جامعة عمار ثليجي —الأغواط —
كلية الحقوق والعلوم السياسية
قسم الحقوق

مذكرة مكملة لنيل شهادة ماستر في الحقوق
-تخصص قانون دولي والعلاقات الدولية —

بعنوان

أمن المعلومات الإلكترونية في القانون الدولي

إعداد الطالبة
وحشي جميلة

إشراف الأستاذين:
الدكتور قريبيز مراد
الدكتور مليناني عبد الوهاب

لجنة المناقشة

لخضر زازة	أستاذ التعليم العالي	رئيسا
مراد قريبيز	دكتور محاضر أ	مشرفا ومقررا
عبد الوهاب مليناني	دكتور محاضر ب	مشرفا مساعدا
بلقاسم ويدوني	دكتور محاضر أ	ممتحنا

السنة الجامعية: 2018/2017

كلمة شكر و عرفان

إذا كان ولابد من كلمة شكر وثناء فإن الحروف تتسابق والعبارات تتزاحم لتبوح بعبق الشكر والامتنان لكل من كان سبباً في ميلاد عملي هذا ،الذي كان فكرةً تلوح في سماء البحث والتنقيب واليوم بات مولودا يافعاً احتصنه أستاذي المشرف **الدكتور مراد قريبيز** الذي تخوننا العبارات وتعجز الألسن عن ذكر ما قدمه لنا من مساعدة وتوجيهات قيمة ،وملاحظات سديدة أنارت درب البحث ومنهجه .

كما لا يفوتني أن أشكر **الدكتور عبد الوهاب ملياني** المشرف المساعد على كرم توجيهاته، ونصائحه القيمة والمفيدة .

أتقدم إلى أساتذتي الأجلاء، الفضلاء أعضاء لجنة المناقشة على كريم تفضلهم بمناقشة عملي وإثراءه .

و إلى موظفي وعمال المكتبة المركزية ومكتبة كلية الحقوق والعلوم السياسية على سعة صدورهم، ورحابة أفقهم وكذا التسهيلات الكبيرة التي حظينا بها منذ كان البحث فكرة وخطة .

فالشكر لمن ساعد والذكر لمن وقف ،والفضل لمن قدم وعبر ونظر .

الإهـــــداء

أهدي هذه الباكورة اليانعة وهذه القطوف الدانية :

إلى من قال فيهم المولى سبحانه و تعالى :" و قل رب ارحمهما كما ربياني صغيرا " و الداي العزيزين البدرين المشرقين والكوكبين النيرين أمدهما الله بالصحة والهناء وألبسهما الحلم والنقاء والعفة والصفاء.

و إلى زوجي العزيز الغالي رفيق دربي الذي تكبد العناء في سبيل مساندتي للوصول إلى ما وصلت إليه .

إلى قرتي عيني أولادي نبراس الوجود وشموع الأمل، و أتمنى لهم التوفيق و السداد .

و إلى أخوتي و أخواتي و أخص بالذّكر أختي الراحلة سامية تغمدها الله برحمته الواسعة وجعل مقامها في العليين .

إلى كل من سقط في ميدان الشرف ذوداً عن الجزائر ، إلى شهداء ضحايا سقوط الطائرة العسكرية التي خلفت 275 شهيدا ببوفاريك نسأل الله أن يجعلهم من الشهداء و الصادقين أحياء عند ربهم يرزقون فهم الذين لا خوف عليهم و لا هم يحزنون .

قائمة الاختصارات

AICAN	القمة العالمية لمجتمع المعلومات
CIRT	أفرقة وطنية للاستجابة للحوادث الحاسوبية
DARPA	وكالة مشاريع الأبحاث الدفاعية المتقدمة
DNS	نطاق اسماء الميادين
EU	الاتحاد الاوروبي
FIRST	افرقة التصدي لحوادث الامن
GCA	برنامج الامن السيبراني العالمي
ITU	الاتحاد الدولي للاتصالات
IT	تكنولوجيا المعلومات
IP	بروتوكول الانترنات
ICT	تكنولوجيا المعلومات و الاتصالات
MPACT	الشراكة الدولية المتعددة الاطراف لمكافحة التهديد السيبراني
NATO	منظمة حلف الشمال الاطلسي
UNCPCJ	مؤتمر الامم المتحدة لمنع الجريمة و العدالة الجنائية
WSIS	القمة العالمية لمجتمع المعلومات

قطاع تقييس الاتصالات في الاتحاد الدولي للاتصالات	

مقدمة

واجه العالم في السنوات الأخيرة تحديا كبيرا في مجال تقنية المعلومات[1] Informatique مما اكسبه اسم عصر المعلومات[2] ، كونها أصبحت الأداة التي تقاس بها قوة الشعوب ، فمن يملك المعلومة يملك القوة ،لذلك حرصت الدول على تأمين هذه المعلومات وحمايتها بشكل مستمر ومحاولة الوصول إلى كل ما هوجديد حول امن المعلومات الالكترونية (Sécurité de l'information électronique) ، ويتضح مما سبق أن لمفهوم امن المعلومات الالكترونية أهمية بالغة في حياتنا المعاصرة نظرا لاعتمادنا الكبير على المعلومات في شتى المجالات.

ومن الصعوبة بما كان وضع مفهوما محددا لأمن المعلومات الالكترونية ذات الطبيعة التقنية والتي باتت تظيف للبشرية وبشكل يومي كل ما هو جديد ومتطور في عالم التكنولوجيات، ولكن محاولة وضع مفهوما جامعا لأمن المعلومات الالكترونية من قبل الأفراد والمؤسسات والمجتمعات والحكومات والدول يساعدها على تحقيق العديد من الفوائد، أهمها مواجهة التهديدات الناشئة في عالم الفضاء الالكتروني[3] Espace électronique كعمليات الاختراق[4] الأمني والتجسس المعلوماتي[5] وبهذا الشأن ولمعرفة المقصود بأمن المعلومات وجب علينا أخذه من ثلاث زوايا:

الزاوية الاكاديمية :يقصد به من خلال هذه الزاوية ،العلم المكون لنظريات واستراتجيات ووسائل حماية المعلومات من المخاطر من أية أنشطة اعتدائية ضارة قد تأثر على فحواها.

---

[1] **تقنية المعلومات**:أية وسيلة مادية او معنوية او مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتحزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقا للأوامر والتعليمات المحزنة بها ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها .....للمزيد اطلع على: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010.

[2] **المعلومات**:ورد تعريف للمعلومات في الموسوعة العربية لمصطلحات علوم المكتبات بأنها (البيانات التي تمت معاجلتها لتحقيق هدف معين) .... للمزيد اطلع على: ملياني عبد الوهاب، امن المعلومات في بيئة الأعمال الالكترونية، رسالة شهادة الدكتوراه في القانون العام، جامعة ابي بكر بلقايد _تلمسان_، كلية الحقوق و العلوم السياسية قسم الحقوق.

[3] **الفضاء الالكتروني**: يمكن تعريف الفضاء الالكتروني بالبنية التحتية الكونية لشبكات نقل وتبادل البيانات والمعلومات (الأنترنت) وقواعد المعلومات، والحاسبات الآلية، والمواقع والمنصات والسيرفرات.... وغيرها من الوسائل التي يتم من خلالها الربط والتواصل الإلكتروني.....للمزيد اطلع على الرابط:http://1asir.com/345236 .

[4] **الاختراق**:بشكل عام هو القدرة على الوصول لهدف معين والدخول على الأجهزة بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بها بهدف التطفل على خصوصيات الآخرين أو التطفل عليهم ..... للمزيد اطلع على :بشرى حسين الحمداني،القرصنة الالكترونية،دار أسامة للنشر والتوزيع ،الأردن،الطبعة الأولى،2014 ،ص13.

الزاوية التقنية:تشير هذه الزاوية إلى الإجراءات والأدوات التكنولوجية الواجب توافرها لضمان حماية المعلومات.

الزاوية القانونية:تتناول هذه الزاوية الدراسات والتدابير الحمائية والسرية اللازمة لتوفير الغطاء الأمني والقانوني للمعلومات،وسن التشريعات القانونية لحمايتها من استغلالها في أنشطة غير مشروعة.

من هذا يمكننا القول كنتيجة أولية أن أمن المعلومات الالكترونية هو عبارة عن "**مجموعة الجهود الوطنية والدولية الرامية لحماية المحتوى المعلوماتي للأفراد والمؤسسات والحكومات والدول بتوفير بيئة قانونية وتقنية آمنة من كل الاعتداءات الالكترونية**"[1]

وعلى الرغم من الصورة الباهرة التي رسمتها تكنولوجيا المعلومات[2] Technologie de l'information للإنسانية ومحاسن الثورة المعلوماتية[3] التي غمرت البشرية بنتائجها في عصرنا الحالي، إلا أنها أدخلت دول العالم في هاجس امني قوي خصوصا وأن هذه الدول قامت بوضع مدخراتها الوطنية على شكل معلومات رقمية عبر فضاء مذاب الخصوصية وضعيف الأمن، وفائق السرعة ،وزئبقي بشكل كبير.

---

[1] هذا التعريف استنتاج شخصي للباحث و هو قابل و خاضع للنقد و التطوير و التصويب

[2] **تكنولوجيا المعلومات:** يحتوي على هذا المصطلح على جزئين، الأول تكنو والتي تعني المهارة الفنية في التعامل مع الأشياء، والثاني لوجيا والتي تعني العلم والأسس في التعامل مع الأشياء، وارتبطت كلمة تكنولوجيا مع كلمة المعلومات لانشاء مفهوم جديد ظهر في أفق العلوم العلمية وأصبح يسمى بتكنولوجيا المعلومات.

هي كافة الأسس والطرق والخطوات المتبعة عند الاتصال، ونشر المعلومات، والقيام بالعمليات الحسابية باستخدام كافة الأجهزة الإلكترونية المعدة لذلك مثل الحاسوب ووسائل الاتصال المختلفة ضمن ثوابت وقوانين علمية وضعت لذلك. ثرت تكنولوجيا المعلومات والاتصالات في الحياة البشرية بشكلٍ كبير، فمنذ الثورة الصناعية بدأ الإنسان بتطوير الآلات والمعدات التي تسهّل من عمله، ومع ظهور تكنولوجيا المعلومات قفزت البشرية قفزة نوعية نحو التطوّر من جهة والرفاهية من جهة أخرى، حيث كانت الأعمال قديماً تقام داخل المكاتب باستخدام الأوراق والمعاملات بشكل يدوي مما يؤدي إلى استغراقها وقتاً طويلاً لإنهائها، وبعد دخول التكنولوجيا عالم الأعمال أصبحت الاتفاقيات والمعاملات تقام من أيّ مكان في العالم وبسرعة بالغة، وبالتالي فإنّ لتكنولوجيا المعلومات والاتصالات لها الأثر الكبير في حياتنا.....للمزيد اطلع على موقع موضوع على الرابط: http://mawdoo3.com

[3] **المعلوماتية:**هي كلمة مكونة من مقطعين المقطع الأول من كلمة معلومات information والمقطع الثاني من كلمة اوتوماتيك automatique وكلمة المعلوماتية مصطلح استعمله لأول مرة A.I.Mikhailov وهو مدير المعهد الاتحادي للمعلومات العلمية والتقنية بالاتحاد السوفيتي سابقا ...للمزيد اطلع طارق إبراهيم الدسوقي عطية ،الأمن المعلوماتي ،دار الجامعة الجديدة ،2009/ص43.

وأعادت الوسائل التقنية والالكترونية الحديثة شريعة الغاب التي عاش بها الإنسان في عصوره الأولى ولكن بمشهد تكنولوجي ومعلوماتي تخلومنه الأخلاق والمبادئ وتعلو فيه صيحة المصلحة حتى وأن كلف ذلك الاعتداء على المعلومات الالكترونية للآخرين وإلحاق الأذى بهم في ترجمة حقيقية لمقولة المها تما غاندي[1] الشهيرة "سياسة بلا مبادئ، تجارة بلى أخلاق، ثروة بلا عمل، تعليم بلا تربية، وعلم بلا ضمير، وعبادة بلا تضحية".

احتلت صراعات الفضاء الالكتروني المشهد الكبير لعصرنا الحالي،حيث تراجعت نغمات التهديد بالأسلحة النووية والبيولوجية والتقليدية التي عهدها الإنسان خلال عصره الحديث والمعاصر لتتحول صراعات الإنسان إلى صدامات هادئة وصامتة وناعمة معتمدة اعتمادا كليا على الأسلحة الالكترونية[2] Armes électroniques كالرسائل الالكترونيةE-mails والهواتف المحمولةTéléphones portables وأجهزة الحاسوب Matériel informatique وصفحات الانترنت Pages Web وغيرها من الأدوات الالكترونية والتي أصبحت تشكل لدول العالم أخطارا تهدد نظامها المعلوماتي[3]Système d'information وتكلفها ملايين الدولارات.

كما أن انتقال النشطات الإنسانية إلى الفضاء السيبراني Cyberespace[4] حمل معه مشاكل وتعقيدات هذه النشطات الشرعية منها وغير الشرعية ومن مبدأ أن ما هو غير شرعي في الحياة المادية

---

[1] **الماهاتماغاندي** : يعتبر غاندي الأب الروحي لحركة الاستقلال الهندية ، فقد قضى المهاتما غاندي 20 عاما في جنوب افريقيا يعمل على مكافحة التمييز والتعصب في المعاملة ، كما انه أسس حركته الخاصة ضد حكم البريطانيين التي اسماها ساتياغراها ، ولكنها كانت حركة غير عنيفة احتجاجا علي الظلم ، أثناء تواجده في الهند ، كانت حياة غاندي مليئة بالبساطة والفضائل التي جعلته محبوب من الشعب وطريقة لبسه البسيطة جعلته قريب منهم.

[2] الاسلحة الالكترونية :

[3] **النظام المعلوماتي**:ويشمل كامل نطاق الوسائل التقنية المستخدمة لإرسال المعلومات وتلقيها وخزنها ،فمثلا وحسب الحالة الواقعية يمكن أن يشير مفهوم نظام المعلومات إلى شبكة الاتصالات وفي حالات أخرى إلى صندوق بريد الكتروني أو حتى إلى ناسخ برقي ....للمزيد اطلع على:موسوعة القانون الالكتروني وتكنولوجيا الاتصالات ،دار المطبوعات الجامعية ،2007،ص48 .

[4] **Cyberespace** : l'espace virtuel contenu par les ordinateurs ou entre eux dans le cas de mise en réseau …… voir :Anne Thida NORODOM, internet et le droit international défi ou opportunité ? ,COLLOQUE DE ROUEN 2014, P 13.

وفي المجتمع التقليدي خارج تقنيات المعلومات والاتصالات يبقى غير شرعي على الانترنت [1] internet والفضاء السيبراني.

وتأسيسا لما تم ذكره فان إمبراطورية التقدم التقني المعلوماتي آخذة بالتوسع بشكل يفوق حجم الوجود الإنساني ،ويتجاوز العديد من المفاهيم الهامة للبشرية وتطبيقاتها على ارض الواقع ،أهمها مفهوم الأمن الدولي والمرتبط أساسا بسيادة الدولةLa souveraineté de l'État ،وهو ما دفع بالرئيس جاك شيراك بالتصريح بأن (...الدول في طريقها لفقدان السيطرة على أعمالها،وهذا دلالة على قوة تأثير التقنيات على سيادة الدول).

وخلاصة القول ،يمكننا التنويه هنا وفي وطأة هذا التلاحم الإنساني الرقمي **انه بات على دول العالم حماية امن معلوماتها الالكترونية ،والذي راح يشكل خطرا كبيرا على بنيتها التحتية الأساسية، وبالتالي تهديد وجودها في عالم تكنولوجي ومعرفي تسوده المخاطر من كل حدب وصوب.**

ومن هذا المنطلق تظهر لنا **أهمية البحث** من حيث التحدي التكنولوجي الحديث للمفاهيم القانونية التقليدية إذ أصبحت المعلومات تتدفق بسهولة اكبر ولم تعد الحدود عائقا أمام هذا التدفق، فضلا على أن المجرمين مافتئوا يتواجدون في أماكن غير تلك التي تنتج فيها أفعالهم أثارها، ولذلك كان لابد من إيجاد حلول على شكل صكوك قانونية دولية ملائمة ومن ثم اكتسب مجال الفضاء الالكتروني مكانة بين الدول،حيث أصبح هذا الفضاء مجالا مستهدفا بشكل كبير خصوصا مع ارتفاع وتيرة التقدم التكنولوجي والتقني والالكتروني مما حدا بالعديد من الدول للسعي من اجل حماية أمنها المعلوماتي.

كما أن لهذه **الدراسة أهمية** في تحديد الآثار السلبية التي حدثت على صعيد العلاقات الدولية نتيجة استخدام الانترنت كأداة لشن الحروب المعلوماتية information warfare في وقت قصير وبتكلفة قليلة، هذا بالإضافة إلى أهمية عملية وهي معرفة التحليلات والنصوص القانونية التي تعنى بالهجمات الالكترونية وسبل الدفاع الشرعي في إطار القانون الدولي والعلاقات الدولية.

[1] **L'internet** : est né dans les années 1960 de la volonté des autorités américaines d'installer un réseau de communication susceptible de transférer en toute sécurité de grandes quantités de données « sensible » et qui soit capable de résister à une guerre nucléare. Les militaires jouérent un rôle essentiel dans la mise en pl ace de l'architecture du réseau des réseaux….. VOIR : ABDELWAHAB BIAD , cyberguerre et lex specialis evolution ou révolution COLLOQUE DE ROUEN 2014 P 254.

ومما سبق ذكره **تهدف دراستنا** إلى إلقاء الضوء على عدد من المسائل التي ترتبط بالأمن المعلوماتي عبر تشخيصها ورصد أبعادها الدولية وهي بذلك تشكل إضافة للمحاولات التي سبقت وتضع بين أيدي الطلبة والباحثين مادة تساعدهم على تكوين رؤية في بحوثهم ودراساتهم ولا ندعي الإحاطة بكل المسائل،لاسيما مع التغيرات المتواصلة والسريعة التي تطال قطاع التقنيات والاتصالات.

ومن هنا يظهر جليا **سبب اختيارنا** لهذا البحث والذي نفرد فيها بين ماهو **ذاتي** ينحصر في عدم تناول الموضوع على غير العادة في أبحاث القانون الدولي،أيضا تأثرنا بالتوترات الدولية الحالية والتي اخذ فيها مجال الفضاء الالكتروني النصيب الأكبر، وما هو **موضوعي** يتلخص في أن مصطلح الأمن المعلوماتي مصطلح غامض وما يفسر هذا الغموض انه مصطلح جديد ظهر على الساحة الدولية فأردنا أن نزيل هذا الغموض بالدراسة والبحث فيه.

ومن هذا المنطلق كانت **أهم الصعوبات** التي واجهتني إثناء البحث مسألة تعريب المصطلحات التقنية الأجنبية وترجمتها إلى اللغة العربية في غياب قواميس متخصصة ،أيضا ندرة المراجع والأبحاث العربية ومكمن الصعوبة الكبرى في تطبيق القواعد القانونية الدولية التقليدية المتعارف عليها في الفضاء المادي على الفضاء الالكترونيEspace électronique وأيضا كثرة المصطلحات التقنية والتي تتعلق بموضوع البحث وعدم اتفاق المراجع على إعطاء تعاريف موحدة لها.

ككل دراسة، فان دراستنا هذه لا تنطلق من فراغ على الرغم من قلة المراجع المتخصصة فيها، وبالقيام بمسح لأهم **الدراسات السابقة** التي كتبت حول الموضوع نستطيع ذكر مايلي:

– كتاب بعنوان (اثر التكنولوجيا المستحدثة على القانون الدولي العام) لصاحبه الدكتور محمد سعادي يتناول المؤلف في الفصل الثامن موضوع السيادة الرقميةSouveraineté numérique او تحديات الانترنت لمبدأ سيادة الدولة في القانون الدولي العام عالج فيه فكرة التحول في مفهوم السيادة بعد ظهور المستحدثات التكنولوجية، وإفراغها من محتواها مما دفع بالدول للمطالبة بسيادة رقمية على فضائها الالكتروني من اجل حماية امنها المعلوماتي،وذلك عن طريق المشاركة في إدارة الانترنت.

– كتاب بعنوان (السيبرانية هاجس العصر)للكاتبة الدكتورة منى الأشقر جبور، جاء فيه الفصل الخامس بعنوان الحرب السيبرانية تعرضت فيه المؤلفة لعدة محطات منها أدوات الحرب الالكترونية،منزلقات المواجهة والرد ،والتعاون لدرء المخاطر.

– كتاب بعنوان (الامن المعلوماتي وإدارة العلاقات الدولية) لمؤلفه عبد الوهاب جعيجع ،عالج فيه الكاتب إشكالية كيف يتم توظيف طرق وأدوات الاختراق الرقميPercée numérique على امن المعلومات في إدارة العلاقات الدولية وتعرض الكاتب في نهاية دراسته الى اهم نماذج الاختراق الرقمي للشبكة المعلوماتية Réseau d'information وتداعيات الاختراق على العلاقات الدولية.

– كتاب بعنوان (internet et le droit international) وهو عبارة على أعمال مؤتمر دولي rouen المنبثق عن الجمعية الفرنسية للقانون الدولي والمنشور في المؤلف الصادر عن دار النشر..... أين تطرقت هذه الأعمال لعدة مواضيع منها اتفاقية بودابست ،دليل تالين،الإرهاب الالكتروني،وموضوع الساعة التحكم في إدارة الانترنت.

انطلاقا من تزايد تداعيات الأفعال المجرمة الماسة بأمن المعلومات وحاجة الدول المتزايدة لتطوير تشريعات دولية لحماية البيانات والمعلومات التي تزداد أهميتها في حالة كون البيانات المراد حمايتها تتبع لجهات أمنية ،مما يتيح الفرصة للطرف الأخر بشن اعتداءات الكترونية Attaques électroniques تضرب باستقرار العلاقات الدولية ومن خلال ما لمسته كباحثة من الدراسات السابقة من وجود فجوة قانونية كبيرة في حماية المعلومات الالكترونية ولذلك يمكن صياغة **إشكالية الدراسة** في السؤال الرئيسي التالي:

إلى أي مدى يحتاج امن المعلومات الالكترونية لحماية قانونية دولية ؟ وخاصة ان المسالة تتعلق بالأمن والسلم الدوليين من اجل الحفاظ على استقرار العلاقات الدولية، وهل تنطبق القواعد القانونية الدولية التقليدية على ما افرزته تكنولوجيا المعلومات من انتهاكات جسيمة للبنى التحتية الرئيسية للدول؟ ام اننا ننتظر بروز تيار قانوني مستحدث يواكب حداثة الموقف ليوفر لنا بيئة معلوماتية آمنة .

وعليه ارتأينا أن تكون الإجابة على هذه الإشكالية وفق **المنهج التحليلي** والذي يعتبر أفضل منهج للقراءة التحليلية والتفسيرية للنصوص القانونية،**والمنهج الوصفي** لتوضيح علاقة امن المعلومات الالكترونية بالأمن والسلم الدوليين ،وأيضا من اجل تسليط الضوء على التوترات الدولية المصاحبة للاعتداءات الالكترونية .

وبناءا على ماتقدم فان خطة البحث التي انتهت إليها الدراسة ،وذلك بالتركيز على ماتتطلبه طبيعة الموضوع، أفردنا الدراسة في فصلين تسبقهما مقدمة .

جاء الفصل الأول بعنوان الإطار القانوني لأمن المعلومات الالكترونية في ضوء العلاقات الودية،وجاء الفصل الثاني بعنوان الإطار القانوني لأمن المعلومات الالكترونية في ضوء العلاقات غير الودية،وقد جاء في الفصل الأول ثلاث مباحث حيث تضمن المبحث الأول محاولة إيجاد إطار قانوني لأمن المعلومات الالكترونية ،والمبحث الثاني محاولة إثراء حماية امن المعلومات في إطار المنظمات الدولية والإقليمية،وتطرقنا في المبحث الثالث الى الدفاع عن السيادة الرقمية للدولة.

بينما يعالج الفصل الثاني من خلال المبحث الأول الهجمات الالكترونية وحضر استخدام القوة وفق المادة4/2 مع تكييف الدفاع الشرعي وفقا للمادة 51 من ميثاق الأمم المتحدة،وتضمن المبحث الثاني الحرب الالكترونية في القانون الدولي الإنساني،أما المبحث الثالث فقد خصصناه للبحث عن السلام السيبراني.

مع الاعتماد المتزايد في حياتنا اليومية على الأنظمة المعلوماتية و الأجهزة المتصلة بالشبكة العالمية للمعلومات و تشعب طبيعة هذه الأجهزة من هواتف خلوية و أجهزة حاسوبية شخصية يزداد عدد المتصلين بالفضاء السيبراني[1] و يزداد عدد احتمالات الاعتداءات و الجريمة فقد أشار تقرير صادر عن ماكينزي [2]إلى توقع زيادة المعلومات الرقمية بمعدل 44% خلال الأعوام الممتدة من 2009 الى 2020.

و تصدر الإخطار و التهديدات السيبرانية عن أعمال قصديه كالاختراقات و الاعتداءات و أعمال غير قصديه كالإهمال و قلة الوعي. و يمكن توزيع الأخطار في الفضاء السيبراني انطلاقا من أهدافها بين ما يطال الدول و ما يطال الأشخاص و يندرج في إطار الفئة الأولى التي هي محل دراستنا كل ما يعرض الأمن الوطني و العسكري و الاقتصادي و الاجتماعي و يهدد البيئة التحتية و الحرجة للدولة و أسواق المال و القطاعات المصرفية و السلم الدولي و المنشآت النووية و المؤسسات الصحية و قطاعات النقل بكل أنواعها و الاعتماد المتزايد للدول على الاستخدام الواسع للتقنيات قد يعرضها لأخطار قد تصل إلى تقويض سيادة الدولة.

و في غياب الأمن القانوني أو حتى في تناقض و تنازع الأنظمة القانونية مع انعدام التعاون بين الدول أو حتى مع وجود تعاون لا يضمن ملاحقة فعالة تتلاءم و طبيعة الأعمال و الجرائم الاعتداءات السيبرانية العابرة للحدود و الأنظمة القانونية [3] .

و وعيا من الدول بهذا الوضع الحرج و سعيا وراء توفير بيئة معلوماتية آمنة ، بات لزاما عليها إيجاد الأطر التشريعية و التنظيمية المناسبة لتعزيز الثقة في الفضاء الالكتروني و تعميم ثقافة الأمن

---

[1] الفضاء السيبراني:يعرف المصطلح على أنه التعامل مع العالم من خلال شبكة إلكترونية لها استقلاليتها من الداخل وتقوم بنيتها الأساسية على التقنيات الحديثة وهو أيضا أنظمة التعامل مع الحاسوب .....للمزيد اطلع على الرابط: https://seconf.wordpress.com

[2] ماكينزي: هي شركة رائدة في مجال استشارات الأعمال، وتشتهر الشركة بالعديد من الأعمال الاستشارية والدراسات الأكاديمية المتميزة وتقدم الحلول الاستشارية للشركات والحكومات على السواء .تأسست الشركة في 1926 ويَعمل لديها ما يزيد على 9,000 مستشار في كافة المجالات الإدارية. اشتهرت منذ العام 1996 باستقطاب أفضل خريجي درجات ماجستير إدارة الأعمال ..... للمزيد اطلع على https://ar.wikipedia.org

3 د. منى جبور، السيبرانية هاجس العصر ، موقع المركز العربي للبحوث القانونية و القضائية بجامعة الدول العربية، مجلس وزراء العدل العرب تم الاطلاع بتاريخ 2017/12/23، على ساعة 12:00على موقع www .carjj.org

المعلوماتي و تحديد المسؤوليات و قواعد ردع الاعتداءات و الجرائم و إنزال العقوبات الخاصة بها في حال حدوثها .

و لقد أثبتت الدراسات المختلفة الصادرة عن المنظمات الدولية مثل الاتحاد الدولي للاتصالات[1] و مكتب الأمم المتحدة المعني بالمخدرات و الجريمة و اللذين وقعا مذكرة تفاهم لتنسيق المساعدة في مجال الأمن ألمعلوماتي ، بحيث نلمس انه أصبح من ضروري الاعتماد على الاتفاقيات بين الدول بشان الأمن المعلومات الالكترونية، إذ تشكل المعاهدات لاسيما المتعددة الأطراف مصدرا أساسيا إن لم يكن المصدر الأساسي لقواعد القانون الدولي و من خلال ما سبق سنتطرق في هذا الفصل لدراسة قانونية تحليلية للاتفاقية الأوروبية (اتفاقية بودابيست2001) و القرارات الصادرة عن مجلس الأمن بخصوص ظاهرة الإرهاب الإلكتروني كجريمة من مجموع الجرائم المستحدثة التي تمس بالدرجة الأولى الأمن و السلم الدوليين و كيف أنها كانت موضوع للتجريم في قرارات مجلس الأمن، هذا في المبحث الأول، و في المبحث الثاني سنتطرق للمساعي الدولية والإقليمية في مجال حماية امن المعلومات و توفير بيئة الكترونية آمنة .

[1]الاتحاد الدولي للاتصالات: أو الاتحاد الدولي للمواصلات السلكية واللاسلكية بالإنجليزية International Telecommunication Unionهو ثاني أقدم تنظيم عالمي ما زال موجوداً (الأقدم كان –اللجنة المركزية للملاحة في نهر الراين–) يعمل على تقييس وضبط الراديو والاتصال عن بعد، وجدت في بادئ الأمر باسم "الاتحاد الدولي للتلغراف" بباريس في 17 أيار 1865، مهمتها الرئيسية تضمين التقييس، تقسيم طيف الراديو، وتنظيم ترتيب وصل المشتركين بالشبكة العامة بين الدول المختلفة للسماح بالمكالمات الهاتفية الدولية، أخذا بعين الاعتبار تنفيذ الاتصال عن بعد كوظيفة مشابهة للوظيفة التي يقوم بها التحاد البريدي العام UPU لإنجاز الخدمات البريدية. وهي واحدة من الوكالات الخاصة (specialized agencies)التابعة للأمم المتحدة. يقع المركز الرئيسي للاتحاد في جنيف بسويسرا بجانب مقر الأمم المتحدة هناك.....للمزيد اطلع على الرابط: Mhttps://ar.wikipedia.org/wik

المبحث الأول:محاولة إيجاد إطار قانوني لأمن المعلومات الالكترونية.

لا تخضع الجريمة المعلوماتية لنظام الحدود الجغرافية للدول و حتى القارات فعن طريق التطور في تكنولوجيا الحواسيب و الاتصالات يمكن لمستخدم شبكة الانترنت[1] أن يكون في تونس مثلا و يرتكب جريمة إتلاف المستندات الالكترونية في نيويورك أو طوكيو أو في أي مكان في المعمورة و من اجل القضاء على هذا النوع من الجرائم الماسة و بالدرجة الأولى لأمن الدول و استقرارها كان لابد من تحقيق قاعدة قانونية وهي " ازدواج التجريم" بمعنى أن تكون الجريمة معاقبا عليها في القوانين الوطنية الداخلية التي يتواجد فيها الجاني و أيضا في الدولة التي يتواجد فيها المجني عليه .و هذا لا يأتي الا عن طريق تكاتف الجهود الدولية من اجل إثراء التعاون الدولي و الإقليمي بموجب اتفاقيات تعدها الأمم المتحدة و المنظمات الدولية و الإقليمية و تشرف على تنفيذها.

كما لعبت قرارات مجلس الأمن الدولي دورا فعالا و مهما في مجال إرساء قواعد قانونية لمواجهة هذا النوع المستحدث من الجرائم و التي تعد من اخطر الأفعال الماسة بأمن و سلامة الدول في مجال العلاقات الدولية

المطلب الأول: تجريم المساس بامن المعلومات في القانون الدولي الاتفاقي

من احدث الاتفاقيات الدولية الإقليمية في الوقت الراهن هي اتفاقية بودابست الخاصة بجرائم تقنية المعلومات الموقعة في بودابست بالمجر سنة 2001 .

