



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY

ماجستير القانون الرقمي

LAW 601
أسس القانون الرقمي

المحاضرة الثامنة
العمليات السيبرانية في النزاعات الدولية

Prepared
by Dr. Ahmed Elkhoully

Lecture

٨

مقدمة

أصبحت المعلومات في القرن الحادي والعشرين هي عملة هذا العالم الرئيسية، ولذلك تعتمد كل الكيانات من الدول القومية إلى الأفراد على نحو متزايد على المعلومات وتكنولوجيا المعلومات، ومن ذلك تقنيات الحاسوب والاتصالات. وتعتمد مؤسسات الأعمال على تكنولوجيا المعلومات في إجراء عملياتها (مثل كشف الرواتب، والمحاسبة، وتسجيل المخزونات والمبيعات، والبحث والتطوير). وتعتمد شبكات توزيع الغذاء والمياه والطاقة على تكنولوجيا المعلومات في كل مرحلة من مراحل عملها، وكذلك خدمات النقل والرعاية الصحية والخدمات المالية. وتستخدم المصانع آلات يتحكم فيها الحاسوب في تصنيع منتجاتها على نحو أسرع وأكثر كفاءة من أي وقت مضى.

والقوات العسكرية ليست استثناء من هذا الوضع. فتكنولوجيا المعلومات تستخدم في إدارة القوات العسكرية- على سبيل المثال في القيادة والتحكم وفي الأمور اللوجستية. علاوةً على ذلك، تُظهر الذخائر الحديثة دقيقة التوجيه كيف أن استخدام تكنولوجيا المعلومات التي تشكل جزءًا من أنظمة الأسلحة يزيد من قوة فتكها ويقلل من الأضرار التي تصاحب استخدام مثل هذه الأسلحة. ويمكن تنسيق تحركات وأفعال القوات العسكرية من خلال شبكات الاتصال التي تتيح تبادل المعلومات والصور المشتركة لميدان المعارك على نطاق واسع. ويستخدم الإرهابيون والمجموعات المسلحة من غير الدول أيضًا تكنولوجيا المعلومات. وعلى الرغم من أن الأسلحة الحركية للإرهابيين ذات تقنية بسيطة بوجه عام، فإن استخدام الإرهابيين لتكنولوجيا المعلومات في التجنيد والتدريب والاتصالات غالبًا ما يتسم بدرجة عالية من التطور والتعقيد.



Lecture

٠٨



والمصطلح الشائع في التعبير عن تكنولوجيا المعلومات من خلال شبكات الاتصال هو «الفضاء السيبراني». وتُعرّف وزارة الدفاع الأمريكية الفضاء السيبراني بأنه مجال يتسم «باستخدام الإلكترونيات [أي تكنولوجيا المعلومات] والطيف الكهرومغناطيسي في تخزين البيانات وتعديلها وتبادلها عن طريق أنظمة شبكات الاتصال والبنية التحتية المادية المرتبطة بها.» وبناء على هذا التعريف، تعمل الكيانات المدنية والعسكرية والإرهابية في الفضاء السيبراني لتنفيذ أنشطتها وعملياتها.

من المهم إدراك أن الفهم الكامل للفضاء السيبراني يتطلب دراية بالتكنولوجيا والسياسات والقانون. وتبدأ هذه المحاضرة بتمهيد مختصر عن طبيعة النزاع في الفضاء السيبراني، فيصف أدوات هذا النزاع وتقنياته، والعمليات العدائية (الهجومية) في الفضاء السيبراني التي تُسهّل تنفيذها هذه الأدوات والتقنيات، والفاعلين الذين قد يستخدمون هذه الأدوات والتقنيات، والأسباب التي تدفعهم إلى ذلك. ويتناول القسم الثاني ثلاث قضايا مهمة تتعلق بالنزاع في الفضاء السيبراني: مقارنة النزاع في الفضاء السيبراني بالنزاع في الفضاء المادي باستخدام أسلحة حركية تقليدية، ونسبة العمليات العدائية إلى طرف مسؤول، والحماية من العمليات العدائية وردعها. ويناقش القسم الثالث عددًا من القضايا القانونية الدولية المهمة التي تتعلق بميثاق الأمم المتحدة واتفاقيات جنيف، ويتناول أيضًا بعض الآثار المحتملة للعمليات الهجومية في الفضاء السيبراني على حقوق الإنسان.

