

تأثير الحرب السيبرانية على العمل الإنساني العالمي
بين التحديات والاستراتيجيات الوقائيةThe Impact of Cyber Warfare on Global Humanitarian Action:
Between Challenges and Preventive Strategie

عبد الله بوجمعة

جامعة حسيبة بن بو علي الشلف كلية الحقوق و العلوم الإنسانية . مخبر القانون و الأمن
الإنساني

تاريخ الإرسال: 2025/ 11/ 02 تاريخ القبول: 2025/ 11 / 18 تاريخ النشر: 2025/ 12 / 06

ملخص: أدت التحولات الرقمية العالمية إلى بروز الحرب السيبرانية كأحد أخطر أشكال الصراع المعاصر، مستهدفة البنى التحتية والمنظمات الإنسانية. تهدد هذه الحرب مبادئ الحياد وحماية بيانات المستفيدين، مما يضعف الثقة في العمل الإنساني. تشمل أدواتها الهجمات الإلكترونية والبرمجيات الخبيثة والتصيد، التي تُعطّل العمليات الميدانية. وتتنوع الجهات المنفذة بين دول وجماعات مسلحة وقراصنة، مما يصعب المساءلة. لذلك يُعد تطوير سياسات أمن سيبراني فعّالة وبناء شراكات تقنية خطوة أساسية لضمان استدامة وأمان العمل الإنساني.

الكلمات مفتاحية: الحرب السيبرانية، المنظمات الإنسانية ، التحولات الرقمية ، الأمن السربراني.

Abstract: The world has undergone major digital transformations leading to the rise of cyber warfare as a new form of modern conflict targeting states and humanitarian organizations. This warfare threatens neutrality, independence, and data protection, undermining trust in humanitarian action. Its tools—such as malware, phishing, and infrastructure attacks—disrupt operations and coordination. Multiple actors, including states and

hackers, make accountability difficult. Thus, developing strong cybersecurity policies and partnerships is vital to ensure the safety and sustainability of humanitarian work.

1- بوجمعة عبد الله : abbdoboudj0@gmail.com

مقدمة

شهد العالم خلال العقود الأخيرة تحولات جذرية في مجال تكنولوجيا المعلومات والاتصالات، جعلت من الفضاء السيبراني بعداً جديداً للصراع الدولي، فيما يعرف بـ "الحرب السيبرانية". وإذا كانت هذه الحرب قد استهدفت في بداياتها البنى التحتية الحيوية للدول والمؤسسات الاقتصادية، فإنها اليوم تمتد لتطال حتى المجال الإنساني، بما في ذلك المنظمات الدولية والإغاثية التي تعتمد على نظم رقمية متطورة في إدارة أعمالها الميدانية. وتكمن خطورة الحرب السيبرانية في العمل الإنساني في كونها تهدد مبادئ الحياد والاستقلالية، وتضعف ثقة المستفيدين والمتبرعين على حد سواء.

تكتسي دراسة موضوع الحرب السيبرانية وتأثيرها على العمل الإنساني العالمي أهمية بالغة باعتباره مجالاً حديثاً لم ينل بعد ما يستحقه من اهتمام في الدراسات العربية، خاصة في ظل التزايد المطرد للاعتماد على التكنولوجيا الرقمية في تسيير الأنشطة الإنسانية، وما يترتب عنه من مخاطر تهدد مبادئ الحياد والاستقلالية وحماية البيانات.

لقد ارتبط ظهور الحرب السيبرانية بتطور أشكال الحروب التقليدية التي انتقلت من المواجهات العسكرية المباشرة إلى الحروب غير المتماثلة ثم إلى الفضاء الرقمي، حيث أضحت السلاح المعلوماتي أكثر فاعلية وأقل تكلفة مقارنة بالأسلحة

التقليدية. كما أن المنظمات الإنسانية، بفعل اعتمادها المتزايد على التقنيات الحديثة، أصبحت عرضة لهجمات تستهدف تعطيل عملياتها أو سرقة بياناتها أو التشويش على حيادها.

وانطلاقاً من هذا الواقع، تبرز الإشكالية الرئيسية التي يسعى البحث إلى معالجتها والمتمثلة في التساؤل: إلى أي مدى تؤثر الحرب السيبرانية على فعالية وحياد العمل الإنساني العالمي، وما هي الآليات الممكنة لمواجهة تداعياتها؟ تتفرع عن هذه الإشكالية مجموعة من الأسئلة الفرعية تتعلق بطبيعة الحرب السيبرانية وأبعادها، وانعكاس الهجمات على المنظمات الإنسانية، والتحديات التقنية والقانونية والأخلاقية المترتبة عنها، وكذا الاستراتيجيات الوقائية الكفيلة بالحد من مخاطرها.

نهدف من خلال هذا البحث إلى توضيح المفهوم وأبعاده المختلفة، وإبراز انعكاساته على الأنشطة الإنسانية، وتحليل التحديات التي تواجهها المنظمات في هذا المجال، وصولاً إلى تقديم مقترحات عملية.

1. ماهية الحرب السيبرانية وأبعادها الدولية.

1.1 تعريف الحرب السيبرانية.

تُعرّف الحرب السيبرانية بأنها شكل من أشكال الصراع المعاصر الذي يُدار عبر الفضاء الرقمي باستخدام أدوات وتقنيات إلكترونية متطورة تستهدف أنظمة وشبكات المعلومات التابعة لدول أو مؤسسات أو حتى أفراد، وذلك بغرض تعطيلها أو تدميرها أو اختراقها أو السيطرة عليها¹. وتمثل هذه الحرب امتداداً لتطور استراتيجيات الصراع التقليدي، حيث لم يعد الميدان العسكري أو السياسي وحده مجال المواجهة، بل أصبح الفضاء الإلكتروني ساحة جديدة للتنافس والنزاع². وغالباً ما ترتبط الحرب السيبرانية بدوافع سياسية أو عسكرية أو

استخباراتية، كما قد تُوظَّف كجزء من استراتيجيات الردع الحديثة، نظراً لفعاليتها العالية وتكلفتها المنخفضة مقارنة بالحروب التقليدية³.

وتتسم الحرب السيبرانية بعدة خصائص رئيسية، من أبرزها:

- **السرية والغموض**: إذ يصعب تحديد الجهة المنفذة للهجمات بشكل دقيق، مما يعرقل جهود المساءلة القانونية.
- **الطابع العابر للحدود**: فالفضاء السيبراني غير خاضع للحدود الجغرافية التقليدية، مما يجعل آثار الهجوم تمتد إلى مناطق متعددة في وقت قصير.
- **انخفاض التكلفة وارتفاع الفاعلية**: حيث لا تتطلب هذه الحرب تجهيزات عسكرية تقليدية ضخمة، بل تعتمد على المعرفة التقنية والبرمجيات.
- **التأثير الواسع**: إذ يمكن أن تستهدف البنى التحتية الحيوية، والمؤسسات الاقتصادية، بل وحتى المنظمات الإنسانية العاملة ميدانياً⁴.

