حرب بلا جنود

د. محمد كمال عرفه الرخاوي

الباحث والمستشار والخبير والفقيه والمؤلف القانوني والمحاضر الدولي في القانون

الاهداء

الي روح امي وابي الطاهره داعيا الله لهم بالرحمه والمغفره والفردوس الاعلي وجنه الخلد يارب العالمين

والي ابنتي الحبيبه قره عيني صبرينال المصريه الجزائريه جميله الجميلات التي تجمع بين جمال نهر النيل الخالد وعظمه الاهرامات وشط المتوسط وجبال الاوراس الشامخه وعظمه الجسور المعلقه

الفصل التاسع والعشرون السيطرة البشرية على قرار الحياة والموت

الفصل الثلاثون نحو دستور رقمي يحمي مستقبل الإنسانية

مقدمة

يشهد العالم تحولاً جذرياً في طبيعة الصراعات حيث انتقلنا من حروب الخنادق والدبابات إلى معارك خفية تدور في الأعماق الرقمية للشبكات العالمية لم يعد الجندي يرتدي زياً عسكرياً واضحاً بل أصبح المقاتل مبرمجاً يجلس في غرفة مكيفة الهواء بعيداً عن خطوط النار المباشرة هذا التغير الهائل وضع القانون الدولي التقليدي أمام اختبار وجودي صعب فالمواثيق التي صيغت في القرن العشرين لتنظيم علاقات بين دول ذات حدود جغرافية ثابتة تبدو عاجزة أمام عدو لا يرى ولا يلمس ويضرب من أي مكان في الكرة الأرضية

في لحظة واحدة هدف هذا الكتاب هو تسليط الضوء على هذه الفجوة الخطيرة بين سرعة تطور التكنولوجيا وبطء استجابة التشريعات الدولية نحن لا نتحدث عن سيناريوهات خيالية للمستقبل بل عن واقع نعيشه الآن حيث يمكن لكود برمجي واحد أن يشل اقتصاد دولة كاملة أو يعطل أنظمة المياه والكهرباء عن مدن بأكملها مما يسبب معاناة إنسانية تفوق أحياناً آثار القصف التقليدي سنغوص في ثلاثين فصلاً لاستكشاف كافة الجوانب القانونية والأخلاقية لهذه الحرب الجديدة بدءاً من مشكلة تحديد المعتدي ومروراً بحماية المدنيين في الفضاء الافتراضي ووصولاً إلى مسألة المساءلة الجنائية للذكاء الاصطناعي إن الرسالة الأساسية هي أن التكنولوجيا قد تغير أدوات الحرب لكن المبادئ الإنسانية يجب أن تظل ثابتة وأن القانون الدولي مطالب بالتطور السريع ليصبح درعاً واقياً يضمن ألا تتحول الشبكة العنكبوتية إلى ساحة للدمار الشامل دون رادع أو قانون يحمي الضعفاء من بطش الأقوياء تقنياً.

الفصل الأول

في بداية القرن الحادي والعشرين تغيرت ملامح الحروب بشكل جذري لم يعد الجنود يرتدون زيًا عسكريًا أخضر أو يحملون بنادق تقليدية في أيديهم بل أصبح العدو خفيًا يجلس أمام شاشة كمبيوتر في غرفة مظلمة بعيدة آلاف الكيلومترات عن ساحة المعركة الحقيقية هذا التحول الكبير فرض تحديات هائلة على القانون الدولي الذي صُمم في الأصل لتنظيم صراعات بين جيوش نظامية تتواجه في حدود جغرافية محددة الآن أصبحت الحدود رقمية وسيادة الدول مهددة بكود برمجي واحد قد يشل حياة ملايين البشر في لحظة واحدة دون إطلاق رصاصة واحدة مما يستدعي إعادة نظر شاملة في مفاهيم السيادة والدفاع الشرعي.

