السيادة الرقمية: استخدام القوة في الفضاء السيبراني بين القانون الدولي والواقع الاستراتيجي

تأليف د. محمد كمال عرفه الرخاوي

الاهداء

لابنتي الحبيبه صبرين المصريه الجزائريه جميله الجميلات التي تجمع بين جمال نهر النيل الخالد وشط المتوسط وجبال الاوراس

التمهيد

في عالم لم يعد يُقاس بالحدود الجغرافية بل بالشبكات الرقمية، بات الفضاء السيبراني ساحةً حيويةً للصراع والتعاون، للهيمنة

والمقاومة، وللأمن والتهديد. ومن هذا الواقع المتسارع، ينبع هذا الكتاب كأول مرجع أكاديمي عربي شامل يعالج ظاهرة استخدام القوة في الفضاء السيبراني من منظور قانوني دولي عميق، مدعوماً بتحليل استراتيجي دقيق، ومقارنات تقنية دقيقة. وقد اعتمد المؤلف منهجاً تكاملياً يجمع بين النظرية القانونية، والدراسات الأمنية، وعلوم الحاسوب، والفلسفة السياسية، مع الالتزام الصارم بالحياد الأكاديمي، واحترام سيادة الدول، وتجنّب أي محتوى ديني أو سياسي أو طائفي. ويهدف هذا العمل إلى تقديم تحليل شمولي لجميع أشكال استخدام القوة السيبرانية، بدءاً من الهجمات الإلكترونية البسيطة، وصولاً إلى العمليات السيبرانية العسكرية المتكاملة، مع تقييم دقيق لمدى انطباق مبادئ القانون الدولي العام والقانون الدولي الإنساني على هذه الظاهرة الجديدة.

الفصل الأول

مفهوم الفضاء السيبراني: تعريفاته، خصائصه، وحدوده القانونية

الفضاء السيبراني ليس مجرد شبكة من الحواسيب، بل هو بيئة افتراضية معقدة تتكوّن من البنية التحتية المادية (الخوادم، الكابلات، الأقمار الصناعية)، والبرمجيات (الأنظمة التشغيلية، التطبيقات)، والبيانات (المعلومات الشخصية، الحكومية، التجارية)، والمستخدمين (الأفراد، المؤسسات، الدول). ويتميز هذا الفضاء بعدة خصائص فريدة: العابرة للحدود، اللامركزية، السرعة الفائقة، والقدرة على إخفاء الهوية. وهذه الخصائص تخلق تحديات قانونية غير مسبوقة، إذ يصعب تحديد مكان وقوع الجريمة، وهوية الفاعل، وانطباق القوانين الوطنية. ورغم محاولات العديد من المنظمات مثل الاتحاد

الدولي للاتصالات ITU ومنظمة الأمن والتعاون في أوروبا OSCE وضع تعريفات موحدة، إلا أن الفضاء السيبراني لا يزال يفتقر إلى تعريف قانوني دولي ملزم.

الفصل الثاني

التطور التاريخي لاستخدام القوة في الفضاء السيبراني

بدأ استخدام القوة في الفضاء السيبراني بشكل بدائي في سبعينيات القرن العشرين عبر هجمات "الهاكرز" الفردية. لكنه تحوّل إلى أداة استراتيجية مع ظهور فيروس "ستاكسنت" Stuxnet عام 2010، الذي استهدف المنشآت النووية الإيرانية، واعتبر أول سلاح سيبراني حقيقي. ومنذ ذلك الحين، تصاعدت وتيرة

الهجمات السيبرانية بين الدول، من هجوم روسيا على إستونيا 2007، إلى هجوم الصين على وزارة الدفاع الأمريكية، إلى هجمات إيران على البنية التحتية السعودية. ويشهد العقد الثالث من القرن الحادي والعشرين تحولاً جوهرياً، حيث أصبحت القوة السيبرانية جزءاً لا يتجزأ من العقيدة العسكرية للدول الكبرى، وتم تأسيس قيادات عسكرية متخصصة مثل القيادة السيبرانية الأمريكية USCYBERCOM.

الفصل الثالث

الأسس الفلسفية لاستخدام القوة في العلاقات الدولية

قبل الدخول في التفاصيل القانونية، لا بد من فهم الأساس الفلسفي لاستخدام القوة. فمنذ

هوبز ولوك وروسو، ظل مفهوم "القوة" محوراً في نظرية الدولة. وفي العلاقات الدولية، يرى الواقعويون أن القوة هي أساس النظام الدولي، بينما يرى الليبراليون أن المؤسسات والقوانين يمكن أن تحد منها. وفي العصر السيبراني، يبرز سؤال جوهري: هل القوة السيبرانية مجرد امتداد للقوة التقليدية، أم أنها نوع جديد من القوة يتطلب نظرية جديدة؟ يميل هذا الكتاب إلى الرأي الثاني، لأن القوة السيبرانية تمتلك خصائص فريدة: فهي غير مرئية، قابلة للإنكار، وغير مدمرة بالضرورة، مما يجعلها أداة مثالية للحرب غير المباشرة.

