OF THE PROSECUTOR

DRAFT POLICY ON CYBER-ENABLED CRIMES UNDER THE ROME STATUTE

6 March 2025

THIS DOCUMENT IS PROVISIONAL AND RELEASED FOR THE PURPOSE OF PUBLIC CONSULTATION ONLY. NOTHING IN THIS DOCUMENT NECESSARILY REFLECTS THE FINAL VIEW OF THE OFFICE OF THE PROSECUTOR.

LIKEWISE, WHILE THIS DOCUMENT MAKES USE OF EXAMPLES TO CLARIFY CERTAIN POINTS, THESE EXAMPLES ARE PURELY HYPOTHETICAL AND FOR ILLUSTRATIVE PURPOSES ONLY.

CONTENTS

EXECUTIVE SUMMARY

1. The Office of the Prosecutor's Policy on Cyber-Enabled Crimes sets out how the Office will use its mandate and powers to investigate and prosecute cyber-enabled crimes within the Court's jurisdiction. It also shows how the Office's work may potentially support relevant national efforts to address unlawful and harmful uses of cyberspace more broadly.

2. This Policy uses the term 'cyber-enabled crimes' to mean the perpetration by cyber means of the international crimes set out in the Rome Statute, and the facilitation by cyber means of such crimes, however committed. In both respects, 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 does not amount to the perpetration or facilitation of crimes within the jurisdiction of the Court, but which provides legally required context, or correlates with, or is otherwise probative of these crimes, and may therefore increasingly form a significant part of all the Office's investigations.[1]

3. 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 numerous 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 remains relevant to the criminal conduct of persons within the Court's jurisdiction irrespective of the technological means they might employ;

d. To emphasise the Office's commitment to establishing an institutional environment that facilitates effective investigation and prosecution of cyber-enabled crimes under the Statute—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 under the Statute;

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 law enforcement action at the international or national level;

g. To contribute to the development of international jurisprudence and best practices concerning the prosecution of cyber-enabled crimes at the ICC and beyond.

[1] *See below* paras. 21-27 ('Key Terms and Concepts').

4. 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.

5. To date, the question of cyber-enabled crimes under the Statute—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 cyber-enabled 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.

6. 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 cyber-enabled crimes within the Court's jurisdiction. Consistent 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. One exception concerns offences against the administration of justice, since such cases are not subject to any gravity requirement, but rather are serious because they threaten the functioning of the Court itself.

7. 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 the same basis as other types of criminality within the Court's jurisdiction. The Office is prepared to investigate and prosecute both the perpetrators and the facilitators of cyber-enabled crimes.

8. 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.

INTRODUCTION

Addressing new technologies

9. In both domestic 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 this would require substantial reform and new lawmaking. 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,[2] by formulating their official national positions on how international law applies in cyberspace,[3] through the adoption of certain soft law instruments, 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. States have been assisted in this adaption process by academic efforts, such as the two *Tallinn Manuals*.[4] 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 other cyber-enabled conduct.[5]

10. International criminal law is no different. As set out in this Policy, the view of the Office is 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.[6] The Statute is technology-neutral in the terms in which it is written. As a matter of law, genocide, crimes against humanity, war crimes and aggression, as well as offences against the administration of justice, can all be perpetrated or facilitated by cyber means. This is the key point that this Policy wishes to convey. This conclusion can be reached using ordinary, long-established means of interpretation, without

[2] The include the work of the Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG).

[3] Most of these positions are usefully compiled here: https://cyberlaw.ccdcoe.org/wiki/List_of_articles#National_positions. In addition to the national positions of individual states, in 2024, the African Union and the European Union both adopted their common positions on the application of international law in cyberspace.

[4] See 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*").

[5] *See 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).

[6] While State have infrequently made specific comment 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 urged States to take 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. *See also* para. 4.

impermissibly stretching existing criminal law by analogy and violating the *nullum crimen sine lege* principle.[7]

11. The commission or facilitation by cyber means of international crimes is yet to be litigated in detail before the Court.[8] Nonetheless, the application of existing international criminal law to cyber-enabled crimes has inspired a substantial body of academic scholarship. The Office wishes to acknowledge two expert-led initiatives in particular. 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*.[9] The Office and the International Committee of the Red Cross participated in this process as observers. 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, providing feedback to the *Manual*'s editors, and has taken the experts' views into account.

12. The Statute does not include 'cybercrimes' as such—that is, criminal offences under domestic law, such as illegal access and interception of data, system interference, or fraud or theft committed by cyber means. 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 remains the case even if they are committed or facilitated by cyber means. That said, under treaties like the Budapest Convention, States (some of which may also be parties to the Rome Statute) have assumed obligations to penalize, investigate, prosecute and cooperate in the investigations of ordinary cybercrimes. There may be numerous synergies between States' efforts to build capacity to effectively investigate these ordinary cybercrimes, and to enhance State cooperation in that regard, and capacity-building efforts with regard to cyber-enabled international crimes within the Court's jurisdiction, in line with the principle of complementarity.

