التوفيق بين حوكمة الإنترنت والأمن السيبراني للدول

Reconciling Internet governance and cyber security for countries

د.مناصرة يوسف [1]،

menasra@hotmail.com [1]

تاريخ الإرسال: 2023/02/21 تاريخ القبول: 2023/03/19 تاريخ النشر: 2023/05/31

ملخص:

تُعد كلا من حوكمة الإنترنت والأمن السيبراني من القضايا المهمة التي يجب على الدول معالجتها من أجل ضمان بيئة رقمية آمنة وموثوقة و على الرغم من ارتباطهما ببعضهما البعض ، إلا أنهما يمثلان أيضًا مجالات اهتمام متميزة ، ويمكن أن يكون التوفيق بين الاثنين مهمة معقدة وصعبة على البلدان .تتمثل إحدى طرق التوفيق بين حوكمة الإنترنت والأمن السيبراني في التركيز على بناء استراتيجية وطنية شاملة ومنسقة تعالج كلتا القضيتين .قد تتضمن هذه الاستراتيجية تحديد ومعالجة التحديات والمخاطر الرئيسية المرتبطة بحوكمة الإنترنت ، بما في ذلك القضايا المتعلقة بالوصول والانفتاح والتنظيم ، بالإضافة إلى تلك المتعلقة بالأمن السيبراني ، مثل التهديدات السيبرانية والهجمات الإلكترونية.

كلمات مفتاحية: حوكمة انترنت، أمن سيبراني، هجمات سيبرانية، إدارة الأنترنت، جرائم الكترونية.

Abstract:

Internet governance and cyber security are both important issues that countries must address in order to ensure a safe and secure digital environment. While they are related, they are also distinct areas of concern, and reconciling the two can be a complex and challenging task for countries.

One approach to reconciling internet governance and cyber security is to focus on building a comprehensive and coordinated national strategy that addresses both issues. Such a strategy would involve identifying and addressing the key challenges and risks associated with internet governance, including issues related to access, openness, and regulation, as well as those related to cyber security, such as cyber threats, and cyber attacks.

Keywords: *Internet governance;cybersecurity;cyberattacks; Internet management;cybercrime.*

1- المؤلف المرسل: د/يوسف مناصرة، **الإيميل:** menasra@hotmail.com

مقدمة :

أصبح الإنترنت جزءًا أساسيًا من حياتنا اليومية على المستويين الشخصي والمهني و الإجتماعي و الإقتصادي و الثقافي و في جميع مناحي الحياة، حيث يتم استخدامها للتواصل والتسوق والبحث عن المعلومات والتعلم و العمل عن بعد والعديد من الأنشطة الأخرى و لم يعد صيحة تكنولوجية جديدة. ومع ذلك ، فإن استخدام الإنترنت ينطوي على مخاطر ، مثل انتهاك الخصوصية وسرقة الهوية والقرصنة والجرائم الإلكترونية والإرهاب الإلكتروني. لحماية مستخدمي الإنترنت ، من الضروري وجود تدابير فعالة للأمن السيبراني وإدارة الإنترنت المناسبة بين جميع الدول على قدم المساواة لا تكون الغلبة فيها للدول المتقدمة تكنولوجيا، لذلك فإن الصراع من أجل حوكمة الإنترنت وتحقيق الأمن السيبراني بين الدول لا يزال محتدما و خفيا لا يُناقش في العلن بشكل جلي بالرغم من المحاولات الدولية لإيجاد حل توفيقي تشارك الحكومات والمجتمعات المدنية والتقنية مع جميع أصحاب المصلحة الآخرين في

الحوارات والمنتديات المتعلقة بالإنترنت ، كما كان في القمة العالمية لمجتمع المعلومات (WSIS) التي عقدت على مرحلتين بجنيف سنة 2003 و الثانية بتونس سنة 2005 [1]، ولا تزال الرهانات قائمة لحد الساعة.

و يواجه العالم تحديات متعددة فيما يتعلق بحوكمة الإنترنت في جانبه المتعلق بالأمن السيبراني، وتشمل هذه التحديات التي تعرض المستخدمين والبنية التحتية الحيوية والحكومات للهجمات السيبرانية المدمرة والتجسس الإلكتروني. ومن الجوانب الأخرى في بعدها الدولي التي تجعل من الإدارة المشتركة للإنترنت عويصاً و عائقا كبيرا في تشارك المعلومات، و لعل أكبر هذه التحديات تطوير إطار قانوني وتشريعي وأخلاقي لتحديد المسؤوليات المشتركة بين الحكومات والشركات والمستخدمين في حماية الأمن السيبراني والخصوصية والحقوق الأساسية والحقوق الرقمية. بالإضافة إلى ذلك، تواجه الدول تحديات في التواصل والتعاون الدولي للتعامل مع المشكلات السيبرانية العابرة للحدود، وتطوير إطار دولي للتحكم في النشاطات السيبرانية المتعددة الأطراف وتحديد المسؤوليات المشتركة في حماية الأمن السيبراني.

لذلك، يحتاج التوفيق بين حوكمة الإنترنت والأمن السيبراني للدول إلى جهود دولية واسعة النطاق وتعاون دولي قوي وإطار تشريعي فعال للتغلب على هذه التحديات .

و إن المتوخى من هذا البحث العلمي ، هو تعزيز فهمنا لحوكمة الأنترنت و الحوكمة الرقمية والتحكم في سياسات الأمن السيبراني لتحقيق الاستقرار الدائم والحفاظ على حقوق المستخدمين فضلا عن إبراز مخاطرالتهديدات السيبرانية وتأثيرها على المؤسسات والمجتمعات و ما يشكله موضوع الأمن السيبراني من هاجس جديد يمس بالنظام العام و أمن الدول.

و بالرغم تعقيد الموضوع و تشعبه لا يمكن أن تستوعبه أسطر هذه المقالة العلمية، و يتطلب تقنيات بحثية متقدمة ومنهجيات شاملة للتعامل مع هذه الموضوعات، لكن سنعمد إلى الإجابة على إشكالية كيفية إيجاد توازن لتحقيق تعادل بين حوكمة الأنترنت مع تزايد المخاطر و التهديدات الماسَة بالأمن السيبراني للدول؟.

و للإجابة على هذا التساؤل، سوف نستكشف القضايا الرئيسية لحوكمة الإنترنت والأمن السيبراني ، والجهات الفاعلة المشاركة في هذه المجالات ، والقوانين واللوائح المعمول بها ، في محور أول أما الثاني فنتطرق لتدابير الحماية والأمن المطبقة و الجهود الدولية لمجابهة تحديات الحوكمة و الأمن السيبراني.

