

Submission in relation to the ICC Office of the Prosecutor's public consultation on policy on cyber-enabled crimes under the Rome Statute

29 May 2025

Office of the Prosecutor | International Criminal Court
Po Box 19519
2500 CM, The Hague
The Netherlands

By email only: otp.cyber.policy@icc-cpi.int

Contact: Timothy Roberts

President, NSW Young Lawyers

Jessica Lighton

Submissions Lead, NSW Young Lawyers

Caity Suchanow

Sub-Committee Chair, NSW Young Lawyers

Contributors: Liam Cross, Jack Dennis, Caity Suchanow, Chloe Saker, Stephanie Douvos, Dheeraj Siji Shibu, James Glissan, Francis Patag, Hannah Stacey, and Ahmad Akram.

The NSW Young Lawyers International Law Sub-Committee (**Sub-Committee**) makes the following submission in response to the ICC Office of the Prosecutor's public consultation on policy on cyber-enabled crimes under the Rome Statute.

NSW Young Lawyers

NSW Young Lawyers is a Committee of the Law Society of New South Wales that represents the Law Society and its members on issues and opportunities arising in relation to young lawyers i.e. those within their first five years of practice or up to 36 years of age. Through its 15 sub-committees, each dedicated to a substantive area of law, NSW Young Lawyers supports practitioners in their professional and career development by giving them the opportunity to expand their knowledge, advance their career and contribute to the profession and community.

The Sub-Committee comprises a group of volunteers and subscribers interested in international affairs and international law (both public and private). Overall, the Sub-Committee seeks to provide a supportive environment for law students and early career lawyers to advance their career in international law and foster valuable professional and personal relationships.

Introduction

1. The NSW Young Lawyers International Law Sub-Committee (**the Sub-Committee**) welcomes the opportunity to make the following submission to the Office of the Prosecutor (**Office**) of the International Criminal Court (**the Court**) regarding its draft policy on cyber-enabled crimes under the Rome Statute (**Draft Policy**).
2. In this submission, the Sub-Committee identifies legal issues which the Sub-Committee respectfully encourages the Office to consider when appraising the Draft Policy.

3. The Sub-Committee commends the Office for the development of this important piece of jurisprudence. The following submission addresses open questions in the Draft Policy in relation to the Court's jurisdiction and identifies areas for further consideration before the finalisation and implementation of the policy.

Summary of submissions

4. In this submission, the Sub-Committee reviews certain aspects of the Draft Policy and explores important gaps.
5. In short, the Sub-Committee:
 - a. Requests clearer jurisdictional standards (**Section A**);
 - b. Supports the need and reliance of the Office on the personality principle (**Section B**);
 - c. Requests further guidance on accessorial liability in cyber-enabled contexts (**Section C**) concerning within the Draft Policy;
 - d. Underlines the need to be vigilant in recognising that gravity in cyber-enabled contexts may manifest differently, but no less seriously, than traditional contexts (**Section D**);
 - e. Discusses the prevalence of cyber-enabled slavery crimes and highlights the importance of the Office and Court collaborating with stakeholders (**Section E**); and
 - f. Requests the Office to develop cyber evidence protocols to protect against integrity risks with respect to digital evidence of cyber-enabled crime (**Section F**).
6. As cyber-enabled operations continue to evolve, so too must our understanding of how international criminal law engages with this new terrain. The following Sections will explore additional legal and practical considerations shaping the ICC's approach to emerging technologies.

A - Jurisdiction: Territoriality

7. Generally speaking, the territorial principle under international law provides that States can exercise exclusive jurisdiction over individuals and legal entities within their territory. Within the

context of the Court, that principle is expressed in Article 12(2)(a)¹ of the Rome Statute which states that the Court has jurisdiction over conduct that occurs within the territory of a State Party.

8. The current application of jurisdiction is grounded in where the conduct or result of a crime takes place - yet cyber operations challenge these physical anchors. Unlike traditional forms of warfare, cyberattacks often transcend national borders in milliseconds, involving actors, infrastructure, and victims dispersed across multiple jurisdictions. This fragmentation complicates the application of the ICC's territorial jurisdiction and calls for a more nuanced approach to establishing a sufficient connection to a State Party's territory.
9. Regarding the applicability of territorial jurisdiction in the context of cyber-enabled crimes, a key question arises in situations where there is only a minimal connection between the alleged conduct and cyber infrastructure on a State's territory. For example, situations where data is transmitted through cables or servers located in territory of a State Party.
10. The Office's current proposed position under the Draft Policy is that it "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."²
11. This view is supported by laws and customs of war. In particular, Article 8 of the Hague Conventions on Laws and Customs of War on Land provides that neutral States need not "forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals" as long as they permit the use of their telecommunications infrastructure impartially.³

¹ *Rome Statute of the International Criminal Court*, opened for signature 17 July 1998, 2187 UNTS 90 (entered into force 1 July 2002) art 12(2)(a) ('Rome Statute').

² Office of the Prosecutor, *Policy on Cyber-Enabled Crimes: For Public Consultation* (International Criminal Court, March 2025) 250306-OTP-Policy-on-Cyber-Enabled-Crimes-for-public-consultation.pdf at 42 ('Draft Policy').

³ *Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land* (entered into force 26 January 1910) art 8.