الفصل الثاني

مفهوم السيادة الوطنية الذي تأسس عليه النظام الدولي الحديث منذ معاهدة وستفاليا يواجه الآن اختبارًا وجوديًا حقيقيًا في الفضاء الإلكتروني فحين

تخترق مجموعة قراصنة خوادم دولة ما وتسرق بيانات حساسة أو تعطل خدمات حيوية هل يعتبر هذا انتهاكًا لسيادة الأرض أم أنه مجرد جريمة عادية الفرق كبير جدًا لأن انتهاك السيادة يبرر ردود فعل دولية وسياسية وعسكرية بينما الجريمة العادية تبقى في إطار التعاون القضائي البوليسي الدول بدأت تدرك أن بيانات مواطنيها وبنيتها التحتية الرقمية هي جزء لا يتجزأ من إقليمها الوطني مما يدفع نحو تطوير نظرية السيادة الرقمية التي تحمي الفضاء الإلكتروني للدولة كما تحمي حدودها البرية والبحرية والجوية من أي اعتداء خارجي.

الفصل الثالث

التحدي الأكبر في حرب المستقبل هو تحديد هوية المهاجم بدقة ففي الحروب التقليدية كان من السهل معرفة الدولة المعتدية من خلال زي الجنود أو علامة الدبابات أما في الحرب السيبرانية فالمهاجم قد يخفي مساره عبر خوادم في دول ثالثة أو يستخدم برمجيات ذكية تمحو آثارها تلقائيًا هذه المشكلة تسمى

مشكلة الإسناد أو النسبة وهي العقبة الرئيسية أمام تطبيق القانون الدولي فإذا لم نستطع إثبات أن دولة ما تقف وراء الهجوم كيف يمكننا محاسبتها أو الرد عليها وفق ميثاق الأمم المتحدة هذا الغموض يمنح المهاجمين حصانة شبه كاملة ويجعل العالم يعيش في حالة من الشك الدائم والترقب الخطير لأي حركة مشبوهة على الشبكة العنكبوتية العالمية.

الفصل الرابع

هل يمكن اعتبار الهجوم الإلكتروني هجومًا مسلحًا بالمعنى القانوني للكلمة هذا السؤال يشغل بال юристين والعسكريين حول العالم فالمادة واحد وخمسون من ميثاق الأمم المتحدة تمنح الدول حق الدفاع عن نفسها إذا تعرضت لهجوم مسلح لكن هل قطع الكهرباء عن مستشفى أو تعطيل شبكة المياه يعتبر استخدامًا للقوة المسلحة إذا تسببت هذه الأفعال في وفيات بشرية فإن الكثير من الخبراء يميلون إلى القول بنعم أما إذا كان الضرر ماديًا فقط فالأمر يختلف القانون الدولي الإنساني يحتاج إلى تحديث

ليشمل بوضوح الهجمات التي تسبب دمارًا وظيفيًا حيويًا حتى لو لم تستخدم متفجرات تقليدية لأن النتيجة النهائية قد تكون مأساوية بنفس القدر من القصف الجوي العنيف.

الفصل الخامس

مبدأ التمييز في القانون الدولي الإنساني يوجب على المقاتلين التمييز بين الأهداف العسكرية والمدنيين وحظر الهجمات العشوائية لكن كيف يطبق الذكاء الاصطناعي هذا المبدأ عند شن هجوم سيبراني الخوارزميات قد لا تفرق بين شبكة كهرباء تخص قاعدة عسكرية وتلك تخص حيًا سكنيًا إذا كانت متصلة بنفس الشبكة هذا الخطأ البشري أو البرمجي قد يؤدي إلى كوارث إنسانية ضخمة بدون نية مسبقة لذلك يطالب نشطاء الحقوق بإنشاء بروتوكولات دولية تلزم الدول باختبار برمجياتها الحربية للتأكد من قدرتها على التمييز قبل استخدامها وإلا تحملت المسؤولية الكاملة عن أي ضرر يلحق بالمدنيين نتيجة خلل تقني في أنظمة الهجوم الإلكتروني الذاتي التشغيل.