Lecture

٠٨

محاور المحاضرة



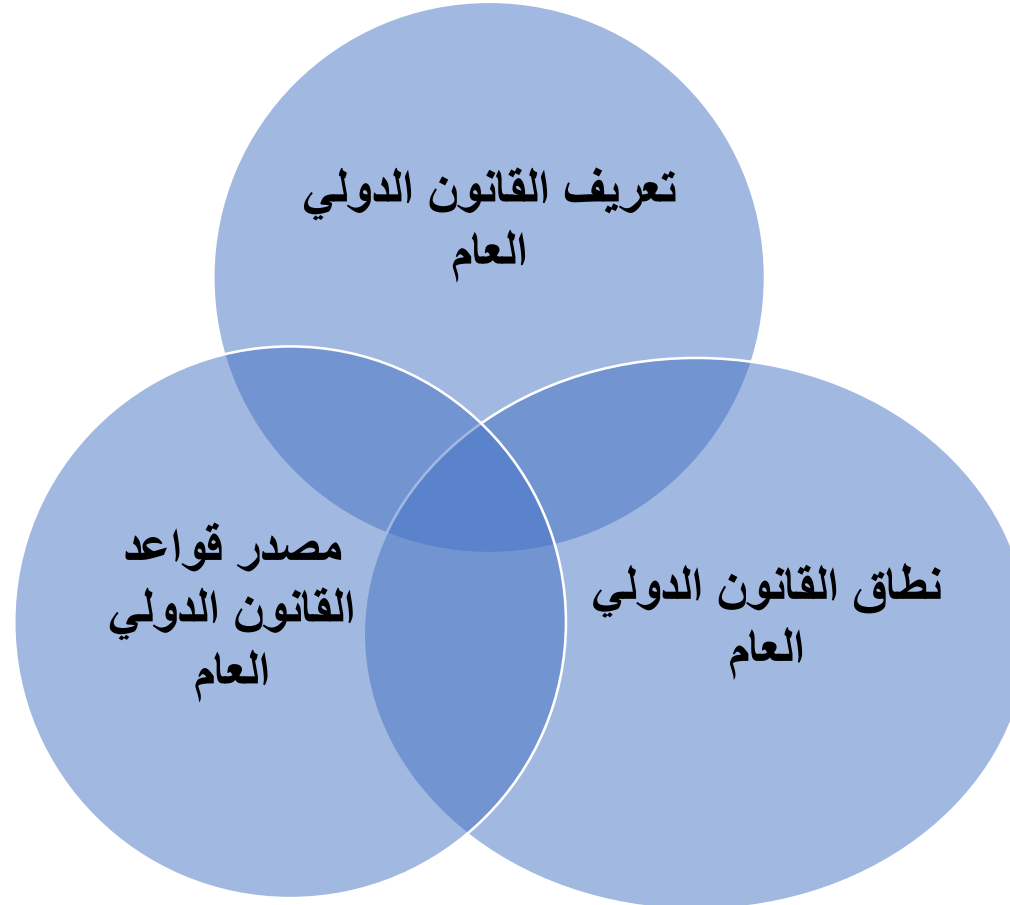
٣- ما هو النزاع في الفضاء السيبراني

١- ماهية القانون الدولي العام

٤- القانون المنطبق على النزاع السيبراني

٢- القوانين الحاكمة للنزاعات الدولية

أولاً: ماهية القانون الدولي العام



Lecture

٠٨

١-تعريف القانون الدولي العام



القانون الدولي العام le droit international public هو مجموعة القواعد القانونية التي تنظم العلاقات بين الدول، سواء أكان ذلك في وقت السلم أو أثناء الحرب . وذلك مثل إبرام المعاهدات، والتبادل الدبلوماسي والقنصلي، وطرق فض المنازعات، ومعاملة الأسرى، ونظام الحياد والحرب.

هو يشمل كذلك مركز المنظمات الدولية والعلاقات فيما بينها وعلاقاتها بالدول، سواء في ذلك المنظمات العالمية كالأمم المتحدة أو الاقليمية كجامعة الدول العربية .

٢- نطاق القانون الدولي العام

يتضمن القانون الدولي العام عدة موضوعات :

١- القواعد التي تحدد العناصر المكونة للدولة حتى تكتسب الشخصية الدولية ويتم الاعتراف بها كعضو في الجماعة الدولية، وتبين أنواع الدول البسيطة والمركبة، كاملة السيادة أو ناقصة السيادة كالدول تحت الوصاية.

٢- القواعد التي تنظم علاقات الدول في وقت السلم، وتبين حقوق الدول وواجباتها قبل بعضها البعض، مثل حق السيادة وحق المساواة والاحترام المتبادل . وتتناول علاقات التمثيل السياسي والقنصلي والحصانة الدبلوماسية، وتنظيم الاتفاقات والمعاهدات الدولية، هذا بالإضافة إلى بيان أحكام المسؤولية الدولية وطرق فض المنازعات بين الدول سواء عن طريق الوساطة أو عن طريق التحكيم الدولي.

٣- يشمل القانون الدولي العام كذلك القواعد التي تنظم علاقات الدول في وقت الحرب، وتسمى هذه القواعد بقانون الحرب، ويتضمن حقوق وواجبات الدول المتحاربة، ومتى تبدأ الحرب ومتى تنتهى، والأسلحة التي يجوز استخدامها والأسلحة المحظور استخدامها، وكيفية معاملة الأسرى وجرحى الحرب، واتفاقيات الهدنة والصلح، وحقوق الدول المحايدة وواجباتها إزاء الدول المتحاربة.



Lecture

٠٨



٤- ويتضمن القانون الدولي العام كذلك القواعد المتعلقة بالمنظمات الدولية، وتسمى قانون التنظيم الدولي الذي يتناول كيفية انشاء المنظمات الدولية والاقليمية وعلاقاتها ببعضها وعلاقاتها بالدول، هذا بالاضافة إلى اختصاصات ووظائف هذه المنظمات . و مسمار القانون من أهم المنظمات الدولية، هيئة الأمم المتحدة بفروعها كمجلس الأمن والجمعية العامة ومحكمة العدل الدولية ومنظمة العمل الدولية . ومن أمثلة المنظمات الاقليمية جامعة الدول العربية، ومنظمة الوحدة الافريقية، ومنظمة الدول المصدرة للبترول .

٣-مصادر القانون الدولي العام



ويستمد القانون الدولي العام قواعده من عدة مصادر أهمها العرف الدولي، ويتمثل في السلوك الذي اعتادت عليه الدول في علاقاتها ويتولد لديها الاعتقاد بأن هذا السلوك أصبح ملزماً لها، مثال ذلك قواعد الحصانة الدولية الخاصة بالسلك الدبلوماسي والقنصلي . وتعتبر المعاهدات الدولية كذلك مصدراً عاماً للكثير من القواعد الدولية التي تعد بمثابة قواعد تشريعية مكتوبة وملزمة للدول الموقعة عليها . وتلعب المبادئ القانونية العامة المستقرة في النظم القانونية للبلاد المتمدينة دوراً هاماً في خلق قواعد القانون الدولي .

ثانياً: القوانين الحاكمة للنزاعات الدولية

Lecture

٨

١- القانون الدولي الانساني و القانون الدولي لحقوق الإنسان:

يعد كل من القانون الدولي الانساني و القانون الدولي لحقوق الإنسان فرعاً من فروع القانون الدولي العام .

فأما القانون الدولي لحقوق الإنسان فهو منظومة من القواعد الدولية المصممة لحماية وتعزيز حقوق الإنسان للجميع. وهذه الحقوق، الطبيعية لدى بني البشر كافة، بصرف النظر عن جنسيتهم أو مكان إقامتهم، أو نوع جنسهم، أو أصلهم القومي أو العرقي، أو لونهم، أو ديانتهم، أو لغتهم، أو أي مكانة أخرى، حقوق مترابطة ومتداخلة وغير قابلة للتجزئة. وغالباً ما ينص عليها ويكفلها القانون، الذي يكون في شكل معاهدات ، والقانون الدولي العرفي، والمبادئ العامة والقانون غير الملزم. وتنطوي حقوق الإنسان على حقوق والتزامات. ويحدد القانون الدولي لحقوق الإنسان التزامات الدول بالتصرف بطرق معينة أو بالإحجام عن اتخاذ إجراءات معينة، وذلك من أجل تعزيز وحماية حقوق الإنسان والحريات الأساسية للأفراد أو الجماعات.



ثانياً: القوانين الحاكمة للنزاعات الدولية

Lecture

٨



يعد الفقيه Max Huber رئيس اللجنة الدولية للصليب الأحمر الأسبق أول من تبني مصطلح القانون الدولي الإنساني International Humanitarian law بصورة رسمية . و قد كان ذلك أثناء المؤتمر الدبلوماسي المنعقد بجنيف خلال أعوام ١٩٧٤ - ١٩٧٧ المتعلق بتأكيد و تطوير القانون الدولي الانساني المطبق في النزاعات المسلحة .

