جامعة محمد خيضر بسكرة

كلية الحقوق والعلوم السياسية

قسم الحقوق

مذكرة ماستر

ميدان الحقوق والعلوم السياسية

فرع : الحقوق

تخصص:قانون دولي عام

رقم ....

اعداد الطالب

بوغديري تقي الدين

يوم ...

تأثير الامن السيبيراني على العلاقات الدولية

لجنة المناقشة

حسونة عبد الغني	أستاذ التعليم العالي	جامعة محمد خيضر بسكرة	رئيسا
يوسفي صفية	أستاذ محاضر أ	جامعة محمد خيضر بسكرة	مشرفا
سلام أمنة	أستاذ محاضر أ	جامعة محمد خيضر بسكرة	مناقشا

السنة الجامعية 2025/2024

شكر وتقدير

الحمد لله رب العالمين، حمدًا يليق بجلال وجهه وعظيم سلطانه، الذي بنعمته تتم الصالحات، وبفضله وكرمه أنهيت هذا العمل المتواضع، رغم ما اعترضني خلاله من صعوبات وتحديات.
فله الحمد والشكر أولًا وآخرًا، ظاهرًا وباطنًا، أن منّ عليّ بالقوة والعزيمة والصبر حتى أتممت هذا العمل.

أتوجه بأسمى عبارات الشكر والامتنان إلى أستاذتي الفاضلة **الدكتورة يوسفي صفية**، المشرفة على هذا العمل، لما بذلته من جهد كبير، وما قدمته من توجيهات قيّمة ونصائح ثمينة، كان لها بالغ الأثر في إنجاز هذا البحث العلمي. لقد كانت سندًا علميًا ومعنويًا طيلة فترة إعداد هذا العمل، فجزاها الله عني كل خير.

كما أتقدم بخالص الشكر والتقدير إلى السادة أعضاء لجنة المناقشة الأفاضل، الذين شرفوني بقبولهم مناقشة هذا العمل، ومنحوني من وقتهم وجهدهم، وأسهموا بملاحظاتهم البنّاءة وتوجيهاتهم السديدة في تقويم هذا البحث والارتقاء به. فلكم مني جميعًا كل الاحترام والتقدير.

الإهداء

إلى من كانت خطواتي الأولى في هذه الحياة تستند على حبهما ودعمهما،إلى من غرسا في نفسي القيم النبيلة، وسقيا روحي بحب العلم والعمل،إلى من تحمّلا عناء السنين، وسهرا الليالي من أجلي، وبذلا من عمرهما وجهدهما ليصل اليوم الذي أرفع فيه رأسي فخرًا بما وصلت إليه...

إلى والدي العزيز **الطاهر بوغديري**، قدوتي في الصبر والثبات، وناصري في كل المحن، ما بخل يومًا بعطاء أو توجيه، وكان دائمًا السند الذي لا يميل.
وإلى والدتي الغالية **الدكتورة سميرة ونجن**، نبع الحنان والحكمة، التي كانت شمعة تحترق لتنير طريقي، وملجئي في كل لحظة ضعف... إليكما يا من أنتما سرّ وجودي ومصدر قوتي، أُهدي هذا العمل المتواضع، عربون حب ووفاء وامتنان لا تفيه الكلمات، وأسأل الله أن يوفقني لأكون دومًا عند حسن ظنكما، فأنال رضاكما وفخركما.

كما أهدي هذه المذكرة إلى أساتذتي الأجلاء، الذين لم يبخلوا عليّ بعلمهم وتوجيهاتهم، فكانوا منارات مضيئة في طريقي العلمي، وفتحوا لي أبواب الفهم والنقد والتحليل، فجزاهم الله عني كل خير.

وإلى إخوتي وأصدقائي الأوفياء، الذين شاركوني لحظات التعب والفرح، وكانوا السند المعنوي والدافع الدائم للمضي قدمًا، أخصّهم بالشكر الصادق على دعمهم وتشجيعهم ووقوفهم بجانبي دون تردد.

وأخيرًا، إلى كل من كان له أثر طيب في مسيرتي العلمية، ولو بكلمة أو دعاء، أهدي هذا العمل المتواضع، راجيًا من الله أن يكون بداية لمسيرة علمية نفعية، أضع من خلالها لبنة في بناء مستقبلي وخدمة وطني ومجتمعي.

مقدمة

شهد العالم في العقود الأخيرة تطورًا تكنولوجيًا هائلًا، أدى إلى ما يمكن تسميته "ثورة رقمية"، والتي أثرت في كافة جوانب الحياة الإنسانية. كان من أبرز نتائج هذه الثورة ظهور "الفضاء السيبراني" أو الفضاء الرقمي، الذي أتاح للإنسان فرصة غير مسبوقة للتواصل، تبادل المعلومات، وممارسة الأنشطة الاقتصادية والتعليمية. إلا أن هذا الفضاء الجديد لم يكن خاليًا من التحديات والمخاطر. فقد أدت تلك التغيرات إلى ظهور تهديدات جديدة تُمثل تحديات جسيمة للأمن القومي والدولي، لعل أبرزها التهديدات السيبرانية .إن التهديدات السيبرانية أصبحت اليوم تشكل مصدر قلق متزايد على مستوى العالم، سواء على مستوى الأفراد أو المؤسسات أو الدول. فقد طالت هذه التهديدات البنى التحتية الحيوية، الأنظمة الاقتصادية، وحتى الأنظمة السياسية، مما جعلها جزءًا لا يتجزأ من التحديات التي تواجه العلاقات الدولية الحديثة.

في هذا السياق، أصبح الأمن السيبراني يمثل أولوية على أجندة الحكومات والمنظمات الدولية. ويُعرف الأمن السيبراني بأنه: مجموعة من الإجراءات، الاستراتيجيات، والتقنيات التي تهدف إلى حماية الأنظمة المعلوماتية، الشبكات، والبيانات الرقمية من أي نوع من الاختراقات، التخريب، أو الاستخدام غير المشروع. ويشمل هذا المجال العديد من الجوانب مثل الأبعاد التقنية، القانونية، والتنظيمية، ويهدف إلى ضمان أمان الفضاء السيبراني ضد التهديدات التي تتطور باستمرار .أما العلاقات الدولية، فهي تُعرف بأنها شبكة من التفاعلات بين الدول، المنظمات الحكومية وغير الحكومية، والشركات متعددة الجنسيات، بهدف تحقيق مصالح مشتركة أو إدارة الخلافات والصراعات.

في هذا السياق، فإن الأمن السيبراني لا يشكل فقط عنصرًا من عناصر الأمن التقليدي، بل أصبح أداة رئيسية في تعزيز الاستقرار الدولي والتأثير على الصراعات العالمية، حيث أضحى تهديدًا غير تقليدي يغير قواعد التفاعل بين الدول ويهدد استقرارها.

.أهمية الموضوع

تتجسد أهمية هذا الموضوع في كونه يسلط الضوء على تهديد معاصر من نوع جديد، وهو التهديد السيبراني، الذي أصبح جزءًا لا يتجزأ من أي استراتيجية أمنية معاصرة. وتتمثل أهمية الأمن السيبراني في كونه أداة ليس فقط للدفاع عن الأنظمة المعلوماتية، بل أيضًا أداة للتأثير في موازين القوى الدولية، حيث أصبح أحد أدوات الصراع في العلاقات الدولية الحديثة. كما أن تأثير الهجمات

السيبرانية لا يتوقف عند تعطيل الأنظمة أو سرقة البيانات، بل قد يتعدى ذلك ليشمل التأثير على العمليات السياسية، الاقتصادية، وحتى الاجتماعية في الدول .إضافة إلى ذلك، أصبح من الضروري أن تتبنى الدول استراتيجيات وتعاونًا دوليًا لمواجهة هذه التهديدات بطريقة فعّالة تضمن أمن الفضاء السيبراني وحمايته من الممارسات الضارة

أهداف الدراسة

تهدف هذه الدراسة إلى تحقيق الأهداف التالية :

توضيح مفهوم الأمن السيبراني من خلال شرح أبعاده المختلفة، وتحديد الأنواع المختلفة للتهديدات السيبرانية.

تحليل أثر التهديدات السيبرانية على العلاقات الدولية، بما في ذلك تأثيرها على السياسة الدولية، الأمن القومي، والعلاقات بين الدول.

إبراز دور الفضاء السيبراني كمنصة جديدة للنزاع والتعاون بين الدول، وكيف يمكن استغلال هذا الفضاء في تعزيز الأمن والتعاون الدولي.

اقتراح آليات لمواجهة التحديات السيبرانية ضمن إطار قانوني دولي، مع التركيز على التعاون بين الدول في مكافحة الجرائم السيبرانية وتأمين الفضاء الرقمي.

