(ISSN: 2356 - 9492)

# الهجمات السيبرانية (الحرب الإلكترونية) واستخدام القوة المسلحة في القانون الدولي العام (الآستغلال السيبراني)

**د/ إيمان أحمد علام**

قسم القانون الدولى العام- كلية الحقوق – جامعة بنها

**ملخص البحث:**

يتناول هذا البحث المشكلات القانونية المتعلقة بالحرب السيبرانية من وجهة نظر قانون الحرب (اي الأحكام المتعلقة بمبررات الدخول في الحرب) في ظل انه لا يوجد صك دولي يغطي الأدوات السيبرانية حتى الآن وبالتالي يتم استخدام المقارنات والأمثلة ذات الصلة من ممارسات القوي الرئيسية (كالولايات المتحدة وروسيا والصين )مع الحلول الدولية الفعليه .

وذلك في إطار و سياق الأحكام المتعلقة باستخدام القوة المسلحة بموجب المادة ٤(٢) من الميثاق "الهجوم المسلح" ، والمادة ٥١ من الميثاق بصدد (شروط الدفاع المشروع عن النفس )اعتمادا على وارتكان إلى تطور وقدرة مفاهيم القانون الدولي الحالية ؛ ومنها مفهوم الهجوم المسلح المباشر وغير المباشر وتحديد الدولة المعتادية وعلاقة الدفاع عن النفس الوقائي او الاعتراضي في مواجهة هجوم مسلح إلكتروني وما شابه ذلك للكشف عن هيكل الحرب السيبرانية وتحدياتها .

ويؤكد الاستنتاج النهائي على أن التطور الفعلي الواقعي للهجمات الإلكترونية انه - على أرض الواقع - لا يوجد دولة على استعداد لتصعيد الهجمات الإلكترونية بحيث يؤدي حجم الدمار الناتج عنها إلى اعتبارها حرب إلكترونية وبالتالي نشوب نزاع مسلح أو حرب شاملة .

وبالتالي تفضل الدول التصرف دون أن يلاحظها احد وبالتالي فإنه الهجمات الإلكترونية اليوم هي مجرد تطورات جديده في مجال التجسس أو العمليات الاستخباراتية أو العمليات المغطاة.

الكلمات المفتاحية:

الهجوم الإلكتروني ، القانون الدولي للحرب ، الهجوم المسلح

التجسس ، الفضاء السيبراني

Research Summary:

Cyber attacks and the international law of armed conflict

This research deals with the legal problems related to cyber warfare from the point of view of the law of war (i.e. the provisions related to the justifications for entering the war) in light of the fact that there is no international instrument that covers cyber tools so far, and therefore comparisons and relevant examples from the practices of the main powers (such as the United States and Russia) are used. China) with actual international solutions.

This is within the framework and context of the provisions relating to the use of armed force under Article 4 (2) of the Charter “armed attack”, and Article 51 of the Charter in relation to (conditions of legitimate self-defense), depending

(ISSN: 2356 - 9492)

on and relying on the development and ability of current concepts of international law; Including the concept of direct and indirect armed attack, identifying the usual state, and the relationship of preventive or interceptive self-defense in the face of an electronic armed attack, and the like, to reveal the structure and challenges of cyber warfare.

The final conclusion confirms that the actual and realistic development of electronic attacks is that - on the ground - there is no country ready to escalate electronic attacks so that the scale of the resulting destruction leads to consider it an electronic war and thus the outbreak of an armed conflict or an all-out war.

Thus, countries prefer to act unnoticed, and therefore cyber attacks today are just new developments in the field of espionage, intelligence operations, or covered operations.

Search keywords:

Electronic attack, international law of war, armed attack , espionage , cyber warfare.

**مقدمة البحث:**

نظرا لعدم وجود تشريع دولي يغطي الهجمات السيبرانية فإنه يتم الاعتماد على توظيف التشابه والاعتماد على الحلول الدولية المتشابهة إلى حد كبير والمأخوذة من عقيدة وممارسات القوى الدولية الرئيسية مثال الولايات المتحدة الأمريكية والصين وروسيا ابتداءا من الأحكام المتعلقة باستخدام القوة المسلحة تطبيقا للمادة ٢(٤) والهجوم المسلح تطبيقا للمادة ٥١ من الميثاق.

حيث تنص المادة ٢(٤) علي أنه :ً يمتنع أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة".

وتنص المادة ٥١ علي أنه :ً ليس في هذا الميثاق ما يضعف أو ينتقص الحق الطبيعي للدول، فرادى أو جماعات، في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء "الأمم المتحدة" وذلك إلى أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدولي، والتدابير التي اتخذها الأعضاء استعمالاً لحق الدفاع عن النفس تبلغ إلى المجلس فورا، ولا تؤثر تلك التدابير بأي حال فيما للمجلس - بمقتضى سلطته ومسؤولياته المستمدة من أحكام هذا الميثاق - من الحق في أن يتخذ في أي وقت ما يرى ضرورة لاتخاذه من الأعمال لحفظ السلم والأمن الدولي أو إعادته إلى نصابهً.

**إشكالية البحث وتساؤلاته:**

وقد أثارت مشكلة البحث الرئيسية عدة تساؤلات مرتبطة بموضوع وهدف البحث وهى:

١- ما هية الهجمات السيبرانية لتكنولوجيا المعلومات والاتصالات؟

(ISSN: 2356 - 9492)

٢- ما المشكلات الأساسية التي تسببها الهجمات السيبرانية؟

٣- ؟ وما انواع وتصنيفات الهجمات السيبرانية؟

٤- ما التكييف القانوني للهجمات السيبرانية؟

_ هل يمكن اخضاع الهجمات السيبرانية لقانون الحرب الدولية قياساً ( أي الدولى القانون لاستخدام القوة المسلحة) م٢ فقرة ٤ الخاصة بحظر استخدام القوة فى العلاقات الدولية او التهديد باستخدامها ، والمادة ٥١ الخاصة بالدفاع الشرع حال استخدام القوة أو الهجوم المسلح؟

**أهمية البحث:**

تتمثل أهمية البحث في كونه يتناول موضوعاً من أهم وأخطر الموضوعات على وجه الإطلاق وهو:

الهجمات السيبرانية؛ كونه يتناول موضوع شائك يتعلق بأمن الدول وأمانها واستقرار وحفظ السلم والأمن الدوليين فى عصر التقدم التكنولوجي وإلإنفتاح العالمي والذكاء الإصطناعي الذي تبعه امكانية استخدام هذا التقدم التكنلوجي كسلاح ذو حدين بمعني استخدامة في أوجه النفع والتقدم الدولي ، أو علي العكس واستغلاله فى أوجه الإضرار بالدول الأخري كالتجسس أو الإستيلاء علي أو تعطيل المصالح الحيوية والمرافق العامة داخل الدولة المستهدفة.

فما التكييف القانوني لهذه الهجمات السيبرانية؟ هل تعد من قبيل الإعتداء بالقوة او يمثل تهديد باستخدام القوة المسلحة؛ وبالتالي ينشئ للدولة المعتدى عليها حق الدفاع الشرعى؛ وهو ماقد يؤدي الي تصاعد الأزمات الدولية وقد ينتهي الأمر باشتعال الحروب الدولية. أم ان تصنف الهجمات الإلكترونية علي انها مجرد أوجه أستغلال

سيبراني سيئ يتم التعامل معه والرد عليه ¬_من قبل الدول المستهدفة _ فى سرية حتي لا تشتعل الحروب بين الدول وبالتالي الحفاظ علي السلم والأمن الدوليين.

