أمن المعلومات الإلكترونية بين متطلبات السيادة الرقمية وجهود المنظمات الدولية والإقليمية

Electronic information security between the requirements of digital sovereignty and the efforts of international and regional organizations

تاريخ الارسال: 2020/02/10	تاريخ القبول: 2020/10/28	تاريخ النشر: 2021/07/15

***د. قريبيز مراد**
جامعة عمار ثليجي - الأغواط
gueribiz.mourad@gmail.com

ملخص :

إن هذه الدراسة تهتم بظاهرة حديثة على الساحة الدولية وهي التحدي التكنولوجي للمفاهيم القانونية التقليدية، إذا أصبحت المعلومات تتدفق بسهولة أكبر ولم تعد الحدود عائق لها وأمام هذه المعضلة كان لا بد من البحث عن الحلول في شكل صكوك قانونية دولية ملائمة ، بإضافة إلى أن مجال الفضاء الالكتروني مستهدفا بشكل كبير من قبل من أي تحديد الطرف مثلا الإرهاب الالكتروني خصوصا مع ارتفاع وتيرة التقدم التكنولوجي والتقني والالكتروني مما دفع بالدول للسعي من أجل حماية أمنها المعلوماتي.

الكلمات المفتاحية: الأمن المعلوماتي؛ المعلومات الالكترونية؛ السيادة الرقمية .

Abstract:

This study is concerned with a recent phenomenon on the international scene, which is the modern technological challenge of traditional legal concepts. If information flows more easily and borders are no longer an obstacle to this flow, therefore it is necessary to find solutions to this problem in the form of appropriate and legal international instruments and laws. The field of cyberspace became a field targeted significantly, especially with the high rate of technical, technological and electronic advances, which prompted countries to strive in order

***المؤلف المرسل:** قريبيز مراد

to protect their information's and the national security.

***Keywords**: Information security; Electronic information; Digital sovereignty.*

مقدمة:

احتلت صراعات الفضاء الالكتروني المشهد الكبير لعصرنا الحالي حيث تراجعت نغمات التهديد بالأسلحة النووية والبيولوجية والتقليدية التي عهدها الإنسان خلال عصره الحديث والمعاصر للتحول إلى صدامات هادئة وصامتة وناعمة معتمدة اعتمادا كليا على الأسلحة الالكترونية كالرسائل الالكترونية والهواتف المحمولة الذكية وأجهزة الحاسوب.....الخ.

وفي ظل هذه التغيرات أصبح الفضاء السيبراني مجالا رئيسا للمواجهة بين القوى الدولية، ظهر أمن المعلومات الالكتروني كتحدي عالمي وبالنظر إلى الطبيعة المختلفة لهذا المجال التي تختلف عن المجالات السيادية التقليدية ممثلة في المجال البري والبحري، الجوي وحتى الفضائي ظهرت الحاجة إلى إعادة التفكير في القالب الكلاسيكي للسيادة، فظهر مفهوم السيادة الرقمية كشكل جديد تماما من القوى السيادية.

ووعي من الدول من هذا الوضع الحرج وسعيا وراء توفير بيئة معلوماتية آمنة بات لزاما عليها إيجاد أطر تشريعية وتنظيمية مناسبة لتعزيز الثقة في الفضاء الالكتروني وتعميم ثقافة الأمن المعلوماتي.

وذلك من خلال مساعي دولية وإقليمية في مجال حماية أمنها المعلوماتي وتوفير بيئة إلكترونية أمنة.

وانطلاقا من المعلومات السابقة فإنه يمكن طرح الإشكالية التالية:

- ما هي الوسائل القانونية المتاحة لتوفير حماية القانونية فعالة لأمن المعلومات الإلكترونية؟

لمعالجة هذا الإشكال لابد من دراسته من خلال محورين أساسين،الأول نخصصه إلى الدفاع عن السيادة الرقمية للدولة لحماية امن المعلومات الالكترونية،والثاني لجهود المنظمات الدولية والإقليمية لحماية امن المعلومات الالكترونية.

المبحث الأول: الدفاع عن السيادة الرقمية للدولة لحماية امن المعلومات الالكترونية

ينص دليل تالين[1] الذي كتب بتكليف من "**مركز التميز التعاوني**" المخصص بالدفاع عن الفضاء الالكتروني، التابع لحلف الناتو، ومقره تالين عاصمة استونيا على ان"**الدول تستطيع ممارسة السيطرة على البنية التحتية الالكترونية، والنشاطات الالكترونية التي تقع وتمارس داخل أراضيها السيادية**".