تتكون الاتفاقية من مقدمة و أربعة فصول توضح أهداف الاتفاقية و منطلقاتها و مرجعياتها السابقة و ما تقوم عليه من جهود إرشادية و توجيهية و تدابير إقليمية و دولية، و تعطي المصطلحات الأساسية و تعالج النصوص الموضوعية لجرائم الحاسوب، و توضح القواعد الإجرائية و جهات الاختصاص المتعلقة بتطبيقها، و كذا المبادئ العامة و النصوص الخاصة بالتعاون الدولي في مكافحة الظاهرة.[2]

---

[1] شبكة الانترنت:مصطلح الانترنت انجليزي الاصل مختصر ومركب من شقين الاول يمثل الحروف الاولى لكلمة International.وترجمتها دولي اما الشق الثاني Net كذلك مأخوذ من الحروف الاولى لكلمة Network و ترجمتها شبكة عمل، و بجمع المختصرات يتكون المصطلح الذي يعني الشبكة العالمية للمعلومات المشار اليها بالاحرف www و التي تعني word wid web اي الشبكة الدولية الالكترونية المتعددة الابعاد و الخدمات....للمزيد اطلع على : ملياني عبد الوهاب، امن المعلومات في بيئة الاعمال الالكترونية، رسالة لنيل شهادة الدكتوراه في القانون العام، كلية الحقوق و العلوم السياسية جامعة ابي بكر بالقايد، تلمسان _الجزائر_، 2017/2016

[2] د/ رائد العدوان، المعالجة الدولية لقضايا الإرهاب الالكتروني، جامعة نايف العربية لعلوم الامنية، الرياض، 2013،مقال تم الاطلاع عليه بتاريخ 2017/1/18، الساعة 12:00، على الرابط: https//repository.nauss.edu.sa

كما كان من أهداف الاتفاقية تسليط الضوء على المخاطر الخاصة باحتمال استخدام شبكات الكمبيوتر والمعلومات الالكترونية في ارتكاب جرائم يعاقب عليها القانون واحتمال تخزين الأدلة المتعلقة بمثل هذه الجرائم ونقلها عبر الشبكات، ومن الضروريات التي أدت إلى حتمية اللجوء إلي هذه الاتفاقية هو عدم كفاية التشريعات الوطنية التي تتصدى لهذه الجرائم المستحدثة ،وأيضا غياب اتفاقيات دولية تعالج الإجرام المعلوماتي وضعف البنى التحتية المعلوماتية لدى دول العالم الثالث.[1]

في هذا المطلب سنحاول إعطاء لمحة خاصة لخطورة الآثار المترتبة عن الأعمال الإجرامية الماسة بأمن المعلومات الالكترونية و تداعياتها على امن و استقرار الدول هذا من خلال **الفرع الأول** و أحكام وصور الأفعال المجرمة الماسة بأمن المعلومات في الاتفاقيات الإقليمية **الفرع الثاني** و التعاون الدولي من اجل حماية امن المعلومات الالكترونية في الاتفاقيات محل الدراسةهذا في **الفرع الثالث**.

الفرع الأول: خطورة المساس بامن المعلومات في الممارسة الدولية.

استغلت العديد من الجماعات المتطرفة الطبيعة الاتصالية للانترنت من اجل بث معتقداتها و أفكارها. بل تعداه الأمر إلى ممارسات تهدد امن الدولة المعتدى عليها خاصة المتمثلة في الإرهاب و الجريمة المنظمة اللذان أخذا معنى أخر باستعمال الانترنت، بل الأخطر من ذلك أتاحت الانترنت لكثير من الدول ممارسة التجسس الالكتروني على دول أخرى و ذلك بالاطلاع على مختلف الأسرار العسكرية و الاقتصادية لهذه الأخيرة[2].

فالدخول غير المشروع هو الجريمة الأساسية التي تؤدي إلى التهديد أو الاعتداء على امن النظم و البيانات المعلوماتية ، حيث يتخذ الدخول غير المصرح به شكل القرصنة ، فيتضمن التسلل إلى السلامة و إلى جزء من نظام المعلومات كالجهاز و المكونات و البيانات المخزنة.[3]

---

[1] مصطفى بن عصام نعوس ،التنظيم القانوني الدولي للانترنت ،رسالة لنيل درجة الدكتوراه في الحقوق ،كلية الحقوق،قسم القانون الدولي،جامعة حلب،سوريا،2013.

[2] سمية مزغيش، جرائم المساس بأمن المعلوماتية، مذكرة مكملة من متطلبات نيل شهادة الماستر في الحقوق تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة،الجزائر، 2010، ص 32.

[3] د/ محمد سعادي، أثر التكنولوجيا المستحدثة على القانون الدولي العام، دار الجامعة الجديدة،عمان، بدون طبعة، 2014، ص 223.

كما أن الاعتراض غير المشروع يعتبر انتهاك حق احترام الاتصالات و قد يكون على شكل تصنت او تسجيلات المكالمات و المحادثات السلكية و اللاسلكية بين الأشخاص.[1] و عادة ما تمس عملية التصنت كبار المسؤولين و قادة الدول و رؤساءها و يتم ذلك عن طريق وسائل تقنية جد متطورة.

و يسجل لنا التاريخ المعاصر نماذج بشأن الأفعال المجرمة الماسة بأمن المعلومات الالكترونية على المستوى الدولي وقد اخترنا بعضا مما ذكره المختصون في هذا الشأن:

اولا : قضية ديفيد بيس

وهوالهجوم الالكتروني الذي تعرض له المفاعل النووي الأمريكي ديفيد بيس david besse لتوليد الطاقة الكهربائية في أوهايو في 2003 بفعل أنظمة اختراق و تعطيل لشبكات السيطرة و التحكم الالكترونية في المفاعل نفسه، إذ صرح المسؤولين الأمريكيين انه لولا وجود وسائل الحماية الخاصة بإطفاء المفاعل ذاتيا لكانت الكارثة اكبر من أن يتوقف المفاعل عن العمل فقط بل يتعدى الأمر إلى انفجارها حيث يصعب تخيل الأضرار و الخسائر البشرية التي تنجم عن هذا الانفجار و ما تزال آثار هذا الهجوم الالكتروني إلى غاية الآن و التي تؤدي من فترة إلى أخرى بتوقف محطات توليد الطاقة الكهربائية النووية الأمريكية مرة أو مرتين منذ 2006.[2]

ثانيا: قضية المفاعل النووي الإيراني

في عام 2010 استهدفت دودة ستاكس نت[3] stuxnet و التي تعد بمثابة علامة فارقة في المجال الأمني حيث اعتبرها عديد من الخبراء أكثر البرامج الخبيثة تعقيدا على الإطلاق محولات التردد و التي تتحكم في سرعة أجهزة الطرد المركزية المستخدمة في عملية تخصيب اليورانيوم في إيران، و بعد أن تم اختراق محولات التردد قامت بالتحكم بسرعة أجهزة الطرد المركزية بحيث زادت في سرعتها إلى الحد الذي لا يلحق بها الضرر.

---

[1] د/ محمد سعادي، نفس المرجع، ص 223.

[2] A.P.Dr. Ahmad oubais al-fatlawi,cyber attacks:its concept and arising international resbonsibility in the light of contemporary international organization, مجلة المحقق الحلي للعلوم القانونية و السياسية، العدد الرابع ، السنة الثامنة ، 2016، ص 624

[3] ستاكس نت: هو دودة حاسوب تصيب نظام الويندوز ويُعتقد أنه من صنع الولايات المتحدة الأمريكية وإسرائيل ، تم اكتشافه أول في حزيران \ يونيو 2010 من قبل "فيروس بلوك أد وهي شركة أمن مقرها في روسيا البيضاء.... للمزيد اطلع على الرابط: https://ar.wikipedia.org

نتج عن هذا الهجوم أن أعلنت إيران بالفعل في نوفمبر 2010 أن أجهزة الطرد المركزية للمفاعل النووي قد تم تدميرها و تأخر افتتاح المفاعل النووي سنة كاملة على الموعد المحدد له و كلف هذا الهجوم الالكتروني على المنظومة المعلوماتية الإيرانية الحكومة خسائر تقدر بمليارات الدولارات في إصلاح ما أفسدته دودة ستاكس نت[1].

ثالثا: قضية التصنت على المكالمات الهاتفية

ومن النماذج الأخرى أيضا تشير معلومات إلى أن التصنت الذي تجريه الولايات المتحدة على الاتصالات الهاتفية و الجوالة في العالم تتخطى ملياري اتصال يوميا وان طاقة أنظمتها تتخطى قدرة التصنت على 2,5 مليار اتصال يوميا كما قامت وكالة الأمن القومي الأمريكي و من خلال سفارة واشنطن في برلين بأعمال تجسس منظمة واسعة المدى، بدأت بالتصنت على هاتف المستشارة الألمانية ذاتها منذ عام 2002 حتى عام 2010 و أن المكالمات الهاتفية التي أجرتها من هاتفها تم تسجيلها طوال هذه المدة.

كردة فعل أعلنت ألمانيا و فرنسا بدء مفاوضات مع الطرف الأمريكي من اجل حظر عمليات التجسس عن طريق إبرام اتفاقيات بين الدول الثلاث حيث تكون هذه الاتفاقيات ملزمة لجميع الأطراف.[2]

رابعا: قضية شركة ارامكو

ان مسلسل الاعتداءات لم ينتهي بل تكرر من جديد على شركة ارامكوا و هي شركة وطنية سعودية تعمل في مجال إنتاج و تصنيع و تسويق و تكرير النفط الخام و الغاز الطبيعي و المنتجات البترولية، و قد تعرضت في 2012/8/15 لهجوم الكتروني من خلال فيروس أطلق عليه اسم شامون shamoon، قام بمسح بيانات من شبكتها الالكترونية و وضع صورة العلم الأمريكي محترقا.

حيث حظي هذا الهجوم بأهمية كبيرة على الرغم من الهجمات المتكررة في العديد من الشركات على مستوى العالم بسبب أهميتها البالغة المتمثلة في كل من استحواذها على 10% من المعروض العالمي و تجاوز إنتاجها من النفط الخام 13 بالمائة من الإجمالي العالمي كما إن مبيعاتها تبلغ سنويا أكثر من 200 مليار دولار.

---

[1] Evelyne AKOTO, les cyberattaques étatiques constituent_elle des actes d'agression en vertu du droit international public ? :premiére partier .U OTTAWA, faculté du droit, 2014 /2015 ,p 17

[2] عبد الوهاب جعيجع، الأمن المعلوماتي وإدارة العلاقات الدولية ، دار الخلدونية،الجزائر، طبعة2017، ص145.

و علاوة على ذلك فقد وجهت أصابع الاتهام لإيران من طرف كل من الولايات المتحدة الأمريكية و السعودية حيث اعتبرته هذه الأخيرة تهديدا لأمنها من إيران و اعتبرته الولايات المتحدة الأمريكية تهديدا الكترونيا مباشرا على قطاع النفط و الذي يؤثر في السوق العالمية بشكل عام.

استغرقت ارامكوا حوالي أسبوعين لإصلاح ما أفسده الفيروس على مستوى شبكتها المعلوماتية من ضياع للبيانات و توقف المحطات عن العمل.

لقد لعب الهجوم الالكتروني على النظام ألمعلوماتي لشركة ارامكو دورا محوريا في توجيه أنظار العالم لخطورة الهجمات الالكترونية على الخدمات الهامة على مستوى العالم.[1]

أظهرت الهجمات السابق ذكرها أنماطا و أشكالا مختلفة لاستخدام الهجوم الالكتروني على البيئة المعلوماتية في تحقيق المصالح المختلفة، فقد كان لكل منها هدف مختلف حيث أظهرت هذه النماذج كيف يمكن أن تستخدم الهجمات لاختراق الأنظمة المعلوماتية للبنى التحتية الحساسة للدولة و قد يأتي الهجوم الالكتروني من اجل غرض التجسس للحصول على معلومات أمنية هامة أو قد يتم في بعض الأحيان اللجوء إلى الأسلحة الالكترونية لأهداف انتقامية.

الفرع الثاني: صور و أحكام تجريم المساس بأمن المعلومات في الاتفاقيات الاقليمية.

تعتبر الجرائم المعلوماتي، الماسة بأمن المعلومات من الجرائم المستحدثة التي افرزها التطور التكنولوجي الهائل، وهي من الجرائم التي تستهدف الكثير من القطاعات مما جعل تحديدها وتصنيفها يتميز بالصعوبة على عكس الجريمة التقليدية.

حيث اختلف الفقهاء في اعتماد المعيار المحدد و المصنف للجرائم الالكترونية فمنهم من يعتمد على الأسلوب المتبع في الجريمة و بعضهم يصنفها و يقسمها الى جرائم ترتكب على نظم الحاسوب و أخرى ترتكب بواسطته، و غيرهم يؤسس تقسيمه على تعدد محل الاعتداء و كذا الحق المعتدى عليه و أخيرا على أساس الجرائم الواقعة على امن الدولة، .[2]

[1] نوران شفيق،اثر التهديدات الالكترونية على العلاقات الدولية،المكتب العربي للمعارف، مصر، طبعة 2016، ص ص 162 163

[2] سمية مزغيش، نفس المرجع السابق، ص 25.

وتتميز جرائم تكنولوجيا المعلومات بعدد من الخصائص منها الخطورة البالغة و سهولة ارتكابها و صعوبة الإثبات كون الدليل الرقمي[1] هو الدليل الوحيد للإثبات إذ نجد أن هناك عدة مناهج اتبعت لمواجهة الإجرام الالكتروني فبعض التشريعات ركنت إلى النصوص العقابية التقليدية و لم تقم بتعديل قوانينها لتتناسب مع هذا النوع الجديد من الجرائم الماسة بأمن المعلومات و أما البعض الأخر من التشريعات فقد تنبه للطبيعة الخاصة لهذا النوع من الجرائم و اوجد نصوص عقابية خاصة تراعي الطبيعة المميزة للجرائم المعلوماتية.[2]

أولا: تجريم موسع في اتفاقية بودابست

إن اتفاقية بودابست 2001 هي المعاهدة الدولية الأولى التي تسعى إلى معالجة الجرائم المتعلقة بالكمبيوتر والانترنت عبر التنسيق بين القوانين الوطنية وقوانين الدول الأخرى.

تهدف الاتفاقية إلى توحيد عناصر القانون الجزائي المحلي مع الأحكام المتعلقة بالجرائم الالكترونية والى توفير الإجراءات القانونية اللازمة للتحري ،وأيضا تعيين نظام سريع وفعال للتعاون الدولي كما تتضمن الاتفاقية المبادئ العامة المتعلقة بالتعاون الدولي في المواضيع التالية:تسليم المجرمين ،المساعدة الدولية المتبادلة ،إعطاء المعلومات بصورة آلية، وإنشاء الولاية القضائية على أي جريمة، وأيضا لإجراءات المتعلقة بطلبات المساعدة في غياب الاتفاقيات الدولية.[3]

-1صور وأحكام الأفعال الماسة بسرية وسلامة وتوافر البيانات وأنظمة الكمبيوتر

حددتها الاتفاقية في النفاذ غير القانوني والاعتراض غير القانوني والتدخل في البيانات والتدخل في النظام وإساءة استعمال أو استخدام الأجهزة.

---

[1] الدليل الرقمي: يعرف بأنه معلومات يقبلها المنطق و العقل يعتمدها العلم، و يتم الحصول عليها بإجراءات قانونية و علمية لترجمة البيانات الحسابية المخزنة في أجهزة النظم المعلوماتية.....للمزيد اطلع على: ملياني عبد الوهاب،رسالة لنيل شهادة الدكتوراه في القانون العام، جامعة أبي بكر بلقايد، تلمسان كلية الحقوق و العلوم السياسية قسم الحقوق، 2017/2016

[2] خلف إدريس الحبابسة، الإرهاب الالكتروني، مقال منشور على موقع lawj mobile ،تم الاطلاع عليه بتاريخ 2018/2/3، الساعة 12:00، على الرابط–https://l.facebook.com

[3] د/جورج لبكي، المعاهدات الدولية للانترنت(حقائق وتحديات)،مقال تم الاطلاع عليه بتاريخ 2018/3/15 الساعة 12:00 على الرابط.https//wwwlebarmy gov Ib

تشمل عبارة النفاذ غير القانوني الجريمة الأساسية للتهديدات الخطيرة الموجهة ضد أمن أنظمة وبيانات الكمبيوتر (أي السرية والسلامة والتوفير).

إن الوسيلة الأكثر فعالية لمنع النفاذ غير المرخص بطبيعة الحال، هو إدخال وتطوير تدابير أمنية فعالة ويمكن للحظر الجنائي للنفاذ غير المرخص أن يوفر حماية إضافية للنظام و البيانات في حد ذاتها و في مرحلة مبكرة ضد المخاطر [1].

كما يعني حكم الاعتراض غير القانوني[2] L'interceptioest illegal . حماية الحق في خصوصية نقل البيانات وتمثل الجريمة نفس الإنهاك لخصوصية الاتصالات مثل التصنت والتسجيل التقليديين للمحادثات الهاتفية الشفوية بين الأشخاص وينطوي الاعتراض بواسطة وسائل فنية على التصنت على محتوى الاتصالات أو رصده أو مراقبته ، ولإلحاق المسؤولية الجنائية يجب ان يرتكب الإعراض غير المشروع عمدا وبدون حق [3]

أما تجريم التدخل في البيانات[4] Interférence avec les données الهدف منه توفير حماية بيانات الكمبيوتر وبرامج الكمبيوتر تكون مماثلة لتلك التي تتمتع بها الأشياء المادية ضد إلحاق الضرر المتعمد وتتمثل المصلحة القانونية المحمية في سلامة البيانات أو برامج الكمبيوتر المخزنة في حسن تشغيلها أو استخدامها بإتقان إلى ذلك يجب أن يكون الجاني قد تصرف عمدا .[5]

أما التدخل في النظام[6] Interférence dans le système يهدف هذا الحكم إلى تجريم العرقلة[7] العرقلة[7] المعتمدة للإستعمال المشروع لأنظمة الكمبيوتر

---

[1] التقرير التفسيري لاتفاقية الجريمة الالكترونية، سلسلة المعاهدات الأوروبية رقم 185، مجلس أوروبا،بودابست في 23نوفمبر 2001 ،ص9

[2] ينظر المادة 3 من اتفاقية بودابست .

[3] التقرير التفسيري ،نفس مرجع سابق،ص10 .

[4]ينظر المادة 4 من اتفاقية بودابست

[5] التقرير التفسيري ، مرجع سابق،ص11.

[6]ينظر المادة 5 من اتفاقية بودابست.

[7] العرقلة : يشير هذا المصطلح إلى الإجراءات التي تعترض التشغيل السليم لنظام الكمبيوتر و تتم هذه العرقلة عبر إدخال بيانات الكمبيوتر، نقلها، إتلافها، حذفها، تغييرها أو تدميرها .....للمزيد اطلع على التقرير التفسيري، مرجع سابق.

حيث يمكن أن يؤدي إرسال بريد إلكتروني غير مرغوب فيه لأغراض تجارية أو لأغراض أخرى إلى إزعاج المتلقي ، لاسيما عندما ترسل هذه الرسائل بكميات كبيرة أو بوتيرة عالية .

كما يجب أن تكون العرقلة L'obstruction بدون حق حتى يجرم هذا الفعل ، فضلا على ذلك يجب أن تكون العرقلة جسيمة لإنشاء عقوبات جنائية مع إختلاف كل دولة طرف في الإتفاقية من أجل تحديد سياسة العرقلة ، كما يجب ان ترتكب الجريمة عمدا بمعنى ان تكون لدى مرتكب الجريمة نية العرقلة الجسيمة.[1]

كما سبق وسميت جريمة إساءة إستخدام الأجهزة[2] في المسودات الأولى للإتفاقية(الأدوات غير القانونية) وإذا كان البعض يرى أن هذا العنوان أكثر دقة وتحتوي هذه الجريمة على نوعين من الأفعال وتشمل الإنتاج المتعمد أو بيع أو شراء أو إستخدام أو استيراد أو توزيع ....أو غير ذلك من الأدوات والوسائل توفير الأجهزة و كذلك الحيازة والتملك لأي عنصر أو أداء.[3]

2- صور و أحكام الأفعال الماسة أو المتصلة بالكمبيوتر:

وهي الجرائم التي تتعلق بالتزوير والإحتيال المتعلق بالكمبيوتر تجدر الإشارة إلى تشابه جرائم التزوير مع جرائم الإحتيال من حيث قيامها على تغيير الحقيقة ، غير أنهما تختلفان من زوايا متعددة ، أهمها ان جريمة تزوير المحررات لابد أن تقع على محرر ولا يشترط ذلك في جريمة الإحتيال[4]

التزوير[5] المتعمد بإستخدام جهاز الكمبيوتر و ذلك بإدخال أو تعديل أو حذف أو إخفاء بيانات الكمبيوتر على نحو يظهر البيانات غير اصلية وبغض النظر عما إذا كانت هذه البيانات مقروءة أو غير مقروءة يحق للدولة أن تشترك نية أو قصد الغش لقيام المسؤولية الجنائية[1]

---

[1] التقرير التفسيري، نفس المرجع السابق،ص12.

[2] ينظر المادة 6 من اتفاقية بودابست

[3] يونس عرب، قراءة في الاتجاهات التشريعية للجرائم الالكترونية مع بيان موقف الدول العربية و تجربة سلطنة عمان،مقال تم الاطلاع عليه بتاريخ 2018/1/18، على ساعة 12:00، على الرابط :http/www.arablow.org.

[4] دراسة بعنوان، صور الجرائم الالكترونية و اتجاهات تبوبها،تم الاطلاع عليها بتاريخ2018/1/20 ،على الرابط http/www.assakina.bom/bppk/.

[5] ينظر المادة 7 من اتفاقية بودابيست .

التزوير: تعد جريمة التزوير في المجال المعلوماتي من اخطر صور غش المعلوماتية و التي مع التطور التكنولوجي الهائل و ارتباط كم هائل من العمليات ذات الآثار القانونية الهامة و الخطيرة بالحاسب الآلي جعلها لايصدق عليها "وصف المكتوب" و قد اثار ذلك الشك حول دلالتها في الاثبات و لهذا كان التدخل التشريعي ذو اهمية بالغة... للمزيد اطلع على

أما الإحتيال[2] المتصل بالكمبيوتر[3] فإن مع وصول الثورة التكنلوجيا تضاعفت فرص إرتكاب جرائم إقتصادية مثل الإحتيال بما في ذلك الإحتيال على بطاقات الإئتمان ، وترمي هذه المادة إلى تجريم أي تلاعب غير مشروع أثناء معالجة البيانات بنية النقل غير المشروع للملكية ، ويجب أن يرتكب الجرم بدون حق كما يجب الحصول على المنفعة الإقتصادية دون حق ، كما يجب أن ترتكب الجريمة عمدا حتى تقوم المسؤولية الجنائية .[4]

3- صور و احكام الافعال الماسة بإنتهاك حق التأليف والنشر والحقوق المجاورة:

كل دولة طرف في الإتفاقية محل الدراسة ملزمة بتجريم الإنتهاكات المتعمدة على حق التأليف والنشر والحقوق ذات صلة [5]التي يشار إليها أحيانا بالحقوق المجاورة الناشئة عن الإتفاقات المدرجة في المادة 1/10 ، عندما تنتهك هذه الحقوق عن طريق نظام الكمبيوتر وعلى نطاق تجاري،وهي تشمل نسخ و تقليد البرامج و إعادة إنتاجها و تصنيعها دون ترخيص و استغلالها ماديا و الاعتداء على العلامة التجارية و براءة الاختراع حيث أن الغرض المباشر المحرك للاعتداء منصبا على قيمتها او ما تمثله.

ويجب أن ترتكب الجرائم ضد حق التأليف والنشر والحقوق ذات صلة عمدا من أجل تطبيق المسؤولية الجنائية.[6]

و من خلال نص هذه المادة يتبين أن الاتفاقية تهتم بتوفير الحماية الجنائية للملكية الفكرية في شكلين احدهما مباشر بالنص صراحة على الجرائم المتصلة بانتهاك حق المؤلف و الحقوق المتصلة به و ذلك في المادة 10، و الثاني مسألة حماية الملكية الفكرية بشكل غير مباشر و في نصوص موضوعية.[7]

"سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجيستير في العلوم الجنائية و علم الاجرام، جامعة ابو بكر بلقايد ، كلية الحقوق و العلوم السياسية، تلمسان ،الجزائر، 2011/2010 ، ص 103

[1] د/وليد طه، التنظيم التشريعي للجرائم الالكترونية في اتفاقية بودابست،2010 تم الاطلاع عليه بتاريخ 2018/1/20، على ساعة 12:00، على الرابط: http/www.fichier_pdf.f/.

[2] الاحتيال الالكتروني: يقوم على فكرة إعادة توجيه حركة مرور الإنترنت من أحد مواقع ويب الاليكتروني إلى موقع مختلف يشبهه تماماً لتتم عملية التسجيل بإدخال اسم المستخدم وكلمة المرور الخاص بالعميل في قاعدة البيانات الخاصة بالموقع الإلكتروني المزيف....للمزيد اطلع على الرابط:http://avb.s-oman.net

[3] ينظر المادة 8 من اتفاقية بودابست

[4] التقرير التفسيري ، مرجع سابق،ص14.

[5] ينظر المادة 10 اتفاقية بودابست .

[6] التقرير التفسيري ، مرجع سابق،ص17.

[7] د/ بن مكي نجاة،السياسة الجنائية لمكافحة جرائم المعلوماتية،دار الخلدونية،الجزائر،2017، ص 127.

4- صور وأحكام إضافية لأفعال الاشتراك بالجرائم المعلوماتية في الاتفاقية

تتمثل في المحاولة والمساعدة أو التحريض[1] Incitation تهدف هذه المادة إلى إنشاء جرائم إضافية تتعلق بمحاولة إرتكاب الجرائم المحددة في الإتفاقية اوالمساعدة في إرتكابها أو التحريض على إرتكابها[2] وقد أوجبت الإتفاقية على الدول الأعضاء إتخاذ التدابير التشريعية للنص على قيام المسؤولية الجنائية لهذه الأفعال وذلك بغرض إيجاد رادع عام لما لهذه الجرائم من تأثير شديد على إقتصاديات الدول وكذلك النص على مسؤولية الأشخاص المعنوية من قبل أي شخص يتصرف لمصلحته[3] **ويلاحظ** هنا وفقا للإتفاقية **إمتداد نطاق المساءلة الجنائية للشخصين الطبيعي والمعنوي** ، أما بالنسبة للعقوبات و التدابير فقد أوجبت الإتفاقية على الدول إقرار العقوبات الملائمة والفعالة لهذه الجرائم بما فيها العقوبات المانعة للحرية بالنسبة للأشخاص الطبيعية والغرامات المالية بالنسبة للشخص المعنوي[4]

و لايزال الخلاف لم ينتهي حول تقسيم طوائف جرائم الكمبيوتر و تصنيفها الأمر الذي حدا بمشرعي الاتفاقية أن يقوموا بعمل حصر مبدئي للأفعال المجرمة والماسة بأمن المعلومات في البيئة الإلكترونية التي لها تأثير مباشر على البيئة التقنية للدول ، مع وضعهم في الحسبان تطور المنظومة الآلية وإحتمالية تغير الجرائم في المستقبل ، فإن الإتفاقية وضعت هذه النصوص التجريمية تطبيقا لمبدأ الشرعية الجنائية الذي مفاده لاعقوبة ولا جريمة إلا بقانون .

ثانيا:تقدير التجريم في الاتفاقية العربية والإفريقية.

اكتسبت جرائم الحاسب الآلي طابع الجرائم الدولية على اعتبار ان البعض منها يشكل جرائم عابرة للحدود و إزاء ذلك كان لا بد من تكاثف الجهود الدولية من اجل مكافحة هذا النوع المستحدث من الجرائم اذ أصبحت تعبر الحدود لتلحق الضرر بعدة دول و مجتمعات مستغلة التطور الكبير للوسائل التقنية الحديثة

---

[1] ينظر المادة 11 من اتفاقية بودابست.

التحريض: هو حث و حض و دفع الغير إلى ارتكاب الجريمة و يستوي أن يكون جالبا إلى فكرة الجريمة لدى الغير أو مشجعا أو داعيا أو مروجا لها إذا كانت الفكرة موجودة لديه من قبل.... للمزيد اطلع على "د/ احمد رشاد سالم، التعاون الدولي و أثره في مكافحة الإرهاب، كلية التدريب قسم البرامج التدريبية الرياض، 2013 ، ص 34 .

[2] التقرير التفسيري ، مرجع سابق،ص19.

[3] د/ وليد طه، مرجع سابق.

[4] ليلى الجناني، فعالية القوانين الوطني و الدولية في مكافحة الجرائم السيبرانية،مقال منشور بتاريخ 2018/1/20 على موقع الحوار المتمدن، تم الاطلاع عليه بتاريخ 2018/2/30، على ساعة 12:00، على الرابط: . http/www.m.hewar.org

و على ما تقدم سنتناول بالدراسة ما جاء في الاتفاقيتين العربية والإفريقية لمكافحة الجرائم الالكترونية وسنتبع في ترتيب الدراسة الترتيب الزمني لصدورهما.

1-الاتفاقية العربية لمكافحة جرائم تقنية المعلومات:

رغبتا من الدول العربية في تعزيز التعاون فيما بينها لمكافحة جرائم تقنية المعلومات التي تهدد امنها و تأكيدا منها على ضرورة الحاجة الى تبني سياسة جنائية مشتركة تهدف الى حماية المجتمع العربي ضد جرائم تقنية المعلومات[1]، وافق مجلس وزراء الداخلية العرب و مجلس العدل العربي في اجتماعهما المشترك المنعقد بمقر الامانة العامة بجامعة الدول العربية بالقاهرة بتاريخ 2010/12/21 على إصدار **الاتفاقية العربية لجرائم تقنية المعلومات[2]**، حيث جاء في الفقرة ثالثة من الأحكام الختامية بأنها تسري (الاتفاقية) بعد مضي 30 يوما من تاريخ إيداع وثائق التصديق عليه او قبولها أو إقرارها من 7 دول عربية كما أجازة الفقرة السادسة من الأحكام الختامية لأية دولة من الدول الأطراف التي تبدي أي تحفظ ينطوي على مخالفة لنصوص هذه الاتفاقية كما تقترح الفقرة السابعة من نفس الأحكام على انه يجوز للدولة الطرف أن تقترح تعديل أي نص من نصوص هذه الاتفاقية، كما يمكن للدولة الطرف أن تنسحب من هذه الاتفاقية بناءا على طلب كتابي يرسل إلى الأمين العام لجامعة الدول العربيةّ.[3]

ركزت الاتفاقية في مادتها 3 على مجالات تطبيق هذه الاتفاقية[4] كما انفردت على نظيرتها (اتفاقية بودابست) في مادتها الرابعة بالتطرق إلى مبدأ المساواة في السيادة الإقليمية للدول و عدم التدخل في شؤونها الداخلية مجسدة بذلك مبادئ ميثاق الأمم المتحدة[5] و هذا يحسب لصالح الاتفاقية كما خصصت الفصل الثاني لحصر قائمة الجرائم الماسة بأمن المعلومات من المادة 6 حتى المادة 18 مضمنة في

---

[1] انظر الديباجة في الاتفاقية العربية لجرائم تقنية المعلومات

[2] للمزيد اطلع على نص الاتفاقية العربية لجرائم تقنية المعلومات

[3] الفقرة 3، 6، 7، من الاحكام الختامية في الاتفاقية العربية لجرائم تقنية المعلومات

[4] المادة 3 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (تنطبق هذه الاتفاقية ما لم ينص على خلاف ذلك، على جرائم تقنية المعلومات بهدف منعها و التحقيق فيها و ملاحقة مرتكبيها، و ذلك في احالات التالية:

- ارتكبت في اكثر من دولة
- ارتكبت في دولة و تم الاعداد و التخطيط لها او توجيهها او االشراف عليها في دولة او دول اخرى.
- ارتكبت في دولة و ضلعت في ارتكابها جماعة اجرامية منظمة تمارس انشطة في اكثر من دولة.
- ارتكب في دولة و كانت لها آثار شديدة في دولة او في دول اخرى.)