أهداف البحث:

يهدف البحث فى الهجمات السيبرانية الي تحديد التكييف القانوني لها_ هل تعد من قبيل القوة الدولية او الهجوم المسلح فيجوز مواجهتها بالدفاع الشرعي _ وبالتالي تحديد أليات المواجهة الدولية لها في عصر التقدم التكنلوجي والذكاء الاصطناعي.

**مفاهيم الدراسة:**

الهجمات السيبرانية :

الإستغلال السيبراني:

القوة فى العلاقات الدولية:

الهجوم المسلح:

الدفاع الشرعي:

الدفاع الشرعي الإستباقى أو الوقائى:

العدوان:

**منهج البحث:**

الدراسة في هذا البحث دراسة وصفية تحليلية، استعان فيها الباحث بمنهج أساسي وهو المنهج الوصفي؛ القائم على وصف وتشخيص موضوع البحث من مختلف جوانبه وإبعاده. وتحديداً؛ منهج دراسة االحالة ومنهج دراسة العلاقات المتبادلة ومنهج

(ISSN: 2356 - 9492)

دراسات القياس والنمو والتطور للمشكلة محل البحث؛ دراسة كمية وكيفية مع مرور الوقت.

الادوات المستخدمة في البحث :

استعان الباحث بعدد من الأدوات الرئيسية والمساعدة وهى:

١-عدد من المراجع العلمية.

٢-بعض الدراسات والبحوث السابقة التى أعدت في هذا المجال.

٣- بعض الأدوات المساعدة:

- حاسب ألي

**خطة البحث:**

في ضوء ما تقدم فقد قسمت هذا البحث إلي مقدمة وأربعة مباحث وخاتمة.

أما المقدمة فقد تناولت فيها أهمية الموضوع وسبب اختياره وإشكالية البحث ومنهجه وخطته.

وقد تناول المبحث الأول: الوسائل السيبرانية ووجهات النظر القانونية والمطلب الأول تناول أشكال وتقنيات البرامج الضارة فى أولاً: هجمات شبكات الكمبيوتر ، ثانياً: دفاعات شبكات الكمبيوتر ، ثالثاً: جمع ومراقبة معلومات الأعداء(التجسس). وتناول المطلب الثاني: الهجمات الإلكترونية من زاوية القانون الدولي: فى أولاً: وسائل الهجمات الإلكترونية من منظور القانون الدولي للصراعات المسلحة ، ثانياً: تطور القانون الدولي للنزاعات المسلحة فيما يتعلق باللجوء الي القوة، ثالثاً: الأساس القانوني لاعتبار الهجمات الإلكترونية حرب وفق ميثاق الأمم المتحدة فيما يتعلق (بحظر استخدام القوة والاستثناء اللاحق للدفاع الشرعي عن النفس ) اعتمادا

على التشابه مع الظواهر الموجودة فيما يتعلق بأليات وسبل حل المنازعات الدولية والدفاع الشرعي عن النفس.

ثم تناول المبحث الثاني: المعايير المنطقية لهجمات الكمبيوتر كحرب؛ وقد تناول المطلب الأول المعيار الموضوعي وميزتة لتوصيف " هجمات الكمبيوتر على أنها ًقوة مسلحة"؛ في أولاً: القيود النصية (حيث يقتصر "الهجوم المسلح "على الأدوات العسكرية التقليدية ) دون الدبلوماسية والاقتصادية والإكراه السياسي ، ثانياً: . النتيجة المدمرة باعتبارها محك، وثالثاً: وفق معايير شميت فالقوي المساحة هي المحك.فقد وضع شميت عدة معايير للتحقق من مدى قرب الهجمات الإلكترونية و تطابقها مع القوى المسلحة وهي:- الشدة، والفورية، والصلة المباشرة نسبيا بين القوى المسلحة والعواقب السلبية مقارنة بالصلة المباشرة لأشكال الإكراه الأخرى ، قابلية النتائج للقياس، وإفتراض انعدام الشرعية.وجاء بالمطلب الثاني:الوسائل الإلكترونية في إطار مفهوم "الهجوم المسلح والدفاع الشرعي؛ فى أولاً : شروط الهجوم المسلح محل الإعتبار فى المادة ٥١ من الميثاق:١-أن تصل الهجمات إلى الحد الأدنى من الشدة- وتوفر نية الهجوم، العواقب الوخيمة .

وجاء بالمبحث الثالث: الإطار القانوني للهجمات الإلكترونية ، ليوضح فى المطلب الأول: صعوبة تحديد الاختصاص الشخصي لتطبيق الإطار الدولي القياسي فيما يتعلق بنسب الهجوم المسلح السيبراني إلى دولة ، وأسباب صعوبة تحديد الاختصاص الشخصي فى الحالات الأتية: فى أولا: الهجمات غير المباشرة ، وثانياً:الأعمال الارهابية ، و الهجمات السيبرانية، التسامح السلبي مع الهجمات الإرهابية . ثالثاً :- تحديد مصدر الهجوم(جنسية الدولة) . وجاء فى المطلب الثاني: شروط الاختصاص الزماني ل "هجوم مسلح "إلكتروني يؤدي إلى تفعيل الدفاع الشرعي عن النفس في لحظات مختلفة لمواجهة الهجوم المسلح وذلك فى حالتين: أولاً- الدفاع الشرعي

(ISSN: 2356 - 9492)

الإستباقي عن النفس، وثانياً- اعتراض الدفاع عن النفس ؛ إذا كان ثمة هجوم مسلح وشيك او على وشك الوقوع .

ثم جاء بالمبحث الرابع: آفاق وتحديات جديدة: في المطلب الأول ؛ هجمات الكمبيوتر كوسيلة للدفاع عن النفس وفقا لتحليل شميت؛ مع مراعاة القيود الموضوعية على حق الدفاع عن النفس وهي معيار الضرورة والتناسب. ثم تناول بالمطلب الثاني الصعوبات التي تواجه البحث ( أي تتعارض مع اعمال القياس )؛ أي صعوبة تطبيق المعايير التقليدية للقوة المسلحة أو الهجوم المسلح على معنى السيبرانية .وأسباب عدم التطابق بين النموذج التقليدي ًللقوات المسلحةً أو ًالهجوم المسلحً والهجمات الإلكترونية: فى أولاً- صعوبة تحديد معنى السيبرانية، وثانياً:- صعوبة وصول هجمات شبكات الكمبيوتر الي حد "الهجوم المسلح"، وثالثاً: استثناء الوسائل الإلكترونية متعددة الأغراض من التجسس.

أما الخاتمة ففيها استعراض لأهم النتائج التي أسفر عنها البحث وأهم التوصيات التي يراها الباحث جديرة بالإتباع وذلك علي النحو التالي:

الهجمات السيبرانية

واستخدام القوة المسلحة في القانون الدولي العام

(الإستغلال السيبراني)

أصبحت الهجمات السيبرانية (الإلكترونية) أكبر مصادر تهديد الأمن القومي لدول العالم تماماً مثل أسلحة الدمار الشامل والتغير المناخي وقد أصبحت الهجمات السيبرانية ميداناً لممارسة النفوذ العالمي والتنافس الدولي عبر تعطيل مواقع حيوية للدول، وأخذ الصراع بين دول العالم يتجه نحو الحروب السيبرانية بسبب ازدياد الاعتماد -في أوجه الحياة كافة- على الحواسيب في ظل الثورة المعلوماتية،ولتحديد

أدوات الحرب الإلكترونية وتحدياتها نتناول مفهوم الهجوم السيبراني في ضوء تطور مفاهيم القانون الدولي فيما يتعلق باستخدام القوة المسلحة أو الهجوم المسلح المباشر وغير المباشر وتحديد حالة المعتدي ومدى ملائمة الدفاع عن النفس الوقائي أو الاعتراضى او الاستباقي في مواجهة الهجمات السيبرانية وما إلى ذلك:

## المبحث الأول

## الوسائل السيبرانية ووجهات النظر القانونية

بدأت ثورة المعلومات في العقد الخامس من القرن العشرين وحققت زخمها في العقود التالية ونشأت هجمات الكمبيوتر والتجسس عن طريق الفاعلين الرئيسين في ثورة المعلومات.