2.1 أدوات الحرب السيبرانية

تتنوع أدوات الحرب السيبرانية بشكل كبير، حيث يستخدم الفاعلون في هذا المجال مزيجاً من التقنيات الرقمية والأساليب الهندسية الاجتماعية لتحقيق أهدافهم، سواء كانت عسكرية أو سياسية أو حتى اقتصادية. ومن أبرز هذه الأدوات:

الهجمات الموزعة لحجب الخدمة (DDoS) تأتي في مقدمة الوسائل الأكثر شيوعاً، إذ تعتمد على توجيه عدد هائل من الطلبات المزيفة إلى خوادم الهدف بشكل يفوق قدرتها الاستيعابية، مما يؤدي إلى تعطيلها عن العمل أو شل قدرتها على تقديم الخدمات الحيوية عبر الإنترنت. وتكتسب خطورتها من بساطتها وسهولة تنفيذها، حيث يمكن لمجموعة محدودة من الأفراد استخدام شبكات

"الحواسيب الزومبي (Botnets) لإحداث شلل واسع في مؤسسات ومنظمات إنسانية تعتمد على أنظمة رقمية للتواصل وتسيير عمليات الإغاثة".⁵

البرمجيات الخبيثة (Malware) تشمل البرمجيات الخبيثة فيروسات، ودوداً (Worms)، وأحصنة طروادة (Trojans)، وبرمجيات الفدية (Ransomware)، وجميعها تُستخدم لاختراق الأنظمة أو تعطيلها أو سرقة بياناتها الحساسة. وتشير تقارير أمنية حديثة إلى أن برمجيات الفدية تمثل التهديد الأكبر للمنظمات الإنسانية، حيث يقوم المهاجمون بتشفير بيانات حساسة وطلب مبالغ مالية ضخمة لفك التشفير، وهو ما يهدد خصوصية المستفيدين من الخدمات الإنسانية ويعرض ثقة المتبرعين لخطر كبير.⁶

هجمات التصيد الإلكتروني (Phishing) وتُعدّ من أكثر الأساليب انتشاراً، إذ يقوم المهاجمون بانتحال هويات مؤسسات أو أفراد موثوقين لإرسال رسائل بريد إلكتروني أو روابط مضلّة، تستهدف إقناع المتلقي بالكشف عن معلوماته السرية مثل كلمات المرور أو بيانات الحسابات المصرفية. وقد استُخدمت هذه الهجمات بكثرة ضد موظفي المنظمات الدولية، مما مكّن جهات معادية من التسلل إلى أنظمة داخلية وسرقة بيانات حساسة.⁷

الاختراقات الموجهة للبنى التحتية الحيوية وتبرز كذلك كأداة ذات تأثير عميق، حيث تسعى هذه الهجمات إلى تعطيل نظم الطاقة، والمياه، والاتصالات، والنقل، واللوجستيات، بل وحتى قواعد بيانات تخص اللاجئين والمحتاجين. ويُعدّ هذا النوع الأخطر، إذ لا يقتصر أثره على تعطيل الأنظمة التقنية، بل يمتد ليوثر بشكل مباشر على حياة الفئات الضعيفة، كما حدث في بعض الحالات التي تعرّضت فيها مستشفيات أو مراكز إغاثة لهجمات إلكترونية أدت إلى توقف خدماتها لفترات حرجية.⁸

إن خطورة هذه الأدوات لا تكمن فقط في قدرتها على إحداث الضرر الآني، وإنما أيضاً في صعوبة التتبع وتحديد هوية المنفذين، الأمر الذي يفتح الباب أمام جهات دولية وغير دولية لاستخدامها كوسيلة ضغط أو ابتزاز، مما يزيد من هشاشة العمل الإنساني في بيئة مضطربة أصلاً.

1. 3 الفاعلون الرئيسيون في الحرب السبرانية.

تتعدد الأطراف الفاعلة في ساحة الحرب السيبرانية، إذ لم تعد مقتصرة على الدول فحسب، بل شملت كذلك فواعل من غير الدول ذات قدرات متنامية. وتصدر الدول الكبرى هذه القائمة، مثل الولايات المتحدة وروسيا والصين، حيث تمتلك هذه القوى قدرات تقنية هائلة تسمح لها بتطوير برمجيات هجومية ودفاعية متقدمة، وتوظيف الفضاء السيبراني كجزء من استراتيجياتها العسكرية والأمنية، سواء في إطار الردع أو التجسس أو حتى الهجمات المباشرة⁹.

إلى جانب ذلك، برزت **الجماعات المسلحة** بمختلف أنواعها كفاعل جديد في هذا الميدان، إذ توظف الفضاء الرقمي في جمع الأموال عبر الهجمات الإلكترونية على المصارف أو من خلال العملات المشفرة، كما قد تستهدف المنظمات الإنسانية لتعطيل عملياتها الميدانية أو للحصول على بيانات حساسة تُستخدم كورقة ضغط سياسية أو عسكرية¹⁰.

كما يظهر في المشهد السيبراني **القراصنة المستقلون** أو ما يعرف بالـ **Hacktivists**، الذين يتحركون بدوافع أيديولوجية أو مالية، حيث يقومون باختراق مواقع ومنصات إلكترونية للتعبير عن مواقف سياسية أو احتجاجية، أو سعياً وراء مكاسب مالية. ورغم محدودية إمكاناتهم مقارنة بالدول، إلا أنهم قد يشكلون تهديداً كبيراً للمنظمات الإنسانية من خلال تسريب بيانات حساسة أو التشويش على جهود الإغاثة¹¹.

إن هذا التداخل بين الفاعلين الرسميين وغير الرسميين يعكس الطابع المعقد للحرب السيبرانية، ويؤكد أن ساحة الفضاء الرقمي باتت مجالاً مفتوحاً تتنافس فيه الدول، التنظيمات المسلحة، والقراصنة المستقلون على حد سواء، بما يحمله ذلك من تهديدات مباشرة وغير مباشرة للعمل الإنساني.

4.1 الأبعاد الدولية للحرب السيبرانية.

أصبحت الحرب السيبرانية في السنوات الأخيرة تمثل أحد أبرز التهديدات غير التقليدية للأمن والسلم الدوليين، إذ لم تعد الهجمات الإلكترونية شأناً محلياً يقتصر تأثيره على حدود دولة معينة، بل باتت ذات تداعيات عابرة للحدود بفعل الطبيعة المفتوحة للفضاء الرقمي¹². فالاختراقات قد تنطلق من قارة لتصيب أهدافاً في قارة أخرى خلال ثوانٍ معدودة، مما يجعل أثارها عالمية، ويعقد من مهمة تحديد المسؤولية السياسية أو الجنائية عن هذه الأفعال¹³.

ومن أبرز التحديات التي تفرضها هذه الظاهرة غياب إطار قانوني دولي موحد ينظم أعمال الحرب السيبرانية، إذ يظل القانون الدولي الإنساني وقواعد ميثاق الأمم المتحدة قاصرين عن معالجة خصوصيات الفضاء الرقمي، خاصة ما يتعلق بالهجمات على البنى التحتية المدنية أو المنظمات الإنسانية³. وعلى الرغم من بعض الجهود الأممية، مثل "مجموعة الخبراء الحكوميين للأمم المتحدة حول تطورات مجال المعلومات والاتصالات في سياق الأمن الدولي (UNGGE)"، إلا أن هذه المبادرات لم تتوصل بعد إلى اتفاق ملزم بشأن وضع قواعد واضحة للهجمات السيبرانية¹⁴.

إن الطابع العابر للحدود للحرب السيبرانية، مقترناً بالغموض وصعوبة التتبع، يجعلها أداة محتملة لتقويض استقرار النظام الدولي، ويفرض على المجتمع الدولي

تحديات غير مسبقة في مجال وضع الأطر القانونية والآليات المؤسسية اللازمة للحد من مخاطرها.

