الحصن الرقمي

الإطار القانوني لمواجهة الهجمات السيبرانية على البنية التحتية الحيوية

دراسة تحليلية مقارنة في سيادة الدولة ومسؤولية الأفراد في الفضاء الإلكتروني

تأليف

الدكتور محمد كمال عرفه الرخاوي

الباحث والمستشار والخبير والفقيه والمؤلف القانوني والمحاضر الدولي في القانون

الإهداء

إلى روح والدي الطاهرة، وروح أبي الطاهر، اللذين علّماني أن حماية الوطن لا تقتصر على الحدود البرية والبحرية، بل تمتد لتشمل الفضاء الرقمي الذي أصبح شريان الحياة الحديث، وأن القانون هو السيف والدرع في مواجهة التهديدات غير المرئية.

وإلى ابنتي الحبيبة صبرينال ، يا من تجمعين في روحك أصالة النيل وعمق المتوسط وشموخ الأوراس؛ لكي تعلمي أن المستقبل يُكتب بالبيانات، وأن حماية البنية التحتية هي حماية للمستقبل نفسه، فكوني دائمًا حارسة للأمن الرقمي، ومدافعة عن السيادة الوطنية في الفضاء الإلكتروني، وليكن هذا الكتاب منهجًا لكِ لفهم أن المعركة القادمة هي معركة عقل وقانون قبل أن تكون معركة سلاح.

مقدمة المؤلف

في عصر الحرب غير المرئية

لم تعد الحروب التقليدية هي التهديد الوحيد للأمن القومي للدول، بل برز تهديد أكثر خطورة وتعقيداً، يأتي من خلال شاشات الحواسيب وشبكات الإنترنت. الهجمات السيبرانية على البنية التحتية الحيوية، سواء كانت شبكات طاقة، أنظمة مياه، مؤسسات مالية، أو شبكات اتصالات، لم تعد مجرد جرائم إلكترونية عابرة، بل تحولت إلى أدوات للضغط الجيوسياسي وأسلحة محتملة في النزاعات الدولية.

يأتي هذا الكتاب الحصن الرقمي كعمل فقهي استباقي، يغوص في أعماق التحديات القانونية التي تواجه الدول والمجتمع الدولي في مواجهة هذا التهديد الوجودي. لا يكتفي الكتاب برصد الوقائع التقنية، بل يحلل الإطار القانوني الدولي والداخلي المنظم للاستجابة، ومساءلة الدول، وحماية الأفراد.

سنناقش بالتفصيل إشكالية النسبة في الهجمات

السيبرانية، وتطبيق قواعد القانون الدولي الإنساني على الفضاء الإلكتروني، وتحديات الاختصاص القضائي عبر الحدود. إنه مرجع ضروري لصانعي السياسات، والقضاة، ومحامي الدفاع، وخبراء الأمن السيبراني، يقدم رؤية شاملة لتحويل الفضاء الإلكتروني من منطقة رمادية إلى فضاء محكوم بالقانون والعدالة.

الجزء الأول

المفاهيم الأساسية والتصنيف القانوني

الفصل الأول

تعريف البنية التحتية الحيوية في القانون الدولي

يستهل هذا الفصل بتعريف دقيق لمفهوم البنية التحتية الحيوية، مفرقًا بين البنية المادية والبنية الرقمية. نحلل كيف تطورت التعريفات في التشريعات

الوطنية والاتفاقيات الدولية لتشمل شبكات الطاقة، المياه، الصحة، النقل، والاتصالات.

نناقش المعايير القانونية لتصنيف المنشأة كبنية حيوية، هل يعتمد على الأهمية الاقتصادية، الأمنية، أم الاجتماعية؟ ندرس التباين في التصنيف بين الدول المتقدمة والدول النامية، وتأثير ذلك على مستوى الحماية القانونية الممنوحة.

نخلص إلى أن تعريف البنية التحتية يجب أن يكون ديناميكيًا يتسع للمستجدات التكنولوجية، وأن الحماية القانونية يجب أن تتناسب مع درجة الحيوية والأثر الكارثي المحتمل لتعطيلها.

الفصل الثاني

طبيعة الهجمات السيبرانية بين الجريمة والحرب

يركز هذا الفصل على التمييز القانوني الدقيق بين الهجوم السيبراني كجريمة إلكترونية عادية، وبينه كعمل من أفعال الحرب أو العدوان. نحلل معايير الشدة والتأثير التي تحول الجريمة إلى عمل حربي، مثل التسبب في وفيات أو أضرار مادية جسيمة.

نناقش إشكالية الهجمات الهجينة التي تجمع بين العمليات السيبرانية والمعلوماتية والعسكرية التقليدية، وكيف يصعب عزل المسؤولية القانونية فيها. ندرس نماذج لهجمات استهدفت بنى تحتية حيوية وتصنيفها قانونيًا دوليًا.