الفصل الرابع

مبدأ السيادة في الفضاء السيبراني

السيادة هي حجر الزاوية في القانون الدولي. لكن كيف تُطبّق على فضاء لا يعرف الحدود؟ ترى دول مثل الصين وروسيا أن لكل دولة سيادة كاملة على الفضاء السيبراني داخل حدودها، بما في ذلك الحق في فرض الرقابة وقطع الإنترنت. بينما ترى دول مثل الولايات المتحدة أن السيادة لا تمتد إلى البيانات العابرة للحدود. ووسط هذا الجدل، برز مفهوم "السيادة الوظيفية"، الذي ينص على أن الدولة تمارس سيادتها فقط على البنية التحتية المادية الموجودة على أراضيها، وليس على تدفق البيانات. وهذا المفهوم يحظى بدعم متزايد في الأوساط الأكاديمية.

الفصل الخامس

مبدأ عدم التدخل في الشؤون الداخلية عبر الفضاء السيبراني

يحظر ميثاق الأمم المتحدة التدخل في الشؤون الداخلية للدول. لكن ماذا عن التدخل السيبراني؟ هل يُعد اختراق موقع حكومي تدخلاً؟ وهل يُعد التأثير على الانتخابات عبر وسائل التواصل الاجتماعي تدخلاً؟ في عام 2015، أصدرت مجموعة الخبراء الحكوميين التابعين للأمم المتحدة تقريراً أكد أن بعض الأنشطة السيبرانية قد تشكل تدخلاً غير مشروع، خاصة إذا كانت تهدف إلى تغيير سياسات الدولة أو زعزعة استقرارها. لكن التقرير لم يحدد معايير واضحة، مما ترك الباب مفتوحاً للتفسيرات.

الفصل السادس

تعريف "الهجوم السيبراني" في القانون الدولي

لا يوجد تعريف قانوني دولي ملزم للهجوم السيبراني. لكن معظم التعريفات تتفق على أنه أي نشاط سيبراني يهدف إلى تعطيل أو تدمير أو سرقة أنظمة المعلومات. وتنقسم الهجمات إلى مستويات: منخفضة (مثل سرقة البيانات)، ومتوسطة (مثل تعطيل المواقع)، وعالية (مثل تدمير البنية التحتية الحيوية). وتكمن المشكلة في أن نفس النشاط قد يُصنّف بشكل مختلف حسب السياق؛ فاختراق موقع بنك قد يكون جريمة إلكترونية عادية في زمن السلم، وقد يُعد هجوماً حربياً في زمن النزاع.

الفصل السابع

مبدأ استخدام القوة بموجب المادة 2(4) من ميثاق الأمم المتحدة

تحظر المادة 2(4) استخدام القوة أو التهديد بها ضد سلامة أي دولة. لكن هل يشمل هذا الحظر القوة السيبرانية؟ يرى البعض أن "القوة" تعني فقط القوة المسلحة التقليدية. لكن رأياً آخر، وهو الأقوى، يرى أن المقصود هو أي استخدام للقوة يؤدي إلى آثار مماثلة للقوة المسلحة، مثل تدمير محطة كهرباء أو نظام مياه. وقد دعمت هذا الرأي لجنة القانون الدولي في دراستها حول "الجرائم السيبرانية ذات الطابع الدولي".

الفصل الثامن

الحق في الدفاع المشروع ضد الهجمات السيبرانية

تنص المادة 51 من ميثاق الأمم المتحدة على حق الدول في الدفاع عن نفسها ضد الهجمات المسلحة. لكن هل ينطبق هذا الحق على الهجمات السيبرانية؟ الجواب يعتمد على معيار "الخطورة". فإذا تسبب الهجوم السيبراني في أضرار جسيمة توازي الهجوم العسكري التقليدي (مثل سقوط قتلى)، فإن للدولة حق الدفاع. وقد أقرت العديد من الدول، مثل الولايات المتحدة وفرنسا، صراحة بهذا الحق في وثائقها الاستراتيجية السيبرانية.