1. الانترنت كتراث إنساني مشترك

عندما نتحدث عن التراث الإنساني، فإننا نشير إلى جملة من السمات الجوهرية التي تميز الإنسان وتعكس ثقافته وتاريخه وإرثه الثقافي[2].. وتعد شبكة الإنترنت من أبرز الإنجازات التكنولوجية في العصر الحديث، حيث أصبحت جزءًا لا يتجزأ من حياتنا اليومية وثقافتنا وتراثنا الإنساني المشترك، نتقاسم حياتنا اليومية و نشاطاتنا المهنية و الشخصية فيها.

الانترنت حقا ثروة مشتركة للمجتمع البشري، حوَلت العالم إلى "قرية عالمية" و في الفضاء السيبراني ، جميع البلدان مترابطة وترى مصالحها ومستقبلها مرتبطا ارتباطًا وثيقًا بها، مما يجعل الانفتاح والتعاون والتنمية وبناء مجتمع دولي بأهداف مشترك ، أكثر من ضرورة ملحة لتعزيز الحفاظ على النظام العام العالمي والأمن في الفضاء السيبراني .

و كما يقول أستاذي البروفيسور جان جاك لافينيو "دعونا لا ننسى أن الإنترنت عابر للحدود ، فمن الضروري في هذا المستوى وضع لائحة دولية تحدد مدونات السلوك وقواعد المسؤولية والمعايير التي تحدد ما يندرج تحت نظام دولي عام... و أن هذا الأمر لا يمكن تحديده وفقًا لمعيار شخص واحد ".[3]. بمختصر القول لا يمكن أن يكون الانترنت تحت سيطرة دولة قوية مهيمنة.

و بالنظر للأنشطة الممارسة في الفضاء السيبراني لما لا نعتبر ونعترف بأن الأنترنت فضاء إلكتروني من ممتلكات البشرية جمعاء و تتم إدارتها من قبل سلطة دولية تعمل نيابة عنها مثل سلطة اتفاقية مونتيغو باي لعام 1982[4] على أساس القواعد الدولية[5].

ومع ذلك، يجب مراعاة العديد من القضايا المتعلقة بحفظ الإنترنت كتراث إنساني مشترك، ومن بين هذه القضايا حماية المعطيات الشخصية والحقوق الرقمية والتعددية الثقافية واللغوية. ويجب تحديد السياسات والإجراءات اللازمة للحفاظ على هذا التراث وضمان أن يظل متاحًا للجميع وللأجيال القادمة، كما يجب التعاون الدولي في حماية الإنترنت كتراث إنساني مشترك، وذلك من خلال تطوير المعايير والاتفاقيات الدولية التي تنظم استخدام الإنترنت وحماية الحقوق الرقمية. كما يجب تعزيز التعاون الدولي في مجال البحث والتطوير التكنولوجي للحفاظ على الإنترنت كتراث إنساني مشترك.

1.1 مفهوم حوكمة الأنترنت والأمن السيبراني و ماهيتهما:

حوكمة الإنترنت هي مجموعة القواعد والمعايير والمبادئ التي تحكم استخدام الإنترنت و قد أعطت القمة العالمية لمجتمع المعلومات تعريفا لحوكمة الإنترنت على النحو التالي: " إدارة الإنترنت هي تطوير وتطبيق الحكومات والقطاع الخاص والمجتمع المدني ، كل في دوره ، للمبادئ والقواعد والقواعد

والقرار المشترك و اتخاذ الإجراءات والبرامج التي تشكل تطور واستخدام الإنترنت(WGIG 2005)" [6]. و تشمل قضايا حوكمة الإنترنت (IG) بشكل عام مواضيع ثلاث هي الوصول المفتوح إلى عمليات الحوكمة و أمن واستقرار الشبكة و الإدارة المسؤولة لموارد الإنترنت الهامة.

و تعتبرحوكمة الانترنت عملية تتيح التحكم والإدارة والتنظيم لشبكة الإنترنت والخدمات المرتبطة بها. وهي تشمل الأسس والمبادئ والإجراءات والآليات التي تحدد كيفية توزيع السلطات والمسؤوليات بين مختلف الأطراف ذات الصلة فيما يتعلق بإدارة الإنترنت، مثل الحكومات والشركات والمؤسسات الأكاديمية والمجتمع المدني. وتشمل حوكمة الإنترنت أيضًا السياسات والقوانين واللوائح التي تحكم استخدام الإنترنت وتحديد الحقوق والواجبات المتعلقة به.

يهدف مفهوم حوكمة الإنترنت إلى تحقيق التوازن بين حماية حرية الوصول والتعبير وحماية الأمن السيبراني والخصوصية والملكية الفكرية. وتشمل مجالات الحوكمة الإنترنتية المختلفة مثل حوكمة نطاقات الإنترنت وتوزيع عناوين الـ IP، وإدارة الأمان والخصوصية والحقوق الرقمية والحقوق الإنسانية على الإنترنت وغيرها. تعد حوكمة الإنترنت مهمة بشكل خاص في ضوء الزيادة المستمرة في استخدام الإنترنت وأهميتها الحيوية في حياتنا اليومية، وذلك يستلزم وضع إطار عمل واضح وملائم لحمايتها وتطويرها بشكل مستدام.

وترتبط حوكمة الانترنت بالأمن اسيبراني للدول، لأنه لا يمكن تصور حوكمة في بيئة مليئة بالتهديدات ، تعمها الفوضى و الخروقات ، بل على الأقل بيئة تتوفر على الحماية و يسودها النظام و هو الأمر الحاصل في العالم الإفتراضي Cyberespace و بالشبكات المعلوماتية المنفصلة و المتصلة .

يعود إنشاء كلمة "علم التحكم الآليcybernétique" إلى الأستاذ نوربرت وينر في معهد ماساتشوستس للتكنولوجيا (MIT) ، ، الذي حدد هذا المصطلح في عام 1948 ، "المجال الكامل لنظرية القيادة والاتصالات سواء في الآلة أو في الحيوان". الذي استلهمه من الكلمة اليونانية kuberneïn، والتي تعني "القيادة". بعد عدة عقود ، في عام 1984 ، استخدم مؤلف الخيال العلمي ويليام جيبسون مصطلح الفضاء الإلكتروني cyberspace في روايته The Neuromancer. وبالتدريج ، استخدمت الكلمة الإفتتاحية" cyber-" في بناء الأسماء الجديدة المتعلقة بمجتمع المعلومات الذي ظهر منذ نهاية القرن العشرين. وبالتالي ، فإن الأمن السيبراني سيهتم بالاستخدامات الدفاعية والهجومية لأنظمة المعلومات التي تغرق منظوماتنا الحديثة. يأخذ في عين الاعتبار الوسائل التقنية (الكمبيوتر ، الهاتف ، شبكات الأقمار الصناعية ، إلخ) المستخدمة في تبادل المعطيات ، والتي قد تكون موضوع عمليات تسلل أو تعديل أو تعليق أو حتى انقطاع ، بمعنى جميع المعلومات التي يتم تداولها أو تخزينها على الوسائط الرقمية (مواقع الويب ، وقواعد المعطيات ، والرسائل والاتصالات الإلكترونية ، والمعاملات غير المادية ، وما إلى ذلك) [7].