والسيادة أحد المفاهيم الأساسية في القانون الدولي المعاصر، والمساواة في السيادة من المبادئ الأساسية التي تحدد العلاقات الدولية المعاصرة.[2]

ومر مفهوم السيادة بعدة محطات ومفاهيم مختلفة من السيادة المطلقة الى السيادة المقيدة وأخيرا إلى اللاسيادة وذلك في العصر الرقمي الذي نعيشه اليوم، وبهذا يكون مفهوم السيادة في طريقه إلى التحول الكامل، مما يفسح المجال لظهور مفهوم جديد سمي السيادة الرقمية، والذي يعرفها الدكتور **محمد سعادي** أستاذ القانون الدولي العام بمعهد الحقوق بجامعة غليزان بأنها "**بسط الدولة لسيطرتها وولايتها القضائية على الفضاء الرقمي المتمثل في الانترنيت**".[3]

ولا 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 مجهودات عديدة للتصدي والدفاع على سيادتها الرقمية وهذا ما سنتطرق له في **المطلب الأول**، ونظرا للأهمية الكبرى والمصيرية التي احتلتها الانترنيت جعل الدول تطالب بالمشاركة في إدارة الانترنيت كحماية لسيادتها الرقمية وأمنها المعلوماتي هذا ما سنبحثه في **المطلب الثاني**.

المطلب الأول: نحو تعزيز السيادة الرقمية للدولة

الدول التي تعتمد على الانترنيت وعلى الشبكات المعلوماتية تعتبر هي الأكثر عرضة للاعتداءات والتهديدات الالكترونية والتي تمس بمجال سيادتها الرقمية.

وبما 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**،وكيف انه يمكن للفضاء المعلوماتي 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،فعلى سبيل المثال قامت كل من :

- انجلترا: بإصدار إستراتيجية الأمن الالكتروني القومية في جويلية/2009، كما قامت بإنشاء وحدة الأمن الالكتروني ومركز العمليات ومقره وكالة الاستخبارات القومية (GCHO) وبدأت وظيفتها عمليا في شهر مارس 2016.

- الولايات المتحدة الأمريكية: في ماي 2009 صادق البيت الأبيض على وثيقة "مراجعة سياسة الفضاء الالكتروني" والتي تم تقديمها من قبل لجنة خاصة إلى الرئيس الأمريكي اوباما، وهي 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" وعينت مدير وكالة الاستخبارات القومية العسكرية الجنرال "كيت الكسندر" قائدا عليها مهمته الحرص على حماية الشبكات الأمريكية العسكرية على الدوام[4]، وذلك للأهمية الخطيرة للشبكات العسكرية وارتباطها الأكيد بشبكة الانترنت وتأمينها 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.[5]

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

طالبت المجموعة الدولية في المؤتمر الثالث للأمم المتحدة حول قانون البحار المنعقد خلال فترة 1974_1982 بتخصيص منطقة من أعالي البحار لا تكون خاضعة لسيادة أي دولة أي بمعنى انها حق مكفول دوليا لصالح الإنسانية،كما ان هذا الحق لا يقتصر على قانون البحار فقط بل سبق ذلك ان تم استخدامه في مجال الفضاء بحيث تم الاتفاق في معاهدة 1967 على ان المجال الفضائي والقمر هما تراث مشترك للإنسانية فلا يمكن استعماره ولا رهنه بسيادة أي دولة ولا حيازته.[6]

وعلى نهج الاتفاقيتين السابقتين فقد أحرزت الدول في هذا المجال بعض النجاحات ففي جويلية 2015 استطاعت مجموعة خبراء الأمم المتحدة بما فيهم خبراء من روسيا والولايات المتحدة الأمريكية (شكلت عام 2004) من التوصل إلى اتفاق بشأن تقرير يتضمن القواعد الأساسية لسلوك الدول في الفضاء الالكتروني وبموجب هذه القواعد تلزم الدول باستخدام تكنولوجيا المعلومات والاتصالات في الأغراض السليمة فقط، والامتناع عن مهاجمة المواقع الحيوية لبعضها البعض في البنى التحتية (المحطات الذرية لتوليد الطاقة الكهربائية النظم المصرفية، وأنظمة النقل وغيرها).[7]