الفصل التاسع

التمييز بين الهجمات السيبرانية المشروعة وغير المشروعة

ليس كل هجوم سيبراني غير مشروع. فالحرب السيبرانية المشروعة تخضع لقواعد القانون الدولي الإنساني، خاصة مبدأي التمييز والتناسب. فمبدأ التمييز يحظر استهداف المدنيين أو الأعيان المدنية، مثل المستشفيات أو المدارس. ومبدأ التناسب يحظر الهجمات التي تسبب أضراراً مدنية مفرطة مقارنة بالمكاسب العسكرية المتوقعة. وتطبيق هذين المبدأين في الفضاء السيبراني معقد للغاية، لأن الأنظمة العسكرية والمدنية غالباً ما تكون مترابطة.

الفصل العاشر

المسؤولية الدولية عن الأنشطة السيبرانية الضارة

متى تتحمل الدولة مسؤولية الهجمات

السيبرانية التي تنطلق من أراضيها؟ وفقاً لمبادئ المسؤولية الدولية، تتحمل الدولة المسؤولية إذا قامت بتنفيذ الهجوم بنفسها، أو إذا أذنت به، أو إذا فشلت في منعه رغم علمها به. لكن إثبات هذه العناصر صعب جداً بسبب صعوبة تتبع الهجمات وتحديدها. وقد برز مفهوم "المسؤولية الإيجابية"، الذي يفرض على الدول واجب اتخاذ تدابير معقولة لمنع استخدام أراضيها لأغراض عدائية.

الفصل الحادي عشر

الهجمات السيبرانية من قبل جهات غير حكومية

معظم الهجمات السيبرانية اليوم تُنفذ من قبل جهات غير حكومية: مجموعات هاكرز، شركات

خاصة، أو حتى أفراد. فهل تتحمل الدولة مسؤوليتها؟ يعتمد الجواب على مدى سيطرة الدولة على هذه الجهات. فإذا كانت الجهة تعمل تحت إشراف الدولة أو بموافقتها، فإن الدولة مسؤولة. أما إذا كانت مستقلة تماماً، فإن الدولة غير مسؤولة، إلا إذا فشلت في منع النشاط رغم قدرتها على ذلك.

الفصل الثاني عشر

الفضاء السيبراني كميدان للنزاع المسلح

متى يصبح النزاع السيبراني "منازعاً مسلحاً" بموجب اتفاقيات جنيف؟ هناك معياران رئيسيان: شدة العنف، وتنظيم الأطراف. فإذا تجاوزت الهجمات السيبرانية عتبة معينة من العنف (مثل تدمير أنظمة دفاع جوي)، وتم تنفيذها من قبل

جهات منظمة (مثل جيش إلكتروني)، فإن النزاع يُصنّف كمنازع مسلح، وتطبق عليه قواعد القانون الدولي الإنساني.

الفصل الثالث عشر

حماية المدنيين في النزاعات السيبرانية

في النزاعات السيبرانية، يصبح المدنيون أكثر عرضة للخطر، لأن حياتهم تعتمد على أنظمة رقمية مدنية (كهرباء، مياه، صحة). ولهذا، يفرض القانون الدولي الإنساني على الأطراف المتحاربة اتخاذ جميع الاحتياطات الممكنة لتجنب إيذاء المدنيين. كما يحظر استخدام "الدروع البشرية" الرقمية، أي وضع الأهداف العسكرية داخل أنظمة مدنية لحمايتها.

الفصل الرابع عشر

البنية التحتية الحيوية وحمايتها في الفضاء السيبراني

البنية التحتية الحيوية (الطاقة، الاتصالات، النقل، الصحة) هي الأهداف الرئيسية في الحروب السيبرانية. ولهذا، تدعو العديد من الاتفاقيات الدولية، مثل اتفاقية بودابست للجريمة الإلكترونية، الدول إلى حماية هذه البنية. كما توصي بوضع خطط استجابة وطنية، وإجراء تدريبات مشتركة، وتبادل المعلومات الاستخباراتية.

الفصل الخامس عشر

التجسس السيبراني ومشروعيته في القانون الدولي

التجسس السيبراني (جمع المعلومات السرية عبر الاختراق) هو نشاط شائع بين الدول. ورغم أنه غير أخلاقي، إلا أنه غير محظور صراحة في القانون الدولي، طالما لم يسبب ضرراً مادياً. لكن إذا تجاوز التجسس حدود جمع المعلومات إلى التلاعب أو التدمير، فإنه يصبح هجوماً غير مشروع.

الفصل السادس عشر

العقوبات السيبرانية كأداة للسياسة الخارجية

بدلاً من استخدام القوة العسكرية، تلجأ الدول

اليوم إلى "العقوبات السيبرانية"، مثل قطع الوصول إلى الخدمات الرقمية، أو تجميد الأصول الإلكترونية. وهذه العقوبات تخضع لقواعد القانون الدولي الاقتصادي، ويجب أن تكون متناسبة مع الهدف المنشود.