2. انعكاسات الحرب السيبرانية على العمل الإنساني

1.2 استهداف قواعد البيانات

تعتمد المنظمات الإنسانية في عملها على نظم رقمية متطورة لإدارة عملياتها الميدانية، وتخزين بيانات المستفيدين من لاجئين ونازحين، فضلاً عن معلومات المتبرعين والشركاء¹⁵. غير أن الاعتماد المتزايد على هذه النظم يجعلها عرضة لهجمات سيبرانية تستهدف اختراق قواعد البيانات الحساسة¹⁶. فقد شهدت بعض الوكالات الإنسانية تسريبات لمعلومات شخصية، مثل الأسماء والمواقع الجغرافية وبيانات الاتصال، مما يهدد حياة الأفراد المستضعفين، لا سيما في مناطق النزاع حيث يمكن استغلال هذه البيانات من قبل أطراف مسلحة¹⁷.

تتجاوز خطورة هذه الهجمات الجانب التقني فحسب، إذ تمس مباشرة مبدأ السرية وحماية المستفيدين، الذي يُعد من الأسس الجوهرية للعمل الإنساني¹⁸. كما أن استهداف قواعد البيانات يضعف ثقة المجتمعات المحلية بالمنظمات، ويؤثر على قدرتها في الوصول الآمن إلى الفئات المتضررة، وهو ما ينعكس سلباً على فاعلية التدخلات الإنسانية ويزيد من هشاشة الدعم المقدم¹⁹.

من ثم، فإن مواجهة هذه التحديات تفرض على المنظمات الإنسانية تطوير استراتيجيات أمن معلومات متقدمة، تشمل التشفير وحماية الهوية الرقمية، وبناء شراكات مع جهات تقنية متخصصة لتعزيز قدراتها في حماية البيانات²⁰. كما يكتسب تطوير بروتوكولات استجابة للطوارئ السيبرانية، وتدريب الموظفين والمتطوعين على الأمن الرقمي، أهمية بالغة لضمان استمرار العمليات الإنسانية

دون انقطاع.⁷ في المستقبل، يمكن أن تساهم التقنيات الناشئة مثل الذكاء الاصطناعي والبلوك تشين في رفع مستوى الأمان الرقمي، وتحسين مراقبة الوصول إلى البيانات الحساسة، بما يخلق بيئة أكثر أماناً وموثوقية للعمل الإنساني العالمي.²¹

2.2 تعطيل أنظمة الاتصالات والإغاثة

تعد أنظمة الاتصالات الرقمية العمود الفقري لعمليات التنسيق الميداني لدى المنظمات الإنسانية، إذ تُمكنها من تبادل المعلومات بين الفرق المنتشرة في مناطق الأزمت ومراكز القيادة لضمان سرعة الاستجابة وفعالية التدخل.²² غير أنّ بعض الهجمات السيبرانية أدت إلى شل هذه الأنظمة أو إبطائها بشكل كبير، وهو ما انعكس سلباً على قدرة المنظمات على توجيه مواردها وإيصال المساعدات في الوقت المناسب.²³

قد بينت تقارير صادرة عن مكتب الأمم المتحدة لتنسيق الشؤون الإنسانية أنّ تعطيل شبكات الاتصال خلال بعض الكوارث الطبيعية أو النزاعات المسلحة أدى إلى تأخر عمليات الإجلاء والإنقاذ، وأسهم في مضاعفة الخسائر البشرية والمادية.²⁴ كما أنّ التشويش على قنوات الاتصال يعرقل التنسيق بين مختلف الفاعلين الدوليين، من منظمات غير حكومية وهيئات أممية، ويقلل بالتالي من فعالية الاستجابة الجماعية.⁴

لذلك فإن تعزيز البنية التحتية الرقمية الإنسانية، وتطوير بدائل آمنة مثل الاتصالات عبر الأقمار الصناعية أو الشبكات المشفرة، يمثلان خياراً استراتيجياً لضمان استمرارية العمل الإنساني في بيئات النزاع والكوارث.

3.2 تهديد مبدأ الحياد والاستقلالية

مثل مبدأ الحياد والاستقلالية، يُعد أحد الركائز الأساسية التي تقوم عليها شرعية العمل الإنساني²⁵، غير أن التطورات الرقمية والحرب السيبرانية جعلت هذا المبدأ أكثر هشاشة، حيث يمكن استغلال البيانات الحساسة للمنظمات الإنسانية، أو شن حملات تضليل رقمية تستهدف تشويه صورتها أمام الرأي العام وأطراف النزاع. وقد يؤدي تسريب أو تزييف المعلومات إلى تقويض ثقة المستفيدين والمتبرعين، ويزيد من صعوبة وصول المنظمات إلى الفئات المستضعفة بسلامة وأمان²⁶.

كما أن مثل هذه الهجمات الرقمية لا تقتصر آثارها على الجانب المعلوماتي فحسب، بل تمتد لتشمل الشرعية العملية للمنظمات، إذ يمكن استغلالها من قبل جهات مسلحة أو منافسة للتشكيك في حيادها واستقلالية عملها، مما يعرض موظفيها ومشاريعها لمخاطر ميدانية متزايدة. وللتصدي لهذه التحديات، يصبح من الضروري تعزيز بروتوكولات الحماية الرقمية، بما في ذلك التشفير، وإدارة الهوية الرقمية، وتدريب الموظفين والمتطوعين على الأمن السيبراني، إلى جانب بناء شراكات استراتيجية مع خبراء التكنولوجيا لضمان حماية البيانات وحفظ مصداقية العمل الإنساني في بيئة رقمية متسارعة التغير.

4.2 حالات واقعية لاستهداف منظمات إنسانية.

قد تجاوزت الحرب السيبرانية الجانب النظري إلى ممارسات عملية كان لها أثر مباشر على العمل الإنساني العالمي، حيث تعرضت اللجنة الدولية للصليب الأحمر سنة 2022 لهجوم إلكتروني واسع النطاق استهدف بيانات أكثر من نصف مليون شخص من الفئات المستضعفة²⁷، وهو ما شكّل تهديداً خطيراً لسلامتهم الشخصية. كما واجهت منظمة الصحة العالمية محاولات متكررة

للاختراق خلال جائحة كوفيد-19²⁸، الأمر الذي عرقل بعض جهودها في التنسيق الدولي لمكافحة الجائحة وأظهر هشاشة البنى الرقمية في المنظمات الإنسانية على مستوى إدارة الأزمات الصحية العالمية. ولم تسلم منظمات أخرى مثل "أطباء بلا حدود" من هذه التحديات، حيث أشارت تقارير إلى محاولات استهداف مكاتبها العاملة في مناطق النزاع كسوريا واليمن²⁹، وهو ما يبرز هشاشة البنى الرقمية للمنظمات الإنسانية ويؤكد الحاجة الملحة إلى تعزيز أمنها السيبراني، وتطوير استراتيجيات استباقية لإدارة المخاطر وحماية البيانات الحساسة.

لا يقتصر تأثير هذه الهجمات على الجانب المعلوماتي فحسب، بل يمتد ليشمل التأثير على مصداقية المنظمات أمام المستفيدين والداعمين الدوليين، مما قد يضعف الثقة في قدراتها على تقديم المساعدات الإنسانية بفعالية وأمان³⁰. ويستلزم هذا الواقع تبني نهج شامل للأمن السيبراني، يتضمن تعزيز التشفير وحماية الهوية الرقمية، واستخدام أدوات الذكاء الاصطناعي لرصد الهجمات والتنبؤ بالتهديدات، بالإضافة إلى بناء شراكات استراتيجية مع شركات التكنولوجيا والحكومات لتعزيز القدرة على الصمود الرقمي³¹.