والقانون الدولي الإنساني هو مجموعة من القواعد تهدف، لأسباب إنسانية، إلى الحد من آثار النزاع المسلح. فهو يحمي الأشخاص الذين لم يعودوا يشاركون في الأعمال القتالية، كما يحدد وسائل الحرب وطرائقها. لذلك فإن مجاله مقصور من ناحية الاختصاص الموضوعي على حالات النزاع المسلح. والقانون الإنساني الدولي هو جزء من قانون الحرب (القانون المتعلق بالكيفية التي يمكن لها استخدام القوة)، الذي يجب التمييز بينه وبين القانون بشأن مشروعية استخدام القوة.

وقد عرفه جانب من الفقه الغربي « الأستاذ ستانيسلاف أ . نليك بأنه « مجموعة قواعد القانون الدولي التي تستهدف حالات النزاع المسلح حماية الأشخاص الذين يعانون ويلات هذا النزاع ، و في إطار أوسع حماية الأعيان التي ليست لها علاقة مباشرة بالعمليات العدائية ».

وقد عرفه الدكتور محمود شريف بسيوني - في جانب الفقه العربي - بأنه « مجموعة الأعراف التي توفر الحماية لفئات معينة من الأفراد و الممتلكات تحرم أي هجمات قد يتعرضون لها أثناء الصراعات المسلحة ، سواء كانت هذه الصراعات ذات صفة دولية أو صفة غير دولية ، و هذه الأعراف مستمدة من القانون الدولي الاتفاقي أو القانون الدولي العرفي » .

Lecture

٨



واستخدام القوة محظور بموجب ميثاق الأمم المتحدة. ومع ذلك، يتعين على جميع الأطراف في جميع النزاعات المسلحة أن تطبق بالتساوي القانون الإنساني الدولي بصرف النظر عما إذا كان لديها ما يبرر موقفها. وتتميز أيضاً هذه المساواة بين المتحاربين بشكل حاسم بين النزاع المسلح، الذي ينطبق عليه القانون الإنساني الدولي، والجريمة التي لا ينطبق عليها سوى القانون الجنائي وقواعد قانون حقوق الإنسان بشأن إنفاذ القانون.

وقد كان الرأي السائد على مدى فترة من السنوات أن الفرق بين القانون الدولي لحقوق الإنسان والقانون الإنساني الدولي هو أن الأول ينطبق في أوقات السلم والثاني ينطبق في حالات التراجع المسلح. بيد أن القانون الدولي الحديث يقر بأن هذا التمييز ليس دقيقاً. وبالفعل، فمن المسلم به على نطاق واسع اليوم على صعيد المجتمع الدولي هو أنه نظراً لأن التزامات حقوق الإنسان تستمد من الاعتراف بالحقوق الأصلية للبشر كافة وبأن هذه الحقوق يمكن أن تتأثر في أوقات السلم وكذلك في أوقات الحرب، فإن تطبيق القانون الدولي لحقوق الإنسان يستمر في حالات النزاع المسلح. وعلاوة على ذلك، ليس هناك في معاهدات حقوق الإنسان ما يشير إلى أنها لا تطبق في حالات النزاع المسلح. ونتيجة لذلك، تعتبر مجموعة القوانين – القانون الدولي لحقوق الإنسان والقانون الإنساني الدولي – مصدرين متكاملين للالتزامات في حالات النزاع المسلح. وعلى سبيل المثال، أشارت اللجنة المعنية بحقوق الإنسان، في تعليقها العام رقم ٢٩ (٢٠٠١) ورقم ٣١ (٢٠٠٤) إلى أن العهد الدولي الخاص بالحقوق المدنية والسياسية ينطبق أيضاً في حالات النزاع المسلح التي تنطبق فيها قواعد القانون الإنساني الدولي).

Lecture

٨



وسلم كذلك مجلس حقوق الإنسان في قراره ٩/٩ بأن قانون حقوق الإنسان والقانون الإنساني الدولي متكاملان ويعزز أحدهما الآخر. واعتبر المجلس أن جميع حقوق الإنسان تتطلب حماية متساوية ، وأن الحماية المقدمة بموجب قانون حقوق الإنسان تستمر أثناء حالات الصراع المسلح ، مع مراعاة الأوقات التي ينطبق فيها القانون الإنساني الدولي بوصفه قانوناً خاصاً ، وكرر التأكيد أنها اتخاذ تدابير فعالة لضمان ورصد تنفيذ معايير حقوق الإنسان في ما يتعلق بالسكان المدنيين في حالات الصراع المسلح، بمن فيهم السكان الواقعون تحت الاحتلال الأجنبي، وأنه ينبغي توفير حماية فعالة ضد انتهاك حقوق الإنسان لهؤلاء السكان ، وفقاً للقانون الدولي لحقوق الإنسان والقانون الإنساني الدولي المنطبق.

وخلال السنوات القليلة الماضية، أثار تطبيق قواعد القانون الدولي لحقوق الإنسان والقانون الإنساني الدولي على حالات النزاع المسلح سلسلة من الأسئلة تتعلق بتنفيذ تدابير حماية محددة تكفلها كلتا مجموعتي القوانين. فقد أدى تطبيقهما بصورة متزامنة إلى لبس بشأن التزامات الأطراف في النزاع ، و نطاق تلك الالتزامات ، و المعايير التي يتعين تطبيقها و المستفيدين من تلك التدابير الحماية .

٢- مصادر القانون الدولي لحقوق الإنسان و القانون الإنساني الدولي :

على الرغم من تباين الجذور التاريخية و الفقهية لكل من القانون الدولي لحقوق الإنسان و القانون الإنساني الدولي ، فإنهما يشتركان في هدف حماية جميع الأشخاص و يستندان إلى مبادئ احترام حياة الأشخاص و رفاههم و كرامتهم . ومن وجهة نظر قانونية ، يستمد كل من القانون الدولي لحقوق الإنسان و القانون الدولي الإنساني مصدرهما من سلسلة من المعاهدات الدولية التي عززها وكملها القانون الدولي العرفي .

لكل قانون من القانونين المصادر الخاصة به حيث يوجد أعراف واتفاقيات خاصة بكل قانون منها ، فالقانون الدولي الإنساني تحكمه قوانين وأعراف الحرب المستقرة عبر القرون وما تم تقنينه وابتداعه في اتفاقيات دولية مثل اتفاقيات لاهاي لعام ١٨٩٩ ، ١٩٠٧ واتفاقيات جنيف لعامي ١٩٢٩ ، ١٩٤٩ ، بينما استطاع القانون الدولي لحقوق الإنسان العثور على مصادر خاصة به حيث تم إصدار العهود و المواثيق و الاتفاقيات التي تحمي الحقوق الأساسية للإنسان ، مثل الإعلان العالمي لحقوق الإنسان ، والعهدين الدوليين للحقوق المدنية والسياسية ، والحقوق الاقتصادية والاجتماعية والثقافية لعام ١٩٦٦ .