13. In this Policy, the Office will set out its views on the interpretation to be given to provisions of the Statute relevant to the investigation and prosecution of cyber-enabled crimes within the Court's jurisdiction. The Policy will explain how crimes under the Statute, including not only article 5 crimes but also offences against the administration of justice, can be committed and facilitated by cyber means. The Policy will also set out the

[7] *See also 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, Partially 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").

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

[9] 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 ("Council of Advisers' Report").

views of the Office on the application of the Court's jurisdictional framework to cyber-enabled crimes. This Policy may sometimes recognise diversity of State or expert opinion, or refrain from taking a definitive position on a certain issue at the present time. This may not be taken to imply, however, the Office's view that such legal issues are necessarily controversial or unclear.

Policy objectives

14. 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 numerous 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 remains relevant to the criminal conduct of persons within the Court's jurisdiction irrespective of the technological means they might employ;

d. To emphasise the Office's commitment to establishing an institutional environment that facilitates effective investigation and prosecution of cyber-enabled crimes under the Statute—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 under the Statute;

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 law enforcement action at the international or national level;

g. To contribute to the development of international jurisprudence and best practices concerning the prosecution of cyber-enabled crimes at the ICC and beyond.

15. 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. After explaining how, in its view, the crimes in the Rome Statute can be committed or facilitated by means of conduct in cyberspace, this Policy articulates fundamental principles underlying the Office's approach to the investigation and prosecution of such crimes and provides guidance as to how these principles inform Office practice.

16. 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.

History and methods

17. In June 2023, the Office announced its intention to develop this Policy in its *Strategic Plan 2023-2025*. 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.[10]

18. 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.

19. This draft of the Policy was released for a first round of public consultation on 7 March 2025. The Office will continue to receive feedback on this draft, with a view to producing a final version to be published by end of 2025.

KEY TERMS AND CONCEPTS

Cyber

20. The term ‘cyber’ is used broadly in this Policy to denote the range of activities involving information and communications (digital) technologies or networks, including artificial intelligence (AI). 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

21. As explained in detail below, ‘cyber-enabled crime’ is used in this Policy 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.

22. 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

[10] *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.

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.

23. 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, 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. 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—for example, conduct in cyberspace might aim at concealing evidence of a crime which has already been committed, or might exploit such a crime for other purposes, such as propaganda. Alternatively, cyber conduct may 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.

25. 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. Similarly, the Office has inevitably been relying on digital evidence, or digital analytical tools, in its work; the use of digital evidence is a topic of enormous importance, but it is not one that will be dealt with extensively in this Policy.

26. 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 electronic 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.

27. 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 cyber-enabled crime under the Statute, 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 software to assign and authorise targets for attack on an automated basis.

Cybercrime

28. '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.

29. Some of the types of conduct prohibited by these ordinary cybercrimes, such as illegal access to a computer system, may also constitute prohibited conduct in the context of crimes within the Court's jurisdiction—for example, illegally accessing a computer system may be the first step in facilitating a war crime. For this reason, the Court and the Office may sometimes share common interests with national jurisdictions with respect to such conduct. Likewise, there may be mutual value in pooling capabilities, techniques, skills, and procedures related to the investigation of conduct in cyberspace.

APPLICABLE LAW AND JURISDICTION

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

31. 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.

32. Article 21(3) further mandates that both the application and interpretation of the Statute must be consistent with internationally recognised human rights. 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, and the right to participate in public affairs.

33. 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.[11]

34. 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 satisfied.[12] Just because

[11] Rome Statute, arts. 5, 11-12.
[12] 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. 110-114.

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 will 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.

35. 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.

36. Cyber-enabled crimes may be seen as posing challenges to the application of this jurisdictional framework, which is based on the territorial and personality principles that are otherwise long-established in international law. Nevertheless, as a general principle, the Office considers that jurisdiction over cyber conduct is regulated in the framework of the same jurisdictional principles applicable to other kinds of conduct under the Statute. The Office further notes that, in interpreting the pre-conditions to the Court's exercise of jurisdiction set out in article 12(2) of the Statute, it may be guided by States' own practice in relevant situations.

37. With regard to the territoriality principle, the key question is where 'the conduct in question occurred,' and how precisely to define the scope of the relevant conduct. The Court has 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.[13] With respect to the term 'conduct' in article 12(2), the Court further held that "the word is used in a factual sense, capturing the *actus reus* element underlying a crime"[14] 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."[15]

38. 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). In appropriate circumstances, and for some crimes of conduct (in which the elements of the crime do not

---

[13] *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.

[14] *Bangladesh/Myanmar* Article 15 Decision, para. 49.