[5] المادة 4 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

مادتها 15 تحديد صور الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات و تجدر الإشارة إلى غياب هذا النوع من التجريم في اتفاقية بودابست بينما تطرقت في المواد 19 و 20 الى الشروع و الاشتراك في ارتكاب الجرائم و تحدثت في آخر الفصل عن المسؤولية الجنائية للأشخاص الطبيعية و المعنوية بصورة مقتضبة حيث جاء في نص المادة 20 (تلتزم كل دولة طرف، و مع مراعاة قانونها الداخلي، بترتيب المسؤولية الجزائية للأشخاص الاعتبارية عن الجرائم التي يرتكبها ممثلوها باسمها و لصالحها دون الإخلال بفرض العقوبة على الشخص الذي يرتكب الجريمة شخصيا).[1]

وجهت مجموعة من الانتقادات للاتفاقية نحصرها في:

- إن صياغة مواد التجريم احتوت على العديد من المصطلحات غير المتناسبة مع واقع تكنولوجيا المعلومات و الاتصالات
- نصت الفقرة الرابعة من المادة 15 على تجريم "نشر النعرات و الفتن و الاعتداء على الأديان و المعتقدات" هذه المادة يمكن استخدامها لتجريم أي رأي أو تعبير يمكنه أن يشكل اختلافا مع المعتقدات الدينية و الاجتماعية السائدة
- تم استخدام مصطلحي المصالح العليا للدولة و الجرائم السياسية حيث لم يتم وضع تعريف واضح لها ضمن الاتفاقية.[2]

2-اتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الالكتروني وحماية البيانات ذات الطابع الشخصي

افتقرت القارة السمراء منذ فترة طويلة إلى بنية قانونية لتعامل مع الجرائم الالكترونية،وهو مابدأ في التغير في يونيو من عام 2014 حين وقعت دول الاتحاد الإفريقي اتفاقية لأمن الكمبيوتر و حماية البيانات والتي قد تدفع الدول الأعضاء لسن تشريعات خاصة بأمن المعلومات.

حيث صرح المستشار السياسي في منظمة (أكسس) لحقوق الإنسان أن (الأمن الالكتروني يمثل مصدرا متزايد الأهمية لقلق دول الاتحاد الإفريقي ،نظرا لنمو استخدام الانترنت)[1]،وتجدر الإشارة إلى

[1] انظر الفصل الثاني من الاتفاقية العربية لجرائم تقنية المعلومات

[2] محمد الطاهر، تعليق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، مقال منشور على موقع حرية الفكر و التعبير تم الاطلاع عليه بتاريخ 2018/4/1 على الساعة 12:17 على الرابط: https://afteegypt.org

إن تطلع القارة الإفريقية ماهو الا استجابة للاحتياجات المتمثلة في وضع تشريعات متناسقة في مجال الأمن الالكتروني بالدول الأعضاء في الاتحاد الإفريقي كما ان هذه الاتفاقية تهدف إلى وضع آلية في كل دولة طرف ،مع مراعاة أفضل الممارسات المعترف بها على الصعيد الدولي ،مع الأخذ بعين الاعتبار أن الحماية الجنائية لمنظومة القيم لمجتمع المعلومات ضرورة حتمية تمليها اعتبارات أمنية،كما أن هذه الاتفاقية تهدف من حيث القانون الجنائي الموضوعي إلى تحديث أدوات قمع الجريمة الالكترونية من خلال وضع سياسات لاعتماد جرائم جديدة خاصة بتكنولوجيا المعلومات والاتصالات وموائمة نظام العقوبات الموجود فعليا في الدول الأعضاء مع المناخ التكنولوجي الحديث و بيئة تكنولوجيا المعلومات و الاتصالات[2].

الفرع الثالث: التعاون الدولي من أجل حماية امن المعلومات الالكترونية في الاتفاقيات محل الدراسة.

ومن اجل التطرق إلى التعاون الدولي[3] في الاتفاقيات محل الدراسة قسمنا هذا الفرع إلى:

أولا: تسليم المجرمين

ثانيا: المساعدة القضائية

اولا: تسليم المجرمين:

استقر الفقه الدولي على اعتبار تسليم المجرمين شكلا من أشكال التعاون الدولي في مكافحة الجريمة والمجرمين ،ويقوم تسليم المجرمين على أساس أن الدولة التي يتواجد على إقليمها المتهم بارتكاب احد الجرائم العابرة للحدود كالجرائم المعلوماتية تقوم بمحاكمته إذا كان تشريعها يسمح بذلك ،وإلا كان

---

[1] افريقيا تواجه مازقا بين مكافحة الجريمة الالكترونية وضمان حقوق الانسان،مقال تم الاطلاع عليه بتاريخ 2018/1/17 الساعة12:00 على الرابط:

[2]انظر الدباجة في تفاقية الاتحاد الافريقي بشان امن الفضاء الاليكتروني و حماية البيانات ذات الطابع الشخصي

[3]التعاون الدولي: يقصد به تبادل العون و المساعدة و تضافر الجهود المشتركة بين طرفين دوليين أو أكثر لتحقيق نفع او خدمة او مصلحة مشتركة في مجال التصدي لمخاطر و تهديدات الإجرام و ما يرتبط به من مجالات أخرى كمجال العدالة الجنائية، و مجال الأمن و التي قد تعرض الجهود الوطنية لملاحقة المجرمين..... للمزيد اطلع على د/ بن مكي نجاة، نفس المرجع السابق.

عليها تسليمه لمحاكمته بمعرفة دولة أخرى مختصة ،وتسليم المجرمين تنظمه الاتفاقيات الدولية الجماعية او الثنائية بين الدول.[1]

أسهب المشرع الأوروبي في وضع مواد و بنود تنظم مسالة تسليم المجرمين بين الدول الأطراف حيث جاء ذلك بالنسبة للاتفاقية الأوروبية في الباب الأول من الفصل الثالث في المادة 24 حيث تنص الفقرة الأولى من هذه المادة على أن الالتزام بالتسليم لا ينطبق إلا على المواد من 2 إلى 11 من الاتفاقية و التي يعاقب عليها بموجب قوانين الطرفين المعنيين بعقوبة سالبة للحرية لمدة أقصاها سنة واحدة على الأقل أو بعقوبة اشد[2].

بحيث تقضي الفقرة 7 من نفس المادة انه ينبغي على الأطراف إبلاغ الأمين العام لمجلس أوروبا باسم و عنوان السلطات المسؤولة عن تقديم أو تلقي طلبات التسليم ، و أن بنود هذه الاتفاقية تكون سارية المفعول في حالة غياب اتفاقية ثنائية بين الأطراف المعنية بالتسليم، كما تجدر الإشارة أن تعيين السلطة لا يستبعد إمكانية استخدام القنوات الدبلوماسية،[3]هذا ماجاءت به اتفاقية بودابست.

راعت الاتفاقية العربية في بنودها أثناء تنظيمها لموضوع التعاون الدولي و من خلال مادتها 21 التطرق إلى توضيح مسألة تسليم المجرمين كأحد ابرز مظاهر التعاون الدولي في القانون ألاتفاقي.[4]

بينما نظم الفصل الرابع من الاتفاقية التعاون القانوني و القضائي بين الدول الأطراف حيث جاء في المادة 30 تحديد الاختصاص إذ تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص عليها في الفصل الثاني و ذلك إذا ارتكبت الجريمة و كانت تمس احد المصالح العليا للدولة.

نصت الاتفاقية الإفريقية من خلال المادة 28 على التعاون الدولي حيث تطرقت إلى المواءمة الإقليمية لتدابير مكافحة الجريمة الاليكترونية مع احترام مبدأ المسؤولية الجنائية المزدوجة، و الملاحظ أن هذه الاتفاقية لم تتطرق بوضوح إلى مسألة تسليم المجرمين بين الدول الأطراف[5].

ثانيا: المساعدة القضائية:

[1] د/حسين بن سعيد الغافري ،نفس المرجع،ص16.

[2] الفقرة الاولى من المادة 24من اتفاقية بودابست.

[3] ينظرالفقرة 7 من المادة 24 من اتفاقية بودابست.

[4] انظر الفصل الرابع من الاتفاقية العربية لجرائم تقنية المعلومات

[5]انظر المادة 28 من اتفاقية الاتحاد الافريقي بشان امن الفضاء الاليكتروني و حماية البيانات ذات الطابع الشخصي

و تعرف المساعدة القضائية الدولية بأنها "**كل إجراء قضائي تقوم به دولة من شانه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم** " [1]

من الممكن أن يتأذى أشخاص أو يلحق ضرر جسيم بممتلكاتهم أن لم يتم جمع الأدلة بسرعة و في مثل هذه الحالات العاجلة يجب التسريع ليس فقط بالطلب، بل و كذلك بالرد لذلك تهدف المادة 25 من الاتفاقية إلى تيسير التعجيل بعملية الحصول على المساعدة المتبادلة بحيث لاتضيع المعلومات أو الأدلة.[2]

و جاءت الفقرة 5 من المادة المذكورة هي الأساس لتعريف ازدواجية التجريم لأغراض المساعدة المتبادلة و هي عندما يسمح لطرف متلقي الطلب باشتراط ازدواجية التجريم لتقديم المساعدة حيث تعتبر ازدواجية التجريم موجودة إذ كان السلوك الذي تنطوي عليه الجريمة التي تطلب المساعدة بشأنها تعتبر جريمة جنائية بموجب قوانين الطرف المتلقي للطلب، حتى و إن تم التصنيف من قبلها بان الجريمة ضمن فئة مختلفة أو استخدمت مصطلحات مختلفة لتسمية الجريمة،[3]

كما جاء ذلك في بنود الاتفاقية العربية لجرائم تقنية المعلومات حيث نصت المادة 32 على المساعدة المتبادلة مع شرط وجود مبدأ ازدواجية التجريم.[4]وعلى عكس اتفاقية بودابست لم توضح الاتفاقية العربية معنى التجريم المزدوج وهذا مايفتح الباب أمام التفسيرات المتباينة من طرف الدول المنضمة

أكدت في هذا الخصوص المادة 28 من الاتفاقية الإفريقية على ان الدول الأطراف التي ليس لديها اتفاقيات المساعدة المتبادلة في مجال الجريمة الاليكترونية تشجع على توقيع اتفاقيات المساعدة القانونية المتبادلة وفقا لمبدأ المسؤولية الجنائية المزدوجة كما أكدت الاتفاقية على تعزيز تبادل المعلومات و البيانات على نحو فعال ثنائي و متعدد الأطراف[5] ،و قد أجمعت الاتفاقيات على أن مظاهر التعاون تنحصر في:

---

[1] د/ حسين بن سعيد بن سيف الغافري، مرجع سابق،ص11.

[2] التقرير التفسيري،نفس المرجع السابق،ص42.

[3] ينظر الفقرة 5 من المادة 25 من اتفاقية بودابست.

[4] ينظر المادة 32 من الاتفاقية العربية.

[5] انظر المادة 28 من اتفاقية الاتحاد الافريقي بشان امن الفضاء الاليكتروني و حماية البيانات ذات الطابع الشخصي.

– يجب على الدول أن تقدم لبعضها البعض المعونة المتبادلة و ذلك بأكبر قدر ممكن لأغراض التحقيق و الإجراءات الخاصة بالجرائم الجنائية المتعلقة بنظم و بيانات الحاسب الآلي.[1]

– يجب على الدول أن تقبل و تستجيب إلى طلبات المعونة من خلال وسائل الاتصال السريعة

– كالفاكس والبريد الالكتروني بالقدر الذي يوفر للطرف الطالب مستوى من الأمن و المصداقية.[2]

– يجوز للدولة المدعى عليها أن ترفض طلب المعونة إذا ما توافرت لديها قناعة بان الالتزام بما ورد في الطلب قد يخل بسيادتها أو أمنها و نظامها العام أو إي من مصالحها الأساسية الأخرى.[3]

– أوجبت الاتفاقيات على الدول الأطراف تعيين نقطة اتصال لضمان توافر المساعدة الفورية بين الدول الأعضاء.[4]

_يجوز في حالة الاستعجال إرسال طلبات المعونة المتبادلة مباشرة إلى السلطات القضائية بما فيها النيابة العامة لدى الدولة المدعى عليها و في مثل هذه الحالة يجب إرسال نسخة من نفس الطلب إلى السلطة المركزية القائمة لدى الدولة المدعى عليها.[5]

على الرغم من أهمية هذه الاتفاقيات و الكثير من مظاهر التعاون الدولي البارز في المجال الالكتروني الذي تلى توقيعها، يمكن إرجاعه إلى ما وضعته هذه الاتفاقيات من الأسس والأطر للتعاون.

– يأتي الانتقاد الأول الموجه لاتفاقية بودابست من روسيا فعلى الرغم من انها عضو في المجلس الأوروبي إلا أنها رفضت الانضمام للدول الموقعة على الاتفاقية، بحيث ترجع روسيا الاعتراض إلى احد بنود الاتفاقية و الذي يقضي بإمكانية قيام سلطات التحقيق بالدخول بشكل فردي إلى الأجهزة الالكترونية الخاصة بالدول الأعضاء أو الوصول إلى ما تتضمنه من بيانات[6] ، و اعتبرت روسا ذلك مساسا و تعديا تعديا على سيادتها.

– اما الانتقاد الذي وجه للاتفاقية العربية فهو يخص الفصل الاول الذي تضمن مجموعة من الافعال اعتبرتها الاتفاقية تشكل جرما الا ان صياغة مواد التجريم احتوت على العديد من المصطلحات

---

[1] ينظر المادة 25 من اتفاقية بودابست.

[2] ينظر الى الفقرة 32/3 من الاتفاقية العربية.

[3] ينظر المادة 35 من الاتفاقية العربية

[4] انظر المادة 28 من اتفاقية الاتحاد الافريقي بشان امن الفضاء الاليكتروني و حماية البيانات ذات الطابع الشخصي.

[5] ينظر المادة 29 من اتفاقية بودابست.

[6] ينظر المادة 31 من اتفاقية بودابست.

غير المتناسبة مع واقع تكنولوجيا المعلومات و الاتصالات ،كما أنتقدت المادة 21 من الاتفاقية التي تشدد العقوبات على الجرائم التقليدية المرتكبة بواسطة تقنية المعلومات وهو تشديد غير مفهوم و غامض ولا يقترن فعليا على الضرر المترتب على الجريمة بقدر ارتباطه باداة الجريمة نفسها.

والملاحظ في مواد الاتفاقية هو التغييب الكامل لمسالة تسوية المنازعات على أهميته في تنظيم العلاقات بين الدول الأطراف[1] .

_نالت الاتفاقية الإفريقية جزءا من الانتقادات كان أولها تحديد الجهات القضائية في حالة النزاع بين الأطراف مستثنية محكمة العدل الدولية على عكس ما جاءت به اتفاقية بودابست انه في حالة اختلاف الأطراف يمكن الرجوع إلى المحكمة كجهة قضائية دولية و هذا العزوف عن اللجوء الى المحاكم الدولية من طرف الدول الإفريقية على غرار المحكمة الدولية الجنائية و التي لا نفسرها الا بوجود خلفيات سياسية كما ان المتصفح لبنود الاتفاقية الإفريقية يلاحظ دمج و خلط المواد الخاصة بتنظيم التجارة الاليكترونية و كان من الأحسن إنشاء اتفاقية خاصة بهذا الموضوع على حدا.

و على ضوء ما سبق دراسته من تجريم للأفعال الماسة بأمن المعلومات و المتصلة مباشرة بأمن و استقرار الدول و تداعيات التهديدات الأمنية على الساحة الدولية، يمكن طرح التساؤل التالي: ما هو دور ميثاق الأمم المتحدة كدستور عالمي لتنظيم العلاقات الدولية ؟ وماهو دور مجلس الأمن الدولي كراعي رسمي للأمن و السلم الدوليين في إطار مكافحة الإرهاب الالكتروني كصورة من اخطر صور الجرائم الالكترونية المستحدثة الماسة بأمن المعلومات؟ هذا ما سنتناوله في **المطلب الثاني**.

المطلب الثاني:التصدي للإرهاب الالكتروني كحماية لأمن المعلومات الالكترونية

لقد ترتب على الثورة الكبيرة والطفرة الهائلة التي جلبتها حضارة التقنية في عصر المعلومات بروز مصطلح الإرهاب الالكتروني (الإرهاب الرقمي) وشيوع استخدامه وزيادة خطورة الجرائم الإرهابية وتعقيدها سواء من حيث تسهيل الاتصال بين الجماعات الإرهابية وتنسيق عملياتها أو من حيث المساعدة على ابتكار أساليب وطرق إجرامية متقدمة[2]

[1] محمد الطاهر، نفس المرجع السابق.

[2] عبدا لله بن عبد العزيز بن فهد العجلان، بحث مقدم الى المؤتمر الدولي الاول "حماية امن المعلومات و الخصوصية في قانون الانترنت"،2008 تم الاطلاع عليه بتاريخ 2018/2/20، على ساعة 12:00، على الرابط: http://www.shaimaaatalla.com/vb

كما بات الإرهاب الالكتروني يمثل تهديدا واضحا للبنى التحتية لارتباطها بأجهزة الكمبيوتر وشبكة الانترنت وهذا ماجعلها عرضة للهجمات الالكترونية والإرهابية بصفة خاصة ،ومع ذلك فحتى الساعة لايوجد تعريف جامع مانع لمفهوم الإرهاب الالكتروني بصفة خاصة ،وان وجدت بعض التعريفات للإرهاب الالكتروني فهي مجرد اجتهادات لاغير.[1]

وتعتبر قضية وضع تعريف محدد ومتفق عليه لظاهرة الإرهاب واحدة من المشاكل بالغة الصعوبة ومستعصية الحل ولا يعود ذلك لغموض المصطلح بل يعود الى الاختلاف والتباين الشديدين في وجهات النظر والإرادات السياسية تبعا لاختلاف الأيديولوجيات والمصالح فما يراه البعض إرهابا يراه آخرون عملا مشروعا،وبالرغم من ذلك فقد كانت هناك العديد من المحاولات الإقليمية والدولية لإعطاء الإرهاب الالكتروني تعريفا[2] ،وعلي سبيل المثال في الموسوعة الالكترونية جرى تعريف الإرهاب الرقمي Terrorisme numérique بأنه "**استخدام التقنيات الرقمية Technologies numériques لاخافة واخضاع الاخرين او هو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية او عرقية او دينية**".[1]

الفرع الأول: الإرهاب الرقمي في ضوء ميثاق الأمم المتحدة

على الرغم من أن ميثاق الأمم المتحدة لم ينص صراحة على تجريم استخدام المعلومات كأداة إرهابية ضمن إطار مايعرف بالإرهاب الالكتروني ،إلا أن روح الميثاق تتفق مع تجريم استخدامه بوصفه انتهاكا لما ورد في الميثاق. وكما سبق الذكر فان منظمة الأمم المتحدة لم تعالج حتى الآن أية حالة يمكن الاستناد إليها من تعريف الإرهاب الالكتروني،وإمكانية التعامل معه من الناحية التجريمية والقانونية فالقانون الدولي لم يعطي تعريفا واضحا أو منهجا معينا للتعامل مع هذا النوع المستحدث من الإرهاب.

غير أن الأمين العام للأمم المتحدة ،بان كيمون أكد على ان الانترنت هي المثال الأهم على كيفية عمل الإرهابيين بطريقة عابرة للحدود الوطنية ،وقد ورد هذا التأكيد في مقدمة تقرير صادر عن مكتب الأمم المتحدة المعني بالمخدرات والجريمة صادر في عام 2012 تحت عنوان **استخدام الانترنت لأغراض**

---

[1] علي مطر، الارهاب الالكتروني في القانون الدولي ،مقال منشور على موقع السكينة ،تم الاطلاع عليه بتاريخ 2018/2/17،على الرابط:https /www.assakina.com

[2] د/مايا حسن ملا خاطر،الإطار القانوني لجريمة الارهاب الالكتروني،كلية الحقوق،جامعة دار العلوم،المملكة العربية السعودية

إرهابية ،ويتألف هذا التقرير من 158 صفحة توزعت على ثماني عناوين انتهت بالتأكيد على التعاون الدولي من اجل مواجهة جرائم الإرهاب الالكتروني.[2]

وبشكل عام فان خرق السيادة الوطنية لأية دولة ،والحصول على معلومات استخباراتية ،وتجنيد العملاء وغيرها من الأنواع المستخدمة محرمة ،حيث أن المادة **الثانية في فقرتها الرابعة** من ميثاق الأمم المتحدة تنص على تحريم استخدام القوة في العلاقات الدولية.[3]

كما أن الفقرة 7من نفس المادة السابقة تقول "**ليس في هذا الميثاق ما يسوغ للأمم المتحدة ان تتدخل في الشؤون التي تكون من صميم السلطان الداخلي لدولة ما**"،و هذا المبدأ لا يخل بتطبيق تدابير القمع الواردة في الفصل السابع الذي يقع ضمن طائلة المادة 39 من ميثاق الأمم المتحدة و التي تنص : "**يقرر مجلس الأمن ما إذا كان قد وقع تهديد للسلم أو الإخلال به او كان ما وقع عملا من أعمال العدوان**"[4].

الفرع الثاني: الإرهاب الرقمي في ضوء قرارات مجلس الأمن

في ظل تصاعد وتيرة التهديدات الإرهابية التي تنطلق من الفضاء الالكتروني Cyberespace و مخاطرها على الأفراد و المجتمعات و الدول سواء لجهة التنسيق بين الجماعات الإرهابية بهدف تبادل المعلومات أو التخطيط لتنفيذ جرائمها الإرهابية، أو لجهة نشر الخطاب المتطرف بهدف التجنيد و التحريض على ارتكاب أعمال إرهابية أو الإشادة بها، أو لجهة بث خطابات الكراهية و العنف و التمييز على أساس ديني أو قومي أو عرقي أو طائفي.[5] لقد اصدر مجلس الأمن الدولي حزمة من القرارات التي جاءت لمواجهة هذا النوع المستحدث من الجرائم المعلوماتية الماسة بأمن المعلومات الالكترونية و التي تغذت من التطور التكنولوجي المتواصل و تبلورت و تجسدت في اخطر حالاتها مشكلة الإرهاب الرقمي (الالكتروني).

---

[1] أ م د/ سامر مؤيد عبد اللطيف، م د/ نورى رشيد الشافعي، دور المنظمات الدولية في مكافحة الإرهاب الرقمي، وزارة التعليم العالي و البحث العلمي جامعة كربلاء، 2016، تم الاطلاع عليه في 2018/3/15، على ساعة 12:00، على الرابط:elearning.uokerbala.edu.iq

[2] د/منى جبور،نفس المرجع السابق،ص94 .

[3] علي مطر،مرجع سابق.

[4] أ م د/ سامر مؤيد عبد اللطيف، م د/ نورى رشيد الشافعي، نفس المرجع ص 18.

[5] الفقرة 1 من إعلان ابوظبي حول تجريم الإرهاب الالكتروني من 15 إلى 16 ماي 2017، ص 2 .

بحيث صدر قرار للمجلس في 2003 و الذي أعرب فيه على "**انه أصبح من السهل في عالم يزداد عولمة أن يشغل الإرهابيون التكنولوجيا و الاتصالات و المتطورة لتحقيق أهدافهم الإجرامية**"[1]، و تزامن صدور هذا القرار بدخول حيز النفاذ الاتفاقية الأوروبية للتجريم الالكتروني و هذا ان دل على شيء فهو يدل على تأخر مجلس الأمن في معالجة القضايا الدولية الماسة بالأمن و السلم الدوليين.

كما أصبح الإرهاب يوظف الانترنت لتجنيد و تدريب العناصر الإرهابية و ذلك من خلال بث الخطابات المضللة بطرق و أساليب ذكية و مغرية، و ايضا استخدام أساليب تحريضية ضد الحكومات و سياساتها و تمنح شبكة الانترنيت تأمين عمليات الاتصال و التخفي و ذلك عن طريق مختلف المواقع الالكترونية كما يعمل على تجنيدهم و تحريضهم نفسيا لتنفيذ عمليات إرهابية مستقبلا.[2]

وكانت دراسات حديثة قد أظهرت لجوء الارهابيين الى تجنيد الشباب التونسي للقتال في سوريا الى جانب داعش وجبهة النصرة عبر استهداف شريحة معينة من الشباب تشكوا من مشاكل اجتماعية واقتصادية او نفسية ،ولا تبقى البدان الغربية بعيدة عن مخاطر تجنيد الشباب على المواقع الالكترونية ،اذ تنشر الصحف والمواقع الاعلامية المختلفة اخبار تجنيد الشباب في بلدان اوروبا وامريكا واستراليا وتتم هذه العملية غالبا عبر مواقع مخصصة للقتال والقتل.[3]

وعلى ذلك جاءت القرارات اللاحقة لتستكمل نهج مجلس الأمن في مكافحة استعمال التكنولوجيا لأغراض إرهابية معربا على قلقه من خلال القرار رقم 1963 عن ازدياد استخدام الإرهابيين في مجتمع معولم للتكنولوجيا الجديدة للمعلومات و الاتصالات و بخاصة الانترنيت لأغراض التجنيد و التحريض و تمويل الأنشطة[4] و محاولة المنظمات الإرهابية استغلال الشبكة إلى أوسع الحدود، مع ما تتميز به الجريمة الإرهابية الالكترونية من خصائص التي تتمثل فيما يلي:

- أنها جريمة تتسم بالخطورة البالغة حيث تؤدي إلى إحداث خسائر كبيرة و الى تهديد الدول و تهديد أمنها.
- صعوبة اكتشاف هذه الجرائم حيث لا يوجد دليل مادي Preuve matérielle يتركه الجاني.

---

[1] ينظر قرار مجلس الأمن رقم 1456 سنة 2003

[2] د/ نصير العرباوي، د/ فاتح النور رحموني، الجريمة الإرهابية الالكترونية، مقال تم الاطلاع عليه بتارخ 2018/2/10، الساعة 12:00، على الرابط:https//www asjp ceist dz articl

[3] د/منى جبور،نفس المرجع السابق ،ص 89 .

[4] ينظر قرار مجلس الأمن، رقم 1963، سنة 2010

– إن مرتكبي الإرهاب الالكتروني هم في العادة أشخاص محترفون و ذوي خبرة في مجال تكنولوجيا المعلومات.[1]

و هذه الخصائص المميزة للجريمة المعلوماتية في نموذجها الإرهابي ترفع من وتيرة خطورتها مما جعل المجلس يواصل إصدار قراراته في هذا المجال معربا عن تصميمه بربط كل من يقوم بتمويل او تسليح أو تجنيد الأشخاص بتنظيم القاعدة[2] و خاصة إذا كان ذلك من خلال تكنولوجيا المعلومات كشبكة الانترنيت.[3]

و بما أن المنظمات الإرهابية تعتمد في نشر أفكارها و مبادئها على أسلوب الخطاب الموجه إلى فئات معينة من اجل اختلاق مقولات منحرفة تستند إلى تحريف الدين و تشويه الحقيقة لتبرير أعمال العنف مستعملين في كل ذلك وسائل التكنولوجيا و الاتصالات بما في ذلك وسائل التواصل الاجتماعي مثل غرف الدردشة[4] Salons de chat و ما تسببه في انتشار لظاهرة الإرهاب الالكتروني و تسهيل تخاطب هذه الجماعات و تواصلها المستمر، و حرصا على أن تكون قرارات مجلس الأمن مواكبة لكل التطورات و المستجدات الحاصلة في مجال استعمال الإرهابيين لوسائل تكنولوجيا المعلومات جاء قراره في فيفري 2017 ليؤكد قلقه من جديد على خدمة التكنولوجيا الحديثة للجريمة الإرهابية.[5]

ويتضح مما سبق عرضه من قرارات لمجلس الامن انها تعاني من عدم وجود اي تعريف او دلالة للإرهاب الالكتروني بشكله العالمي العابر للحدود ،وبالتالي فمن غير المنطق القول بان ذلك يشكل جريمة من الناحية القانونية ،ذلك ان القاعدة القانونية تقول :بانه لا جريمة ولا عقوبة بغير نص وللتغلب على هذا العيب فلا بد من الوصول لتعريف متفق عليه للإرهاب الالكتروني في المجتمع الدولي.[6]

---

[1] خلف ادريس الحبابسة، مرجع سابق

[2] **تنظيم القاعدة:** هو تنظيم سلفي مسلح أنشأ في أفغانستان من قبل عبدالله يوسف عزام في سنة 1988 وهذا التنظيم مدرج في قائمة المنظمات الإرهابية لدى مجلس الأمن الدولي...للمزيد اطلع على الرابط: https://www.marefa.org

[3] ينظر قرار مجلس الامن رقم 2178، سنة 2014

[4] **غرف الدردشة:** يعني هذا المصطلح أي تكنولوجيا تتراوح بين الدردشة عبر الإنترنت والرسائل الفورية عن طريق الايمايلات والمنتديات الموجودة علي شبكة الإنترنت.....للمزيد اطلع على الرابط: https://ar.wikipedia.org

[5] ينظر قرار مجلس الأمن رقم 2354، سنة 2017

[6] جمال زايد هلال ابو عين ،الإرهاب وأحكام القانون الدولي ،عالم الكتب الحديث للنشر والتوزيع ، الطبعة الاولى، سنة 2009 ، ص227 .

الفرع الثالث: توصيات مؤتمر ابو ظبي في مجال مكافحة الارهاب الالكتروني

باتت جرائم الإرهاب الالكتروني هاجسا يشغل الدول التي أصبحت عرضة لهجمات الإرهابيين والجماعات المتطرفة عبر الانترنيت حيث أضحت تمارس نشاطاتها من أي مكان في العالم، و في أي لحظة و قد سعت الدول إلى اتخاذ التدابير و الإجراءات اللازمة لمواجهة الإرهاب الالكتروني، إلا أن هذه الجهود قليلة و مازالت بحاجة إلى المزيد من البحوث و الدراسات و التنسيق و التشريع و التنظيم، كما يجب تشخيص الظاهرة و دراستها من مختلف الجوانب و الرؤى لما لها من أخطار على امن البيئة المعلوماتية الماسة بأمن الدول و استقرارها.

و كمحاولة لإرساء قواعد قانونية تنظم و تأطر الجريمة الإرهابية عن طريق تكنولوجيا الاتصالات لتوفير حماية كافية لأمن المعلومات الالكترونية.

عقد مؤتمر أبو ظبي في الفترة ما بين 15 و 16 ماي 2017 المعنون بتجريم الإرهاب الالكتروني و ما يحتويه هذا المؤتمر من جدول أعمال و أوراق عمل تتطرق إلى وضع إطار قانوني دولي محدد لقواعد و أسس التعاون الجنائي مع الأعمال الإرهابية الالكترونية حيث اجمع فيه خبراء في القانون الدولي و حقوق الإنسان، و سياسيون بارزون عالميا، إضافة إلى ممثل الأمين العام للأمم المتحدة على ضرورة إيجاد قانون دولي و الوصول لإطار تشريعي شامل لتجريم الإرهاب الالكتروني[1].

إذ شدد المشاركون في أعمال المؤتمر الدولي على ضرورة سد الفراغ التشريعي لتعقب المجربين و الإرهابيين الذين اتخذوا الفضاء الالكتروني ساحة لممارساتهم الإرهابية.

أكد "جورج سلامة" رئيس قسم السياسات العامة و العلاقات الحكومية في تويتر الشرق الأوسط من خلال مداخلته أن تويتر[2] قامت بإغلاق مايزيد على 600000 لداعش كانت تستهدف تجنيد مستخدمي التوتير و إغوائهم للانضمام إليهم كما قال العميد القاضي العسكري "زيد توفيق العدوان" النائب العام لمحاكم امن

---

[1] ابراهيم سليم/ منى الحمودي، تقرير بعنوان إجماع لاستصدار تشريع دولي لمكافحة جرائم الارهاب الالكتروني ، تاريخ النشر 2017/5/16 على موقع الاتحاد، تم الاطلاع عليه بتاريخ 2018/3/18، على ساعة 12:00، على الرابط: http://www.alittihad.ae/modile.

