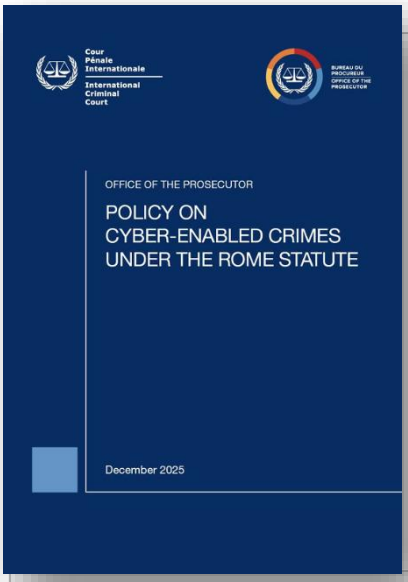
قراءات المرصد الوطني للإجرام

وحدة اليقظة الاستراتيجية

قراءة في التقرير الصادر عن مكتب المدعي العام لدى المحكمة الجنائية الدولية حول السياسة المعتمدة بشأن الجرائم الميسّرة عبر الفضاء السيبراني في إطار نظام روما الأساسي



العنوان	السياسة المعتمدة بشأن الجرائم الميسّرة عبر الفضاء السيبراني في إطار نظام روما الأساسي
الجهة المصدرة	مكتب المدعي العام لدى المحكمة الجنائية الدولية
لغة التقرير وتاريخ نشره	صدر باللغة الإنجليزية – دجنبر 2025
عدد الصفحات	72 صفحة
طبيعة الوثيقة	وثيقة سياسات مؤسسية موجّهة لعمل الادعاء حول الجرائم ذات الطابع السيبراني في إطار نظام روما.

الملّخص التنفيذي

يقدم مكتب المدّعي العام لدى المحكمة الجنائية الدولية، من خلال هذه الوثيقة السياسية، رؤية واضحة لمعالجة الجرائم المنصوص عليها في نظام روما الأساسي عندما ترتكب أو تُيسَّر عبر الفضاء السيبراني. وتؤكد الوثيقة منذ بدايتها أن التطور السريع للتكنولوجيا، ولا سيما في مجالات الاتصالات والذكاء الاصطناعي، يفرض على العدالة الدولية أن تتقدم بوتيرة متناسبة، حتى لا تتحول البيئة الرقمية إلى مساحة للإفلات من العقاب .

وتوضح الوثيقة أن الحديث عن الجرائم ذات التمكين السيبراني ليس استحداثا لفئة جرمية جديدة، بل هو توصيف للوسيلة التي يمكن أن ترتكب بها جرائم الإبادة الجماعية، الجرائم ضد الإنسانية، جرائم الحرب، والجرائم ضد إدارة العدالة، وفق ما ينص عليه نظام روما، عندما تنفّذ أو تُسهَّل من خلال الأنظمة الرقمية أو الهجمات المعلوماتية أو أدوات الذكاء الاصطناعي . كما تشدّد الوثيقة على أن اختصاص المحكمة لا يمتد تلقائيا إلى الجرائم المعلوماتية ذات الطبيعة الوطنية مثل الاختراق أو الاحتيال الإلكتروني، إلا إذا شكّلت هذه الأفعال جزءا من جريمة دولية تندرج ضمن النظام الأساسي، أو كانت وثيقة الصلة بها على نحو جوهري .

ويظلّ الخط الفاصل بين اختصاص القضاء الوطني واختصاص المحكمة أمرا جوهريا لضمان التكامل وعدم التداخل. ويرتكز التقرير على مبدأ الحياد التكنولوجي، بمعنى أن إمكانية ارتكاب الجريمة بوسائل غير تقليدية لا تغير من قابلية تطبيق قواعد القانون الدولي الجنائي، بل يجب أن يخضع الفعل لنفس التحليل القانوني من حيث العناصر المادية والمعنوية للجريمة، مع ضرورة ضمان ألا تتيح التكنولوجيا مساحة للهروب من المساءلة .