الفصل السادس

مبدأ التناسب هو حجر الزاوية في قوانين الحرب وينص على ألا يكون الضرر المدني الناتج عن هجوم عسكري مفرطًا مقارنة بالميزة العسكرية المتوقعة في الحرب السيبرانية يصبح تطبيق هذا المبدأ معقدًا جدًا فهجوم إلكتروني صغير قد يتسبب في سلسلة تفاعلية غير متوقعة تعطل أنظمة طيران مدنية أو أسواق مالية عالمية كيف نحسب التناسب هنا القانون الدولي يحتاج إلى معايير جديدة لتقييم الأضرار غير المباشرة والمتسلسلة في الفضاء الرقمي فلا يمكن قبول رد فعل عسكري تقليدي ضخم مقابل ضرر رقمي محدود إلا إذا كانت العواقب البشرية للهجوم الرقمي تعادل قصفًا تقليديًا مدمرًا للمدن والسكان الأبرياء.

الفصل السابع

دور الشركات الخاصة في الحرب السيبرانية أصبح

محوريًا وخطيرًا في آن واحد فشركات التكنولوجيا الكبرى تملك بنية تحتية رقمية تفوق قوة العديد من الدول وقد تستأجر حكومات خدماتها للهجوم أو الدفاع هذا يخلق فئة جديدة من المرتزقة الرقميين الذين يعملون تحت غطاء تجاري بعيدًا عن المساءلة القانونية المباشرة إذا ارتكبت شركة خاصة جريمة حرب إلكترونية بناءً على عقد مع دولة من يتحمل المسؤولية هل الدولة الأمرة أم الشركة المنفذة القانون الدولي الحالي لا يغطي هذا الفراغ بوضوح مما يستدعي وضع اتفاقيات جديدة تنظم عمل المقاولين العسكريين والأمنيين في المجال الرقمي وتخضعهم للمساءلة الدولية المباشرة مثل أي جيش نظامي.

الفصل الثامن

الحصانة الدبلوماسية تواجه تحديًا جديدًا في العصر الرقمي فحين يتم اختراق أجهزة دبلوماسيين أو سرقة وثائق من سفارات عبر وسائل إلكترونية هل ينطبق مبدأ حرمة البعثات الدبلوماسية على البيانات الرقمية المخزنة في خوادم خارج الإقليم الجغرافي للسفارة

البعض يقول إن البيانات هي امتداد للمبنى الدبلوماسي والبعض الآخر يرى أنها مجرد معلومات عادية هذا الجدل القانوني يحتاج إلى حسم لأن انتهاك البيانات الدبلوماسية قد يكون أخطر من اقتحام مبنى فعلي لأنه يكشف أسرار دولة كاملة دون ترك أثر مادي واضح مما يهدد استقرار العلاقات الدولية ويثير شكوكًا عميقة بين الدول المتحالفة سابقًا.

الفصل التاسع

جرائم الحرب في الفضاء الإلكتروني تحتاج إلى تعريف دقيق في نظام روما الأساسي للمحكمة الجنائية الدولية حاليًا النصوص تركز على الأفعال المادية الملموسة مثل القتل والتعذيب وتدمير الممتلكات لكن التدمير الرقمي الذي يؤدي إلى مجاعة أو انهيار نظام صحي قد لا يندرج بوضوح تحت هذه التعريفات هناك دعوات متزايدة لإضافة بروتوكول رقمي لنظام روما يجرم الأفعال الإلكترونية التي تسبب معاناة بشرية واسعة النطاق هذا التطور ضروري لضمان عدم إفلات مجرمي الحرب الرقميين من العقاب ولإرسال رسالة واضحة بأن

القانون الدولي يطال كل من يسبب الدمار بغض النظر عن الوسيلة التقنية المستخدمة في تنفيذ جريمته البشعة.