و يُعرف الأمن السبيراني من طرف الإتحاد الدولي للإتصالات بأنه ((مجموع الأدوات و السياسات و مفاهيم الأمن و المباديء التوجيهية و نهج إدارة المخاطر و الإجراءات و التدريب و أفضل الممارسات و آليات الضمان و تكنولوجيات التي استخدامها في حماية البيئة السيبيرانية و أصول المؤسسات و المستعملين. و تشمل أصول المؤسسات و المستعملين أجهزة الحوسبة الموصولة بالشبكة و الموظفين و البنية التحتية و التطبيقات و الخدمات و أنظمة الاتصالات و مجموع المعلومات المنقولة و / أو المحفوظة في البيئة السيبرانية و يسعى الأمن السيبراني إلى تحقيق خصائص أمن أصول المؤسسة و المستعملين و الحفاظ عليها و حمايتها من المخاطر الأمنية ذات الصلة في البيئة السيبرانية و تضم أهداف العامة للأمن مايلي: التيسر، السلام ، التي قد تضم الإستيقان و عدم الرفض، السرية)) [8].

كما يعرفه Edward Amoroso بأنه ((مجموع الوسائل التي من شأنها الحذ1من خطر الهجوم على البرمجيات أو أجهزة الكمبيوتر أو الشبكات و تشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة و كشف الفيروسات الرقمية و ووقفها، و توفير الاتصالات المشفرة.[9]

و عليه يمكن القول بأن الأمن السيبراني هو حماية تقنية و تشريعية أيضا للأنظمة المعلوماتية و للأجهزة الإلكترونية والشبكات بمختلف أنواعها و أحجامها والبرامج والمعطيات من الهجمات السيبرانية والتهديدات الإلكترونية وتأمينها ضد التخريب أو القرصنة أو الجوسسة."الخ.

وفقًا للمرجع العالمي للمعهد القومي للمعايير والتكنولوجياNIST بالولايات المتحدة الأمريكية حول تقييم المخاطر و الأداء في الأمن السيبراني[10]، يشمل الأمن السيبراني خمسة مكونات رئيسية هي: الحماية :(Protect) وهي القدرة على تحديد وتنفيذ إجراءات الحماية الواجب اتخاذها لمنع الهجمات الإلكترونية .و الكشف :(Detect) وهو القدرة على رصد الهجمات الإلكترونية وتحديد مصادرها والتصدي لها، ثم الاستجابة :(Respond) وهي القدرة على التعامل مع الهجمات الإلكترونية المكتشفة واتخاذ الإجراءات اللازمة لمعالجتها.، وتليها عملية الاسترجاع :(Recover) وهي القدرة على استعادة المعطيات والنظم والشبكات المتأثرة بالهجوم الإلكتروني بسرعة وفعالية. و بعدها الإدارة :(Govern)وهي القدرة على توفير الإطار القانوني والتنظيمي والإداري اللازم للحماية السيبرانية[11].

و يهدف الأمن السيبراني إلى ضمان أمن البيئة السيبرانية في الأنظمة المعلوماتية، و هو نظام قد يشمل أصحاب المصلحة الذين ينتمون إلى العديد من منظمات القطاعين العام و الخاص، باستخدام مكونات متنوعة و أساليب مختلفة لتحقيق الأمن.

أما بالجزائر، فإن الأمن السيبراني يعد من أولويات الحكومة في الوقت الراهن في خضم التغيرات و المعطيات الجيوستراتيجية الإقليمية و الدولية، لذلك فقد تم إنشاء منظومة وطنية لأمن الأنظمة المعلوماتية موضوعة لدى وزارة الدفاع الوطني، حيث تعتبر أداة الدولة في هذا المجال[12]، كما أنها تشكل الإطار التنظيمي لإعداد الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية و تنسيق تنفيذها. و تشمل هذه المنظومة، مجلسا وطنيا يكلف بإعداد الاستراتيجية الوطنية و الموافقة عليها وتوجيهها ووكالة تضطلع بتنسيق تنفيذ هذه الاستراتيجية.

و من بين المهام التي يتولاها المجلس الذي يرأسه وزير الدفاع الوطني أو ممثله، "الموافقة على اتفاقات التعاون والاعتراف المتبادل مع الهيئات الأجنبية في مجال أمن الأنظمة المعلوماتية و سياسة التصديق الالكتروني و تصنيف الأنظمة المعلوماتية"، فضلا عن "إبدائه رأيا متطابقا في أي مشروع نص تشريعي أو تنظيمي" ذي صلة بهذا الموضوع.

وبالنسبة للوكالة أمن الأنظمة المعلوماتية، تعتبر مؤسسة عمومية ذات طابع إداري و تتمتع بالشخصية المعنوية و الاستقلالية المادية، وتتكفل بجملة من المهام، على غرار "اقتراح كيفيات اعتماد مزودي خدمات التدقيق في مجال أمن هذا النوع من الأنظمة و "السهر على جمع و تحليل و تقييم المعطيات المتصلة بمجال أمن الأنظمة المعلوماتية لاستخلاص المعلومات الملائمة التي تسمح بتأمين منشآت المؤسسات الوطنية.

كما تعمل هذه الوكالة أيضا على تحديد معايير و إجراءات منح علامات الجودة و/أو التصديق و/أو اعتماد المنتجات و مقدمي الخدمات في مجال أمن الأنظمة المعلوماتية"، إلى غير ذلك.و بمقتضى ذات المرسوم الرئاسي، فإن الوكالة "مؤهلة لطلب أي وثيقة أو معلومة مفيدة للقيام بالمهام الموكلة إليها من الهيئات

والمؤسسات والمتعاملين المزودين بنظام إعلام. و سيكون على المؤسسات و الإدارات والهيئات العمومية والمتعاملين الخواص، تعيين مسؤولهم المكلف بأمن الأنظمة المعلوماتية "في أجل أقصاه سنة" ابتداء من نشر المرسوم في الجريدة الرسمية[13].

كما تشارك وزارة البريد و الاتصالات الالكترونية في أمن المعلومات من خلال إعدادها المرجع الوطني لأمن المعلومات(RNSI) ، الذي يهدف إلى إقامة حوكمة و نهج موحّد لأمن المعلومات داخل الهيئات والمؤسسات. لأنه يحدد الحد الأدنى من المتطلبات المتعلقة بالأمن، وذلك من أجل تسيير ومقاومة والتقليل من أثر التهديدات المتوقعة. زيادة على ذلك، إن مرجع امن المعلومات يقدم الضوابط الأمنية و أفضل الممارسات التي يجب أن تتبناها الهيئات العمومية، مع التركيز على تدريب وتوعية المستخدمين بالمخاطر التي تنطوي عليها، والتقييم الدوري للضوابط من أجل ضمان الرضا المستمر للمتطلبات الأمنية و الامتثال للالتزامات التنظيمية.