في المستقبل، يمكن أن تساهم التقنيات الناشئة مثل البلوك تشين والذكاء الاصطناعي في رفع مستوى الأمان الرقمي، وتحسين موثوقية البيانات وشفافية العمليات الإنسانية، ما يتيح للمنظمات تعزيز قدرتها على الحفاظ على المبادئ الأساسية للعمل الإنساني، كالحيد والاستقلالية والشفافية، حتى في ظل بيئة رقمية متسارعة التطور. كما يمكن أن يؤدي تعزيز الوعي الأمني لدى الموظفين والمتطوعين إلى تقليل المخاطر المرتبطة بالخطأ البشري، وهو عامل رئيسي في أي استراتيجية أمنية ناجحة³².

5.2 التهديدات الإعلامية الرقمية

لا تقتصر انعكاسات الحرب السيبرانية على الجانب التقني فحسب، بل تمتد لتشمل المجال الإعلامي والاجتماعي من خلال الحملات الممنهجة لنشر معلومات مضللة حول أداء المنظمات الإنسانية³³. ففي العصر الرقمي الحالي، أصبحت وسائل التواصل الاجتماعي والمنصات الرقمية أدوات قوية يمكن توظيفها لنشر شائعات أو تحريف الحقائق، وهو ما يتيح للأطراف المعنية التشكيك في نزاهة عمليات الإغاثة أو اتهام المنظمات بالانحياز لطرف دون آخر³⁴. ويؤدي هذا التشكيك إلى تراجع الثقة في المؤسسات الإنسانية، سواء لدى المستفيدين المباشرين أو الداعمين والمتبرعين، وهو ما يشكل تهديداً مباشراً لمصداقية المنظمات وقدرتها على أداء مهامها بفعالية³⁵.

أظهرت العديد من الدراسات أن الحملات المضللة الرقمية لا تقتصر آثارها على فقدان الثقة فحسب، بل قد تترتب عليها عواقب عملية، مثل تأخير وصول المساعدات أو تقليل التمويل المخصص للمشاريع الإنسانية، مما يضعف قدرة المنظمات على الاستجابة السريعة للأزمات ويزيد من هشاشة الفئات المستهدفة³⁶. كما يمكن لهذه الهجمات أن تؤثر على سمعة المنظمة دولياً، مما يحد من قدرتها على إقامة شراكات استراتيجية مع الجهات الحكومية أو الجهات المانحة الدولية، ويجعلها أكثر عرضة للتضييق الرقابي والسياسي في بعض مناطق النزاع.

من هذا المنطلق، يصبح من الضروري للمنظمات الإنسانية تطوير استراتيجيات متكاملة لمواجهة الحرب السيبرانية الإعلامية، تشمل المراقبة المستمرة للمنصات الرقمية، والاستجابة السريعة للتضليل والمعلومات المغلوطة، إلى جانب بناء حملات توعية تعزز شفافية العمليات وتوضح مبادئ الحياد والاستقلالية أمام

المستفيدين والجمهور العام³⁷. كما أن الاستثمار في التدريب الإعلامي للموظفين والمتطوعين على التعامل مع المعلومات المضللة، واستخدام أدوات الذكاء الاصطناعي لرصد الحملات التضليلية، يمثل جزءاً أساسياً من الجهود الاستباقية لحماية مصداقية العمل الإنساني في البيئة الرقمية المعاصرة.

باختصار، يمكن القول إن الحرب السيبرانية الإعلامية ليست مجرد تهديد تقني، بل هي عامل يغير ديناميكيات العمل الإنساني، ويتطلب من المنظمات دمج الأمن الرقمي والتواصل الاستراتيجي كركائز أساسية لاستدامة مصداقيتها وقدرتها على حماية المستفيدين وضمان استمرارية العمليات الإنسانية بفعالية وأمان.

3. التحديات التي تواجه المنظمات الإنسانية

1. التحديات التقنية

تعدّ محدودية البنية التحتية الرقمية في عدد من دول الجنوب أحد أبرز المعوقات التي تواجه المنظمات الإنسانية، إذ يجعلها ذلك أكثر عرضة للهجمات الإلكترونية، لاسيما في ظل غياب الكوادر المتخصصة في مجال أمن المعلومات³⁸.

1. التحديات المالية:

تعاني المنظمات الإنسانية من نقص واضح في الموارد المالية³⁹، وهو ما يصعب عليها تخصيص ميزانيات كافية لتعزيز أمنها السيبراني، خاصة وأن أولويات الإنفاق غالباً ما تنتج نحو البرامج الإغاثية المباشرة وخدمات الميدان، والتي تُعد الأكثر وضوحاً وتأثيراً على المستفيدين⁴⁰. ويؤدي هذا النقص في التمويل إلى اعتماد بعض المنظمات على أنظمة رقمية أقل أماناً أو تقليل الاستثمارات في تدريب الموظفين والمتطوعين على الأمن السيبراني، مما يزيد من هشاشة بنيتها الرقمية ويعرض مشاريعها ومصالح المستفيدين لمخاطر محتملة.

وللتغلب على هذه المعضلة، أصبح من الضروري للمنظمات تطوير حلول مبتكرة ومستدامة، مثل إقامة شراكات مع شركات تكنولوجيا لتقديم الدعم الأمني كجزء من برامج المسؤولية الاجتماعية، أو تخصيص جزء من التمويل المقدم من الجهات المانحة لتعزيز البنية الرقمية، بما يضمن قدرة هذه المنظمات على الاستمرار في أداء رسالتها الإنسانية بأمان وكفاءة، دون التضحية بخدماتها الميدانية الأساسية.

2. التحديات القانونية:

تمثل هذه التحديات في غياب إطار قانوني دولي ملزم ينظم المساءلة عن الهجمات السيبرانية الموجهة ضد المنظمات الإنسانية⁴¹، وهو ما يُضعف قدرتها على المطالبة بالإنصاف ويزيد من هشاشتها أمام التهديدات الرقمية⁴². ويؤدي هذا الغياب القانوني إلى فجوة واضحة في حماية البيانات والمعلومات الحساسة، مما يجعل المنظمات أكثر عرضة للاستغلال من قبل جهات مسلحة أو أطراف تضليلية، ويزيد من تعقيد قدرتها على الرد القانوني الفعال عند حدوث اختراقات أو تسريبات.

من هنا، تبرز الحاجة الملحة إلى تطوير آليات دولية واضحة تضع معايير لحماية المنظمات الإنسانية، وتفرض مسؤوليات على الدول والأطراف الفاعلة في النزاعات لحماية البيانات الرقمية، بما يضمن استمرارية العمل الإنساني ويعزز مصداقيته أمام المستفيدين والداعمين على حد سواء. كما يصبح من الضروري أن تتبنى المنظمات مبادرات تعاونية مع الجهات القانونية والدولية لتطوير بروتوكولات مشتركة للرد على الهجمات السيبرانية، وتحسين قدرتها على حماية البيانات في بيئة رقمية متزايدة التعقيد.