وهذا يشمل أيضا التحديات القانونية ذات الصلة بالاستخدام المتقدم للذكاء الاصطناعي في تنفيذ الأفعال الإجرامية. وفي تقييم القضايا، وتبقى معايير القبول أمام المحكمة ثابتة دون تعديل، وعلى رأسها معيار الخطورة عند تحديد أي القضايا تحظى بالأولوية للتحقيق والملاحقة، باستثناء الجرائم الواقعة على إدارة العدالة (المادة 70)، التي تعالج وفق منطق مختلف نظرا لطبيعتها الخاصة في حماية سير العدالة، وتشير الوثيقة بوضوح إلى أن فعالية هذه السياسة مشروطة بامتلاك المكتب للخبرات والموارد اللازمة للتعامل مع أدلة رقمية معقدة ومتغيرة، وبناء القدرات التقنية والقانونية المؤسسية، وتعزيز التعاون مع الدول، ومزودي التكنولوجيا، والجهات المدنية المعنية، لما لهذه الأطراف من دور في توفير الأدلة وحماية المصادر الرقمية الحساسة.

معالجة التكنولوجيات الجديدة:

ينطلق التقرير في مقدمته بتأكيد أن التطورات التكنولوجية، وفي مقدمتها تكنولوجيا المعلومات والاتصال والذكاء الاصطناعي، فرضت تحولات عميقة على واقع النزاعات المعاصرة، وعلى شكل الجرائم التي تدخل ضمن اختصاص المحكمة الجنائية الدولية. وقد أصبحت هذه التقنيات تطرح تساؤلات ملحّة حول مدى كفاية القواعد القانونية القائمة في مواكبة المخاطر المستجدة في الفضاء السيبراني. ويبرز التقرير أن النقاش الدولي حول هذه الإشكالات ليس جديدا، بل تتولاه منذ سنوات مجموعات حكومية داخل الأمم المتحدة مثل مجموعتي الخبراء الحكوميين (GGE) والفريق العامل مفتوح العضوية (OEWG) ، كما عبّرت دول عديدة عن مواقفها الرسمية بشأن كيفية تطبيق القانون الدولي في الفضاء السيبراني، وهو ما تم تجميعه في مراجع متخصصة يستند إليها التقرير.

كما يؤكد التقرير أن القانون الدولي قائم على الحياد التكنولوجي؛ أي أن قواعده ومرجعياته القانونية الحالية — وخاصة تلك المتعلقة بالقانون الجنائي الدولي والقانون الإنساني الدولي وحقوق الإنسان — صالحة للتطبيق على الجرائم المرتكبة عبر الوسائط الرقمية دون حاجة إلى تشريع جديد، باستثناء بعض المجالات التي قد تستفيد من تطوير أطر خاصة. ويضرب التقرير مثالا على ذلك بالمعاهدات المتخصصة في "الجرائم السيبرانية الوطنية" مثل اتفاقية بودابست وبروتوكولاتها، والاتفاقية الأممية الجديدة حول الجرائم السيبرانية، موضحا أن تلك الصكوك لا تمتد بنصوصها إلى الجرائم الدولية المنصوص عليها في نظام روما الأساسي، ما يبرر ضرورة أن تتعامل المحكمة مع الجرائم السيبرانية عندما ترتقي إلى مستوى الجرائم الدولية.

ويشير التقرير بوضوح إلى أن التكنولوجيات الناشئة — وعلى رأسها الذكاء الاصطناعي — تستخدم بشكل متزايد في العمليات السيبرانية التي قد تفضي إلى آثار جسيمة، مثل الهجمات الواسعة وغير المتحكَّم فيها، أو الإضرار بالبنى التحتية المدنية، أو تصعيد النزاعات المسلحة. وهو ما يستدعي يقظة قانونية عالية وتفسيرا ديناميا لنظام روما. ثم ينتقل التقرير لتوضيح مسؤولية مكتب الادعاء الدولي: فالسرعة المذهلة للتطور التكنولوجي قد تجعل الجرائم في المستقبل غير مرئية إذا لم تكن آليات العدالة مواكبة. لذلك يلتزم المكتب بتكييف أدواته، وتوسيع قدراته الفنية والبشرية، لضمان عدم إفلات الجرائم المرتكبة بوسائل رقمية من المساءلة. كما يبرز التقرير كون التعاون الخارجي عنصر محوري، وخاصة مع القطاع الخاص الذي يمتلك قدرات تقنية وبيانات جوهرية قد تسهم في إثبات الجرائم الدولية، وذلك وفق مبادئ حقوق الإنسان ومسؤوليات الشركات في احترامها.