12. Conversely, some scholars have suggested that this exception should not apply to war crimes facilitated by the internet given the nature and severity of cyberwarfare.⁴
13. For example, a malware or a distributed denial of service (**DDOS**) attack sent from State A to attack civilian infrastructure in State B which routed through servers in State C ought to be viewed differently than in a situation where State A simply communicated troop movements to their combatants in State B using the same transmission route. This is because such malware or DDOS attack can result in significant and severe civilian harm and may politically implicate State C in the harm caused.
14. However, two issues arise in this context:
- a. As noted by the Office, there is disagreement as to whether the territoriality principle can be applied when there is only a 'minimal connection' with a State Party's cyber infrastructure. The term 'minimal connection' is not defined beyond the mere transmission of data; nor is there clarity regarding the criteria the Prosecutor will use to assess whether a connection is 'minimal'; and
 - b. The extent of States' obligations in such contexts. In other words, at what point will State C be seen to have facilitated the crime?
15. Both these issues are explored further below.

Issue 1: Minimal Connection

16. We respectfully submit that further clarification is needed as to whether certain critical aspects of cyber-enabled crimes alone would amount to 'minimal connection' sufficient to ground the Court's jurisdiction. These include:
- a. if servers are merely located in a State Party territory;
 - b. if a State Party is the routed territory of a Virtual Private Network (**VPN**); and
 - c. where 'zombie computers' are used in a State Party's territory.

⁴ See e.g. Michael Gervais, 'Cyber Attacks and the Laws of War' (2012) 30(2) *Berkeley Journal of International Law* 92.

17. Clarification may also assist where a group of individuals, dispersed in various global locations, are operating simultaneously to facilitate cyber-enabled crimes.
18. The Court adopted a broad interpretation of the territoriality principle in the Situation in Bangladesh/Myanmar, *Decision pursuant to article 15 of the Rome Statute on the authorisation of an investigation*,⁵ where territorial jurisdiction was considered to apply when ‘at least part of the conduct (i.e. the actus reus of the crime) [took] place in the territory of a State Party’.⁶
19. Given this precedent, it is arguable that the Court has jurisdiction even where only the servers, ‘zombie computers’, or VPN servers/service providers are within the territory of a State Party. If so, it is further arguable that the Court will have jurisdiction over the conduct even if the perpetrator(s) or the victim(s) are not located in a State Party.
20. Victor Tsilonis suggests an alternative approach: the ubiquity principle.⁷ The ubiquity principle states that, under customary international law, state jurisdiction over a crime can be established if part of the crime (whether the criminal conduct or the consequences) occurred within its territory even if that part is not a constitutive element of the crime. Within the context of the Rome Statute, the Court found that State Parties transferred territorial jurisdiction to the Court.⁸ Therefore, pursuant to the ubiquity principle, the Court would have jurisdiction under Article 12(2)(a) if at least part of the conduct took place within the territory of a State Party.⁹
21. Consider the following example:
- A group of hackers are based in multiple locations (States A and B);
 - The hackers are using ‘zombie computers’ located in States C and D;
 - The hackers are also using VPNs through service providers and servers located in State E; and
 - The hackers attack civilian infrastructure and hospitals in State F.

⁵ 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 (‘Situation in Bangladesh/Myanmar’).

⁶ Ibid 61; see also 43.

⁷ Victor Tsilonis, *The Jurisdiction of the International Criminal Court* (Springer, 2nd ed, 2024) 332-336.

⁸ Situation in Bangladesh/Myanmar (n 5) 60.

⁹ Ibid 58-62.

22. By employing the ubiquity principle, Tsilonis argues that that the place of the crime will be States A and B (i.e. the States linked to the group's physical location and operations), States C and D (being the States where the 'zombie computers' are located), State E (being the state where the VPN servers are located, or service provider is incorporated), and State F (being the victim state). The Court will have jurisdiction over the conduct if any one of those States are signatories to the Rome Statute.
23. Irrespective of which side of the territorial principal versus ubiquity principle debate the Office falls on, there needs to be further clarity surrounding what factors the Office views as being indicative of a "sufficient" territorial connection to ground the Court's jurisdiction under Article 12(2)(a).¹⁰ As noted by Michael Gervais, the 'traditional conceptions of "battlefield" or "Zone of Conflict" do not translate well into the cyber realm', which lacks the geographical fixture that underpins much of international humanitarian law. The reliance on physical effects or territorial anchors in jurisdictional reasoning is increasingly strained in cyber contexts, where harmful consequences may manifest far from the source of the attack or in multiple locations simultaneously.¹¹
24. The Draft Policy properly acknowledges the potential risks of overreach if the Court asserts jurisdiction based solely on minimal or incidental territorial links but stops short of providing such indicative factors. The Sub-Committee submits that providing a non-exhaustive list of key factors and hypotheticals would offer further clarity of international criminal law and State responsibilities, and better align the current order with the *nullum crimen sine lege* principle.
25. Relevant factors might include:
- a. The significance and centrality of cyber infrastructure (e.g., servers, data centres, zombie computers, etc.) located in the State Party;
 - b. The degree to which the criminal conduct or its harmful effects are experienced within that territory; and
 - c. The extent of the State's response, including any preventative or remedial action undertaken by domestic authorities.