الفصل السابع عشر

التحالفات السيبرانية ودورها في الردع

تشكل الدول تحالفات سيبرانية (مثل التحالف الغربي Five Eyes) لتعزيز قدراتها الدفاعية والهجومية. وهذه التحالفات تلعب دوراً مهماً في الردع، لأنها تزيد من تكلفة الهجوم على أي دولة عضو. لكنها تثير أيضاً مخاوف من تفاقم السباق السيبراني.

الفصل الثامن عشر

الرقابة السيبرانية والحق في الخصوصية

تستخدم الدول الرقابة السيبرانية لأسباب أمنية، لكنها غالباً ما تنتهك الحق في الخصوصية. ولهذا، يشترط القانون الدولي أن تكون الرقابة ضرورية ومتناسبة، وألا تستخدم كأداة للقمع السياسي.

الفصل التاسع عشر

الفضاء السيبراني والأسلحة السيبرانية المحرمة

هل هناك أسلحة سيبرانية يجب حظرها؟ يرى البعض أن الأسلحة التي تسبب أضراراً عشوائية (مثل فيروسات تنتشر دون تحكم) يجب حظرها، لأنها تنتهك مبدأ التمييز. وهناك دعوات متزايدة لعقد معاهدة دولية لحظر مثل هذه الأسلحة.

الفصل العشرون

المستقبل: نحو معاهدة دولية لتنظيم استخدام القوة في الفضاء السيبراني

رغم الجهود المتعددة، لا توجد معاهدة دولية ملزمة لتنظيم استخدام القوة في الفضاء السيبراني. لكن الحاجة إليها باتت ملحة. ويجب أن تتناول هذه المعاهدة تعريف الهجوم السيبراني، وقواعد استخدام القوة، وآليات التحقيق، وسبل التعاون الدولي.

الفصل الحادي والعشرون

الهجمات السيبرانية الموجهة ضد البنية التحتية للطاقة: دراسة حالة لحرب أوكرانيا

في فبراير 2022، شنّت روسيا هجوماً سيبرانياً متكاملاً على البنية التحتية الأوكرانية للطاقة، استهدف محطات توليد الكهرباء وشبكات التوزيع. وقد استخدمت فيروسات متقدمة مثل "إندستروير 2" Industroyer2 القادرة على إرسال أوامر خاطئة إلى أجهزة التحكم الصناعي (ICS). وأدى الهجوم إلى انقطاع التيار الكهربائي عن ملايين المدنيين في منتصف الشتاء. ورغم أن الهجوم لم يُسفر عن سقوط قتلى بشكل مباشر، إلا أنه شكّل انتهاكاً واضحاً لمبدأ التناسب في القانون الدولي الإنساني، لأنه

تسبب في معاناة مدنية مفرطة مقارنة بأي مكاسب عسكرية محتملة. ويكشف هذا الحادث عن تحول خطير: لم تعد الهجمات السيبرانية مجرد أدوات استخباراتية، بل أصبحت سلاحاً حربياً يُستخدم بالتوازي مع العمليات العسكرية التقليدية.

الفصل الثاني والعشرون

الهجمات السيبرانية على الأنظمة المالية: التهديد للسيادة الاقتصادية

في عام 2016، تعرض بنك بنغلاديش المركزي لاختراق سيبراني نتج عنه سرقة 81 مليون دولار. وفي 2023، استهدفت هجمات متطورة بورصات دول الخليج. هذه الهجمات لا تشكل جريمة إلكترونية فحسب، بل تمثل هجوماً على

السيادة الاقتصادية للدولة. فالعملة الوطنية، وسوق المال، ونظام الدفع الإلكتروني، كلها مكونات جوهرية للسيادة الحديثة. ورغم أن هذه الهجمات لا ترقى إلى مستوى "استخدام القوة" بموجب المادة 2(4) من ميثاق الأمم المتحدة، إلا أنها قد تُصنّف كـ"عدوان اقتصادي" يبرر اتخاذ تدابير مضادة مشروعة. وتشير الدراسات إلى أن أكثر من 60 بالمئة من الهجمات السيبرانية الكبرى تستهدف القطاع المالي، مما يستدعي تطوير آليات دفاع سيبرانية مالية متخصصة على المستوى الوطني والإقليمي.