[15] *Bangladesh/Myanmar* Article 15 Decision, para. 50.

require specific prohibited results), the Court's jurisprudence seems to suggest that it may also include the State (or States) where those results occurred (*i.e.*, where an intrinsic "part of" the crime occurred, factually speaking, even if no legal "element" took place there).[16]

> For example, if, in the context of an armed conflict, a person physically located in State A and using a computer system on its territory launched a cyber operation that affected the systems of a hospital in State B, causing death or injury to its patients and intending to do so, the war crimes of intentionally directing attacks against civilians or medical facilities would be committed in both States A and B. Therefore, the Court would have territorial jurisdiction over this offence if either of these States was a Party to the Statute or accepted the Court's jurisdiction on the basis of a declaration under article 12(3) of the Statute. The position is simply no different here than with a kinetic attack—if a ballistic missile was launched from the territory of State A at civilians on the territory of State B, the potential war crime would be committed in both of these States.[17]

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, seen here as an extension of the territoriality principle).

> For example, if a person aboard a civilian airliner, registered with State A, used the plane's wireless connection and launched a cyber attack against a hospital in State B as in the scenario above, the Court would have jurisdiction over the potential war crime if State A was a party to the Statute even if State B was not. Similarly, if an individual in the territory of State A launched a cyber operation that affected the navigational systems of a civilian airliner registered in State B, thus causing the plane to crash and killing hundreds of people on board, the potential war crime or crime against humanity of murder (assuming the contextual requirements were met) would be within the Court's jurisdiction if State B was a Party to the Statute, even if State A was not.

40. Furthermore, in both of the examples above, the Court would have jurisdiction on the basis of the nationality (active personality) principle even if neither States A or B were Parties to the Statute, but the offender was a national of State C, which was a Party to the

[16] The Office notes, however, that this would not apply *de minimis*. Relevant considerations might include the direct causal connection between the prohibited conduct and the result on a State's territory, and the gravity of the harm caused on that State's territory.

[17] *See also* Tallinn Manual 2.0, at 54-57; 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"). As defined in the Rome Statute, the war crimes of intentionally directing attacks against civilians or civilian objects are completed at the moment the attack is launched ('directed'), and do not require the attack to actually harm the targeted civilians or civilian objects.

Statute. By contrast, the nationality of the offender is irrelevant if the Court already has jurisdiction on the basis of the territoriality principle.[18]

41. In the view of the Office, the analysis of the territoriality principle above would equally cover situations in which the cyber conduct in question took place in the territory of more than two States simultaneously.[19] The use of cloud computing technology to commit or facilitate crimes under the Rome Statute may pose one such example.

42. 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.[20] Bearing in mind the carefully calibrated jurisdictional regime of the Rome Statute, and in the specific context of cyberspace, the Office does not presently anticipate that it would regard the mere transit of data through a State Party's territory as a sufficient basis to assert the Court's territorial jurisdiction.

43. In State practice, there is also substantial reliance on the so-called 'effects doctrine' as an extension of the territoriality principle, especially in the anti-trust context.[21] Arguments have been put forward in the literature that this doctrine could be particularly useful in establishing jurisdiction over cyber-enabled crimes.[22] The Office has considered the matter carefully, and is presently of the view that the territoriality principle as articulated in the Court's jurisprudence and applied to the cyber context above, appears to be sufficiently flexible to cover the great majority of situations involving cyber-enabled crimes likely to be of relevance to the Office. Therefore, it does not consider it necessary, at this time, to take a position on the effects doctrine and its potential applicability to cyber-enabled crimes within the subject-matter jurisdiction of the Court.

44. While crimes within the Court's jurisdiction can be committed by cyber means, the *facilitation* of (physical, kinetic or cyber) crimes by cyber means may be particularly likely. This raises the question of how the Court's territorial and personal jurisdiction framework

---

[18] *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.

[19] *See* *Tallinn Manual 2.0*, at 54.

[20] *Tallinn Manual 2.0*, at 54. 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.

[21] *See also* *Bangladesh/Myanmar* Article 15 Decision, paras. 56-57 (summarising the effects doctrine as allowing the assertion of "territorial jurisdiction if the crime takes place outside the State territory but produces effects within the territory of the State").

[22] *See e.g.* 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), at 820 (arguing that for "future investigation and possible prosecutions of cybercrimes, the Court will need to adopt an approach to territorial jurisdiction based upon effects"). *See further* K. Ambos, *Treatise on International Criminal Law, Volume III: International Criminal Procedure* (OUP, 2016), at 213-216. *See also* *Tallinn Manual 2.0*, at 57-60.

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 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.[23]

COMMITTING ROME STATUTE CRIMES BY CYBER MEANS

45. As noted above, the position of the Office is that all 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. 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.