الفصل العاشر

مسألة الاختصاص القضائي في الجرائم السيبرانية العابرة للحدود معقدة للغاية فالمهاجم قد يكون في دولة والضحية في ثانية والخادم في ثالثة أي قانون يطبق وأي محكمة تختص بالنظر في القضية القانون الدولي التقليدي يعتمد على الإقليمية أو الجنسية لكن هذه المعايير تهتز أمام طبيعة الإنترنت السائلة هناك حاجة ماسة لإنشاء محكمة دولية متخصصة في الجرائم السيبرانية أو على الأقل توحيد التشريعات الوطنية لتسهيل التسليم والمحاكمة دون ثغرات يستغلها المجرمون للاختباء وراء حدود دول لا تتعاون قضائيًا مع المجتمع الدولي في ملاحقة هذه الجرائم الخطيرة.

الفصل الحادي عشر

الدفاع السيبراني الجماعي أصبح ضرورة استراتيجية للدول الصغيرة التي لا تملك موارد كافية لحماية بنيتها التحتية الرقمية حلف الناتو مثلاً أعلن أن الهجوم السيبراني الكبير قد يثير بند الدفاع الجماعي لكن شروط تطبيق هذا البند لا تزال غامضة ومتروكة للتقدير السياسي كل حالة على حدة هذا الغموض قد يشجع المهاجمين على اختبار حدود التحالفات الدولية بهجمات متوسطة لا تصل لعتبة الحرب الشاملة لكنها كافية لإلحاق ضرر كبير القانون الدولي يحتاج إلى توضيح عتبات الرد الجماعي على الهجمات الرقمية لضمان ردع فعال وحماية حقيقية للأعضاء الضعفاء في النظام الدولي من الابتزاز الرقمي المستمر.

الفصل الثاني عشر

البيانات الضخمة أصبحت سلاحًا استراتيجيًا في الحروب الحديثة فجمع معلومات عن مواطني دولة أخرى وتحليلها للتأثير على انتخاباتها أو زعزعة

استقرارها الداخلي يعتبر شكلاً جديداً من أشكال التدخل في الشؤون الداخلية المحظورة دولياً لكن صعوبة إثبات المصدر والتأثير المباشر تجعل المساءلة القانونية شبه مستحيلة كيف نثبت أن حملة إعلانية ممولة خارجياً غيرت نتيجة انتخابات دولة ما القانون الدولي يحتاج إلى آليات جديدة للتحقيق في عمليات التأثير النفسي والمعرفي عبر الإنترنت واعتبارها انتهاكاً للسيادة إذا تم تمويلها وتنسيقها من قبل جهات أجنبية بهدف الإضرار بالاستقرار السياسي للدولة المستهدفة بشكل ممنهج.

الفصل الثالث عشر

الأسلحة ذاتية التشغيل بالكامل تثير مخاوف أخلاقية وقانونية جسيمة فحين يفوض القائد العسكري آلة لاتخاذ قرار القتل دون تدخل بشري مباشر من يتحمل المسؤولية القانونية عن الخطأ هل المبرمج أم الآلة أم القائد القانون الدولي الحالي يفترض وجود إنسان يتخذ القرار ويحمل النية الإجرامية غياب العنصر البشري في حلقة القتل يفرغ مبدأ المسؤولية الجنائية من محتواه

لذلك هناك حركة دولية قوية تدعو إلى حظر كامل للأسلحة القاتلة المستقلة قبل تطويرها بشكل واسع الحفاظ على السيطرة البشرية على استخدام القوة المميتة هو خط أحمر يجب عدم تجاوزه لضمان بقاء الأخلاق ضمن معادلات الحرب المستقبلية.