لكن في إعتقادي أن مهمة الأمن السيبراني ليست منوطة بشكل حصري للدولة فقط، بل إن الأمن السيبراني ليس من اختصاص الحكومات أو الجيوش النظامية، و إنما هم جزء كبير من مع جهات فاعلة أخرى من بين آخرين، من المستخدم البسيط إلى المنظمات الدولية .

2.1. الجهات الفاعلة المشاركة في إدارة الإنترنت والأمن السيبراني:

تشمل الجهات الفاعلة المشاركة في إدارة الإنترنت والأمن السيبراني الحكومات، المنظمات الدولية، الشركات، مجموعات المجتمع المدني والمستخدمين أنفسهم. ويتضمن الأطراف الرئيسية التالية:

1. **الحكومات**: تضع الحكومات قوانين ولوائح لحماية المستخدمين من المخاطر السيبرانية وضمان حرية الوصول إلى الإنترنت. كما تقوم بإنشاء هيئات تنظيمية لإدارة الإنترنت وتعزيز الأمن السيبراني[14].
2. **المنظمات الدولية**: تلعب المنظمات الدولية دوراً هاماً في تحديد المعايير والمبادئ التوجيهية لإدارة الإنترنت والأمن السيبراني، بالإضافة إلى توفير الدعم الفني والمالي للدول والمنظمات ذات الصلة[15].
3. **الشركات**: تلعب الشركات دوراً مهماً في تقديم حلول تقنية للحد من المخاطر السيبرانية، وتحسين الأمن والخصوصية للمستخدمين. وتساهم الشركات أيضاً في تطوير المعايير الصناعية والتوجيهات التقنية للأمن السيبراني[16].
4. **مجموعات المجتمع المدني**: تعزز مجموعات المجتمع المدني الوعي بالمخاطر السيبرانية وتحث على إنشاء إطار تشريعي ورقابي فعال للحفاظ على الأمن والخصوصية على الإنترنت. كما تقوم هذه المجموعات بمراقبة تنفيذ السياسات والقوانين ذات الصلة[17].
5. **المستخدمون**: يلعب المستخدمون دوراً هاماً في الحفاظ على أمنهم على الإنترنت من خلال اتباع الممارسات الآمنة وتجنب التصرفات الخطرة.

علاوة على ذلك ، في كثير من البلدان ، ليست الدولة هي اللاعب الأساسي في تحقيق الحوكمة و الأمن السيبراني. فيجب التعامل في كثير من الأحيان مع القطاع الخاص لاسيما الشركات و المؤسسات التجارية ، الذين غالبًا ما يكونون أقل مرونة وتفاعلًا مع طلبات سلطات إنفاذ القانون، ودرجة الإستجابة متفاوتة بين الأطراف الفاعلة السالف ذكرها أعلاه.[18]

والملاحظ أن مجال حوكمة الانترنت و الأمن السيبراني يواجه العديد من التحديات، من أصعبها على الإطلاق الحفاظ على حرية الإنترنت،إذ يجب أن

تكون حوكمة الإنترنت شفافة وتعزز حقوق الأفراد في الوصول إلى المعلومات وتبادلها والتواصل الحر و بدرجة ثانية يجب أن تتخذ إدارة الإنترنت تدابير فعالة لحماية المستخدمين من التهديدات السيبرانية، والتي تتضمن الهجمات الإلكترونية والبرمجيات الخبيثة والاحتيال والاختراقات...الخ، فضلا عن حماية الخصوصية الشخصية للمستخدمين، ومنع جمع المعطيات الشخصية بشكل غير مشروع أو استخدامها بطريقة غير مشروعة.

في الوقت الراهن، هناك العديد من المنظمات المشاركة في إدارة الإنترنت على مستوى العالم ومعالجة القضايا المذكورة أعلاه ، من بينها وأولها منظمة الإنترنت العالمية ICANN[19] وIANA و الاتحاد الدولي للاتصالات (ITU)، ثم المنظمات الإقليمية مثل أفرينيك التي تتعاون عن كثب مع هذه المنظمات العالمي مثل AF*[21],IGFXNUMX[20]، NRO[22]، WTDC[23]،و أصحاب المصلحة الآخرين والمؤسسات الأخرى ذات الصلة التي تهتم بقضايا حوكمة الإنترنت على المستوى العالمي. لكن أمل الشعوب و الدول في إنشاء هيئة دولية أممية لإدارة الانترنت لم يتحقق لإختلاف المصالح الدولية و يتطلب بذل مجهودات دولية كبرى لتحقيقها و هذا ما تسعى إليه القمة العالمية لمجتمع المعلومات في لقاءاتها الدورية.

2. الجهود الدولية لتحقيق الأمن السيبيراني و حوكمة انترنت مشتركة

إن تحقيق حوكمة إنترنت مشتركة هو موضوع مثير للجدل وله العديد من الجهود الدولية لتحقيقه. تقوم العديد من المنظمات الدولية بالعمل معًا لتحقيق هذه الهدف، مثل الأمم المتحدة، والاتحاد الأوروبي، ومنظمة التعاون الاقتصادي والتنمية.

يعمل الاتحاد الأوروبي على وضع تشريعات لحماية الخصوصية والمعطيات الشخصية للمواطنين، كما أنه يعمل على تحسين الأمن السيبراني من خلال الإستثمار في تكنولوجيا الأمن السيبراني وتعزيز الوعي بالأمان السيبراني. وفي عام 2016، قام الاتحاد الأوروبي بإطلاق خطة عمل الأمن السيبراني الأوروبية بهدف تحقيق الأمن السيبراني في الاتحاد الأوروبي.

وفي الأمم المتحدة، تم إنشاء مجموعة العمل الحكومية حول تحقيق الأمن السيبراني في عام 2004، والتي تهدف إلى تحسين الحوكمة والتعاون الدولي في مجال الأمن السيبراني. كما أن المنظمة الدولية للاتصالات تعمل على توفير إرشادات للدول حول كيفية تحسين الأمن السيبراني والحوكمة في القطاعات العامة والخاصة.

وفي إطار المنظمات الإقليمية، تعمل جمعية دول جنوب شرق آسيا (ASEAN)على تطوير الاستراتيجيات الإقليمية لتعزيز الأمن السيبراني، كما أن منظمة شنغهاي للتعاون (SCO) تعمل على تعزيز التعاون في مجالات الأمن السيبراني بين دولها الأعضاء.أما بدول الإتحاد الإفريقي تم ابرام اتفاقية مالابو عام 2014 تعنى بمكافحة الجرائم الالكترونية و الأمن السيبراني و حماية المعطيات الشخصية(لم تصادق عليها الجزائربعد).