[2] **تويتر:** هو إحدى المواقع الاجتماعية الموجود على شبكة الانترنت الذي ظهر في عام 2006 التي أجرته شركة Obviousالأميركية في مدينة سان فرانسيسكو واطلق رسميا للمستخدم في اكتوبر 2006 وانتشر الموقع في عام 2007 ثم في شهر ابريل 2007 قامت شركة Obvious بفصل الخدمة وظهرت شركه تحمل اسم الموقع الا وهي تويتر...للمزيد اطلع على الرابط: http://mawdoo3.com

الدولة بالأردن في مداخلته أن العالم بحاجة لإطار تشريعي شامل لتجريم الإرهاب الالكتروني معتبرا أن هذا النوع من الإرهاب هو أخطرها للوقت الحاضر.[1]

حيث جاء في الإعلان الختامي للمؤتمر الدولي لتجريم الإرهاب الالكتروني لابو ظبي مجموعة من البنود تصب جميع محتوياتها في مكافحة ظاهرة الإرهاب الالكتروني كإنشاء هيئات وطنية للمعلومات لرصد و مجابهة المحتوى الرقمي الذي ينطوي على مخاطر إرهابية، كما دعت الأطراف المشاركة في المؤتمر الدولي من خلال الإعلان النهائي إلى إدراج قانون خاص يتعلق بالجرائم الالكترونية مع تبني ما جاء في الاتفاق الملزم للمؤتمر في القوانين الوطنية.

و أهم بند صاغته الأطراف المشاركة يخدم بالدرجة الأولى الفراغ التشريعي و الهوة القانونية الحالية في مجال مكافحة ظاهرة الإرهاب الالكتروني هو اعتماد اتفاقية دولية ملزمة تحظر الإرهاب الالكتروني بكافة أشكاله بما في ذلك محاولات التجنيد، التحريض على الإرهاب، و الدعوى إليه، الإشادة به،تمويله، عدم التبليغ عنه.[2]

ومما سبق يتضح لنا ان تلك الاتفاقية ليست كافية و غير فعالة بدون الجهود الاخرى و التي يجب ان يقوم بها كل من اشخاص لقانون الدولي في مجتمع المعلومات العالمي سواء كانت شركات تكنولوجية، او حكومات.....الخ و لن يتحقق الامن المعلوماتي إلا بتحمل الجميع المسؤولية باعتبار الفضاء الالكتروني مرفق عالمي تتعاون جميع الدول من اجل ارساء قاعد قانونية لتأمين بيئتها المعلوماتية من اجل الحفاظ على الامن و السلم الدوليين.

المبحث الثاني: جهود المنظمات الدولية و الاقليمية لحماية امن المعلومات الالكترونية

إن الجهود المبذولة من أجل توفير بيئة آمنة إلكترونيا لنظم المعلومات الحساسة و الحيوية الخاصة بالبنى التحتية للدول، لن تكون لهذه الجهود أي أثر فعال إلا إذا كان هناك تعاونا و تنسيقا يتجاوز الحلول الوطنية، و ذلك لا يتحقق إلا عن طريق طرح مشكلة الأمن الإلكتروني لنظم المعلومات في المحافل الدولية والإقليمية و عليه سنعالج هذا الموضوع عبر المطلبين التاليين:

1- المطلب الأول : جهود منظمة الامم المتحدة

[1] ابراهيم سليم، منى الحمودي، مرجع سابق.

[2]- بيان ختامي للمؤتمر الدولي لتجريم الارهاب الالكتروني 15 و 16 ماي 2017

2- المطلب الثاني : مساعي الإتحاد الأوروبي و الحلف الأطلسي

المطلب الأول : جهود منظمة الامم المتحدة

بذلت الهيئة الأممية جهودا في سبيل العمل على مكافحة الجرائم المعلوماتية و ذلك لما تسببه هذه الجرائم من خسائر اقتصادية ومشاكل سياسية واجتماعية جد خطيرة ، وإن التصدي لهذا التهديد و مكافحته يتطلبان إستجابة دولية في ضوء الطابع و الأبعاد الدولية لإساءة إستخدام الكمبيوتر و الجرائم المتعلقة به.[1]

حيث أصدرت منظمة الأمم المتحدة عبر جمعيتها العامة عددا من القرارات التي توضح مدى تصاعد الإهتمام العالمي بإستخدام تكنولوجيا الإتصالات و المعلومات إستخداما غير سلمي جاء ذلك عبر سلسلة من القرارات سنتطرق لها من خلال **الفرع الاول**، واصلت المنظمة جهودها من اجل الحد من انتشار الجرائم الالكترونية الماسة بأمن المعلومات و ذلك من خلال اشرافها على عقد مجموعة من المؤتمرات **الفرع الثاني**، كما لعب الاتحاد الدولي للاتصالات كمنظمة متخصصة تابعة للمنظمة دورا لا يستهان به في مجال الأمن المعلوماتي **الفرع الثالث** :

الفرع الأول: جهود المنظمة من خلال قرارات جمعيتها العامة

ومن الجدير بالذكر أن منظمة الأمم المتحدة على علم تام بمدى الأخطار التي تنجم عن ظاهرة الإجرام الالكتروني والدليل على ذلك صدور العديد من القرارات.

أولا: قرارات بشأن التطورات في ميدان المعلومات و الإتصالات السلكية و اللاسلكية في سياق الأمن الدولي.

- ومن هذه القرارات القرار رقم 49/ 54 و المعبر عن قلق الجمعية العامة عن احتمال أن تستخدم هذه التكنولوجيا و الوسائل في أغراض لا تتفق و أهداف صون الاستقرار و الأمن الدولي، و قد تأثر تأثيرا سلبيا على أمن الدولة في الميدانيين، المدني والعسكري ، إذ ترى الجمعية أنه من الضروري تكثيف التعاون الدولي من اجل منع إساءة إستخدام موارد أو تكنولوجيا المعلومات أو إستغلالها في تحقيق أغراض إجارمية أو إرهابية،[2]واقتناعا منها بخطورة تأثير الاستخدام السيئ لتكنلوجيا المعلومات علي

[1]نجاري بن حاج فايزة، الآليات القانونية لمكافحة الإرهاب الإلكتروني، مذكرة لنيل شهادة ماجيستر في القانون، جامعة مولود معمري تيزي وزو، كلية الحقوق،الجزائر ،بدون سنة.

[2]ينظر القرار رقم 54/49، الدورة 54، البند 71 من جدول الأعمال، سنة 1999.

مصالح المجتمع الدولي أكدت من جديد في قرارها رقم 55/28على ضرورة التعاون الدولي،[1]واصلت الامم المتحدة اهتمامها بمكافحة الإجرام ألمعلوماتي عن طريق جمعيتها حيث تهيب بالدول الأعضاء من اجل اتخاذ تدابير للحد من الأخطار القائمة والمحتملة في ميدان امن المعلومات جاء ذلك في القرار رقم 56/19 وما يتماشى والحفاظ على التدفق الحر للمعلومات[2] .

– و تلاحظ الجمعية العامة في قرارها الصادر سنة 2003 أن نشر و إستخدام تكنولوجيا ووسائل المعلومات يؤثران في مصالح المجتمع الدولي بأكمله، و أن الفاعلية المثلى من اجل التصدي لهذه الآثار التي تكمن في تعزيز التعاون الدولي الواسع النطاق.[3]

ثانيا: **بشأن مكافحة إساءة إستعمال تكنولوجيا المعلومات لأغراض إجرامية.**

القرار رقم 65/63 والذي جاء يحمل مجموعة من التدابير الرامية الى مكافحة هذا النوع من إساءة الاستعمال نذكر منها.

أ– ينبغي للدول أن تكفل عدم توفير قوانينها وممارستها ملاذا أمنا للذين يسيؤن إستعمال تكنولوجيا المعلومات لأغراض إجرامية.

ب– ينبغي أن تتبادل الدول المعلومات المتعلقة بالمشاكل التي تواجهها في مكافحة إساءة إستعمال تكنولوجيا المعلومات لأغراض إجرامية.

ج– ينبغي تدريب العاملين في مجال إنفاذ القوانين و تجهيزهم بما يمكن من مكافحة إساءة إستعمال تكنولوجيا المعلومات لأغراض إجرامية.

وتدعو الجمعية العامة الدول إلى أخذ هذه التدابير المذكورة أعلاه بعين الاعتبار في جهودها الرامية إلى مكافحة إساءة إستعمال تكنولوجيا المعلومات لأغراض إجرامية.[4]

كما عكست قرارات الجمعية العامة للأمم المتحدة الإدراك الكبير لمشكلات أمن المعلومات الدولية، و تمت لأول مرة الإشارة إلى الإستخدام العسكري المحتمل لتكنولوجيا الإتصال و المعلومات في القرار المقدم في ديسمبر 1999.[1]

---

[1] ينظر القرار رقم 55/28 ،الدورة 55،البند68من جدول أعمال ،سنة2000

[2]ينظر القرار 56/19،الدورة69،من جدول أعمال سنة2002

[3]ينظر القرار رقم 57/53، الدورة 57، البند 61 من جدول الأعمال، سنة 2002

[4]نفس المرجع السابق.

و دعت القرارات الدول للمزيد من النظر في الأخطار القائمة و المحتملة في ميدان أمن المعلومات، و كذلك في ما يمكن اتخاذه من تدابير للحد من المخاطر التي تبرز في هذا الميدان.

الفرع الثاني: جهود المنظمة من خلال مؤتمراتها

واصلت المنظمة جهودها مؤكدة على وجوب تعزيز العمل المشترك بين أعضاء المنظمة، من أجل التعاون على الحد من انتشار الجرائم الإلكترونية الماسة بأمن المعلومات على الصعيد الدولي، و هذا من خلال مؤتمراتها، و الذي يعنينا في هذه الدراسة هو جهودها من خلال مؤتمراتها الخاصة بمنع الجريمة و معاملة المجرمين المتعلقة بالجرائم التقنية او جرائم الحاسب الآلي بدءا بالمؤتمر السابع عام 1985 المنعقد في مدينة ميلانو بايطاليا إذ انبثقت عنه مجموعة من القواعد التوجيهية و التي اكتملت صياغتها في الاجتماعات الاقليمية التحريرية للمؤتمر الثامن الذي اجاز هذه المبادئ و الذي عقد بهافانا بكوبا 1990، واصلت منظمة الامم المتحدة عقد مؤتمراتها حيث كانت تؤكد التوصيات في كل مرة على:

- وجوب حماية الانسان في حياته الخاصة و ملكيته الفكرية من مخاطر التكنولوجيا
- تحسين امن الحاسب الآلي و التدابير المنيعة
- تحديث القوانين الجنائية الوطنية
- زيادة التعاون الدولي من اجل مكافحة هذه الجرائم.

إلى غاية المؤتمر الثاني عشر. لمنع الجريمة و العدالة الجنائية و ذلك بالبرازيل 12_19 أفريل 2010 حيث ناقشت فيه الدول الأعضاء بنوع من التعمق مختلف التطورات الأخيرة في إستخدام العلم و التكنولوجيا.[2]

كما تشجع منظمة الأمم المتحدة على التعاون مع الإتحاد الأوروبي و منظمة الأمن و التعاون مع أوروبا و كذلك مع الأنتربول[1] و الأيروبول[2] الخاص بالإتحاد الأوروبي، و تسعى تلك الجهود في إطار تنفيذ الأجندة العالمية للأمن الإلكتروني.[3]

---

[1] د/ عادل عبد الصادق، الأمم المتحدة و دعم الإستخدام السلمي للفضاء الإلكتروني، المركز العربي لأبحاث الفضاء الإلكتروني، تم الإطلاع عليه في 2017/12/20، على ساعة 12:00، على الرابط: http//:www.accronline.com article-detail

[2] د/ محمود احمد عبابنة،جرائم الحاسوب و أبعادها الدولية، دار الثقافة للنشر و التوزيع الطبعة الأولى، الإصدار الثاني، 2009، ص ص ص ،156 157 158

المطلب الثاني: دورالمنظمات الإقليمية في حماية امن المعلومات الالكترونية

ان خطر الجرائم المعلوماتية الماسة مباشرة بأمن المعلومات الالكترونية جعل المنظمات تكثف جهودها على مستوى أقاليمها قصد الحد من انتشار هذه الجرائم حيث برز الاتحاد الأوروبي كمنظمة بجهوده التي تمثل تحديا جديدا للمجتمع الدولي خاصة في ظل التطور السريع لهذه الجرائم هذا **الفرع الاول**، لم يتأخر حلف الناتو عن مواكبة بقية المنظمات في تبني إستراتيجية خاصة من اجل توفير حماية للبيئة المعلوماتية لدوله الأعضاء **الفرع الثاني**.

الفرع الأول:جهود الاتحاد الأوروبي في مجال حماية امن المعلومات الالكترونية.

يقدم لنا الاتحاد الأوروبي نموذجا مميزا للتعاون الإقليمي لتحقيق الأمن ألمعلوماتي، حيث يسعى من خلال تطوير إستراتيجية دفاعية هدفها حماية الدول الأعضاء من الاعتداءات الالكترونية، كما يركز على التنسيق بين الدول في الاتحاد على الجوانب التشريعية و تقوية البنى التحتية المعلوماتية لأجهزة الاتحاد.[4]

بذل الاتحاد الأوروبي جهودا لا يستهان بها في مجال الحماية القانونية لأمن المعلومات الالكترونية و التي تمس جوانب عديدة من القطاعات الهامة في الدولة و على سبيل المثال:

التوجيه 2000/31/EC الصادر عن البرلمان الأوروبي و مجلس أوروبا بشان جوانب قانونية معينة من خدمات مجتمع المعلوماتية

---

[1] **الانتربول:** تم إنشاؤها في 1923/9/7 و تعد من أهم المنظمات الناشطة في مجال مكافحة الجريمة نظرا إلى ما تقدمه من إمكانيات تعقب و ضبط مرتكبي الجرائم على اختلاف أنواعها تضم حاليا 190 بلد عضو و يعمل لديها 541 موظف من 79 جنسية مختلفة و تباشر مهامها بأربع لغات رسمية، مقرها الحالي ليون/فرنسا..... للمزيد اطلع على: د/ بن مكي نجاة، مرجع سابق

[2] **الأيروبول:** هي وكالة تطبيق القانون الأوروبية، وضيفتها حفظ الأمن في أوروبا عن طريق تقديم الدعم للدول الأعضاء في الاتحاد الأوروبي في مجالات مكافحة الجرائم الدولية الكبيرة و الإرهاب، تمتلك الوكالة اكثر من 700 موظف في مقرها الرئيسي الكائن في لاهاي في هولندا و هي تعمل بشكل وثيق مع اجهزة امن دول الاتحاد الأوروبي و دول من خارج الاتحاد كأستراليا، كندا، الولايات المتحدة الأمريكية، النرويج.. تم الموافقة على تأسيس اليوروبول في معاهدة ماسترخت عام 1992 و باشرت الوكالة بالقيام بعمليات محدودة عام 1994 و في عام 1998 تمت مراجعة طبيعة عمل اليوروبول من قبل دول الاتحاد الأوروبي و بدأت الوكالة بالقيام بمهامها كاملة بتاريخ 1 جويلية 1999 .... للمزيد اطلع على: موسوعة ويكيبيديا على الرابط: https://wikipidia.org

[3] د/ عادل عبد الصادق، مرجع سابق.

[4] نوران شفيق،نفس المرجع السابق، ص 103

– القرار الإطاري لمجلس الاتحاد الأوروبي 2000/413/GHA بشان مكافحة الاحتيال و تزوير وسائط الدفع الغير نقدي (قرار الاتحاد الأوروبي بشأن الاحتيال و التزوير).

– القرار الإطاري لمجلس الاتحاد الأوروبي 2005/222/GHA بشان الهجمات على النظم المعلوماتية (قرار الاتحاد الأوروبي لشأن الهجمات ضد نظم المعلومات).

– التوجيه 2006/24/EC الصادر عن البرلمان الأوروبي و مجلس الاتحاد الأوروبي بشان الاحتفاظ بالبيانات التي تستخلص أو تعالج في إطار توفير خدمات الاتصالات الالكترونية المتاحة للجمهور.[1]

و بخلاف النهج الإقليمية الأخرى فان تنفيذ الصكوك التي يعتمدها الاتحاد الأوروبي إلزامية على جميع الدول الأعضاء .

و بالرغم من إلزامية الصكوك الصادرة عن الاتحاد الأوروبي إلا انه كان هنالك عائق في تنفيذها يتمثل في الصلاحيات المحدودة في مجال القانون الجنائي .

وقد غيرت معاهدة لشبونة هذا الوضع وهي تعطي ألان الاتحاد الأوروبي ولاية أقوى لمواءمة التشريعات الوطنية للدول الأعضاء بشان جرائم المعلوماتية و هذا يقتصر على الدول الأعضاء في الاتحاد فقط .

وقد اعد مجلس أوروبا صك لتنسيق التشريعات الخاصة بالإجرام الالكتروني هو الاتفاقية المتعلقة بجرائم الفضاء الحاسوبي التي تم إعدادها بين 1997 و 2001 و شملت هذه الاتفاقية مجموعة من البنود تعلقت بالجانب الموضوعي و الإجرائي في الشق الجنائي و أيضا بالتعاون الدولي كما تم إصدار بروتوكول إضافي في هذه الاتفاقية من اجل تغطية موضوع تجريم العنصرية و توزيع مواد تثير كراهية الأجانب المرتكبة بواسطة الحاسوب.[2]

[1] دراسة شاملة عن الجريمة السيبرانية، مسودة فيفري 2013، مكتب الامم المتحدة المعني بالمخدرات و الجريمة، الامم المتحدة نيويورك 2013، ص ص 10 11

[2] مؤتمر الامم المتحدة 12 لمنع الجريمة و العادلة الجنائية، البند الثامن من جدول الأعمال المؤقت، التطورات الأخيرة في استخدام العلم و التكنولوجيا من جانب المجرمين و السلطات المختصة في مكافحة الجريمة بما في ذلك الجرائم الحاسوبية ، المنعقد في سالفادور (البرازيل)19/12 أفريل 2010 ، موقع الأمم المتحدة تم الاطلاع عليه بتاريخ 2018/02/24

الفرع الثاني: دور منظمة حلف شمال الاطلنطي (الناتو)

إن تعرض استونيا سنة 2007 للهجوم الالكتروني الخارجي جعل حلف الناتو[1] يعيد حساباته من جديد و ذلك لعجزه التام على الرد على هذا النوع من الهجوم و بالرغم من ان استونيا نالت العضوية في الحلف منذ 2004 و المادة الخامسة من ميثاقه تنص عل وجوب الدفاع المشترك من قبل الدول الأعضاء في حالة إذا تعرضت أي منهم لهجوم خارجي لم يبادر حلف الناتو بالدفاع وذلك لصعوبة تحديد العدو وأيضا لنوعية الأسلحة التي استعملت في هذا الهجوم و التي تختلف على ما عرفت به الأسلحة التقليدية. [2]

وعليه بدأ الناتو في مراجعة سياسته الدفاعية بناءا على المعطيات الجديدة و التي برزت مع التطور التكنولوجي الهائل و المتسارع و العابر للحدود الجغرافية الدولية ضاربا في عمق البنى الأساسية و الحساسة للدول مستعملا الجانب ألمعلوماتي كمدخل رئيسي لهدم أمن و سلامة الدولة .

في عام 2008 قام الحلف بإنشاء مركز الدفاع الالكتروني التعاوني للتميز مقره بتالين العاصمة الإستونية يهدف هذا المركز لتقييم القدرات الدفاعية لدول الحلف و أيضا لزيادة الوعي بقضايا الأمن الالكتروني و في 2012 خصص الحلف مبلغ 58 مليون يورو وذلك لترسيخ قدرة الناتو على الرد الفوري على الهجمات الالكترونية و في 2013 تم الاتفاق على إنشاء فرق للرد الالكتروني لحماية كافة الأنشطة و الشبكات الالكترونية للمنظمة [3]،ويعمل حلف الناتو على تنسيق سياسات الدول الأعضاء في مابينها لاعتماد سياسة دفاع مشتركة ضد خطر الهجمات الالكترونية ، كما يقوم الناتو بمتابعة الأخطار المحتملة من خلال مراكز تقنية مختصة في رصد أخطار الهجمات الالكترونية ،ويسعى حلف الناتو كمنظمة إلى دمج مفهوم الدفاع الالكتروني في برامج الشراكات مع المنظمات الدولية والبلدان الأعضاء في الناتو.

---

[1] **حلف الناتو**: هو تحالف دولي يتكون من 28 دولة عضو من أمريكا الشمالية وأوروبا .والحلف أنشئ عند التوقيع على معاهدة حلف شمال الاطلسي في 4 أبريل 1949. وتنص المادة الخامسة من المعاهدة على أنه في حالة حدوث هجوم مسلح ضد واحدة من الدول الأعضاء ينبغي أن يكون أمن مشترك، ويجب أن يساعد الأعضاء الآخرون الأعضاء المعتدى عليهم، بالقوات المسلحة إن لزم الأمر.....للمزيد اطلع على: www.wikipidia.org

[2] نوران شفيق ، مرجع سابق، ص 99.

[3] نوران شفيق ، مرجع سابق، ص ،ص،ص،102،101،100

والفضاء الالكتروني حسب دراسة أونيل سليمان[1] يحتاج إجماعا دوليا جديدا ولذلك يعمل الناتو على تقديم توصيات إلى الدول والهيئات المتابعة للإخطار الالكترونية الماسة بأمن المعلومات ،كما أكدت الدراسة بان الناتو يعمل على تحديد تطور مخاطر فضاء الانترنت خصوصا بين 2010و2020.[2]

و بهذا نستطيع القول إن الإطار الدفاعي للناتو هو من انجح، إن لم نقل هو الأنجح على الإطلاق مقارنة بالمنظمات الدولية و الإقليمية الأخرى

المبحث الثالث: الدفاع عن السيادة الرقمية للدولة

ينص دليل تالين[3] الذي كتب بتكليف من "**مركز التميز التعاوني**" المخصص بالدفاع عن الفضاء الالكتروني، التابع لحلف الناتو، و مقره تالين عاصمة استونيا على ان"**الدول تستطيع ممارسة السيطرة على البنية التحتية الالكترونية، و النشاطات الالكترونية التي تقع و تمارس داخل أراضيها السيادية**".

و السيادة احد المفاهيم الأساسية في القانون الدولي المعاصر، و المساواة في السيادة من المبادئ الأساسية التي تحدد العلاقات الدولية المعاصرة.[4]

و قد مر مفهوم السيادة بعدة محطات و مفاهيم مختلفة من السيادة المطلقة الى السيادة المقيدة و أخيرا إلى اللا سيادة و ذلك في العصر الرقمي الذي نعيشه اليوم، و بهذا يكون مفهوم السيادة في طريقه الى التحول الكامل، مما يفسح المجال لظهور مفهوم جديد سمي السيادة الرقمية.

و الذي يعرفها الدكتور **محمد سعادي** أستاذ القانون الدولي العام بمعهد الحقوق بجامعة غليزان بأنها "**بسط الدولة لسيطرتها و ولايتها القضائية على الفضاء الرقمي المتمثل في الانترنيت**"[5]

و لا احد يمكن إنكار ما فرضته التكنولوجيا الحديثة من صبغة جديدة في إطار العلاقات الدولية ومن ضمنها التطور الالكتروني من اعتداءات على مفهوم السيادة الرقمية للدولة حيث بذلت الدول

---

[1] اونيل سليمان :رئيس قسم الدفاع وتحديات الامن الالكتروني،اعد دراسة بعنوان (ظهور تحديات جديدة للامن)....للمزيد اطلع على المقال بصحيفة الراي ،العدد 12138الصادرة في 2012/9/12.

[2] عماد المرزوقي،الناتو يرفع درجة خطر الهجمات الالكترونية ،مقال منشور على صحيفة الراي ،العدد (12138)، الاثنين 24 سبتمبر 2012

[3]

[4] تانغ لان، مقال بعنوان السيادة الوطنية و الفضاء الالكتروني، على موقع الخليج، تاريخ النشر 2016/4/27، تم الاطلاع عليه بتاريخ 2018/3/18، على ساعة 12:00، على الرابط http://alkaly.ea/mob/detail

[5] د/ محمد سعادي،نفس المرجع السابق، ص ص، 209 210

مجهودات عديدة للتصدي و الدفاع على سيادتها الرقمية و هذا ما سنتطرق له في **المطلب الأول**، و نظرا للأهمية الكبرى و المصيرية التي احتلتها الانترنيت جعل الدول تطالب بالمشاركة في إدارة الانترنيت كحماية لسيادتها الرقمية و أمنها المعلوماتي هذا ما سنبحثه في **المطلب الثاني**.

المطلب الأول:نحو تعزيز السيادة الرقمية للدولة

بما أن أكثر الدول اعتمادا على الانترنيت و على الشبكات المعلوماتية تعتبر هي الأكثر عرضة للاعتداءات و التهديدات الالكترونية و التي تمس بمجال سيادتها الرقمية.

و بما أن ميدان الفضاء الالكتروني هو ميدان لا تناظري أي بمعنى انه ميدان تختلف فيه موازين القوى من طرف إلى آخر تتدرج من الضعيف إلى القوي، عكفت الدول على تطوير قدراتها الدفاعية في مجال فضائها الالكتروني بحثا عن توفير فضاء معلوماتي آمن، تفرض فيه الدولة سيادتها الرقمية بدون منازع.

سنتطرق من خلال هذا المطلب إلى ما بذلته الدول من جهود من اجل الدفاع عن سيادتها الرقمية هذا في **الفرع الأول** ،و كيف انه يمكن للفضاء ألمعلوماتي أن يكون إرثا مشتركا للإنسانية يخضع لمبادئ القانون الدولي العام هذا من خلال **الفرع الثاني**.

الفرع الأول: الجهود الفردية للدول للدفاع عن السيادة الرقمية من اجل حماية البيئة المعلوماتية

تنافست الدول فيما بينها من اجل تعزيز دفاعاتها الالكترونية عن السيادة الرقمية حتى توفر بيئة معلوماتية آمنة من الاختراقات الخارجية لمجالها السيادي الرقمي.

– انجلترا: قامت على سبيل المثال بإصدار إستراتيجية الأمن الالكتروني القومية في جويلية/2009، كما قامت بإنشاء وحدة الأمن الالكتروني و مركز العمليات و مقره وكالة الاستخبارات القومية (GCHO) و بدأت وظيفتها عمليا في شهر مارس 2016.

– الولايات المتحدة الأمريكية: في ماي 2009 صادق البيت الأبيض على وثيقة "مراجعة سياسة الفضاء الالكتروني" و التي تم تقديمها من قبل لجنة خاصة إلى الرئيس الأمريكي اوباما، و هي تلخص الخطوات التي يجب على الولايات المتحدة الأمريكية إتباعها من اجل وضع خارطة طريق لأمنها المعلوماتي في المستقبل، وذلك لتأمين سيادتها الرقمية في الفضاء الالكتروني، كما قامت الولايات المتحدة

الأمريكية في ماي 2010 بإنشاء قيادة الانترنيت "سايبركوم" و عينت مدير وكالت الاستخبارات القومية العسكرية الجنرال "كيت الكسندر" قائدا عليها مهمته الحرص على حماية الشبكات الأمريكية العسكرية على الدوام[1] ، و ذلك للأهمية الخطيرة للشبكات العسكرية و ارتباطها الأكيد بشبكة الانترنيت و تأمينها هو ضمان لعدم اختراق السيادة الرقمية للدولة.

- الكيان الصهيوني:أعلن بن يامين نتنياهو في 18/ماي/2011 عن إنشاء"هيئة السايبر الوطنية " في إسرائيل ،وذكر نتنياهو أن أهداف هذه الهيئة هو تعزيز قدرات إسرائيل الدفاعية عن أنظمة البنى التحتية الحيوية من أخطار الفضاء الالكتروني.[2]

الفرع الثاني: وضع تشريع دولي جديد لتنظيم الفضاء المعلوماتي بصفته إرثا مشتركا للإنسانية

حاولت الدول وضع نموذج تشريعي دولي تنظم به علاقاتها في الفضاء المعلوماتي حتى تتمكن الدول من التحكم في سيادتها الرقمية و الدفاع عنها بشكل قانوني.[3]

فقد أحرزت الدول في هذا المجال بعض النجاحات ففي جويلية 2015 استطاعت مجموعة خبراء الأمم المتحدة بما فيهم خبراء من روسيا و الولايات المتحدة الأمريكية (شكلت عام 2004) من التوصل إلى اتفاق بشأن تقرير يتضمن القواعد الأساسية لسلوك الدول في الفضاء الالكتروني و بموجب هذه القواعد تلزم الدول باستخدام تكنولوجيا المعلومات و الاتصالات في الأغراض السليمة فقط، و الامتناع عن مهاجمة المواقع الحيوية لبعضها البعض في البنى التحتية (المحطات الذرية لتوليد الطاقة الكهربائية النظم المصرفية، و أنظمة النقل وغيرها).[4]

---

[1] المجال الخامس الحروب الالكترونية في القرن 21، مقال منشور على موقع مركز الجزيرة للدراسات، تم الاطلاع عليه بتاريخ 2018/3/11، على ساعة 12:00، على الرابط: studies.alja.eera.net

[2] شموئيل ايفن ،دافيد بن سيمان ،مراجعة كتاب حرب في الفضاء الالكتروني اتجاهات وتأثيرات على اسرائيل ،معهد دراسات الأمن القومي،تل أبيب 2011 على موقع المركز العربي للأبحاث ودراسة السياسات.

[3] د/محمد سعادي،نفس المرجع السابق،ص 255

[4] الفضاء الالكتروني للمناورة، مقال في صحيفة "كوميرسانت"، تاريخ النشر 2016/12/6، تم الاطلاع عليه بتاريخ 2018/3/11، على ساعة 12:00، على الرابط: http://ar.rt.com

و تعتبر هذه الخطوة الأولى لمحاولة جعل الفضاء الالكتروني إرثا مشتركا للإنسانية يستخدم للأغراض الإنسانية فقط، و يجب حمايته بصفته هذه، في جعل الفضاء الالكتروني ميدان للتفاعلات التشاركية و السليمة كلما تبلورت لدينا قواعد قانونية دولية ملزمة لرواد هذا الفضاء.[1]

كما بينه لويس كفاري "louis cavari" حين يقول: بأن القانون الدولي سيتأقلم مع الحاجيات الاجتماعية و ينظمها ليصلوا في النهاية الى وضع مشروع تشريع دولي يتكون من مجموعة من النصوص نذكر منها:

-المادة 1: يجب أن يستعمل الفضاء المعلوماتي من اجل خير و مصلحة جميع الدول مهما كانت قوتها الالكترونية أو الاقتصادية فهو وقف على الإنسانية جمعاء.

-المادة 2: لا يسمح بممارسة أي نشاط في الفضاء المعلوماتي سوى للنشاطات السليمة.

-المادة 3: لا يسمح بتملك الفضاء المعلوماتي و ذلك بإعلان السيادة عليه.

-كما اقترحت المادة 4 بأن تنشأ سلطة قضائية دولية تنظم و تراقب نشاطات الدول في الفضاء المعلوماتي و التزامها بهذه المعاهدة، أو التشريع الدولي المقترح.

-و تحدثت المادة رقم 5 على قيام المسؤولية الدولية في حالة مخالفة الدول الأعضاء بنود المعاهدة الخاصة بنشاطات الممارسة و أن مجال هذه المسؤولية يتسع ليشمل نشاطات المنظمة الدولية أيضا، كما أكدت المادة رقم 6 على التعاون الدولي بين الدول في الفضاء المعلوماتي و اعتبار الدول بمصالح بقية الأطراف.[2]

و بهذا المنوال تكون السيادة الرقمية للدولة محمية بموجب قواعد القانون الدولي العام مما يوفر حماية للبيئة المعلوماتية الحساسة و الخاصة بميادين البنى التحتية للدولة.