### المطلب الأول

### أشكال وتقنيات البرامج الضارة

**أولاً: هجمات شبكات الكمبيوتر .**

تطورت التقنيات والبرامج الضارة فظهرت الفيروسات التي سمحت للقراصنة بالتحكم في جهاز كمبيوتر شخص آخر بغرض سرقة أو تغيير أو تدمير المعلومات ومع سعة انتشار الإنترنت لاحقا تطورت هذه التقنيات( الفايروسات والآفات ) وأصبح بامكانها التكاثر والانتشار عبر الشبكات وكذلك تطورت التقنيات الخبيثة التي تصيب الشبكات.

وبحلول نهاية العقد الثامن من القرن العشرين أصبحت وزارة الدفاع الأمريكية على دراية كاملة بالتهديدات الجديدة. لكن التهديدات الحقيقية تمثلت فى الهجمات الدولية التي ارتكبت خارج مجال الدولة الفاعلة وذلك عن طريق عناصر إرهابية نيابة عن الدولة أو بواسطة دولة أخرى ولكن وزارة الدفاع الأمريكية اعتبرت أن التهديدات

(ISSN: 2356 - 9492)

الحقيقية هي الهجمات الدولية التي ارتكبت خارج مسرح الجريمة من قبل دولة ،ونيابة عن دولة من قبل إرهابيين وما إلى ذلك. . وتأتي «الهجمات السيبرانية» جنباً إلى جنب وأدوات أخرى مثل الحروب بالوكالة والحصار الاقتصادي وحروب المعلومات، ونشر الشائعات لإضعاف وزعزعة الجبهة الداخلية بالنسبة للدولة المستهدفة، وجميعها أدوات لحروب الجيل الرابع.

تعريف هجمات شبكات الكمبيوتر:-وهي عمليات لتعطيل او رافض او إضعاف او إتلاف المعلومات الموجودة في أجهزة الكمبيوتر أو شبكات الكمبيوتر.

ثانياً- دفاعات شبكات الكمبيوتر : وهي تدابير دفاعية للدفاع عن المعلومات وحماية أجهزة الكمبيوتر والشبكات من التعطيل أو الإنكار أو التدهور أو التدمير وذلك عن طريق استخدام الإجراءات الامنية التي تسعى إلى منع العدو من التعرف على قدرات الجيش و مخططاته.

ثالثاً- جمع ومراقبة معلومات الأعداء(التجسس) : وعادة ماتقوم دفاعات شبكات الكمبيوتر بمراقبة الأعداء والتجسس عليهم باستخدام أدوات اختراق الأنظمة وارجاع المعلومات أو نسخ الملفات.

وعادة مايقوم الأعداء بالتجسس على شبكات الكمبيوتر ولكن يستطيع الجيش القيام باختراق الأنظمة وإرجاع المعلومات او نسخ الملفات بما يمتلكه من أدوات وهو ما يعد ميزة وتفوق على الأعداء حيث تعد الحرب السيبرانية جزء من نهج الحرب الشاملة (أي احد مفردات الحرب الشاملة).

وتبني استراتيجيات الجريمة على معلومات الحرب التي تقوم على استخدام الصور المتعددة للقوة ومنها الأساليب أو الصور الخطية والمعلومات المتعددة للحرب.

المطلب الثاني

الهجمات الإلكترونية من زاوية نظر القانون الدولي

يقوم القراصنة وهم من المواطنين العاديين بتنفيذ الهجمات الإلكترونية وهو ما يستلزم اللجوء إلى سبل الانتصاف المحلية حال الهجمات العابرة للحدود وهو ما تتناوله وتعالجه ( اتفاقية الجرائم الإلكترونية ) تحديداً.

و اتفاقية الجرائم الإلكترونية: هي اتفاقية دولية تسعى إلى معالجة جرائم الكمبيوتر والإنترنت من خلال موائمة القوانين الوطنية، وتحسين تقنيات التحقيق وعن طريق زيادة التعاون الدولي.

أولاً: وسائل الهجمات الإلكترونية من منظور القانون الدولي للصراعات المسلحة:

نتناول هنا الوسائل السيبرانية-هجمات ، ودفاعات، .... - بالتحليل والدراسة والمناقشه وذلك من خلال زاوية نظر قانون الحرب باعتبارها مجموعة من القواعد القانونية التي تحكم اللجوء إلى القوة كأداة للسياسة الوطنية ، ومنظور "قانون الحرب " وهو مجموعة من القواعد القانونية التي تتعلق بسلوك الدولة أثناء الحرب.

ثانياً: تطور القانون الدولي للنزاعات المسلحة فيما يتعلق باللجوء الي القوة:-

يعد ميثاق كيلوج - برياند عام ١٩٢٨ هو أول ميثاق وردت فيه قواعد حظر اللجوء إلى الحرب ولكن أول حظر شامل من اللجوء إلى الحرب ورد في ميثاق الأمم المتحدة بعد الحرب العالمية الثانية فقد انتقل الميثاق من مجرد إدانة الحرب إلى حظر عام من التهديد بالقوة او استخدامها في المادة ٤/٢ .

ولكنه وضع استثناء صريح فيما يتعلق بحق الدفاع عن النفس ويحدد ظروف وشروط ذلك الحق.

(ISSN: 2356 - 9492)

ثالثاً: الأساس القانوني لاعتبار الهجمات الإلكترونية حرب وفق ميثاق الأمم المتحدة فيما يتعلق (بحظر استخدام القوة والاستثناء اللاحق للدفاع الشرعي عن النفس ) اعتمادا على التشابه مع الظواهر الموجودة فيما يتعلق بأليات وسبل حل المنازعات الدولية والدفاع الشرعي عن النفس .

وباتباع القياس بدقة شديدة في هذا الشأن فيركز التحليل على الهجمات الإلكترونية على النحو التالي:-

## المبحث الثاني

## المعايير المنطقية لهجمات الكمبيوتر كحرب

وهنا نبحث فى ميزة ًالاختصاص الموضوعيً وتصفيات هجمات الكمبيوتر على أنها "قوة مسلحة " ، والقيود النصية "لهجوم مسلح " حيث أنه يقتصر على الأدوات العسكرية التقليدية

فنبحث فى الهجمات الإلكترونية والقانون الدولي للنزاعات المسلحة أي قانون الحرب؛ ونوضح الوسائل الإلكترونية الهجومية. والمعايير المنطقية لهجمات الكمبيوتر كحرب وذلك فى مطلبين:

### المطلب الأول

### المعيار الموضوعي

ميزة المعيار الموضوعي لتوصيف " هجمات الكمبيوتر على أنها ًقوة مسلحة"

تنص المادة ٤/٢ من ميثاق الأمم المتحدة على أنه يمتنع جميع الأعضاء في علاقاتهم الدولية عن استخدام القوة المسلحة أو التهديد باستخداميها ضد السلامة الإقليمية او

الاستقلال السياسي لأي دولة او في أي دولة أخرى بطريقة تتعارض مع أهداف الأمم المتحدة؛ وهذا الحظر المشدد من القواعد الأمرة ينطبق على جميع الدول الأعضاء وغير الأعضاء بالامم المتحدة.