3. التحديات الأخلاقية:

برز الإشكاليات الأخلاقية في إمكانية إساءة استخدام بيانات المستفيدين من المساعدات الإنسانية لأغراض سياسية أو تجارية⁴³، وهو ما يتعارض بشكل مباشر مع المبادئ الأساسية للعمل الإنساني، مثل الحياد والاستقلالية وحماية المستفيدين⁴⁴. فقد يؤدي هذا الانتهاك إلى تآكل الثقة بين المجتمعات المحلية والمنظمات الإنسانية، ويجعل الفئات المستهدفة أكثر ترددًا في طلب المساعدة، مما يعيق قدرة المنظمات على تقديم الدعم الفعال ويهدد استدامة مشاريعها الإنسانية.

ومن ثم، تبرز الحاجة الملحة إلى وضع ضوابط أخلاقية صارمة لإدارة البيانات، تشمل الالتزام بالسرية، وضمان الشفافية في جمع واستخدام المعلومات، وتدريب العاملين والمتطوعين على المبادئ الأخلاقية المتعلقة بحماية البيانات. كما يجب أن تُدعم هذه الجهود بسياسات مؤسسية واضحة، فضلاً عن آليات رقابية وطنية ودولية تحمي المستفيدين من الاستغلال، بما يضمن تعزيز ثقة المجتمع واستمرارية العمل الإنساني وفق مبادئه الأساسية.

4. استراتيجيات المواجهة والحماية

1.4 تطوير سياسات أمن السيبراني

شكّل وضع سياسات شاملة وواضحة للأمن السيبراني أولوية استراتيجية للمنظمات الإنسانية؛ إذ تُعدّ هذه السياسات الإطار التنظيمي الذي يُحدّد كيفية التعامل مع البيانات الحساسة، واستجابة الطوارئ الرقمية، وضمان استمرارية الأنشطة الحيوية في بيئاتٍ معرضة للمخاطر⁴⁵. وتشمل هذه السياسات – بوجه خاص – ما يلي: تنفيذ إجراءات التشفير القويّة لحماية سرّية المعلومات ومنع الوصول غير المصرّح به⁴⁶، والنسخ الاحتياطي المنتظم للبيانات كضمان

لاستعادة التشغيل في حال وقوع الخلل أو الهجوم⁴⁷، وتطبيق نظم الإنذار المبكر لرصد التهديدات ومحاولات الاختراق بكفاءة، إلى جانب إعداد خطط استجابة شاملة للأنزمات الإلكترونية (Incident Response) تضم سيناريوهات متعددة، وتعريف الأدوار والمسؤوليات، وآليات التواصل الفوري مع الفرق التقنية والإدارية. وإنّ تبني هذه الممارسات لا يُصبح مجرد إجراء تقني، بل يتحوّل إلى عنصر أساسي من عناصر الحوكمة المعلوماتية والمرونة التشغيلية، مما يُسهم في رفع درجة الجاهزية للمنظمة وتعزيز قدرتها على الاستمرار في أداء مهامها، ويحدّ بدرجة كبيرة من احتمالية توقف أو تعطل تلك الأنشطة الحيوية أثناء الأزمات⁴⁸.

إضافةً إلى ذلك، تتطلّب هذه السياسات استراتيجيات شاملة لتثقيف العاملين وإكسابهم وعياً أمنياً مستمراً، باعتبار أنّ أحد أبرز منابع المخاطر هو العامل البشري سواء من خلال الإهمال أو التصيد الاجتماعي (social engineering) أو الاستخدام غير الحذر للأنظمة¹. كما تستلزم أيضاً تعزيز تحالفات تقنية ومعرفية مع الشركاء والموردين ضمن سلسلة التوريد، لأنّ ضعف أحد الأطراف الثالثة قد يُشكّل مدخلاً للتهديدات إلى داخل منظومة المنظمة².

بذلك، فإنّ الأمن السيبراني يتحوّل من كونه مهمة «فنية» إلى وظيفة استراتيجية تكاملية داخل الهيكل التنظيمي للمنظمة الإنسانية، تُحفّز على تبني ثقافة أمنية مؤسسية، وتُعزّز الموثوقية والشفافية، وتكسب ثقة المانحين والمستفيدين على حدّ سواء، في بيئة دولية معقّدة ومتغيّرة.

2.4 الشراكات مع شركات التكنولوجيا:

تُعَدّ الشراكات مع الشركات التكنولوجية العالمية أداة فعّالة لتعزيز الحماية الرقمية للمنظمات الإنسانية، إذ توفر هذه الشركات الدعم التقني، والبرمجيات المرخصة،

وخدمات الحوسبة السحابية الآمنة بأسعار رمزية أو مجاناً. ومن أبرز الأمثلة على ذلك مبادرة مايكروسوفت للأمن الرقمي للمنظمات غير الحكومية، التي تقدم برامج حماية متقدمة وتدريبات متخصصة لرفع مستوى الأمان السيبراني في المؤسسات العاملة بالمجال الإنساني. كما أن التعاون بين المنظمات والشركات الخاصة يعزز تبادل الخبرات التقنية ويضمن الوصول إلى أحدث الحلول في مجال أمن المعلومات⁴⁹.

3.4. بناء القدرات البشرية:

تُعَدّ القدرات البشرية محوراً أساسياً في منظومة الحماية السيبرانية، حيث تُظهر الدراسات أن أكثر من نصف الحوادث الإلكترونية تعود إلى أخطاء بشرية أو ضعف الوعي الأمني لدى العاملين. ومن ثم، فإن تدريب الموظفين والمتطوعين على مبادئ الأمن الرقمي، مثل إدارة كلمات المرور، واستخدام البريد الإلكتروني الآمن، والتعرف على محاولات التصيد الإلكتروني، يمثل خط الدفاع الأول ضد الهجمات السيبرانية. كما يُستحسن أن تعتمد المنظمات دورات مستمرة في الأمن المعلوماتي لضمان تحديث معارف كوادرها بما يتناسب مع تطور التهديدات الرقمية⁵⁰.

4.4. المبادرات الدولية:

شهدت الساحة الدولية إطلاق عدد من المبادرات الهادفة إلى تعزيز أمن الفضاء الرقمي للمنظمات الإنسانية، من أبرزها مبادرة جنيف للأمن السيبراني لعام 2017، التي جاءت استجابة لتزايد التهديدات الرقمية ضد المنظمات العاملة في الأزمات والنزاعات. وتعمل هذه المبادرة على تعزيز الحوار بين الحكومات، والمنظمات الإنسانية، والشركات التقنية من أجل تطوير أطر أخلاقية وقانونية لحماية البيانات الإنسانية. كما تشجع على تبادل الخبرات وبناء شبكات إنذار مبكر إقليمية تسهم في الوقاية من الهجمات وتعزيز التعاون الدولي في هذا المجال⁵¹.

5. الإطار القانوني الدولي لحماية العمل الإنساني في الفضاء السيبراني

1.5 موقف القانون الدولي الإنساني

كل القانون الدولي الإنساني الإطار القانوني الرئيسي المنظم لأعمال النزاعات المسلحة، حيث يقوم على مبدأ التمييز بين الأهداف العسكرية والأعيان المدنية، ويُحرّم أي استهداف مباشر للأشخاص أو المنشآت ذات الطبيعة الإنسانية. غير أنّ التطور التكنولوجي الهائل الذي شهده العالم خلال العقدين الأخيرين أفرز واقعاً جديداً يتمثل في انتقال جزء كبير من أنشطة العمل الإنساني إلى الفضاء الرقمي، وهو ما لم يكن في الحسبان عند صياغة اتفاقيات جنيف سنة 1949 وبروتوكولاتها الإضافية⁵².