46. While the following discussion will necessarily focus on the *actus reus* elements of relevant crimes, it would in each case also be necessary to establish the corresponding *mens rea* as required by the Statute.

Genocide (including direct and public incitement to genocide)

47. The crime of genocide, as defined in article 6 of the Statute and article II of the Genocide Convention, can be committed by cyber means. The main distinguishing feature of genocide—genocidal intent—is a mental element, which can therefore 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 postings 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.[24]

48. 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 critical infrastructure, including water and electricity supply, heating, medical facilities, or food production. 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. Similarly, digital technologies can be used as part of a programme of measures

[23] *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.
[24] *See* Council of Advisers' Report, at 74.

intended to prevent births within the group, or to forcibly transfer children from the group to another group.[25]

49. 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.[26] 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.

50. A more likely scenario for the standalone prosecution of cyber operators arises from the offence of direct and public incitement to genocide, as provided for in article 25(3)(e) of the Statute. This is an inchoate offence that does not itself require genocide actually to have been committed—or, if it was committed, for the act of direct and public incitement to have causally contributed to it.[27] 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 they were made, and provided that the statement(s) concerned was sufficiently direct.[28]

Crimes against humanity

Contextual elements

51. 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).[29] For the purpose of the contextual element of crimes against humanity, an attack simply means a course of conduct involving the multiple commission of acts referred to in article 7(1) of the Statute against any civilian population, pursuant to or in furtherance of a State or organizational policy.[30]

52. 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 as long as it is committed "as part of a widespread or systematic attack directed against any civilian population" and "pursuant to or in furtherance of a State or

[25] *See* Council of Advisers' Report, at 77-85.
[26] *See also e.g.* Elements of Crimes, art. 6(a), Element 4.
[27] In that respect, direct and public incitement to genocide should be distinguished from inducing or soliciting genocide, or any other crime within the Court's jurisdiction, as a form of responsibility for participation in the completed crime of another person: *see* Rome Statute, art. 25(3)(b). The actual commission of genocide as a result of any act of direct and public incitement would be taken into account in the Office's gravity assessment.
[28] *See* Council of Advisers' Report, at 86-88.
[29] These acts "need not constitute a military attack": Elements of Crimes, Introduction to Article 7, para. 3.
[30] Rome Statute, art. 7(2)(a).

organizational policy to commit such 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, if it was done as part of a wider attack meeting the threshold 'widespread' or 'systematic' criterion and other requirements.

53. 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."[31] 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 rebel or terrorist 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 corporations.[32]

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

55. The Office further notes that conduct in cyberspace may well be relevant in establishing the required policy to commit an article 7 attack.[33] 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."[34]

Examples of underlying crimes

56. Assuming the contextual elements are satisfied, almost all crimes against humanity in the Statute may potentially be committed by cyber means.[35] 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.

57. 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

[31] *See e.g.* *Prosecutor v. Ongwen*, Trial Judgment, ICC-02/04-01/15-1762-Red, 4 February 2021 ("*Ongwen* Trial Judgment"), para. 2677.
[32] *See also* Council of Advisers' Report, at 56-60.
[33] *See also* Council of Advisers' Report, at 53-56, 60-63.
[34] *See e.g.* *Ongwen* Trial Judgment, para. 2678.
[35] *See* Council of Advisers' Report, at 65-70.

hospitals, with this conduct resulting in death, and the perpetrator either intending to kill or being aware that death would occur in the ordinary course of events.

58. 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,"[36] 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."[37] 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.

59. 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 act referred to in this paragraph or any crime within the jurisdiction of the Court.[38] 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."[39] Conduct in cyberspace may readily 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.[40] For example, a particular ethnic and religious group may be subjected to a campaign of persecution, which, in part, involves the use of various techniques of mass electronic surveillance of every aspect of their daily lives. Likewise, conduct in cyberspace, such as social media postings, may also be relevant in establishing that the alleged perpetrator acted with the necessary discriminatory intent.

60. 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. Consequently, even if certain kinds of intentional cyber conduct causing serious harm to mental health were not considered to fall within the scope of other article 7(1) acts, they might still be captured by article 7(1)(k)—for example, the intentional 'hack and leak' of the most sensitive personal information, such as certain kinds of medical records (relating

[36] Elements of Crimes, article 7(1)(b), Element 1 n. 8.
[37] Rome Statute, article 7(2)(b).
[38] 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*, 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. 1208-1212; ICC OTP *Policy on the Crime of Gender Persecution*, paras. 56-58.
[39] Rome Statute, article 7(2)(g).
[40] *See also e.g. Al Hassan* Trial Judgment, para. 1201.

to inherently private topics such as psychological treatment, reproductive treatment, etc.) might well meet the threshold.

War crimes

Contextual elements

61. A cyber-enabled act that satisfies the conduct 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.[41] The conflict must have "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."[42] 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.