أسباب اختيار الموضوع

جاء اختياري لهذا الموضوع بناءً على سببين رئيسيين

-الاسباب الذاتية:

الاهتمام الشخصي بعالم التكنولوجيا والمعلومات والتحديات الرقمية والغرغبة في فهم كيفية تأثير التكنولوجيا الحديثة على العلاقات الدولية. فمع تزايد دور الأمن السيبراني في التأثير على السياسات الدولية، يسعى هذا البحث إلى استكشاف العلاقة بين التهديدات السيبرانية وكيفية إدارتها ضمن استراتيجيات الأمن الوطني والدولي

التحفيز الاكاديمي والبحثي والتطلع للمساهمة في الوعي المجتمعي لمدى أهمية وخطورة الامن السيبراني على استقرار العلاقات بين الأطراف الفاعلة في المجتمع الدولي

الأسباب الموضوعية:

- نظرًا للزخم المتزايد الذي يكتسبه موضوع الأمن السيبراني في الحقل الأكاديمي والسياسي، فإن هذا البحث يسعى إلى تسليط الضوء على الدور المتزايد للأمن السيبراني كأداة لحماية الأمن القومي، فضلاً عن تأثيره العميق في العلاقات بين الدول سواء من حيث استقرارها او توترها

-البعد الاستراتيجي للأمن السيبيراني واهميته في العصر الرقمي خاصة مع تزايد التهديدات والهجمات الالكترونية ضعف الوعي المجتمعي بقضايا الامن الرقمي وتاثيرها على استقرار النظام الدولي

صعوبات البحث

واجهت هذه الدراسة بعض الصعوبات التي أثرت على سير العمل، أبرزها :

ندرة المراجع الأكاديمية العربية المتخصصة في موضوع الأمن السيبراني، مما تطلب البحث عن مصادر أخرى خارج السياق العربي.

صعوبة ترجمة المصطلحات التقنية إلى لغة سياسية واضحة، حيث إن المصطلحات السيبرانية تتطور بسرعة ويصعب مواكبة تطوراتها.

التطور السريع للتهديدات السيبرانية مقارنة بالقدرة الأكاديمية على مواكبة تلك التطورات، وهو ما يتطلب وقتًا أطول لمواكبة كل جديد في هذا المجال.

السرية المحيطة بالمعلومات السيبرانية والتي تجعل من الصعب الحصول على بيانات دقيقة وموثوقة لدراستها. ومن هذا نطرح **الإشكالية** التالية

ما هو تأثير الأمن السيبراني على العلاقات الدولية، وكيف يمكن مواجهته ضمن أطر قانونية وتعاونية دولية؟**الفرضيات**

-الأمن السيبراني قد يتحول إلى ساحة صراع جديد بين الدول نتيجة تنامي الهجمات الإلكترونية ذات الطابع العدائي

-غياب اتفاقيات دولية ملزمة لتنظيم الفضاء السيبراني يزيد من احتمالية النزاعات الإلكترونية بين الفاعلين الدوليين

-استخدام القدرات السيبرانية لأغراض التجسس والتدخل في الشؤون الداخلية للدول الأخرى يعزز من مناخ التوتر والصراع.

المناهج العلمية المعتمدة

تم الاعتماد في هذه الدراسة على مناهجين علميين:

المنهج التحليلي: لفهم الظاهرة السيبرانية في إطارها الأمني والسياسي، وتحليل التأثيرات المختلفة لهذه الظاهرة على العلاقات الدولية.

المنهج الوصفي: لمتابعة تطور التهديدات السيبرانية عالميًا وكيفية تعامل الدول معها، وتقديم رؤية واضحة حول الأنماط المتبعة في إدارة هذه التهديدات .

الخطة

وتناولنا في هذا البحث فصلين

الفصل الأول تداعيات الامن السيبيراني على العلاقات الدولية ويشمل التداعيات الإيجابية والسلبية للأمن السيبيراني على العلاقات الدولية

الفصل الثاني تحديات إدارة الامن السيبيراني وسبل مواجهتها في مجال العلاقات الدولية ويشمل تحديات إدارة الامن السيبراني في مجال العلاقات الدولية وسبل مواجهتها

الفصل الأول

تداعيات الامن السيبيراني على العلاقات الدولية

في عصر العولمة الرقمية، بات الأمن السيبراني أحد المحاور الرئيسة التي تشكل ملامح العلاقات الدولية الحديثة. فقد أتاح التطور التقني السريع للدول فرصاً لتعزيز التعاون والاستقرار العالمي، مما انعكس إيجابياً على حماية البنى التحتية الحيوية ومكافحة الجريمة الإلكترونية، ودعم الابتكار الاقتصادي والعلمي. ومع ذلك، فإن لهذا الفضاء الرقمي وجهاً آخر مظلماً، حيث أدى اتساع نطاق التهديدات السيبرانية إلى تعقيد التفاعلات الدولية، من خلال التدخل في الشؤون الداخلية للدول، والتجسس الإلكتروني، وسرقة المعلومات الحساسة، مما تسبب بتوترات سياسية وأمنية متزايدة. وعليه، يستعرض هذا البحث في مبحثه الأول الآثار او التداعيات الإيجابية للأمن السيبراني على العلاقات الدولية، فيما يتناول المبحث الثاني التداعيات السلبية التي نتجت عن سوء استخدام الفضاء الرقمي في الصراع بين الدول.

المبحث الأول

التداعيات الإيجابية للأمن السيبيراني على العلاقات الدولية

مع تطور العصر الرقمي، غيّر الأمن السيبراني شكل العلاقات الدولية، وأصبح قوة مؤثرة لا تقل أهمية عن الأدوات السياسية والعسكرية التقليدية. فلم يعد الفضاء الرقمي مجرد مجال للتواصل أو الترفيه، بل تحول إلى ساحة تفاعلات سياسية وأمنية واقتصادية معقدة بين الدول. ومن أبرز آثار الأمن السيبراني في هذا السياق، دوره في تحسين الاستقرار العالمي عبر تقليل فرص التصعيد والنزاعات، وإرساء مبادئ جديدة لضبط السلوك في الفضاء الرقمي، مما أدى إلى ظهور اتفاقيات ومعاهدات تهدف إلى الحد من الحرب السيبرانية وتعزيز الثقة المتبادلة بين الدول .كما أن التحديات المتزايدة المرتبطة بالتهديدات الإلكترونية العابرة للحدود دفعت الدول إلى البحث عن أشكال متقدمة من التعاون الدولي، سواء عبر التحالفات الأمنية المشتركة أو آليات تبادل المعلومات والإنذار المبكر، من أجل بناء شبكة عالمية قادرة على التصدي الفوري للمخاطر الرقمية المتزايدة .وفي الجانب الآخر، أبرز الأمن السيبراني أهمية حماية الأصول الحيوية التي أصبحت العمود الفقري للاقتصاد الرقمي العالمي، مثل شبكات المال والطاقة والنقل والصحة، مما فرض على الدول والمؤسسات تطوير خطط لحماية أصولها الرقمية وتعزيز قدرتها على الابتكار التكنولوجي.

فالابتكار لم يعد خياراً، بل ضرورة لضمان التفوق في عالم قائم على الذكاء الاصطناعي، البيانات الضخمة، والحوسبة السحابية، وكلها تعتمد في وجودها واستمرارها على وجود بيئة سيبرانية آمنة ومستقرة .انطلاقاً من هذه الأهمية المزدوجة للأمن السيبراني، يتناول هذا المبحث من خلال مطلبين رئيسيين :الأول يركز على دور الأمن السيبراني في تحقيق الاستقرار وتعزيز التعاون الدولي، والثاني يستعرض كيف يسهم الأمن السيبراني في حماية الأصول الحيوية ودعم الابتكار كرافعة أساسية للنمو المستدام في العصر الرقمي.

المطلب الأول

تحسين الاستقرار والتعاون الدولي

في ظل تنامي التهديداتالسيبيرانية وتعاظم اثارها على الامن والاستقرار الدوليين ثم ادراك ضرورة بذل جهود شاملة ومنسقة من اجل تحسين الاستقرار العالمي من جهة وتعزيز التعاون الدولي في مجال الامن السيبراني من جهة أخرى بما يضمن حماية الفضاء الرقمي ويرسخ الثقة في استخدام التكنولوجيا الحديثة ويسهم بالتالي في توطيد العلاقات بين الدول في هذا المجال .