مع ملاحظة ان نطاق المادة ٤/٢ وفيما يتعلق "باستخدام القوة " يغطي القوى المسلحة وليس الضغط الاقتصادي أو النفسي. وعلى أساس ما سبق نستخلص الخصائص القانونية للحرب الإلكترونية.

وبمناظرة المظاهر المباشرة للوسائل الإلكترونية مع القوى المسلحة يتضح جليا أن المادة ٤/٢تشمل بلا شك القوة المسلحة.

مثال علي ذلك عمليةً"اورشارد" وهي غارة جوية اسرائيلية على منشأة نووية في سوريا تم تنفيذها في ٦ سبتمبر ٢٠٠٧ وقد تكهنت مصادر صناعية وعسكرية أمريكية أن إسرائيل ربما استخدمت تقنية مماثلة لنظام هجوم شبكة سوتر الأمريكية المحمولة جواً للسماح لطائراتها بالمرور دون أن يكتشفها الرادار السوري.

والسوتر هو برنامج كمبيوتر عسكري تم تطويره لمهاجمة شبكات الكمبيوتر وهياكل الاتصال التابعة للخصوم وقد تم تطوير ثلاثة أجيال منه وكان آخرها الذي تم اختياره عام ٢٠٠٦ لتمكين العدو من غزو الروابط و الأهداف ذات الأهمية الزمنية مثل قاذفات صواريخ بالستية في ساحة المعركة او قاذفات صواريخ أرض جو متحركة . ويبدو أن الطاقة العالية الحزم بمثابة أبواب سرية عالمية ( ) لغزو الشبكات العسكرية للعدو.

وكان بالإمكان تصنيف الوضع السابق ذكره بسهولة على أنه "قوة مسلحة إلكترونية" إذا كان الهجوم الإسرائيلي هو الضربة الأولى لحرب جديدة ولكن لم يكن هذا هو

(ISSN: 2356 - 9492)

الحال حيث لم يبرم كلا من البلدين إسرائيل وسوريا معاهدة تسليم بعد حرب يوم الغفران عام ١٩٧٣ .

وإلى جانب حالات الهجمات الإلكترونية عبر الإنترنت التي يغطيها توصيف "القوة المسلحة" هناك بعض المشاكل المتعلقة بتعريف الفضاء السيبراني حيث انه لا ينطبق عليه التعريفات التقليدية.

أولاً: القيود النصية (حيث يقتصر "الهجوم المسلح "على الأدوات العسكرية التقليدية ) دون الدبلوماسية والاقتصادية والإكراه السياسي أي أنه يجب استثناء الإكراه السياسي كبدائل سلمية لحرب شاملة وبالتالي يجب استثناء الهجمات الإلكترونية وعدم اعتبارها قوة مسلحة صراحة بموجب قانون الحرب؛ حتى ولو كان ذلك محظور بموجب أحكام نصوص أخرى في القانون الدولي. وبالطبع فهذا النهج يفشل في التصدي للهجمات الإلكترونية التدميرية المستجدة مع التقدم التكنولوجي.

ثانياً- النتيجة المدمرة باعتبارها محك :

هناك وجهات نظر مختلفة ترى تطبيق النظام القانوني التقليدي للحرب على الهجمات الإلكترونية من خلال تجاهل وسائل الهجوم مع التركيز فقط على مقدار الضرر الناتج.

فلا يجب أن نضع في الاعتبار ما إذا كان المصنع قد دمرته قنبلة او شفرة خبيثة إنما ما يهم هو حجم الدمار الذي خلفه الهجوم( ) .

فالقاعدة هي أن أي هجوم على شبكة الكمبيوتر يتسبب عن قصد في أي تأثير مدمر داخل اقليم دولة أخرى يعتبر استخدام غير قانوني للقوة المسلحة وينطبق عليه نص المادة ٤/٢ التي قد يترتب عليها حق الدفاع الشرعي .

وهناك معضلة بصدد تحديد معنى وحدود مصطلح "مدمر": هل يعني تدمير مادي أم يشمل الضرر الاقتصادي ؟

و الإجابة:- انه في بعض الظروف يعني الضرر المادي والاقتصادي.

وبالتالي فإن المادة ٤/٢ لا تشمل جميع العقوبات الاقتصادية والسياسية القسرية والتي تهدف إلى التأثير على سياسة أو إجراءات دولة أخرى وتهدد السلامة الإقليمية او الاستقلال السياسي لها ( ) وبالتالي فهي عقوبات غير مادية ، وبالتالي فإنه اعتبار التأثير المدمر مثل (إضطراب الأسواق المالية ) قوة وفق المادة ٤/٢ إذا كان على القدر والدرجة من الخطورة الكافية لتهديد سلامة اقليم الدولة المستهدفة أو استقلالها ؛ فإن هذا الاستنتاج يضعف الفكرة برمتها وغير متوافق مع ثقل وزن السلطة القانونية أو العقيدة الدولية.

**ثالثاً- وفق إجابة شميت؛ القوة المسلحة هي المحك:-**

( ) وهناك رأي آخر وهو رأي (شميت): أنه يجب التحقق من مدى توافر المعايير التقليدية في الهجمات الإلكترونية عن طريق التحقق مما إذا كان الهجوم السيبراني مدعم بكافة المعايير التي تميز القوة المسلحة عن الإكراه السياسي أو الاقتصادي.

ويري (شميت ) أنه في ظل الهيكل الحالي للقانون الدولي ومعاييره فإنه يمكن اعتبار الهجمات الإلكترونية استعمال للقوة وفقا مادة ٤/٢ وذلك فقط عندما تشبه (الهجمات ) بشكل كاف "القوة المسلحة"

ونلاحظ هنا النمط التقليدي المتمثل في إسناده مفاهيم القوة إلى الأدوات ؛ حيث تحظر المادة ٤/٢ استخدام أداة معينة أي القوة العسكرية ضد دولة أخرى وقرن هذا الاستخدام بالنتائج المترتبة عليه وهو الدمار المادي والإصابة.

(ISSN: 2356 - 9492)

وهذا ما يفسر دائما الارتباط الوثيق بين استخدام القوة المسلحة والتدمير الجسدي أو الإصابات وذلك لا ينطبق على (حظر الإكراه الاقتصادي أو السياسي الوارد بنفس المادة ٤/٢؛ والذي كانت صلته بالتدمير المادي أو الإصابة الجسدية ضعيفة.

وقد وضع شميت عدة معايير للتحقق من مدى قرب الهجمات الإلكترونية و تطابقها مع القوى المسلحة وهي:-

١_الشدة: وتتمثل في اكبر و أخطر إصابة جسدية أو إتلاف للممتلكات المرتبطة باستخدام القوة المسلحة .

٢_ الفورية :- أي السرعة النسبية للضرر الناشئ عن القوة المسلحة مقارنة بالضرر الناشئ عن أشكال الإكراه الأخرى .

٣_ الصلة المباشرة نسبيا بين القوى المسلحة والعواقب السلبية مقارنة بالصلة المباشرة لأشكال الإكراه الأخرى.

٤_ قابلية النتائج للقياس : حيث أن الفعل المسبب للضرر يعبر عادة إلى أراضي الدولة المستهدفة وهذا متوفر بالنسبة للقوة المسلحة وغير متوفر بالنسبة للإكراه الاقتصادي والسياسي فهو غير قابل للقياس بنفس القدر والدرجة من السهولة واليقين لتقييم عواقب القوة المسلحة مقارنة بأشكال الإكراه الأخرى.