62. In the view of the Office, an armed conflict can, in principle, commence and be fought exclusively by using cyber means.[43] This depends on the commission of 'attacks,' as that term is understood in IHL, by cyber means – a point discussed further below. This may be the case more easily for international armed conflicts (IACs) rather than non-international armed conflicts (NIACs), since the former lack the intensity requirement inherent in the latter. In practice, however, both IACs and NIACs are more likely to be fought using a combination of kinetic and cyber means. Similarly, and probably more frequently, cyber means can be used in the context of a pre-existing armed conflict whose constitutive requirements are established purely kinetically.

Examples of underlying crimes

63. A number of war crimes in the Statute may be committed by cyber means. As noted above, the examples given below are again illustrative, and failing to mention a particular war crime does not preclude its possible commission by cyber means.

64. The applicable underlying rules of IHL, and the list of war crimes in the Statute, vary depending on the classification of the armed conflict as an IAC or a NIAC (although with significant overlaps). In principle, war crimes involving violations of IHL rules on the conduct of hostilities and the rules on the protection of persons in the power of the enemy can both be committed by cyber means.

65. Several war crimes relating to the conduct of hostilities require the existence of an 'attack.' 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)

[41] Elements of Crimes, article 8, chapeau.
[42] *See e.g.* *Situation in Afghanistan*, Judgment on the appeal against the decision on the authorisation of an investigation,' ICC-02/17-138 OA4, 5 March 2020, 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, para. 68.
[43] *See* *Tallinn Manual 2.0*, at 375-391; Council of Advisers' Report, at 30-36

(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)(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).

66. In the view of the Office, cyber operations can qualify as an 'attack' for the purpose of these and other war crimes requiring the existence of an attack.[44] 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,[45] with the requisite *mens rea*, the requirements of the war crime of intentionally directing attacks against civilians would be met.

67. Likewise, the Office further 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 objectives" alongside military objectives, rather than as a mere incidental harm.[46] 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.[47] 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 or individual civilians—for example, by the intentional use of a destructive, proliferating worm, which is capable of causing the requite degree of harm through its effects on a wide variety of different computer systems, without discrimination.[48]

68. The Office likewise considers that cyber operations whose (actual or potential) direct and indirect effects include physical damage to objects qualify as an 'attack' for the

[44] *See* *Tallinn Manual 2.0*, at 415-420; Council of Advisers' Report, at 37-39.
[45] *See e.g.* *Ongwen* Trial Judgment, para. 2760 (emphasis supplied); *Prosecutor v. Katanga*, Trial Judgment, ICC-01/04-01/07-3436-tENG, 7 March 2014 ("*Katanga* Trial Judgment"), para. 802.
[46] *See* *Katanga* Trial Judgment, para. 802; *Prosecutor v. Ntaganda*, Trial Judgment, ICC-01/04-02/06-2359, 8 July 2019 ("*Ntaganda* Trial Judgment"), para. 921. *See also* *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.
[47] *See* *Katanga* Trial Judgment, para. 802; *Ntaganda* Trial Judgment, para. 921.
[48] 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, at 43.

purpose of article 8(2)(b)(ii) (intentionally directing attacks against civilian objects). The Office is aware that the issue of so-called 'dual-use' objects has been the subject of much discussion in contemporary practice and scholarship, both in and outside the cyber context. The application of the principles of distinction and proportionality to such objects, or to the effects that targeting such objects might produce, can raise challenges. In the view of the Office, these will be fact-heavy assessments, on which it is difficult to pronounce in the abstract. However, it is clear that attacks (whether committed by cyber means or otherwise) that treat *as a single target* both civilian infrastructure *and* objects which qualify as a military objective may amount to indiscriminate attacks, 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.[49]

69. There is some debate as to whether cyber operations that only cause loss of functionality to computer systems can qualify as 'attacks.'[50] 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 scenario 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 position on this matter.

70. 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.[51] 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.

71. 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.

72. 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

[49] *See* *Tallinn Manual 2.0*, at 470; Council of Advisers' Report, at 43-44.
[50] *See* *Tallinn Manual 2.0*, at 417-418.
[51] *See* *Tallinn Manual 2.0*, at 436-437; Council of Advisers' Report, at 39.

NIACs pursuant to an amendment adopted in 2019.[52] Objects indispensable to survival include "foodstuffs, agricultural areas for the production of foodstuffs, crops, livestock, drinking water installations and supplies and irrigation works."[53] Cyber operations intended to disrupt the production of food or the supply of drinking water, or those targeting humanitarian agencies providing relief to the civilian population, may thus qualify as the war crime of starvation if those actions deprive the civilians of objects indispensable for their survival.[54] 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.