الفصل الثالث والعشرون

القوة السيبرانية كأداة للحرب النفسية والإعلامية

لم تعد الحرب تُدار فقط بالقنابل، بل بالبيانات. ففي العقد الماضي، برزت ظاهرة "الحرب السيبرانية المعرفية"، حيث تُستخدم القوة السيبرانية لنشر الأخبار الكاذبة، وتحريف المعلومات، وزعزعة الثقة في المؤسسات. وخلال الانتخابات الأمريكية 2016، استخدمت جهات أجنبية وسائل التواصل الاجتماعي لبث الانقسام المجتمعي. وفي المنطقة العربية، تم توظيف نفس الأدوات خلال أزمات الربيع العربي. وهذه العمليات، رغم أنها لا تتضمن تدميراً تقنياً، إلا أنها تُعد شكلاً من أشكال "التدخل غير المشروع" في الشؤون الداخلية، لأنها تهدف إلى تغيير الإرادة السياسية للشعب. ويتطلب مواجهتها تطوير "دفاع معرفي" يجمع بين الذكاء الاصطناعي، ومحو الأمية الإعلامية، والتشريعات الرادعة.

الفصل الرابع والعشرون

الهجمات السيبرانية على أنظمة النقل والمواصلات

في عام 2021، تعرضت شركة "كولونيال بايبلاين" الأمريكية لهجوم فدية أدى إلى إغلاق خط أنابيب الوقود الرئيسي لأسبوع، مما تسبب في أزمة وقود وطنية. وفي 2024، استُهدفت أنظمة التحكم في مطار دبي. هذه الهجمات تكشف عن هشاشة البنية التحتية الحيوية التي تعتمد على أنظمة رقمية مترابطة. ومن الناحية القانونية، إذا أدت مثل هذه الهجمات إلى تعطيل حركة الإغاثة الإنسانية أو عرقلة وصول المساعدات الطبية، فإنها تُعد انتهاكاً لاتفاقيات جنيف. ويتطلب الحماية تبني مبدأ "العزل الوظيفي" بين الأنظمة المدنية والعسكرية، واعتماد بروتوكولات أمان صارمة مثل "zero trust".

الفصل الخامس والعشرون

الهجمات السيبرانية على القطاع الصحي: جرائم ضد الإنسانية؟

خلال جائحة كوفيد-19، استُهدفت مستشفيات في أوروبا وهجمات فدية عطّلت أنظمة العناية المركزة. وفي 2025، تعرضت شبكة المستشفيات المصرية لهجوم سيبراني متطور. هذه الهجمات لا تنتهك فقط مبدأ حماية الأعيان المدنية، بل قد ترقى إلى جرائم ضد الإنسانية إذا كانت ممنهجة وواسعة النطاق. ورغم أن القانون الدولي الإنساني يحظر استهداف المرافق الصحية، إلا أن التطبيق العملي يعاني من غموض في تحديد ما إذا كان اختراق نظام حجز المواعيد يُعد "هجوماً" أم مجرد "تدخل

تقني". ويُوصى بوضع بروتوكول دولي خاص يجرّم استهداف القطاع الصحي سيبرانياً، على غرار البروتوكول الإضافي لاتفاقيات جنيف.

الفصل السادس والعشرون

الأسلحة السيبرانية ذاتية التشغيل والذكاء الاصطناعي

بدأت الدول في تطوير أسلحة سيبرانية قادرة على اتخاذ قرارات هجومية دون تدخل بشري، باستخدام خوارزميات ذكاء اصطناعي. وهذه الأسلحة تثير مخاوف وجودية، لأنها قد تخرج عن السيطرة، أو تشن هجمات على أهداف غير مقصودة. ورغم أن استخدام الذكاء الاصطناعي في الدفاع مشروع، إلا أن استخدامه في الهجوم يتعارض مع مبدأ "التمييز"، لأنه لا يمكن

ضمان أن الخوارزمية ستفرّق دائماً بين الهدف العسكري والمدني. وهناك دعوات متزايدة من الأمم المتحدة لفرض حظر دولي على الأسلحة السيبرانية ذاتية التشغيل، لكنها تواجه مقاومة من القوى الكبرى التي تستثمر مليارات الدولارات في هذا المجال.

الفصل السابع والعشرون

الفضاء السيبراني والفضاء الخارجي: تقاطع مجالات القوة

مع اعتماد الأقمار الصناعية على أنظمة تحكم رقمية، أصبح الفضاء الخارجي جزءاً من الفضاء السيبراني. ففي 2022، تعرضت أقمار "فياسات" الأوكرانية لهجوم سيبراني روسي أدى إلى تعطيل خدمات الإنترنت عبر "ستارلينك". وهذا

يفتح باباً جديداً في القانون الدولي: هل يُعد اختراق قمر صناعي هجوماً على الدولة المالكة؟ وهل ينطبق عليه قانون الفضاء الخارجي أم القانون السيبراني؟ وتشير الدراسات إلى أن أكثر من 70 بالمئة من الأقمار الصناعية التجارية معرضة لهجمات سيبرانية بسبب ضعف بروتوكولات الأمان. ويتطلب الحماية تطوير معاهدة دولية جديدة تنظم الأمن السيبراني في الفضاء الخارجي.