¹⁰ Rome Statute (n 1) art 12(2)(a).

¹¹ Gervais (n 4) 544.

26. The second suggested factor bears further consideration. Where multiple States are affected by a cyber-enabled crime, a key question emerges regarding what level of harm (if any) is sufficient to enliven the Court's jurisdiction. Does even a modest degree of impact in a single State Party suffice to establish jurisdiction, or must a specific threshold be met? If a threshold is required, can it be satisfied collectively across all affected States and would they all need to be State Parties? For instance, if a cyberattack causes consequences in ten States but only one is a State Party, would that be enough to ground jurisdiction if the impact in that single State Party would not meet the threshold on its own, but the cumulative effects across all ten would? The Court's preliminary view seems to suggest that it would.¹²
27. In the Comoros situation, it was reiterated that conduct and decisions made outside of the jurisdiction of the Court can be taken into account when determining the gravity analysis, with the Office supporting the decision of the Pre-Trial Chamber and subsequently developed a test to ensure that extra-jurisdictional conduct was rationally and adequately linked to the crimes that are within the jurisdiction to be considered.¹³
28. The Draft Policy at paragraphs [36]-[38]¹⁴ suggests that jurisdiction may be triggered when harmful effects manifest within a State Party's territory. However, it does not yet clarify the threshold for this connection between jurisdiction and harm, or provide indicative factors related specifically to harm. For example, whether the mere presence of victims in a State Party is sufficient.

Issue 2: State Responsibilities

29. As to the issue of State Responsibility, clarity is needed as to what is expected from States to prevent crimes under the Rome Statute and manage their liabilities.
30. Michael Gervais argues that it is impractical to require neutral States to prevent cyberattacks from originating or transmitting through their territory given that:

¹² Jennifer Trahan, 'The Criminalisation of Cyber-Operations Under the Rome Statute' (2021) 19 *Journal of International Criminal Justice* 1148.

¹³ Ibid 1149; 'Application for Judicial Review by the Government of the Comoros', *Situation on Registered Vessels of the Union of the Comoros et al.* (ICC-01/13-111), Pre-Trial Chamber I, 16 September 2020.

¹⁴ Draft Policy (n 2).

- a. The nature of information technology and cable transmission means that information will take the shortest route to reach its destination; and
- b. It is impossible to predict which route information will take to reach its destination.¹⁵

31. Imposing such a requirement would require a State to sever all internet connections to maintain neutrality. Therefore, Gervais argues for the adoption of the 'means at its disposal' test or an 'intent-based view'.¹⁶

- a. Under the 'means at its disposal' test, a State would only need to use the means at its disposal to prevent cyber-related conduct being transmitted through its cyber infrastructure. This could mean engaging domestic law enforcement or collaborating with other States to prevent individuals from engaging in conduct within their territory or taking down 'zombie computers' within their territory.
- b. Under the 'intent-based view', States would have a duty to not knowingly allow their territory to be used for criminal conduct. Practically, this would mean that a State would not be held responsible for unintentionally allowing cyber-related conduct in its jurisdiction but will be required to take action if and when put on notice.

32. It is beyond the scope of this submission to recommend one test over the other or advise on the practical outcomes of the respective tests. However, the Sub-Committee notes that an express position in respect of such tests would help guide States in carrying out their responsibilities in managing cyber-related criminal conduct within their territory under international criminal law. The Sub-Committee suggests that the Office may consider adopting a combination of both tests where States have a duty not to knowingly allow their territory to be used for the commission of criminal conduct and, when put on notice, to use available means to prevent the conduct.

Application to Cyber-Crimes and Emerging Threats

33. The Draft Policy rightly notes that the Rome Statute does not currently include standalone cybercrimes within its express jurisdiction. Nonetheless, it is important to consider how cyber-

¹⁵ Gervais (n 4) 92.

¹⁶ Ibid 94.

enabled conduct may intersect with existing crimes under the statute, particularly when such acts are committed in the context of armed conflict or widespread and systematic attacks.

34. Take, for example, a scenario in which a cyber actor unlawfully accesses and disseminates personal medical records from hospitals within a State Party, using the information for coercion, ransom, or exploitation. If this conduct intentionally targets protected medical infrastructure during an armed conflict, or with the intent to commit genocide, or conduct crimes against humanity, then it could meet the threshold where the actor:
- a. Intentionally targets civilian medical infrastructure during an armed conflict, thus implicating Article 8(2)(b)(ix);¹⁷ or
 - b. Acts in a manner that causes severe suffering, discrimination, or denial of healthcare, potentially constituting persecution (Article 7(1)(h))¹⁸ or other inhumane acts (Article 7(1)(k)).¹⁹
35. Once the nature of the conduct is established as falling within one of the Rome Statute's crimes and *ipso facto* the Court's jurisdiction, Article 30²⁰ requires proof of both intent and knowledge on the part of the perpetrator. In cyber contexts, this means establishing that the perpetrator intended to engage in the conduct and understood that harm would result in the ordinary course of events. Despite the anonymity and remoteness of many cyber operations, intent may still be inferred where the actor knew the civilian character of the target and foresaw the likely consequences, such as disruption of medical care or the exploitation of vulnerable persons.
36. While cyber operations often occur at a distance, and actors may obscure their identities or operate via intermediaries (e.g., malware, botnets), the requirement of intent can still be satisfied where there is evidence that the actor was aware of the civilian nature of the target and acted with the purpose or understanding that harm would result. The foreseeability of certain outcomes such as disruption to medical care or exploitation of vulnerable populations may be relevant in proving intent and knowledge, particularly where attacks are systematic or

¹⁷ Rome Statute (n 1) art 8(2)(ix).