الفرع الأول

تحسين الاستقرار العالمي

اصبح الفضاء السيبيراني اليوم مجالا جديدا للصراع بين الدول واز للبر وابحر والجو والفضاء الا انه يتميز عن باقي المجلات بطبيعته الخفية وانخفاض تكلفة الدخول اليه وسهولة إخفاء مصدر الهجوم ما يجعله محفزا لما يعرف بالحرب الرقمية الباردة. وقد أدى ادراك هذه الخطورة الى بروز توجه دولي نحو التهدئة وتقليل احتمالات التصعيد وتتمثل ابرز مساهمات هذا التوجه في العمل على الحد من الصراعات الدولية السيبيرانية وحماية البنية التحتية الحيوية العالمية وبذل الجهود في مكافحة الجريمة السيبرانية.

أولًا :الحد من الصراعات الدولية السيبرانية

دفعت الهجمات السيبرانية المتكررة مثل الهجوم على شركة "سوني بيكتشرز" عام2014، والهجوم الشهير "WannaCry"سنة 2017، الذي أصاب مئات آلاف الحواسيب في أكثر من 150 دولة، إلى

تعزيز الوعي الدولي بضرورة وضع حدود واضحة للسلوك في الفضاء الرقمي .وقد سعت عدة منظمات أممية وإقليمية إلى صياغة مدونات سلوك دولية لضبط هذا الفضاء، وعلى رأسها الأمم المتحدة التي أنشأت منذ سنة 2004 "مجموعة الخبراء الحكوميينGGE "، والتي أكدت في تقاريرها على مبدأ احترام سيادة الدول في الفضاء السيبراني، وعدم استخدام البنية التحتية الرقمية في شنّ هجمات على المصالح الحيوية للدول الأخرى. وقد توصّلت هذه المجموعة سنة 2015 إلى توافق مهم، حيث نص التقرير النهائي على أن نفس المبادئ التي تحكم العلاقات الدولية في الفضاء الواقعي، يجب أن تطبق أيضًا في الفضاء الرقمي، بما في ذلك مبدأ عدم التدخل في الشؤون الداخلية، ومبدأ الامتناع عن استخدام القوة .من جهة أخرى، بدأت القوى الكبرى في الدخول في مفاوضات ثنائية للحد من التهديدات السيبرانية التي قد تؤدي إلى صراع شامل، كما حدث بين الصين والولايات المتحدة. ففي سبتمبر 2015، تم توقيع اتفاق مشترك بين الرئيس الأمريكي باراك أوباما والرئيس الصيني شي جين بينغ، ينص على عدم تنفيذ أو دعم أي عمليات سيبرانية تهدف إلى سرقة الملكية الفكرية أو الأسرار الصناعية لتحقيق مكاسب اقتصادية. ورغم التوترات اللاحقة، شكّل هذا الاتفاق سابقة دبلوماسية مهمة في العلاقات السيبرانية بين الدول .كما أن التعاون بين روسيا والعديد من الدول في إطار منظمة شنغهاي للتعاون تضمن مقترحات بخصوص إنشاء "اتفاقية دولية للأمن السيبراني"، تهدف إلى الحد من عسكرة الفضاء الرقمي ووضع ضوابط قانونية للاستخدام المسؤول لتكنولوجيا المعلومات .واللافت في هذه التحولات أن الأمن السيبراني أصبح يُستخدم كأداة دبلوماسية ناعمة، حيث تعمد الدول إلى عقد اتفاقيات ومبادرات لحفظ الأمن الرقمي، ما يمنحها صورة إيجابية دوليًا ويُجنبها الدخول في صراعات مكلفة، خاصة في ظل الطبيعة المتشابكة للاقتصاد الرقمي العالمي. فهجوم سيبراني واسع على البورصات المالية أو أنظمة التحكم في الطيران مثلًا قد يتسبب في انهيار عالمي يصيب الدول المُهاجِمة والمُهاجَمة على حد سواء .ومع تزايد خطورة "الهجمات الردعية" أو ما يُعرف بـ Cyber Deterrence، ظهرت الحاجة إلى "قواعد اشتباك سيبرانية"، على غرار القوانين التي تحكم النزاعات المسلحة، ما يُشير إلى تحول الأمن السيبراني من مجرد مسألة تقنية إلى عنصر حيوي في إدارة النزاعات وتفاديها[1].

ثانيًا: حماية البنية التحتية الحيوية العالمية

في ظل العولمة الرقمية، أصبحت البنية التحتية الحيوية للدول مرتبطة بشكل وثيق بالأنظمة التكنولوجية المعقدة التي تعتمد على الاتصال بالإنترنت، مما جعلها عرضة مباشرة لمخاطر الهجمات السيبرانيةالمنظمة.

[1] حسن عبد الكريم ؛**الأمن السيبراني والتحولات في العلاقات الدولية المعاصرة** المركز العربي للأبحاث ودراسة السياسات، 2022، ص. 45-52.

ويُقصد بالبنية التحتية الحيوية تلك المنشآت والقطاعات الأساسية التي يُعد تعطلها تهديدًا مباشرًا للأمن القومي، مثل الكهرباء، الغاز، الاتصالات، النقل، الصحة، المياه، والمصارف .لقد أفرز هذا الواقع معادلة جديدة في العلاقات الدولية، إذ أصبح الفضاء السيبراني يمثل "منطقة حرب خامسة"، تتنافس فيها الدول على النفوذ والتحكم، بل وتسعى بعضها إلى توظيف الهجمات الرقمية كوسيلة ضغط سياس واقتصادي. وقد بات من المؤكد أن اختراق نظام طاقة في بلد ما، قد يُوازي في أثره ضرب منشأة نووية أو تدمير جسر استراتيجي، بل أكثر خطورة أحيانًا بسبب سرعة الانتشار وصعوبة التعقب .إن أبرز مثال على هذا النوع من التهديد كان الهجوم الذي استهدف شبكة الكهرباء الأوكرانية في ديسمبر 2015، حين استخدم القراصنة برامج خبيثة للتحكم عن بعد في محطات الكهرباء، ما أدى إلى حرمان أكثر من230 ألف مواطن من الطاقة لعدة ساعات. وقد بيّنت التحقيقات أن الهجوم كان منسقًا وذا طابع سياسي، مما كشف هشاشة البنى التحتية أمام الحروب غير التقليدية .وفي 2021، تعرضت شركةColonial Pipeline ، المسؤولة عن نقل ما يقارب 45% من وقود الساحل الشرقي للولايات المتحدة، لهجوم إلكتروني عبر برنامج فدية (Ransomware)من قبل مجموعة"DarkSide" ، مما تسبب في إغلاق تام لأنابيب نقل الوقود لعدة أيام، وزعزعة الأمن الطاقوي والاقتصادي الأمريكي، مع خسائر قدرت بملايين الدولارات. هذا الحدث أعاد تشكيل إستراتيجيات الأمن القومي الأمريكي، حيث أعلن الرئيس جو بايدن حالة الطوارئ، وتم تعزيز صلاحيات الوكالة الفيدرالية للأمن السيبراني .أما على صعيد المبادرات الدولية، فقد أنشأ الاتحاد الأوروبي نظامًا مشتركًا لتبادل المعلومات حول التهديدات السيبرانية التي تستهدف البنية التحتية، وذلك ضمن مبادرة NIS (Directive on Security of Network and Information Systems)، والتي تلزم الدول الأعضاء باتخاذ تدابير صارمة لحماية شبكات الطاقة، المصارف، والخدمات الصحية .كما أسست منظمة حلف شمال الأطلسي (الناتو) "مركز التميز للدفاع السيبراني" في إستونيا، والذي يُشرف على تدريبات دورية مثلLocked Shields ، حيث تُحاكي فرق من دول مختلفة هجمات إلكترونية حقيقية على بنى تحتية كالمطارات، المستشفيات، شبكات المياه والغاز. وتكمن أهمية هذه التمارين في اختبار قدرة التحالفات الدولية على التصدي للأزمات الرقمية بشكل جماعي ومنسق .إن الأمن السيبراني، في هذا السياق، لا يُعنى فقط بمنع الاختراقات، بل بتعزيز ما يسمى بـ"المرونة السيبرانية"، أي قدرة المؤسسات الحيوية على مواصلة العمل أثناء الهجوم أو بعده، وذلك عبر نسخ احتياطية مؤمنة، شبكات بديلة، ونُظم إنذار مبكر .وقد أدركت دول الجنوب أيضًا أهمية هذه الخطوات، حيث بدأت الجزائر، مثلًا، بتحديث نظم الحماية في قطاعات الكهرباء والنقل عبر شراكات مع شركات أوروبية وآسيوية، كما تم تطوير منظومة الأمن السيبراني الخاصة بالبنك المركزي الجزائري لحماية المعاملات الرقمية .في النهاية، إن حماية البنية

التحتية الحيوية لم تعد خيارًا تقنيًا داخليًا، بل صارت رهانًا إستراتيجيًا دوليًا تُبنى عليه قرارات السياسة الخارجية، وشراكات التحالف، وقدرة الدول على الصمود أمام التحولات الكبرى في طبيعة الحروب المعاصرة[1] .