و معلوم لدى العام و الخاص أن العالم اليوم يشهد تزايداً في حالات الهجمات السيبرانية، مما يستدعي تعزيز الجهود الدولية للحد من هذه الجرائم وتحقيق الأمن السيبراني[24]. وتتمثل الجهود الدولية في هذا المجال في إبرام عدة اتفاقيات و صكوك دولية و إقليمية ذات بعد دولي كالاتفاقية الدولية لمكافحة الجريمة الإلكترونية، أو ما تعرف باتفاقية بودابست التي وقعت عام 2001 وتهدف إلى تحديد أشكال الجرائم السيبرانية وتوحيد الجهود الدولية لمكافحتها و الإتفاقية

الأوروبية لحماية حقوق الإنسان والحريات الأساسية على الإنترنت الموقعة عام 2014 وتعتبر الأولى من نوعها التي تهتم بحماية الحقوق والحريات على الإنترنت.و المبادرة العالمية للأمن السيبراني وهي مبادرة أمريكية تم إطلاقها عام 2011 تهدف إلى تعزيز التعاون الدولي في مجال الأمن السيبراني وتطوير القدرات الوطنية في هذا المجال[25].و إقتراحات المجلس الأوروبي بشأن استراتيجية الاتحاد الأوروبي للأمن السيبراني بشأن أمن الشبكات والمعلومات (عام2014)[26] أين تؤكد استنتاجات مجلس الاتحاد الأوروبي على الحاجة الملحة إلى تعزيز التعاون الدولي لضمان أمن ومرونة البنى التحتية الرقمية.، و كذا المنتدى الحكومي لتعزيز الأمن السيبراني وهو منتدى دولي يجمع ممثلين من الحكومات والقطاع الخاص والمجتمع المدني لمناقشة أفضل السياسات والممارسات لتعزيز الأمن السيبراني،و جدير بالتنويه بأهمية حذو نهج الولايات المتحدة الأمريكية و الصين في تقليل التجسس الإلكتروني بإبرام إتفاقية ثنائية عام 2015 تهدف إلى تقليل التجسس الإلكتروني بين البلدين[27].

يمكن القول أن هناك العديد من الجهود الدولية التي تسعى إلى تحقيق حوكمة إنترنت مشتركة و تحقيق حد أدنى من الأمن السيبراني العالمي.

1.2. تحديات حوكمة الإنترنت والأمن السيبراني:

يواجه العالم اليوم العديد من التحديات المعقدة والمتطورة باستمرار في مجال حوكمة الإنترنت والأمن السيبراني، ومن بين هذه التحديات :

1- **الهجمات الإلكترونية** حيث يشكل الهجوم الإلكتروني تحديًا كبيرًا للأمن السيبراني، و يمكن أن يؤدي إلى تسريب المعلومات الحساسة والمالية، وإيقاع الأضرار الكبيرة بالمؤسسات الحكومية والشركات والأفراد، **مما يتطلب حماية من الجرائم الإلكترونية** بحماية أنظمة وشبكات الكمبيوتر من

الهجمات الضارة ، مثل الفيروسات والبرامج الضارة وبرامج الفدية وهجمات رفض الخدمة.

2- **حماية الخصوصية و المعطيات الشخصية**: يجب أن يتأكد مستخدمو الإنترنت من أن بياناتهم الشخصية محمية ضد سوء الاستخدام والتجميع المفرط. و تعد حماية المعطيات الشخصية موضوعًا مهمًا هذه الأيام ، أين يتم جمع المزيد والمزيد من المعطيات حول الأشخاص .تتضمن المعطيات الشخصية معلومات مثل الأسماء والعناوين وأرقام الهواتف وعناوين البريد الإلكتروني وأرقام الضمان الاجتماعي والمعلومات المالية .يتم تنظيم جمع هذه المعطيات ومعالجتها بموجب القوانين واللوائح ، مثل اللائحة العامة لحماية المعطيات (GDPR) بأوروبا وقانون خصوصية المستهلك في كاليفورنيا (CCPA) بالولايات المتحدة و قانون حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي بالجزائر(رقم 18-07) .تتطلب هذه القوانين من الشركات والمؤسسات حماية المعطيات الشخصية واستخدامها بشكل شرعي والسماح للأفراد بممارسة حقوقهم في بياناتهم .من المهم للأفراد فهم كيفية جمع معطياتهم الشخصية واستخدامها واتخاذ خطوات لحماية معلوماتهم الشخصية .تشمل تدابير حماية المعطيات الشخصية استخدام كلمات مرور قوية ، والتحقق من أمان مواقع الويب والتطبيقات، والتحقق من سياسات خصوصية الشركات ، وممارسة حقوقها على بياناتها، مثل حق الوصول والتصحيح والحذف وقابلية النقل .في النهاية ، تعد حماية المعطيات الشخصية مهمة لضمان خصوصية الأفراد وأمنهم ، وكذلك لبناء الثقة بين الشركات والمستهلكين.

3- **تنظيم المحتوى**: الإنترنت هو مساحة مفتوحة حيث يمكن لأي شخص نشر محتوى ، مما قد يؤدي إلى إساءة استخدام المحتوى وغير القانوني ، مثل المواد الإباحية للأطفال والدعاية الإرهابية وخطاب الكراهية.و يهدف تنظيم

المحتوى على الإنترنت إلى ضمان حماية المستخدمين من المحتوى غير المشروع وضمان عدم تعرضهم للإساءة عبر الإنترنت.

4- **تنظيم منصات الإنترنت**: المنصات على الإنترنت ، مثل الشبكات الاجتماعية ومحركات البحث ومواقع التجارة الإلكترونية ، لها تأثير كبير على حياة مستخدمي الإنترنت ، ويجب تنظيمها لضمان شفافيتهم ومسؤوليتهم. و تنظيم منصات الإنترنت يشمل تنظيم الشركات المشغلة للمنصات والتأكد من موائمتها للمعايير الأخلاقية والقانونية.