لم يُحسم بعدُ موقف القانون الدولي الإنساني من تصنيف البنى التحتية الرقمية للمنظمات الإنسانية مثل أنظمة البيانات، وخوادم الاتصالات، ومنصات التنسيق الميداني — ضمن "الأعيان المدنية" المحمية، الأمر الذي يجعلها عرضة للاستهداف في النزاعات السيبرانية الحديثة². كما تبرز الحاجة إلى تطوير فهم قانوني موسّع لمفهوم "العمل الإنساني" بحيث يشمل النشاط الإلكتروني الذي يُسهم في إيصال المساعدات أو حماية المدنيين عبر الوسائط الرقمية⁵³.

2.5 الثغرات القانونية:

رغم وجود قواعد عامة في القانون الدولي الإنساني تحظر الهجمات على الأعيان المدنية، إلا أن البيئة السيبرانية تطرح تحديات قانونية غير مسبقة تتعلق بالإسناد والمسؤولية. فمن الناحية التقنية، يصعب غالباً تحديد مصدر الهجوم أو الجهة الفاعلة بدقة، وهو ما يعيق مبدأ المساءلة الدولية⁴. كما أن غياب نصوص صريحة في اتفاقيات جنيف أو البروتوكولات اللاحقة بشأن الجرائم الإلكترونية يجعل من الصعب إدراج الهجمات الرقمية ضمن الانتهاكات الجسيمة للقانون

الإنساني⁵⁴.

تزداد الإشكالية تعقيداً عندما تكون الهجمات من تنفيذ جهات غير حكومية أو مجموعات مسلحة تستخدم الفضاء الرقمي كأداة لتحقيق أهدافها السياسية أو العسكرية. في هذه الحالات، تظل قواعد المسؤولية الدولية مبهمّة، ويصعب تطبيق مبادئ "النية" و "التمييز" و "التناسب" التي يقوم عليها القانون الدولي الإنساني التقليدي⁵⁵.

3.5 مقترحات تطوير القانون الدولي:

أمام هذا الواقع المستجد، برزت دعوات متزايدة من المنظمات الدولية والباحثين المتخصصين إلى تحديث الإطار القانوني الدولي الإنساني بما يستجيب للتحولات الرقمية. وتتمثل أبرز المقترحات في إدراج حماية البنى الرقمية التابعة للمنظمات الإنسانية ضمن فئة "الأعيان المدنية" المشمولة بالحماية، وتضمن هذا المبدأ في اتفاقيات جنيف أو من خلال بروتوكولات إضافية جديدة تُعنى بالفضاء السيبراني⁷. كما طُرحت فكرة إنشاء ميثاق دولي للأمن الإنساني الرقمي يحدد التزامات الدول والأطراف غير الحكومية تجاه حماية العمل الإنساني الإلكتروني⁵⁶.

ومن شأن هذا الميثاق أن يضع معايير واضحة لتصنيف الهجمات السيبرانية كجرائم حرب في حال استهدفت أنظمة المنظمات الإنسانية أو بياناتها، وأن يُنشئ آليات للتحقيق والمساءلة بالتعاون بين الدول، والمحاكم الدولية، والهيئات التقنية المختصة. كما يمكن للمجتمع الدولي، من خلال الأمم المتحدة واللجنة الدولية للصليب الأحمر، تطوير أطر أخلاقية وتكنولوجية تضمن احترام مبادئ الإنسانية والحياد في البيئة الرقمية⁵⁷.

الخاتمة

إن الحرب السيبرانية تمثل تحدياً معقداً ومنتامياً للعمل الإنساني العالمي، حيث لم تعد تهديداتها تقتصر على الأضرار المادية المباشرة، بل تشمل أيضاً اختراق البيانات، والتلاعب بالمعلومات، وإضعاف قدرة المنظمات على الوصول إلى المستفيدين بشكل آمن وفعال. ولعل أخطر تداعياتها هو تهديد المبادئ الجوهرية للعمل الإنساني: الحياد، الاستقلالية، والشفافية، مما يجعل الحاجة إلى تطوير استراتيجيات وقائية متكاملة أمراً ملحاً.

من هنا، يصبح إلزاماً على المنظمات الإنسانية ليس فقط تعزيز التعاون مع شركات التكنولوجيا والحكومات لوضع بروتوكولات أمان رقمية صارمة، بل والسعي نحو صياغة إطار قانوني دولي ملزم يحمي البيانات الإنسانية ويضع معايير واضحة لمواجهة الهجمات السيبرانية. كما تشير الدراسة إلى أن المستقبل قد يشهد بروز تحالفات إنسانية رقمية بين المنظمات العالمية، واعتماد أدوات الذكاء الاصطناعي وتقنيات البلوك تشين لتأمين البيانات وتعزيز الشفافية، مع إمكانية استخدام التحليلات التنبؤية للتعامل الاستباقي مع المخاطر.

لا يقل أهمية عن ذلك تعزيز الوعي الأمني لدى العاملين والمتطوعين، وتدريبهم على مواجهة التهديدات السيبرانية والحد من أخطارها، بما يضمن استمرار قدرة المنظمات على أداء رسالتها الإنسانية بفعالية. ومن هذا المنطلق، يمكن القول إن الحرب السيبرانية، رغم ما تحمله من مخاطر، قد تشكل أيضاً فرصة للابتكار وتطوير أدوات رقمية أكثر أماناً ومرونة للعمل الإنساني، بما يعزز قدرة المنظمات على الصمود واستمرارية تقديم المساعدة للمحتاجين في عالم متغير رقمياً.

¹ منصور، خالد. الحرب السيبرانية: المفهوم، التهديدات، وآليات المواجهة، القاهرة: المركز العربي للأبحاث، 2020، ص 15.

² Nye, Joseph S. *Future of Power*. New York: Public Affairs, 2011, p. 113.

³ Rid, Thomas. *Cyber War Will Not Take Place*. Oxford University Press, 2013, p. 18.

⁴ الخطيب، عبد الرحمن. الأمن السيبراني والتحول الاستراتيجي في العلاقات الدولية، عمان: دار وائل، 2019، ص 44

⁵ Clarke, Richard A. & Knake, Robert, *Cyber War: The Next Threat to National Security and What to Do About It* HarperCollins, 2010.P 87-90 .

⁶ Singer, P.W. & Friedman, A., *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, 2014.P121-130.

⁷ Thomas, *Cyber War Will Not Take Place*, Oxford University Press, 2013.P 45-50.

⁸ International Committee of the Red Cross (ICRC), *Cyber Operations and the Law of Armed Conflict*, Geneva.2020.p32

⁹ Nye, Joseph S., *The Future of Power*, New York: Public Affairs, 2011.P 119.

¹⁰ الخطيب، عبد الرحمن، الأمن السيبراني والتحول الاستراتيجي في العلاقات الدولية، عمان: دار وائل، 2019، ص. 66-70.

¹¹ Denning, Dorothy E., *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tooluencing Foreign Policy*, Washington D.C.: Georgetown University Press, 2001 .p 34.

¹² Rid, Thomas, *Cyber War Will Not Take Place*, Oxford: Oxford University Press, 2013.p 82.

¹³ Tikk, Eneken et al., *International Cyber Norms: Legal, Policy & Industry Perspectives*. Geneva: UNIDIR. 2017.P 25.

¹⁴ الأمم المتحدة، تقرير مجموعة الخبراء الحكوميين بشأن التطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي، نيويورك: الجمعية العامة للأمم المتحدة، 2015، ص. 10-12.