وتعتبر هذه الخطوة الأول لمحاولة جعل الفضاء الالكتروني إرثا مشتركا للإنسانية يستخدم للأغراض الإنسانية فقط، ويجب حمايته بصفته هذه، في جعل الفضاء الالكتروني ميدان للتفاعلات التشاركية والسملية كلما تبلورت لدينا قواعد قانونية دولية ملزمة لرواد هذا الفضاء.[8]

كما بينه لويس كفاري "louis cavari" حين يقول: بأن القانون الدولي سيتأقلم مع الحاجيات الاجتماعية وينظمها 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 ومصلحة 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 وذلك بإعلان السيادة عليه.

- كما اقترحت المادة 4 بأن تنشأ سلطة قضائية دولية تنظم وتراقب نشاطات الدول في الفضاء المعلوماتي والتزامها بهذه المعاهدة، أو التشريع الدولي المقترح.
- وتحدثت المادة رقم 5 على قيام المسؤولية الدولية في حالة مخالفة الدول الأعضاء بنود المعاهدة الخاصة بنشاطات الممارسة وأن مجال هذه المسؤولية يتسع ليشمل نشاطات المنظمة الدولية أيضا، كما أكدت المادة رقم 6 على التعاون الدولي بين الدول في الفضاء المعلوماتي واعتبار الدول بمصالح بقية الأطراف.[9]

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

المطلب الثاني: المشاركة في إدارة الانترنت كوسيلة لحماية السيادة الرقمية

تسمى المؤسسة التي تشرف على الانترنت بمجلس إدارة شبكة الانترنيت وتعرف اختصارا(ICANN)[10]، ومقرها يوجد بلوس انجلوس وهي مؤسسة خاصة بغايات غير ربحية[11]، ويسير مجلسها الشبكة من خلال 14 جهاز معروفة باسم "الموزعات الجذور" والتي تمول الآلاف من الموزعين حول مجموعة الكرة الأرضية، مما يجعل توزيعها يبدوغير عادل إذ يوجد 10 من هذه الموزعات الجذر بالولايات المتحدة الأمريكيةو4 موزعة على كل من انجلترا واسبانيا وسويد والرابع موجود في اليابان.

وتجدر الإشارة إلى أن نظام تسيير أسماء الميادين DNS [12] يوجد حاليا بيد الشركة الأمريكية المكلفة بتسيير نظام أسماء الميادين وتخصيص فضاء عناوين بروتوكولات الانترنيت (ICANN).[13]

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

تعد سيطرت الولايات المتحدة الأمريكية على عمل الشبكة الدولية للأنترنت مبعث قلق للعديد من الدول التي طالبت بنصيب في هذه الإدارة، وعلى رأسها الدول النامية والاتحاد الأوروبي المطالبين بإنشاء هيئة دولية للإدارة على الانترنيت والرقابة عليها، لمالها من أهمية على مستوى السيادة الرقمية للدولة وفضائها الالكتروني.

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

وفي مواجهة هذه الضغوط لجعل الانترنت يخضع في إدارته للأمم المتحدة تمسك الموقف الأمريكي بالسيطرة على عمل الشبكة وإدارتها بحجة أنت مسكه يتعلق بالجانب التقني لا أكثر.

وأن مسألة احتكار الولايات المتحدة الأمريكية للكود التقني للشبكة يرجع ذلك إلى كون أن الولايات المتحدة الأمريكية تاريخيا هي مخترعة الانترنت،ومن ثم يصبح لها حق الملكية الفكرية.

لكن الدول النامية ترى أن الانترنت أصبحت مرفقا عالميا وليس خاصا، وأن منظمة الأيكان لا تخضع لأي اتفاقيات دولية مما يعني أن تكون عرضه للقرارات تعسفية أحادية الجانب بدون أن يكون لأي دولة الحق فيا لرفض.