5- **الوصول إلى الإنترنت**: يجب ضمان الوصول إلى الإنترنت للجميع ، دون تمييز أو قيود ، من أجل ضمان تكافؤ الفرص وحرية التعبير.و يعتبرالوصول إلى الإنترنت هو حق أساسي للجميع ومن أهم الوسائل لتحقيق التنمية الاجتماعية والاقتصادية والثقافية في العالم الحديث. ومع ذلك، فإن هناك عددًا من العوائق التي يواجهها بعض الأفراد والجماعات في الوصول إلى الإنترنت. تتضمن هذه العوائق على سبيل المثال لا الحصر، نقص التغطية الجغرافية لخدمات الإنترنت في بعض المناطق، وعدم توفر بنية تحتية كافية للاتصالات، وارتفاع تكلفة الوصول إلى الإنترنت بالنسبة لبعض الأفراد والجماعات الفقيرة، والحظر الحكومي للمواقع والخدمات على الإنترنت.و تعمل العديد من المنظمات والحكومات على تقليل هذه العوائق وزيادة فرص الوصول إلى الإنترنت، من خلال تطوير البنية التحتية وتخفيض التكلفة وتعزيز التغطية الجغرافية، بالإضافة إلى تشجيع الحكومات على عدم فرض حظر على الإنترنت إلا في الحالات المشروعة والضرورية.ومن الجدير بالذكر أن الوصول إلى الإنترنت لا يعتبر مجرد حق فقط، بل هو أيضًا فرصة لتعزيز التعليم والثقافة والتنمية الاجتماعية والاقتصادية للفرد والمجتمع ككل.

لأجل مواجهة هذه التحديات يتوجب تطوير السياسات والإجراءات اللازمة لحماية الإنترنت والأجهزة الإلكترونية، وتعزيز التعاون الدولي لوضع المعايير الدولية المناسبة وتطوير التقنيات الحديثة والتدريب على الأمن السيبراني.

2.2 الصراع الدولي من أجل حوكمة أنترنت و توفير الأمن السيبراني:

تلعب الدول المتقدمة دورًا هامًا في حوكمة الإنترنت، حيث تمتلك موارد تكنولوجية ومؤسساتية وقانونية وسياسية تساعدها على التأثير في السياسات والمعايير الدولية المتعلقة بالإنترنت. ومن أمثلة هذه المؤسسات الدولية هي منظمة الأمم المتحدة ومنظمة الأيكان وغيرها. ويتم تحديد سياسات الإنترنت وتطوير المعايير الدولية وفقًا لمبادئ الحوكمة الإلكترونية، مثل التشاور والشفافية والمساءلة والمشاركة.

من جهة أخرى، تواجه الدول المتخلفة تحديات عديدة في تحسين حوكمة الإنترنت، حيث أنها تعاني من نقص الموارد التكنولوجية والمؤسساتية والقانونية والسياسية التي تدعم التأثير في السياسات والمعايير الدولية. وتواجه هذه الدول أيضًا تحديات في تنظيم النفاذ إلى الإنترنت وتطبيق القوانين وحماية الحقوق الرقمية.لذا يتعين على الدول المتخلفة العمل على تحسين حوكمة الإنترنت من خلال توفير الموارد التكنولوجية والمؤسساتية والقانون.

غير أن الواقع الدولي يخفي بين جنباته صراعا خفيا حول حوكمة الإنترنت يشير إلى التنافس بين الدول والمنظمات الدولية بُغية السيطرة على شبكة الإنترنت وتطبيق القواعد واللوائح على استخدامها التي تناسبها. تتراوح هذه الصراعات من النزاعات السياسية والاقتصادية حول التحكم في المعلومات والتكنولوجيا وحماية الخصوصية والأمن السيبراني و تطبيق القوانين واللوائح

على الشركات التكنولوجية العملاقة. كما تشمل المناقشات حول حقوق الأفراد والحريات الأساسية على الإنترنت وحماية المعطيات الشخصية.

تعمل المنظمات الدولية مثل الأمم المتحدة والاتحاد الأوروبي ومنظمة التجارة العالمية على وضع القواعد واللوائح والاتفاقيات الدولية التي تنظم استخدام الإنترنت. وتعمل بعض الدول على تطوير قوانين ولوائح محلية للحد من الانتهاكات على الإنترنت كما أسلفنا أعلاه، لكن من الصعب التوصل إلى اتفاق دولي واحد حول حوكمة الإنترنت بسبب اختلاف الرؤى والمصالح الاقتصادية والسياسية للدول المختلفة. ومع ذلك، يمكن تحسين حوكمة الإنترنت من خلال تعزيز التعاون الدولي والتشاور والحوار وتطوير القواعد واللوائح الدولية المناسبة لتنظيم استخدام الإنترنت بشكل أفضل.

الخاتمة:

تشهد حوكمة الإنترنت والأمن السيبراني تطورات قانونية وتشريعية مستمرة على المستوى الدولي والمحلي. فعلى الصعيد الدولي تم تبني العديد من الاتفاقيات والقوانين على المستوى الدولي لتعزيز حوكمة الإنترنت والأمن السيبراني، مثل ميثاق الأمم المتحدة الخاص بحقوق الإنسان ومبادئه المتعلقة بحرية التعبير والخصوصية على الإنترنت، واتفاقية مجلس أوروبا بشأن الجرائم الإلكترونية وغيرها. أما على الصعيد المحلي تعمل الحكومات على تطوير قوانين ولوائح محلية لتعزيز حوكمة الإنترنت والأمن السيبراني، وذلك للتعامل مع التهديدات السيبرانية وضمان حماية حقوق المستخدمين على الإنترنت.

ومن المتوقع مستقبلا أن تشهد حوكمة الإنترنت والأمن السيبراني تطورات متسارعة في ظل التقدم التكنولوجي والاعتماد المتزايد على الإنترنت. ومن

المتوقع أن تستمر الجهود القانونية والتشريعية لتحسين حوكمة الإنترنت وتعزيز الأمن السيبراني، بتطوير تشريعات وقوانين جديدة للتعامل مع التحديات الناشئة مثل الذكاء الاصطناعي وإنترنت الأشياء.

إقتراحات من أجل حوكمة الإنترنت والأمن السيبراني

إن تحسين حوكمة الإنترنت والأمن السيبراني يتطلب جهودًا متعددة ومنسقة من قبل الحكومات والشركات والمجتمع المدني والأفراد. وفيما يلي بعض الاقتراحات التي يمكن تبنيها لتحسين حوكمة الإنترنت والأمن السيبراني:

1- تشجيع التعاون الدولي، إذ ينبغي على الدول والمؤسسات الدولية التعاون والتنسيق للحد من الجرائم السيبرانية وتطوير المعايير الدولية لحماية الأمن السيبراني.
2- ينبغي على الحكومات والمؤسسات التعاون لتعزيز الوعي بالأمن السيبراني وتوعية المستخدمين بالمخاطر المتعلقة بالإنترنت وكيفية الحماية منها و تقوية التدريب.
3- يجب على الدول تحديث وتحسين القوانين واللوائح المتعلقة بالأمن السيبراني وإدارة الانترنت على الإنترنت.
4- يُرجى من الشركات المنتجة للبرامج والأجهزة الحاسوبية تطوير التكنولوجيا الأمنية وتشجيع المستخدمين على استخدام هذه التقنيات.
5- يجب على الحكومات والشركات العاملة في مجال الإنترنت تعزيز الشفافية والمساءلة فيما يتعلق بالحماية من الجرائم السيبرانية والتعامل مع المعطيات الشخصية للمستخدمين.
6- يجب على جميع الأطراف المعنية - الحكومات والشركات والمستخدمين أن يتحملوا مسؤولية مشتركة للحفاظ على الأمن السيبراني وتحقيق

الحوكمة الرقمية الفعالة، و ينبغي تعزيز التعاون بين القطاعين العام والخاص لتحقيق الحوكمة الرقمية الفعالة وتعزيز الأمن السيبراني.