ثالثًا: مكافحة الجريمة السيبرانية

في ظل التطور التكنولوجي المتسارع والتحوّل الرقمي العالمي، برزت الجريمة السيبرانية كأحد أكثر التحديات الأمنية تعقيدًا في العصر الحديث، لما تتصف به من ديناميكية، وعالمية، وسرعة في الانتشار، وارتفاع في درجة التخفي. فمجرمو الإنترنت لا يحتاجون إلى عبور حدود مادية لتنفيذ جرائمهم، بل يمكنهم، باستخدام أدوات رقمية بسيطة نسبيًا، شلّ مؤسسات مالية، اختراق أنظمة حساسة، سرقة بيانات ملايين الأفراد، أو تنفيذ عمليات ابتزاز وهجمات فدية على حكومات أو مستشفيات أو مطارات.أمام هذا التهديد غير التقليدي، أصبح الأمن السيبراني أحد أبرز محاور التعاون الدولي، ووسيلة محورية لحماية سيادة الدول وصيانة الأمن القومي، إلى جانب كونه محفّزًا لإعادة تشكيل بنية العلاقات الدولية، بما في ذلك التحالفات والخصومات والاتفاقيات .

ا-الطابع العابر للحدود للجريمة السيبرانية

أحد أخطر خصائص الجريمة السيبرانية أنها لا تعترف بالحدود الجغرافية أو القانونية التقليدية. قد يُنفذ الهجوم من دولة آسيوية، ويستهدف مؤسسة في أمريكا اللاتينية، ببرمجية صُممت في أوروبا، وتموّل بعملة مشفرة من خوادم في إفريقيا. هذا الطابع المعقّد جعل مكافحة الجريمة السيبرانية شأنًا دوليًا بامتياز، يتطلب التعاون عبر قنوات الشرطة الدولية، الاستخبارات، المنظمات القضائية، والهيئات التنظيمية المالية.ففي سنة 2022، تم تنفيذ عملية مشتركة أطلق عليها اسم "عملية دايموند نيت(Diamond Net) "، بين الولايات المتحدة وألمانيا وكندا وكوريا الجنوبية، حيث نجحت في تفكيك شبكة دولية معقدة استخدمت خوادم منتشرة في أكثر من 25 دولة، لاستهداف أكثر من 150 بنكًا ومؤسسة طبية في أوروبا وأمريكا. وأسفرت العملية عن اعتقال 40 شخصًا ومصادرة أصول رقمية تزيد قيمتها عن 50 مليون دولار.

ب-الأمن السيبراني كأداة لحماية الاقتصاد الرقمي العالمي

لقد أصبح الاقتصاد الرقمي ركيزة أساسية للنمو العالمي، ومع ذلك، تشير تقارير البنك الدولي إلى أن أكثر من 30% من الشركات في الدول النامية تعرّضت لهجمات سيبرانية أدت إلى خسائر مالية معتبرة. من هنا برز الأمن السيبراني كعنصر استراتيجي لحماية الاقتصاد، خاصة مع تصاعد استخدام العملات الرقمية

[1] الحدّاد ياسين **«البنية التحتية والأمن السيبراني في العالم المعاصر»**مجلة السياسات الأمنية الدولية، العدد 10، 2021، ص. 87–95

وتقنيات البلوكشين التي قد تُستغل لغسيل الأموال أو تمويل الإرهاب .جهود مكافحة هذا النوع من الجرائم دفعت العديد من الحكومات إلى تأسيس وحدات استخبارات رقمية متخصصة، وتعزيز التعاون مع المؤسسات المصرفية العالمية لمراقبة التحويلات المشبوهة. على سبيل المثال، أطلقت بريطانيا "الفرقة الوطنية للأمن المالي السيبراني" لمواجهة الجرائم الرقمية التي تستهدف بورصة لندن والمصارف الكبرى.

ج-أثر الأمن السيبراني في تعزيز العدالة والحوكمة

يؤدي الأمن السيبراني دورًا متزايد الأهمية في ضمان نزاهة العمليات الديمقراطية، من خلال كشف التلاعب بالانتخابات، أو حماية أنظمة التصويت الإلكتروني من الاختراق. ففي الانتخابات الرئاسية الأمريكية لسنة 2020، تم إحباط عدة محاولات تدخل رقمية يُعتقد أن مصدرها دول أجنبية، حيث استخدمت هيئة الأمن السيبراني CISA أنظمة إنذار مبكر ونماذج ذكاء اصطناعي لكشف الأنماط المشبوهة .كما قامت المفوضية الأوروبية بإنشاء وحدة لمكافحة التضليل الإعلامي السيبراني، وهي متخصصة في تعقب الأخبار الزائفة والموجهة التي قد تؤثر على الرأي العام الأوروبي، خاصة أثناء الأزمات (مثل جائحة كورونا، والحرب في أوكرانيا.

الدول النامية والأمن السيبراني: التحديات والفرص في العالم العربي وإفريقيا، تزداد الهشاشة أمام الجريمة السيبرانية بسبب ضعف التشريعات، وقلة الكفاءات المتخصصة، ونقص التمويل. ومع ذلك، تشهد بعض الدول خطوات مشجعة نحو التحديث. ففي الجزائر، تم إطلاق "الاستراتيجية الوطنية للأمن السيبراني 2023–2027"، والتي تشمل إنشاء مركز وطني للاستجابة للطوارئ السيبرانية، وتعزيز التعاون مع شركاء أوروبيين وصينيين لتكوين مهندسين جزائريين في مجال الأمن الرقمي .أما في مصر، فقد أنشأت الحكومة "المركز القومي لإدارة مخاطر الإنترنت"، وبدأت في تدريب آلاف الموظفين الحكوميين على استخدام أدوات الحماية الرقمية، خاصة في وزارات المالية، الصحة، والتعليم.

التعاون الدولي: من الردع إلى الوقاية لم يعد التعاون الدولي في مجال الأمن السيبراني يقتصر على الاستجابة بعد وقوع الهجمات، بل تطوّر ليشمل الوقاية المسبقة والردع الجماعي. إذ تنظم منظمات مثل الأمم المتحدة، والاتحاد الأوروبي، والاتحاد الإفريقي، دورات تدريبية وندوات دولية لتقاسم الخبرات وبناء قدرات الدول الأضعف .وقد دعت الأمم المتحدة في تقريرها السنوي لعام 2023 إلى إنشاء معاهدة دولية

ملزمة لمكافحة الجريمة السيبرانية، تقضي بإنشاء قواعد واضحة لتسليم المطلوبين، وتبادل الأدلة الرقمية، وتوحيد تعريفات الجرائم الإلكترونية[1].

الفرع الثاني

تعزيز التعاون الدولي في مجال الأمن السيبراني

في العصر الرقمي الذي نعيشه اليوم، لم تعد التهديدات الأمنية تقف عند حدود الدولة القومية، بل أصبحت تمتد عبر الأقاليم والقارات بفعل الطبيعة العابرة للحدود للفضاء السيبراني. وقد أدّت هذه التغيرات إلى ظهور حاجة ملحة إلى تعزيز التعاون الدولي كخيار استراتيجي تفرضه الضرورة لا الرغبة، نظرًا لأن أي تهديد سيبيراني قد يُهدّد استقرار دول متعددة في وقت متزامن، وهو ما لا يمكن لدولة واحدة مواجهته بمفردها.

أولًا: التحالفات الأمنية المشتركة وتبادل المعلومات

ا-طبيعة التحالفات السيبرانية وأهميتها

التحالفات السيبرانية تمثل نوعًا جديدًا من الشراكات الأمنية التي لم تكن موجودة قبل العقدين الماضيين. فهي تجمع بين دول مختلفة، وأحيانًا حتى بين كيانات حكومية وخاصة، بهدف تنسيق الجهود المشتركة للوقاية من الهجمات الإلكترونية ومواجهتها .أهمية هذه التحالفات تتجلى في أنها تُتيح للدول تقاسم أعباء الدفاع، وتبادل الخبرات التقنية، وبناء قدرات بشرية وتكنولوجية مشتركة. فهي لا تقتصر على رد الفعل بعد وقوع الهجوم، بل تتبنى استراتيجيات استباقية تشمل التدريب، والبحث العلمي، وتطوير وسائل الدفاع الإلكتروني.