73. War crimes can also be committed by cyber means outside the context of the conduct of hostilities. For example, this may be the case with the war crime in articles 8(2)(b)(xxi) and 8(2)(c)(ii) (committing outrages upon personal dignity, in particular humiliating and degrading treatment). Publishing humiliating images of persons in captivity, or deceased persons, could potentially qualify in appropriate circumstances.

Aggression

74. Article 8bis(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 8bis(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 8bis(2) include invasion, military occupation, bombardment, and attack by the armed forces of one State against the armed forces of another.

75. 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.[55] 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 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.

76. 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. The leadership requirement largely does not pose issues that are

[52] The amendment was adopted pursuant to article 121(5) of the Rome Statute. To date, it has been ratified by 12 States.
[53] Additional Protocol II, art. 14.
[54] *See also* *Tallinn Manual 2.0*, at 531-533.
[55] *See* *Tallinn Manual 2.0*, at 330-337; Council of Advisers' Report, at 9-16.

unique to the cyber context. Similarly, the crime of aggression requires a predicate use of force between States. The cyber conduct of a non-State actor, such as a hacking group, can constitute such as use of force if the conduct of the non-State actor was attributable to a State. In other words, a State's act of aggression, by cyber means or otherwise, can be committed through a proxy non-State actor if a sufficient relationship of control can be shown.

77. Whether an act of aggression constitutes "a manifest violation of the Charter of the United Nations" is determined by its "character, gravity, and scale."[56] 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 set of acts, including those 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 cyber-enabled aspects of aggression in isolation.

Offences against the administration of justice

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

> (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.

79. 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

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

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.

80. The offence 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, 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 deep fakes. 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.

81. The commission of offences against the administration of justice by cyber means is more than a mere theoretical possibility. It is a real and present danger to the work of the Office and the Court as a whole, which has already been subjected to malicious cyber 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. In the same statement, the Registrar also drew attention to the risk of "disinformation campaigns targeting the ICC and its officials […] in an effort to tarnish the ICC image and delegitimize its activities."[57] 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.

FACILITATING ROME STATUTE CRIMES BY CYBER MEANS

82. 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 in the offence. 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.

83. 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; for contributing to a crime committed by a group of persons acting with a common purpose; and for attempting to commit a crime (an inchoate offence, rather than a form of responsibility). Thus, an individual can use cyber means to engage in conduct that could render them responsible on one of the bases above. An order can be communicated by means of digital communications technology, as can statements that amount to inducing or soliciting a crime. A crime, whether physical or cyber in character, can likewise be aided and abetted by cyber means—for example, a military unit engaged

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

in the killing of civilians can be assisted by cyber operators, who use methods of electronic surveillance to locate the intended victims. The same applies for common purpose crimes committed by a group. The Office also notes that it is entirely possible for crimes under the Statute 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.

84. While the Office charges those forms of responsibility that it considers most appropriate in a given case, in light of the evidence, it notes that the responsibility of accessories to crimes committed by groups acting with a common purpose under article 25(3)(d) of the Statute might be especially effective in prosecuting conduct facilitating cyber-enabled crimes, given their factual nature and the circumstances in which they may often be committed.

85. 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. In the view of the Office, consistent with the principles above, the underlying crime can be committed by cyber means.[58] For example, the commander of a military cyber unit can be held responsible as a superior for any cyber-enabled war crime or crime against humanity committed by his or her subordinates, if the *mens rea* requirements are met. Similarly, even for physical or kinetic crimes, cyber conduct may be probative, for instance, of the existence of a command relationship or of the superior's knowledge of the commission of the crime, as with various forms of digital communication.

86. 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.

87. The Office is also keenly aware of rapid developments in the field of artificial intelligence (AI), which may become relevant to issues of individual criminal responsibility under the Statute. On one end of the spectrum, AI may be used as a mere tool to commit such crimes. On the other end of the spectrum lies the potential development of artificial *general* intelligence (AGI) that can surpass human cognition and achieve a level of sentience, even personhood. Somewhere in the middle of that spectrum would be the use of various autonomous AI tools that produce effects that are not intended, or even foreseen, by those who designed or used them. While it will likely become necessary to address the question of crimes resulting from the use of such technologies, at the present stage the Office can only note that such cases before the Court would need to be resolved in accordance with the same principles as any other case including the requirement for *mens rea*. The provisions of the Statute on individual responsibility, especially article 30 (on the default mental elements of intent and knowledge) and article 32 (on mistakes of fact and law) would be particularly relevant in making prosecutorial decisions for crimes committed or facilitated through the use of AI.

[58] *See* Tallinn Manual 2.0, at 396-400.

PRINCIPLES

88. 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: working consistently; prioritising cases in accordance primarily with their gravity; investigating 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 cyber-enabled crimes.

Consistency

89. 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 environmental crimes[59]—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.

90. It follows from this that the conduct addressed in this policy—cyber-enabled crimes—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.