المصطلحات والمفاهيم الأساسية:

- **مصطلح "Cyber"** يستخدم التقرير هذا المصطلح بمعناه الواسع الذي يشمل منظومات تكنولوجيا المعلومات والاتصال، والشبكات التي تعمل عليها، والتطبيقات المرتبطة بها، بما في ذلك تقنيات الذكاء الاصطناعي، سواء كانت هذه الأنظمة متصلة بالإنترنت أو مستقلة عنه. ويهدف هذا التعريف الشامل إلى ضمان أن النطاق يغطي كل البيئات الرقمية التي يمكن أن تكون أداة أو ساحة لارتكاب الجرائم الدولية.
- **الجرائم ذات التمكين السيبراني** يعرفها التقرير بوصفها جرائم تدخل ضمن نطاق نظام روما الأساسي –مثل الإبادة الجماعية أو الجرائم ضد الإنسانية أو جرائم الحرب أو الجرائم ضد إدارة العدالة– عندما ترتكب أو تُسهّل عبر الوسائل الرقمية أو الهجمات المعلوماتية أو الأدوات التقنية. وهذا التعريف ليس فئة قانونية جديدة، بل مجرد وصف لوسيلة ارتكاب الجريمة مع الإبقاء على نفس العناصر القانونية المنصوص عليها في النظام الأساسي.
- **الجرائم المعلوماتية التقليدية** (Cybercrime) كما تُعرف في التشريعات الوطنية –ومنها اختراق الأنظمة أو الاحتيال الإلكتروني– فهي تظل في الأصل من صميم اختصاص القضاء الوطني، ولا تنتقل إلى اختصاص المحكمة الجنائية الدولية إلا إذا كانت جزءا من جريمة دولية منصوص عليها في نظام روما أو ترتبط بها ارتباطا جوهريا يجعلها جزءا من بنيتها الإجرامية.
- **الدليل الرقمي** يقدمه التقرير باعتباره عنصرا مركزيا في التحقيق في الجرائم ذات البعد السيبراني. ومع أن الوثيقة لا تتوسع في الجوانب التقنية التفصيلية، فإنها تنبّه إلى ما يحيط بالأدلة الرقمية من مخاطر التلاعب أو الإتلاف أو الفقدان، مما يستوجب آليات حفظ وتحليل دقيقة تضمن موثوقيتها وسلامتها أثناء المسار القضائي.
- **الذكاء الاصطناعي** يتناوله التقرير باعتباره تكنولوجيا قد تُستخدم كأداة في تنفيذ أفعال إجرامية على المستوى الدولي. ويبرز في هذا السياق تمييز بين حالتين: الأولى عندما يكون الذكاء الاصطناعي في خدمة شخص يتخذ القرار ويملك النية، وهنا تبقى المسؤولية الجنائية على ذلك الشخص؛ والثانية سيناريوهات متقدّمة محتملة يصبح فيها النظام قادرا على اتخاذ قرارات مستقلة ذات آثار خطيرة، مما قد يثير تحديات في إسناد المسؤولية الجنائية نظرا لإمكانية غياب الفاعل البشري الذي تتجه إليه النية والعلم.

وفي ضوء هذه المفاهيم، يتخذ التقرير موقفا متوازنا يرفض الاستعجال نحو خلق تصنيفات جنائية دولية جديدة مرتبطة بالفضاء الرقمي، معتبرا أن الإطار القانوني الدولي الحالي كاف لمعالجة الجرائم الدولية المرتكبة عبر الوسائل السيبرانية، شريطة تطوير القدرات التقنية والتحقيقية للمؤسسات القضائية لتمكينها من مواكبة طبيعة هذه الأدلة الجديدة.

الإطار القانوني والاختصاص:

يرتكز التقرير في هذا المحور على التأكيد بأن تطبيق أحكام نظام روما الأساسي يظل هو المرجعية الأولى عند النظر في الجرائم التي ترتكب أو تُسهَّل عبر الوسائل السيبرانية، وذلك وفق المادة 21 التي تحدد مصادر القانون الواجب التطبيق أمام المحكمة الجنائية الدولية. وبعد النظام الأساسي، يأتي دور القواعد العامة للقانون الدولي والمعاهدات ذات الصلة، ثم — عند الحاجة — استلهام المبادئ العامة للقوانين الوطنية بشرط ألا تتعارض مع روح وأحكام نظام روما.