المطلب الثاني: المشاركة في إدارة الانترنت كوسيلة لحماية السيادة الرقمية

تسمى المؤسسة التي تشرف على الانترنت بمجلس إدارة شبكة الانترنيت و تعرف اختصارا (ICANN)[3]، و مقرها يوجد بلوس انجلوس و هي مؤسسة خاصة بغايات غير ربحية[4]، و يسير المجلس

[1] Anne-Thida NORODOM, internet et droit international: défi ou opportunité, clloque de Rouen, 2014 P 19.

[2] د/ محمد سعادي، نفس المرجع السابق، ص ص 255 256

[3] L'ICANN: voit le jour en 1998 sous la forme d'une organisation à but non lucratif, enregistrée en Californie, et donc soumise au droit bienveillant du non prpfit public benefit corporations low …….. VOIR: INTERNET :considération techniques à destination des juristes, alain Godon , 2014 P 13.

[4] التحكم في شبكة المعلومات العالمية للانترنيت، مقال منشور على موقع الجزيرة

الشبكة من خلال 14 جهاز معروفة بإسم "الموزعات الجذور" و التي تمول الآلاف من الموزعين حول مجموعة الكرة الأرضية، مما يجعل توزيعها يبدو غير عادل إذ يوجد 10 من هذه الموزعات الجذر بالولايات المتحدة الأمريكية و 4 موزعة على كل من انجلترا و اسبانيا و سويد و الرابع موجود في اليابان.

و تجدر الإشارة إلى أن نظام تسيير أسماء الميادين DNS[1] يوجد حاليا بيد الشركة الأمريكية المكلفة بتسيير نظام أسماء الميادين و تخصيص فضاء عناوين بروتوكولات الانترنيت (ICANN).[2]

الفرع الاول: التحكم في الانترنت مسألة سيادة تتكفل بها منظمة حكومية

تعد سيطرت الولايات المتحدة الأمريكية على عمل الشبكة الدولية للانترنيت مبعث قلق للعديد من الدول التي طالبت بنصيب في هذه الإدارة، و على رأسها الدول النامية و الاتحاد الأوروبي المطالبين بإنشاء هيئة دولية للإدارة على الانترنيت و الرقابة عليها، لما لها من أهمية على مستوى السيادة الرقمية للدولة و فضائها الالكتروني.

والى جانب هذه المواقف، اخذت العديد من منظمات المجتمع المدني الدولي ممارسة الضغوط من اجل إنهاء السيطرة الأمريكية على تسيير شبكة الانترنت باعتبارها تمثل تهديد لحقوق السيادة الرقمية.

و في مواجهة هذه الضغوط لجعل الانترنت يخضع في إدارته للأمم المتحدة تمسك الموقف الأمريكي بالسيطرة على عمل الشبكة و إدارتها بحجة أن تمسكه يتعلق بالجانب التقني لا أكثر.

و أن مسألة احتكار الولايات المتحدة الامريكية للكود التقني للشبكة يرجع ذلك الى كون ان الولايات المتحدة الامريكية تاريخيا هي مخترعة الانترنيت ،و من ثم يصبح لها حق الملكية الفكرية.

لكن الدول النامية ترى بأن الانترنت أصبحت مرفقا عالميا و ليس خاصا،و أن منظمة الأيكان لا تخضع لأي اتفاقيات دولية مما يعني أن تكون عرضه للقرارات تعسفية أحادية الجانب بدون أن يكون لأي دولة الحق في الرفض.

---

[1] DNS:هو نظام يخزن معلومات تتعلق باسماء نطاقات الانترنيت بقاعدة بيانات لا مركزية على الانترنيت يستطيع خادم اسم النطاق ربط العديد من المعلومات بأسماء النطاقات، و يعتبر نظام اسماء النطاقات مفيدا لعدة اسباب اكثرها وضوحا انه يجعل من الممكن استبدال عناوين ال IP الصعبة التذكر(مثل 206، 131، 142، 207) بأسماء نطاقات سهلة التذكر مثل (wikipidia.org) و هذا يسهل على البشر التعامل مع عناوين الشبكة... للمزيد اطلع على الموقع : https://wikipidia.org

[2] د/محمد سعادي، المرجع السابق، ص85.

كل هذا دفع بالدول الأعضاء في الأمم المتحدة إلى تنظيم قمة عالمية حول مجتمع المعلومات في جينيف 2005 و قبله تونس 2003 و بعدها تنظم قمة عالمية لمجتمع المعلومات بجينيف سويسرا 2010 أن النقاشات التي دارت خلال القمم الثالث المذكورة أعطت بعدا سياسيا لموضوع التحكم في إدارة الانترنيت ،و هذا ما جاء في تقرير مجموعة العمل حول التحكم في إدارة الانترنيت مما جعلها تطالب (مجموعة العمل) بنقل سلطات إدارة الانترنيت من الهيئة الأمريكية (ICANN) إلى الاتحاد الدولي للاتصالات أو لمنظمة الأمم المتحدة.[1]

الفرع الثاني: الاتفاق على إنشاء آليات التحكم في إدارة الانترنت

كانت الآلية الأولى هي مجموعة العمل حول التحكم في إدارة الانترنيت و التي أنشأها الأمين العام للأمم المتحدة سنة 2003 أثناء القمة العالمية لمجتمع الإعلام بتونس تتكون من مزيج من دول و قطاع خاص و مجتمع مدني ،و منظمات حكومية و منتديات معنية، و ينصب عمل المجموعة على النقل التدريجي للتحكم في الانترنيت إلى سلطة المجتمع الدولي من اجل كفالة للسيادة الرقمية للدولة ،والآلية الثانية هي منتدى استشاري تناقش على مستواه جميع المسائل المتعلقة بالتحكم في الانترنيت و إدارته ،تبنته الأمم المتحدة في قمة تونس 2003 لمجتمع المعلومات، قام بتنظيم عدة منتديات ابتداء من أثينا 2006 إلى 2010 بلتوانيا، حيث يعتبر إنشاءه كتقدم حقيقي اذ يشكل إطارا رسميا و دوليا دائما من اجل النقاش حول مسألة المعايير الواقعية حول التنظيم الديمقراطي و الحقيقي لمرفق الانترنيت.[2]

ويتضح من ماسبق بان سيادة الدولة تفرض نفسها بقوة من جديد و بمقياس جديد في مجتمع تطور بطريقة جديدة تجعل من صناع القرار على المستوى الدولي التفكير من جديد في تأسيس إطار قانوني محكم لحماية سيادة الدولة في عالم الرقمنة، من الانتهاكات و الاعتداءات بطرق جديدة.

[1] مصطفى بن عصام نعوس،نفس المرجع السابق، ص341

[2] د/محمد سعادي، نفس المرجع، ص

لقد شهد العالم ثورة غيرت مجرى التاريخ وهي الثورة الصناعية ،ويشهد العالم الآن ثورة ولكنها من نوع جديد، ثورة تعتمد على المعلومات والمعرفة،الآ وهي الثورة التكنولوجية،هذه الثورة لم يتم استخدامها في الأعمال السلمية فقط،ولكن تم استخدامها بشكل سلبي يضر بالبشرية بأكملها،و أصبح للفضاء الالكتروني أهمية كبيرة في النظام الدولي خاصة بعد تزايد الاعتماد على التكنولوجيا حيث ساعد على انتهاء احتكار القوة بمفهومها التقليدي ،والمتمثلة في القوة الصلبة، وظهور نوع جديد من القوة وهي القوة الالكترونية او الافتراضية وأصبحت تلك القوة في متناول كل من يملك المعرفة التكنولوجية وله القدرة على استخدامها لتحقيق أهدافه، ولكن بصورة مختلفة نوعا ما باستخدام تقنيات الكترونية في نطاق أعمال عدائية على شكل هجمات الكترونية تشكل تهديدا على صعيد الأمن والسلم الدوليين بمستوى لايقل جسامة عن اخطر التهديدات المعروفة دوليا.

تتميز الانترنت بالسرعة الفائقة هذا ماجعل جميع البوابات مفتوحة ويمكن من خلالها للجميع الدخول غير المأذون به ،وتقتضي الحكمة أن تحذر الدول من جميع الفيروسات وهجمات القراصنة المتوقعة لان أفعالهم الإجرامية غدت عمليات حرب معلوماتية حقيقية،مما يقتضي تحديد مصدر الاعتداء وملاحقة فاعليه ،أو الرد عليه بممارسة حق الدفاع الشرعي عن النفس، وتبعا لذلك يبرز التساؤل حول مدى توافق المعايير الدولية القائمة مع الأوضاع الجديدة؟.ومما سبق ذكره تداعت الدول الالكترونية الكبرى على غرار الولايات المتحدة وروسيا والصين إلى البحث في إعداد معاهدة جديدة تحظر استخدام الأسلحة المستحدثة ،لما يمكن لهذا السلاح النظيف من إلحاق الخراب والدمار والشلل بالمنظومة المعلوماتية للدولة.[1]

[1] مصطفى نعوس،حقوق والتزامات الدول في الحرب المعلوماتية ،مقال منشور على مجلة دراسات ،علوم الشريعة والقانون المجلد 40 الملحق،1،من الصفحة 784حتى الصفحة 800 ،تصدر مجلة دراسات عن عمادة البحث العلمي في الجامعة الاردنية ،2013

المبحث الأول: الهجمات الالكترونية و حضر استخدام القوة وفق المادة 4/2 مع تكييف الدفاع الشرعي من خلال المادة 51 من ميثاق الأمم المتحدة.

أكد ميثاق الأمم المتحدة تحريم استخدام القوة المسلحة أو التهديد باستخدامها ضد السلامة الإقليمية، أو الاستقلال السياسي للدول الأعضاء في الأمم المتحدة، كما أورد الميثاق استثناءات لحالة الاستخدام المشروع للقوة في القانون الدولي، و هي حالات الدفاع[1] و التي تضمنتها المادة 51 و ذلك وفق مجموعة من الشروط الموضعية و الإجرائية لكن مع التطور التكنولوجي الهائل أصبح المجتمع الدولي أمام نمط جديد من الهجمات و الاعتداءات حيث تحمل طابعا و أسلوبا جديدا غير تقليدي في بيئة غير تقليدية، و لها نتائج جد خطيرة على امن و استقرار العلاقات الدولية، و قد تمس هذه الهجمات و الاعتداءات بالدرجة الأولى البنى التحتية الكونية للمعلومات و ذلك عن طريق الدخول إلى الشبكات المعلوماتية بطرق غير شرعية مما يهدد بوقوع خسائر قد يقف ورائها دول أو أي شخص من أشخاص القانون الدولي. مما يستوجب على الدول المعتدى عليها المطالبة بتفعيل حقها في الدفاع الشرعي كحق مكتسب بقوة القانون،[2] ومن خلال الطرح التالي يمكن لنا صياغة الإشكالية التالية:

هل يحظر القانون الدولي استخدام القوة السيبرانية في العلاقات الدولية وفقا للمادة 4/2 من الميثاق؟ هذا في **المطلب الأول** وهل للدولة الحق في الدفاع الشرعي لحماية أمنها الالكتروني في إطار قواعد القانون الدولي؟ هذا ما سنتطرق له في **المطلب الثاني**.

المطلب الأول: الهجمات الالكترونية و حظر استخدام القوة وفق المادة 4/2 من ميثاق الأمم المتحدة.

إن الهجوم الالكتروني له أهمية بالغة في معرفة أبعاده و نطاقه، و كذلك طرق التعامل معه لأنه يؤسس لحروب و نزاعات دولية، كذلك أن الهجوم الالكتروني أصبح احد الأسلحة الفتاكة التي تهدد امن الدولة و سيادتها، إذ أصبحت الهجمات الالكترونية مستخدمة استخداما واسعا لما تحمله من تأثير على المواقع المستهدفة، كما ان الهجمات الالكترونية (cyber attack) أصبحت من المواضيع التي تطفو على ساحة العلاقات الدولية، و خاصة بعد الهجمات التي تعرضت لها استونيا 2007، حيث أن الكثير

[1] **حالات الدفاع:** الدفاع النفسي و الجماعي، حق تقرير المصير، حروب التحرير، العمليات التي يقوم بها المجتمع الدولي و يقرها مجلس الأمن وفقا للفصل السابع من الميثاق....للمزيد اطلع على: عادل عبد الصادق، مرجع سابق، ص 109

[2] د/عادل عبد الصادق، نفس المرجع السابق، ص ص 109 110

من فقهاء القانون الدولي بدؤوا يقارنون الاعتداءات الالكترونية بالهجوم النووي لما يخلفانه من آثار تدميرية خاصة في الدول التي تربط نظامها ألمعلوماتي لإدارة مرافقها الحيوية بشبكة الانترنت.[1]

الفرع الأول: ماهية الهجوم الالكتروني

في بادئ الأمر لم يكن للهجمات الالكترونية صدى على المستوى الدولي إذ نشأت الجريمة المعلوماتية أولا على شكل جرائم طالت المؤسسات المالية والمصرفية ،وقد دأبت الدول على سن التشريعات واتخاذ التدابير لتجريم الأفعال وتحديد العقوبات ،[2] ولكن مع تسارع وتيرة استخدام التكنولوجيا الحديثة وربطها بالبنى التحتية للدول ومع الصراع المستمر من اجل اكتساب آخر ما أفرزته الثورة التكنولوجية من وسائل للتفوق على الصعيد الدولي برز مفهوم الهجمات الالكترونية إذ تشير العديد من التقارير إلى تزايد عدد هذه الهجمات في العالم،ونذكر منها على سبيل المثال مايلي:

أوردت حكومة كورية الجنوبية تقرير في ديسمبر 2009 عن تعرضها لهجوم الكتروني و اتهمت قراصنة كوريا الشمالية بسرقة معلومات سرية و خطط دفاعية في حالة قيام حرب في شبه الجزيرة الكورية، أيضا صرحت ألمانيا في جويلية 2010 أنها تعرضت لعمليات تجسس شديدة التعقيد موجهة أصبع الاتهام إلى كل من الصين و روسيا حيث أن هذا الهجوم استهدف البنى التحتية الحساسة و القطاعات الصناعية و أهمها هي شبكة الكهرباء التي كانت تغذي الدولة.[3] كما وقعت مجموعة من الهجمات الالكترونية في 27يونيو2017 ضد مواقع اكرانية باستخدام البرمجيات الخبيثة بيتيا[4]، حيث استهدفت بنوك ووزارات وصحف وشركات كهرباء وابلغ فيما بعد عن هجمات مماثلة في كل من فرنسا وايطاليا وبولندا وغيرهم من الدول.[5] والشكل الموضح في الأسفل يبين متوسطة تكلفة الهجمات الالكترونية للدول المبينة في الأعمدة وذلك خلال السنة بالدولار. واتفق غالبية فقهاء القانون الدولي و المتخصصون

---

[1] م.م/ ليث ناجح حميد، موقف القانون الدولي من الهجمات الالكترونية ، مقال منشور على مجلة كلية القانون للعلوم القانونية و السياسة، كلية الحقوق، جامعة الفلوجة، العراق،ص ص ص 302 303 304

[2] A.P.Dr. Ahmad oubais al-fatlawi,cyber attacks:its concept and arising international resbonsibility in the light of contemporary international organization, نفس المرجع السابق

[3] علي باكير، مفهوم الحروب الالكترونية، مقال منشور على موقع المقالات، بتاريخ 2011/3/9، تم الاطلاع عليه بتاريخ 2018/3/1 على الرابط: www.articles.islamweb.net

[4] **بيتيا:** اخترق "بيتيا" شبكات الشركات من خلال رسائل إلكترونية مشفرة احتوت على روابط خبيثة، تقوم عند تفعيلها بتعطيل عمل الكمبيوتر وطلب فدية مادية بقيمة 300 "بيتكوين" لاستعادة الوصول إلى بيانات الجهاز...للمزيد اطلع على موقع موسوعة ويكيبيديا .

[5] مقال منشور على موقع ويكيبيديا تم الاطلاع عليه بتاريخ 2018 /3/12

في مجال الأمن ألمعلوماتي في تعريفهم للهجمات الالكترونية على العواقب التي تخلفها استخدامات هذه الأنشطة الالكترونية.

حيث عرفها البروفيسور ريتشارد كلارك (ritcherd Clarke)المتخصص في مجال الأمن الحكومي الأمريكي بأنها "**أفعال صادرة عن دولة ما ضد أجهزة الكمبيوتر و الشبكات التابعة لدولة أخرى الغرض منه تعطيل هذه الأنظمة أو خلق اضطراب الكتروني**"[1]

كما عرف معجم هيئة الأركان المشتركة للولايات المتحدة الأمريكية لعام 2011 الهجمات الالكترونية بأنها "**الأعمال العدائية عبر استخدام الكمبيوتر أو الشبكات و الأنظمة ذات الصلة تهدف إلى تعطيل أو تدمير نظم الكترونية ذات أصول أو وظائف هامة أو حساسة للخصم**"[2]

و يخلط الكثير من المهتمون في هذا المجال (الفضاء الالكتروني) بين الهجوم الالكتروني Attaque électroniqueو الجريمة الالكترونية Crime électronique إذ انه أهم ما يميزهما عن بعض أن الهجوم الالكتروني المعتدى فيه يكون دولة أو منظمة إرهابية أما في الجريمة الالكترونية فقد تكون جهة الاعتداء مجموعة من القراصنة و بذلك فالجريمة الالكترونية لا ترتكبها دولة بحيث يكون الهجوم الالكتروني ضمن اختصاص القانون الدولي لما يمثله من اعتداء وانتهاك لسيادة الدول على عكس الجريمة الالكترونية تدخل ضمن نطاق الاختصاص الوطني كما أن الهجوم الالكتروني لا يرتكب إلا لأغراض سياسية أو من اجل المساس بالأمن الوطني وهذا لا نجده في الجريمة الالكترونية التي تنفذ دائما للحصول على منافع مالية .[3]

الفرع الثاني: تكييف الهجمات الالكترونية كاستخدام للقوة وفقا للمادة 4/2 من ميثاق الأمم المتحدة.

[1] م م/ ليث ناجح حميد، نفس المرجع السابق،ص405

[2] شريف نسيم قلته، الهجمات الالكترونية وحظر استخدام القوة في القانون الدولي،مقال منشور على موقع المركز العربي لابحاث الفضاء الالكتروني بتاريخ2017/11/52 وتم الاطلاع عليه بتارخ 2018/3/15، على ساعة 12:00، على الرابط occoronline com

[3] م.م/ ليث ناجح حميد، نفس المرجع السابق، ص ص407 408

نصت المادة 2 في فقرتها الرابعة من ميثاق الأمم المتحدة على ما يلي "**يمتنع أعضاء الهيئة جميعا في علاقاتهم الدولية عن التهديد باستعمال القوة، أو باستخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على وجه لا يتفق مع مقاصد الأمم المتحدة**"[1].

لقد اكتسب مبدأ تحريم استعمال القوة في العلاقات الدولية في مطلع القرن الماضي على القوة القانونية، انطلاقا من ميثاق الأمم المتحدة فنص المادة 2 حرم كل أشكال القوة الموجهة ضد الاستقلال السياسي و الوحدة الإقليمية سواء كانت هذه القوة مباشرة أو غير مباشرة.[2]

و هذا ما جعل السؤال التالي يطفو إلى السطح: **هل تدخل الهجمات الالكترونية كنوع مستحدث من القوة تحت طائلة المادة 4/2 من ميثاق الأمم المتحدة؟**

للإجابة على السؤال كان لا بد من دراسة المادة دراسة تحليلية من اجل الوقوف على المعنى الدقيق لكلمة القوة.

أولا: تحليل نص المادة 4/2 من ميثاق الأمم المتحدة

إذ نلاحظ أن لفظ القوة Puissance في نص المادة 4/2 جاء مطلقا و شاملا لكل أشكال القوة أي بمعنى جاء على سبيل المثال و ليس الحصر و يرجع ذلك إلى أن واضعي الميثاق لم يدر في خلدهم أثناء صياغة بنوده ما ستحدثه الثورة التكنولوجية من تطور الذي يشهده العالم الآن بل جل تفكيرهم كان ينصب نحو القوة المسلحة لذلك فانه من الممكن تفسير المادة تفسيرا موسعا بحيث تشمل المادة الهجمات الالكترونية كصورة من صور القوة في الوقت المعاصر، و هذا التوسع يخدم بالدرجة الأولى التوسع الأساسي لمنظمة الأمم المتحدة و هو حماية الأمن و السلم الدوليين.

كما أن مجموعة من فقهاء القانون الدولي و السياسة اختلفوا حول تفسير كلمة القوة التي جاءت في المادة خلال الحرب الباردة بين من أيد فكرة التوسع في تفسير مفهوم القوة حيث يرى انه يشمل الضغط و الإكراه السياسي و الاقتصادي، و كان أنصار هذا الاتجاه هم الدول الآسيوية و النامية، أما أنصار الدول المتقدمة فأيدوا المفهوم الضيق للمادة ليشمل القوة المسلحة فقط، لان التطور التكنولوجي كان في مصلحتهم.[3]

---

[1] المادة 2 من ميثاق الأمم المتحدة

[2] م.م/ ليث ناجح حميد، نفس المرجع السابق،415.

[3] المرجع نفسه،ص423.

ونرى انه إذا لم تعتبر الهجمات الالكترونية الموجهة ضد امن المعلومات الماسة بالبنى التحتية للدولة هجوما مسلحا فعلى الأقل يجب اعتبارها تشمل على تهديدا للأمن و السلم الدوليين الذي هو من مقاصد و روح ميثاق الأمم المتحدة.

ثانيا: الاختلاف الفقهي حول تفسير المادة 4/2 من ميثاق الأمم المتحدة

في غياب توجه رسمي من الأمم المتحدة لتكييف الهجمات الالكترونية ظهرت اتجاهات فقهية عديدة لمعالجة مسألة الهجمات الالكترونية حيث يبرز تياران رئيسيان يتنازعان حول هذه المسألة نتعرض لهما فيما يلي:

الموقف الأول: المقاربة المقيدة

و يعتمد مؤيدي هذا الاتجاه على التفسير الحرفي للمادة 4/2 بمعنى أنهم يرون بأن أي هجمات الكترونية لا تحدث أضرار مادية جسيمة لا تندرج ضمن نطاق المادة 4/2 بغض النظر على تأثيراتها على الأمن الدولي، و بذلك هم يرون إن الهجوم الذي وقع على المنشأة النووية سنة 2010 بإيران و الذي تسبب بتدمير بعض أجهزة الطرد المركزية يحمل مواصفات استخدام القوة الذي ينص عليه ميثاق الأمم المتحدة من خلال المادة سابقة الذكر.

الموقف الثاني: المقاربة الموسعة

و هو يعتمد على تفسير عكس الموقف السابق إذ يرى أنصاره انه ليس بالضرورة أن تحدث الهجمات الالكترونية أضرار مادية حتى تدرج تحت طائلة المادة 4/2 بل إن أي هجوم يتسبب في تعطيل لأنظمة الحاسب الرئيسية للدولة يكون سبب في تعطيل الأجهزة المسؤولة عن البنى التحتية يمكن اعتبارها استخدام للقوة وفقا للمادة 4/2. [1]

وهذا ما أكده المستشار القانوني السابق للوكالة القومية الأمريكية هارولد كوه harole koh بان الهجوم الالكتروني يشكل عدوانا يسمح باللجوء إلى حق الدفاع الشرعي و أن فرضيات الهجوم الالكتروني تستدعي تجاوز القانون الموجود .[2]

[1] شريف نسيم قلته، نفس المرجع السابق.

[2] Philipe LaGrange,internet et l'évolution normative du droit international : d'un droit international applicable à l'internet à un droit international du cyberespace ? , clloque de Rouen 2014 P 74

حيث انه في عام 2012 صرحت وزيرة خارجية الولايات المتحدة الأمريكية "هيلاري كلينتون" **بأنه فيما إذا "تعرضت بلادها إلى هجوم الكتروني فإنها سوف ترد على هذا الهجوم لأنه لا يقل عن التهديد أو الهجوم العسكري التقليدي**" إذ جاء حديثها يحمل في طياته حق الولايات المتحدة الأمريكية في الدفاع الشرعي إذا قالت.

"States, terrorist and those who would act as their proxies must know that the United State will protect our network, those who engage in cyber-attack should

face consequences and international condemnation in an interconnected world, an attack an one nation's network can be an attack on all.

في الأخير نستنتج أن الإدارة الأمريكية تؤيد موقف الفقهاء المؤيدين لأي هجوم الكتروني بغض النظر عن نتائجه إذ يعتبر بمثابة الهجوم العسكري التقليدي و هو بذلك يدخل تحت طائلة المادة 4/2 من ميثاق الأمم المتحدة.[1]

و بعد تعرضنا للمواقف الفقهية لفقهاء القانون الدولي العام و موقف الولايات المتحدة الأمريكية من تكييف الهجمات الالكترونية وفق المادة 4/2 نعرج في موضوعنا إلى دراسة حق الدولة في الدفاع الشرعي عند تعرضها للهجمات الالكترونية و ذلك من خلال المطلب الآتي:

المطلب الثاني: حق الدولة في الدفاع الشرعي ضد الهجمات الالكترونية لحماية أمنها ألمعلوماتي.

أصبح المجتمع الدولي أمام نمط جديد من الحرب يحمل أساليب جديدة و هجوم غير تقليدي في بيئة غير تقليدية و لها تداعيات غير محسوبة، و إذا ما نجحت تصيب المنشآت المدنية و بذلك فان هجمات الفضاء الالكتروني قد تتم من خلال الدخول إلى شبكات المعلومات بشكل غير شرعي مما يؤثر على البنية التحتية الكونية للمعلومات، هذه الشبكات إن أصابها الضرر فإنها تهدد بوقوع خسائر و أضرار مما يستدعي بروز عمليات دفاع شرعي تأتي في مضمونها مع الحق الذي اقره القانون الدولي إلا أن ظروف استخدام هذا الحق و شروطه الموضوعة في ميثاق الأمم المتحدة أصبحت غير ملائمة لممارسته داخل بيئة جديدة يفرضها استخدام الفضاء الالكتروني أثناء الدفاع الشرعي.[2]

[1] م.م/ ليث ناجح حميد، مرجع سابق،ص413

[2] عادل عبد الصادق، اسلحة الفضاء الالكتروني في ضوء القانون الدولي الانساني، مكتبة الاسكندرية، مصر، بدون طبعة، 2016.

الفرع الأول: السند القانوني للدفاع الشرعي ضد الهجمات الالكترونية.

جاء ميثاق الأمم المتحدة من خلال المادة 51 موضحا حق الدولة في الدفاع الشرعي في حالة تعرضها إلى اعتداء[1]، إذ نصت المادة على ما يلي: "**ليس في هذا الميثاق ما يضعف أو ينقص الحق الطبيعي للدول فرادى أو جماعات في الدفاع عن أنفسهم إذ اعتدت قوة مسلحة على احد أعضاء الهيئة، و ذلك إلى أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم و الأمن الدوليين**"[2] و كما أن عصبة الأمم كرست هذا الحق في ميثاقها السابق، وفي بروتوكول جينيف عام 1964 ذكر حق الدفاع الشرعي في المادة الثانية حيث جاء فيها "**أن الدول الموقعة قد اتفقت على أنها لن تلجأ إلى الحرب كوسيلة لفض النزاعات بأي حال إلا في حالة مقاومة العدوان**" .[3]

ولنتمكن من وضع إطار للدفاع الشرعي ضد الهجمات الالكترونية فلابد من النظر بداية في الشروط و الضوابط اللازمة لثبوت هذا الحق للدولة من اجل الدفاع عن نفسها دفاعا مشروعا.

من حيث الشروط فهي أن يكون الهجوم مسلحا ،و ثانيا إن يكون الهجوم واقعا و ليس احتمالي الوقوع ،و ثالثا أن يكون هذا الهجوم غير مشروع.

أما بالنسبة للضوابط فهي تناسب رد الفعل مع الاعتداء ،و ثانيا تقدير الضرورة و ثبوت نسبة الاعتداء للدولة المتهمة بالهجوم، وأخيرا إبلاغ مجلس الأمن فورا بالاعتداء ليتمكن من اتخاذ التدابير اللازمة لحفظ السلم و الأمن الدوليين.[4]

الفرع الاول: الاستنباط القانوني للدفاع الشرعي ضد الهجمات الالكترونية بحسب ما جاء في الميثاق من شروط.

اولا:بالنسبة لشرط أن يكون الهجوم مسلحا: اختلف فقهاء القانون الدولي في مدى إمكانية اعتبار الهجوم الالكتروني هجوما مسلحا يستوجب قيام حالة الدفاع الشرعي فظهرت ثلاث مذاهب:

---

[1] Svetlana zasova, la légitime defense desE tats et la guerre cybernétique, , clloque de Rouen, 2014 P 268

[2] المادة51 من ميثاق الامم المتحدة

[3] د/ عادل عبد الصادق، نفس المرجع السابق، ص 107

[4] د/ يحيى مفرح الزهراني، الأبعاد الإستراتيجية و القانونية للحرب السيبرانية، بحث منشور في مجلة البحوث و الدراسات، العدد 23، سنة 2017، ص ص 237 238

1- **المذهب الأول:** اعتمد فقهاء القانون الدولي على نظرية "**الوسيلة المستخدمة**" بمعنى أن الهجوم الالكتروني لا يتوفر فيه الصفة الأساسية التي ترتبط بالسلاح التقليدي، و يرون أن الهجوم الالكتروني يكون هجوما مسلحا إذا استخدم المهاجمون أسلحة عسكرية تقليدية، و استندوا في رأيهم هذا إلى المادة 41 من ميثاق الأمم المتحدة إذ اعتبرت أن الرسائل اللاسلكية و تعطيل أجهزة الراديو لا تصل إلى درجة القوة المسلحة ، وكذلك استندوا إلى قرار الجمعية العامة الذي وضع قائمة بالأعمال التي تؤسس ما يسمى بالعدوان و لم يكن من بينها الهجوم الالكتروني.[1]

2- **المذهب الثاني:** ويعتمد فقهاء هذا المذهب على نظرية (الأثر) بحيث تم تصنيف الهجوم الالكتروني كهجوم مسلح إذا كانت الآثار المترتبة على هذا الهجوم لا يمكن ترتيبها إلا عن طريق القوة المادية (الحركية) كالتلاعب بالأنظمة المالية و البنكية لدولة ما. [2]

3- **المذهب الثالث:** جمع فقهاء هذا المذهب بين نظريتين السابقتين إذ اعتمدوا على العلاقة السببية بين الفعل و الضرر النهائي الناتج من الهجوم، فعلى سبيل المثال الهجوم على البورصات أو الهجوم الالكتروني على الخطوط الجوية لدولة ،اوالهجوم الذي وقع على استونيا 2007 يعد هجوما الكترونيا و يستوجب قيام حق الدفاع الشرعي لان الضرر النهائي أو تأثيراته كافية لقيام هذا الحق.[3]

إن استهداف البنى التحتية للدول عن طريق شن هجوم الكتروني على بنيتها المعلوماتية الالكترونية يعد من أكثر المخاطر التي تهدد امن أي دولة و استقرارها و تعد انتهاكا صريحا لسيادتها مما يجعل انطباق الحق في الدفاع الشرعي واجبا.

و من وجهة نظر أخرى، يمكن القياس على الأجهزة النووية و المفاعلات النووية حيث اعتبرها الميثاق من قبل الأسلحة بالرغم من أنها ليست مدفعا و لا جنود، لهذا يمكن اعتبار الفيروسات التي تقوم بالاختراق و الهجوم في البيئة الالكترونية سلاحا له نفس تأثيرات بقية الأسلحة التقليدية و في بعض الأحيان قد تكن تأثيراته اشد دمارا منها.