ب-نماذج من التحالفات الدولية

التحالف السيبراني للناتو :(NATO Cyber Defence) يُعد هذا التحالف من أوائل النماذج المتقدمة في التنسيق السيبراني العسكري، حيث يشمل التعاون في إعداد الأطر السياسية، وتنظيم مناورات افتراضية تحاكي الهجمات السيبرانية الكبرى، ويمتلك مركزًا للتميز في إستونيا يُعَد بمثابة العقل المفكر لاستراتيجيات الدفاع السيبراني .المنظمات الإقليمية كمثال على التحالفات :في القارة الأمريكية، تُعد منظمة الدول الأمريكية (OAS) من أبرز الهيئات الإقليمية التي أدركت مبكرًا خطورة التهديدات السيبرانية، فأنشأت

[1] علي مروان« **التحولات الرقمية ومكافحة الجريمة السيبرانية في العلاقات الدولية**» . المجلة العربية للعلوم السياسية، العدد 58، 2023، ص. 45

وحدة متخصصة في الأمن السيبراني، تُشرف على إعداد البرامج التدريبية، وتوفير الدعم الفني للدول الأعضاء، وتطوير أطر قانونية وطنية متناسقة مع المعايير الدولية.

ج-آليات تبادل المعلومات كأداة استباقية

التهديدات السيبرانية لا تنتظر ردود الأفعال؛ لذلك كان لا بد من إنشاء أدوات استباقية تهدف إلى تشارك المعلومات المتعلقة بالهجمات والتهديدات بين الدول. من أهم هذه الآليات :شبكات الإنذار المبكر المشتركة : وهي عبارة عن منظومات رقمية مرتبطة بشبكات المراقبة العالمية، تعمل على رصد النشاطات المشبوهة في الزمن الحقيقي، وإرسال تنبيهات للدول أو المؤسسات المشاركة فورًا لتمكينها من التصدي للهجمات قبل تفاقمها .منصات تبادل بيانات التهديدات :مثل "MISP" و"STIX/TAXII"، وهي منصات تسمح للجهات الأمنية بتبادل معلومات دقيقة جدًا حول طبيعة البرمجيات الخبيثة، ومسارات الهجوم، وهويات المهاجمين إن توفرت، وكذا الثغرات المستغلة. هذه البيانات تمكن من تعزيز الذكاء الاصطناعي الدفاعي وتعليم الأنظمة الأمنية كيف تتعامل مع نفس التهديد مستقبلًا[1]

ثانيًا: التنسيق التشريعي والقانوني بين الدول

ا-التحديات القانونية في ظل غياب قانون دولي ملزم

يُعَد غياب إطار قانوني دولي موحد أحد أبرز التحديات في مجال مكافحة الجريمة السيبرانية. فالدول تختلف في تعريفها للجرائم الإلكترونية، وكذلك في أدوات إثباتها والعقوبات المقررة لها، مما يُصعّب التعاون القضائي وخصوصًا في حالة المجرمين العابرين للحدود.

ب-محاولات توحيد القوانين والتشريعات

هناك مساعٍ دولية حثيثة لتقريب وجهات النظر القانونية بين الدول، منها :اتفاقيات إقليمية ودولية مثل اتفاقية بودابست، وهي أول اتفاقية دولية تُنظّم الجريمة السيبرانية، وتعتمدها اليوم عشرات الدول من مختلف القارات .تتضمن هذه الاتفاقية تعريفات دقيقة للجرائم، وآليات للتعاون القضائي .اللجان القانونية المشتركة

[1] علي حسن الجابري« **أمن المعلومات والأمن السيبراني: تحديات الواقع واستراتيجيات المواجهة »** مجلة دراسات قانونية وسياسية، جامعة باتنة، العدد 13، 2022،ص 218

التي تشتغل تحت مظلة منظمات دولية كالأمم المتحدة، مجلس أوروبا، الاتحاد الإفريقي، وجامعة الدول العربية، والتي تعمل على إعداد مشاريع قوانين نموذجية يمكن للدول تبنيها[1] .

ج-جهود الأمم المتحدة في التشريع السيبراني

تلعب الأمم المتحدة دورًا بارزًا في محاولة رسم معالم قانون دولي سيبراني، من خلال :فريق الخبراء الحكوميين :(GGE) أنشئ لدراسة التحديات القانونية المتعلقة بالأمن السيبراني، وصياغة مبادئ توجيهية لسلوك الدول في الفضاء الرقمي .مجموعة العمل المفتوحة العضوية :(OEWG) تهدف إلى إشراك جميع الدول، خصوصًا النامية منها، في الحوار حول الأمن السيبراني، وتوفير منصة نقاش مفتوح لإعداد قواعد سلوك ومسؤولية مشتركة .

د-مبادرات إقليمية نحو التنسيق القانوني

أوروبا: تسير بخطى ثابتة نحو التنسيق عبر المؤسسات الأوروبية، مثل البرلمان الأوروبي والمجلس الأوروبي، حيث تم سن لوائح صارمة مثل اللائحة العامة لحماية البيانات .(GDPR) العالم العربي: رغم التفاوت بين الدول، إلا أن مجلس وزراء الداخلية العرب قام بإعداد مشروع اتفاقية عربية لمكافحة الجريمة السيبرانية، وهي خطوة هامة نحو توحيد التشريعات في هذا المجال الحساس[2].

المطلب الثاني

تعزيز الاقتصاد العالمي

اصبح الاقتصاد العالمي يعتمد بشكل متزايد على النظم الرقمية والبنيه التحتية السيبرانيه الامر الذي يجعل من حمايه الاصول الرقمية وتعزيز الابتكار العلمي والتكنولوجي ضروره ملحه لضمان النمو المستدام عبر تسهيل التجارة الرقمية والتبادل الدولي واعتماد الاليات التي تضمن سلامه التجارة العالمية وحمايتها من التهديدات السيبرانيه

الفرع الأول

حمايه اصول وتعزيز الابتكار

[1] يوسف الحوامدة« **الحوكمة الأمنية السيبرانية وتحديات التعاون الدولي**» ، المجلة الأردنية للأمن والحماية، 2021،

[2] أحمد عبد العزيز شقير، ؛**الجريمة الإلكترونية والتحديات القانونية المعاصرة**، دار الجامعة الجديدة، الإسكندرية، 2021، ص. 142-145.

ان التأسيس لنظام اقتصادي رقمي عالميه من خلال عده عناصر مترابطة اهميه التكامل بين الامن الرقمي وتطور التكنولوجي وذلك على الوجه التالي .

اولا حمايه الاصول المالية والاقتصادية

تمثل حمايه الاصول المالية في عصر العولمة والاقتصاد الرقمي تحديا مركزيا للدول والمؤسسات حيث اصبحت هذه الاصول بما فيها البيانات المالية والتكنولوجيا والبنيه التحتية السيبرانيه هدفا مباشرا لهجمات سيبيرانيه متزايدة في التعقيد والتنظيم ويمكن تناول هذه المسالة من عده زوايا اهمها

ا-حماية البنوك والاسواق المالية

في الحروب الاقتصادية الحديثة لم تعد المعارك تخاض بالسلاح التقليدي بل عبر هجمات السيبرانيه نستهدف تعطيل البنوك بيانات الحسابات او تعطيل البوسات ولتفادي ذلك تبذل الدول جهودا مكثفه من خلال تبني استراتيجيات متعددة الاوجه تشمل تطوير الأطر القانونية والتنظيمية والتعاون وتبادل المعلومات وتبني استراتيجيات وتقنيات متقدمة وتعزيز القدرات المؤسسية [1] .

ب-استمرارية الأعمال في بيئات التهديد المعولمة:

بروتوكولات استمرارية الخدمة :(BCP) تعتمد المؤسسات العالمية على خطط دقيقة لضمان استمرارية العمليات حتى في ظل الهجمات أو الكوارث الرقمية. وتشمل هذه البروتوكولات استخدام خوادم احتياطية، نقل البيانات بشكل آني(real-time replication) ، وتدريب العاملين على إدارة الأزمات .الاستجابة السريعة للحوادث :(Incident Response) لا يكفي منع الاختراق، بل يجب أن تتوفر فرق متخصصة في الاستجابة السريعة عند حدوث هجوم. ويشمل ذلك تحليل الهجوم، عزل النظام المصاب، واستعادة العمليات في أسرع وقت ممكن لتقليل الخسائر[2].