نخلص إلى أن الخط الفاصل بين الجريمة والحرب في الفضاء السيبراني لا يزال ضبابيًا، مما يستدعي تطوير بروتوكولات دولية واضحة لتحديد العتبة التي تستدعي تطبيق قانون النزاعات المسلحة.

الفصل الثالث

سيادة الدولة في الفضاء الإلكتروني

يتناول هذا الفصل مبدأ سيادة الدولة وتطبيقه على البنية التحتية الرقمية الواقعة ضمن إقليمها. نحلل هل تمتد السيادة لتشمل البيانات المخزنة سحابيًا خارج الإقليم ولكن تخص مواطنين وطنيين؟

نناقش مبدأ عدم التدخل في الشؤون الداخلية وكيف ينطبق على الهجمات السيبرانية التي تشنها دول ضد بنى تحتية لدول أخرى. ندرس الاجتهادات الفقهية حول حق الدولة في الدفاع عن سيادتها الرقمية باستخدام وسائل سيبرانية مضادة.

نخلص إلى أن سيادة الدولة في الفضاء الإلكتروني هي امتداد للسيادة التقليدية، وأن انتهاك البنية التحتية الحيوية يعتبر مساسًا بالسيادة الوطنية

يستدعي مسؤولية دولية.

الجزء الثاني

المسؤولية الدولية ونسبة الهجمات

الفصل الرابع

إشكالية النسبة في الهجمات السيبرانية

يعالج هذا الفصل أحد أكبر التحديات القانونية، وهي صعوبة إثبات هوية المهاجم بدقة. نحلل التقنيات المستخدمة لإخفاء الهوية مثل الشبكات الوكية والخوادم الوسيطة، وتأثيرها على الإجراءات القانونية.

نناقش معايير إثبات النسبة في القانون الدولي، هل يكفي الدليل الفني أم يتطلب دليلًا استخباراتيًا

وسياسيًا؟ ندرس دور الشركات الخاصة في الأمن السيبراني في تقديم أدلة النسبة ومدى حجيتها قانونيًا.

نخلص إلى أن تطوير آليات دولية موثوقة للنسبة هو شرط جوهري لتفعيل المسؤولية الدولية، وأن غياب اليقين في النسبة يشجع على الإفلات من العقاب.

الفصل الخامس

مسؤولية الدولة عن أفعال الفاعلين غير الدوليين

يركز على مدى مسؤولية الدولة عن الهجمات التي تنطلق من أراضيها بواسطة أفراد أو جماعات غير تابعة لها رسميًا. نحلل مبدأ العناية الواجبة والتزام الدولة بمنع استخدام إقليمها لأعمال تضر بدول أخرى.

نناقش معايير السيطرة الفعالة والسيطرة الشاملة في نسبة أفعال المجموعات الإلكترونية للدول الداعمة لها. ندرس حالات عملية حيث تم تحميل دول مسؤولية هجمات نفذتها مجموعات قرصنة تابعة لها ضمنيًا.

نخلص إلى أن الدولة تتحمل مسؤولية قانونية إذا قصرت في منع الهجمات من أراضيها أو إذا قدمت دعمًا لوجستيًا للمهاجمين، مما يعزز مبدأ المساءلة الدولية.

الفصل السادس

تطبيق قانون النزاعات المسلحة على الفضاء السيبراني

يتناول مدى انطباق اتفاقيات جنيف وبروتوكولاتها الإضافية على الهجمات السيبرانية. نحلل مبادئ التمييز والتناسب والاحتياطات في الهجوم وكيف يمكن

تطبيقها تقنيًا وقانونيًا في الفضاء الإلكتروني.

نناقش حماية المدنيين والبنية التحتية المدنية من الهجمات السيبرانية، وهل تعتبر انقطاع خدمات الإنترنت هجومًا عشوائيًا؟ ندرس وثيقة تالين/manual Tallinn Manual كمحاولة فقهية لتقعيد هذه القواعد.

نخلص إلى أن القانون الدولي الإنساني ينطبق على الفضاء الإلكتروني، ولكن التطبيق العملي يتطلب تفسيرات مرنة تراعي طبيعة الأضرار غير المباشرة للبرمجيات الخبيثة.

الجزء الثالث

التشريعات الوطنية والآليات الجنائية

الفصل السابع

تجريم الهجمات على البنية التحتية في القوانين الوطنية

يستعرض هذا الفصل كيفية تجريم الهجمات السيبرانية في التشريعات الداخلية للدول. نقارن بين النصوص العامة في قوانين العقوبات والنصوص الخاصة في قوانين مكافحة الجرائم الإلكترونية.