Objectivity and diligence

91. 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.[60]

92. Conduct in cyberspace provides a means of perpetrating, facilitating, or proving crimes under the Statute. As a consequence, and increasingly so as time passes, many investigations carried out by the Office will have a cyber dimension in some form. This is irrespective of whether cyber conduct may itself form the basis of criminal charges (either carrying out an article 5 or article 70 crime, or facilitating such acts by another person), or whether it merely helps prove charges which arise from purely kinetic conduct.

[59] *See e.g.* ICC OTP *Policy on Gender-Based Crimes* (2023); *Policy on Children* (2023); *Policy on Slavery Crimes* (2024). The Office also intends to launch its policy on environmental crimes in 2025.
[60] Rome Statute, art. 54.

93. 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. It will also seek to charge cyber-enabled conduct as a crime under the Statute when appropriate.

Gravity, impact, and practicality

94. The premise behind 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.

95. The Office has previously explained how it selects and prioritises cases for investigation and, where appropriate, prosecution.[61] In this regard, one key consideration is the gravity of the alleged conduct, having regard to all the relevant circumstances.[62] 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.[63] 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.

96. Cyber-enabled crimes under the Statute will be investigated and, where appropriate, prosecuted, according to these 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.

97. The Office will assess the gravity of cases concerning cyber-enabled crimes in accordance with the standard criteria used by the Court, including the scale, impact, factual nature, and manner of commission of the relevant criminal acts.[64] In this context, the Office will take account of the potential for some categories of victims to be disproportionately affected by such crimes.[65] It will also have due regard to second-order and 'spill-over' effects, including on critical services and infrastructure. 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.

[61] *See* ICC OTP, *Policy on Case Selection and Prioritisation*.
[62] 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.
[63] *See* ICC OTP, *Policy on Case Selection and Prioritisation*, paras. 42-44.
[64] *See e.g.* ICC OTP, *Policy on Case Selection and Prioritisation*; ICC OTP, *Policy on Situation Completion*.
[65] *See also below* para. 129.

Partnership and vigilance

98. 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.[66] 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.

99. As set out in more detail below, improved 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 law applies equally in this domain, as in any other.

100. The Office will maintain and develop existing partnerships, and build new partnerships, to meet these requirements. Where possible, 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

101. 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.

102. The Office will adapt its institutional structures as necessary and feasible for this purpose, and carry out the necessary capacity-building and training activities. 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.

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

103. 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

104. The primary expertise of the Office lies in carrying out complex investigations and prosecutions concerning alleged crimes under the Statute. 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 exercise of their mandate as guaranteed and required by article 42 of the Statute.

105. The Office has already appointed a special adviser to the Prosecutor, with a portfolio for cyber-enabled crimes, 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 strategic advice in this area from leading experts, including from the private sector, through appropriate institutional structures. The Office may also commission specific advice from approved third party providers, including on a *pro bono* or commercial basis as necessary.

106. 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), and all-source analysis (the Information Fusion Centre). Specific expertise in the investigation and prosecution of cyber-enabled crimes will be developed and integrated within these existing structures as required.

Capacity-building and training

107. The Office recognises the need to 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. It 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 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).

108. 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.

109. 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

110. 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.[67] Where there is a 'reasonable basis to proceed', the preliminary examination will be resolved in favour of investigation.[68]

111. 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.

112. 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.

113. 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, however, 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, including from the private sector, under article 15(1) of the Statute.

114. In carrying out preliminary examinations in which cyber-enabled crimes under the Statute may allegedly have occurred, the Office will as appropriate seek additional information from States, organs of the United Nations, intergovernmental and non-governmental organisations, and/or other reliable sources, including from the private

[67] *See above* paras. 30-34.

[68] Specifically, 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, arts. 15(3), 53(1); ICC RPE, rule 48.

sector.[69] 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.[70]

Investigations

115. 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 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.

116. 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.[71] 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.

117. 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.[72] 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.

118. 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.[73] 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.[74]

119. Importantly, while the Office investigates each situation within its jurisdiction with a view to prosecuting at least one case before the Court,[75] this is not to the exclusion of other prosecutorial and non-prosecutorial outcomes which may serve to deter or to disrupt

[69] ICC RPE, rule 104(2).
[70] *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,' 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. 125-126.
[71] *See above* paras. 10, 21-27, 45-86.
[72] *See also* ICC OTP, *Policy on Case Selection and Prioritisation*.
[73] *See above e.g.* paras. 34, 94-97.
[74] *See* ICC OTP, *Policy on Situation Completion*, para. 21.
[75] *See* ICC OTP, *Policy on Situation Completion*, para. 20.

crimes under the Statute, or to mitigate the harm caused.[76] 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.

120. To carry out effective investigations into cyber-enabled crimes, the Office will actively cooperate with external partners, including those with access to 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.[77]

121. 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

122. 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.