٥- إفتراض انعدام الشرعية : فالعنف واستخدام القوة غير قانوني علي المستوي الوطني والدولي.

في حين أن معظم او العديد من أوجه الإكراه الاقتصادي أو السياسي (مثل التدابير الاحترازية ) قانونية.

المعيار الكمي الجامع لكل هذه المعايير السابقة :-

فكل هذه (المعايير)تتجمع وتقترب من أحد طرفي الصراع (القوى المسلحة مقابل القوة الاقتصادية أو السياسية) .

تقييم وتحليل شميت والذي ترجم وحول مكونات نموذج الميثاق النوعي إلى كمي وبالتالي فقد قدم أفضل إطار عمل للعلماء والممارسين على حد سواء( ).

ومن الناحية العملية فإن البنتاجون على سبيل المثال يطبق تحليل شميت الكمي هذا على أساس يومي في مواجهة الهجمات الإلكترونية ومثال ذلك ما حدث عام ٢٠٠٦ حيث فقد البنتاجون معظم اتصالاته السلكية واللاسلكية شمال ووسط الولايات المتحدة وقد كان المحللون يحاولون معرفة سبب هذا التقصير بعد ١٥ دقيقة وكذلك فقد جميع الاتصالات مع جنوب وسط الولايات المتحدة وقد ثبت أنه حدث عرضي حيث قام طاقم بناء في مدينة كانساس سيتي بولاية ميسوري بحفر الأرض لوضع محرك خدمة من كابلات الألياف الضوئية وتمزيق ١٥٠ أنبوب توصيل بين الولايات المتحدة دون قصد أثناء الحفر . وفي اوكلاهوما سيتي أيضا تحطم ٤٠٠ أنبوب توصيل كبير حيث قطعه العمال دون قصد فقطع الاتصال لمدة ٣٦ ساعة. باستخدام تحليل شميت قرر فريق العمل الإلكتروني التابع للبنتجون أن هذا ربما لم يكن هجوما مسلحا الكترونياً( ).

(ISSN: 2356 - 9492)

## المطلب الثاني

## الوسائل الإلكترونية في إطار مفهوم "الهجوم المسلح والدفاع الشرعي

الوسائل الإلكترونية في مفهوم الهجوم المسلح ؛ فيما يتعلق بالدفاع الشرعي عن النفس كاستثناء رئيسي من حظر استخدام (القوة المسلحة) طبقا لنص المادة ٥١ من ميثاق الأمم المتحدة والتي تؤكد أنه "لا يوجد في هذا الميثاق ما يخل بالحق الطبيعي في .....الدفاع عن النفس في حالة الهجوم المسلح".

وهذا الترتيب مهم لانه بمجرد بدأ الهجوم المسلح يترتب عليه السماح للدولة المعتدي عليها بالرد العسكري وفقا حقها القانوني في الدفاع الشرعي .

مع ملاحظة أن اختيار الكلمات في مادة ٥١ من الميثاق مقيد بحالة "الهجوم المسلح" فقط دفاعا عن النفس نظرا لأن المادة ٤/٢ من الميثاق تحظر استخدام القوة فهناك فجوة واضحة بين المفهوممين "القوة المسلحة" مقابل "الهجوم المسلح".

أولاً - شروط الهجوم المسلح محل الإعتبار فى المادة ٥١ من الميثاق:

وقد فسرت محكمة العدل الدولية مصطلح هجوم مسلح في قضية نيكاراجوا.

١-أن تصل الهجمات إلى الحد الأدنى من الشدة : وقد أوضحت المحكمة ان الهجمات المسلحة يجب أن تصل إلى الحد الأدنى من الشدة وهو ما يظهره التمييز بين "القوة الأكثر خطورة " "والهجوم المسلح "وصور القوة الأخرى الأقل حدة فالتشديد هنا محل إعتبار.

وفي نفس القضية ميزت المحكمة بين "الهجمات المسلحة " "ومجرد الحدود "

٢-توفر نية الهجوم: فقد تكون المواجهات المسلحة الواقعة بالقرب من الحدود هجوم مسلح إذا كانت هذه المواجهات بنية الهجوم أما إذا كانت عمليات التوغل عرضية على الحدود فإنها لا تؤدي إلى اللجوء إلى الدفاع عن النفس فلا يعطي الحق للدولة في التمسك به حال المواجهات المسلحة العرضية غير المقصودة.

٣- العواقب الوخيمة: ومن أوجه الجدل الأخرى فيما يتعلق "بالهجوم المسلح" أن الهجوم المسلح يفترض على الاقل استخدام القوة على النحو الذي ينجم عنه عواقب وخيمة مثل التدخلات الإقليمية والخسائر البشرية وتدمير الممتلكات فهنا يتحقق التشديد .

وبالتالي فإن استخدام القوة التي لا تصل إلى الشدة العالية قد تبيح للدولة اتخاذ تدابير مضادة غير عنيفة اي انها لا تصل إلى حد الدفاع الشرعي عن النفس .وبالقياس على ذلك يمكن إجراء قياس لهذه الفروق في "استخدام القوة " مع الهجمات الإلكترونية من أجل تصنيف الهجوم السيبراني على انه هجوم مسلح.

مع ملاحظة أن المعيار الوحيد الذي يجب أخذه في الاعتبار هو "مدى الخطورة "أو "العواقب الوخيمة " اما معيار نية الهجوم التي تظهر من خلال عبور الحدود فهو عديم الجدوى هنا لان للحدود دور ثانوي في الهجمات السيبرانية.

ملاحظة أخرى بالنسبة لمعيار "العواقب الوخيمة" فهي مبنية على درجة الخطورة وهو ما جاء في تحليل - معيار - شميت ؛ لذلك تم تطبيق هذا التحليل بالفعل على الهجمات الإلكترونية كقوى مسلحة وحين تشتد الهجمات الإلكترونية فإنها تصل إلى درجة الهجوم المسلح اما باقي العناصر الاخرة -المشكلة للفجوة بين المادة ٤/٢ المتعلقة بمنع استخدام القوة والمادة ٥١ التي تجيز الدفاع الشرعي باستخدام القوة

(ISSN: 2356 - 9492)

المسلحة في حالة الهجوم المسلح - والمطورة للقوات المسلحة ستبقى هذه العناصر الأخرى كما هي؛ وبالتالي سيتم تغطية هذه الفجوة حتى في حالة الهجمات السيبرانية.

## المبحث الثالث

## الإطار القانوني للهجمات الإلكترونية

لتحديد الضوابط القانونية للهجمات "الإلكترونية السيبرانية"؛ تطبيقا لعملية القياس على المادة ٤/٢ والمادة ٥١ .

### المطلب الأول

### صعوبة تحديد الاختصاص الشخصي

صعوبة تحديد الاختصاص الشخصي لتطبيق الإطار الدولي القياسي فيما يتعلق بنسب الهجوم المسلح السيبراني إلى دولة معينة؛ فوفقا" لتحليل شميت فإنه لا يكفي مجرد استخدام القوة أو الهجوم المسلح ولكن يجب نسبته إلى الدولة المعادية أو دولة أخرى تنوب عنها. وأسباب صعوبة تحديد الاختصاص الشخصي فى الحالات الأتية:

أولا- الهجمات غير المباشرة : وهي التي ترتكبها جهات خاصة تتحمل الدولة مسؤوليتها وقد وصفت هذه الهجمات بعدوان عسكري غير مباشر يرتكبه اعوان الدولة وهو المقابل للعدوان العسكري المباشر( )؛ وهو ما أكدته محكمة العدل الدولية في قضية نيكاراجوا حينما اعترفت المحكمة بالهجمات المسلحة التي تمت بالإرسال أو بواسطة او نيابة عن عصابات مسلحة من الدولة أو النظاميين أو المرتزقة بشرط أن يتجاوز حجم وتأثير هذه الهجمات مجرد حوادث الحدود( ).