كل هذا دفع بالدول الأعضاء في الأمم المتحدة إلى تنظيم قمة عالمية حول مجتمع المعلومات في جينيف 2005 و قبله تونس 2003 وبعدها تنظم قمة عالمية لمجتمع المعلومات بجينيف سويسرا 2010 أن النقاشات التي دارت خلال القمم الثالث المذكورة أعطت بعدا سياسيا لموضوع التحكم في إدارة الانترنت،وهذا ما جاء في تقرير مجموعة العمل حول التحكم في إدارة الانترنت مما جعلها تطالب (مجموعةالعمل) بنقل سلطات إدارة الانترنت من الهيئة الأمريكية (ICANN) إلى الاتحاد الدولي للاتصالات أو لمنظمة الأمم المتحدة.[14]

الفرع الثاني: الاتفاق على إنشاء آليات التحكم في إدارة الانترنت

كانت الآلية الأولى هي مجموعة العمل حول التحكم في إدارة الانترنت والتي أنشأها الأمين العام للأمم المتحدة سنة 2003 أثناء القمة العالمية لمجتمع الإعلام بتونس تتكون من مزيج من دول وقطاع خاص ومجتمع مدني،ومنظمات حكومية ومنتديات معنية، وينصب 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 وإدارته،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 إذ يشكل إطارا رسميا ودوليا دائما من اجل

النقاش حول مسألة المعايير الواقعية حول التنظيم الديمقراطي والحقيقي لمرفق الانترنيت.[15]

ويتضح من مما سبق بأن مبدأ سيادة الدولة عاد ليفرض نفسه بقوة من جديد وبمقياس جديد في مجتمع تطور بطريقة جديدة تجعل من صناع القرار على المستوى الدولي إعادة التفكير من جديد في تأسيس إطار قانوني محكم لحماية سيادة الدولة في عالم الرقمنة، من الانتهاكات والاعتداءات بطرق جديدة.

المبحث الثاني: جهود المنظمات الدولية والإقليمية لحماية امن المعلومات الالكترونية

إن الجهود المبذولة من أجل توفير بيئة آمنة إلكترونيا لنظم المعلومات الحساسة والحيوية الخاصة بالبنى التحتية للدول، لن تكون لهذه الجهود أي أثر فعال إلا إذا كان هناك تعاونا وتنسيقا يتجاوز الحلول الوطنية، وذلك لا يتحقق إلا عن طريق طرح مشكلة الأمن الإلكتروني لنظم المعلومات في المحافل الدولية والإقليمية وعليه سنعالج هذا الموضوع عبر المطلب الأول جهود منظمة الأمم المتحدة، والمطلب الثاني مساعي الإتحاد الأوروبي والحلف الأطلسي.

المطلب الأول : جهود منظمة الأمم المتحدة

بذلت الهيئة الأممية جهودا في سبيل العمل على مكافحة الجرائم المعلوماتية وذلك لما تسببه هذه الجرائم من خسائر اقتصادية ومشاكل سياسية واجتماعية جد خطيرة،وإن التصدي لهذا التهديد ومكافحته يتطلبان استجابة دولية في ضوء الطابع والأبعاد الدولية لإساءة استخدام الكمبيوتر والجرائم المتعلقة به.[16]

حيث أصدرت منظمة الأمم المتحدة عبر جمعيتها العامة عددا من القرارات التي توضح مدى تصاعد الاهتمام العالمي باستخدام تكنولوجيا الاتصالات والمعلومات استخداما غير سلمي جاء ذلك عبر سلسلة من القرارات سنتطرق لها من خلال **الفرع الأول**، واصلت المنظمة جهودها من اجل الحد من انتشار الجرائم الالكترونية الماسة بأمن المعلومات وذلك من خلال إشرافها على عقد مجموعة من المؤتمرات **الفرع الثاني**.

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 والاتصالات السلكية واللاسلكية في سياق الأمن الدولي

ومن هذه القرارات نجد القرار رقم 54/49والمعبر عن قلق الجمعية العامة عن احتمال أن تستخدم هذه التكنولوجيا والوسائل في أغراض لا تتفق وأهداف صون الاستقرار والأمن الدولي، وقد أثر تأثيرا سلبيا على أمن الدولة في الميدانيين، المدني والعسكري، إذ ترى الجمعية أنه من الضروري تكثيف التعاون الدولي من اجل منع إساءة استخدام موارد أو تكنولوجيا المعلومات أو استغلالها في تحقيق أغراض إجرامية أو إرهابية،واقتناعا منها بخطورة تأثير الاستخدام السيئ لتكنلوجيا المعلومات على مصالح المجتمع الدولي أكدت من جديد في قرارها رقم 55/28على ضرورة التعاون الدولي،[17]واصلت الأمم المتحدة اهتمامها بمكافحة الإجرام المعلوماتي 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.[18]