¹⁸ Ibid art 7(1)(h).

¹⁹ Ibid art 7(1)(h).

²⁰ Ibid art. 30.

repeated. As such, even in technologically mediated environments, the mental element under Article 30 provides a robust standard for assessing responsibility.

Observations of the above scenario:

37. In considering the applicability of the territoriality principle and the evolving nature of modern threats, it is crucial to examine whether such conduct could, under certain circumstances, fall within the existing categories of crimes under the Court's jurisdiction.
38. If the perpetrator intentionally targets civilian medical infrastructure in a conflict setting, or aims to disrupt healthcare access as part of a coercive campaign against a civilian population, this could support a finding of a war crime (Article 8(2)(b)(ix)) or persecution (Article 7(1)(h)).²¹ The required mental element - the knowledge and intent under Article 30 - may be satisfied where the cyber actor knowingly engages in an attack on protected persons or facilities, and where there is intent to exploit, coerce, or punish a civilian population through the exposure or commercialisation of their medical data. Moreover, where the actor's intent is to profit from such exploitation - whether through ransom demands, sale to third parties, or use as leverage - it may amount to an 'other inhumane act' under Article 7(1)(k), particularly if the consequences for victims include stigma, discrimination, or denial of essential services.
39. Another consideration and more of a central challenge for the Court in prosecuting cyber-enabled crimes under the Rome Statute lies in identifying the relevant territorial nexus where both the act and the harm may be dispersed across multiple jurisdictions. However, in the cyber domain, these boundaries blur. A perpetrator may operate from a non-State Party, and use infrastructure located in another territory of a State Party. The Draft Policy rightly notes (paragraph [36]-38)) that jurisdiction may attach where the harmful effects manifest within a State Party, even if the perpetrator and servers are elsewhere. Yet, the Draft Policy leaves open what constitutes a 'minimum territorial connection' sufficient to ground jurisdiction.
40. Where neither the perpetrator's location nor the cyber infrastructure is situated in a State Party, and the only connecting factor is the location of the victims or the effects, further clarification in the Draft Policy is needed. For example, is the mere presence of impacted data subjects in a

²¹ Rome Statute (n 1) art 8(2)(ix) and art 7(1)(h).

State Party - such as hospital patients whose records are compromised - sufficient? These questions underscore the need for a clear threshold to determine when a cyber crime's impact within a State Party's borders is sufficiently direct and substantial enough to engage the Court's jurisdiction. In the absence of cooperation mechanisms with non-State Parties, physical enforcement of jurisdiction is also practically constrained, highlighting the importance of defining territoriality in a manner that is both legal and operationally feasible.

41. While the physical location of a State and the mental elements mentioned earlier are both important for triggering the Court's jurisdiction, one of the first key questions is whether the conduct in question actually falls within the scope of the Rome Statute's four core crimes: crimes against humanity, genocide, the crime of aggression, and war crimes.
42. The Draft Policy explores how cyber-related conduct might intersect with these crimes but is not intended to be an exhaustive account. Instead, the Draft Policy is better understood as a way of framing how cyber capabilities could shape or even escalate modern warfare in ways that engage these crimes.

B - Personality Principle

43. Notwithstanding the Sub-Committee's view that doctrinal clarification and potential expansion could enhance the jurisprudential clarity of international criminal law in addressing cyber operations, the Sub-Committee recognises that many jurisdictional challenges arising from the application of the territoriality principle may be mitigated through reliance on the personality principle under Article 12 of the Rome Statute. In this sense, the existing framework does already provide an interpretive pathway for addressing cross-border or geographically dispersed conduct.
44. The personality principle, also known as the active nationality principle, is the doctrine by which States may exercise jurisdiction over offences committed by their nationals abroad. The principle is enshrined in Article 12(2)(b) of the Rome Statute, which grants the Court jurisdiction over crimes committed by nationals of State Parties.

45. The Draft Policy complies with the personality principle under Article 12(2)(b) by virtue of the fact that it treats cyber-enabled crimes as functionally equivalent to physical crimes for the purpose of determining jurisdiction.
46. Like the territoriality principle discussed at **Section A** above, the personality principle is a jurisdictional precondition for the Court. However, it is not the case that both the territoriality and personality principles need to be engaged for the Court to have jurisdiction in respect of a particular crime. Indeed, this is acknowledged in the Draft Policy at paragraph [40]. In the context of cyber-enabled crimes, as with any crime within the remit of the Court, this means that it is not imperative that the perpetrator of the cyber-enabled crime be a national of a State Party for the Court to have jurisdiction to investigate or prosecute.
47. It follows that, if a cyber-enabled crime is perpetrated in such a way that the location of the perpetrator is not readily discernible (meaning it is difficult to establish territoriality as a precondition) but the perpetrator can be identified as a national of a State Party, then the Court will have jurisdiction by virtue of the personality principle (assuming all other legal thresholds for the Court's intervention are satisfied). Conversely, if the cyber-enabled crime is committed by a perpetrator who has managed to remain anonymous (perhaps by virtue of the cyber aspects of the crime), but the impact of the crime is such that the territoriality principle is engaged, then the Court's jurisdiction can be enlivened despite the personality principle not being satisfied.
48. This is always how the Court's jurisdiction has operated pursuant to the Rome Statute. For this reason, the Draft Policy does not present any challenges for the application of the personality principle other than those that already exist as a function of the Court's jurisdiction.