الفصل الرابع عشر

حماية البنية التحتية الحيوية مثل السدود ومحطات الطاقة النووية والمستشفيات من الهجمات السيبرانية تعتبر أولوية قصوى للقانون الدولي الإنساني هذه الأهداف محمية تقليديًا من القصف لكن حمايتها من الهجمات الإلكترونية تحتاج إلى ضمانات تقنية وقانونية إضافية فاختراق نظام تحكم في سد قد يسبب فيضانًا مدمرًا يعادل قصفه بالطائرات الدول مطالبة باتخاذ احتياطات خاصة لتأمين هذه الأنظمة وعدم استخدامها كأدوات هجومية حتى في حالات الرد لأن العواقب قد تكون كارثية ولا يمكن السيطرة عليها مما يهدد حياة سكان دول بأكملها وليس فقط دولة العدو المباشر في النزاع المسلح الحالي.

الفصل الخامس عشر

دور الأمم المتحدة في تنظيم الفضاء الإلكتروني لا يزال محدوداً وغير فعال مقارنة بسرعة التطور التكنولوجي اللجان الحالية تفتقر إلى السلطة التنفيذية وتعتمد على توافق الآراء الذي نادراً ما يتحقق بسبب المصالح المتضادة للدول الكبرى هناك دعوات لإنشاء وكالة دولية جديدة متخصصة في الأمن السيبراني تحت مظلة الأمم المتحدة تملك سلطة التحقيق ووضع المعايير الملزمة وفرض عقوبات على الدول المنتهكة بدون هذه الهيئة الفعالة سيبقى الفضاء الإلكتروني منطقة رمادية يسودها قانون الغاب وتغيب فيها سيادة القانون الدولي العادل الذي يحمي الضعفاء من بطش الأقوياء تقنياً.

الفصل السادس عشر

العقوبات الدولية في العصر الرقمي تأخذ أشكالاً

جديدة غير مسبوقة فبدلاً من حظر التجارة التقليدية يمكن شل اقتصاد دولة ما بمنعها من الوصول إلى أنظمة الدفع العالمية أو خوادم الإنترنت الأساسية هل يعتبر هذا الفعل عقوبة قانونية أم حرباً إلكترونية غير معلنة الخط الفاصل بينهما رفيع جداً وقد يؤدي إلى تصعيد غير محسوب العقوبات الرقمية الشاملة قد تسبب معاناة إنسانية واسعة للمدنيين العاديين مما قد ينتهك مبادئ القانون الدولي الإنساني الذي يحظر تجويع السكان كأسلوب للحرب لذا يجب وضع ضوابط صارمة لاستخدام الأدوات الرقمية كأداة للعقوبات الدولية لضمان عدم تحولها إلى أداة دمار شامل اقتصادي واجتماعي.

الفصل السابع عشر

الخصوصية الفردية في زمن الحرب السيبرانية تصبح ضحية سهلة فجمع البيانات البيومترية والسلوكية للمدنيين تحت ذريعة الأمن الوطني أو مكافحة الإرهاب قد يتحول إلى أداة قمع ومراقبة جماعية تنتهك حقوق الإنسان الأساسية القانون الدولي لحقوق الإنسان

يظل ساريًا حتى في أوقات النزاع المسلح لكن التطبيق يصبح صعبًا مع التقنيات الخفية هناك حاجة لآليات رقابة دولية مستقلة لمراقبة استخدام الدول للتقنيات الرقمية في مراقبة مواطنيها أو مواطني الدول الأخرى وضمان عدم استخدام هذه البيانات لأغراض تتجاوز الضرورة العسكرية المباشرة والمشروعة وفقًا للقانون الدولي الإنساني الواجب التطبيق.

الفصل الثامن عشر

الحرب النفسية عبر وسائل التواصل الاجتماعي أصبحت جزءًا لا يتجزأ من الصراعات الحديثة فنشر الشائعات والأخبار المزيفة لبث الرعب أو تحريض الطوائف على بعضها البعض يعتبر سلاحًا فتاكًا قد يسبب حروبًا أهلية دون طلقة واحدة هل ينطبق قانون الحرب على هذه العمليات المعلوماتية إذا كانت تهدف إلى إضعاف معنويات العدو نعم لكن إذا استهدفت المدنيين مباشرة لترويعهم فهي محظورة التحدي يكمن في إثبات النية والمصدر القانون الدولي يحتاج إلى تطوير مفاهيم جديدة لحماية العقل البشري من

التلاعب المنظم عبر الشبكات واعتبار الفضاء المعرفي مجالًا محميًا من الهجمات المضللة التي تهدد السلم والأمن الدوليين بشكل جدي.