¹⁵ ICRC, *The Humanitarian Data Protection Handbook*, Geneva: International Committee of the Red Cross, 2020.

¹⁶ United Nations Office for the Coordination of Humanitarian Affairs (OCHA), *Digital Humanitarianism: Risks and Opportunities*, New York, 2021

¹⁷ C. Kuner, *Data Protection and Humanitarian Action in Conflict Zones*, Cambridge University Press, 2019

¹⁸ D. Fidler, *Cybersecurity and Humanitarian Principles*, Journal of International Humanitarian Policy, Vol. 4, No. 2, 2022, pp. 45–63

¹⁹ M. Hildebrandt, *Trust, Technology and Humanitarian Operations*, Humanitarian Practice Network, 2021

²⁰ S. Raymond, *Cybersecurity Strategies for NGOs*, London: Routledge, 2020

²¹ A. Latonero, *Emerging Technologies and Humanitarian Security*, Stanford Center for Human Rights, 202

²² Humanitarian Futures Programme, *Humanitarian Space and Cyber-Security: Exploring the Implications for Humanitarian Action*, King's College London, 2014.p 09.

²³ Rid, Thomas, *Cyber War Will Not Take Place*, Oxford: Oxford University Press, 2013.p68.

²⁴ United Nations Office for the Coordination of Humanitarian Affairs (OCHA), *The Humanitarian Data Strategy*, New York: OCHA 2021.P22.

²⁵ CRC, *Fundamental Principles of the Red Cross and Red Crescent Movement*, Geneva : International Committee of the Red Cross, 2020.

²⁶ D. Fidler, *Cybersecurity and Humanitarian Principles*, Journal of International Humanitarian Policy, Vol. 4, No. 2, 2022, pp. 45–63.

²⁷ ICRC, *Annual Report 2022: Cybersecurity Incidents*, Geneva: International Committee of the Red Cross, 2022

²⁸ HO, *Digital Security and Cyber Threats during the COVID-19 Pandemic*, Geneva: World Health Organization, 2021

²⁹ Medecins Sans Frontières, *Security and Cybersecurity in Field Operations*, Brussels,2022

³⁰ D. Fidler, *Cybersecurity and Humanitarian Principles*, p 46.

³¹ S. Raymond, *Cybersecurity Strategies for NGOs*, London: Routledge, 2020

³² A. Latonero, *Emerging Technologies and Humanitarian Security*, Stanford Center for Human Rights, 2021.

33 المركز العربي للبحوث القانونية والسياسية، تحديات الأمن السيبراني والعمل الإنساني في الشرق الأوسط، القاهرة، 2021، ص. 15–12.

- 34 عبد الله، محمد، الإعلام الرقمي وأثره على ثقة المجتمع في المنظمات الإنسانية، مجلة العلوم الإنسانية، العدد 5، جامعة دمشق، 2020، ص. 34-37.
- 35 المركز العربي للسياسات الإنسانية، حماية السمعة والثقة في المنظمات الإنسانية الرقمية، عمان، 2022، ص. 22-28.
- 36 صالح، ريم، الحملات التضليلية الرقمية وتأثيرها على العمل الإنساني، مجلة الدراسات الاجتماعية، الجامعة الأردنية، 2021، ص. 50-55.
- 37 عبد الرحمن، هالة، استراتيجيات المنظمات الإنسانية لمواجهة التضليل الرقمي، بيروت: دار الفكر العربي، 2022، ص. 18-25.
- 38 برنامج الأمم المتحدة الإنمائي، تقرير التنمية الإنسانية في العصر الرقمي، نيويورك: الأمم المتحدة، 2022، ص. 47.
- 39 المركز العربي للبحوث القانونية والسياسية التمويل. المرجع السابق. ص. 45-47.
- 40 عبد الله محمد. المرجع السابق. ص. 22-26.
- 41 المركز العربي للبحوث القانونية والسياسية التمويل، المرجع السابق، ص. 33-36.
- 42 عبد الرحمان هالة. المرجع السابق. ص. 12.
- 43 حسن، علي، حماية البيانات الشخصية في المنظمات الإنسانية: أبعاد أخلاقية وقانونية، المجلة العربية للعلوم الإنسانية، العدد 12، القاهرة، 2021، ص. 40-45.
- 44 فوزي، ريم، السرية والشفافية في العمل الإنساني الرقمي، عمان: دار الفكر المعاصر، 2022، ص. 22-27.
- 45 جمال زمورة، ليلي بن عيسى، «أهمية حوكمة الأمن السيبراني لضمان تحول رقمي آمن-الخدمة العمومية في الجزائر»، مجلة البحوث الاقتصادية المتقدمة، المجلد 7، العدد 2 (30 سبتمبر 2022)، ص. 414-429.
- 46 إبتسام محمود القصير، «حوكمة تقنية المعلومات للحد من المخاطر السيبرانية وتعزيز أمن المعلومات المحاسبية في المؤسسات الليبية العامة»، مجلة البحوث الأكاديمية، المجلد 28، عدد 2 (2024)، ص. 1-14.
- 47 محمد هاني صباغ، «النسخ الاحتياطي وحفظ البيانات في العالم الرقمي»، موقع «أكاديمية حسوب»، 21 ديسمبر 2020.
- 48 هالة عبد المجيد عبد الحافظ العوده، «التحديات التي تواجه الأمن السيبراني»، مجلة العلوم الإنسانية والطبيعية، المجلد 6، العدد 7 (2025)، ص. 720-73.
- 49 Microsoft Philanthropies، Digital Security for Nonprofits Initiative، تقرير منشور على موقع مايكروسوفت، 2023، ص. 4.

50 اللجنة الدولية للصليب الأحمر، دليل التدريب على الأمن الرقمي للعاملين في المجال الإنساني، جنيف: منشورات اللجنة، 2021، ص. 19

51 Geneva Centre for Security Policy (GCSP), *The Geneva Cybersecurity Initiative 2017: Protecting Humanitarian Space Online*, Geneva, 2018, p. 11.

52 اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني في الفضاء السيبراني: حدود الحماية والتحديات الراهنة، جنيف: منشورات اللجنة، 2022، ص. 01.

53 Schmitt, Michael N., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, p150.

54 Droege, Cordula, *Cyber Operations and the International Humanitarian Law Framework*, ICRC Review, Vol. 99, No. 906, 2018, p 543.

55 Tikk, Eneken, *Legal Gaps in the Application of IHL to Cyber Conflicts*, NATO CCDCOE Publications, Tallinn, 2022, p. 34

56 Brown, David, *Cyber Accountability in Humanitarian Contexts*, Journal of International Humanitarian Legal Studies, Vol. 12, No. 2, 2023, p. 88

57 Geneva Centre for Security Policy (GCSP), *Toward a Digital Humanitarian Law Charter*, Geneva, 2024, p15.

قائمة المراجع

المراجع

- Nye, Joseph S. The Future of Power. New York: PublicAffairs, 2011.
- Rid, Thomas. Cyber War Will Not Take Place. London: Hurst, 2013.
- Singer, P.W., and Allan Friedman. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford: Oxford University Press, 2014.
- اللجنة الدولية للصليب الأحمر، "الهجوم السيبراني على بيانات المستفيدين"، تقرير رسمي، 2022.
- الأمم المتحدة، "تقرير حول التهديدات السيبرانية خلال جائحة كوفيد" 19-، نيويورك. 2021 :
- Kello, Lucas. The Virtual Weapon and International Order. Yale University Press, 2017.
- Clarke, Richard A., and Robert K. Knake. Cyber War: The Next Threat to National Security and What to Do About It. HarperCollins, 2010.
- عبد الكريم طلب، الحوكمة والإدارة الرشيدة في المؤسسات العامة والخاصة، عمان: دار صفاء، 2018.
- خالد وليد محمود، "الأمن السيبراني والعمل الإنساني"، مجلة الدراسات الإستراتيجية، العدد 15، 2022.
- Ali, Syed. "Cybersecurity Challenges in Humanitarian Aid." Journal of Humanitarian Studies, 2021.
- مجمع اللغة العربية بالقاهرة، مصطلحات معاصرة: دليل المصطلحات المعتمدة، القاهرة : المجمع، 2002.
- European Union Agency for Cybersecurity (ENISA). "Cybersecurity in Humanitarian Operations," Report, 2020.
- Geneva Internet Platform. "Cybersecurity and International Humanitarian Law," Policy Brief, 2019.