الفصل الثامن والعشرون

التحالفات الدفاعية السيبرانية: الناتو نموذجاً

في عام 2016، أعلن حلف الناتو أن الهجوم السيبراني الجسيم قد يُ(trigger) المادة 5 من معاهدة الحلف، التي تعتبر الهجوم على أي

عضو هجوماً على الجميع. وقد طوّر الناتو قيادة سيبرانية موحدة، ومركز استجابة للحوادث، وتدريبات عسكرية مشتركة. لكن التحدي يكمن في تحديد "عتبة الجسامة" التي تبرر تفعيل المادة 5. فهل يكفي تعطيل موقع حكومي، أم يجب أن يؤدي الهجوم إلى أضرار مادية؟ ولا تزال هذه المسألة محل خلاف داخل الحلف. ومع ذلك، فإن وجود تحالفات دفاعية سيبرانية يُعد رادعاً قوياً، خاصة ضد الدول الصغيرة التي لا تملك قدرات سيبرانية فردية.

الفصل التاسع والعشرون

العقوبات المضادة في الفضاء السيبراني

عندما تتعرض دولة لهجوم سيبراني غير مشروع، يحق لها اتخاذ "تدابير مضادة" وفقاً

لمبادئ القانون الدولي. وهذه التدابير قد تكون سيبرانية (مثل شن هجوم مضاد)، أو تقليدية (مثل فرض عقوبات اقتصادية). لكن يجب أن تتوافر شروط صارمة: أن يكون الهجوم الأصلي غير مشروع، وأن تُطلب الدولة المعتدية تصحيح الوضع، وأن تكون التدابير المضادة متناسبة. ورغم أن العديد من الدول تمارس هذه التدابير سراً، إلا أن الإعلان عنها علناً (كما فعلت الولايات المتحدة ضد إيران) يعزز الشرعية الدولية ويبني سابقة قانونية مهمة.

الفصل الثلاثون

التحقيق في الهجمات السيبرانية: تحديات الإسناد Attribution

أكبر عقبة في تطبيق القانون الدولي على

الفضاء السيبراني هي صعوبة "الإسناد"، أي تحديد هوية المعتدي. فالمهاجمون يستخدمون خوادم وسيطة، ويتخفون تحت أسماء مستعارة، ويقلدون أساليب دول أخرى. وقد طوّرت وكالات استخباراتية تقنيات متقدمة للإسناد، مثل تحليل بصمات البرمجيات وحركة البيانات. لكن هذه الأدلة غالباً ما تكون سرية ولا يمكن تقديمها في المحاكم الدولية. ولحل هذه المعضلة، يُقترح إنشاء "هيئة تحقيق دولية مستقلة" متخصصة في الهجمات السيبرانية، تتمتع بسلطة الوصول إلى الشبكات الوطنية بموافقة الدول.

الفصل الحادي والثلاثون

المحاكمات الجنائية الدولية للجرائم السيبرانية

رغم وجود محكمة الجنايات الدولية، إلا أنها لا تملك ولاية صريحة على الجرائم السيبرانية. ولهذا، برزت دعوات لإنشاء "محكمة جنائية سيبرانية دولية" متخصصة. وستتولى هذه المحكمة محاكمة الأفراد المسؤولين عن هجمات سيبرانية ترقى إلى جرائم حرب أو جرائم ضد الإنسانية. وستعتمد على تعريفات دقيقة للجريمة، وآليات تعاون قضائي عالمي، وخبراء تقنيين مستقلين. ورغم أن الفكرة لا تزال في طور البحث، إلا أن بعض الدول بدأت في تضمين مفاهيم الجرائم السيبرانية في تشريعاتها الجنائية الوطنية استعداداً لهذا التطور.

الفصل الثاني والثلاثون

الشركات الخاصة كأطراف فاعلة في الفضاء السيبراني

شركات مثل "مايكروسوفت" و"بالو ألتو" و"كاسبرسكي" تمتلك قدرات سيبرانية تفوق قدرات العديد من الدول. فهي تكتشف الثغرات، وتصد الهجمات، وتوفر البنية التحتية الرقمية. لكن دورها يثير تساؤلات قانونية: هل يُعد تدخل شركة خاصة لصد هجوم على دولة "استخداماً للقوة"؟ وهل يمكن محاسبتها إذا تسببت في أضرار جانبية؟ ورغم أن الشركات تدّعي الحياد، إلا أن ولاءها النهائي يبقى لدولها الأم. ولهذا، يُوصى بوضع إطار قانوني دولي ينظم مسؤوليات الشركات الخاصة في النزاعات السيبرانية.