الفصل التاسع عشر

مسؤولية الدول عن أفعال القراصنة غير التابعين لها تظل موضوعًا شائكًا في القانون الدولي إذا لم توجه الدولة القراصنة أو تسيطر عليهم فعليًا فلا تتحمل المسؤولية المباشرة لكن إذا كانت تعلم بنشاطهم ولم تتخذ إجراءً لمنعه من أراضيها فقد تكون مسؤولة عن الإهمال هذا المبدأ يحتاج إلى تشديد في العصر الرقمي فالقدرة على المراقبة والتحكم في الفضاء الإلكتروني الوطني أصبحت متاحة للدول لذا يجب أن تتحمل مسؤولية أكبر في منع استخدام أراضيها الرقمية كمنطلق لهجمات ضد دول أخرى وإلا تعرضت للمساءلة الدولية والتعويضات عن الأضرار الناتجة عن تقصيرها الواضح.

الفصل العشرون

التعاون الدولي في مجال الأدلة الجنائية الرقمية يعاني من بطء شديد مقارنة بسرعة محو الآثار في الفضاء الإلكتروني اتفاقيات المساعدة القانونية المتبادلة تستغرق أشهرًا بينما يمكن حذف البيانات في ثوانٍ هذا الفجوة الزمنية تجعل ملاحقة مجرمي الحرب الرقميين شبه مستحيلة هناك حاجة ملحة لإجراءات سريعة ومبسطة لتجميد البيانات وتبادل الأدلة في حالات الجرائم الدولية الخطيرة دون الانتظار للإجراءات البيروقراطية الطويلة إنشاء قنوات اتصال مباشرة بين وحدات الجرائم السيبرانية الوطنية تحت إشراف دولي قد يكون حلاً عمليًا لسد هذه الفجوة وإنقاذ الأدلة قبل فوات الأوان في التحقيقات الدولية المهمة.

الفصل الحادي والعشرون

حماية الصحفيين والنشطاء في الحروب السيبرانية أصبحت ضرورة ملحة فاستهداف حساباتهم أو اختراق أجهزتهم لكشف مصادرهم أو إسكات أصواتهم يعتبر

انتهاكًا صريحًا لحرية التعبير والحقوق الإنسانية القانون الدولي يحمي الصحفيين في مناطق النزاع لكن هذه الحماية لا تمتد بوضوح إلى الفضاء الرقمي حيث يتعرضون لمخاطر أكبر قد تصل إلى التهديد بالقتل الحقيقي بعد تحديد مواقعهم رقميًا يجب تعزيز الآليات الدولية لحماية هوية الصحفيين الرقميين وضمان عدم استخدام التقنيات العسكرية لتتبعهم أو استهدافهم لأن دورهم في كشف الحقائق أهم من أي اعتبار عسكري في الحفاظ على شفافية النزاعات ومساءلة المرتكبين.

الفصل الثاني والعشرون

الذكاء الاصطناعي في جمع المعلومات الاستخباراتية يثير تساؤلات حول حدود التجسس المسموح به دوليًا فبينما يعتبر التجسس التقليدي ممارسة مقبولة ضمنيًا بين الدول رغم عدم شرعيته رسميًا فإن استخدام الذكاء الاصطناعي لجمع بيانات شاملة عن كل مواطن في دولة أخرى يغير المعادلة تمامًا هذا الكم الهائل من البيانات قد يستخدم لتدمير الاقتصاد أو

التلاعب السياسي مما يتجاوز مفهوم التجسس التقليدي إلى مفهوم الحرب الخفية القانون الدولي يحتاج إلى تحديد خط أحمر واضح بين جمع المعلومات الاستخباراتية المشروع وبين العمليات الهجومية المقنعة التي تهدد استقرار الدول بشكل جوهري ومباشر.