٣- القانون الدولي الجنائي :

القانون الدولي الجنائي هو أحد فروع القانون الدولي العام الذي يطبق على الجرائم الدولية، فيقرر ماهيتها وأركانها والعقوبات المقرر لها والتي تقضي بها محكمة جنائية دولية باسم المجتمع الدولي لإضرارها بالسلم و الأمن الدولي.

ويجب علينا أن نفرق بين القانون الدولي الجنائي و القانون الجنائي الدولي حيث يطبق الأول على طوائف الجرائم الدولية التي تم إدراجها في المادة الخامسة من النظام الأساسي للمحكمة الجنائية الدولية، والتي تتمثل في أربع طوائف هي جرائم الحرب ، وجرائم الإبادة ، والجرائم ضد الإنسانية وجريمة العدوان ، أما القانون الجنائي الدولي فلا ينطبق على هذه الطوائف من الجرائم الدولية، وإنما ينطبق على الجرائم المنظمة عبر الحدود الوطنية، وهي جرائم معاقب عليها بموجب القانون الداخلي للدول، ولكنها ترتكب في عدة دول أو من أشخاص ينتمون لعدة دول كجرائم غسيل الأموال والاتجار بالأشخاص والاتجار بالمخدرات أو جرائم الإرهاب . وعلى ذلك فالقانون الجنائي الدولي هو فرع من فروع القانون الداخلي يعاقب على جرائم ذات طبيعة عالمية لارتكابها في عدة دول أو بواسطة أشخاص ينتمون لعدة دول مما يثير مشكلة القانون الجنائي الواجب التطبيق وكيفية تحقيق التعاون القضائي بين سلطات الدولتين أو الدول المعنية بالجريمة وتبادل تسليم المجرمين أو المحكوم عليهم ... الخ . أما القانون الدولي الجنائي فيطبق بشأن الجرائم الدولية و المبينة أركانها و العقاب عليها في نظام روما الأساسي وغيره من الاتفاقيات الدولية المتعلقة بتلك الجرائم .

٤- التمييز بين القانون الدولي الإنساني و القانون الدولي الجنائي :

فقد ذهب البعض إلى حد القول بأن العلاقة بين القانونين – باعتبارهما فرعين للقانون الدولي العام – تتقارب و تتفاعل وتتداخل إلى حد كبير لدرجة إمكانية استيعاب القانون الدولي الجنائي في القانون الدولي الإنساني بما قد يشكل قانوناً واحداً ، حيث يكون الأول أداة تطبيق و تنفيذ للثاني . و قد استدل هذا الجانب إلى عدة حجج لتأييد نظريتهم القائلة بوحدة القانونين تتمثل فيما يلي :

أ- أن كلا القانونين يعمل في إطار واحد وهو تحقيق الأمن و السلام للفرد الإنساني على المستوى العالمي .

ب- أن كلا القانونين ينتميان إلى رافد واحد وهو القانون الدولي العام و يستقيان مصادرها من الاتفاقيات و الأعراف الدولية .

وعلى الرغم من أوجه التقارب ، تظل هناك بعض الفروق الجوهرية بين القانون الدولي الإنساني و القانون الدولي الجنائي :

أ- القانون الدولي الإنساني لا يطبق إلا في الحرب و النزاعات المسلحة الدولية و الداخلية ، بينما لا يرتبط تطبيق القانون الدولي الجنائي بحالة الحرب أو وجود نزاع مسلح بل هو يطبق – في الغالب بعد أن تضع الحرب أوزارها و يتم البحث و التحقيق عن من يكون قد ارتكب جرائم دولية خلالها .



Lecture

٨



ب - القانون الدولي الجنائي له مبادئه الخاصة مثل مبدأ الشرعية الجنائية حيث لا يتم المحاكمة و العقاب على جريمة ما لم يكن منصوصا عليها فيه من قبل ، بينما القانون الدولي الإنساني لا تهيمن عليه تلك المبادئ .

ج - القانون الدولي الجنائي يعد بمثابة أثر أو نتيجة لمخالفة القانون الدولي الإنساني ، وبالتالي فإن تطبيقه يأتي لاحقا على ارتكاب مخالفات للقانون الدولي الإنساني .

د - لكل قانون من القانونين مصادره الخاصة ، فالقانون الدولي الإنساني مصادره تتمثل في الأعراف والاتفاقيات المتعلقة بالحرب ومن أمثلتها اتفاقيات جنيف لعام ١٩٤٩ وبروتوكولاتها لعام ١٩٧٧ ، واتفاقيات لاهاي لعامي ١٨٩٩ ، ١٩٠٧ ، بينما القانون الدولي الجنائي ينحصر في الاتفاقيات والقواعد التي تتضمن الجرائم الدولية كالنظام الأساسي للمحكمة الجنائية الدولية.

ثالثاً: ما هو النزاع في الفضاء السيبراني؟



الآثار
المحتملة
على
حقوق
الإنسان

المقارنة
بين النزاع
السيبراني
و النزاع
التقليدي

الفاعلون و
المشاركون
في
العمليات
السيبرانية

العمليات
الهجومية
المحتملة
في
الفضاء
السيبراني

أدوات و
تقنيات
النزاع
السيبراني

ماهية
النزاع
السيبراني

Lecture

٨

١- ماهية النزاع السيبراني

يشير تعبير النزاع في الفضاء السيبراني إلى الأفعال التي يتخذها أطراف نزاع ما، لتحقيق ميزة على خصومهم في الفضاء السيبراني باستخدام أدوات تقنية مختلفة وتقنيات تعتمد على البشر. ومن الناحية النظرية، يمكن تحقيق المزايا عن طريق إتلاف أو تدمير أو إعطاب أو نهب أنظمة الحاسوب لدى الخصم («الهجوم السيبراني»)، أو بالحصول على معلومات يُفضل الخصم أن تبقى سرية («التجسس السيبراني» أو «الاستغلال السيبراني»). ويُتاح لطائفة متنوعة من الفاعلين الحصول على هذه الأدوات والتقنيات، ومنهم الدول القومية، والأفراد، ومجموعات الجريمة المنظمة، والمجموعات الإرهابية، وتتباين بشدة الدوافع إلى استخدام الهجمات السيبرانية و/ أو التجسس السيبراني، ويشمل ذلك التجسس أغراضا مالية وعسكرية وسياسية وشخصية. ويختلف النزاع في الفضاء السيبراني عن النزاع في الفضاء المادي في كثير من النواحي، وقد تصعب نسبة العمليات السيبرانية المعادية إلى طرف مسؤول. وما زالت مشاكل الحماية من العمليات السيبرانية المعادية وردعها بلا حل من الناحية الفكرية. ولميثاق الأمم المتحدة واتفاقيات جنيف صلة وثيقة بالعمليات السيبرانية لكن سمات هذه الصلة غير واضحة اليوم لأن الفضاء السيبراني شيء جديد بالمقارنة بهذه الصكوك.

