COMMENTS ON THE DRAFT POLICY ON CYBER-ENABLED CRIMES UNDER THE ROME STATUTE

30 May 2025

As armed conflicts increasingly extend into the digital space and freedom of expression and digital rights violations enable the commission of atrocities, ARTICLE 19 has consistently called on international courts and accountability mechanisms, including the International Criminal Court (the ICC or Court), to address the role these violations play in the commission of international crimes. We therefore welcome the Office of the Prosecutor's (OTP or Office) policy initiative to advance accountability for cyber-enabled crimes under the Rome Statute and appreciate the opportunity to contribute to its development through the open consultation process.

While there is broad agreement that international law applies to cyberspace, views differ on what this means in practice. There is also limited case law directly connecting and authoritatively interpreting conduct in cyberspace in relation to the commission or facilitation of international crimes. At this critical juncture, the OTP's draft cyber-policy (the Draft Policy) presents an important opportunity to advance these discussions, to strengthen accountability for cyber-enabled crimes committed by State and non-State actors alike, and to do so in a manner that will protect those affected from digital harms.

At the same time, ARTICLE 19 emphasises that the task before the ICC is a challenging one – not only because cybercrimes are notoriously hard to prosecute but also because of the need to avoid unintended consequences. Many recent responses adopted in the name of combatting cybercrimes - including with respect to data collection and evidence-sharing practices - have breached international human rights standards, frequently targeting journalists and human rights defenders who are essential in gathering information and preserving evidence relevant to the work of the OTP and drawing public attention to potential violations of international criminal law. The recently negotiated UN Convention against Cybercrime – referenced in the Draft Policy – has been widely criticised by ARTICLE 19 and other human rights organisations, and was described as a "A Trojan Horse For Transnational Repression" by former UN Special Rapporteur on Freedom of Expression, David Kaye.

The ICC, and the OTP specifically, will have to carefully navigate these complexities. Embedding strong human rights safeguards throughout the development and implementation of the Draft Policy will be of paramount importance.

Against this backdrop, and drawing on ARTICLE 19's recent policy paper on freedom of expression in armed conflict, we offer the following comments aimed at strengthening the Draft Policy.

1. **Enhancing the focus on digital rights violations**

The ICC is uniquely positioned to influence how international law, including international humanitarian law, is interpreted and applied in cyberspace. While this will primarily depend on case law, the Draft

Policy also has significant potential – well before any specific case is brought before the Court – in clarifying how digital rights and freedom of expression violations may amount or contribute to international crimes and, we believe, should focus more on this specific aspect.

The Draft Policy would benefit from increased reference to attacks on ICT infrastructure and in particular the shutting down of communication networks. Today, people's reliance on ICT – and in particular access to information - is unprecedented. UN Special Rapporteur on Freedom of Expression, Irene Khan, described the right to access information in times of crises and armed conflict as a 'survival right' on which people's lives, health, safety, security and dignity depend. In the context of armed conflicts, a resolution adopted at the 34th International Conference of the Red Cross and Red Crescent recognised that modern societies rely heavily on ICT infrastructure for communications and for the provision of essential services such as education and health care. Indeed, as highlighted by the UN Human Rights Council, both hospitals and humanitarian organisations - which enjoy specific protections under international humanitarian law - depend on functioning ICT infrastructure, and internet shutdowns can threaten the delivery of humanitarian aid. Civilians increasingly depend on functioning communication technologies for their emotional well-being.

We therefore suggest that cyber attacks that result in the shutting down of communication networks be added to the list of examples mentioned in the sections of the Draft Policy covering substantive crimes under the Rome Statute - for example on genocide (paragraph 48); crimes against humanity (paragraphs 57 and 58); and war crimes (paragraph 66 and 72). We also suggest that the section on war crimes (in paragraph 66) state that cyber operations qualifying as attacks include those whose direct and indirect effects include serious illness and severe mental suffering (in line with the suggested understanding of injury in the Tallinn Manual, Rule 92).