ثانيا: بالنسبة لان يكون الهجوم واقعا: بمعنى انه لا يكفي مجرد التهديد بالهجوم أو يكون محتمل الوقوع فقط كامتلاك احد الدول المعادية لذلك الفيروس لا يكون سببا منطقيا للقيام بالدفاع

[1] م.م/ ليث ناجح حميد، نفس المرجع السابق، ص 415

[2] د/ يحيى مفرح الزهراني، نفس المرجع، ص 238

[3] م.م/ ليث ناجح حميد، نفس المرجع السابق، ص ص 416 417

الشرعي، و إنما يشترط إن يكون ذلك الهجوم قد تم بالفعل و قد يضاف إلى ذلك الخطر الوشيك الوقوع[1] و في هذه الحالة تستطيع الدولة المعنية إن تطبق ما يسمى في القانون الدولي بالدفاع ألاستباقي[2] أو الدفاع التوقعي[3].

ثالثا: بالنسبة لشرط عدم مشروعية الهجوم: بمعنى أن الهجوم الذي تعرضت له الدولة المعتدى عليها يكون هجوما غير مشروع كأن يكون عملا انتقاميا أو ثأريا يخرج من دائرة الأعمال المرخص بها من طرف مجلس الأمن الدولي أو يكون دفاعا شرعيا بسبب هجوم من تلك الدولة بداية و هذا الشرط من السهل التحقق منه و إثباته.[4]

الفرع الثاني: الاستنباط القانوني للدفاع الشرعي الالكتروني بحسب ما جاء في الميثاق من ضوابط

أولا: بالنسبة لضابط مبدأ التناسب: استخدم مصطلح مبدأ التناسب أول مرة في عام 1928 في أثناء تقنين قواعد الحرب الجوية في لاهاي،واستمر التنظيم الدولي في الإشارة إلى هذا المبدأ في الفقرة 5/ب من المادة 51 من البرتوكول الإضافي الأول لعام 1977.[5]

و يقصد بالتناسب بين عملية الدفاع الشرعي و الهجوم، على سبيل المثال لا يجوز لدولة الدفاع بالقيام بعملية غزو لإقليم الدولة المتهمة بالهجوم كرد فعل دفاعي لهجمة الكترونية، و هذا يشكل صعوبة في الفضاء الالكتروني،[6]

---

[1] د/ يحيى مفرح الزهراني، نفس المرجع السابق، ص 238

[2] **الدفاع ألاستباقي:** هو الحق في اتخاذ كافة التدابير الفعالة ضد أي عمليات أولية أو تطويرية لم يتم اكتمالها بعد و لاتشكل خطرا في وضعها الحالي و لكنها ستشكل خطرا و تهديدا اذ تم الانتهاء منها و تجهيزها....للمزيد اطلع على: يحيى مفرح الزهراني، نفس المرجع

[3] **الدفاع التوقعي:** (وسيلة احترازية) و هو الحق في اتخاذ كافة التدابير الفعالة ضد اي تهديد أو خطر لم يقع بعد، و لكن يشترط أن يكون هذا الخطر وشيك الوقوع، و قد اقر ذلك تقرير الأمم المتحدة 2004، و جعل للدول الحق في الدفاع الشرعي ضد أي خطر يهددها مادام وشيكا، و أيضا أكد الخبراء المشاركين في إعداد دليل تالين للقانون الدولي في الحرب الالكترونية على انه إذا كانت الهجمات السبرانية وشيكة فيحق للدولة الدفاع التوقعي.....للمزيد اطلع على: د/ يحيى مفرح الزهراني، نفس المرجع.

[4] د/ يحيى مفرح الزهراني، نفس المرجع، ص 239 .

[5] A.P.Dr. Ahmad oubais al-fatlawi,cyber attacks:its concept and arising international resbonsibility in the light of contemporary international organization, نفس المرجع السابق، 2016، ص ص 637

[6] د/ يحيى مفرح الزهراني، نفس المرجع السابق، ص 239

لان الفضاء الالكتروني يمر عبر حدود العديد من الدول، و من ثم فان الطابع الدولي لهذا الفضاء يجعل أيا من أطراف النظام الدولي معرضين للإصابة من جراء شن تلك الهجمات بحيث تمر (الهجمات) عبر دولة ثالثة أو أكثر غير متورطة في الصراع،[1] مثل ما وقع فعلا في الهجوم بفيروس ستاكس نت و الذي استهدف الأجهزة الالكترونية الإيرانية، فقد تم رصد ما يزيد عن 40% من أجهزة الكومبيوتر تضررت خارج الحدود الإيرانية، فلا بد من التأكد و التثبيت من إن عملية الدفاع ستنحصر في هدف معين و لا تطال دول أخرى ليس لها علاقة بالهجوم.[2]

إن السؤال الجوهري الذي يطرح بمناسبة التعرض إلى هذا المبدأ يتلخص في الآتي:**هل يمكن تأكيد احترام مبدأ التناسب قبل التخطيط لاستخدام وسائل أو طرائق سيبرانية معدة لأغراض هجومية؟**

في إشارة لتصريح لوزارة الدفاع الأمريكية عام 2012 و التي لم تفرق بين الهجوم الذي قد تتعرض له أكان بالصواريخ أو بالهجمات الالكترونية و اعتبارها مبررا للرد باستخدام القوة المسلحة المناسبة.[3]

ثانيا:بالنسبة لضابط تقدير الضرورة :والمقصود بهذا الضابط هو محاولة الدول الأطراف في النزاع اللجوء إلى الحلول السلمية كالقيام بالمفاوضات أو التحكيم قبل اللجوء إلى استعمال القوة والذي حرمها ميثاق الأمم المتحدة من خلال بنوده.

ثالثا :بالنسبة لضابط ثبوت نسبة الاعتداء للدولة المتهمة إن محاولة الدولة لإثبات الاعتداء الالكتروني الذي وقع عليها أمرا في غاية الصعوبة ،حيث انه ليس من السهولة تقديم الدليل مقنع يحدد مصدر الهجمة الالكترونية، وذلك لصعوبة التخفي وعدم ترك الدليل بعد تنفيذ عملية الهجوم.وحتى في حالة المقدرة على إيجاد دليل فذلك يستغرق وقتا طويلا فلابد من التحقق في إسناد الفعل إلى جهة معينة وهنا يمكن أن يطرح السؤال نفسه،إذا كان العالم الواقعي أغلقت فيه قضايا بإسنادها إلى فاعل مجهول فماهو الحل بالعالم الافتراضي[4]؟

---

[1] د/ عادل عبد الصادق، نفس المرجع السابق، ص 105

[2] د/ يحيى مفرح الزهراني، نفس المرجع ، ص 239

[3] A.P.Dr./ Ahmad oubais al-fatlawi,cyber attacks:its concept and arising international resbonsibility in the light of contemporary international organization,638ص،نفس المرجع السابق

[4] يحي مفرح الزهراني ، نفس المرجع السابق ،ص 240

المبحث الثاني: الحرب العدوانية الالكترونية في القانون الدولي الإنساني

صُبغ عصرنا الحالي بالصبغة الالكترونية، و رسمت جل ملامحه بالألوان التكنولوجية و هذا ما جعل أمنه يرتبط بالوسائل الرقمية و التقنية، و بفعل ذلك تحول العالم كله إلى كرة ضخمة من المعلومات الالكترونية و التي لازالت آخذة بالتضخم و التوسع، و بنت العديد من دول عالمنا المعاصر قواعدها البيانية بشكل يعتمد على شبكات الانترنيت، و مزايا التدفق ألمعلوماتي السريع، و سرية العمل المحسوب، و عدم الانكشاف الغير شرعي على فحوى المعلومات و غيرها من الصفات، احتل هذا الفضاء الناشئ مكانة مميزة بين الدول بحيث أصبح مجالا مستهدفا خاصة مع ارتفاع وتيرة التقدم التقني، شكل هذا الاستهداف المستمر منافسات شديدة بين الدول ادخلها فيما يعرف اليوم **بالحرب الالكترونية**[1] حيث تتسم هذه الحرب بالصمت و الظلام، و شبه انعدامية لمعرفة هوية المهاجم، و الخلفية الإيديولوجية، و غيرها من المواصفات التي تجعل منها حرب شديدة الخطورة[2] على البيئة الأمنية الالكترونية للدول. و مما سبق سنتطرق إلى الحرب الالكترونية من خلال التعريج على مفهومها وآلياتها في **المطلب الاول** حيث سنحاول دراسة مدى انطباق قواعد القانون الدولي الإنساني على الحرب العدوانية الالكترونية في **المطلب الثاني**.

المطلب الأول: الحرب العدوانية الالكترونية مفهومها و آلياتها

من اجل دراسة الحرب العدوانية الالكترونية كان ولابد ان نعرج على مفهومها وذلك في **الفرع الاول** ثم محاولة التعرف على الأسلحة الخاصة بها **الفرع الثاني** والجيوش الالكترونية كأحد آلياتها .

الفرع الأول: مفهوم الحرب الالكترونية

أصبحت تكنولوجيا المعلومات والاتصالات جزءاً لا يتجزأ من الحياة اليومية لكثير من الأشخاص في أنحاء العالم. والاتصالات الرقمية والشبكات والأنظمة تقدم موارد حيوية وتمثل بنية تحتية لا غنى عنها في كل جوانب المجتمع العالمي، وهي ضرورات لا يمكن لكثير من سكان العالم الازدهار أو حتى البقاء بدونها. وهذه الهياكل والأنظمة تمثل ميداناً جديداً تقترن به تحديات جديدة للحفاظ على السلام والاستقرار. وبدون آليات كفالة السلام فإن مدن العالم ومجتمعاته ستكون عرضة لهجمات تتسم بتنوع غير

[1] وليد غسان سعيد جلعود،دور الحرب الالكترونية في الصراع العربي الاسرائيلي ،اطروحة لاستكمال متطلبات الحصول على درجة الماجستيرفي التخطيط والتنمية السياسية بكلية الدراسات العليا في جامعة النجاح الوطنية ،نابلس،فلسطين،2013.

[2] وليد غسان سعيد، دور الحرب الالكترونية في الصراع العربي الاسرائيلي، اطروحة لاستكمال متطلبات الحصول على درجة ماجيستير في التخطيط و التنمية السياسية بكلية الدراسات العليا، جامعة النجاح الوطنية، نابلس فلسطين، 2013

مسبوق وغير محدود. وهذه الهجمات يمكن أن تأتي دون مقدمات. فالحواسيب والهواتف الخلوية تتوقف عن العمل فجأة كما أن شاشات آلات صرف النقد والآلات المصرفية تنطفئ في وجه العملاء وتتعطل أنظمة مراقبة الحركة الجوية والسكك الحديدية وحركة السيارات وتعم فوضى الطرق السريعة والجسور والممرات المائية وتتوقف السلع غير المعمرة بعيداً عن السكان الجائعين. ومع اختفاء الكهرباء تهوي المستشفيات والمساكن والمراكز التجارية بل ومجتمعات بأكملها في غياهب الظلام. ولن تستطيع السلطات الحكومية معرفة مدى الضرر أو الاتصالات ببقية العالم لإبلاغه بالكارثة أو حماية مواطنيها الضعفاء من الهجمات التالية. وهذه هي المحنة القاسية التي يواجهها مجتمع تعرض للشلل بسبب ضياع شبكاته الرقمية في لحظة واحدة. وهذا هو التدمير الذي يُمكن أن ينجم عن نوع جديد من الحروب هي "الحرب السيبرانية". [1]

و تعرف لجنة الصليب الأحمر الحرب الالكترونية (السيبرانية) بأنها "**عمليات ضد حاسوب او نظام حاسوبي من خلال دفق بيانات عندما تستخدم كوسيلة او أساليب حرب**"[2]، و اخطر صور الحرب الالكترونية (السيبرانية) هي العمليات التي تستهدف مواقع عسكرية أو أمنية إذ تمثل تعديا صارخا على سيادة الدولة و يكون ذلك عن طريق اختراق النظام المعلوماتي للبيئة الأساسية.

كما أن التكلفة الرخيصة نسبيا لأجهزة الإعلام الآلي المستعملة في شن الهجمات الالكترونية و التي أصبحت بديل لصرف أموال طائلة من اجل اقتناء أو صنع معدات عسكرية ضخمة جعل من إستراتيجية الحرب تتغير فقد أصبح المطلوب في الظروف الراهنة هو التدريب الالكتروني كإجراء أولي و سريع من اجل تجهيز ما يسمى "اللواء الالكتروني"[3].

الفرع الثاني: الأسلحة الالكترونية في الحرب العدوانية الالكترونية للأسلحة أهمية إستراتيجية مؤثرة في توازن القوى و بسط النفوذ و تمكن الدول من ممارسة الضغوط و التكتلات في ظل

[1] حمدون إ .توريه،البحث عن السلام السيبراني ،بقلم الامين العام للاتحاد الدولي للاتصالات وفريق الرصد الدائم لامن المعلومات ،جانفي 2011،تم الاطلاع عليه بتاريخ: 2018/2/12، الساعة 12:00، على الرابط:
https://www.shatharat.net

[2] الوثيقة IC/15/XXX 32 من المؤتمر الثاني و الثلاثون للصليب الاحمر و الهلال الاحمر، جنيف سويسرا، 8_10/ديسمبر/ 2015

[3] د/ يحيى مفرح الزهراني، نفس المرجع السابق ،ص ص ،226 236

بيئة أمنية يمتلكها الشك و مصالح حساسة قد تدمر في لحظات[1]، و لذلك فهي تتميز بقدرة تدميرية هائلة حتى انه قال احدهم انه" **لا أعرف على وجه التحديد السلاح الذي سيستخدمه الإنسان في الحرب العالمي الثالثة، لاكني اعلم انه سيستخدم العصي و الحجارة في الحرب العالمية الرابعة**".

و دفع التطور في مجال الفضاء الالكتروني إلى بروز ترسانة غير تقليدية لأسلحة الكترونية مختلفة.[2]

حيث قامت إيران بتأسيس مقر الدفاع الالكتروني في أكتوبر 2011 و أصبحت ضمن الدول التي تمتلك منظومة دفاعية كاملة في مواجهة تهديدات الحرب الالكترونية، و ظهرت هذه الإستراتيجية الدفاعية في احتواء الاختراق الالكتروني عن طريق فيروس" **دوكو doko**" في عام 2012 بعد ساعة من إطلاقه فقط.

كما قامت الحكومة البريطانية بتطوير برامج أسلحة الكترونية، و أقرت بأنها جزءا لا يتجزأ من ترسانتها الحربية و هو ما يمثل أول اعتراف رسمي بوجود هذه البرامج الالكترونية و تجري الولايات المتحدة سنويا محاكاة التعرض لحرب الكترونية ضمن قواتها المسلحة، حيث قامت بتشكيل قيادة عسكرية للفضاء الالكتروني وخصصت 500 مليون دولار في ميزانية عام 2012 لمواجهة التهديدات الالكترونية.

و تمتلك الصين و إيران و كوريا الشمالية و روسيا قدرات هجومية الكترونية بحيث يمكن أن تشكل بذلك خطرا محدقا بالولايات المتحدة الأمريكية و حلفائها، كما يتم بين الباكستان و الهند و ما بين الصين و اليابان و ما بين إسرائيل و العالم العربي سباق نحو التسلح الالكتروني.

و مع زيادة الاهتمام الأمني بالشبكة التحتية الحيوية مثل أنظمة الدفاع القومية، و صناعات أنظمة التحكم و شبكات الاتصال، إلى تصاعد الاهتمام العالمي لتجارة الأسلحة الالكترونية و تشير التقارير إلى ارتفاع سوق الأسلحة الالكترونية بنسبة 4,4% من عام 2015 إلى عام 2021[3].

الفرع الثالث: الجيوش الالكترونية لاختراق الحدود الافتراضية عادة ما تشكل الجيوش الحربية من ثلاثة اذرع عسكرية و هي القوة الجوية و القوة البرية و البحرية تستخدمها في الهجوم على

[1] د/ عادل عبد الصادق، القوة الالكترونية اسلحة الانتشار الشامل في عصر الفضاء الالكتروني، سلسلة قضايا استراتيجية، المركز العربي لابحاث الفضاء، عدد اكتوبر 2012

[2] سعيد درويش، نفس المرجع السابق، ص 125

[3] د/ عادل عبد الصادق، اسلحة الفضاء الالكتروني في ضوء القانون الدولي الانساني، نفس المرجع السابق، ص ص 73 74

أعدائها أو للدفاع عن سيادة أقاليمها، و لكن في عصر الانترنيت أصبحت رحى الحرب تدور في الفضاء الالكتروني مع خصوم مجهولي الهوية يهاجمون البنى التحتية الرقمية حيث تهدف هذه الهجمات إلى تدمير مثلا بنية الاقتصاد الذي بدأ يعتمد على المعلوماتية بشكل كبير.[1]

و إدراكا من الدول لواقع الفضاء الالكتروني و التغير الحاصل في إستراتيجية الحرب تنشط العديد من الدول خاصة الصين و روسيا و الولايات المتحدة الأمريكية، فرنسا، انجلترا، و الكيان الصهيوني و بعض الدول من الصف الثاني و الثالث مثل الهند و باكستان و إيران بصورة صامتة للتحسين في قدراتها الدفاعية الالكترونية و إنشاء جيوش الكترونية من خبراء قد يكونون نواة الجيش الالكتروني للدولة.[2]

بالنسبة لإيران فبعد الهجوم على المفاعل النووي "**بوشاهر**" سنة 2010 فقد طور الجيش الالكتروني برامج وقائية استباقية تمكنه من رصد الهجوم الالكتروني قبل او بعد وقوعه بما سهل قدرات إيران على التصدي له و أن تأسيس جيش إيراني الكتروني جاء كمنصة فعالة تتمتع بقدرة تدميرية هائلة لإلحاق الضرر بأعداء إيران و ذلك عندما يعجز الجيش الإيراني النظامي.[3]

المطلب الثاني: مدى انطباق قواعد القانون الدولي الإنساني على الحرب العدوانية الالكترونية

تنطبق قواعد القانون الدولي الإنساني بصفة عامة على النزاعات المسلحة دولية كانت او غير دولية هذا بالنسبة للنزاعات التقليدية المتعارف عليها في إطار العلاقات الدولية و التي نظمها القانون الدولي الإنساني من خلال اتفاقيات جنيف الأربعة 1949و البروتوكولين الإضافيين لهم1977، و لكن مع التطور التكنولوجي الحاصل ظهرت معطيات جديدة في مجال الحروب و النزاعات حيث أصبحت قوات اي جيش تستطيع ان تقهر اشد أعدائها دون أن تحرك ساكنا من أسلحتها أو إفرادها و بدون حتى إن تنتقل إلى ارض المعركة ،هذا ما أفرزته التكنولوجيا الحديثة التي جعلتنا نطرح السؤال التالي:

---

[1] د/ يحيى مفرح الزهراني، نفس المرجع السابق، ص 236

[2] علي حسن باكير، المجال الخامس الحروب الالكترونية في القرن ال 21، مقال منشور على موقع مركز الجزيرة للدراسات، تم الاطلاع عليه بتاريخ 2018/3/18، الساعة 12:00، على الرابط: https://studies.aljazira.net

[3] كفاح الزين، جيش ايران الكتروني، مقال منشور على موقع العربية تم الاطلاع عليه بتاريخ 2018/3/18، الساعة 12:00، على الرابط:https://alarabiya. net

بما أن النزاع انتقل إلى الفضاء الالكتروني، و الأسلحة المستعملة ذات خواص حديثة، و غير تقليدية فهل تنطبق قواعد القانون الدولي على هذا النموذج المستحدث من الحروب الالكترونية.؟ و التي كانت لها تداعيات جد خطيرة على الأمن ألمعلوماتي المرتبط بالبنى الأساسية للدول؟

و من اجل الإجابة على السؤال المطروح ارتأينا أن نقسم إجابتنا إلى ثلاث أقسام بحيث نسلط الضوء في دراسة تحليلية على مدى انطباق قواعد القانون الدولي الإنساني على الحرب العدائية الالكترونية هذا في **الفرع الأول**، وما جاء به دليل تالين من قواعد غير ملزمة تنظم الحروب الالكترونية كآلية لحماية امن المعلومات، ومدى توافقها مع ما أقرته اللجنة الدولية للصليب الأحمر هذا في **الفرع الثاني**.

الفرع الأول: دراسة تحليلية لمدى انطباق مبادئ القانون الدولي الإنساني على الحرب العدائية الالكترونية

لا يستطيع أكمل تقنين أن يبني صورة عن ما سيحدث في المستقبل، و القانون الدولي الإنساني لا يتضمن اي قواعد صريحة بشأن العمليات في الفضاء الالكتروني و الماسة بأمن المعلومات، حيث ان قواعده جاءت بصفة عامة من اجل توفير الحماية للمدنيين أثناء الحروب، و بالموازاة فإن الاعتداءات السيبرانية Cyber-attaques تعرض الأشخاص و الممتلكات للخطر و يعود ذلك الى ارتباط البنى التحتية الأساسية للدولة بالبيئة المعلوماتية الالكترونية و على سبيل المثال المنشآت المدنية مثل السدود والمستشفيات و شبكات الكهرباء هذه المنشآت تعتبر شريان الحياة بالنسبة للمدنيين أثناء الحروب العدائية الالكترونية[1] و من اجل ربط مبادئ القانون الدولي الإنساني و أهميتها بحماية امن المعلومات الالكترونية سنحاول إسقاط هذه المبادئ في دراسة تحليلية على الحرب العدائية الالكترونية: [2]

اولا: مبدأ التقيد في استخدام أسلحة الحرب

تعد البروتوكولات الإضافية لاتفاقية جنيف أكثر ملائمة لتقديم خريطة عمل للموقف من خلال استخدام الاعتداءات الالكترونية على المنظومة المعلوماتية للدولة وجاء ذلك واضحا في المادة 36 من البروتوكول الإضافي الأول إذ جاءت تنص على "**يلتزم أي طرف سامي متعاقد عند دراسة أو تطوير او**

[1] Climentines bories, « Appréhendre la cyberguerre en droit international. Quelques réflexions et mises au point », la revue des droit de l'homme (online) le 06/2014 , vu le 11/03/2018 sur le lien suivant URL :http:// revdh.revues.org/984,publisher center de recherche et d'études sur les droits fondamentaux , page 02

[2]

اقتناء سلاح جديد أو أداة للحرب أو إتباع أسلوب للحرب بأن يتحقق مما إذا كان ذلك محظورا في جميع الأحوال أو في بعضها بمقتضى هذا الملحق (البروتوكول) أو أي قاعدة أخرى من قواعد القانون الدولي"[1].

يفهم من محتوى المادة انه على كل طرف سامي متعاقد الالتزام بالتأكد من توافق الأسلحة الجديدة لقواعد القانون الدولي الإنساني قبل استخدامها، حيث طالبت الدول الأطراف في اتفاقيات جنيف أثناء المؤتمر الدولي الثامن و العشرين للصليب الأحمر و الهلال الأحمر المنعقد في عام 2003 بأن تخضع جميع الأسلحة الجديدة و وسائل و أساليب الحرب الجديدة لاستعراض دقيق و متعدد التخصصات و ذلك لضمان أن لا تتخطى التكنولوجيا الحماية القانونية المكفولة، و يعد استخدام العمليات الالكترونية الضارة بأمن المعلومات مثلا مناسبا على هذا التطور التكنولوجي السريع،[2] و هذا ما يقضي إلى أن الحديث عن فراغ قانوني فيما يخص الأسلحة الجديدة غير مبرر في كل الأحوال[3]، كما أن المادة 35 من نفس البروتوكول جاءت مشددة على عدم حرية الدول الأطراف في اختيار وسائل القتال و طرقه و استخدمت عبارة هذا الحق(أي اختيار وسائل القتال) ليس مطلقا بمعنى انه يجب ان يخضع لقواعد القانون الدولي الإنساني.[4]

ثانيا: مبدأ حضر الهجمات العشوائية

ورد مصطلح الهجمات العشوائية في البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لعام 1977 و تحديدا في الفقرة 4 و 5 من المادة 51 كما أشارت محكمة العدل الدولية للهجمات العشوائية في رأيها الاستشاري حول التهديد بالأسلحة عندما ذكرت "**على الدول ان لا تجعل من المدنيين هدف للهجوم**".[5]

---

[1] المادة 36 من البروتوكول الاضافي الاول1977،لاتفاقيات جنيف 1949.

[2] لجنة الصليب الاحمر، ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية،مقال تم الاطلاع عليه بتاريخ 2018/3/20، الساعة12:00، على الرابط: https://www.icrc.org

[3] ساعد العقون، ظوابط سير الاعمال العدائية في القانون الدولي الانساني، اطروحة مقدمة لنيل شهادة الدكتوراه في العلوم القانونية، تخصص القانون الدولي الانساني، جامعة الحاج لخضر باتنة، كلية الحقوق و العلوم السياسية، قسم الحقوق، سنة 2014/2015.

[4] المادة 35 من البروتوكول الاول 1977 الملحق باتفاقيات جنيف.

[5] مقال منشور على الانترنيت، على موقع مجلة المحقق الحلي للعلوم القانونية و السياسية، العدد الثاني، السنة الثامنة 2016 .

في العصر الحالي يتم ربط أجهزة الانترنيت و الاتصالات من اجل الإمدادات الضرورية للمدنيين و في نفس الوقت يستخدم العسكريون هذه الاتصالات مما يعرض المنظومة المعلوماتية المدنية الى الاستهداف أثناء الاعتداءات الالكترونية.

هذا ما كشفت عنه الاعتداءات التي تعرضت لها استونيا سنة 2007 أثناء الحرب الجورجية الروسية إذ كانت الاعتداءات الالكترونية غير تمييزية (عشوائية) أصابت أعيان مدنية حيث توقفت أرقام الطوارئ التي تستخدم في استدعاء الإسعاف و خدمات المطافئ لما يزيد عن ساعة و هي منشآت مدنية محمية بموجب قواعد القانون الدولي.[1]

ثالثا: مبدأ الحياد

يتميز الفضاء الالكتروني بطبيعته اللاحدودية إذ لا تقيده حدود الدول، فهو يتحرك عبر شبكات الاتصال و المعلومات التي لا تعترف بالحدود الجغرافية.

و جاء في اتفاقيات جنيف" **إن الدول الأطراف المشاركة في النزاع تمتنع عن تحريك القوات او ارسال مستلزمات الحرب أو الإمدادات عن طريق أراضي الطرف المحايد**"و استخدام الفضاء الالكتروني لشن اعتداءات الكترونية يجعل من أطراف النظام العالمي معرضين للإصابة من جراء تلك الاعتداءات و بالرغم من عدم كونها طرف في النزاع فإنها تصبح متورطة، و هذا ما يعد انتهاكا للقواعد قانون الدولي الإنساني،[2] و بالتالي مبدأ الحياد الدولي يكون من الصعب تطبيقه في حالة الاعتداءات الالكترونية دون المساس بقواعد القانون الدولي الإنساني، و هذا ما يجعل من الأمر أكثر خطورة على سلامة بنية النظام المعلوماتي للدول الأطراف في النزاع و حتى الأطراف المحايدة، حيث نعود و نذكر بواقعة الهجوم على المفاعل النووي بإيران (بوشاهر) سنة 2010 أين تسبب هذا الاعتداء الالكتروني بأضرار بالغة بالنسبة للمفاعل و أيضا انتقل الفيروس المستخدم (ستاكس نت) إلى مجموعة من الدول المحايدة الأخرى.

على الرغم بأن المسلم به في القانون الدولي أن الأسلحة الجديدة يجب ان تستخدم بحسب ماجاء في المادة 36 من البروتوكول الاول 1977 وفقا لقواعد القانون الدولي الإنساني، والذي قواعده تنظم مجريات العمليات العدائية،اذ تنشأ صعوبات في تفسير و تطبيق هذه القواعد على التكنولوجيات الجديدة للحرب نظرا لخصائصها الفريدة و عواقبها الإنسانية غير المتوقعة و قد تثير هذه الصعوبات مسألة ما إذا كان

[1] د/ عادل عبد الصادق، نفس المرجع السابق، ص 99

[2] د/ نفس المرجع ، ص 105

القانون موجود واضحا بما فيه الكفاية أو أن ثمة حاجة لتوضيح قواعد القانون الدولي الإنساني، أو وضع قواعد جديدة للتعامل مع هذه التحديات الجديدة؟[1]

الفرع الثاني:موقف دليل تالين واللجنة الدولية للصليب الأحمر من الحرب الالكترونية

تشكل الحرب الالكترونية العدوانية تعدي صارخ على المنظومة المعلوماتية و المرتبطة بالبنى الأساسية للدول في جميع الميادين الحساسة و الضرورية و التي تعتبر هي شرايين الحياة بالنسبة للمدنيين أثناء هذه الحروب و ذلك عند المساس بالاحتياجات الضرورية للسكان المدنيين كالمساس بالتحكم في مصادر المياه كالسدود أو كمصادر الطاقة كشبكات الكهرباء.

و حرصا من المجتمع الدولي بعد زيادة الاستخدامات المدنية و العسكرية للتكنولوجيا إخضاع هذا النوع من العمليات الالكترونية العدائية إلى قواعد القانون الدولي الإنساني و من المبادرات السباقة إلى صياغة قواعد تتناسب و هذا النوع المستحدث من الحروب هو ما قام به حلف الناتو حيث اشرف على إعداد "**دليل تالين للقانون الدولي المنطبق على الحرب السيبرانية**" سنة 2013[2] .

و هو نتاج لمناقشات و مشاورات[3] شارك فيها خبراء من حلف الناتو كما شاركت اللجنة الدولية

للصليب الأحمر[1]بصفة مراقب في إعداد هذا الدليل.

---

[1] الوثيقة 32/C/15/XXX، نفس المرجع السابق.

[2] ساعد العقون،نفس المرجع السابق، ص 318.

[3]توجهت الاعمال المتعلقة بالحرب الاليكترونية سواء التي تقوم بها الامم المتحدة او دليل تالين صوب تحديد قواعد القانون الدولي التي تطبق في حالة حرب اليكترونية بالنسبة لمجموعة الخبراء الحكوميين للامم المتحدةGGE وفي تقرير لهم سنة 2013 فانهم لم ياتوا على ذكر الدفاع الشرعي بل اكتفوا بان القانون الدولي و بالتحديد ميثاق الامم المتحدة يطبق في حالة الحرب الاليكترونية و يمكن ارجاع هذا الموقف الى غياب اغلب الخبراء. و هنا نتساءل هل هذا الغياب مقصود و مسيس؟

الا ان اهم المناقشات التي تطرقت الى موضوع الدفاع الشرعي و علاقته بالدفاع الاليكتروني تكت في ايطار دليل تالين اذ انه و بحسب مؤلفي الدليل فان الممارسة الدولية اقرت حق الدفاع الشرعي في حالة اعتداء مسلح من فاعلين غير الدولة و بالتالي فان اغلب المؤلفين اعتبروا بانه و بالرغم من غياب ادارة او رقابة في دولة فان مؤسسة متخصصة في تكنولوجيات الاعلام الالي او مورد الانترنات يمكنهم ان يكونوا محل لممارسة حق الدفاع الشرعي .

الا ان هذا الفريق مؤلفي الدليل انقسموا بشان مجموعة من النقاط بسبب الاعتداء: المجموعة الاولى اعتبرت بان الاعتداءات الالكترونية تكون فقط بدافع خاص مصلحة خاصة فانها لا تعطي الحق لممارسة الدفاع الشرعي و مجموعة ثانية اعتبرت بان الاسباب غير مهمة ..... للمزيد اطلع على :

Svetlana zasova, la légitime defense des etats et la guerre cybernétique, , clloque de Rouen 2014 P 271

و من أهم الرؤى الحديثة[2] التي جاء بها خبراء دليل تالين manuel de tallinnهي التأكيد على عدم وجود فراغ قانوني ينظم هذه الأساليب الحربية المستحدثة نظرا للتطور التكنولوجي الحاصل،[3] و هذا ما أكدته لجنة الصليب الأحمر حيث جاء في تقريرها عن القانون الدولي الإنساني و تحديات النزاعات المسلحة المعاصرة " على الرغم من حقيقة أنها جديدة نسبيا و تتطور بسرعة، فإن التكنولوجيا السيبرانية، كما ذكر سابقا، لا تحدث في فراغ قانوني....."[4]

أكدت "كوردولا دروغيه" المستشارة القانونية في اللجنة الدولية للصليب الأحمر Comité de la Croix–Rouge على أن الإطار القانوني القائم واجب التطبيق و يجب احترامه حتى في الفضاء السيبراني[5]

و بهذا تكون لجنة الصليب الأحمر اتفقت و ما جاء به خبراء دليل تالين من حيث أن الحرب الالكترونية لا تقع في فراغ قانوني بل هي مؤطرة تأطيرا قانونيا دوليا تنطبق فيه القواعد القانونية المطبقة أثناء النزاعات على مجريات الحرب الالكترونية و لتوضيح ذلك أفردنا في ما سيأتي لبعض القواعد القانونية غير الملزمة التي جاء بها دليل تالين لينظم مسألة الحروب الالكترونية محاولين إبراز أن هذه القواعد تتوافق و التوجهات الرئيسية لمبادئ لجنة الصليب الأحمر.