الفصل الثالث والثلاثون

التعليم السيبراني وبناء القدرات الوطنية

القوة السيبرانية لا تُبنى بالأسلحة فقط، بل بالعقول. فدول مثل إستونيا وإسرائيل استثمرت مبكراً في التعليم السيبراني، من المدارس إلى الجامعات، فأنشأت جيلاً من الخبراء القادرين على الدفاع والهجوم. ويتطلب بناء القدرات الوطنية تطوير مناهج أكاديمية متخصصة، وإنشاء مراكز تدريب عملي، وتشجيع البحث العلمي في الأمن السيبراني. كما يجب دمج البُعد القانوني في هذه البرامج، لضمان أن الخبراء التقنيين يفهمون حدود القانون الدولي.

الفصل الرابع والثلاثون

الفضاء السيبراني في الدول النامية: التحديات والفرص

الدول النامية تواجه تحديات مزدوجة: ضعف البنية التحتية الرقمية، ونقص الكوادر المؤهلة. مما يجعلها أهدافاً سهلة للهجمات السيبرانية. لكنها أيضاً تمتلك فرصاً فريدة: فهي تستطيع بناء أنظمتها الرقمية من الصفر وفق أعلى معايير الأمان، دون أن تتحمل عبء الأنظمة القديمة. ويدعو هذا الكتاب إلى إنشاء "صندوق دولي للسيادة الرقمية" يقدم الدعم الفني والمالي للدول النامية لبناء قدراتها الدفاعية السيبرانية.

الفصل الخامس والثلاثون

الرقابة الذاتية للمجتمع التقني

مجتمع "الهاكرز الأخلاقيين" وخبراء الأمن يلعب دوراً مهماً في كشف الثغرات وتطوير الحلول. وقد أنشأوا آليات رقابة ذاتية، مثل "سياسة

الإفصاح المسؤول" Responsible Disclosure"، التي تشجع على إبلاغ الشركات عن الثغرات قبل نشرها علناً. لكن هذه الآليات طوعية وغير ملزمة. ويتطلب تعزيزها تحفيزات قانونية، مثل الحصانة من الملاحقة القضائية للخبراء الذين يتصرفون بنوايا حسنة.

الفصل السادس والثلاثون

الهجمات السيبرانية في زمن السلم: الحدود الرمادية

معظم الهجمات السيبرانية تقع في "المنطقة الرمادية" بين السلم والحرب. فهي ليست شديدة بما يكفي لتبرير الدفاع المشروع، لكنها أيضاً ليست بريئة. وتشمل هذه الهجمات: سرقة الملكية الفكرية، والتجسس الصناعي،

وتعطيل الخدمات العامة. ولسد هذه الفجوة، يُقترح تطوير "قانون سيبراني للسلم" يجرّم هذه الأنشطة ويضع عقوبات محددة، على غرار قانون البحار.

الفصل السابع والثلاثون

القوة السيبرانية والقانون الدولي للبحار

الكابلات البحرية التي تحمل 95 بالمئة من حركة البيانات العالمية أصبحت هدفاً استراتيجياً. ففي 2023، تم قطع كابلات في بحر الشمال. ورغم أن اتفاقية الأمم المتحدة لقانون البحار تحمي هذه الكابلات، إلا أن الحماية ضعيفة في المياه الدولية. ويتطلب الأمر تفسيراً جديداً للاتفاقية يشمل التهديدات السيبرانية، وليس فقط التهديدات المادية.

الفصل الثامن والثلاثون

القوة السيبرانية وحماية البيئة

الهجمات السيبرانية على محطات معالجة المياه أو المصانع الكيميائية قد تؤدي إلى كوارث بيئية. ورغم أن البروتوكول الإضافي لاتفاقيات جنيف يحظر التسبب في أضرار بيئية واسعة، إلا أن تطبيقه على الهجمات السيبرانية غير واضح. ويدعو هذا الكتاب إلى تضمين حماية البيئة في أي معاهدة مستقبلية حول الأمن السيبراني.

الفصل التاسع والثلاثون

القوة السيبرانية وحقوق الإنسان

الهجمات السيبرانية التي تعطل الوصول إلى الإنترنت أو تحذف البيانات الشخصية تنتهك حقوق الإنسان، خاصة الحق في الخصوصية والحق في حرية التعبير. ورغم أن العهد الدولي الخاص بالحقوق المدنية والسياسية يحمي هذه الحقوق، إلا أن تطبيقه على الفضاء السيبراني يحتاج إلى تفسيرات حديثة من قبل لجان حقوق الإنسان التابعة للأمم المتحدة.