ثانياً-الأعمال الارهابية ، و الهجمات السيبرانية: لا تترك الهجمات الإرهابية التقليدية أي دليل في كثير من الأحيان وتحاول الدول الداعمة للإرهاب اخفاء علاقتها بهذه الهجمات، وتحاول الدول الواقع عليها الهجمات الإرهابية إثبات العلاقة بين الدول الداعمة للإرهاب والعناصر المنفذة له لتحميلها المسؤولية الدولية . وبالمثل في

(ISSN: 2356 - 9492)

الهجمات السيبرانية فهي شبيهة بالهجمات الارهابية حيث أنها تتم باتباع نهج مماثل ؛ حيث أنها بطبيعتها سهلة الاستخدام ، مجهولة الهوية ؛ لذا فهي مجال خصب للعمليات السرية والتحريض على الصراع بين الدول.

ولكن ما يجب ملاحظته هو انه حال أن استخدام القوة أو وقوع الهجوم المسلح عن طريق هجوم إلكتروني إرهابي يستلزم وجود عنصر قوي داعم على الاقل من المفترض أن يكون دولة اجنبية داعمة للإرهاب تتمتع بقوة اقتصادية عالية( ).

٣- التسامح السلبي مع الهجمات الإرهابية : والأبعد من ذلك ؛ أن الدولة أ أحيانا تكون مقيدة بإعتبارات سياسية أو عسكرية فتغض الطرف عن استخدام اراضيها كقاعدة للأنشطة الارهابية ضد الدولة ب الضحية دون رعاية ناشطة أو حتى تشجيع لهذه الأنشطة الإرهابية وهو ما يعد حجاب حماية لهم ضد الدولة ب والتي يجوز لها استهداف العصابات المسلحة على أراضي الدولة أ إذا ظلت حكومة الدولة أ جامدة ( ) .

ثانياً - تحديد مصدر الهجوم أي جنسية الدولة بشكل عام:-المشكلة الثانية وهي تتعلق بالتحديد الواضح للدولة التي شنت هجوما الكترونيا( بشكل مباشر أو غير مباشر ) .فالنقطة التي وقع منها الهجوم قد لا تكون داخل أراضي الدولة التي بدأت فعل معين (فقد يؤدي استخدام الوكلاء أو شبكات الربوت إلى اخفاء أصل الهجوم وأخفاء حقيقة انه وقع في أي وقت ويخلق حالة من الشك لدي الضحية حول ما إذا كانت شبكة الكمبيوتر المتأثرة قد تعرضت لهجوم خارجي .

وهنا تتضح ضرورة وأهمية تحليل شميت إذا بلغ الهجوم حد استخدام "القوة المسلحة " أو " الهجوم المسلح " و أنه غالبا ما يقع هذا الهجوم بعد أزمة سياسية دولية كنتيجة لها، وقد يؤدي التحليل السياسي والعسكري إلى حصر دائرة الشك حول دول معينة

بناءاً على تحديد مصادر المكالمات الهاتفية الواردة على سبيل المثال وقد تسهل التطورات المستقبلية التكنولوجية تحديد المهاجمين بناءاً على تحليل الظروف الدولية.

**بعض الأمثلة:**

بعد أن نقلت استونيا النصب التذكاري السوفيتي للحرب العالمية الثانية في أبريل ٢٠٠٧ عانت البلاد من هجمات واسعة النطاق أدت إلى تعطيل مواقع الويب فجأة نتيجة زيادة التحميل على النطاق الترددي للخادم .

وقد كانت الخوادم المستهدفه هي تلك التي تستضيف مواقع الويب المتعلقة أو المتصلة بالرئيس الإستوني ووكالات الأنباء الكبرى بأستونيا ومنها الوزارات الحكومية واثنين من اكبر البنوك في أستونيا .

ولذلك كانت هذه المصالح والوزارات نموذج مثالي مناسب لروسيا كي تختبر من خلاله قدرات أستونيا وحلفائها في الناتو من مقاومة هجوم إلكتروني( ).

ونخلص من ذلك: أنه لو كانت هذه الهجمات قد بلغت الحد الأدنى من الشروط وفق تحليل شميت لأصبح لأستونيا حق الدفاع عن النفس وكان يتعين على أعضاء حلف الناتو تطبيق ألية الدفاع الشرعي الجماعي ولكن هذا المستوى من "الهجوم المسلح "لم يصل إلى الحد الأدنى في تحليل شميت ( ) .

وحتى إذا فرض ان تحليل شميت قد صنف رفض الخدمة على انه "هجوم مسلح" فإن الخطوة الاخيرة وهي نسبة هذا الهجوم المسلح إلى روسيا كان من الصعب للغاية إثباته رغما المحاولات التي بذلت لتعقب أصل الهجمات بزعم أنها منسوبة إلى مؤسسات الدولة الروسية وهو ما يصعب إثباته ( ) وبالتالي لا يزال موضوع الهجمات السيبرانية موضوع مثير للجدل إلى حد كبير.

(ISSN: 2356 - 9492)

ولو افترضنا جدلا انه تم إثبات ذلك لكان رد الفعل الدفاعي التقليدي عن النفس خطير جدا لان أي تصعيد يمكن أن ينتج عنه ما لا يحمد عقباه من اثار( ). مع ملاحظة أن الجرائم الألكترونية تضم الآلاف من الأفراد العاديين والمحترفين من القراصنة العسكرية السيبرانية يرتكبون هذه الهجمات السيبرانية من أجل المال والمجد ويشتبه في استخدامهم من قبل جيوش القوى الكبرى مثل الجيش الصيني( تحالف ريد هاكر أو تشاينا يونيون ايجل) وهذه الهجمات تعمل كجيش احتياطي نشط ومؤثر- بالنسبة للدول التي ترتكب هذه الهجمات لصالحها في حرب غير تقليدية او غير متكافئة .

فإذا قام هؤلاء المخترقون بتنفيذ هجوم مسلح عبر الإنترنت يستوفي الحد الأدنى لمعايير شميت -إنجاز شبه مستحيل - ومع ذلك ينبغي النظر في مسؤولية هذه الدول و مواجهتها بالدفاع الشرعي العسكري عن النفس. اما إذا لم يصل هذا الهجوم السيبراني إلى الحد الأدنى لمعايير شميت فيجب اعتبار هذه الدولة تثير مشاكل القانون الدولي مما يترتب عليه المسؤولية الدولية او القانون الجنائي الدولي .

وأخيرا يجب أن تكون التحليلات الفنية أو القانونية أو السياسية متوازنة دائما مع الخيارات الاستراتيجية في هذه المسألة الحساسة للغاية.

## المطلب الثاني

## شروط الاختصاص الزماني ل "هجوم مسلح "إلكتروني

## يؤدي إلى تفعيل الدفاع الشرعي

يعتد بالعنصر الزمني في الهجوم الالكتروني لاعتباره هجوم مسلح يترتب عليه حق الدفاع الشرعي؛ فإن توقيت الدفاع عن النفس هنا عنصر حاسم حيث انه يمكن القيام بحق الدفاع عن النفس في لحظات مختلفة لمواجهة الهجوم المسلح وذلك فى حالتين:

أولاً- الدفاع الشرعي الإستباقي عن النفس:

من الضروري فحص ما إذا كان الهجوم على الكمبيوتر قد وقع بالفعل من أجل بدء التشغيل ؛ هنا اختلفت وجهات النظر إلى رأيين:-

الرأي الأول :- وهو يرى رفض حق اللجوء إلى الدفاع الشرعي الإستباقي وفق مادة ٥١ استنادا إلى أنه استثناء من حظر استخدام القوة وفق مادة ٤/٢ ويجب التضييق منه - الدفاع الشرعي الوقائي - تمسكا" بحرفية نص المادة ٤/٢ في حالة وقوع "هجوم مسلح "( ).