In the context of dual-use objects (paragraph 68), we believe that additional wording could be added to better highlight the relevance of the principle of proportionality. According to the 2021 Council of Advisers' Report on the Application of the Rome Statute of the International Criminal Court to Cyberwarfare (Council of Advisers' Report) "the requirement that cyber operations adhere to the principle of proportionality helps to offset the limitations of the principle of distinction […] and requiring that incidental civilian harm expected to be caused by an attack on a dual-use system or network must not be excessive to the anticipated military advantage, creates a potentially important outer limit for cyber operations". We suggest the Draft Policy should also reflect this – including with reference to Article 8(2)(b)(iv) of the Rome Statute – and state that "it is also clear that even where it is not possible to isolate and target only the military objective, an attack could still amount to a disproportionate attack if it results in excessive incidental civilian harm".

We welcome the Draft Policy's recognition (paragraph 24) that "often cyber conduct may be correlated with the commission of a crime within the jurisdiction of the Court and can be probative of the suspect's crime. For example, conduct in cyber space might aim at concealing evidence of a crime which has already been committed". However, we submit that the issue extends beyond the concealing of specific evidence. Extremely restrictive information environment marked by repression (including through online harassment, internet shutdowns and surveillance) are often designed to hinder the free flow of information about atrocity crimes, thereby contributing towards an environment of impunity where atrocities proliferate. We therefore invite the Office to add that "systematic freedom of expression and digital rights violations targeting journalist, human rights defenders and communities impacted by potential crimes under the Rome Statute means that often information cannot be collected and evidence not be produced in the first place".

In addition, we invite the Office to state in the Draft Policy that such measures could:

- give rise to liability for the crimes they are intended to conceal (at least under Article 25(3)(d) of the Statute; although many of these measures will not happen after the commission of the crime, it is noteworthy that Article 25(3)(d) has held by Pre-Trial Chamber in *Prosecutor v. Callixte Mbarushimana*, Decision on the confirmation of the charges to be able to cover *ex post facto* contributions if they were part of a common plan prior to the perpetration of the crime); and
- be evidence of the chapeau elements of crimes against humanity. The *Decision on the Prosecutor's Application Pursuant to Article 58 as to Muammar Mohammed Abu Minyar GADDAFI, Saif Al-Islam GADDAFI and Abdullah AL- SENUSSI* is highly instructive in this context – to find that there were reasonable grounds to believe that there was a State policy to commit a widespread and systematic attack, the Pre-Trial Chamber factored in: targeting journalists to prevent them for reporting events, and punishing them from having done so; repeatedly blocking satellite transmission of channels such as Al-Jazeera and Al-Hurra and disrupting internet and telecommunications services and confiscating laptops, cameras, mobile phones SD and SIM cards from persons stopped at checkpoints. The court also relied on the use and control of various communication media, the monitoring of emails and the blocking of various internet and international television channels to infer the existence of a coordinated plan to commit crimes against humanity. While not all such actions fall within the scope of the Draft Policy, it is easy to see how conduct in cyberspace could have the equivalent effect.

Finally, we welcome that the Draft Policy recognises in paragraph 26 that certain forms of "intrusive electronic surveillance" could potentially amount to the actus reus of a crime under the Statute such as persecution under article 7(1)(h) – we would welcome an addition that this may include in particular "biometric and AI-enabled surveillance".

2. Embedding human rights-based considerations throughout the Draft Policy

As mentioned in the introductory remarks, ARTICLE 19 believes it is crucial that human rights considerations are embedded throughout the development and implementation of the Draft Policy.

We welcome the Draft Policy's explicit reference to the fact that Article 21(3) of the Rome Statute "mandates that both the application and interpretation of the Statute must be consistent with internationally recognised human rights" and that "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, and the right to participate in public affairs".

We encourage the OTP to expand on this point and reflect the fact that international human rights bodies and courts have developed substantial practice allowing for a more advanced understanding of how human rights apply in the digital space than currently exists in international criminal law. This should inform the interpretation of the crimes under the Statute. For example, "cyber torture" as described by the former UN Special Rapporteur on Torture, Nils Melzer, is referenced among conduct that could qualify as a crime against humanity in the 2021 Council of Advisers' Report. Beyond interpretation of the substantive crimes, human rights considerations should also guide the OTP's

relationships with different stakeholders, including their cooperation with state parties or private entities. This is particularly important in the context of the Draft Policy given the mentioned human rights risks associated with domestic and international instruments dealing with cybercrimes.

More specifically, we recommend:

- To add to paragraph 32: "The Office may, for example, consider international human rights law and the practice of international human rights institutions, tribunals, and courts, when interpreting the elements of certain crimes under the statute, or when addressing procedural questions, including in the cooperation with State Parties and the private sector."