ويبرز التقرير أن حقوق الإنسان تمثل إطارا حاكما في عملية التفسير والتطبيق، إذ يُشترط أن يكون كل توظيف للقواعد القانونية متوافقا مع الالتزامات الدولية بحماية الحقوق الأساسية مثل الحق في الحياة، الحق في الخصوصية، وحرية التعبير، وغيرها من الحقوق التي قد تتأثر بالعمليات الرقمية والتحقيقات المتعلقة بها. أما فيما يتعلق بالاختصاص، فيؤكد التقرير أن الوسائل السيبرانية لا تغيّر من القواعد التقليدية للاختصاص القضائي، فمبادئ الإقليمية والجنسية تظل المعايير الأساسية لتحديد سلطة المحكمة. غير أن الفضاء السيبراني يفرض تعقيدات إضافية، لأن البيانات والأنظمة قد تمتد أو تمرّ عبر مناطق متعددة في وقت واحد، وهو ما يستوجب تحليلا أدق لمعرفة ما إذا كانت الجريمة قد ارتُكبت داخل إقليم دولة طرف أو من قبل شخص يخضع لاختصاص المحكمة.

ويلفت التقرير الانتباه إلى مسألة محورية تتمثل في أن مجرد مرور البيانات عبر بنية تحتية موجودة داخل دولة طرف لا يكفي وحده لإثبات اختصاص المحكمة، فالعبرة ليست بمرور البيانات بشكل عابر، بل بكون ذلك المرور جزءا جوهريا من السلوك الإجرامي، بحيث يمثل مساهمة ذات وزن في تنفيذ الفعل غير المشروع، وفي سياق التسهيل أو التواطؤ عن بُعد، يوضح التقرير أن الفاعل الذي يوجد خارج إقليم الدولة التي ترتكب فيها الجريمة قد يخضع لاختصاص المحكمة إذا كان دوره في التيسير أو التحريض أو المساعدة يشكل إسهاما فعليا في وقوع الجريمة داخل دولة طرف، وهذا يفتح الباب أمام تحديات جديدة في الإثبات وربط الفعل الإلكتروني بارتكاب الجريمة على أرض الواقع.

كيف تُرتكب جرائم نظام روما بوسائل سيبرانية؟

ينطلق التقرير من مبدأ أساسي مفاده أن الجرائم الدولية المنصوص عليها في نظام روما الأساسي — مثل الإبادة الجماعية والجرائم ضد الإنسانية وجرائم الحرب والجرائم ضد إدارة العدالة — يمكن أن تُرتكب أو تُيسَّر بواسطة الفضاء السيبراني، بشرط تحقق العناصر المادية والمعنوية للجريمة كما في أي سياق تقليدي. فالوسيلة الرقمية لا تمنح وصفا قانونيا جديدا للجرائم، وإنما تقدّم ساحة وأداة لتنفيذ السلوك الإجرامي على نطاق واسع وسريع التأثير.

ويقدم التقرير أمثلة تطبيقية توضح هذا التكييف القانوني. فعلى مستوى الإبادة الجماعية، يمكن للهجمات السيبرانية أن تستهدف البنى التحتية الحيوية لجماعة محمية — مثل المستشفيات، الكهرباء، المياه — بما يؤدي إلى وفاة أعداد كبيرة بشكل متوقع، مما قد يحقق الركن المادي للجريمة إذا اقترن ذلك بنية التدمير الكلي أو الجزئي لجماعة معيّنة. كما يشير التقرير إلى أن التحريض المباشر والعلني على الإبادة عبر المنصات الرقمية يدخل ضمن نطاق التجريم، باعتباره سلوكا قائما بذاته في القانون الدولي الجنائي.

أما الجرائم ضد الإنسانية، فيركز التقرير على عنصر «الهجوم الواسع أو المنهجي» باعتباره شرطا أساسيا، ويبرز أن الحملات المنسقة عبر الفضاء السيبراني لاستهداف مجموعة من السكان — سواء من خلال تجريدهم من الخدمات الأساسية أو ملاحقتهم أو التنكيل بهم أو نشر الكراهية والعنف ضدهم — قد تُعد «هجوما» بمعناه القانوني، خصوصا حين يكون ذلك جزءا من سياسة دولة أو تنظيم. وقد يؤدي تعطيل الأنظمة الرقمية الحساسة، مثل الأنظمة الطبية، إلى وفيات أو إصابات خطيرة يمكن تكييفها بوصفها جرائم قتل أو أفعال لا إنسانية أخرى إذا ثبت عنصري السببية والقصد الجنائي.