C - Accessorial Conduct

49. According to the Draft Policy, the Office is of the view that the Court would have jurisdiction in situations where a person facilitates a crime that is committed within the territory of a State Party, even if the person is not acting within the territory of a State Party.
50. The Sub-Committee supports the Office's view. However, the Sub-Committee is also mindful that further clarification may be needed to address issues of accessorial liability for private

enterprises (such as social media platforms, Internet sites, instant messaging services, blogs, Internet service providers, etc) in the facilitation of Rome Statute crimes. This is especially the case when these services are located and incorporated in non-State Party territory but operate globally.

51. Such complications can be seen in domestic cases throughout the world. For example, in 2000, the decision of the Tribunal de Grande Instance of Paris, *Ligue contre le racisme et l'antisémitisme et Union des étudiants juifs de France c. Yahoo! Inc. et Société Yahoo! France* involved certain complaints brought against Yahoo! for the display and sale of Nazi memorabilia on its auction websites. The Tribunal de Grande Instance of Paris found that Yahoo! violated French criminal law given the images were accessible to people within French territory.
52. As with the complexities around minimum connection discussed in **Section A** above, the Sub-Committee recommends that further consideration be given to the issue of accessorial liability for private enterprises.

D - Assessing Gravity in Cyber-Enabled Incidents under the Rome Statute

53. The Rome Statute affirms that only 'the most serious crimes of concern to the international community as a whole' fall within the jurisdiction of the Court, invoking gravity as a threshold requirement under Articles 1 and 5 of the Rome Statute. When assessing whether a cyber-enabled incident meets this standard, gravity must be evaluated with fidelity to the Rome Statute's object and purpose, being the prevention of impunity for atrocity crimes, the promotion of lasting peace and security, and the preservation of a common humanity. The *Policy Paper on Case Selection and Prioritisation (Case Selection Policy)*²² further emphasises

²² International Criminal Court, *Policy Paper on Case Selection and Prioritisation* (15 September 2016).

gravity as 'the predominant case selection criteria', considering factors such as the scale, nature, manner of commission, and impact of the crimes.

54. While cyber conduct may be virtual in form, its consequences can be devastatingly real. The Draft Policy acknowledges that digital tools can be used to perpetrate, facilitate, or conceal Rome Statute crimes, including war crimes, crimes against humanity, and genocide. The scale of harm caused, especially to vulnerable civilian populations, remains central to the gravity analysis. For instance, a coordinated cyber-attack on critical infrastructure (e.g., hospitals or water supply systems) during armed conflict that intentionally deprives civilians of essential services, may reflect gravity through both the quantitative extent of suffering and the qualitative targeting of protected persons.
55. The manner of commission of the cyber-enabled crimes further refines this assessment. Cyber-enabled crimes that involve deceptive, anonymous, or transboundary means may implicate calculated orchestration, technical sophistication, and a high degree of impunity, aggravating their seriousness. The Office's 2016 Case Selection Policy recognises that such characteristics, particularly where crimes are committed against defenceless populations or through means that provoke terror, underscore the need for prosecution.²³
56. Equally pertinent is the impact of cyber-enabled crimes on victims and affected communities. Cyber-enabled incitement to genocide or the systemic dissemination of disinformation to instigate ethnic cleansing, for example, may not immediately present physical damage but may incite long-term social fracturing, polarisation, or mass violence. As the Draft Policy rightly notes, the Office will adopt a 'technology-neutral' approach in evaluating such harms.
57. Importantly, the gravity assessment framework proposed in the Draft Policy does not depart from the Court's existing practice. Rather, it reaffirms that the same evaluative criteria (scale, nature, manner of commission, and impact) apply equally to cyber-enabled conduct as to traditional forms of criminality.²⁴ However, what is novel is the application of those criteria to non-kinetic acts which may cause psychological, societal, or structural harm in less immediately visible ways. As such, the Sub-Committee is wary that the Office and Court must

²³ International Criminal Court, *Policy Paper on Case Selection and Prioritisation* (15 September 2016), [40]-[41].

²⁴ *Ibid*, [32].

be especially vigilant in recognising that gravity in cyberspace may manifest differently but no less seriously than physical crimes. For instance, a cyber-facilitated campaign of persecution or incitement may cause community-wide terror or displacement, even absent physical destruction.

58. This approach reflects the principle of 'technology-neutrality' identified in the Draft Policy. The Court need not reinvent its gravity framework for cyber-enabled crimes, but it must remain attuned to how digital means may obfuscate responsibility, scale rapidly, and transcend borders—attributes that may exacerbate the gravity of offences rather than diminish them. By adopting a consistent, principle-based approach to gravity that adapts to new modalities of harm, the Court can reinforce its legitimacy while maintaining doctrinal coherence.