- To distinguish more clearly throughout the Draft Policy between cyber-enabled crimes under the Rome Statute and other cyber-enabled offences that fall outside this scope. The separate codification under domestic law of offences that are "cyber-enabled" rather than "cyber-dependent" raises serious human rights concerns, often criminalising protected forms of speech and granting authorities far-reaching investigatory powers without adequate procedural safeguards. We also recommend removing broad references to the OTP "supporting national efforts to address unlawful and harmful uses of cyberspace more broadly" given the human rights risks associated with tackling the vague concept of "harmful" uses of cyberspace in a regulatory and criminal context. Overall, related to the point just above, we invite the OTP to explicitly state in the section on "Cooperation and Complementarity" that "any cooperation with domestic law enforcement authorities – as well as private entities – will be subject to human rights due diligence and all necessary steps will be taken to protect the rights of affected parties". This seems essential to ensure that the OTP does not inadvertently support investigative practices that violate human rights standards.

- To expand the references to cooperation with civil society organisations (paragraphs 3 and 14) to emphasise that their role will not be limited "to support[ing] law enforcement action" but also "to ensuring that human rights considerations permeate all aspects of the OTP's implementation of the policy and throughout investigative and prosecutorial processes. This includes engagement to strengthen the OTP's understanding of the implications of cyber operations on affected communities and their human rights and support efforts to avoid any negative human rights consequences of its investigations, including those arising from cooperations with State actors and private entities".

- Remove any suggestion, in the context of Article 70 of the Statute (Offences against the administration of justice), that the OTP might investigate or prosecute "disinformation campaigns" or other conduct that could "undermine the court's mandate". While it is possible that similar conduct could fall under Article 70 of the Statute, the concept of 'disinformation' is too broad to make it subject to any investigation, covers speech that must be protected under freedom of expression standards and risks being conflated with criticism or opposition to the Court. Generally speaking, any expression-related conduct should only be investigated by the ICC in a manner consistent with the principles of legality, legitimacy, necessity and proportionality required under Article 19 of the International Covenant on Civil and Political Rights.

3. Reflecting the increasingly central role of corporate actors

In its current form, the Draft Policy primarily refers to private entities in the context of potential cooperation with investigations (see, e.g., paragraph 125). We recommend that the Draft Policy also reflect the increasingly central role of corporate actors in the facilitation and commission of cyber-enabled crimes under the Rome Statute. Technology companies often manage and secure the digital infrastructure at the core of the conduct addressed by the Draft Policy, whether through providing cloud computing infrastructure, telecommunications equipment enabling mass surveillance, or data analytics and AI technology used to support military operations. There is growing attention on the responsibilities of technology companies in armed conflict to respect international human rights and humanitarian law as articulated in the UN Guiding Principles on Business and Human Rights. The Draft Policy should explicitly reflect these developments and acknowledge the responsibilities of the private sector under international human rights and humanitarian law.

We note that the OTP's draft policy on environmental crimes – also currently under development - references corporate actors more explicitly, recognising their prominent role in acts that have harmed the environment. For the reasons outlined, we believe that technology companies should be similarly addressed in the Draft Policy. Without a focus on private entities, the OTP will not be able to effectively respond to the challenges of addressing cyber-enabled crimes under the Rome Statute. The OTP should consider transposing relevant language from the draft policy on environmental crimes to ensure a consistent approach to the role of corporate actors under the Rome Statute.

This includes adding to the objectives of the Draft Policy "to engage with corporate and other private actors in order to put them on notice of legal risks related to the provision of technology services that may enable conduct covered by this policy"; and to its jurisdiction chapter "in terms of personal jurisdiction, although the Office cannot bring charges for cyber-enabled crimes against a corporation on the basis of its legal personhood because the Statute limits the Court's jurisdiction to natural persons, it can prosecute individual corporate officers who satisfy the requirements of territorial or nationality jurisdiction and are personally responsible for the commission of a cyber-enabled crime pursuant to articles 25 or 28 of the Statute". In a similar vein, we would also welcome language clarifying that "if cyber-enabled crimes are committed through corporate structures, senior corporate officers may potentially qualify as non-military superiors for purposes of article 28(b)." We also recommend incorporating paragraphs 94 and 95 from the draft policy on environmental crimes (Engaging with Corporate and other Private Actors), adapted to the cyber-context.