وفيما يتعلق بجرائم الحرب، يوضح التقرير أن النزاعات المسلحة الحديثة باتت تتضمن جبهات رقمية موازية، يمكن أن تستهدف المنشآت المدنية أو المرافق المحمية بموجب القانون الدولي الإنساني. فإذا أدت العمليات السيبرانية إلى تدمير أعيان مدنية أو تعريض السكان لمخاطر جسيمة، فإن ذلك قد يمثل انتهاكا لمبدأي التمييز والتناسب، وبذلك يدخل ضمن نطاق الجرائم المحددة في نظام روما. ويؤكد التقرير أن تطبيق قواعد القانون الإنساني الدولي على الفضاء السيبراني يظل خاضعا لذات المبادئ المألوفة دون أي استثناءات تقنية.

كما يتناول التقرير الجرائم ضد إدارة العدالة المنصوص عليها في المادة 70، مشيرا إلى أن الطابع الرقمي لهذه الأفعال أصبح متزايدا وخطيرا. وتشمل الأمثلة: تخريب الأدلة الرقمية، عرقلة التواصل مع

المحكمة، استهداف الشهود أو موظفي المحكمة إلكترونيا، أو نشر معلومات مضللة تقوض سير العدالة. ويميز التقرير هذه الفئة بخصوصيتها من حيث عدم اشتراط مستوى الخطورة نفسه المطبق على الجرائم الدولية الرئيسية، مما يجعلها مجالا عمليًا جدّيًا أمام مكتب المدّعي العام في سياق الجرائم السيبرانية.

ويخلص التقرير في هذا المحور إلى كون التحدي الأكبر ليس في تحديد الطبيعة القانونية للجرائم، بل في الإثبات: إثبات السببية بين الفعل السيبراني والنتيجة المادية، وإثبات النية والقصد في بيئة رقمية متعددة الفاعلين، وتعقيدات تتبّع المسؤولية عبر شبكات موزعة وعابرة للحدود. غير أن الأدلة الرقمية — مثل سجلات الدخول، التعليمات البرمجية، الاتصالات المشفرة — قد توفر في المقابل فرصا جديدة لإثبات النية والعلم، إذا توفرت الخبرات اللازمة للتحليل والتحصيل السليم لها.

المبادئ الموجهة لعمل مكتب المدعي العام:

يرسخ التقرير في هذا المحور الأسس القانونية والقيمية التي يعتمدها مكتب الادعاء العام عند التعامل مع الجرائم ذات التمكين السيبراني، حيث يؤكد أن الانخراط في هذا النمط من التحقيقات لا ينشئ إطارا موازيا أو استثناء من منهجية عمل المكتب، بل يأتي امتدادا طبيعيا للمبادئ التي تحكم جميع الملاحقات القضائية أمام المحكمة الجنائية الدولية. غير أن السياق السيبراني، بما يحمله من تعقيدات، يضفي على هذه المبادئ تطبيقات خاصة تستدعي توضيحا.

أول هذه المبادئ هو الامتثال لحقوق الإنسان المعترف بها دوليا، إذ يشدد التقرير على أن تفسير نظام روما الأساسي وتطبيقه يجب أن يظل متوافقا مع هذه الحقوق دون استثناء، سواء تعلق الأمر بجمع الأدلة الرقمية، أو بطلبات التعاون الدولي، أو بطرق الحصول على المعلومات من جهات خاصة أو شركات تكنولوجية. فحقوق الضحايا والشهود تُعتبر منطلقا أساسيا لأي نشاط تحقيق، تماما كما تصان ضمانات المشتبه فيهم والمتهمين وفقا للإطار القانوني للمحكمة.

ويتصل المبدأ الثاني بالاتساق في العمل، حيث يوضح المكتب أن تطوير هذه السياسة يأتي ضمن جهد أوسع يهدف إلى تجويد الممارسات القضائية، وإدراج الجرائم السيبرانية ضمن منظومة سياسات موضوعاتية مثل التي سبق أن اعتمدها في مجالات أخرى مثل الجرائم القائمة على النوع الاجتماعي، والجرائم ضد الأطفال، والرق والبيئة. والغاية من ذلك هي ضمان وحدة التطبيق وتذليل العوامل التي قد تحول دون رصد الجرائم السيبرانية في سياقات التحقيق الكبرى.