59. In sum, gravity in cyber-enabled contexts must be appraised not only in terms of visible devastation but also in the latent, insidious effects of digital harm. A cyber-enabled incident may attain the threshold of gravity under the Rome Statute where it demonstrably undermines the peace, security, and dignity of persons at scale—aligning with the Preamble's resolve to guarantee 'lasting respect for and the enforcement of international justice'²⁵.

E - Cyber-enabled slavery crimes

60. The Sub-Committee would like to take this opportunity to provide a brief discussion on the increasingly prevalent issue of cyber-enabled slavery crimes by way of example of the types of conduct warranting further assessment and consideration by the Court.

61. Importantly, we note that international slavery crimes are a focus area for the Court, as indicated in the *Office of the Prosecutor's Policy on Slavery Crimes* recently released on 2 December 2024.²⁶ Slavery crimes fall squarely within the purview of the Court; specifically, enslavement and sexual slavery are considered crimes against humanity under Article 7 of the

²⁵ Rome Statute (n 1) preamble.

²⁶ Office of the Prosecutor, *Policy on Slavery Crimes* (International Criminal Court, December 2024) 2 <https://www.icc-cpi.int/sites/default/files/2024-12/policy-slavery-web-eng.pdf>.

Rome Statute, and sexual slavery is considered a war crime under Article 8 of the Rome Statute.

62. Any meaningful effort by the Court to pursue accountability for slavery crimes must appreciate the prevalent role of cyber technologies as means of enabling, perpetrating and facilitating forms of slavery.
63. On 12 July 2023, the United Nations Special Rapporteur submitted a report focusing on the use of technology in both facilitating and preventing contemporary forms of slavery.²⁷ It was found that the Internet has broadened the pool of potential victims who can easily be contacted and recruited by perpetrators without needing to be in the same physical or geographical location.²⁸ Online chat rooms and social media platforms including Facebook, Instagram, and OnlyFans are used to recruit and survey victims, build trust, access information and exert control over victims' lives in ways that lead to exploitation.²⁹ It is common for grooming to take place online, followed by sexual and other forms of exploitation offline including through live streaming. Digital platforms have become a tool of control to blackmail individuals into slavery including forced marriage and sexual slavery.³⁰
64. The Internet is also considered a feeding ground for deceptive recruitment practices and trafficking activities. For example, it is estimated that hundreds of thousands of people have fallen victim to human traffickers running illegal cyber-fraud schemes in South-East Asia. Victims are lured into fake promises of employment through fraudulent online advertisements

²⁷ Tomoya Obokata, Special Rapporteur, *Report of the Special Rapporteur on contemporary forms of slavery, including its causes and consequences*, UN Doc A/78/161 (12 July 2023) <https://docs.un.org/en/A/78/161>.

²⁸ Ibid 4.

²⁹ Ibid 4.

³⁰ Ibid 5.

only to be held in situations of slavery and forced labour including working long hours with minimal pay, strict control and surveillance, and confiscation of passports.³¹

65. Additionally, the use of technology to facilitate sexual exploitation of children is an issue of significant gravity on a global scale. Most child exploitation material is held online.³²

INTERPOL's International Child Sexual Exploitation database has identified 42,300 victims of child sexual abuse material worldwide since its inception and identifies 14 victims on average every day.³³ The issue is worsening due to advancing technologies which enable instantaneous production, limitless distribution of child exploitation material, and unregulated access to children online.³⁴

66. In cases of online child exploitation (to the level of slavery), the conduct may be committed by both physical and cyber means, through a network of individuals that are directly or indirectly involved. Take an instance where the physical exploitation of a child takes place in State A in order to produce digital material:

- a. An organised crime network with perpetrators located in States B and C facilitate cyber exploitation of that child to several States worldwide, including by distributing, selling and profiting from the online material.
- b. We note the Court's view that its territorial jurisdiction extends to both the territory of the State in which the criminal conduct began (subjective territoriality), and to the State in which it is completed (objective territoriality).³⁵ Applying these principles, it could be considered that the criminal conduct occurred within the territory of State A (where the

³¹ Ibid 5; UN News, *Hundreds of thousands trafficked into online criminality across SE Asia* (Web article, 29 August 2023) <https://news.un.org/en/story/2023/08/1140187>; Cherylann Molan, *Cambodia: Hundreds of Indians rescued from cyber-scam factories* (Web article, 1 April 2024) <https://www.bbc.com/news/world-asia-india-68705913>.

³² Tony Krone et al, *Online child sexual exploitation offenders: A study of Australian law enforcement data* (Report, January 2017) Foreword, <https://www.aic.gov.au/sites/default/files/2020-05/58-1213-FinalReport.pdf>.

³³ INTERPOL, *International Child Sexual Exploitation Database* (Web article) <https://www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database>.

³⁴ Childlight, *Over 300 million children a year are victims of online sexual exploitation and abuse* (Web page, 4 December 2024) <https://www.childlight.org/newsroom/over-300-million-children-a-year-are-victims-of-online-sexual-exploitation-and-abuse>.

³⁵ Draft Policy (n 2) 38.

physical exploitation took place), States B and C (being where the perpetrators are physically located and operating from) and on the territory of any State which received or purchased the material.