Lecture
08

2- أدوات و تقنيات النزاع السيبراني

قد يكون من المفيد تقسيم أدوات وتقنيات النزاع في الفضاء السيبراني إلى أدوات تركز على التكنولوجيا وتقنيات تُركّز على البشر. وتُتيح الأدوات والتقنيات الهجومية لطرف معاد أن يرتكب فعلاً ضاراً. أمّا الأدوات والتقنيات الدفاعية فتسعى إلى منع طرف معادٍ من أن يفعل هذا.

- أدوات تقوم على التكنولوجيا :

تتطلب الأدوات الهجومية ثلاثة عناصر:

١. تشير إمكانية الوصول إلى الكيفية التي يصل بها الطرف المعادي إلى تكنولوجيا المعلومات ذات الاهتمام. وقد يكون هذا الوصول عن بعد (على سبيل المثال من خلال الإنترنت، أو خط هاتفي عادي مرتبط به، أو اختراق الشبكة اللاسلكية المتصل بها. وعوضاً عن ذلك، قد يتطلب الوصول القُرب الشديد) على سبيل المثال جواسيس يعملون أو يخدمون كمُشغّلين أو فنيي خدمات، أو مُورّدين).

وقد يكون الوصول عن قُرب أيضاً في أي موضع في سلسلة التوريد (على سبيل المثال أثناء تصنيع رقائق الحاسوب أو تجميعها، أو تحميل برمجيات الحاسوب، أو إرسالها إلى المتلقي أو تشغيلها).

٢. موطن الضعف هو جانب من تكنولوجيا المعلومات يمكن استغلاله في النيل من هذه التكنولوجيا. وقد يتم إيجاد مواطن الضعف بلا قصد من خلال عيب في التصميم أو التنفيذ،

أو يتم إدخاله عمداً
www.esu.ac.ae



Lecture

٨



٣. الحمولة هي التعبير المستخدم للإشارة إلى الآلية التي تُستعمل للتأثير على تكنولوجيا المعلومات بعد استخدام إمكانية الوصول في استغلال موطن الضعف. على سبيل المثال، حالما يتم إدخال عامل تأثير في البرمجيات (مثل فيروس) إلى حاسوب، يمكن برمجة حمولته لتفعل أشياء كثيرة- إعادة إنتاج أو إرسال نفسه، أو تدمير الملفات على الجهاز أو تغييرها. ويمكن تصميم الحمولة لتفعل أكثر من شيء واحد أو لتتصرف في أوقات مختلفة. وإذا كانت قناة الاتصال متاحة، فإنه يمكن تحديث الحمولة عن بعد.

وتتناول الأدوات الدفاعية واحدًا أو أكثر من هذه العناصر. فبعض الأدوات (مثل جدران الحماية الإلكترونية) تُغلق طرق الوصول التي قد تُترك بطريق السهو مفتوحة. وتُحدّد أدوات أخرى أخطاء البرمجة (مواطن الضعف) التي يمكن إصلاحها قبل أن يستطيع طرف معادٍ استغلالها. لكن أدوات أخرى تعمل على منع طرف معادٍ من إحداث ضرر باستخدام أي حمولة معينة) على سبيل المثال ملف سري قد يجري تشفيره بحيث إنه حتى إذا سُرقَت نسخة منه من نظام الحاسوب، يصبح عديم الجدوى للطرف المعادي .

Lecture

٨

- تقنيات تعتمد على البشر

يتفاعل الناس مع تكنولوجيا المعلومات، وفي الغالب يكون خداع أو رشوة أو ابتزاز شخص مطلع على الأسرار الداخلية لتنفيذ أوامر طرف معادٍ أسهل من تحقيق الوصول من خلال وسائل تقنية محضة. على سبيل المثال، الوصول عن قرب إلى نظام قد يتحقق من خلال رشوة حارس لإدخال وحدة تخزين محمولة إلى جهاز حاسوب. ويمكن إحداث نقطة ضعف واختراق عن طريق ابتزاز مُبرمج لتسجيل شفرة معيبة. يُرجى ملاحظة أنه في مثل هذه الحالات، يمكن الجمع بين الأدوات التقنية والتقنيات التي تستند إلى البشر.

وتتضمن التقنيات الدفاعية المستندة إلى البشر في معظمها حث الناس على أن لا يتصرفوا على نحو يُعرض الأمن للخطر. ويفيد التعليم في توعية بعض الناس أن لا يندفعوا بعمليات الاحتيال التي يُقصد منها الحصول على أسماء تسجيل الدخول وكلمات السر. وتقع عمليات مراجعة النشاط بعض الناس أن لا يستخدموا تكنولوجيا المعلومات على نحو مريب مثير للشبهات. وتقع مكافآت الإبلاغ بعض الناس بالمبادرة إلى إبلاغ السلطات المختصة عن أي نشاط مريب أو مشكوك فيه.



يوصف النشاط الهجومي في الفضاء السيبراني بأنه هجوم سيبراني أو استغلال سيبراني.

● يقصد بالهجوم السيبراني استخدام أنشطة متعددة لتغيير أو إفساد أو خداع أو إضعاف أو تدمير أنظمة الحاسوب أو شبكات الحاسوب للخصم أو المعلومات و/ أو البرامج المدرجة في هذه الأنظمة أو الشبكات أو تُرسل من خلالها. وقد تُؤثر هذه الأنشطة أيضاً في الكيانات المرتبطة بهذه الأنظمة والشبكات. وقد يستخدم الهجوم السيبراني في منع المستخدمين المرخص لهم من الوصول إلى حاسوب أو خدمة معلومات (هجوم الحرمان من الخدمة)، أو لتدمير الآلات التي يتحكم فيها الحاسوب (الغرض المزعوم للهجوم السيبراني بالفيروس «ستوكسنت»)، أو لتدمير أو تغيير بيانات حيوية (مثل الجداول الزمنية لاستخدام عمليات لوجستية عسكرية) . ويُرجى ملاحظة أن الآثار المباشرة لهجوم سيبراني (الأضرار التي تصيب الحاسوب) قد تكون أقل أهمية من الآثار غير المباشرة (الأضرار التي تصيب النظام الذي يرتبط به الحاسوب) .