أما المبدأ الثالث فهو الاستقلالية والموضوعية والدقة في التحقيقات، إذ يؤكد المكتب أن الاعتماد على الأدلة الرقمية يجب أن يتم وفق أعلى درجات الحيادية، وبناء على تحليل علمي وقانوني صارم. كما يلتزم المكتب بتقدير مدى أهمية الدليل السيبراني عند تحديد التكييف القانوني للجرائم، وقد يسعى إلى توجيه الاتهام مباشرة بالجرائم المرتكبة عبر الوسائط الرقمية متى توفرت أسس ذلك.

ويخصص التقرير مبدأ رابعا يتعلق بمحددات gravity (الخطورة) وأثر الجريمة، معتبرا أن الجرائم السيبرانية التي تدخل في اختصاص المحكمة لن تتناول عادة بمعزل عن سياقات جنائية أوسع، وإنما ضمن ملفات متعددة الأبعاد يراعى فيها حجم الضرر، وعدد الضحايا، وطبيعة الأنظمة المتضررة رقميا، ومدى ارتباط الجريمة بانتهاكات واسعة النطاق للحقوق الأساسية. فمعايير الانتقاء والترتيب تظل جزءا جوهريا من ترشيد موارد المحكمة وتركيزها على الجرائم الأشد خطورة.

ويختتم المحور بمبدأ الشراكة واليقظة، إذ يبرز التقرير أن مواجهة الجرائم السيبرانية ذات الطابع الدولي تتطلب انفتاحا متزايدا على الخبرات المتخصصة، وتعزيز التعاون مع السلطات الوطنية، والمؤسسات التقنية، ومزودي الخدمات، والقطاع الخاص، ومنظمات المجتمع المدني. وفي هذه الشراكات يظل المكتب يقظا لضمان احترام الالتزامات القانونية للمحكمة والحفاظ على استقلاليتها بهذا الإطار، تعد المبادئ المبينة في هذه السياسة الركيزة التي يستند إليها المكتب في عمله المقبل داخل الفضاء السيبراني، ليس باعتباره مجالا استثنائيا، بل لأنه أصبح امتدادا طبيعيا لمسرح الجرائم الدولية التي تتطور وسائلها كما تتطور الحياة الإنسانية ذاتها.

الاعتبارات العملية:

يركز التقرير في هذا المحور على الأبعاد العملية لتنزيل السياسة المتعلقة بالجرائم ذات التمكين السيبراني داخل مكتب الادعاء العام، مبينا أن الفضاء الرقمي يفرض متطلبات جديدة على مستوى الموارد البشرية والتقنية والمؤسسية لضمان قدرة المكتب على ملاحقة هذه الجرائم بكفاءة.

أول ما يتوقف عنده التقرير هو البنية المؤسسية والموارد البشرية، إذ يشدد على ضرورة إدماج الخبرات التقنية داخل الهياكل القائمة للمكتب، بدل إنشاء وحدات معزولة منفصلة، وذلك عبر تقوية الوحدات المتخصصة في الأدلة الرقمية، والتحليل المعلوماتي، والتحقيقات المالية. كما يقترح المكتب الاستعانة بخبراء خارجيين ضمن ترتيبات مهنية مرنة — مثل الاستشارات قصيرة الأمد أو الانتدابات — لدعم قدراته عند معالجة حالات تفرض مهارات متقدمة جدا في الأمن السيبراني أو الهندسة الرقمية.

ويتناول التقرير أيضا أهمية التدريب وبناء القدرات، مشيرا إلى أن المواكبة التقنية ليست خيارا بل ضرورة، بما يستلزم برامج تدريبية متقدمة لفِرق التحقيق الموحدة داخل المكتب، إضافة إلى فتح مسارات تبادل الخبرات مع هيئات وطنية وأخرى خاصة تمتلك مؤهلات تقنية عالية. فالتحقيق في الجرائم الدولية المدعومة سيبرانيا يتطلب مهارات مختلفة عن تلك المعتمدة في الملفات التقليدية. وفي محور الأدلة والتحقيقات الرقمية، يشير التقرير إلى التحدي الجوهري المتمثل في الوصول إلى الأدلة قبل ضياعها أو إتلافها، مما يفرض على المكتب استخدام أدوات قانونية تحفظ البيانات سريعا، مثل أوامر الحفاظ على البيانات وطلبات التعاون القضائي الدولي. ويؤكد التقرير في هذا السياق أن الأدلة الرقمية قد تكون مفتاحا لإثبات النية والعلم والمسؤولية، لكنها تبقى هشة وعرضة للضياع، ما يستلزم جاهزية تقنية ولوجستية عالية.