67. However, there are other complicating factors. As indicated in our submission above, the extent to which individuals operating across various global locations to commit cyber-enabled crimes simultaneously fall within the territorial jurisdiction of the Court, and the level of “minimum connection” required to attract the Court’s jurisdiction is unclear. The extent of responsibility attributed to online platforms (e.g. OnlyFans) who profit from cyber enabled crimes, particularly in the context of online child exploitation, has also not yet been sufficiently explored and warrants deeper analysis. We refer again to the need for further clarification on the territorial jurisdiction (**Section A**) and accessorial liability in this context (see **Section C**).
68. Perpetrators of cyber-enabled slavery are hidden behind computer screens out of sight. To enable meaningful investigation, it will be absolutely imperative for the Court to collaborate with stakeholders across a number of sectors including with national and regional authorities, law enforcement, anti-slavery organisations, civil society actors, technical and IT experts, and survivors. Information and data-sharing between the Court and other investigative agencies to assist with identifying victims, finding suspects and coordinating arrests will also be essential.
69. Finally, we emphasise the importance of continued survivor engagement and a trauma-informed approach when assessing slavery crimes committed by cyber or other means.

F - Integrity of Evidence of Cyber-Enabled Crime

70. The term 'cyber' is defined broadly in the Draft Policy as 'the range of activities involving information and communications (digital) technologies or networks, including artificial intelligence (AI).'³⁶ The Draft Policy acknowledges the pervasive nature of information technology and the Office's consequentially increased reliance on digital evidence. That said, the Draft Policy does not consider in detail the potential evidence integrity risks of an increased reliance on digital evidence in the context of cyber-enabled crime, nor does it set out a protocol

³⁶ Draft Policy (n 2) 9.

for addressing such implications. In this submission, evidence integrity risk refers to the risk of loss, deterioration, destruction, alteration, manipulation or fabrication of evidence.

71. The Sub-Committee encourages the Office to consider that the investigation of cyber-enabled crime, by its very nature and definition, requires the Office to wholly or substantially rely on digital evidence. For this reason, the Sub-Committee respectfully submits that development of a cyber evidence protocol is crucial to the Office's commitment to establishing an institutional environment that facilitates effective investigation and prosecution of cyber-enabled crimes under the Rome Statute.
72. Broadly, the Sub-Committee submits that evidence integrity risk with respect to digital evidence of cyber-enabled crime arises from two sources:
 - a. unintentional interference with the integrity of evidence during collection, transmission, and processing. This is a particular risk in circumstances where the Office is reliant in its investigations on the cooperation and facility of State and private parties to collect and preserve cyber evidence; and
 - b. intentional interference with the integrity of evidence, including the creation of false evidence. This is colloquially referred to as "anti-forensics" and arises as a heightened risk in circumstances where perpetrators and/or facilitators of cyber-enabled crime often have above-average technical skill.
73. The Sub-Committee submits that each of the above sources of potential evidence integrity issues present discrete and significant risk to the effective prosecution of cyber-enabled crime. The Sub-Committee further submits that a cyber evidence protocol must be drafted so as to adequately address evidence integrity risk arising from each of these sources.
74. Measures currently in place and under consideration in the Draft Policy to address integrity of evidence considerations, including digital evidence, in Court prosecutions include:
 - a. Pursuant to Article 64(9) of the Rome Statute, the Trial Chamber has the power to rule on the admissibility of evidence. In making this assessment, the Trial Chamber is to have regard to the three-part test under which the evidence must be relevant to the case, have probative value, and be sufficiently relevant and probative so as to outweigh any prejudicial

effect its admission may cause. This may include consideration of indicia of authenticity and reliability of the evidence.

- b. The Unified Technical protocol (“**E-court Protocol**”) for the provision of evidence, witness and victims information in electronic form defines the standards according to which the participants should prepare and provide evidence, potential evidence and material in electronic form with the Court.³⁷ This includes the provision of metadata which may be used to validate the date, source, author, history and authenticity of digital evidence.
- c. The Court has issued guidelines to assist parties on how to collect and preserve information that may ultimately become admissible evidence in court, including digital information.³⁸
- d. The Draft Policy sets out that the Office will take all steps within its power to access, preserve, store, manage and review technical digital evidence relevant to proving cyber-enabled crimes.³⁹
- e. The Draft Policy threatens prosecution of intentional measures to compromise the collection or integrity of evidence used in Court prosecutions as an offence against the administration of justice.⁴⁰
- f. The Draft Policy includes a commitment by the Office to strengthen its in-house expertise on cyber-enabled crimes, and to take steps to ensure access to strategic advice from leading experts, and commission specific advice from approved third party providers as necessary.⁴¹

75. The Sub-Committee recognises the importance of each of the above measures; however, respectfully submits that these measures are discrete, and do not together set out a complete

³⁷ International Criminal Court, *Unified Technical Protocol (“E-Court Protocol”) for the Provision of Evidence, Material and Witness Information in Electronic Form* (Protocol, 20 November 2017).

³⁸ Eurojust and International Criminal Court, *Guidelines for Civil Society Organisations: Cooperation and Information Sharing with the International Criminal Court* (September 2022) https://www.icc-cpi.int/sites/default/files/2022-09/2_Eurojust_ICC_CSOs_Guidelines_2-EN.pdf.