● يشير تعبير الاستغلال السيبراني إلى الأنشطة المتعمدة المُصمَّمة لاختراق أنظمة أو شبكات الحاسوب التي يستخدمها الخصم، وذلك بقصد الحصول على معلومات موضوعة على هذه الأنظمة والشبكات أو يجري تداولها من خلالها. ولا يسعى الاستغلال السيبراني إلى تعطيل التشغيل المعتاد لنظام أو شبكة حاسوب من وجهة نظر المستخدم، وإنما أفضل استغلال سيبراني هو الاستغلال الذي لا يلاحظه المستخدم أبدًا. والمعلومات المطلوبة هي بوجه عام المعلومات التي يريد الخصم أن لا يتم الكشف عنها. وقد تقوم الدولة بعمليات استغلال سيبراني لجمع معلومات استخبارات قيمة، مثلما قد تنشر جواسيس من البشر لأداء هذه المهمة. وقد تسعى إلى الحصول على معلومات عن برنامج الخصم للبحث والتطوير من أجل إنتاج أسلحة نووية، أو عن نظام المعركة لدى الخصم، وخطط عملياته العسكرية، وما إلى ذلك. أو قد تسعى إلى الحصول على معلومات من شبكة حاسوب شركة في بلد آخر لتستفيد منها شركة منافسة محلية في ذلك البلد. ومن بين المعلومات التي لها أهمية كبيرة تلك التي تتيح للبلد إجراء مزيد من الاختراقات لأنظمة أو شبكات حاسوب أخرى بغية جمع معلومات إضافية.

ويُرجى ملاحظة أن البيانات الصحفية تشير في الغالب إلى وقوع «هجمات سيبرانية» لكن النشاط الذي يجري في الواقع هو استغلال سيبراني.



من هم الفاعلون الذين قد يقومون بمثل هذه العمليات؟
نظرًا لطبيعة تكنولوجيا المعلومات فإن نطاق الفاعلين الذين قد يقومون بعمليات ذات أهمية على المستوى الوطني قد يكون كبيرًا. وتُعتبر على نطاق واسع بعض الدول مثل الولايات المتحدة والصين وروسيا وإسرائيل أنها تمتلك قدرات سيبرانية هجومية قوية، لكن دول أقل تقدمًا يمكنها أيضًا القيام بعمليات هجومية في الفضاء السيبراني.
وحتى الآن، كان الفاعلون المعروفون الذين نفذوا أعمال استغلال سيبراني وهجمات سيبرانية هم أطراف دون المستوى الوطني، أفراد في معظمهم. وفي الغالب بقصد الربح.
وكثيرًا ما يقال إن روسيا مسؤولة عن الهجمات السيبرانية على إستونيا في ٢٠٠٧ ، وجورجيا في ٢٠٠٨ ، وأن الصين مسؤولة عن عدد من عمليات الاستغلال السيبراني الشهيرة في الكثير من البلدان ، وأن الولايات المتحدة و/ أو إسرائيل مسؤولة عن الهجوم السيبراني على المنشآت النووية الإيرانية (الفيروس «ستوكسنت »). ولكن لم يقر أحد من هذه البلدان رسميًا بالقيام بأي من هذه الأنشطة، ولم يُجرَ الإعلان عن دليل قاطع- إن وُجد- على أن القيادة السياسية لأي بلد أمرت أو أشرفت على أي من هذه الأنشطة.

- وثمة مجموعة متنوعة من الفاعلين دون المستوى الوطني- منهم أفراد ومجموعات الجريمة المنظمة ومجموعات إرهابية- قد تقوم بتنفيذ هجمات سيبرانية و/ أو عمليات استغلال للفضاء السيبراني. وفي الواقع، يمكن إجراء بعض من هذه العمليات باستخدام معلومات وبرمجيات موجودة على شبكة الإنترنت ومكونات مادية متاحة في نظام تخزين أي حاسوب محلي.
- وتُغطّي أيضاً الدوافع إلى إجراء مثل هذه العمليات- أي للانغماس في النزاع السيبراني- طائفة واسعة. وأحد أكثر الدوافع شيوعاً اليوم هو الدافع المالي. ولأن قدرًا كبيرًا من التجارة يجري إنجازه من خلال شبكة الإنترنت أو باستخدام تكنولوجيا المعلومات، فإن بعض الأطراف هم مجرمون يسعون إلى تحقيق مكسب مالي غير مشروع من خلال عملياتهم الهجومية في الفضاء السيبراني. وقد تجلب عمليات الاستغلال السيبرانية معلومات قيمة مثل أرقام بطاقات الائتمان أو بيانات الولوج إلى الحسابات المصرفية، أو الأسرار التجارية، أو خطط تطوير الأعمال، أو استراتيجيات التفاوض على العقود. وقد تُؤدّي الهجمات السيبرانية إلى تعطيل جداول إنتاج المنافسين، أو تدمير بيانات قيمة تخص أحد المنافسين، أو تُستخدم كأداة لابتزاز المال من الضحية. وقد يُنفذ الجناة هجومًا سيبرانيًا كعملية ارتزاق مأجورة (ويعتقد على نطاق واسع أن الهجوم السيبراني على إستونيا جرى تنفيذه باستخدام سلاح سيبراني مستأجر).
- وثمة سبب محتمل آخر ذو طابع سياسي لمثل هذه العمليات، فقد يستخدم الجاني العملية السيبرانية في خدمة غرض سياسي مُعيّن. فالهجوم السيبراني أو استغلال الفضاء السيبراني قد يُستخدم في إرسال رسالة سياسية إلى أمة، أو تجميع معلومات استخبارات لأغراض سياسية، أو لإقناع طرف آخر أو التأثير عليه ليتصرف على نحو مُعيّن، أو لإثراء طرف آخر عن القيام بأفعال مُعيّنة.
- وثمة سبب آخر ذو طابع شخصي للقيام بمثل هذه العمليات، فقد ينفذ الجاني العملية للفوز «بحقوق التباهي» أو لإظهار إتقانه مهارات فنية مُعيّنة أو إرضاء جوانب فضول شخصية. وأخيرًا، قد تُستخدم مثل هذه العمليات لأغراض عسكرية بنفس الطريقة التي تستخدم بها العمليات العسكرية التقليدية التي تعتمد على الأسلحة الحركية التقليدية.