كما يعرض التقرير البدائل الممكنة لتعزيز فعالية التحقيق عبر التعاون المشترك، سواء مع الدول الأطراف أو الجهات الدولية المختصة أو الجامعات ومراكز البحوث التقنية، وذلك بهدف توفير الخبرة والموارد التي قد تنقص المكتب بمفرده. وينظر إلى مثل هذه الشراكات باعتبارها آلية عمل واقعية في ظل التوزع الجغرافي والقطاعي للأدلة الرقمية.

وتحت عنوان التعامل مع القطاع الخاص، يعترف التقرير بالدور المحوري لشركات التكنولوجيا ومزودي خدمات الاتصالات ومنصات التواصل الاجتماعي، نظرا لسيطرتهم على أجزاء كبيرة من البنية التحتية الرقمية التي ترتكب عبرها الأفعال الإجرامية أو تتولد فيها الأدلة. ويؤكد المكتب أن التعاون هنا يقوم على أسس طوعية وقانونية تحترم حقوق الإنسان، دون فرض قيود أو متطلبات تمس حرية الشركات أو خصوصية المستخدمين خارج ما يسمح به القانون الدولي.

وبذلك يقدم التقرير رؤية عملية متكاملة لفهم كيف يمكن للمكتب الانتقال من مستوى السياسة إلى مستوى الممارسة، انطلاقا من قناعة بأن النجاح في معالجة الجرائم السيبرانية يستلزم توفر منظومة موارد بشرية وتقنية وتشريعية قادرة على الصمود أمام التطور المتسارع للفضاء الرقمي.

التعاون والتكامل:

يبرز التقرير في هذا المحور أن نجاح مكتب المدعي العام في التعامل مع الجرائم ذات التمكين السيبراني يعتمد بصورة جوهرية على التعاون الدولي والتكامل بين اختصاص المحكمة واختصاصات الدول. فالغالبية

الساحقة من الأدلة الرقمية ليست موجودة في نطاق سيطرة المحكمة، بل تقع تحت ولاية الدول أو القطاع الخاص، مما يجعل المشاركة والتفاعل عنصرين مؤسسين في العمل على هذا النوع من القضايا.

ويركز التقرير على الدول الأطراف باعتبارها الشريك الأول للمحكمة، إذ تقع على عاتقها مسؤولية تمهيد الطريق لإجراءات التحقيق وجمع الأدلة الرقمية، سواء عبر توفيرها للمعلومات، أو دعم أنشطة الحفظ والتحليل، أو الاستجابة لطلبات التعاون القضائي. كما يدعو التقرير الدول — خاصة في سياق تحديث تشريعات الجرائم السيبرانية — إلى أن تراعي إمكانية التعاون مع المحكمة، حتى تتاح آليات تسليم الأدلة الرقمية أو حفظها قبل اندثارها.

ويمتد التعاون ليشمل الدول غير الأطراف عندما تكون الأدلة بحوزتها أو تقع بنيتها التحتية الرقمية داخل نفوذها. وفي هذه الحالات، يطرح التقرير إمكانية تفعيل اتفاقات ثنائية، أو آليات تعاون مخصصة، تقوم على الإرادة الطوعية والاحترام المتبادل للسيادة الوطنية، وذلك لتفادي هروب الأدلة من متناول العدالة الدولية.

ويتناول التقرير أيضا دور القطاع الخاص —وخصوصا شركات التكنولوجيا العالمية ومنصات التواصل الاجتماعي — التي تمتلك قدرا هائلا من البيانات الحساسة ذات الصلة بالجرائم الدولية. ويوصي المكتب ببناء علاقات تعاون مهنية وطوعية مع هذه الجهات، بحيث يتم تقاسم المعلومات ضمن أطر واضحة تحترم الخصوصية وحقوق المستخدمين، مع التأكيد على أن المكتب لا يسعى إلى فرض التزامات قانونية عليها خارج قواعد القانون الدولي ذات الصلة.