- وتلاحظ الجمعية العامة في قرارها الصادر سنة 2003أن نشر واستخدام تكنولوجيا ووسائل المعلومات يؤثران في مصالح المجتمع الدولي بأكمله،وأن الفاعلية المثلى من اجل التصدي لهذه الآثار التي تكمن فيتعزيز التعاون الدولي الواسع النطاق.[19]

ثانيا: بشأن مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية

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

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

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

ج- ينبغي تدريب العاملين في مجال إنفاذ القوانين وتجهيزهم بما يمكن من مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية.

وتدعو الجمعية العامة الدول إلى أخذ هذه التدابير المذكورة أعلاه بعين الاعتبار في جهودها الرامية إلى مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية.[20]

كما عكست قرارات الجمعية العامة للأمم المتحدة الإدراك الكبير لمشكلات أمن المعلومات الدولية، وتمت لأول مرة الإشارة إلى الاستخدام العسكري المحتمل لتكنولوجيا الاتصال والمعلومات في القرار المقدم في ديسمبر1999[21].

و دعت القرارات الدول للمزيد من النظر في الأخطار القائمة والمحتملة في ميدان أمن المعلومات، وكذلك 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، وهذا من خلال مؤتمراتها، والذي يعنينا في هذه الدراسة هو جهودها من خلال مؤتمراتها الخاصة بمنع الجريمة ومعاملة المجرمين المتعلقة بالجرائم التقنية أو جرائم الحاسب الآلي بدءا بالمؤتمر السابع عام 1985 المنعقد في مدينة ميلانو بايطاليا،إذ انبثقت عنه مجموعة من القواعد التوجيهية والتي اكتملت صياغتها في الاجتماعات الإقليمية التحريرية للمؤتمر الثامن الذي أجاز هذه المبادئ والذي عقد بهافانا بكوبا 1990، واصلت منظمة الأمم المتحدة عقد مؤتمراتها حيث كانت تؤكد التوصيات في كل مرة على:

- وجوب حماية الإنسان في حياته الخاصة وملكيته الفكرية من مخاطر التكنولوجيا.
- تحسين امن الحاسب الآلي والتدابير المنيعة.
- تحديث القوانين الجنائية الوطنية.
- زيادة التعاون الدولي من اجل مكافحة هذه الجرائم.

إلى غاية المؤتمر الثاني عشر. لمنع الجريمة والعدالة الجنائية وذلك بالبرازيل 12_19 أفريل 2010 حيث ناقشت فيه الدول الأعضاء بنوع من التعمق مختلف التطورات الأخيرة في استخدام العلم والتكنولوجيا.[22]

كما تشجع منظمة الأمم المتحدة على التعاون مع الإتحاد الأوروبي ومنظمة الأمن والتعاون مع أوروبا وكذلك مع الأنتربول[23]والأيروبول[24] الخاص بالإتحاد الأوروبي، وتسعى تلك الجهود في إطار تنفيذ الأجندة العالمية للأمن الإلكتروني.[25]

المطلب الثاني: دور المنظمات الإقليمية في حماية امن المعلومات الالكترونية

إن 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 الأول**، 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 وتقوية البنى التحتية المعلوماتية لأجهزة الاتحاد،[26]حيث بذل الاتحاد الأوروبي جهودا لا يستهان بها في مجال الحماية القانونية لأمن المعلومات الالكترونية والتي تمس جوانب عديدة من القطاعات الهامة في الدولة وعلى سبيل المثال:

-التوجيه 2000/31/EC الصادر عن البرلمان الأوروبي ومجلس أوروبا بشأن جوانب قانونية معينة من خدمات مجتمع المعلوماتية

- القرار الإطاري لمجلس الاتحاد الأوروبي2000/413/GHA بشان مكافحة الاحتيال وتزوير وسائط الدفع الغير نقدي (قرار الاتحاد الأوروبي بشأن الاحتيال والتزوير).

- القرار الإطاري لمجلس الاتحاد الأوروبي2005/222/GHA بشأن الهجمات على النظم المعلوماتية (قرار الاتحاد الأوروبي لشأن الهجمات ضد نظم المعلومات).