التهميش و الإحالات :

[1] أول حدث في جنيف استضافته حكومة سويسرا في الفترة من 10 إلى 12 ديسمبر 2003 ، والثاني في تونس استضافته حكومة تونس في الفترة من 16 إلى 18 نوفمبر 2005. للمزيد عن https://www.itu.int/net/wsis

[2] التراث المشترك للإنسانية يسمى أيضًا التراث المشترك للبشرية أو التراث المشترك للجنس البشري أو مبدأ التراث المشترك) هو مبدأ من مبادئ القانون الدولي ينصّ على وجوب حماية مناطق إقليمية محددة وعناصر من التراث المشترك للإنسانية (ثقافية وطبيعية) من استغلال فرادى الدول أو الشركات وإبقائها في أمان للأجيال القادمة.

[3] Professeur Jean-Jacques Lavenue, Directeur de l'IREENAT Université de Lille 2, « Internet, droit et administration électronique », *Revue Tunisienned'Administration Publique*,conférence à l'ENA de Tunis, 10 mars 2004.

[4] إتفاقية الأمم المتحدة لقانون البحار United Nations Convention on the Law of the Sea (UNCLOS)، والمعروفة أيضًا باسم اتفاقية قانون البحار أو معاهدة قانون البحار المبرمة بـمونتيغو باي –جمايكا،10ديسمبر 1982. تاريخ النفاذ 16 نوفمبر 1994.

[5] يقول الأستاذ جون جاك لافينو "

« *Pourquoi ne pas envisager à propos des activités s'exerçant dans un espace virtuel Cyberespace incoercible) que celui-ci soit reconnu appanage de l'humanité toute entière et gérée par une autorité internationale agissant en son nom (comme l'Autorité de la Convention de Montego Bay de 1982) le fait, sur la base de règles internationales?*» Professeur Jean-Jacques Lavenue, « Cyberespace et Droit International :pour un nouveau Jus Communicationis », *Revue de la Recherche Juridique: Droit prospectif*, n° 1998.

[6] القمة العالمية، لمجتمع المعلومات، جنيف 2003 – تونس 2005،الوثيقة -WSIS 03/GENEVA/DOC/4-A، 12 ديسمبر 2003

[7] Nicolas Arpagian, La cybersécurité, Année : 2015, Pages : 128, Collection : Que sais-je ? Éditeur : Presses Universitaires de France

[8] التوصية X-1205 (04/2008) للإتحاد الدولي للإتصالات. ، أنظر
http://www.itu.int/ITU-T/ipr

[9] Edward Amoroso Cyber Security Relié – 27 septembre 2006, Éditeur : Silicon Pr (27 septembre 2006) Langue : Anglais Relié : 177 pages ISBN-10 : 0929306384.

[10] https://www.nist.gov/cyberframework

[11] يمكن الاستشهاد بالعديد من المراجع المهمة لفهم مفهوم الأمن السيبراني، أهمها:

- "Cybersecurity: What You Need to Know" من قبل RSA Conference// https://www.rsaconference.com/usa
- "NIST Cybersecurity Framework" من قبل معهد المعايير والتكنولوجيا الوطني (NIST)
- "Understanding Cybersecurity: A Guide for Business Leaders" من قبل Harvard Business Review
- Joseph Steinberg ,Cybersecurity For Dummies (For Dummies (Computer/Tech)), ISBN-10 :1119560322 , Edition :1st , Publisher :For Dummies, Publication date :October 15, 2019 ,368 pages.

[12] تسهر الدولة على سلامة شبكات الاتصالات الالكترونية فهي مهمة من مهمات الدولة طبقا للمادة 4 من القانون رقم قانون رقم18-04، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية

[13] مرسوم رئاسي رقم 20-05 ممضي في 20 يناير 2020، وزارة الدفاع الوطني، الجريدة الرسمية عدد 4 مؤرخة في 26 يناير 2020، الصفحة 5، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.

[14] 1.- Cybersecurity in the European Union: Maintaining and Enhancing Security and Freedom in the Digital Age" (European Commission, 2013) : https://ec.europa.eu/digital-single-market/en/news/cybersecurity-european-union-maintaining-and-enhancing-security-and-freedom-digital-age.2.- "National Cyber Strategy of the United States of America" (The White House, 2018) : https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

[15] 1- "World Summit on the Information Society" (International Telecommunication Union, 2005) :

https://www.itu.int/net/wsis/docs2/declaration/Mission_Statements/Building_confidence_security_WSIS_Geneva_2003.pdf

2- "The Budapest Convention on Cybercrime" (Council of Europe, 2001) : https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[16] 1- "Internet Security Threat Report" (Symantec, 2021) : https://www.symantec.com/content/dam/symantec/docs/reports/istr-26-2021-en.pdf

2- "The State of Cybersecurity 2020" (ISACA, 2020) : https://www.isaca.org/-/media/info/cybersecurity/cybersecurity-nexus/2020-state-of-cybersecurity-report.pdf

[17] 1- "The Cybersecurity Canon: Must-Read Books" (Cybersecurity Ventures, 2020) : https://cybersecurityventures.com/cybersecurity-canon-must-read-books/

2- "Global Cybersecurity Index 2020" (International Telecommunication Union, 2020) : https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2020-PDF-E.pdf

[18] Nicolas Arpagian, La cybersécurité, Année : 2015, Pages : 128, Collection : Que sais-je ? Éditeur : Presses Universitaires de France.

[19] منظمة آيكان (ICANN):منظمة شركة الإنترنت للأسماء والأرقام المخصصة (ICANN) هي منظمة غير ربحية تنسق نظام اسم النطاق (DNS) ، وعناوين بروتوكول الإنترنت (IP) ، وتخصيص المساحة ، وتعيين معرف البروتوكول ، العام (gTLD) ورمز الدولة (ccTLD) وتقوم بإدارة نظام اسم نطاق المستوى الأعلى ، وخادم الجذر وظائف إدارة النظام.

منظمة أيانا (IANA): منظمة هيئة الأرقام المخصصة للإنترنت (IANA) مسؤول عن التنسيق العالمي لجذر DNS وعناوين وموارد بروتوكول الإنترنت IP . تدير IANA المجموعة العالمية لأرقام الإنترنت (بروتوكولات الإنترنت وبروتوكولات الإنترنت المستقلة وأرقام النظام الذاتي (ASNs) وتوزيعها على سجلات الإنترنت الإقليمية الخمسة (RIRs).