كما يشير التقرير إلى أهمية التعاون مع المجتمع المدني، سواء من خلال توفير الإبلاغ المبكر عن الانتهاكات، أو تقديم الخبرات في مجالات الرصد الرقمي والأمن المعلوماتي، أو دعم جهود توثيق الهجمات السيبرانية التي تستهدف المدنيين أو البنية التحتية الإنسانية. ويؤكد التقرير أن المجتمع المدني لطالما لعب دورا محوريا في إحالة القضايا إلى المحكمة، وأن توسيع هذا الدور في السياق الرقمي سيُسهم في تعزيز العدالة.

ويختتم هذا المحور بإبراز أهمية مبدأ التكامل(Complementarity) ، الذي يعد أساس اختصاص المحكمة. إذ تبقى المسؤولية الأولى في مواجهة الجرائم ذات التمكين السيبراني على عاتق السلطات الوطنية، وتأتي المحكمة كملاذ عندما تكون الدول غير قادرة أو غير راغبة في القيام بواجبها. ومن هنا تأتي أهمية بناء

قدرات الدول وتحسين التشريعات الوطنية بما يمكنها من التعامل مع هذا النوع من الجرائم قبل أن تتحول إلى تهديدات دولية كبرى.

بهذا التصور، يرسخ التقرير فهما واضحا لمكانة المحكمة داخل منظومة العدالة في الفضاء السيبراني: ليست جهة بديلة عن الدول، ولكنها شريك داعم يضمن عدم إفلات أخطر الجرائم من المساءلة عندما تعجز الأنظمة الوطنية عن مواجهتها منفردة.

خلاصات ونتائج:

يخلص التقرير إلى أن الفضاء السيبراني لم يعد مجرد مجال تقني ملحق بالنزاعات، بل أصبح مسرحا كاملا يمكن أن ترتكب فيه الجرائم الدولية أو تيسر من خلاله على نطاق واسع، سواء في سياقات السلم أو الحرب. التطور المتسارع للتكنولوجيا، خاصة الذكاء الاصطناعي، أوجد مستويات جديدة من المخاطر يمكن أن تلحق أذى جسيما بالمدنيين والبنى التحتية الحيوية وتسهم في ارتكاب جرائم الإبادة الجماعية والجرائم ضد الإنسانية وجرائم الحرب. ولأن الطبيعة الرقمية لهذه الأفعال قد تخفي آثارها أو تعقد نسبتها إلى الجناة، كان لزاما على المحكمة الجنائية الدولية تطوير سياسة مؤطرة لكيفية التعامل مع هذا النمط من الجرائم.

ويؤكد التقرير أن القواعد القانونية الدولية القائمة كافية لملاحقة الجرائم ذات التمكين السيبراني، من دون الحاجة إلى استحداث تصنيفات جنائية جديدة. فمبدأ الحياد التكنولوجي يحكم تطبيق القانون: ما كان جريمة في الواقع المادي يبقى جريمة ولو تم بوسيلة رقمية. غير أن التطبيق العملي يفرض تطوير آليات تحقيق، وقدرات تقنية، وتعاون مؤسسي قادر على مجابهة تعقيدات الإثبات والسيادة الرقمية وطبيعة الأدلة السريعة الزوال.

كما يبرز التقرير أن نجاح المحكمة في هذا المجال يعتمد على الشراكة والتكامل؛ إذ تبقى الدول صاحبة الاختصاص الأول، بينما تتدخل المحكمة عندما تكون الدول غير قادرة أو غير راغبة في المتابعة. وتشكل شركات التكنولوجيا والمجتمع المدني والجهات الدولية محاور رئيسية في منظومة التعاون الضرورية لتأمين الأدلة الرقمية وحماية الضحايا والشهود وتعزيز المعرفة التقنية لدى مكتب الادعاء.

ويقدم التقرير في النهاية رؤية عملية تقوم على ترسيخ مبادئ حقوق الإنسان والموضوعية والاستقلالية داخل عمل الادعاء، وعلى بناء قدرات مؤسسية وتقنية تواكب التحولات الرقمية، بما يضمن

ألا تتجاوز التكنولوجيا منظومة العدالة وأن تبقى الجرائم الدولية — أينما ارتكبت وكيفما كانت وسيلتها — خاضعة للمساءلة وعدم الإفلات من العقاب.