نحلل تعريفات الأفعال المجرمة مثل التخريب الإلكتروني، الوصول غير المصرح به، وتعطيل الأنظمة الحيوية. ندرس العقوبات المقررة ومدى كفايتها للردع مقارنة بخطورة الأضرار المحتملة.

نخلص إلى ضرورة وجود نصوص جنائية خاصة وصريحة تجرم استهداف البنى التحتية الحيوية بعقوبات مشددة توازي خطورة الجريمة المادية.

الفصل الثامن

الاختصاص القضائي في الجرائم السيبرانية العابرة للحدود

يركز على تحديات تحديد المحكمة المختصة نظرًا لطبيعة الجريمة التي تتجاوز الحدود الجغرافية. نحلل مبادئ الاختصاص الإقليمي، الشخصي، والعالمي في الجرائم السيبرانية.

نناقش إشكالية تعارض الاختصاص بين دول متعددة، ودور اتفاقيات التسليم القضائي في مواجهة هذه التحديات. ندرس مبدأ مكان وقوع الأثر كأساس للاختصاص في حماية البنى التحتية.

نخلص إلى أن التعاون القضائي الدولي هو السبيل الوحيد لمعالجة مشكلة الاختصاص، وأن الاعتماد على

الاختصاص الإقليمي وحده غير كافٍ في الفضاء الإلكتروني.

الفصل التاسع

التعاون الدولي في مجال الأدلة الجنائية الرقمية

يتناول الإجراءات القانونية لجمع الأدلة الرقمية وحفظها ونقلها بين الدول. نحلل اتفاقية بودابست للجرائم الإلكترونية ودورها في توحيد إجراءات التعاون.

نناقش تحديات السرية المصرفية وخصوصية البيانات عند طلب الأدلة من شركات تكنولوجيا عالمية. ندرس آليات الحفظ السريع للبيانات ومنع العبث بها قبل استلام طلبات التعاون الرسمي.

نخلص إلى أن سرعة تبادل الأدلة هي عامل حاسم

في نجاح التحقيقات، وأن البيروقراطية في طلبات التعاون الدولي قد تؤدي إلى ضياع الأدلة الرقمية الزائلة.

الجزء الرابع

آليات الدفاع والاستجابة القانونية

الفصل العاشر

الدفاع السيبراني النشط والإجراءات المضادة

يستعرض هذا الفصل الجدل القانوني حول مشروعية الإجراءات المضادة النشطة مثل اختراق مصدر الهجوم لتعطيله. نحلل الفرق بين الدفاع المشروع عن النفس والإجراءات الانتقامية غير القانونية.

نناقش حدود تفويض القطاع الخاص في اتخاذ إجراءات دفاعية نشطة نيابة عن الدولة أو عن أنفسهم. ندرس المخاطر القانونية لتصعيد النزاع عبر إجراءات مضادة غير محسوبة.

نخلص إلى أن الإجراءات المضادة يجب أن تخضع لرقابة دولة صارمة وتلتزم بمبادئ التناسب والضرورة، لمنع تحول الفضاء الإلكتروني إلى ساحة فوضى قانونية.

الفصل الحادي عشر

دور القطاع الخاص في حماية البنية التحتية

يركز على الشراكة بين الحكومة والقطاع الخاص الذي يملك ويدير معظم البنى التحتية الرقمية. نحلل الالتزامات القانونية للشركات في الإبلاغ عن الحوادث وتطبيق معايير الأمن.

نناقش المسؤولية القانونية للشركات عن الإهمال في حماية الأنظمة التي تؤدي لأضرار جسيمة للجمهور. ندرس نماذج للحوافز القانونية والتأمينية لتعزيز الامتثال الأمني.

نخلص إلى أن الحماية الفعالة تتطلب شراكة استراتيجية حيث تتحمل الدولة مسؤولية التنسيق والسياسات، ويتحمل القطاع الخاص مسؤولية التنفيذ والامتثال الفني.

الفصل الثاني عشر

التأمين السيبراني وإدارة المخاطر القانونية

يتناول الدور المتزايد للتأمين في إدارة المخاطر القانونية والمالية الناتجة عن الهجمات. نحلل شروط تغطية الهجمات السيبرانية واستثناءات الحرب

السيبرانية في بوالص التأمين.

نناقش كيف يؤثر وجود التأمين على الدعاوى القضائية ومسؤولية التعويض. ندرس دور شركات التأمين في فرض معايير أمنية كشرط للتغطية.

نخلص إلى أن التأمين السيبراني أصبح أداة قانونية واقتصادية هامة لنقل المخاطر، ولكنه لا يغني عن الالتزام بالوقاية والمسؤولية القانونية المباشرة.