ج-حماية أصول المعرفة والابتكار:

الملكية الفكرية كأصل اقتصادي حساس :تُعد براءات الاختراع والملفات البحثية جزءًا لا يتجزأ من القوة الاقتصادية للدول. فسرقة خوارزمية جديدة أو تصميم تقني مبتكر قد يُكلّف سنوات من البحث وجهودًا ضخمة تُسلب في دقائق عبر هجوم إلكتروني .الابتكار كمصدر للثروة القومية :في الاقتصاد الجديد، لم تعد

[1] محمد الرويني؛**أمن المعلومات في المؤسسات الاقتصادية**دار الفكر الجامعي، الإسكندرية، 2020،ص 218

[2] فوزي بن خليل« **التهديدات السيبرانية وتأثيرها على الأمن الاقتصادي للدولة** » ، المجلة الجزائرية للدراسات الأمنية، العدد 5، 2021 ص 211

الموارد الطبيعية وحدها أساس الثروة، بل أصبحت "المعرفة الرقمية" والتقنيات الحديثة أساس التنافس بين الأمم. وحماية هذه المعرفة تتطلب استثمارات ضخمة في الأمن السيبراني، والقوانين، والتعاون الدولي.

د-الأمن السيبراني كجزء من السيادة الوطنية:

تُستخدم الهجمات الإلكترونية كوسيلة للتجسس أو للتخريب بين الدول. وقد شهد العالم أمثلة عديدة على تدخلات في الانتخابات، أو تعطيل منشآت حيوية، أو ابتزاز مؤسسات اقتصادية كبرى.الاعتماد على الأمن المحلي في البنى الرقمية :بدأت الدول تسعى إلى بناء "سيادة رقمية" من خلال تطوير أنظمتها وبرمجياتها الخاصة، والحد من الاعتماد على البنية التحتية الأجنبية التي قد تُستغل كحصان طروادة. وهو توجه يعزز من الحماية طويلة المدى لأصولها الاقتصادية.

ثانيًا: تعزيز الابتكار[1]

يُعد الابتكار من أبرز محركات النمو الاقتصادي في العصر الرقمي، حيث تعتمد التنافسية الاقتصادية للدول والمؤسسات على قدرتها على تطوير تقنيات جديدة، وتكييفها مع حاجات السوق المتغيرة. غير أن هذا الابتكار لا يمكن أن يتحقق في بيئة غير آمنة، ما يجعل من الأمن السيبراني ركيزة أساسية في خلق بيئة مواتية للإبداع والابتكار. ويتجلى هذا في عدة محاور أساسية :

ا-توفير بيئة آمنة للبحث والتطوير

الابتكار لا يُولد من فراغ، بل يتطلب بنية تحتية رقمية مؤمّنة ومُحفِّزة، تحمي نتائج البحث وتضمن سريته وخصوصيته :حماية المختبرات الافتراضية وبيئات الاختبار الرقمية :في ظل التقدم التكنولوجي، أصبحت الكثير من الأبحاث تتم داخل مختبرات رقمية أو بيئات افتراضية تعتمد على الحوسبة السحابية أو الذكاء الاصطناعي. هذه البيئات، رغم مرونتها، تُعد عرضة للاختراق، مما قد يؤدي إلى تدمير نتائج بحثية، أو سرقتها لصالح جهات منافسة .ضمان سرية البيانات البحثية والبرمجيات التجريبية :المشاريع الابتكارية، خصوصًا تلك المتعلقة بالتقنيات الحساسة مثل التشفير أو الذكاء الاصطناعي، تتطلب سرية عالية. أي خرق في هذه البيئة قد يؤدي إلى تسريب الأفكار قبل تسجيلها كبراءات اختراع، مما يُفقد الجهة الباحثة تفوقها التنافسي .أمان التعاون الدولي بين الجامعات ومراكز البحث :مع ازدياد التعاون البحثي عبر القارات، بات

[1] منظمة التعاون والتنمية الاقتصادية،**تقرير حول حماية البنى التحتية الرقمية الحيوية**،' ترجمة مركز دراسات الوحدة العربية، بيروت 2018 ص 46-55

من الضروري تأمين القنوات الرقمية التي يتم من خلالها تبادل الملفات والنماذج والنتائج، وذلك عبر تشفير الاتصالات، والتحقق من الهوية، ومراقبة سلوك الشبكة .

ب-دعم الابتكار في التقنيات الناشئة

تعتمد الاقتصادات الحديثة على الريادة في مجالات مثل الذكاء الاصطناعي، إنترنت الأشياء، والميتافيرس، مما يجعل تأمين هذه المجالات أمرًا استراتيجيًا :تطوير حلول أمنية للذكاء الاصطناعي والبيانات الضخمة : الذكاء الاصطناعي لا يعمل بمعزل عن البيانات، بل يعتمد على كميات هائلة من "البيانات الضخمة". وإذا لم تكن هذه البيانات مؤمّنة، فإن النماذج الناتجة قد تُعطي قرارات مغلوطة، أو تتعرض لتلاعب خفي في مرحلة "التعلّم"، مما يؤدي إلى اختلالات في نتائج الأعمال أو توقعات السوق .تعزيز أمن أنظمة التعلم الآلي والتعلم العميق :تعتبر خوارزميات الذكاء الاصطناعي حساسة جدًا للهجمات الموجهة، مثل إدخال بيانات مغلوطة عمداً (Data Poisoning) أو الهجمات الخصامية .(Adversarial Attacks) لذا، يجب تطوير بروتوكولات أمان خاصة بها لضمان سلامة النماذج وعدم انحرافها .تأمين تطبيقات الميتافيرس والواقع المعزز في القطاعات الصناعية :تشهد الصناعات الكبرى توجهًا متسارعًا نحو دمج الواقع الافتراضي والمعزز في سلاسل الإنتاج والتكوين المهني. ومع تزايد الاعتماد على هذه التطبيقات، تظهر تهديدات جديدة مثل سرقة الهويات الرقمية، التحكم عن بعد في أجهزة الواقع المعزز، أو التجسس على محتوى الاجتماعات الصناعية السرية[1] .

ج-تحفيز الاستثمار في التكنولوجيا

الاستثمار في الابتكار التكنولوجي لا يتحقق إلا في مناخ مستقر وآمن، يسمح لرأس المال بالمخاطرة بثقة، ويضمن الحماية من الانتهاكات والاختراقات :ثقة المستثمرين في المؤسسات الآمنة :تميل رؤوس الأموال إلى الاتجاه نحو الشركات التي تُظهر نضجًا في إدارة أمن المعلومات، باعتبار ذلك مؤشراً على الاحترافية والجدية. فشركات التكنولوجيا التي تعتمد معايير مثل ISO 27001 أو NIST تُعتبر أكثر جذبًا للمستثمرين مقارنة بنظيراتها غير المؤمَّنة .الأمن كميزة تنافسية في السوق الرقمية :أصبح الأمن الرقمي أحد معايير تقييم الشركات الناشئة، خاصة تلك التي تُعنى بالخدمات الرقمية مثل تطبيقات الصحة، التعليم، والتمويل. ووجود نظام أمن متكامل يُمكن أن يُترجم إلى فرص تمويل أكبر، ودخول أسهل إلى الأسواق

[1] عبد الله الجلود؛**الاقتصاد الرقمي والابتكار التكنولوجي**، مكتبة الرشد، الرياض، 2021 ص 113-119

الدولية .تحفيز الشراكات بين القطاعين العام والخاص :توفر البيئة الرقمية الآمنة شروطًا مثالية لإبرام شراكات بين الدولة والقطاع الخاص لتطوير حلول ذكية في قطاعات حساسة كالصحة، الطاقة، والتعليم، وهو ما يعزز الاقتصاد الوطني ويُسرّع عجلة الابتكار المحلي[1].

الفرع الثاني

تسهيل التجارة والتبادل الدولي

يشهد الاقتصاد العالمي تحولات كبيرة مع تزايد الاعتماد على التجارة الرقمية والتبادل الدولي عبر الحدود. في هذا السياق، يصبح الأمن السيبراني حجر الزاوية في تسهيل هذه العمليات بشكل آمن وموثوق. يساهم في حماية المعلومات والبيانات، ويؤمن المعاملات التجارية التي تتم عبر الإنترنت، ويشمل العديد من الآليات التي تضمن سلامة التجارة العالمية وحمايتها من التهديدات السيبرانية.

1. حماية أنظمة الدفع والتحويلات المالية

تعتبر أنظمة الدفع والتحويلات المالية من الركائز الأساسية التي تسهم بشكل كبير في تسهيل التجارة الدولية والنمو الاقتصادي في العصر الرقمي. مع التوسع الكبير في التجارة الإلكترونية والزيادة المستمرة في المعاملات المالية عبر الإنترنت، أصبحت الحاجة إلى تأمين هذه الأنظمة من أي تهديدات أو هجمات سيبرانية أمرًا بالغ الأهمية. بالإضافة إلى ذلك، تزداد حاجة الشركات والمستهلكين إلى ضمان أمان وسرية البيانات المالية الخاصة بهم عند إجراء المعاملات التجارية، مما يتطلب أنظمة حماية ذات مستوى عالٍ من الكفاءة.