و تجدر الإشارة في هذا الطرح أن كل هذه المساعي الدولية هي من اجل إيجاد أرضية قانونية تشمل ماهو حاصل من تحديات في الفضاء الالكتروني الهدف منه تحقيق اكبر قدر ممكن من الأمن المعلوماتي للدول في إطار العلاقات الدولية.

---

[1] اللجنة الدولية للصليب الأحمر: اللجنة الدولية للصليب الأحمر منظمة مستقلة ومحايدة تقوم بمهام الحماية الإنسانية وتقديم المساعدة لضحايا الحرب والعنف المسلح. وقد أوكلت إلى اللجنة الدولية، بموجب القانون الدولي، مهمة دائمة بالعمل غير المتحيز لصالح السجناء والجرحى والمرضى والسكان المدنيين المتضررين من النزاعات. وإلى جانب مقرها الرئيسي في جنيف، هناك مراكز للجنة الدولية في حوالي 80 بلداً ويعمل معها عدد من الموظفين يتجاوز مجموعهم 12000 موظف. هذا وفي حالات النزاع، تتولى اللجنة الدولية تنسيق العمل الذي تقوم به الجمعيات الوطنية للصليب الأحمر والهلال الأحمر واتحادها العام. واللجنة الدولية هي مؤسس الحركة الدولية للصليب الأحمر والهلال الأحمر ومصدر إنشاء القانون الدولي الإنساني لاسيما اتفاقيات جنيف.....للمزيد اطلع على: http:// www.wikipidia.org

[2] Une cyberarme : serait, pour reprendre le manuel de tallinn, tout dispositif, matériel, instrument,mécanisme, équipement ,ou logiciel destiné à être utilisé pour mener une cyberattaque…….. VOIR : Abdelwahab Biad cyberguerre et lex specialis évolution ou révolution 2014 P 262.

[3] ساعد العقون، المرجع السابق، ص318.

[4] الوثيقة 32/IC/15/XXX، نفس المرجع السابق .

[5] مقابلة مع المستشارة " كوردولا دروغيه" بتاريخ 2011/8/16 على موقع اللجنة الدولية للصليب الاحمر، على الرابط: https//: www.ICR.org

أولا: حظر مهاجمة المدنيين عن طريق الاعتداءات الالكترونية على المنظومة المعلوماتية

جاء في القاعدة 32 من دليل تالين[1] انه يحظر مهاجمة المدنيين أثناء النزاع الالكتروني كما تضمنت القاعدة 37 حظر مهاجمة أغراض المدنيين من أعيان و معدات.....الخ[2]، و هذا تطبيقا لمبادئ القانون الدولي الإنساني الذي ينص في اتفاقياته الأربعة 1949 و البروتوكولين الإضافيين 1977 على انه أثناء النزاعات يحظر المساس بالمدنيين و الأعيان المدنية كما يتماشى هذا مع الدور الرئيسي للجنة الدولية للصليب الأحمر حيث تذكر اللجنة أطراف النزاع بتوخي الحرص بشكل مستمر من اجل حقن دماء المدنيين، فالحروب لها قواعد و حدود تنطبق أيضا على الحروب الالكترونية بنفس القدر في حالة استخدام البنادق و المدفعية و الصواريخ.[3]

ثانيا: في إطار حماية البيانات المدنية الأساسية

أفردت قواعد دليل تالين حماية خاصة لفئات معينة من المدنيين كالفرق الطبية عن طريق حماية حواسبهم من الاستهداف ضد أي هجوم الكتروني من خلال القاعدة 71 من الدليل[4]، و بالموازاة جاء في تقرير اللجنة الدولية للصليب الأحمر سنة 2015 أن حذف البيانات أو العبث بها يمكن أن تؤدي بسرعة إلى الشلل الكامل لخدمات الحكومة و خاصة تلك المتعلقة بفئات معينة من الأعيان المدنية و التي تتمتع بحماية خاصة بموجب القانون الدولي الإنساني فالالتزام باحترام و حماية المرافق الطبية يجب ان يفهم انه ينطبق على البيانات الطبية التي تخص هذا المرفق.[5]

ثالثا: حماية البيئة المعلوماتية عن طريق منع الهجمات العشوائية

تطرق معدوا دليل تالين في القاعدة 56 إلى انه من الضروري أثناء الحرب الالكترونية توخي الحذر أثناء اختيار الأهداف و يكون ذلك بكل دقة[6] حتى لا تكون الأعيان المدنية عرضة لذلك الاعتداء و هو ما يحظره مبدأ التميز في القانون الدولي الإنساني.

---

[1] دليل تالين:

[2] سعيد درويش، امرجع السابق، ص123.

[3] نفس المرجع، ص 123.

[4] نفس المرجع، ص 121.

[5] الوثيقة 32/IC/15/XXX، نفس المرجع السابق.

[6] tallinn

و هذا ما أقرته اللجنة الدولية للصليب الأحمر في مؤتمرها 32 حيث ترى انه من بين التدابير الواجبة حماية المدنيين من حظر العمليات السيبرانية العشوائية بفصل البيئة التحتية المعلوماتية العسكرية عن البيئة التحتية المعلوماتية المدنية.

وفي الأخير لايمكننا التنصل من أحكام القانون الدولي الإنساني بحجة أن ميدان الحرب هو الفضاء السيبراني، فبالرغم من ان الحروب الجوية و البحرية تكونت مجالاتها طبيعيا إلا أن الحرب الالكترونية مجالها تكون بفعل الإنسان و بغض النظر عن هذا الاختلاف بين هذه المجالات تبقى قواعد القانون الدولي الإنساني تنطبق جملة إن لم نقل تفصيلا على الحرب الالكترونية المعلوماتية، و هذا ما أكدته محكمة العدل الدولية بقولها "**ان مبادئ و قواعد القانون الدولي الإنساني المنطبق في النزاع المسلح تنطبق على جميع أشكال الحروب و على جميع أنواع الأسلحة بما في ذلك تلك المستقبلية**".[1]

كما نخلص أيضا إلى القول بأن دليل تالين هو الوثيقة القانونية الوحيدة إلى حد الآن (2018) التي تتضمن قواعد القانون الدولي الإنساني

و التي تنظم مسألة اللجوء إلى الحرب الالكترونية، و بالرغم من انها قواعد غير ملزمة إلا أنها في الوقت الحالي يأخذ بها أشخاص المنتظم الدولي على سبيل الاستئناس.

كما تجدر الإشارة بأن هذه القواعد غير الملزمة قد تكون بداية لتكوين الركن المادي لعرف دولي ينظم مسألة الحرب العدوانية الالكترونية في انتظار انقضاء فترة زمنية غير معلومة لتبلور و تكون الركن المعنوي لهذا العرف الدولي تمهيدا لظهور قواعد قانونية دولية ملزمة تنظم مسألة الحروب المعلوماتية الماسة بشكل خطير بأمن المعلومات الالكترونية.

المبحث الثالث: نحو البحث عن السلام السيبراني

في السنوات الأخيرة تزايد عدد الدول الأعضاء التي أصبحت تقر بأن امن المعلومات على الصعيد الدولي آخذ في اكتساب الأهمية كموضوع من مواضيع الساعة، و ينبغي النظر إليه باعتباره مسألة لها وزنها في جدول المهام الأمنية الدولية. و تحولت المخاطر السيبرانية بما تمثله تهديد للفرد و المجتمع و الدولة إلى مسألة تدرج على لوائح الطوارئ الدولية حيث أصبحت من المسائل التي لابد معالجتها قبل أن تتحول إلى سبب لاندلاع الحروب، و الكوارث تهدد البشرية جمعاء.[2]

[1] سعيد درويش، نفس المرجع السابق، ص 242

[2] د/ منى الاشقر جبور، نفس المرجع السابق، ص 47

و مما سبق يتضح لنا انه حان الوقت للمبادرة فورا لإيجاد سبل لإقرار تشريعات و قوانين دولية لمكافحة الجرائم المعلوماتية الماسة بأمن و استقرارية الدول و أيضا اعتماد آليات تعاون تقني و فني و قضائي لأجل القضاء على هذه الظاهرة المستحدثة وليدة التطور التكنولوجي الحاصل.

و لدراسة ما سبق طرحه قسمنا هذا المبحث إلى:

المطلب الأول(برنامج الأمن السيبراني العالمي للاتحاد الدولي للاتصالات **ITU**)**والمطلب الثاني** (اقتراح إنشاء تنظيم دولي كحماية لأمن المعلومات الالكترونية)

المطلب الأول: برنامج الأمن السيبراني العالمي للاتحاد الدولي للاتصالاتITU

يقوم الاتحاد الدولي كمنظمة متخصصة تابعة للأمم المتحدة بتعزيز الأمن المعلوماتي (السيبراني) و اعترفا بخبرة الاتحاد الطويلة و قدرته و تجربته فقد عينه قادة العالم و الحكومات بصفته الجهة الميسرة بتولي زمام الأمور من خلال اتخاذ خطوات ملموسة لكبح التهديدات و أوجه عدم الأمن فيما يتعلق بمجتمع المعلومات[1] Société de l'information (بناء الثقة و الأمن العام للاتحاد الدولي في استعمال تكنولوجيا المعلومات و الاتصالات).

حيث أطلق الأمين العام للاتحاد الدولي للاتصالات سنة 2007 بموجب القرار 140 (برنامج الأمن السيبراني العالمي GCA) و أعيد التأكيد على هذا البرنامج من طرف الدول الأعضاء في عام 2010 بموجب القرار 130 (المراجع في غوادا لاخارا_2010) كما قام الاتحاد بمبادرة لمكافحة الإرهاب السيبراني MPACT و ذلك عن طريق شراكة دولية متعددة الأطراف و أقام عدة فرق من اجل التصدي لحوادث الأمن (FIRST) كما يعطي الاتحاد أولوية عالية في أعماله المتعلقة بأمن شبكات المعلومات و الاتصالات، و يرمي برنامج الأمن السيبراني إلى تحقيق سبعة أهداف إستراتيجية رئيسية هي[2] :

- تبني نهج واضح من اجل استحداث قوانين نموذجية لمكافحة الجريمة السيبرانية تكون قابلة للتطبيق عالميا و متوافقة مع التدابير التشريعية الوطنية الدولية الحالية.
- وضع استراتيجيات لإيجاد إطار عالمي للرصد و الإنذار و لاستجابة للحوادث لضمان التنسيق عبر الحدود بين المبادرات الجديدة و الحالية.

---

[2] حمدون إ.تورية، برنامج الأمن السيبراني العالمي للاتحاد الدولي للاتصالات، حقوق الطبع محفوظة للعمل الجماعي 2011، ص 97 ،الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء....وللمزيد اطلع على الرابط:strategy@itu.int .

– وضع مقترحات بشأن إطار لإستراتيجية عالمية لأصحاب المصلحة المتعددين لتحقيق التعاون و الحوار و التنسيق على الصعيد الدولي في جميع المجالات.[1]

الفرع الأول: تدابير قانونية إجرائية وتقنية وبناء القدرات

يقوم الاتحاد حاليا بمساعدة الدول الأعضاء في فهم الجوانب القانونية للأمن السيبراني من اجل تنسيق أطرها القانونية و الخاصة بالجرائم المعلوماتية و يعزي ذلك للارتفاع الواضح في هذه الجرائم المعلوماتية نظرا لان الشبكة (الانترنيت) أثبتت أنها في مجال التجارة الالكترونية منخفضة المخاطر، و ذلك لوجود ثغرات في التشريعات الوطنية و الإقليمية و الهدف من هذه الركيزة هو تأسيس تشريعات وطنية موحدة تكون قابلة للتطبيق و التنفيذ على الصعيد الدولي.

كما يحتل الاتحاد الدولي للاتصال و لاسيما قطاع تقييس الاتصالات (ITU_T) مكانة فريدة في أعمال التقييس المتعلقة بتكنولوجيا المعلومات و الاتصالات و من اجل الحد من المخاطر السيبرانية و إيجاد تدابير وقائية يعمل الاتحاد بشأن توفير امن للبيانات المتعلقة من طرف إلى طرف و قد انشأ فريق متخصص معني بالشبكات الذكية اعتمد آليات فعالة لتحقيق هذه الأهداف.

وهناك حاجة ماسة إلى بناء القدرات للدول الأعضاء و غيرها من الأطراف لاستحداث ثقافة استباقية مستدامة من اجل إدراك الخاطر المحتملة في الفضاء المعلوماتي حتى يتوفر فضاء آمن لمستخدمي تكنولوجيا المعلومات و الاتصالات و في إطار ولاية الاتحاد الدولي للاتصالات و المتمثلة في مساعدة الدول الأعضاء في تطوير قدراتها في مجال الأمن السيبراني قام الاتحاد بعدة نشاطات في هذا المجال مثل دليل الأمن السيبراني الوطني للاتحاد، و موارد الاتحاد المتعلقة بالجريمة المعلوماتية، و مجموعة أدوات الاتحاد للحد من البرمجيات الخبيثة. [2]

الفرع الثاني : التعاون الدولي و الهياكل التنظيمية

تؤكد ركيزة التعاون الدولي على وضع استراتيجيات من اجل الحوار و التنسيق حيث يمثل التعاون في إطار مؤسسة امباكت تقدما كبيرا في هذا المجال اذ يوفر محفلا دوليا لمناقشة السياسة العامة و تبادل المعلومات.

---

[1] الوثائق الصادرة عن القمة العالمية لمجتمع السلم، جنيف 2003 _ تونس 2005، الاتحاد الدولي للاتصالات،موقع الأمم المتحدة، ديسمبر 2005.

[2] حمدون إ.تورية،نفس المرجع السابق،ص ص ص98 99 100.

وينص إعلان المبادئ الصادر عن القمة العالمية لمجتمع المعلومات على تعزيز إطار الثقة العالمية بما في ذلك امن المعلومات و الشبكات و بناء الثقة بين مستعملي تكنولوجيا المعلومات و الاتصالات و من اجل تحقيق ذلك لا بد من تشجيع ثقافة عالمية بشأن الأمن المعلوماتي عن طريق التعاون الفعال بين جميع الأطراف.

وترمي ركيزة إقامة هياكل و استراتجيات تنظيمية للمساعدة في منع شن هذه الهجمات ضد البنى التحتية الحيوية للمعلومات و كشفها و الاستجابة لها و في هذا الإطار تتعاون الدول الأعضاء مع الاتحاد لتحديد احتياجاتها الخاصة في مجال الأمن المعلوماتي، و قد تكون هذه المساعدة على شكل إنشاء أفرقة وطنية للاستجابة للحوادث الحاسوبية (CIRT).

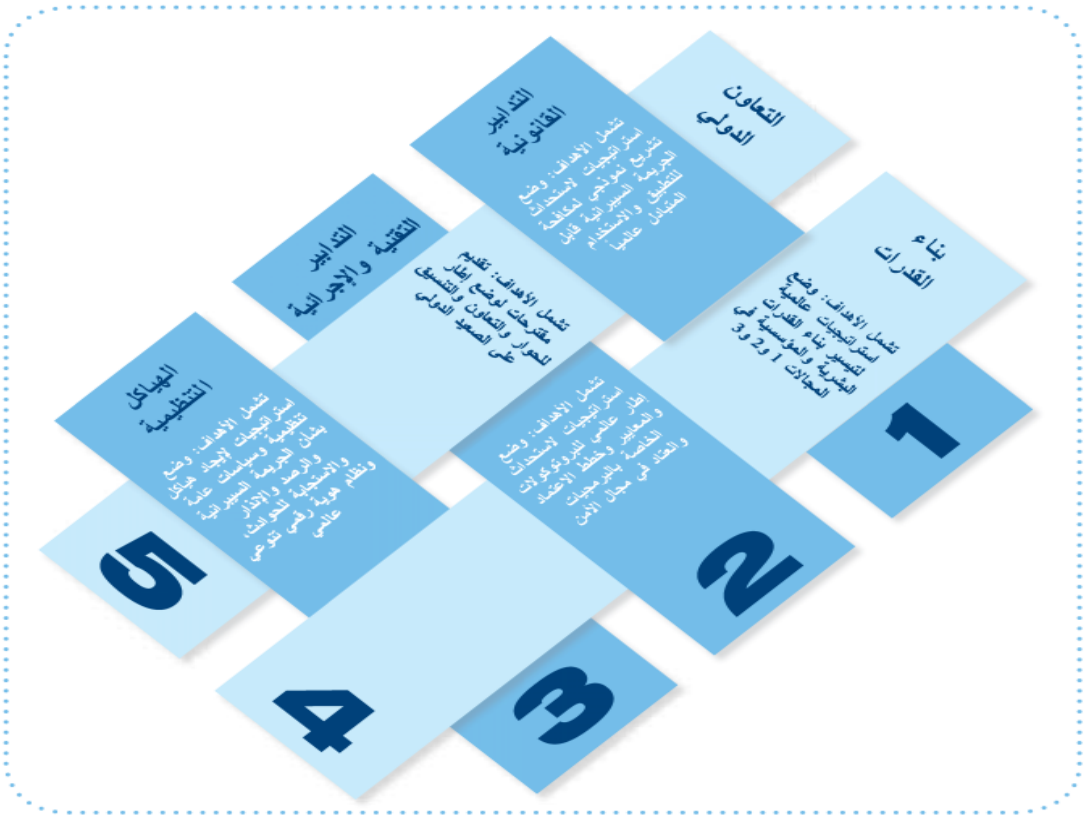
كما انه في اطار التعاون بين الاتحاد الدولي للاتصالات و الشراكة الدولية متعددة الأطراف لمكافحة الإرهاب السيبراني (IMPACT) لعب مركز الاستجابة العالمية (CIRT) دورا محوريا من اجل تدعيم هذا التعاون.

و بعد ان ابرم الاتحاد الدولي للاتصالات مذكرة للتفاهم اصبح المقر الرئيسي لمؤسسة امباكت بماليزيا و هو المقر الفعلي لبرنامج الأمن السيبراني العالمي، و تعتبر هذه الشراكة بمثابة خطوة منطقية في اطار التصدي العالمي للتهديدات السيبرانية و قد انظم الى هذا التعاون ما يقارب 60 دولة.

كما أن مركز الاستجابة العالمي مجهز بغرف لإدارة الأزمات و أجهزة اتصالات و غيرها من المرافق الضرورية لتأدية دوره الرئيسي في تحقيق أهداف برنامج الامن السيبراني العالمي، كما ان برنامجي نظام الانذار المبكر (NEWS) و منصة تطبيقات التعاون الآمن الكترونيا من اجل الخبراء ESCAPE[1] يلعب دورا محوريا في تحديد التهديدات السيبرانية و أيضا يوفر للدول فرصة النفاذ إليها (التهديدات) كما تقدم مؤسسة امباكت أيضا منحا دراسية للدول الأعضاء من البلدان النامية و ذلك لحضور دورات تدريبية.[2]

[1] ESCAPE: هو أداة الكترونية تمكن الخبراء السيبرانيين المخولين في بلدان مختلفة من تجميع الموارد و التعاون فيما بينهم..... للمزيد اطلع على: حمدون إ.تورية، برنامج الامن السيبراني العالمي للاتحاد الدولي للاتصالات، حقوق الطبع محفوظة للعمل الجماعي 2011، الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماءعلى الرابط:strategy@itu.int .

[2] حمدون إ.تورية،نفس المرجع،ص99.



الشكل رقم 01: برنامج الأمن السيبراني العالمي(الركائز الاستراتيجية الخمس)

المطلب الثاني: اقتراح إنشاء تنظيم دولي للانترنت كحماية لامن المعلومات الالكترونية.

تقضي طبيعة الفضاء الالكتروني و واقع انتشار الانترنت كشبكة اتصالات عالمية البحث عن الجهة التي تستطيع حكم الانترنت و السيطرة عليها، و لقد كان موضوع حكومة الانترنت واحدا من الأسئلة التي جرت مناقشتها خلال عملية التحضير لمؤتمر القمة العالمي للأمم المتحدة لمجتمع المعلومات و يعود ذلك إلى تمسك الدول جميعها بالسيادة ضمنيا و طرحه خلال المناقشات المتعلقة بإدارة الانترنت.[1]

و من خلال ما سبق يتضح انه لا بد للمنظمة الدولية التي ستقوم بإدارة الانترنيت من أن تتوفر فيها مجموعة من الشروط أهمها الشخصية القانونية الدولية و الأجهزة و الإدارة المستقلة و أن تنشأ باتفاق دولي و ان تتوافر على الأجهزة الدائمة الخاصة بها (جمعية عامة، مجلس تنفيذي، أمانة عامة) و إرادة ذاتية تميزها عن شخصية أعضائها، و أيضا الصفة الدولية أي أعضاءها دول و تكون مختصة ضمن

[1] مصطفى بن عصام نعوس، نفس المرجع السابق، ص 364.

منظومة دولية الأمم المتحدة غير أنها تتميز من ناحية شروط العضوية لأنه يسمح لأصحاب الحصص بالانتساب إليها.

الفرع الأول:اقتراح منظمة دولية متخصصة من منظومة الأمم المتحدة

بمعنى يجب ان تكون من ضمن عائلة الأمم المتحدة

أولا: ينبغي لهذا الكيان أن يكون تحت مظلة الأمم المتحدة و إشرافها

بحيث تتوافق أهدافه و مبادئه مع ما جاء به ميثاق الأمم المتحدة و لا تأثر فيه التقلبات السياسية إداريا كما انه من الضروري أن يكون هذا الكيان متخصص إداريا و فنيا.[1] و إن يتمتع بسلطة تنفيذ القرارات الصادرة عنه، كما يتبنى الإعلانات و المبادئ الصادرة عن الأمم المتحدة بشأن حقوق الإنسان التقليدية و الرقمية[2] و أن يكون له القدرة و القوة على الإنفاذ لاستمرار الانترنيت.

ثانيا: أن يكون التنظيم دوليا

يجب أن يكون هذا التنظيم الخاص بإدارة الانترنت تجمعا إداريا لعدد من أشخاص القانون الدولي و يتم إنشاءه بموجب اتفاق دولي و يتمتع بإدارة ذاتية و مزود بنظام قانوني متميز. و أجهزة مستقلة يمارس من خلالها مهامه و نشاطاته، و... من أن يؤسس هذا الكيان على شكل شركة لان تأسيس الشركة يحتاج إلى التأسيس في دولة ما، و قد تكون قوانين هذه الدولة متوافقة مع القانون الدولي العام او غير متوافقة معه كما هو الوضع في شركة الأيكان.

الفرع الثاني: منظمة غير اعتيادية من حيث العضوية فيها و آلية المشاركة

تقوم طبيعة نشاط الانترنيت على تقنية إدارية متميزة و متطورة

اولا: مشاركة المنظمات غير الحكومية و المجتمع المدني و القطاع الخاص

---

[1] المرجع نفسه، ص ص 476 477

[2] يعاني الأفراد حول العالم من انتهاكات عديدة لحقوق الإنسان ومنها حرية التعبير التي تجد لها تطبيقا رحبا بالانترنت وتثير سؤالا يتعلق بمعرفة فيما إذا كان حق النفاذ إلى الانترنت نتيجة طبيعية لحق التعبير أي انه حق للإنسان وهنا مغزى حرية التعبير حيث أصبح الارتباط والاتصال بالشبكة حقا معترفا به مند إعلانات المبادئ للقمة العالمية لمجتمع المعلومات وعلى الرغم من ذلك نجد دول لديها فيض هائل من الاتصال والتواصل تم تسميتها بدول ميسورة المعلومات على العكس من دول أخرى تفتقد لأدنى شروط الاتصال والتواصل العالمي تم تسميتها بالدول معدومي المعلومات وبكلمات أخرى انقسام رقمي آو فجوة رقمية ...للمزيد اطلع على مصطفى بن عصام نعوس،ص427.

أبدى جميع المشاركين في المؤتمر العالمي لمجتمع المعلومات الذي نعقد في جنيف 2003 و تونس 2005 من منظمات غير حكومية و أصحاب الحصص و المنظمات الدولية وجهات نظرهم حول كيفية الانتقال إلى عالم المعرفة و أبدت الأمم المتحدة إرادتها في استمالة جميع الأطراف للمساهمة في إدارة الانترنت و ترى الولايات المتحدة الأمريكية انه في حال فقدت إدارتها للانترنيت نتيجة الضغوط الدولية، ستعود و تشارك في إدارتها على أنها الطرف المساهم و صاحب الحصة الأكبر.

و تجدر الإشارة أن الدول المختلفة و الدول العربية ستكون مشاركتها شبه وهمية في عملية التنظيم و الإدارة للانترنت و هذا يعتبر خطرا محدق بالدول سابقة الذكر و ما عليها إلا بمطالبة تحويل القيادة لانترنت بالاستناد على قواعد القانون الدولي إلى تراث مشترك للإنسانية على غرار ما تم طرحه و معالجته و تنفيذه في مسألة أعالي البحار سابق

ثانيا: ان يكون هذا الكيان معبرا عن الإرادة الجماعية للدول و المنظمات

إن تدعيم الجهود الوطنية بإقامة تعاون دولي عالمي و إقليمي فعال بين بين الحكومات و القطاع الخاص و المجتمع المدني و أصحاب المصلحة الآخرين، يجب بالضرورة تنظيمه في شكل اتفاق دولي حتى يأخذ طابع الإلزامية للحكومات و للدول، كما أن التكامل الإقليمي يسهم في تنمية مجتمع المعلومات العالمي و يجعل التعاون الوثيق داخل الأقاليم آمر لا غنى عنه.

و قد جاء في تقرير الفريق العامل المعني بإدارة الانترنت و من خلال مناقشة السياسة العامة العالمية و الإشراف بأن الفريق العامل يسلم بأن اي شكل تنظيمي لمهمة إدارة الانترنت ينبغي له التمسك بالمبادئ التالية:

- لا يجوز لحكومة واحدة بسط نفوذها في مجال الإدارة الدولية للانترنت
- أن تمارس الشفافية و التعددية اللغوية و الديمقراطية أثناء الإدارة و الإشراف.[1]

و في الاخير نخلص الى انه على الرغم من أن التهديدات التي تصاحب التطور السيبراني وزيادة الاعتماد على تكنولوجيا المعلومات والاتصالات تتسم بالخطورة، تظل الفوائد المحتملة أهم بكثير. وعلى الرغم من أننا شهدنا فعلاً بعض مخاطر الحرب السيبرانية، فقد جنيْنا أيضاً فوائد الفضاء السيبراني كما أن إمكانية تحقيق فوائد في المستقبل لا حدود لها. ويتعين علينا، ونحن نمضي قدماً، أن نعالج بصورة استباقية مسألة كيفية الاستمرار في زيادة الاعتماد على الفضاء السيبراني وتطويره وتكامله فضلاً عن

[1] مصطفى بن عصام نعوس، نفس المرجع السابق، ص ص 478 481

كيفية حماية الموارد وتهيئة بيئة مستقرة لاستمرار ازدهار البنية التحتية والتكنولوجيات الجديدة وكفالة سلام دائم. وعلى الرغم من أن العديد من النهج الحالية تمثل خطوات إيجابية، فإنها لا ترتقي إلى التوقعات وقد لا يوفر كثير منها أكثر الحلول كفاءة. ولكن هناك إمكانية كبيرة تقوم على مبدأ يفيد أن العمل معاً يمكّن من تحقيق هذه الأهداف وتجنب الظروف العصيبة للنزاع السيبراني، إننا نقترب من حافة هاوية خطيرة في الوقت الذي يلقي فيه الجانب الأسود للإنترنت بظلاله لحجب الفوائد الهائلة لتكنولوجيا المعلومات والاتصالات وزعزعة النظام العالمي لقد حان الوقت الآن لإحلال السلام السيبراني[1].

.

1

يطيب لي أن ابدأ تسطير الخاتمة بكلمات هي بحق معبرة فحواها ليس الغرض من الخاتمة تلخيص الدراسة و استعراض أبوابها بما تضمنته من فضول و مباحث بشكل منسق يسلم بكل شاردة و واردة فهذا آمر يجاوز حدودها و إنما الغرض منها إبراز مغزى الدراسة.

و نضيف الى هذه الأسطر أن الخاتمة تحوي فكرة الباحث و رؤيته لموضوع البحث، و تعرج بخلاصة العمل القانوني فهي إن صح الوصف و التشبيه _نهاية المطاف و كشف النقاب الذي يأتي في نهاية العمل_ .

ملخص الدراسة:

لقد حاولنا عبر هذه الدراسة أن نطرح الموضوع على بساط البحث بحيث تعرضنا أولا: في الفصل الأول للحديث عن ما خلفته التطورات التقنية و التكنولوجية الحديثة من تهديدات أمنية معلوماتية خاصة على مستوى الأمن الدولي الذي أصبح أكثر عرضة و خطرا نظرا لسهولة الانكشاف المعلوماتي الذي وفرته وسائل الاتصال و التواصل الحديثة و انتشار أنواع المعلومات بزخم كبير على شبكات الانترنت ترافقها العديد من أساليب الجرائم المعلوماتية في طابعها الدولي و الوطني كالتجسس و الاختراق الأمني المعلوماتي الرامي للاستحواذ على المعلومات المنتشرة عبر الفضاء الالكتروني بكافة الطرق و الوسائل.

حيث عرضنا لنماذج تطبيقية و قضايا عملية في مجال الجرائم المعلوماتية و الانترنت الماسة بأمن و استقرار الدول و سبل مكافحتها مع التركيز افضل ما توصل له المجتمع الدولي من حلول قانونية عملية في مكافحة هذه الجرائم المستحدثة

التعقيب: في الميكرو.....

كما أن مجال الإجرام المعلوماتي تناهى بشكل ملحوظ على الصعيدين الوطني و الدولي و ظهرت الجرائم الإرهابية في صورتها الرقمية حيث صخر الإرهابيون التكنولوجيا المعاصرة لتنفيذ أفعاله الجنائية و تحقيق غاياتهم الإجرامية و من أبرزها بث الرعب و الخوف لدى أفراد و تعد ذلك إلى حكومات و الدول.

.....

و في الأخير لا يسعنا من خلال مذكرتنا إلا أن نوجه الدعوى إلى الباحثين و الدارسين أن يتصدوا لهذا النوع من الدراسات القانونية التي لا تزال لحد اليوم محتشمة رغم ما يحمله الزحف المعلوماتي من مخاطر.

نحن لا نزعم أننا من خلال هذا البحث قد وصلنا إلى منتهى جادة الصواب لكن أملنا أن يحقق القدر المعقول من المساعدة للطلبة الباحثين في الدفعات القادمة إن شاء الله.

و في هذا المقام نختم بقول **عماد الدين الأصفهاني**

"**لا يكتب احد في يومه كتابا الا قال في غده لو غُير هذا لكان احسن، و لو زيد هذا لكان يستحسن، و لو قُدم هذا لكان افضل، و لو تُرك هذا لكان اجمل، و هذا من اعضم العبر و من دلائل استيلاء النقص على البشر....**"

{ وَ مَا أُتِيْتُمْ مِنَ العِلْمِ إلا قَلِيلا }

سورة الإسراء الآية_85_

قائمة المراجع

أولا : المراجع باللغة العربية:

I- الكتب

-1الكتب العامة

1. احمد رشاد سالم، التعاون الدولي وأثره في مكافحة الإرهاب، كلية التدريب قسم البرامج التدريبية الرياض، 2013

2. جمال زايد هلال ابو عين ،الإرهاب وأحكام القانون الدولي ،عالم الكتب الحديث للنشر والتوزيع ، الطبعة الاولى، سنة 2009 .