الرأي الثاني:- وهو يرى عكس ذلك تمسكاً بأن حق الدفاع الشرعي الوقائي متأصل بموجب القانون العرفي القديم فهو الذي يسمح بالدفاع الاستباقي مستندين في ذلك علي حادثة كارولين عام ١٨٣٧ وحجتهم أيضا انه في العصر النووي لا يتوقع من الدول الإنتظار إلى "الضربة الأولى".
وغالبية العلماء يرفضون مقارنة قيمة منع وحظر استخدام القوة وقيمة حادثة كارولين ( ).

وأيضا يحذرون من نتائج التصعيد المبني على قبول الإجراءات الاستباقية في حال الهجوم الألكتروني، وأخيرا يجب أن يكون حظر الدفاع الشرعي الاستباقي حظر صريح واضح تماما.

ثانياً- اعتراض الدفاع عن النفس :- إذا كان ثمة هجوم مسلح وشيك او على وشك الوقوع فقد لا ينتظر الضحية المستهدفة بلا حول ولا قوة الضربة الحتمية ، وهنا يمكن اعتراض هذا الهجوم بشكل شرعي وهنا يعد دفاع شرعي عن النفس وفقا مادة ٥١ من الميثاق( ).

ويعد اعتراض الدفاع عن النفس وثيق الصلة بهجمات الكمبيوتر إذا استهدفت الطفل رغم أنها ليست قاتلة للأشخاص ولا مدمرة للممتلكات باستخدام تحليل شميت وهنا

(ISSN: 2356 - 9492)

يكفي اعتبار مجرد الاقتحام هو الخطوة الأولى في "هجوم مسلح " لا مفر منه نتيجة صعوبة تفسير المعلومات المتاحة وقت اتخاذ الإجراءات (مثال التحذيرات والتقارير الاستخباراتية وغيرها من البيانات المتاحة).

## المبحث الرابع

## آفاق وتحديات جديدة

في هذا المبحث نناقش مدى إمكانية استخدام الوسائل الإلكترونية للدفاع عن النفس قياسا على المفهوم التقليدي "للقوة المسلحة أو الهجوم المسلح " في ضوء العديد من التحديات النظرية والعملية المحيطة بهذا الموضوع الاستكشافي

### المطلب الأول

### هجمات الكمبيوتر كوسيلة للدفاع عن النفس

وفقا لتحليل شميت يمكن اعتبار هجوم الكمبيوتر "هجوم مسلح" وبالتالي فإنه يمكن استخدام هجمات الكمبيوتر كدفاع شرعي .

وكما يسمح باستخدام جميع الوسائل العسكرية ضد أي عدوان فإنه يسمح كذلك بكافة الوسائل الإلكترونية ضد أي هجمات سيبرانية.

مع مراعاة القيود الموضوعية على حق الدفاع عن النفس وهي معيار الضرورة والتناسب كما حدث في قضية نيكاراجوا حيث أقرت محكمة العدل الدولية بهذين المعيارين لتطبيق المادة ٥١ ( ).

**أولاً- الضرورة :**

وتعني الضرورة انه لا توجد طريقة بديلة متاحة للانتصاف ويجب أن يتفق يكون الهدف العسكري الأساسي مع قواعد القانون الدولي الإنساني.

كما أن الضرورة أيضا تتطلب أن يكون الوقت بين الهجوم المسلح والدفاع عن النفس قصير إلى حد معقول مع الاخذ في الاعتبار الحاجة إلى إجراء تحقيقات أو القيام

(ISSN: 2356 - 9492)

بالمفاوضات او الاستعدادات العسكرية وهذا هو الحد الأقصى للوقت اللازم لشرعية الدفاع الشرعي الاعتراضى عن النفس .

**ثانياً- التناسب :**

ومن ناحية أخرى يفترض التناسب أن استخدام الدفاع عن النفس يقاس بمقابلته للهجمات المسلحة من حيث الشدة والمدة والموقع والنطاق والأهداف المحددة وهنا تكمن مشكلة حقيقية في تصنيف الهجمات الإلكترونية على أنها دفاع عن النفس لأن هذه الهجمات غير مؤكدة النتائج بشكل طبيعي وبالتالي يصعب تقدير هذه الشروط والضمانات سالفة الذكر النطاق والأهداف المحددة .

وهنا تكمن مشكلة حقيقية في تصنيف الهجمات الإلكترونية على أنها دفاع عن النفس لأن هذه الهجمات غير مؤكدة النتائج بشكل طبيعي وبالتالي يصعب تقدير هذه الشروط والضمانات سالفة الذكر- النطاق والأهداف و....- وقد تكون عواقب الهجوم السيبراني مباشرة أو غير مباشرة وقد تكون العواقب غير المباشرة أعلى من العواقب المباشرة( ).

**رأي الباحث :-**

ومما سبق يتضح مدي الصعوبة البالغة في تطبيق معايير التناسب في حالة الدفاع الشرعي عن النفس علي الهجوم السيبراني حيث يجب تضيق نطاق خطر التصعيد في استخدام الهجمات الإلكترونية على النطاق الدولي الحالي ونأمل في المستقبل ان يتم صياغة حل نهائي يسمح بالسيطرة على الهجمات الإلكترونية مثل تطوير الدفاعات الإلكترونية.

## المطلب الثاني

## الصعوبات التي تواجه البحث

( أي تتعارض مع إعمال القياس )

أي صعوبة تطبيق المعايير التقليدية للقوة المسلحة أو الهجوم المسلح على معنى السيبرانية .

أسباب عدم التطابق بين النموذج التقليدي ًللقوات المسلحةً أو ًالهجوم المسلحً والهجمات الإلكترونية:

يعد تعبير استخدام الهجمات الإلكترونية ردا على هجوم مثله اوقع ولكن لا يصل إلى درجة الهجوم المسلح (وفق معيار شميت).

**أولاً: صعوبة تحديد معنى السيبرانية-**

تثار بعض المشكلات بسبب عدم وضوح طبيعة الوسائل السيبرانية لاسيما وأنها وسائل متعددة الأغراض -سلاح ذو حدين - وطرق استغلال شبكة الكمبيوتر تتشابه مع طرق استخدام الكمبيوتر في الهجمات السيبرانية رغم اختلاف الهدف في الحالتين "الهجمات والإستغلال العادي ".

مثال لتوضيح ذلك :- زعمت صحيفة وول ستريت جورنال أن بعض الوكالات من الصين وروسيا وعدة دول أخرى تسللت إلى أنظمة الكمبيوتر المكلفة بإدارة الكهرباء في الولايات المتحدة الأمريكية حيث أنهم تركو ورائهم برامج يمكن استخدامها للتحكم او لتعطيل الشبكات الكهربائية في الولايات المتحدة الأمريكية .

(ISSN: 2356 - 9492)

وقد أظهر هذا الحادث ثغرات في البنية التحتية الأمنية الأمريكية وقت النزاع، بالإضافة إلى أنه من الممكن أن يكون لهذا الهجوم آثار كارثية هنا مثل جمع المعلومات الاستخباراتية وهو ما يجعلها صالحة للهجوم الإلكتروني في المستقبل .