٤-المقارنة بين النزاع السيبراني و النزاع التقليدي



يقلب الكثير من النزاع السيبراني رأسًا على عقب فهمنا لما قد يتكشف عنه النزاع. وعلى الرغم من أن الكثير من المراقبين يقرون بوجود اختلافات واضحة بين الفضاءين السيبراني والمادي التقليدي، فإنه من السهل التهوين من مدى أهمية هذه الاختلافات. انظر على سبيل المثال تأثير ما يلي:

إسناد المسؤولية. النزاع الحركي التقليدي تخوضه قوات عسكرية يُفترض أنها تحت سيطرة حكومات وطنية. ولا تصدق مثل هذه الافتراضات على الفاعلين المشاركين في النزاع السيبراني، ونسبة الأفعال التي تجري في الفضاء السيبراني بشكل قاطع إلى حكومات وطنية أمر صعب للغاية أو مستحيل (انظر المناقشة الواردة أدناه في هذا الشأن).

- قدرات الفاعلين من غير الدول. في النزاع الحركي التقليدي، تكون الآثار التي تتحقق بوجه عام مرهونة بعدد القوات العسكرية التي يمكن أن تشارك في القتال، وحيث إن مثل هذه الأعداد تكون في العادة أصغر لدى الفاعلين من غير الدول عما هو متاح للدول، فإن الآثار التي يمكن للفاعلين من غير الدول إحداثها تكون صغيرة نسبيًا بالمقارنة بما يمكن أن يحدثه فاعلون تابعون للدول مجهزون تجهيزًا جيدًا. أمّا في النزاع السيبراني، فإن الفاعلين من غير الدول يمكنهم استخدام قدرات تكنولوجيا المعلومات لإحداث بعض الآثار واسعة النطاق التي يستطيع تحقيقها فاعلون كبار.

Lecture

٨



- أهمية بُعد المسافات والحدود الوطنية. في النزاع الحركي التقليدي، تبدو المسافات كبيرة وانتهاكات الحدود الوطنية مهمة. أمّا في النزاع السيبراني، فإن المسافات ليست ذات أهمية، واختراقات الحدود الوطنية للهجوم أو بغرض الاستغلال تحدث بشكل روتين دون أن يلحظها أحد.

5- الآثار المحتملة على حقوق الإنسان



تُقيد حقوق الإنسان تصرفات الحكومة في ما يتعلق بالأفراد الذين يخضعون للولاية القضائية للحكومة. وقد يكون منشأ مثل هذه الحقوق وطنياً (مثل الحقوق الممنوحة للأمريكيين بموجب دستور الولايات المتحدة)، أو في معاهدات دولية (مثل اتفاقية القضاء على كل أشكال التمييز ضد المرأة)، أو في القانون الدولي العرفي. وقد **يتعلق بالقضاء السيبراني اثنان من الحقوق** التي أوردها العهد الدولي للحقوق المدنية والسياسية (الذي صدّقت عليه الولايات المتحدة في أيلول/ سبتمبر ١٩٩٢). قد تكون المادة ١٧ (**حماية الخصوصية والسمعة**) ذات صلة بالعمليات السيبرانية التي يقصد بها الإضرار بسمعة فرد ما- على سبيل المثال بتزوير مستندات تستند على الحاسوب عن معاملات انخرط فيها- أو الكشف عن معلومات خاصة عن فرد (قد تشكل استفزازاً قبل نشوب نزاع إذا كان شخصاً بارزاً أو ذا نفوذ سياسي). وقد تكون المادة ١٩ (**حماية الحق في طلب المعلومات**) ذات صلة بالهجمات السيبرانية التي تهدف إلى منع الأفراد من الحصول على خدمات عن طريق شبكة الإنترنت أو وسائل تواصل أخرى. وقد يتعلق الأمر أيضاً بعدد من الحقوق الأخرى مثل الحق في الحياة والرعاية الصحية والغذاء، وذلك تبعاً لطبيعة الهجوم السيبراني وأهدافه. وقد يشير احترام هذه الحقوق الأخرى على سبيل المثال إلى أن هجوماً سيبرانياً بقصد فرض عقوبات اقتصادية يجب مع ذلك أن يسمح بإجراء معاملات متصلة بالحصول على الغذاء والدواء.



وقد أعلن عدد من الدول أن الوصول إلى شبكة الإنترنت حق أساسي من حقوق مجتمعاتهم (حتى آب/ أغسطس ٢٠١١ ، كان من بين هذه الدول إستونيا وفرنسا وإسبانيا وفنلندا). وعليه، إذا كان الوصول إلى شبكة الإنترنت حقًا من حقوق الإنسان، فإن الأعمال التي تقلص الوصول إلى الإنترنت أو تمنعه تُعد انتهاكًا لذلك الحق.

وعلاوةً على ذلك، ثمة نقطة مهمة مثار جدل في قانون حقوق الإنسان هي مدى انطباقه أثناء نزاع مسلح أو عمليات عدائية. ويذهب موقف الحكومة الأمريكية إلى أن ضرورات التقليل قدر الإمكان من المعاناة الإنسانية التي لا داعي لها يتم الوفاء بها من خلال متطلبات قانون النزاعات المسلحة، ومن ثم يجب أن لا يضع قانون حقوق الإنسان قيودًا إضافية على تصرفات قواتها المسلحة. وعلى النقيض من ذلك، عدد من الهيئات الدولية مثل المحكمة الجنائية الدولية، ولجنة حقوق الإنسان، ترى أن قانون حقوق الإنسان يجوز بل ويجب أن ينطبق مثل قانون النزاعات المسلحة على الأعمال العدائية.



ليس لدى اللجنة الدولية للصليب الأحمر أي شك في أن القانون الدولي الإنساني ينطبق على العمليات السيبرانية خلال النزاعات المسلحة، وبالتالي يحد من استخدامها، تمامًا مثلما ينظم استخدام الأسلحة والوسائل والأساليب الأخرى للقتال في أي نزاع مسلح، جديدة كانت أو قديمة. وهذا صحيح سواء إذا كان الفضاء السيبراني يعتبر مجالاً جديداً للحرب يشبه الفضاء الجوي والبري والبحري والفضاء الخارجي، أو إذا كان مجالاً مختلفاً، لأنه مجال من صنع الإنسان في حين أن المجالات السابقة مجالات طبيعة، أم أنه ليس مجالاً في حد ذاته.

وتعتمد الدول معاهدات القانون الدولي الإنساني بهدف تنظيم النزاعات الحالية والمستقبلية. إذ أدرجت الدول - في معاهدات القانون الدولي الإنساني - قواعد تتوقع تطوير وسائل وأساليب جديدة للقتال، على افتراض أن القانون الدولي الإنساني سينطبق عليها. على سبيل المثال، إذا لم ينطبق القانون الدولي الإنساني على وسائل وأساليب القتال في المستقبل، فلن يكون من الضروري استعراض شرعية استخدام هذه الوسائل والأساليب بموجب القانون الدولي الإنساني الحالي، حسبما تقتضيه المادة ٣٦ من البروتوكول الإضافي الأول المؤرخ ٨ حزيران /يونيو. 1977 .