³⁹ Draft Policy (n 2) 33, [126].

⁴⁰ Ibid.

⁴¹ Ibid, 29, [105].

and comprehensive protocol of how evidence of cyber-enabled crime is to be uniformly dealt with by the Office. Rather this is currently left largely to the discretion of key decision-makers.

76. Although the Sub-Committee accepts the inherent difficulties of the Office attempting to predict the advent of technology that may change the Office's position on how digital evidence is to be handled, the Sub-Committee submits that a cyber evidence protocol can be drafted with sufficiently broad terminology to cover future technological developments whilst retaining efficacy in the present. Further, the Sub-Committee submits that, during development, the Office should establish periodic review of the cyber evidence protocol for currency.
77. The Sub-Committee recognises that the Court is empowered to apply principles and rules of law derived from multitudes of international and domestic sources, pursuant to Article 21 of the Rome Statute. The position the Sub-Committee puts forward is that, whilst these sources remain available to the Office, codification or synthesis of the Court's position on digital evidence of cyber-enabled crime should be concretised in consolidated form, akin to handbooks published by international organisations such as the Red Cross.
78. The Sub-Committee thus recommends the development and publication of a comprehensive protocol that mandates the steps to be taken to validate and maintain the integrity of digital evidence of cyber-enabled crimes, ensuring transparency and building public confidence in the Court's investigation into and prosecution of cyber-enabled crimes under the Rome Statute.
79. The Sub-Committee submits that the cyber evidence protocol should be developed in consultation with leading cyber experts across the public and private sectors, and should consider such matters as the collection, transmission, documentation, processing, use, validation, protection, preservation, storage, encryption, retention and destruction of cyber evidence. To this end, we draw the Office's attention to such publications as the *E-Procedure*:

Evidence in Time of Increased Use of Technology and Digitalisation by the International Nuremberg Principles Academy.⁴²

Conclusion

80. The Draft Policy reflects a clear recognition of the increasing relevance and complexity of such crimes in the modern era. In this submission, the Sub-Committee has sought to provide constructive commentary on key aspects of the Draft Policy, including definitional clarity, evidentiary issues, investigative scope, and inter-jurisdictional cooperation.
81. While the Draft Policy represents a significant step forward, the Sub-Committee submits that further refinement and development are recommended to ensure the Office is fully equipped to meet the evidentiary and procedural challenges inherent in prosecuting cyber-enabled crimes under the Rome Statute. In particular, the Sub-Committee stresses the importance of clear and comprehensive definitions that accurately capture the nature and scope of cyber-enabled crimes. Precise terminology is essential to guide investigations, prosecutions, and judicial assessments in a rapidly evolving technological landscape.
82. Equally important is adopting a nuanced approach to jurisdiction, complementarity, and admissibility that reflects the transnational and often state-involved character of cyber-enabled crimes. The complexities of cross-border conduct and multiple actors operating from various jurisdictions require careful legal analysis to establish the Court's competence and ensure effective accountability.
83. Moreover, the development of procedural safeguards and technical protocols designed to uphold the integrity of digital evidence is critical. Given the heightened risks of evidence loss, alteration and manipulation inherent in cyber-enabled crimes, the Court must implement robust standards for the collection, preservation, transmission, and validation of digital material.
84. Finally, continued engagement with cyber experts, States, civil society, and other relevant stakeholders will be key to ensuring that the Policy remains adaptable and responsive to ongoing technological advances and evolving international best practices. Such collaboration

⁴² International Criminal Court, *Unified Technical Protocol ("E-Court Protocol") for the Provision of Evidence, Material and Witness Information in Electronic Form* (Protocol, 20 November 2017).

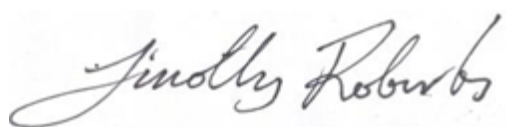
will strengthen the Office's institutional capacity and foster transparency and public confidence in the Court's efforts.

85. The Sub-Committee strongly supports the Office's commitment to transparency and technical advancement in this area. It encourages the Office to consider the recommendations contained within this submission and to develop in consultation with relevant stakeholders, a robust and adaptable policy framework that enables the effective investigation and prosecution of cyber-enabled crimes while upholding the highest standards of due process and evidentiary integrity.
86. NSW Young Lawyers and the Sub-Committee thank you for the opportunity to make this submission. The Sub-Committee remains available to provide further advice or assistance as the Office may require. If you have any further queries or require further submissions, please contact the undersigned at your convenience.

Concluding Comments

NSW Young Lawyers and the Sub-Committee thank you for the opportunity to make this submission. If you have any queries or require further submissions please contact the undersigned at your convenience.

Contact:



Timothy Roberts

President

NSW Young Lawyers

Email: president@younglawyers.com.au

Alternate Contact:



Jessica Lighton

Submissions Lead

NSW Young Lawyers

Email: submissions.YL@lawsociety.com.au

Alternate Contact:

A handwritten signature in black ink that reads "Caity Suchanow". The signature is written in a cursive, flowing style.

Caity Suchanow

Chair

NSW Young Lawyers International Law Sub-Committee

Email: nswylinternationalallawexec@gmail.com