123. 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.[78]

Accessing relevant evidence

124. The Office will seek to rely on diverse and innovative sources of 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

[76] *See further below* paras. 137-138.
[77] Rome Statute, art. 93(10).
[78] *See also above* paras. 107-108.

of evidence, broadly conceived, will likely remain relevant in establishing individual criminal responsibility more broadly.

125. 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.[79] In accordance with the provisions of their national law, States Parties are required to provide such assistance, including by executing measures to compel private 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.

126. 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. Accordingly, the Office will not only consider requests for voluntary measures to preserve evidence during the preliminary examination,[80] but will also take such measures when warranted during its investigation—including where permitted on a compulsory basis.[81] In this context, as necessary, the Office will also seek the assistance of the Court in relation to unique investigative opportunities.[82] Intentional measures to destroy, tamper with, or interfere with the collection of evidence by the Office constitute an offence against the administration of justice, regardless of motive, and may be prosecuted as such.[83]

127. 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.[84] While recognising legitimate interests of national security, the Office will seek to resolve any such issues arising in cooperation with concerned States.[85]

128. 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.

---

[79] Rome Statute, art. 93(1).
[80] *See above* para. 114.
[81] Rome Statute, art. 93(1)(j).
[82] Rome Statute, art. 56.
[83] Rome Statute, art. 70(1)(c). *See also* Rome Statute, art. 30; *Prosecutor v. Bemba et al.*, Judgment on the appeals of Mr Jean-Pierre Bemba Gombo, Mr Aimé Kilolo Musamba, Mr Jean-Jaques Mangenda Kabongo, Mr Fidèle Babala Wandu and Mr Narcisse Arido against the decision of Trial Chamber VII entitled 'Judgment pursuant to Article 74 of the Statute', ICC-01/05-01/13-2275-Red A A2 A3 A4 A5, 8 March 2018, para. 738 (affirming that the mental element required is that the perpetrator "meant" to engage in the relevant conduct).
[84] Rome Statute, art. 54(3)(e), (f).
[85] Rome Statute, arts. 72-73, 93, 97, 99.

129. 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

130. The Office has already stated its intention to seek to expand its participation, where appropriate, in joint investigations.[86] 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[87]—now also including the Ljubljana-Hague Convention on International Cooperation in Investigating International Crimes,[88] the Second Additional Protocol to the Budapest Convention on Cybercrime,[89] and the UN Convention against Cybercrime.[90]

131. The Office recognises that cyber-enabled crimes under the Statute 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. By participating in joint investigations where appropriate, the Office may in particular help secure tangible results in disrupting ongoing cyber-enabled crimes under the Statute, and reducing their harmful consequences.

Suspected offences against the administration of justice at the Court

132. 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.[91] The Office will prioritise such investigations especially in circumstances where the IT infrastructure of the Court itself has been materially affected.

133. 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."[92] The Office

[86] *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).
[87] 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).
[88] *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.
[89] *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, art. 12.
[90] *United Nations Convention against Cybercrime*, art. 48.
[91] ICC RPE, rule 165(1).
[92] Rome Statute, art. 70(2). *See also* ICC RPE, rule 167.

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.

134. 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.[93] 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,[94] 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

135. 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.[95]

136. 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.[96]

137. 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, the Office will also consider adopting measures to disrupt such conduct or mitigate the resulting harm.

138. 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').[97] 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 of the proceeds of crimes, and all property and assets of suspects, for the purpose of eventual forfeiture.[98]

---

[93] Rome Statute, art. 70(4); ICC RPE, rule 162.
[94] Rome Statute, art. 70(4).
[95] *See e.g.* ICC OTP, *Policy on Situation Completion*, para. 35.
[96] Where necessary in such circumstances, a waiver of the rule of speciality may be requested from a surrendering State: Rome Statute, art. 101.
[97] Rome Statute, art. 93(1)(k).
[98] 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).

139. In presenting cases of cyber-enabled crimes at trial, 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

140. The Office incorporates considerations of cooperation and complementarity into each stage of its proceedings as described above. Given the particular significance of these principles in responding effectively to cyber-enabled crimes under the Statute, however, some further general matters are set out with regard to cooperation with States Parties under the Statute, the possibility of enhanced cooperation by States, and cooperation with the private sector.

Cooperation with States Parties under the Statute

141. 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.

142. 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.

143. 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.

Enhanced cooperation by States and organisations in providing access to evidence

144. States and organisations 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.[99]

145. 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

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

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.

146. 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.

Cooperation with private sector entities and non-governmental organisations

147. 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.[100] The Office understands this to include private entities, such as corporations and non-governmental organisations. Recognising the unique role that such institutions may play in the management and evolution of cyberspace, the Office will explore avenues for enhancing direct cooperation with them on matters of mutual interest.

WAY FORWARD

148. 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.

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