المراجع

أولا المؤلفات (كتب ودراسات منشورة)

- منصور، خالد. الحرب السيبرانية: المفهوم، التهديدات، وآليات المواجهة. القاهرة: المركز العربي للأبحاث، 2020.
- الخطيب، عبد الرحمن. الأمن السيبراني والتحول الاستراتيجي في العلاقات الدولية. عمان: دار وائل، 2019.
- Clarke, Richard A. & Knake, Robert. *Cyber War: The Next Threat to National Security and What to Do About It*. HarperCollins, 2010.
- Singer, P.W. & Friedman, A. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, 2014.
- Nye, Joseph S. *Future of Power*. New York: Public Affairs, 2011.
- Rid, Thomas. *Cyber War Will Not Take Place*. Oxford University Press, 2013.
- Denning, Dorothy E. *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool Influencing Foreign Policy*. Georgetown University Press, 2001.
- C. Kuner. *Data Protection and Humanitarian Action in Conflict Zones*. Cambridge University Press, 2019.
- S. Raymond. *Cybersecurity Strategies for NGOs*. London: Routledge, 2020.
- A. Latonero. *Emerging Technologies and Humanitarian Security*. Stanford Center for Human Rights, 2021.
- عبد الرحمن، هالة. استراتيجيات المنظمات الإنسانية لمواجهة التضليل الرقمي. بيروت: دار الفكر العربي، 2022.
- فوزي، ريم. السرية والشفافية في العمل الإنساني الرقمي. عمان: دار الفكر المعاصر، 2022.

ثانياً المقالات العلمية المحكمة

- عبد الله، محمد. «الإعلام الرقمي وأثره على ثقة المجتمع في المنظمات الإنسانية». *مجلة العلوم الإنسانية*، العدد 5، جامعة دمشق، 2020.
- صالح، ريم. «الحملات التضليلية الرقمية وتأثيرها على العمل الإنساني». *مجلة الدراسات الاجتماعية*، الجامعة الأردنية، 2021.
- حسن، علي. «حماية البيانات الشخصية في المنظمات الإنسانية: أبعاد أخلاقية وقانونية». *المجلة العربية للعلوم الإنسانية*، العدد 12، القاهرة، 2021.
- هالة عبد المجيد عبد الحافظ العودة. «التحديات التي تواجه الأمن السيبراني». *مجلة العلوم الإنسانية والطبيعية*، المجلد 6، العدد 7، 2025.
- جمال زمورة، ليلي بن عيسى. «أهمية حوكمة الأمن السيبراني لضمان تحول رقمي آمن للخدمة العمومية في الجزائر». *مجلة البحوث الاقتصادية المتقدمة*، المجلد 7، العدد 2، 2022.
- إبتسام محمود القصير. «حوكمة تقنية المعلومات للحد من المخاطر السيبرانية وتعزيز أمن المعلومات المحاسبية في المؤسسات الليبية العامة». *مجلة البحوث الأكاديمية*، المجلد 28، العدد 2، 2024.
- D. Fidler. "Cybersecurity and Humanitarian Principles". *Journal of International Humanitarian Policy*, Vol. 4, No. 2, 2022.
- Brown, David. "Cyber Accountability in Humanitarian Contexts". *Journal of International Humanitarian Legal Studies*, Vol. 12, No. 2, 2023.
- Droege, Cordula. "Cyber Operations and the International Humanitarian Law Framework". *ICRC Review*, Vol. 99, No. 906, 2018.
- Tikk, Eneken. "Legal Gaps in the Application of IHL to Cyber Conflicts". NATO CCDCOE Publications, Tallinn, 2022.

رابعاً المداخلات والأوراق البحثية / تقارير

- International Committee of the Red Cross (ICRC). *Cyber Operations and the Law of Armed Conflict*. Geneva, 2020.

- Tikk, Eneken et al. *International Cyber Norms: Legal, Policy & Industry Perspectives*. Geneva: UNIDIR, 2017.
- الأمم المتحدة. تقرير مجموعة الخبراء الحكوميين بشأن التطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي. نيويورك: الجمعية العامة للأمم المتحدة، 2015.
- Humanitarian Futures Programme. *Humanitarian Space and Cyber-Security: Exploring the Implications for Humanitarian Action*. King's College London, 2014.
- United Nations Office for the Coordination of Humanitarian Affairs (OCHA). *Digital Humanitarianism: Risks and Opportunities*. New York, 2021.
- United Nations Office for the Coordination of Humanitarian Affairs (OCHA). *The Humanitarian Data Strategy*. New York: OCHA, 2021.
- CRC. *Fundamental Principles of the Red Cross and Red Crescent Movement*. Geneva, 2020.
- ICRC. *Annual Report 2022: Cybersecurity Incidents*. Geneva: International Committee of the Red Cross, 2022.
- Geneva Centre for Security Policy (GCSP). *The Geneva Cybersecurity Initiative 2017: Protecting Humanitarian Space Online*. Geneva, 2018.
- Geneva Centre for Security Policy (GCSP). *Toward a Digital Humanitarian Law Charter*. Geneva, 2024.
- Schmitt, Michael N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press, 2017.
- المركز العربي للبحوث القانونية والسياسية. تحديات الأمن السيبراني والعمل الإنساني في الشرق الأوسط. القاهرة، 2021.
- المركز العربي للسياسات الإنسانية. حماية السمعة والثقة في المنظمات الإنسانية الرقمية. عمان، 2022.

- برنامج الأمم المتحدة الإنمائي تقرير التنمية الإنسانية في العصر الرقمي. نيويورك: الأمم المتحدة، 2022.

خامسا مواقع الإنترنت والمصادر الإلكترونية

- محمد هاني صباغ. «النسخ الاحتياطي وحفظ البيانات في العالم الرقمي». موقع أكاديمية حسوب 21 ديسمبر 2020.
- Microsoft Philanthropies. *Digital Security for Nonprofits Initiative*, 2023، موقع مايكروسوفت.
- اللجنة الدولية للصليب الأحمر. دليل التدريب على الأمن الرقمي للعاملين في المجال الإنساني. جنيف: منشورات اللجنة، 2021.
- اللجنة الدولية للصليب الأحمر. القانون الدولي الإنساني في الفضاء السيبراني: حدود الحماية والتحديات الراهنة. جنيف: منشورات اللجنة، 2022.
- HO. *Digital Security and Cyber Threats during the COVID-19 Pandemic*, جنيف: World Health Organization، 2021.
- Medecins Sans Frontières. *Security and Cybersecurity in Field Operations*, Brussels, 2022.