الفصل الثالث والعشرون

مسألة الحياد في الفضاء الإلكتروني تواجه اختبارات صعبة فحين تمر هجمات سيبرانية من دولة محايدة ضد دولة أخرى عبر خوادمها هل تفقد دولة المرور حيادها القانون الدولي التقليدي ينص على واجب الدولة المحايدة في منع استخدام إقليمها لأعمال حربية لكن تطبيق هذا على تدفق البيانات الصعب التحكم فيه يمثل تحديًا تقنيًا وقانونيًا كبيرًا الدول المحايدة مطالبة بتطوير قدراتها على مراقبة حركة البيانات عبر حدودها الرقمية واتخاذ إجراءات فورية لقطع أي هجمات تمر عبر بنيتها التحتية وإلا تعرضت للمساءلة القانونية وقد تفقد حصانتها كدولة محايدة

في النزاع الدائر حولها.

الفصل الرابع والعشرون

تعويض ضحايا الحروب السيبرانية يظل حلمًا بعيد المنال في كثير من الأحيان فصعوبة إثبات الضرر المادي المباشر وربطه بهجوم إلكتروني محدد تجعل مطالبات التعويض تفشل في المحاكم الدولية بالإضافة إلى أن العديد من الدول تتمتع بالحصانة السيادية التي تمنع مقاضاتها أمام محاكم دول أخرى هناك حاجة لإنشاء صندوق دولي لتعويض ضحايا الهجمات السيبرانية الكبرى يمول من مساهمات الدول أو من غرامات تفرض على الدول المنتهكة هذا الصندوق قد يوفر شبكة أمان للضحايا الذين يفقدون مدخراتهم أو خدماتهم الحيوية بسبب هجمات لا يستطيعون مقابلة مرتكبيها قضائيًا بشكل مباشر وفعال.

الفصل الخامس والعشرون

دور المجتمع المدني والمنظمات غير الحكومية في رصد انتهاكات القانون الدولي في الفضاء الإلكتروني أصبح حاسمًا فهذه المنظمات تملك مرونة وقدرة تقنية عالية قد لا تتوفر للدول أو المنظمات الدولية الرسمية يمكن لهذه الجهات توثيق الهجمات وتحليل البرمجيات الخبيثة وكشف هويات المهاجمين بشكل مستقل تقديم تقارير موثقة من جهات محايدة يساعد في بناء سجل تاريخي للانتهاكات ويضغط على الدول للامتثال للقانون الدولي تعزيز دور هذه المنظمات ومنحها صفة مراقب في المحافل الدولية المعنية بالأمن السيبراني قد يوازن ميزان القوى ويكشف الحقائق التي تحاول الدول إخفاءها خلف ستار الأمن القومي المزيف.

الفصل السادس والعشرون

التعليم والتدريب على القانون الدولي الإنساني يجب أن يشمل الآن وحدات متخصصة في الحرب السيبرانية للقوات المسلحة والمبرمجين على حد سواء فالجندي التقليدي يحتاج لفهم قواعد الاشتباك الرقمية والمبرمج العسكري يحتاج لفهم العواقب القانونية

لكوده البرمجي دمج هذه المعرفة في المناهج العسكرية والأكاديمية ضروري لبناء جيل جديد من المقاتلين الرقميين الواعين بالتزاماتهم القانونية تجاه الإنسانية عدم الاهتمام بهذا الجانب التدريبي قد يؤدي إلى ارتكاب جرائم حرب غير مقصودة نتيجة جهل بالقواعد الناظمة للعمليات الإلكترونية في ساحات المعارك الحديثة والمعقدة تقنيًا.