- التوجيه 2006/24/EC الصادر عن البرلمان الأوروبي ومجلس الاتحاد الأوروبي بشأن الاحتفاظ بالبيانات التي تستخلص أو تعالج في إطار توفير خدمات الاتصالات الالكترونية المتاحة للجمهور.[27]

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

وبالرغم 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 الآن الاتحاد الأوروبي ولاية أقوى لمواءمة التشريعات الوطنية للدول الأعضاء بشان جرائم المعلوماتية وهذا 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 و2001 وشملت هذه الاتفاقية مجموعة من البنود تعلقت بالجانب الموضوعي والإجرائي في الشق الجنائي وأيضا بالتعاون الدولي كما تم إصدار بروتوكول إضافي في هذه الاتفاقية من اجل تغطية موضوع تجريم العنصرية وتوزيع مواد تثير كراهية الأجانب المرتكبة بواسطة الحاسوب.[28]

الفرع الثاني: دور منظمة حلف شمال الأطلنطي (الناتو)

إن تعرض استونيا سنة 2007 للهجوم الالكتروني الخارجي جعل حلف الناتو[29] يعيد حساباته من جديد وذلك لعجزه التام على الرد على هذا النوع من الهجوم وبالرغم من أن استونيا نالت العضوية في الحلف منذ 2004 والمادة 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 والتي تختلف على ما عرفت به الأسلحة التقليدية. [30]

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

في عام 2008 قام الحلف بإنشاء مركز الدفاع الالكتروني التعاوني للتميز مقره بتالين العاصمة الإستونية يهدف هذا المركز لتقييم القدرات الدفاعية لدول الحلف وأيضا لزيادة الوعي بقضايا الأمن الالكتروني وفي 2012 خصص الحلف مبلغ 58 مليون يورو وذلك لترسيخ قدرة الناتو على الرد الفوري على الهجمات الالكترونية وفي 2013 تم الاتفاق على إنشاء فرق للرد الالكتروني لحماية كافة الأنشطة والشبكات الالكترونية للمنظمة [31]،ويعمل حلف الناتو على تنسيق سياسات الدول الأعضاء في ما بينها 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.

والفضاء الالكتروني حسب دراسة أونيل سليمان[32] 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.[33]

وبهذا نستطيع القول إن الإطار الدفاعي للناتو هو من انجح، إن لم نقل هو الأنجح على الإطلاق مقارنة بالمنظمات الدولية والإقليمية الأخرى.

الخاتمة:

إن التقدم الواسع في العلوم والتكنولوجيا، والطفرة الرقمية الناتجة عن ذلك فاقت قدرة المجتمع الدولي على إدارتها والسيطرة عليها.

فثورة الانترنت تطلب على نطاق واسع مراجعة العديد من المسلمات والمفاهيم ، مع ظهور الفضاء السيبراني حيث هددت مكانة الدولة وأدوارها وقللت من سيادتها المرتبطة بالحدود الجغرافية الصلبة.

وخلاصة القول أنه بات على دول العالم حماية أمن معلوماتها الالكترونية والذي راح يشكل خطرا كبيرا على بنيتها التحتية الأساسية وبالتالي تهديد وجودها في عالم تكنولوجي معرفي تسدوه المخاطر من كل حدب وصوب.

ومن خلال تعرضنا لهذه الورقة البحثية توصلنا إلى مجموعة من النتائج نلخصها فيما يلي:

1 يلعب الأمن المعلوماتي الالكتروني دورا مهما في حماية أمن الدول واستقرارها فهو قد يهدد أمن الدولة كليا إذا ما تعرض للانكشاف والاختراق.

2 ازدياد حجم خسائر الجرائم المعلوماتية والتي أخذت أبعاد دولية.

3 إطلاق العديد من المبادرات التي تقوم بها المنظمات الحكومية والوكالات المتخصصة التابعة للأمم المتحدة

ومما سبق من نتائج خلصنا لبعض الاقتراحات:

1 التزام القرارات الصادرة عن الأمم المتحدة الداعية إلى نشر ثقافة الأمن السيبراني.

2 تنظيم مؤتمرات وندوات علمية في جامعات ومراكز البحث في مختلف دول العالم تضم خبراء. وباحثين ومختصين من مختلف التخصصات لدراسة مشكلة أمن المعلومات الالكترونية.