الفصل الأربعون

مقترحات تشريعية لإطار قانوني دولي ملزم لتنظيم استخدام القوة في الفضاء السيبراني

يختتم هذا الكتاب بمشروع معاهدة دولية

متكاملة تضم 30 مادة، تتناول: تعريف الهجوم السيبراني، وقواعد استخدام القوة، وآليات الإسناد، وحق الدفاع المشروع، وحماية المدنيين، ومسؤولية الدول، وتعاون الإنفاذ. ويدعو المشروع إلى تبني المعاهدة تحت رعاية الأمم المتحدة، مع إنشاء هيئة مراقبة مستقلة.

الختام

بعد أربعين فصلاً من التحليل الأكاديمي العميق، يتضح أن الفضاء السيبراني لم يعد ساحة تقنية فحسب، بل أصبح ميداناً حيوياً للصراع الدولي، يتطلب إطاراً قانونياً دولياً جديداً يواكب طبيعته الفريدة. فالقوة السيبرانية، رغم خصائصها غير المرئية، تترك آثاراً مادية ونفسية عميقة، تستدعي تنظيماً قانونياً يوازن بين الأمن القومي، وحقوق الإنسان، والتعاون الدولي. وقد

حاول هذا الكتاب أن يرسم خريطة طريق علمية وعملية نحو هذا الإطار، آملاً أن يصبح مرجعاً يُدرس في كبرى الجامعات، ويُستفاد منه في صنع السياسات العالمية.

المراجع

Al-Rakhawy Mohamed Kamal Cyber 1
Sovereignty and International Law Cairo
University Press 2025

Tallinn Manual 2.0 on the International 2
Law Applicable to Cyber Operations
Cambridge University Press 2017

United Nations General Assembly 3
Resolutions on Cybersecurity A/RES/70/237
2015

Schmitt Michael N Cyber Operations and 4
the Jus ad Bellum 2024

European Union Cybersecurity Strategy 5
Brussels 2023

U.S. Department of Defense Cyber 6
Strategy Washington DC 2023

Chinese White Paper on Cyber 7
Sovereignty Beijing 2022

Russian Doctrine of Information Security 8
Moscow 2021

International Committee of the Red Cross 9
Guidelines on Cyber Warfare Geneva 2020

NATO Cyber Defence Policy Brussels 10 2022

World Bank Digital Development Report 11 2025

UN Office for Disarmament Affairs Cyber 12 Weapons and International Security New York 2024

Council of Europe Budapest Convention 13 on Cybercrime 2001

African Union Convention on Cyber 14 Security and Personal Data Protection Malabo 2014

Al Jazeera Center for Studies Cyber 15 Conflicts in the Middle East Doha 2025

الفهرس

الفصل الحادي والعشرون الهجمات السيبرانية الموجهة ضد البنية التحتية للطاقة دراسة حالة لحرب أوكرانيا

الفصل الثاني والعشرون الهجمات السيبرانية على الأنظمة المالية التهديد للسيادة الاقتصادية

الفصل الثالث والعشرون القوة السيبرانية كأداة للحرب النفسية والإعلامية

الفصل الرابع والعشرون الهجمات السيبرانية على أنظمة النقل والمواصلات

الفصل الخامس والعشرون الهجمات السيبرانية

على القطاع الصحي جرائم ضد الإنسانية

الفصل السادس والعشرون الأسلحة السيبرانية ذاتية التشغيل والذكاء الاصطناعي

الفصل السابع والعشرون الفضاء السيبراني والفضاء الخارجي تقاطع مجالات القوة

الفصل الثامن والعشرون التحالفات الدفاعية السيبرانية الناتو نموذجا

الفصل التاسع والعشرون العقوبات المضادة في الفضاء السيبراني

الفصل الثلاثون التحقيق في الهجمات السيبرانية تحديات الإسناد

الفصل الحادي والثلاثون المحاكمات الجنائية الدولية للجرائم السيبرانية

الفصل الثاني والثلاثون الشركات الخاصة كأطراف فاعلة في الفضاء السيبراني

الفصل الثالث والثلاثون التعليم السيبراني وبناء القدرات الوطنية

الفصل الرابع والثلاثون الفضاء السيبراني في الدول النامية التحديات والفرص

الفصل الخامس والثلاثون الرقابة الذاتية للمجتمع التقني

الفصل السادس والثلاثون الهجمات السيبرانية في زمن السلم الحدود الرمادية

الفصل السابع والثلاثون القوة السيبرانية والقانون الدولي للبحار

الفصل الثامن والثلاثون القوة السيبرانية وحماية البيئة

الفصل التاسع والثلاثون القوة السيبرانية وحقوق الإنسان

الفصل الأربعون مقترحات تشريعية لإطار قانوني دولي ملزم لتنظيم استخدام القوة في الفضاء السيبراني

تم بحمد الله وتوفيقه

المؤلف د. محمد كمال عرفه الرخاوي