ا-أهمية أنظمة الدفع في تسهيل التجارة الدولية

في العصر الرقمي، أصبحت أنظمة الدفع الرقمية أداة أساسية لتيسير التجارة عبر الحدود. من خلال ربط المؤسسات المالية عبر شبكات متقدمة وآمنة، تتيح هذه الأنظمة إجراء المعاملات بسرعة وفعالية، مما يقلل من الزمن المستغرق لتنفيذ المعاملات ويعزز من تدفق التجارة بين البلدان. نظام سويفت يعد من أبرز الأنظمة التي تساهم في تسهيل العمليات المالية عبر الحدود، حيث يُستخدم من قبل البنوك والمؤسسات

[1] عبد العزيز اللويحق،**مستقبل التقنيات الناشئة: الذكاء الاصطناعي، البيانات الضخمة، والميتافيرس**، مركز الملك عبد الله للدراسات، 2022 ص 28-36

المالية في تبادل الرسائل الخاصة بالتحويلات المالية بشكل مشفر وآمن. يقوم نظام سويفت بتأمين نقل البيانات بين الأطراف التجارية، مما يتيح للعملاء إجراء المدفوعات الدولية بسلاسة وثقة، وهو ما يساهم بشكل مباشر في تسريع تدفق الأموال بين الشركات والدول.

ب-أدوات التشفير في حماية المعاملات المالية

التشفير هو الأساس الذي يعتمد عليه في ضمان أمان المعاملات المالية .يُستخدم التشفير لحماية البيانات الشخصية والحساسة من أن يتم اعتراضها أو التلاعب بها أثناء نقلها عبر الإنترنت. تعتمد التقنيات المتقدمة مثل التشفير باستخدام المفتاح العام و التشفير المتماثل لضمان أن البيانات تظل محمية أثناء الانتقال عبر الشبكات العالمية. تضمن هذه العمليات أن تكون المعاملات المالية، سواء كانت عبر بطاقة ائتمان أو تحويل مصرفي، محمية من أي هجمات تهدف لاختراق الحسابات أو سرقة البيانات .من أهم أساليب التشفير التي تستخدمها المؤسسات المالية لتأمين المعاملات عبر الإنترنت هي طبقة المقابس الآمنة(SSL) و أمن طبقة النقل(TLS) ، حيث تستخدم هذه البروتوكولات في تشفير البيانات بين المتصفح والموقع الإلكتروني لضمان عدم الوصول إلى المعلومات الحساسة من قبل أي أطراف غير مصرح لها .تعمل هذه البروتوكولات على تأمين جميع بيانات الدفع والمعاملات المالية عبر الإنترنت، مما يقلل من خطر تعرض المستخدمين للقرصنة أو الاحتيال.

ج-التوثيق متعدد العوامل في المعاملات المالية

في سياق حماية المعاملات المالية الرقمية، يتجه العديد من المزودين والمصارف إلى اعتماد التوثيق متعدد العوامل (MFA) لتعزيز الأمان في المعاملات. يضيف هذا النظام طبقات متعددة من الحماية تتطلب من المستخدم تقديم أكثر من وسيلة واحدة للتحقق من هويته. يشتمل هذا على خطوات إضافية مثل إرسال رمز تحقق عبر الهاتف المحمول أو استخدام تطبيقات التوثيق، بالإضافة إلى استخدام أساليب بيومترية مثل بصمة الإصبع أو التعرف على الوجه .تُعد هذه الإجراءات ضرورية للحد من مخاطر الاحتيال، حيث يصعب على القراصنة تجاوز جميع هذه الأساليب لتحقيق هدفهم في اختراق الحسابات أو إجراء معاملات غير قانونية. هذه التقنية تساعد في زيادة ثقة الأفراد والشركات في إجراء المعاملات المالية عبر الإنترنت، مما يؤدي إلى تحفيز نمو التجارة الإلكترونية العالمية.

ح-تقنيات الذكاء الاصطناعي في مكافحة الاحتيال المالي

تساهم تقنيات الذكاء الاصطناعي في تعزيز أمن أنظمة الدفع والتحويلات المالية من خلال تحليل البيانات الكبيرة للكشف عن الأنشطة غير العادية أو المشبوهة التي قد تشير إلى وجود محاولات احتيال. باستخدام الخوارزميات المتقدمة، تقوم أنظمة الذكاء الاصطناعي بمراقبة المعاملات بشكل لحظي، مما يسمح بالكشف المبكر عن عمليات قد تكون مشبوهة. على سبيل المثال، إذا تم إجراء معاملة مالية غير عادية أو إذا كانت هناك تغييرات غير مبررة في نمط الدفع، يمكن للنظام أن يرفع تحذيرات أو يقوم بإيقاف المعاملة للتحقيق فيها .كما يمكن للذكاء الاصطناعي أن يساعد في تحسين القدرة على التنبؤ بأنماط الاحتيال المستقبلية بناءً على البيانات الحالية والماضية، وهو ما يسمح بتطوير استراتيجيات دفاعية أكثر تطورًا لمكافحة الاحتيال المالي.

د-التحديات المرتبطة بأنظمة الدفع الدولية

رغم الفوائد العديدة لأنظمة الدفع الرقمية، إلا أن هناك بعض التحديات التي تواجهها هذه الأنظمة. أولاً، يظل هناك خطر الاختراقات السيبرانية، حيث تستهدف بعض الهجمات الإلكترونية المؤسسات المالية بغية سرقة البيانات أو الأموال. ثانيًا، قد تكون الأنظمة القانونية المتباينة بين الدول عائقًا أمام تأمين المعاملات، حيث تختلف اللوائح والقوانين المتعلقة بحماية البيانات بين الدول مما قد يزيد من تعقيد تأمين المعاملات المالية عبر الحدود .إضافة إلى ذلك، تواجه بعض الدول النامية تحديات في البنية التحتية للأمن السيبراني، مما يجعلها عرضة للتهديدات الخارجية. على سبيل المثال، قد تواجه بعض البلدان صعوبة في توفير نظم حماية متقدمة مثل التشفير المتطور أو التقنيات المستخدمة لمكافحة غسيل الأموال.

ه-الحاجة إلى تعزيز الثقة في الأنظمة المالية الرقمية

من أجل تحقيق التجارة العالمية الفعالة والآمنة، يتعين تعزيز الثقة بين الأطراف التجارية من خلال اعتماد أنظمة تحقق موثوقة وتطبيق شهادات الأمان .على سبيل المثال، الشركات التي تتعامل في التجارة الإلكترونية العابرة للحدود يجب أن تحصل على شهادات أمان متوافقة مع المعايير الدولية مثل شهادة ISO

27001للأمن السيبراني، والتي توفر ضمانًا للأطراف المتعاملة في أن أنظمتها المالية آمنة وقادرة على حماية البيانات من أي تهديدات محتملة[1].

2 تشفير المعاملات المصرفية الدولية (مثل نظام سويفت)

تعتبر المعاملات المصرفية الدولية من الأنشطة الأساسية في الاقتصاد الرقمي المعاصر، حيث تُجرى العديد من العمليات المالية عبر الحدود بين مختلف البلدان، مما يتطلب توافر آليات أمنية متقدمة لضمان سرية المعلومات وحمايتها من التهديدات السيبرانية. في هذا السياق، يُعتبر نظام سويفت من أبرز الأنظمة المستخدمة في التبادل المالي بين البنوك العالمية .أهمية تشفير المعاملات المصرفية تُستخدم تقنيات التشفير لحماية المعاملات المصرفية عبر الإنترنت من محاولات القرصنة أو التلاعب. يعزز التشفير باستخدام مفتاح التشفير العام من أمان المعاملات، حيث يتضمن استخدام مفتاح خاص للتشفير وآخر لفك التشفير، مما يضمن أن البيانات المرسلة بين الأطراف ستكون محمية ولن يتمكن من الوصول إليها إلا المرسل والمستقبل المصرح لهما. وبفضل هذه التقنية، يمكن للمؤسسات المالية إتمام المعاملات بسرعة وأمان.
التحديات في تشفير المعاملات المصرفية الدولية رغم فوائد التشفير في ضمان أمان المعاملات، إلا أن هناك بعض التحديات المرتبطة به، أبرزها الحاجة إلى توافق الأنظمة الأمنية بين الدول المختلفة .قد تعاني بعض البلدان من ضعف في تنفيذ تقنيات التشفير الحديثة أو قد تفرض قيودًا على أنواع التشفير التي يمكن استخدامها في المعاملات الدولية. لذلك، تعتبر الاتفاقات الدولية بشأن الأمان السيبراني ضرورية لتوحيد الجهود في هذا المجال .نظام سويفت وأمان المعاملات نظام سويفت يعد أحد أهم الأنظمة التي تساهم في تسهيل التجارة الدولية وتبادل الأموال بين البنوك في مختلف أنحاء العالم. يُستخدم هذا النظام في إرسال الرسائل المالية المشفرة بين البنوك، وتتمثل أبرز فوائد النظام في ضمان سرعة تحويل الأموال مع الحفاظ على أمان وسرية البيانات. علاوة على ذلك، يُسهم في تقليل من مخاطر الاحتيال المالي، مما يجعل التجارة الدولية أكثر ثقة وأمانًا .الخلاصة إن تشفير المعاملات المصرفية الدولية عبر نظام سويفت يعزز من أمان وموثوقية التحويلات المالية بين الدول، ويعد من العوامل الأساسية التي تساهم في تحسين فعالية التجارة العالمية، مع ضمان حماية المعلومات المالية من الهجمات الإلكترونية[2].