[20] منتدى حوكمة الإنترنت العالمي: منظمة منتدى حوكمة الإنترنت (IGF) الذي أنشأه الأمم المتحدة في أعقاب جلسات عمل القمة العالمية لمجتمع المعلومات (WSIS). منتدى حوكمة الإنترنت هو عبارة عن منصة سنوية للتشاور مع أصحاب المصلحة المتعددين من أجل الإخاء العالمي للإنترنت لاستكشاف ومناقشة وحل المشكلات ذات الصلة بالإنترنت. منذ عام

2006 ، يجمع منتدى إدارة الإنترنت بين أصحاب المصلحة من القطاع الحكومي والصناعة والمجتمع المدني لمناقشة قضايا إدارة الإنترنت في الاجتماعات السنوية.

[21] * AF هي المنظمات التي تشكل النظام البيئي للإنترنت الأفريقي. تعود فكرة إنشاء منظمات إعادة تجميع * AF التي تدعم تطوير الإنترنت في إفريقيا إلى ديسمبر 1998. تم تنظيم اجتماع عُقد في كوتونو ، بنين حيث ناقش رواد الإنترنت الأفارقة موضوع إدارة الإنترنت في إفريقيا. كان هذا أول اجتماع عالمي حول إدارة الإنترنت لمناقشة قضايا إدارة الإنترنت في المنطقة الأفريقية.

[22] في 24 أكتوبر 2003 ، الأربعة سجلات الإنترنت الإقليمية الموجودة RIR s - APNIC و ARIN و LACNIC و NCC RIPE - أبرمت مذكرة تفاهم مع الآيكان ICANN لتشكيل منظمة موارد الأرقام (NRO).

منظمة موارد الأرقام (NRO) هي هيئة تنسيق لسجلات الإنترنت الإقليمية الخمسة (RIR s) التي تدير توزيع موارد أرقام الإنترنت بما في ذلك عناوين IP وأرقام النظام المستقل. كل RIR يتكون من مجتمع الإنترنت في منطقته.

[23] المؤتمر العالمي لتنمية الاتصالات (WTDC 2014) - طريق أفرينيك لبناء القدرات الاتحاد السادس المؤتمر العالمي لتنمية الاتصالات (WTDC) في دولة الإمارات العربية المتحدة اختتم الأسبوع الماضي في دبي. وكان موضوع WTDC-14 هو "النطاق العريض من أجل التنمية المستدامة".

لمزيد من التفصيل أنظر https://www.afrinic.net/ar/internet-governance#others

[24] "Global Commission on Internet Governance" (Centre for International Governance Innovation, 2016) : https://www.ourinternet.org/report. "Cyber Diplomacy" (The Hague Centre for Strategic Studies, 2017) : https://hcss.nl/report/cyber-diplomacy.

[25] "International Strategy for Cyberspace" (US Department of State, 2011) : https://www.state.gov/international-strategy-for-cyberspace/

[26] https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/ ar / jha / 144424.pdf

[27] يمكن الاطلاع على نص الاتفاقية وتفاصيلها من خلال الموقع الرسمي لوزارة الخارجية الأمريكية:

https://www.state.gov/the-u-s-china-cyber-agreement/

أنظر أيضا مقال نشره موقع "فورين بوليسي(Foreign Policy)، "في 27 يوليو 2021 والذي يتحدث عن تداعيات هذه الاتفاقية وعن الوضع الراهن للعلاقات الأمريكية الصينية في مجال السيبرانية:

https://foreignpolicy.com/2021/07/27/china-us-cyber-agreement-trump-xi/

قائمة المراجع:

- **المؤلفات:**

1. Nicolas Arpagian, La cybersécurité, Année : 2015, Pages : 128, Collection : Que sais-je ? Éditeur : Presses Universitaires de France
2. Edward Amoroso Cyber Security Relié – 27 septembre 2006, Éditeur : Silicon Pr (27 septembre 2006) Langue : Anglais Relié : 177 pages ISBN-10 : 0929306384.
3. Joseph Steinberg ,Cybersecurity For Dummies (For Dummies (Computer/Tech)), ISBN-10 :1119560322 , Edition :1st , Publisher :For Dummies, Publication date :October 15, 2019 ,368 pages.

- **المقالات والتقارير:**

1. Professeur Jean-Jacques Lavenue, Directeur de l'IREENAT Université de Lille 2, « Internet, droit et administration électronique », *Revue Tunisienned'Administration Publique*,conférence à l'ENA de Tunis, 10 mars 2004.
2. Professeur Jean-Jacques Lavenue, « Cyberespace et Droit International :pour un nouveau Jus Communicationis », *Revue de la Recherche Juridique: Droit prospectif*, n° 1998.
3. Cybersecurity in the European Union: Maintaining and Enhancing Security and Freedom in the Digital Age" (European Commission, 2013).
4. .-"National Cyber Strategy of the United States of America" (The White House, 2018).
5. "World Summit on the Information Society" (International Telecommunication Union, 2005).
6. "Internet Security Threat Report" (Symantec, 2021).

7. "The State of Cybersecurity 2020" (ISACA, 2020)
8. "The Cybersecurity Canon: Must-Read Books" (Cybersecurity Ventures, 2020).
9. "Global Cybersecurity Index 2020" (International Telecommunication Union, 2020).
10. "International Strategy for Cyberspace" (US Department of State, 2011).

- **مواقع الانترنيت:**

1. https://www.itu.int/net/wsis
2. http://www.itu.int/ITU-T/ip
3. https://www.nist.gov/cyberframework
4. https://www.rsaconference.com/usahttps://ec.europa.eu/digital-single-market/en/news/cybersecurity-european-union-maintaining-and-enhancing-security-and-freedom-digital-age. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
5. https://www.itu.int/net/wsis/docs2/declaration/Mission_Statements/Building_confidence_security_WSIS_Geneva_2003.pdf
6. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
7. https://www.symantec.com/content/dam/symantec/docs/reports/istr-26-2021-en.pdf
8. https://www.isaca.org/-/media/info/cybersecurity/cybersecurity-nexus/2020-state-of-cybersecurity-report.pdf
9. https://cybersecurityventures.com/cybersecurity-canon-must-read-books/
10. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2020-PDF-E.pdf
11. https://www.afrinic.net/ar/internet-governance#others
12. https://hcss.nl/report/cyber-diplomacy.
13. https://www.state.gov/international-strategy-for-cyberspace/
14. https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/ ar / jha / 144424.pdf

15. https://www.state.gov/the-u-s-china-cyber-agreement/
16. https://foreignpolicy.com/2021/07/27/china-us-cyber-agreement-trump-xi/.