الجزء الخامس

المستقبل والتطوير التشريعي

الفصل الثالث عشر

نحو اتفاقية دولية شاملة للجرائم السيبرانية

يستشرف هذا الفصل الحاجة إلى معاهدة دولية جديدة تحت مظلة الأمم المتحدة تحكم السلوك في الفضاء الإلكتروني. نحلل مقترحات الدول الكبرى ومواقفها من مسودة الاتفاقية المرتقبة.

نناقش التحديات السياسية في التوصل لإجماع حول تعريف الهجوم السيبراني وآليات العقاب. ندرس دور المنظمات الدولية المتخصصة في صياغة المعايير الفنية والقانونية.

نخلص إلى أن الاتفاقية الدولية هي الهدف الاستراتيجي لتحقيق الاستقرار، ولكنها تتطلب تنازلات سياسية كبيرة من الدول الكبرى بشأن سيادتها الرقمية.

الفصل الرابع عشر

الذكاء الاصطناعي والهجمات ذاتية التشغيل

يتناول التحديات القانونية الناشئة عن استخدام الذكاء الاصطناعي في شن الهجمات أو الدفاع عنها. نحلل مسؤولية الإنسان عن أفعال الأنظمة المستقلة التي تتخذ قرارات هجومية.

نناقش الحاجة إلى حظر دولي لأسلحة السيبرانية ذاتية التشغيل التي لا تخضع لرقابة بشرية ذات معنى. ندرس الثغرات القانونية الحالية في مواجهة الخوارزميات الهجومية.

نخلص إلى أن القانون يجب أن يسبق التكنولوجيا في هذا المجال، وأن مبدأ المسؤولية الإنسانية يجب أن يظل ركنًا أساسيًا في أي استخدام للقوة السيبرانية.

الفصل الخامس عشر

حماية البيانات الشخصية أثناء الهجمات السيبرانية

يركز على التوازن بين ضرورة جمع البيانات للتحقيق في الهجمات وحماية خصوصية الأفراد. نحلل القيود القانونية على مراقبة الاتصالات أثناء حالات الطوارئ السيبرانية.

نناقش حقوق الضحايا في التعويض عن انتهاك بياناتهم الشخصية نتيجة الهجمات على البنى التحتية. ندرس التزامات الجهات المشغلة بإخطار الأفراد عند حدوث خروقات.

نخلص إلى أن حماية الخصوصية لا يجب أن تتعطل أثناء الأزمات، وأن الشفافية في التعامل مع بيانات الضحايا هي واجب قانوني وأخلاقي.

الفصل السادس عشر

بناء القدرات القانونية والقضائية الوطنية

يتناول الحاجة لتطوير الكوادر القانونية والقضائية المتخصصة في الجرائم السيبرانية. نحلل ضرورة إنشاء نيابات ومحاكم متخصصة ذات خبرة تقنية وقانونية.

نناقش برامج التدريب المشترك بين القانونيين وخبراء الأمن السيبراني. ندرس أهمية تبادل الخبرات الدولية ورفع كفاءة الأجهزة القضائية الوطنية.

نخلص إلى أن التكنولوجيا وحدها لا تكفي، بل تحتاج إلى عقل قانوني قادر على توظيفها في إطار العدالة، وأن الاستثمار في التعليم القانوني التقني هو استثمار في الأمن القومي.

الخاتمة

نحو ميثاق أخلاقي وقانوني للفضاء الإلكتروني

يختتم هذا الكتاب بتوليفة شاملة تؤكد أن الفضاء الإلكتروني لم يعد منطقة برية، بل أصبح مجالًا حيويًا يتطلب حكم القانون. يطرح الكتاب رؤية مستقبلية تقوم على ثلاثة أركان: التعاون الدولي الفعال، والتشريعات الوطنية الرادعة، والشراكة الاستراتيجية مع القطاع الخاص.

يختتم المؤلف بالتأكيد على أن حماية البنية التحتية الحيوية هي مسؤولية مشتركة، وأن القانون هو الضامن الوحيد لاستخدام التكنولوجيا لخدمة البشرية لا لتدميرها. وأن المستقبل سيكون للدول التي تستطيع بناء حصن رقمي قانوني يردع المعتدي ويحمي الم innocent.

إن التحدي القانوني للهجمات السيبرانية هو تحدي وجودي، يتطلب إرادة سياسية وفقهًا قانونيًا جريئًا يواكب سرعة التطور التكنولوجي، ويحافظ في نفس الوقت على مبادئ العدالة وسيادة القانون.

والله ولي التوفيق، وهو الهادي إلى سواء السبيل.

تم بحمد الله وتوفيقه

الدكتور محمد كمال عرفه الرخاوي

الباحث والمستشار والخبير والفقيه والمؤلف القانوني والمحاضر الدولي في القانون