ويحظى هذا الاستنتاج بدعم قوي في فتوى محكمة العدل الدولية بعنوان " مشروعية التهديد بالأسلحة النووية أو استخدامها"، حيث أشارت المحكمة إلى أن المبادئ والقواعد الثابتة للقانون الدولي الإنساني السارية في النزاعات المسلحة تنطبق "على كافة أشكال الحرب وعلى كافة أنواع الأسلحة"، بما في ذلك "ما سيكون في المستقبل". وترى اللجنة الدولية أن هذا الاستنتاج ينطبق على استخدام العمليات السيبرانية خلال النزاعات المسلحة.

وترحب اللجنة الدولية بتأكيد عدد متزايد من الدول والمنظمات الدولية على أن القانون الدولي الإنساني ينطبق على العمليات السيبرانية خلال النزاعات المسلحة، وتتطلع إلى إجراء مناقشات حول كيفية انطباق القانون الدولي الإنساني في هذا المجال.

وقد تقرر الدول أيضاً فرض قيود على العمليات السيبرانية بالإضافة إلى القيود الموجودة في القانون الحالي، وقد تضع قواعد تكميلية، لا سيما لتعزيز حماية المدنيين والبنية التحتية المدنية من آثار العمليات السيبرانية. وترى اللجنة الدولية أن أي قواعد جديدة يجري التفكير بشأنها ينبغي أن تستند إلى الإطار القانوني الحالي وتعززه، بما في ذلك القانون الدولي الإنساني.

وفي الحالات التي لا تشملها القواعد الحالية للقانون الدولي الإنساني، يظل المدنيون والمقاتلون محميين بما يسمى "شرط مارتنز"، مما يعني أنهم يظلون تحت حماية وسلطان مبادئ القانون الدولي كما استقر بها العرف، ومبادئ الإنسانية، وما يمليه الضمير العام.



ويجدر التوضيح أن التأكيد على انطباق القانون الدولي الإنساني على العمليات السيبرانية خلال النزاعات المسلحة لا يضيفي الشرعية على الحرب السيبرانية أو يشجع على عسكرة الفضاء السيبراني. في الواقع، يفرض القانون الدولي الإنساني بعض القيود على عسكرة الفضاء السيبراني من خلال حظر تطوير القدرات السيبرانية العسكرية التي تنتهك القانون الدولي الإنساني . وعلاوة على ذلك، يظل أي لجوء من الدول إلى القوة – ذات الطابع السيبراني أو الحركي - محكومًا بميثاق الأمم المتحدة وقواعد القانون الدولي العرفي ذات الصلة، لا سيما حظر اللجوء للقوة. ويجب تسوية النزاعات الدولية بالوسائل السلمية، في الفضاء السيبراني كما في جميع المجالات الأخرى .

مفهوم "الهجوم" بموجب القانون الدولي الإنساني والعمليات السيبرانية



تعتمد بشكل متزايد البنية التحتية المدنية الأساسية التي تتيح توفير الخدمات الأساسية على الأنظمة الرقمية. ويلزم حماية هذه البنية التحتية والخدمات ضد الهجمات السيبرانية أو الأضرار العرضية من أجل حماية السكان المدنيين.

ويوفر القانون الدولي الإنساني حماية خاصة لبنية تحتية معينة، مثل الخدمات الطبية والأعيان التي لا غنى عنها لبقاء السكان المدنيين، بغض النظر عن نوع العملية التي تلحق بها الضرر. ومع ذلك، فإن معظم القواعد الناشئة عن مبادئ التمييز والتناسب والاحتياط - التي توفر حماية عامة للمدنيين والأعيان المدنية - تنطبق فقط على العمليات العسكرية التي تشكل "هجمات" على النحو المحدد في القانون الدولي الإنساني. وتعرّف المادة ٤٩ من البروتوكول الإضافي الأول الهجمات بأنها "أعمال العنف الهجومية والدفاعية ضد الخصم". وبالتالي، فإن مدى تفسير مفهوم "الهجوم" على نطاق واسع أو ضيق فيما يتعلق بالعمليات السيبرانية أمر ضروري لانطباق هذه القواعد والحماية التي توفرها للمدنيين والبنية التحتية المدنية.



ومن المتفق عليه على نطاق واسع أن العمليات السيبرانية التي يُتوقع منها أن تسبب وفاة أو إصابة أو ضررًا ماديًا تشكل هجمات بموجب القانون الدولي الإنساني. ويشمل ذلك، من وجهة نظر اللجنة الدولية، العمليات السيبرانية التي تلحق ضررًا نتيجة الآثار المباشرة أو غير المباشرة (أو الارتدادية) المتوقعة للهجوم، على سبيل المثال وفاة المرضى في وحدات العناية المركزة نتيجة لعملية سيبرانية ضد شبكة الكهرباء مما تسبب بقطع إمداد المستشفى بالتيار الكهربائي. وعلاوة على ذلك، تشكل الهجمات التي تعطل الخدمات الأساسية بشكل كبير دون أن تتسبب بالضرورة في إلحاق أضرار مادية أحد أهم المخاطر على المدنيين. ومع ذلك، هناك اختلاف في الرأي حول ما إذا كانت العملية السيبرانية التي تؤدي إلى تعطل الخدمات دون التسبب في ضرر مادي تصنف على أنها هجوم على النحو الوارد في القانون الدولي الإنساني. وتعتبر اللجنة الدولية أيضًا أن العملية التي تهدف إلى تعطيل حاسوب أو شبكة حاسوبية خلال النزاع المسلح تشكل هجومًا بموجب القانون الدولي الإنساني، سواء عن طريق وسائل حركية أو سيبرانية.



. وإذا فسر مفهوم الهجوم على أنه يشير فقط إلى العمليات التي تسبب الوفاة أو الإصابة أو الضرر المادي، فإن أي عملية سيبرانية تهدف إلى تعطيل شبكة مدنية (مثل الكهرباء أو الخدمات المصرفية أو الاتصالات)، أو من المتوقع أن تتسبب في حدوث هذا التأثير بصورة عرضية، قد لا تكون مشمولة بقواعد القانون الدولي الإنساني الأساسية التي تحمي السكان المدنيين والأعيان المدنية. وسيكون من الصعب التوفيق ما بين مثل هذا الفهم التقييدي المفرط لفكرة الهجوم وبين هدف قواعد القانون الدولي الإنساني بشأن سير العمليات العدائية والغرض منها. ومن الضروري أن تتوصل الدول إلى فهم مشترك لمفهوم الهجوم لضمان الحماية الكافية للسكان المدنيين من آثار العمليات السيبرانية.

Lecture

٨





مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