1-2 : الكتب المتخصصة

1. بشرى حسين الحمداني، القرصنة الالكترونية، دار أسامة للنشر والتوزيع الأردن، الطبعة الأولى، 2014.

2. بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية، دار الخلدونية، الجزائر،2017.

3. جمال زايد هلال ابو عين ،الإرهاب وأحكام القانون الدولي ،عالم الكتب الحديث للنشر والتوزيع ، الطبعة الاولى، سنة 2009 .

4. عادل عبد الصادق، اسلحة الفضاء الالكتروني في ضوء القانون الدولي الانساني، مكتبة الاسكندرية، مصر، بدون طبعة، 2016.

5. عبد الوهاب جعيجع، الأمن المعلوماتي وإدارة العلاقات الدولية ، دار الخلدونية، الجزائر، طبعة2017.

6. مايا حسن ملا خاطر، الإطار القانوني لجريمة الارهاب الالكتروني، كلية الحقوق، جامعة دار العلوم، المملكة العربية السعودية.

7. محمد سعادي، أثر التكنولوجيا المستحدثة على القانون الدولي العام، دار الجامعة الجديدة، عمان، بدون طبعة، 2014.

8. محمود احمد عبابنة، جرائم الحاسوب و أبعادها الدولية، دار الثقافة للنشر و التوزيع الطبعة الأولى، الإصدار الثاني، 2009.

9. نوران شفيق، اثر التهديدات الالكترونية على العلاقات الدولية، المكتب العربي للمعارف، مصر، طبعة 2016.

10. وائل أنور بندق ، موسوعة القانون الالكتروني وتكنولوجيا الاتصالات ،دار المطبوعات الجامعية ،2007.

قائمة المراجع

II- الدراسات

1 – الدراسات الجامعية

أ – الرسائل:

1. ساعد العقون، ظوابط سير الاعمال العدائية في القانون الدولي الانساني، اطروحة مقدمة لنيل شهادة الدكتوراه في العلوم القانونية، تخصص القانون الدولي الانساني، جامعة الحاج لخضر باتنة، كلية الحقوق و العلوم السياسية، قسم الحقوق، سنة 2014/2015.

2. مصطفى بن عصام نعوس ،التنظيم القانوني الدولي للانترنت ،رسالة لنيل درجة الدكتوراه في الحقوق ،كلية الحقوق، قسم القانون الدولي، جامعة حلب،سوريا،2013.

3. ملياني عبد الوهاب، امن المعلومات في بيئة الاعمال الالكترونية، رسالة لنيل شهادة الدكتوراه في القانون العام، كلية الحقوق و العلوم السياسية جامعة ابي بكر بالقايد، تلمسان _الجزائر_، 2017/2016 .

ب – المذكرات

1. سمية مزغيش، جرائم المساس بأمن المعلوماتية، مذكرة مكملة من متطلبات نيل شهادة الماستر في الحقوق تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، 2010.

2. سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجيستير في العلوم الجنائية وعلم الاجرام، جامعة ابو بكر بلقايد، كلية الحقوق والعلوم السياسية، تلمسان الجزائر، 2011/2010 .

3. نجاري بن حاج فايزة، الآليات القانونية لمكافحة الإرهاب الإلكتروني، مذكرة لنيل شهادة ماجيستر في القانون، جامعة مولود معمري تيزي وزو، كلية الحقوق، الجزائر ،بدون سنة.

4. وليد غسان سعيد جلعود، دور الحرب الالكترونية في الصراع العربي الاسرائيلي اطروحة لاستكمال متطلبات الحصول على درجة الماجستير في التخطيط والتنمية السياسية بكلية الدراسات العليا في جامعة النجاح الوطنية ،نابلس،فلسطين،2013.

2 – الدراسات والبحوث المتنوعة

الدراسات والبحوث القانونية :

دراسة بعنوان، صور الجرائم الالكترونية و اتجاهات تبوبها،تم الاطلاع عليها بتاريخ2018/1/20 ،على الرابط http/www.assakina.bom/bppk/.

شموئيل ايفن ،دافيد بن سيمان ،مراجعة كتاب حرب في الفضاء الالكتروني اتجاهات وتأثيرات على اسرائيل ،معهد دراسات الأمن القومي،تل أبيب 2011 على موقع المركز العربي للأبحاث ودراسة السياسات.

دراسة شاملة عن الجريمة السيبرانية، مسودة فيفري 2013، مكتب الامم المتحدة المعني بالمخدرات و الجريمة، الامم المتحدة نيويورك 2013.

قائمة المراجع

سامر مؤيد عبد اللطيف / ونوري رشيد الشافعي، بحث مقدم حول دور المنظمات الدولية في مكافحة الإرهاب الرقمي، وزارة التعليم العالي والبحث العلمي جامعة كربلاء، 2016.

وليد طه، بحث بعنوان التنظيم التشريعي للجرائم الالكترونية في اتفاقية بودابست،2001

حمدون إ .توريه، البحث عن السلام السيبراني ، بقلم الامين العام للاتحاد الدولي للاتصالات وفريق الرصد الدائم لامن المعلومات ،جانفي 2011،تم الاطلاع عليه بتاريخ: 2018/2/12، الساعة 12:00، على الرابط: https://www.shatharat.net

حمدون إ.تورية، برنامج الأمن السيبراني العالمي للاتحاد الدولي للاتصالات، حقوق الطبع محفوظة للعمل الجماعي 2011، ص 97 ،الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء....وللمزيد اطلع على الرابط: strategy@itu.int.

III – المجلات والمؤتمرات والوثائق

أ – المجلات:

التحكم في شبكة المعلومات العالمية للانترنيت، مقال منشور على موقع الجزيرة

مصطفى نعوس، حقوق والتزامات الدول في الحرب المعلوماتية ،مقال منشور على مجلة دراسات ، علوم الشريعة والقانون المجلد 40 الملحق،1،من الصفحة 784حتى الصفحة 800 ،تصدر مجلة دراسات عن عمادة البحث العلمي في الجامعة الاردنية ،2013

ليث ناجح حميد، موقف القانون الدولي من الهجمات الالكترونية ، مقال منشور على مجلة كلية القانون للعلوم القانونية و السياسة، كلية الحقوق، جامعة الفلوجة، العراق.

مجلة المحقق الحلي للعلوم القانونية و السياسية، العدد الرابع ، السنة الثامنة ، 2016.

عادل عبد الصادق، القوة الالكترونية اسلحة الانتشار الشامل في عصر الفضاء الالكتروني، سلسلة قضايا استراتيجية، المركز العربي لابحاث الفضاء، عدد اكتوبر 2012

ب – المؤتمرات:

مؤتمر الامم المتحدة 12 لمنع الجريمة والعادلة الجنائية، البند الثامن من جدول الأعمال المؤقت، التطورات الأخيرة في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة بما في ذلك الجرائم الحاسوبية، المنعقد في سالفادور (البرازيل)19/12 أفريل 2010 ، موقع الأمم المتحدة تم الاطلاع عليه بتاريخ 2018/02/24

ج – الوثائق:

الوثيقة IC/15/XXX 32 من المؤتمر الثاني و الثلاثون للصليب الاحمر و الهلال الاحمر، جنيف سويسرا، 8_10/ديسمبر/ 2015

الوثائق الصادرة عن القمة العالمية لمجتمع السلم، جنيف 2003 _ تونس 2005، الاتحاد الدولي للاتصالات، موقع الأمم المتحدة، ديسمبر 2005.

IV- النصوص القانونية:

أ – المواثيق والإتفاقيات الدولية:

- ميثاق الأمم المتحدة
- اتفاقية الاتحاد الافريقي بشان امن الفضاء الاليكتروني و حماية البيانات ذات الطابع الشخصي
- الاتفاقية العربية لجرائم تقنية المعلومات
- اتفاقية بودابست 2001.
- البروتوكول الاضافي الاول1977،لاتفاقيات جنيف 1949.

ب – القرارات والإعلانات :

- **قرارات مجلس الأمن:**

قرار مجلس الأمن رقم 1456 سنة 2003

قرار مجلس الامن رقم 2178، سنة 2014

قرار مجلس الأمن رقم 2354، سنة 2017

- **قرارات الجمعية العامة**

القرار رقم 54/49، الدورة 54، البند 71 من جدول الأعمال، سنة 1999.

القرار رقم 55/28 ،الدورة 55،البند68من جدول أعمال ،سنة2000

القرار 56/19،الدورة69،من جدول أعمال سنة2002

القرار رقم 57/53، الدورة 57، البند 61 من جدول الأعمال، سنة 2002

- **الإعلانات**

إعلان مؤتمر أبو ظبي حول مكافحة الإرهاب الإلكتروني 2017.

V – التقارير والمقابلات

أ – التقارير :

ابراهيم سليم/ منى الحمودي، تقرير بعنوان إجماع لاستصدار تشريع دولي لمكافحة جرائم الارهاب الالكتروني ، تاريخ النشر 2017/5/16 على موقع الاتحاد، تم الاطلاع عليه بتاريخ 2018/3/18، على ساعة 12:00، على الرابط:

http://www.alittihad.ae/modile.

التقرير التفسيري لاتفاقية الجريمة الالكترونية، سلسلة المعاهدات الأوروبية رقم 185، مجلس أوروبا، بودابست في 23نوفمبر 2001 .

ب – المقابلات

مقابلة مع المستشارة " كوردولا دروغيه" بتاريخ 2011/8/16 على موقع اللجنة الدولية للصليب الاحمر، على الرابط: https//: www.ICR.org

VII- المواقع الإلكترونية

أ – مواقع الكترونية متخصصة:

رائد العدوان، المعالجة الدولية لقضايا الإرهاب الالكتروني، جامعة نايف العربية لعلوم الامنية، الرياض، 2013، مقال تم الاطلاع عليه بتاريخ 2017/1/18، الساعة 12:00، على الرابط: https//repository.nauss.edu.sa

خلف إدريس الحبابسة، الإرهاب الالكتروني، مقال منشور على موقع lawj mobile ،تم الاطلاع عليه بتاريخ 2018/2/3، الساعة 12:00، على الرابط–https://l.facebook.com

جورج لبكي، المعاهدات الدولية للانترنت(حقائق وتحديات)،مقال تم الاطلاع عليه بتاريخ 2018/3/15 الساعة 12:00 على الرابط.https//wwwlebarmy gov lb

محمد الطاهر، تعليق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، مقال منشور على موقع حرية الفكر و التعبير تم الاطلاع عليه بتاريخ 2018/4/1 على الساعة 12:17 على الرابط: https://afteegypt.org

افريقيا تواجه مازقا بين مكافحة الجريمة الالكترونية وضمان حقوق الانسان، مقال تم الاطلاع عليه بتاريخ 2018/1/17 الساعة12:00 على الرابط:

عبدا لله بن عبد العزيز بن فهد العجلان، بحث مقدم الى المؤتمر الدولي الاول "حماية امن المعلومات و الخصوصية في قانون الانترنت"، 2008 تم الاطلاع عليه بتاريخ 2018/2/20، على ساعة 12:00، على الرابط: http://www.shaimaaatalla.com/vb

علي مطر، الارهاب الالكتروني في القانون الدولي ،مقال منشور على موقع السكينة ،تم الاطلاع عليه بتاريخ 2018/2/17،على الرابط:https /www.assakina.com

ليلى الجناني، فعالية القوانين الوطني و الدولية في مكافحة الجرائم السيبرانية، مقال منشور بتاريخ 2018/1/20 على موقع الحوار المتمدن، تم الاطلاع عليه بتاريخ 2018/2/30، على ساعة 12:00، على الرابط: http/www.m.hewar.org.

نصير العرباوي، د/ فاتح النور رحموني، الجريمة الإرهابية الالكترونية، مقال تم الاطلاع عليه بتارخ 2018/2/10، الساعة 12:00، على الرابط: https//www asjp ceist dz articl

المجال الخامس الحروب الالكترونية في القرن 21، مقال منشور على موقع مركز الجزيرة للدراسات، تم الاطلاع عليه بتاريخ 2018/3/11، على ساعة 12:00، على الرابط: studies.alja.eera.net

قائمة المراجع

تانغ لان، مقال بعنوان السيادة الوطنية و الفضاء الالكتروني، على موقع الخليج، تاريخ النشر 2016/4/27، تم الاطلاع عليه بتاريخ 2018/3/18، على ساعة 12:00، على الرابط http://alkaly.ea/mob/detail

عماد المرزوقي، الناتو يرفع درجة خطر الهجمات الالكترونية ،مقال منشور على صحيفة الراي ،العدد (12138)، الاثنين 24 سبتمبر 2012

يونس عرب، قراءة في الاتجاهات التشريعية للجرائم الالكترونية مع بيان موقف الدول العربية و تجربة سلطنة عمان،مقال تم الاطلاع عليه بتاريخ 2018/1/18، على ساعة 12:00، على الرابط :http/www.arablow.org.

اونيل سليمان :رئيس قسم الدفاع وتحديات الامن الالكتروني،اعد دراسة بعنوان (ظهور تحديات جديدة للامن)....للمزيد اطلع على المقال بصحيفة الراي ،العدد 12138الصادرة في 2012/9/12.

الفضاء الالكتروني للمناورة، مقال في صحيفة "كوميرسانت"، تاريخ النشر 2016/12/6، تم الاطلاع عليه بتاريخ 2018/3/11، على ساعة 12:00، على الرابط: http://ar.rt.com

التحكم في شبكة المعلومات العالمية للانترنيت، مقال منشور على موقع الجزيرة

مصطفى نعوس،حقوق والتزامات الدول في الحرب المعلوماتية ،مقال منشور على مجلة دراسات ،علوم الشريعة والقانون المجلد 40 الملحق،1،من الصفحة 784حتى الصفحة 800 ،تصدر مجلة دراسات عن عمادة البحث العلمي في الجامعة الاردنية ،2013

ليث ناجح حميد، موقف القانون الدولي من الهجمات الالكترونية ، مقال منشور على مجلة كلية القانون للعلوم القانونية و السياسة، كلية الحقوق، جامعة الفلوجة، العراق.

علي باكير، مفهوم الحروب الالكترونية، مقال منشور على موقع المقالات، بتاريخ 2011/3/9، تم الاطلاع عليه بتاريخ 2018/3/1 على الرابط: www.articles.islamweb.net

مقال منشور على موقع ويكيبيديا تم الاطلاع عليه بتاريخ 2018 /3/12

شري نسيم قلته، الهجمات الالكترونية وحظر استخدام القوة في القانون الدولي، مقال منشور على موقع المركز العربي لابحاث الفضاء الالكتروني بتاريخ2017/11/52 وتم الاطلاع عليه بتارخ 2018/3/15، على ساعة 12:00، على الرابط occoronline com

يحيى مفرح الزهراني، الأبعاد الإستراتيخلف إدريس الحبابسة، الإرهاب الالكتروني، مقال منشور على موقع lawj mobile ،تم الاطلاع عليه بتاريخ 2018/2/3، الساعة 12:00، على الرابط–https://l.facebook.com

جورج لبكي، المعاهدات الدولية للانترنت(حقائق وتحديات)،مقال تم الاطلاع عليه بتاريخ 2018/3/15 الساعة 12:00 على الرابط.https//wwwlebarmy gov lb

يونس عرب، قراءة في الاتجاهات التشريعية للجرائم الالكترونية مع بيان موقف الدول العربية و تجربة سلطنة عمان،مقال تم الاطلاع عليه بتاريخ 2018/1/18، على ساعة 12:00، على الرابط :http/www.arablow.org.

قائمة المراجع

ليلى الجناني، فعالية القوانين الوطني و الدولية في مكافحة الجرائم السيبرانية، مقال منشور بتاريخ 2018/1/20 على موقع الحوار المتمدن، تم الاطلاع عليه بتاريخ 2018/2/30، على ساعة 12:00، على الرابط: http/www.m.hewar.org.

محمد الطاهر، تعليق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، مقال منشور على موقع حرية الفكر و التعبير تم الاطلاع عليه بتاريخ 2018/4/1 على الساعة 12:17 على الرابط: https://afteegypt.org

افريقيا تواجه مازقا بين مكافحة الجريمة الالكترونية وضمان حقوق الانسان، مقال تم الاطلاع عليه بتاريخ 2018/1/17 الساعة12:00 على الرابط:

عبدا لله بن عبد العزيز بن فهد العجلان، بحث مقدم الى المؤتمر الدولي الاول "حماية امن المعلومات و الخصوصية في قانون الانترنت"،2008 تم الاطلاع عليه بتاريخ 2018/2/20، على ساعة 12:00، على الرابط: http://www.shaimaaatalla.com/vb

علي مطر، الارهاب الالكتروني في القانون الدولي ،مقال منشور على موقع السكينة ،تم الاطلاع عليه بتاريخ 2018/2/17،على الرابط:https /www.assakina.com

نصير العرباوي، د/ فاتح النور رحموني، الجريمة الإرهابية الالكترونية، مقال تم الاطلاع عليه بتارخ 2018/2/10، الساعة 12:00، على الرابط:https//www asjp ceist dz articl

المجال الخامس الحروب الالكترونية في القرن 21، مقال منشور على موقع مركز الجزيرة للدراسات، تم الاطلاع عليه بتاريخ 2018/3/11، على ساعة 12:00، على الرابط: studies.alja.eera.net

عماد المرزوقي، الناتو يرفع درجة خطر الهجمات الالكترونية ،مقال منشور على صحيفة الراي ،العدد (12138)، الاثنين 24 سبتمبر 2012

تانغ لان، مقال بعنوان السيادة الوطنية و الفضاء الالكتروني، على موقع الخليج، تاريخ النشر 2016/4/27، تم الاطلاع عليه بتاريخ 2018/3/18، على ساعة 12:00، على الرابط http://alkaly.ea/mob/detail

اونيل سليمان :رئيس قسم الدفاع وتحديات الامن الالكتروني،اعد دراسة بعنوان (ظهور تحديات جديدة للامن)....للمزيد اطلع على المقال بصحيفة الراي ،العدد 12138الصادرة في 2012/9/12.

عادل عبد الصادق، الأمم المتحدة و دعم الإستخدام السلمي للفضاء الإلكتروني، المركز العربي لأبحاث الفضاء الإلكتروني، مقال تم الإطلاع عليه في 2017/12/20، على ساعة 12:00، على الرابط:
http//:www.accronline.com article-detail

مقال منشور على الانترنيت، على موقع مجلة المحقق الحلي للعلوم القانونية و السياسية، العدد الثاني، السنة الثامنة 2016 .

علي باكير، مفهوم الحروب الالكترونية، مقال منشور على موقع المقالات، بتاريخ 2011/3/9، تم الاطلاع عليه بتاريخ 2018/3/1 على الرابط: www.articles.islamweb.net

مقال منشور على موقع ويكيبيديا تم الاطلاع عليه بتاريخ 2018 /3/12

قائمة المراجع

شريف نسيم قلته، الهجمات الالكترونية وحظر استخدام القوة في القانون الدولي،مقال منشور على موقع المركز العربي لابحاث الفضاء الالكتروني بتاريخ2017/11/52 وتم الاطلاع عليه بتارخ 2018/3/15، على ساعة 12:00، على الرابط occoronline com

علي حسن باكير، المجال الخامس الحروب الالكترونية في القرن ال 21، مقال منشور على موقع مركز الجزيرة للدراسات، تم الاطلاع عليه بتاريخ 2018/3/18، الساعة 12:00، على الرابط:
https://studies.aljazira.net

كفاح الزين، جيش ايران الكتروني، مقال منشور على موقع العربية تم الاطلاع عليه بتاريخ 2018/3/18، الساعة 12:00، على الرابط:https://alarabiya. net

لجنة الصليب الاحمر، ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية،مقال تم الاطلاع عليه بتاريخ 2018/3/20، الساعة12:00، على الرابط: https://www.icrc.org

الفضاء الالكتروني للمناورة، مقال في صحيفة "كوميرسانت"، تاريخ النشر 2016/12/6، تم الاطلاع عليه بتاريخ 2018/3/11، على ساعة 12:00، على الرابط: http://ar.rt.com

ب – مواقع الكترونية عامة

Mhttps://ar.wikipedia.org/wik

www .carjj.org

https://ar.wikipedia.org

https://seconf.wordpress.com

https://www.marefa.org

https://ar.wikipedia.org

http://mawdoo3.com

http://avb.s-oman.net

ثانيا : المراجع باللغة الفرنسية

Ouvrages

****

Articles:

- Abdel wahab Biad cyber guerre et les specialis évolution ou révolution 2014.
- ABDELWAHAB BIAD , cyber guerre et les spécialisé évolution ou révolution COLLOQUE DE ROUEN 2014.
- Ahmad oubais al-fatlawi, cyber attacks: its concept and arising international responsibility in the light of contemporary international organization,

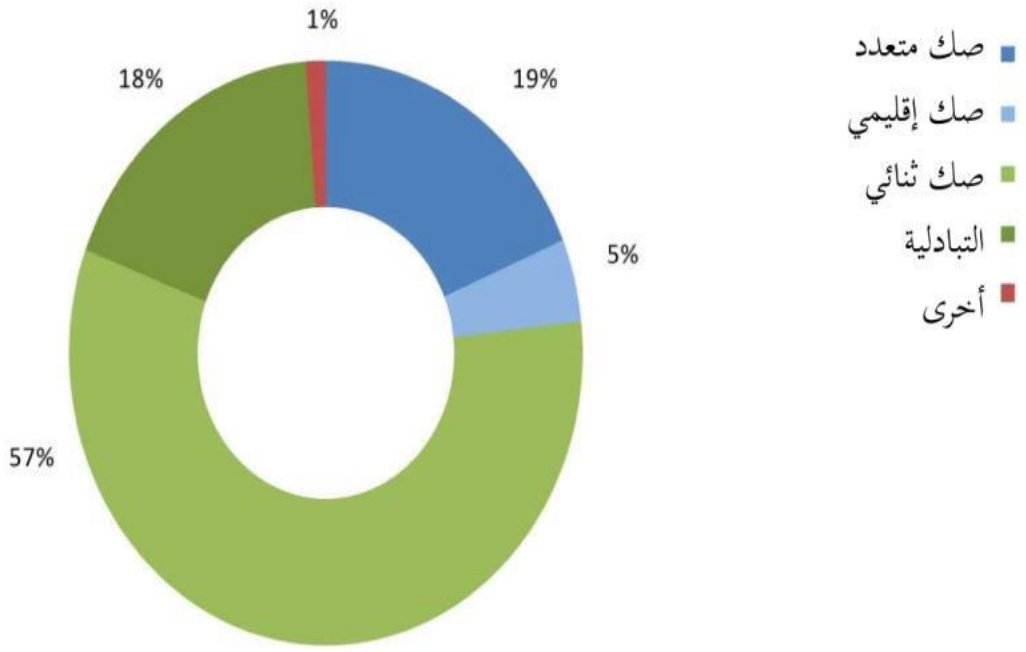
- Anne Thida NORODOM, internet et le droit international défi ou opportunité ? ,COLLOQUE DE ROUEN 2014.
- Anne-Thida NORODOM, internet et droit international: défi ou opportunité, clloque de Rouen, 2014 .
- Climentines bories, « Appréhendre la cyberguerre en droit international. Quelques réflexions et mises au point », la revue des droit de l'homme (online) le 06/2014 , vu le 11/03/2018 sur le lien suivant URL :http:// revdh.revues.org/984,publisher center de recherche et d'études sur les droits fondamentaux
- Evelyne AKOTO, les cyberattaques étatiques constituent_elle des actes d'agression en vertu du droit international public ? :premiére partier .U OTTAWA, faculté du droit, 2014 /2015
- Evelyne AKOTO, les cyberattaques étatiques constituent_elle des actes d'agression en vertu du droit international public ? :premiére partier .U OTTAWA, faculté du droit, 2014 /2015 .
- Philipe La Grange, internet et l'évolution normative du droit international : d'un droit international applicable à l'internet à un droit international du cyberespace ? , clloque de Rouen 2014 .
- Svetlana zasova, la légitime défense des Etats et la guerre cybernétique, , clloque de Rouen, 2014 .
- Svetlana zasova, la légitime défense des états et la guerre cybernétique, , clloque de Rouen 2014 . 271

جدول رقم : القدرات الالكترونية للدول

الدولة	الهجوم الاليكتروني	الاعتماد على الفضاء الالكتروني	الدفاع الالكتروني	المجموع
الولايات المتحدة	8	2	1	11
روسيا	7	5	4	16
الصين	5	4	6	15
ايران	4	5	3	12
كوريا الشمالية	2	9	7	18

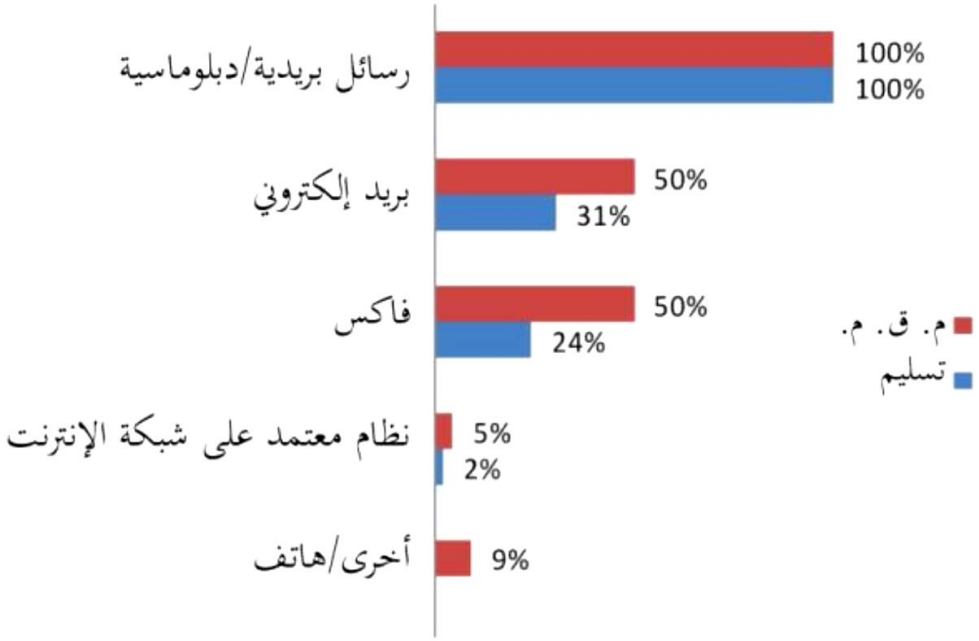
Richard A. Clarke & Robert K. Knake.(2010) cyber war : the next threat to national security and what to do about it . Harper Collins. P147

الملحق رقم 01: الأساس القانوني لتسليم مرتكبي الجريمة السيبرانية وطلبات المساعدة القانونية المتبادلة



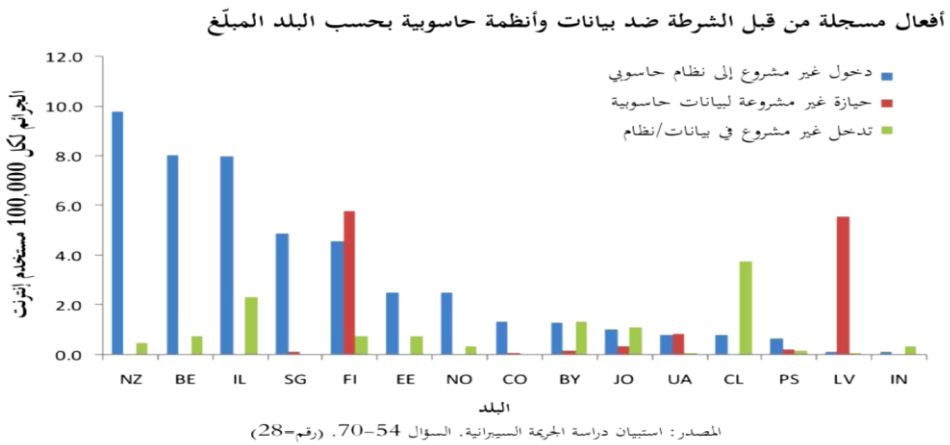
المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 202-207 و227-232. (رقم=21، 50)

الملحق رقم 02 : أشكال الإتصال في قضايا الجريمة السيبرانية



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 197 و219. (رقم=44، 47، رقم=77، 94)

الشكل رقم 03: أفعال مسجلة من قبل الشرطة ضد بيانات وأنظمة حاسوبية بحسب البلد المبلغ



المصدر: استبيان دراسة الجريمة السيبرانية. السؤال 54-70. (رقم=28)

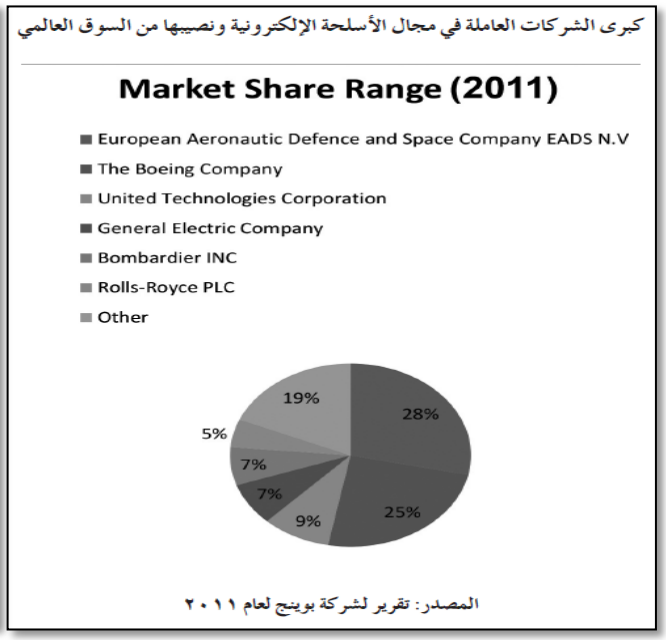
الشكل رقم04:

المصدر: كتاب أسلحة الفضاء الالكتروني لعادل عبد الصادق ص65 (مذكور في

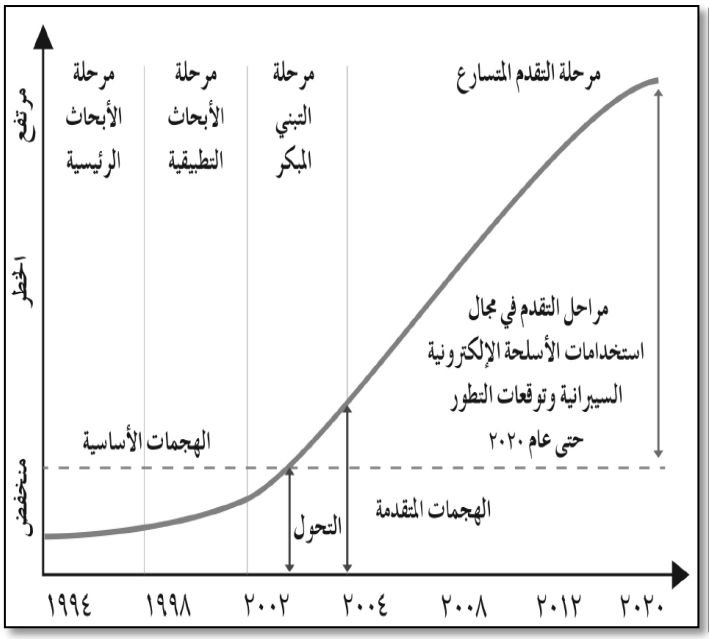
الشكل رقم05:

المصدر: شركة كاسبرسكي 2014

الشكل رقم 06



الشكل رقم 07



فهرس المحتويات

فهرس المحتويات

فهرس المحتويات