3 يمكن أن تشكل إمكانية التوصل إلى اتفاقية دولية حول الفضاء الالكتروني قوة دولية في مجال. الدبلوماسية للعمل على الحفاظ أمن وسلامة البيئة المعلوماتية الالكترونية.

الهوامش:

1- دليل تالين: قام بإعداده مجموعة من فقهاء القانون الدولي نشر الإصدار الأول منه عام 2016 يحتوي على 95 قاعدة قانونية إرشادية لعمل او لسلوك الدول في سياق الحرب الالكترونية، و صدر الإصدار الثاني منه في 2017، و يحتوي على 154 قاعدة ليشكل مستوى اكثر اتساعا لمعالجة العمليات الالكترونية و مراجعة و حسم لنقاط عدم الاتفاق في الإصدار الأول... للمزيد اطلع على شريف نسيم قلتة بخية، دليل، الهجمات الالكترونية و حظر استخدام القوة في القانون الدولي، على الرابط: www.accronline.com

2- تانغلان،مقالبعنوانالسيادةالوطنيةوالفضاءالالكتروني،علىموقعالخليج،تاريخالنشر 2016/4/27،تم الاطلاع عليه بتاريخ 2018/3/18، على ساعة 12:00،على الرابطhttp://alkaly.ea/mob/detail

3- د/ محمد سعادي، أثر التكنولوجيا المستحدثة على القانون الدولي العام، دار الجامعة الجديدة، بدون طبعة، ص ص 209 210

4- 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

5- 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.

6- أ.د/ زازا لخضر، محاضرات في القانون الدولي لحقوق الانسان ،دار الضحى للنشر والإشهار ،الجلفة ، الجزائر،2016،ص86.

7- 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

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

9- د/ محمد سعادي، نفس المرجع السابق، ص ص 255 256

10- 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.

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

12- DNS: هو نظام يخزن معلومات تتعلق بأسماء نطاقات الانترنيت بقاعدة بيانات لا مركزية على الانترنيت يستطيع خادم اسم النطاق ربط العديد من المعلومات بأسماء النطاقات، و يعتبر نظام أسماء النطاقات مفيدا لعدة أسباب أكثرها 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

13- د/محمد سعادي، المرجع السابق، ص85.

14- د/ مصطفى بن عصام نعوس ،التنظيم القانوني الدولي للانترنت ،رسالة لنيل درجة الدكتوراه في الحقوق 2كلية الحقوق، قسم القانون الدولي، جامعة حلب،سوريا،2013. ص341

15- محمد سعادي، نفس المرجع، ص ص ص 302 300 299.

16- 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.

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

18- ينظر القرار رقم 55/28 ،الدورة 55،البند68من جدول أعمال ،سنة2000

19- ينظر القرار 56/19، الدورة69 ، من جدول أعمال سنة2002

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

21- نفس المرجع السابق.

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

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

24- 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

25- 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 أكثر من 700 موظف في

مقرها الرئيسي الكائن في لاهاي في هولندا و هي تعمل بشكل وثيق مع أجهزة 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

26- د/ عادل عبد الصادق، مرجع سابق.

27- نوران شفيق، اثر التهديدات الالكترونية على العلاقة الدولية،المكتب العربي للمعارف، الطبعة الأولى 2016، ص 103.

28- دراسة شاملة عن الجريمة السيبرانية، مسودة فيفري 2013، مكتب الأمم المتحدة المعني بالمخدرات و الجريمة، الأمم المتحدة نيويورك 2013، ص ص 10 11.

29- مؤتمر الامم المتحدة 12 لمنع الجريمة و العادلة 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

30- 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 المعتد عليهم، بالقوات المسلحة إن لزم الأمر.....للمزيد اطلع على: www.wikipidia.org

31- نوران شفيق ، مرجع سابق، ص 99، 100،101،102

32- اونيل سليمان: رئيس قسم الدفاع وتحديات الأمن الالكتروني، اعد دراسة بعنوان (ظهور تحديات جديدة للأمن)...لمزيد اطلع على المقال بصحيفة الرأي، العدد 12138الصادرة في 2012/9/12.

33- عماد المرزوقي، الناتو يرفع درجة خطر الهجمات الالكترونية، مقال منشور على صحيفة الراي، العدد (12138)،