الفصل السابع والعشرون

الأخلاقيات التقنية يجب أن تسبق التشريعات القانونية في مجال الحرب السيبرانية فالقانون دائمًا يتأخر عن التكنولوجيا لذا فإن التزام المهندسين والمطورين بمدونات سلوك أخلاقية تمنعهم من تطوير أدوات هجومية عشوائية أو قاتلة ذاتيًا يعتبر خط الدفاع الأول قبل تدخل المشرع الدولي الجمعيات المهنية العالمية للتكنولوجيا مطالبة بوضع معايير صارمة لعضويتها تربط بين الممارسة المهنية والالتزام بحقوق الإنسان والقانون الدولي رفض تطوير برمجيات تنتهك هذه المبادئ يجب أن يكون خيارًا متاحًا ومحميًا للمطورين

الذين يرفضون المشاركة في صناعة أدوات الدمار الرقمي التي تهدد مستقبل البشرية جمعاء.

الفصل الثامن والعشرون

مستقبل المعاهدات الدولية يحتاج إلى مرونة غير مسبوقة لمواكبة التغير التكنولوجي السريع فالمعاهدات التقليدية تستغرق سنوات للتفاوض والتصديق بينما تتطور التقنيات في أشهر لذا يجب اعتماد نموذج المعاهدات الإطارية التي تضع مبادئ عامة قابلة للتحديث عبر بروتوكولات فنية سريعة الإصدار هذا النموذج يسمح للمجتمع الدولي بالاستجابة السريعة للتهديدات الجديدة دون الحاجة لإعادة التفاوض على المعاهدة كاملة من البداية كل مرة تبني نظام قانوني مرن وقابل للتكيف هو السبيل الوحيد لضمان فعالية القانون الدولي في مواجهة تحديات الحرب السيبرانية المتسارعة باستمرار.

الفصل التاسع والعشرون

الرؤية المستقبلية للحرب بلا جنود تتجه نحو زيادة الاعتماد على الأنظمة المستقلة تمامًا مما قد يفقد البشر السيطرة النهائية على قرار بدء الحرب أو إنهائها هذا السيناريو الكارثي يتطلب تدخلاً دوليًا عاجلاً لفرض سيطرة بشرية إلزامية على أي نظام سلاح مهما بلغت درجة ذكائه الحفاظ على الكرامة الإنسانية يتطلب ألا تكون الحياة والموت بيد خوارزمية لا ترحم لا تفهم قيمة الروح البشرية القانون الدولي يجب أن يكون الحارس الأخير لهذه القيمة الجوهرية بمنع تفويض قرار القتل للآلات وضمان بقاء الإنسان هو صاحب القرار النهائي والمسؤول الأول عن أي دم يراق في ساحة المعركة الرقمية أو التقليدية.

الفصل الثلاثون

في الختام فإن حرب بلا جنود ليست خيالًا علميًا بل هي واقع نعيشه الآن ويتطلب استجابة قانونية وإنسانية فورية لا يمكن الانتظار حتى وقوع الكارثة الكبرى لبدء التحرك تطوير القانون الدولي في العصر

الرقمي مسؤولية مشتركة بين الدول والشركات والمجتمع المدني والأفراد كل طرف يجب أن يلعب دوره في بناء نظام قانوني يحمي الإنسانية من وحشية التكنولوجيا غير المنضبطة الأمل يكمن في وعي البشرية بأن الحدود الرقمية هي حدود إنسانية مشتركة وأن انتهاكها هو انتهاك للجميع فالقانون الدولي يجب أن يتطور ليصبح درعًا رقميًا يظلل العالم كله ويضمن مستقبلاً آمناً للأجيال القادمة بعيدًا عن شبح الحرب الخفية التي لا ترحم.

تم بحمد الله وتوفيقه

د. محمد كمال عرفه الرخاوي

الباحث والمستشار والخبير والفقيه والمؤلف القانوني والمحاضر الدولي في القانون

او النشـر الا باذن المؤلف