**ثانياً- صعوبة وصول هجمات شبكات الكمبيوتر الي حد "الهجوم المسلح":**

إذا لم يصل الهجوم (الإلكتروني)الأول إلى درجة أو إلى حد هجوم مسلح فلا يوجد حق الدفاع عن النفس ولكن هذا الهجوم (رد الفعل) يعد انتقام أو عدوان وليس دفاعا عن النفس شرعي نظرا لتوفر عنصر التخطيط المسبق لاستخدام هجمات الكمبيوتر المضادة كرد فعل لاستخدام أدوات هجومية للهجوم( الفعل).

مثال ذلك استخدام الولايات المتحدة الأمريكية -كدولة مستهدفة - بهجمات الكمبيوتر( ) لروبوتات عسكرية ذات محركات أقراص ثابتة وخاصة بهم وفلاتر مدمجة تمنع استهداف أجهزة الكمبيوتر العسكرية والحكومية الأمريكية ؛ فهذا فعل من الدولة القائمة بالهجمات السيبرانية ورد فعل من الولايات المتحدة الأمريكية مخطط له مسبقا قبل وقوع الهجمة ولا يعد حالة دفاع شرعي وقائي أو غير وقائي وإنما رد فعل انتقامي وهو يؤدى الي زيادة مخاطر التصعيد السيبراني كرد فعل يتفق مع الطبيعة العشوائية لهجمات الكمبيوتر وبالتصعيد والتجميع لهذه القوي والهجمات والنتائج المترتبة عليها، وهو ما قد يؤدي إلى نشوب نزاع مسلح تقليدي.

فالاخطار هنا اكبر من أن تجعلنا نعتمد نظرية وفكرة اعتبار الهجمات المضادة لهجمات الكمبيوتر دفاع شرعي أو اعتماد الدفاع الشرعي الوقائي - م ٥١ - وفقا لتحليل شميت المبني على جسامة النتائج ولكن اعتماد نظرية الفعل وردة الفعل الانتقامي.

**ثالثاً- استثناء الوسائل الإلكترونية متعددة الأغراض من التجسس:**

نظرا للطبيعة متعددة الأغراض للوسائل الإلكترونية فالتجسس لا يصنف في ب فمن زاوية نظر النزاع المسلح للتجسس في العلاقات الدولية فهو يستثنى من الأعمال الضارة غير القانونية التي تستخدمها كل دولة باستمرار ( ) .

وهنا يكون الحل الوحيد للدولة المتضررة استخدام أدوات الدفاع السيبراني في حين أن استخدام هجمات الكمبيوتر في الانتقام سيكون اختيار لا يتفق مع العقل والمنطق كرد فعل لهجوم انتقامي سيبراني للرد على هجوم سابق لم يرقى إلى درجة هجوم مسلح تقليدي وفق مادة ٤/٢ .

وهذا المثال يوضح الاختلاف الواضح بين خصائص النزاع المسلح التقليدي وخصائص الهجمات السيبرانية.

(ISSN: 2356 - 9492)

## الخاتمة:

### أولا: الخلاصة:

اعتمد توصيف الهجوم السيبراني على الركائز الأساسية للتحليل القانوني للمادة ٢(٤) المتعلقة باستخدام "القوة المسلحة "و المادة ٥١ من الميثاق المتعلقة "بالهجوم المسلح " لتوصيف الهجوم السيبراني على انه استخدام تقليدي للقوة المسلحة أو هجوم مسلح .

وقد وضع شميت عدة معايير كشروط لاعتماد ذلك التوصيف وأيضا التدمير ونتيجة الهجمات السيبرانية ولكن ذلك التوصيف تعارض مع العديد من المعضلات ومنها إثبات نسب الهجمات السيبرانية إلى الدولة التي ينتمي إليها السيبرانييون مرتكبي الهجمة وكذلك تتعارض مع فكرة الدفاع الشرعي الوقائي او الإستباقي او الاعتراضي.

وهو ما كاشف عن صعوبة توصيف الهجموم السيبراني على انه نزاع مسلح فعلي . هذا على الجانب القانوني النظري اما على الجانب التطبيقي العملي أو الواقعي فعلي الدول الكبرى أن تعمل جاهدة على توفير وضمان الاستقرار الدولي .

ويظهر تطور الهجمات الإلكترونية الفعلية أن الدول تتصرف في الخفاء عن طريق جهات فاعلة خاصة (كما هو الحال في روسيا والصين ) أو أنها تستخدم قوات عسكرية عالية الكفاءة ودقيقة التخصص (كما هو الحال في الولايات المتحدة الأمريكية ) ؛ وهو ما يعكس الواقع وهو أنه لا يوجد دولة على استعداد لتصعيد هجمات شبكة الكمبيوتر لمطابقة( لبلوغ) معيار الهجوم المسلح (وفقا لمعايير شميت ) وللمخاطرة بإثارة ملف دفاع شرعي وهو ما قد يمثل عدوان إذا لم تنطبق معايير الدفاع الشرعي على حالة الهجوم السيبراني محل النظر وهو ما قد يؤدي إلى حرب شاملة.

لذلك فإنه عندما نطلق على كل استخدامات الإنترنت الحرب السيبرانية؛ فذلك كاستعاره فقط ولكن الأقرب والأكثر ملائمة فعليا للإطار المعياري الدولي الفعلي هو أن نطلق على الأعمال الإلكترونية المرتبطة بالدولة ًالاستغلال السيبرانيً وليس ًالهجمات السيبرانيةً.

ونأمل في المستقبل القريب ومع التطور أن يكون للدول أعضاء المجتمع الدولي بما لديها من وسائل إلكترونية جديدة اهداف سياسية نحو وقف التطورات الأكثر خطورة المؤدية إلى حرب إلكترونية حقيقية .

**ثانياَ: - أهم النتائج والتوصيات**

من خلال دراسات الهجمات السيبرانية أو الحرب الإلكترونية أو هجمات الكومبيوتر والتي تمت دراستها وتحليلها فى ضوء قواعد استخدام القوة في القانون الدولي العام ( أي الاستغلال السيبراني) ، وعلي ضوء التهديدات والتحديات المصاحبة لتكنولوجيا المعلومات والذكاء الإصطناعي وفى إطار القواعد الأمرة المتعلقة بالنظام العام الدولى والمصلحة الدولية المتمثلة فى حفظ السلم والأمن الدوليين؛ كانت النتائج النحو التالي:

**النتائج:**

١- يواجه الإنسان العديد من المشكلات المعقدة والمركبة قدراً، ونوعا، وكماً ؛ جراء التهديد الناجمة عن أوجه الاستغلال السيبراني المختلفة لاسيما الضارة منها مثل التسلل الي أنظمة الكمبيوتر المكلفة بإدارة المرافق العامة في الدولة المستهدفة بالهجمات ومنها شبكة الكهرباء وتعطيلها مثل ما حدث في الولايات المتحدة الأمريكية، وكذلك الإستغلال السيبراني في جمع المعلومات ثم القيام بهجمات الكترونية فى المستقبل.

(ISSN: 2356 - 9492)

٢- يمثل هذا النوع من التكنولوجيا الخطر الداهم علي الدول وينعكس علي السلم والأمن الدوليين أذا تم استخدامها علي هذا الوجه السلبى.

**التوصيات:**

لابد من تضافر الجهود السياسية للمجتمع الدولي بألياته القانونية والمؤسسية والإجرائية لمواجهة الوجه السلبي لهذه التكنولوجيا المقيتة ووقف التطورات الأكثر خطورة التي قد تؤدى الي حرب إلكترونية فعلية ؛ وبالتالي حفظ السلم والأمن الدوليين

وأخر دعوانا

أن الحمد لله رب العالمين