[1] عبد العظيمحسام؛**التجارة الإلكترونية: النظرية والتطبيق.** القاهرة: دار الكتب العلمية، 2018.ص 220-225
[2] نبيل صلاح العربي 1؛**الاقتصاد الرقمي: المبادئ والتطبيقات.** القاهرة: مكتبة النهضة المصرية، 2017ص 180-200.

3. تأمين اختراق حسابات الشركات المستوردة/المصدرة في ظل التحول المتسارع نحو الرقمنة في مجال التجارة الدولية، أصبحت حسابات الشركات الناشطة في الاستيراد والتصدير عرضة بشكل متزايد للاختراقات الإلكترونية. تحتوي هذه الحسابات على معطيات حساسة تشمل العقود الدولية، تفاصيل التحويلات البنكية، ملفات الشحن، قواعد بيانات العملاء والموردين، والوثائق التجارية الرسمية. لذلك، فإن أي اختراق لهذه الحسابات قد يؤدي إلى خسائر مالية جسيمة، إرباك في المعاملات الدولية، وحتى توقف تام في العمليات التجارية، ناهيك عن الأضرار المعنوية المرتبطة بفقدان ثقة الشركاء الدوليين.وللوقاية من هذه المخاطر، أصبح من الضروري أن تعتمد المؤسسات آليات حماية متكاملة لحساباتها الرقمية، والتي يمكن تفصيلها كما يلي :

ا-تعزيز ضوابط الدخول للحسابات:

لا يكفي الاعتماد على كلمات المرور التقليدية، مهما بلغت قوتها. بل يتوجب استخدام آليات دخول متعددة الطبقات، مثل التحقق عبر رمز يُرسل إلى الهاتف المحمول، أو عبر البريد الإلكتروني، أو باستخدام وسائل تعريف بيومترية كالبصمة أو التعرف على الوجه. هذا النوع من التحقق المزدوج أو المتعدد يزيد من صعوبة اختراق الحسابات، حتى في حالة تسريب البيانات الأصلية .

ب-تشفير كامل للمعلومات أثناء التخزين والإرسال:

تشفير البيانات هو عملية تحويل المعلومات إلى رموز يصعب فكها من قبل غير المخوّلين. وعليه، فإن أي محاولة لاختراق الحسابات ستواجه بمحتوى غير مقروء وعديم الفائدة بالنسبة للمهاجم، مما يشكّل حاجزًا تقنيًا فعالًا ضد استغلال البيانات .

ج-مراقبة السلوك الرقمي للمستخدمين داخل الحسابات:

تعتمد الشركات الرائدة على أنظمة ذكية قادرة على تحليل سلوك المستخدمين داخل النظام، ورصد أي تصرفات مشبوهة، كالدخول من مناطق جغرافية غير معتادة، أو تنزيل كميات كبيرة من البيانات بشكل غير مبرر. هذه المراقبة اللحظية تسمح بالكشف المبكر عن محاولات الاختراق والتفاعل معها بسرعة قبل وقوع الضرر[1].

[1] عبد الحافظ، أحمد؛**أمن المعلومات وحمايتها في التجارة الإلكترونية** القاهرة: دار الفكر الجامعي، 2019 . ص 44-54

د-تحديث مستمر للبرامج وأنظمة الحماية:

الثغرات الأمنية غالبًا ما تكون ناتجة عن استخدام برمجيات قديمة لم يتم تحديثها. لذلك يجب الحرص على تنزيل التحديثات الأمنية بشكل دوري وفوري، سواء بالنسبة لنظام التشغيل أو تطبيقات إدارة الحسابات والمعاملات التجارية .

و-التوعية والتدريب الأمني للموظفين:

يمثل العنصر البشري أحد أهم ثغرات الأمن الرقمي. فكثير من الهجمات تنجح نتيجة انخداع الموظف برسائل احتيالية، أو ضغطه على روابط ضارة. ولهذا، يجب تنظيم دورات تدريبية دورية لجميع العاملين لتعريفهم بأساليب الخداع الحديثة، وطرق التبليغ عن أي نشاط مريب .

ه-استخدام أنظمة إدارة الهوية والصلاحيات:

يتوجب على الشركات ضبط من له حق الدخول إلى كل نوع من المعلومات داخل الحسابات، بحيث لا يمكن لأي موظف أن يصل إلى معلومات تفوق اختصاصه أو مهمته. هذا يقلل من احتمالات التسريب الداخلي أو الاختراق الناتج عن استغلال صلاحيات غير مضبوطة .

كما تعمل على التحقيق في محاولات الدخول الفاشلة متابعتهالأنها قد تكون مؤشرًا على هجمات إلكترونية يجري التحضير لها. وجود سجلات كاملة للدخول والخروج من الحسابات يساعد على التتبع والمساءلة.تُعد حماية هذه الحسابات من الاختراق ضمانًا مباشرًا لاستمرارية النشاط التجاري في البيئة الرقمية العالمية، وتُسهم بشكل مباشر في تعزيز الثقة بين الفاعلين الاقتصاديين، وتثبيت موقع الشركة كمؤسسة موثوقة وآمنة إلكترونيً[1]

4.تمكين التجارة الإلكترونية العابرة للحدود:

تأمين منصات البيع العالمية أصبحت التجارة الإلكترونية العابرة للحدود من أبرز مظاهر العولمة الاقتصادية الحديثة، حيث تُمكّن الأفراد والمؤسسات من بيع وشراء السلع والخدمات عبر الإنترنت، دون التقيد بالحدود الجغرافية أو القيود التقليدية التي كانت تعرقل التبادل التجاري الدولي. وقد ساهمت المنصات الرقمية الكبرى، مثل الأسواق الإلكترونية العالمية، في تسهيل هذه العمليات، مما جعلها عنصرًا حاسمًا في

[1]زكرياعماد ؛**أمن المعلومات وحماية الخصوصية في التجارة الإلكترونية.** القاهرة: مكتبة الشروق الدولية، 2020. ص 188

نمو التجارة الرقمية وتوسّعها .غير أن هذا التوسع ترافق مع تحديات أمنية خطيرة، أبرزها التزوير، الاحتيال، سرقة البيانات، وانتهاك الخصوصية، الأمر الذي يجعل من تأمين منصات التجارة الإلكترونية العالمية ضرورة قصوى لضمان بيئة رقمية آمنة للمستخدمين والمستثمرين على حد سواء .وتتجلى آليات التأمين الأساسية لهذه المنصات في عدة محاور رئيسية، نعرضها فيما يلي:

ا-تعزيز بنية الحماية الرقمية للمنصة

يشمل ذلك استخدام أنظمة حماية متطورة قادرة على صدّ الهجمات الإلكترونية، ومراقبة حركة البيانات، والتصدي لمحاولات الاختراق، مع الاعتماد على تقنيات تحليل سلوك المستخدمين لاكتشاف الأنشطة المشبوهة فورًا .

ب-التشفير الكامل للمعاملات والبيانات

يجب أن تكون جميع البيانات المتبادلة على المنصة – سواء كانت معلومات شخصية، أو بيانات دفع، أو تفاصيل الطلبيات مشفّرة بالكامل لحمايتها من أي محاولة اعتراض أو تسريب خلال عمليات الإرسال أو التخزين .

ج-ضمان مصداقية البائعين والمشترين

تقوم المنصات الموثوقة بفرض شروط صارمة للتسجيل، من خلال التحقق من الهوية، وربط الحسابات التجارية بوثائق رسمية معتمدة، ما يقلل من احتمالات وجود أطراف وهمية أو احتيالية.

ح-حماية أنظمة الدفع الإلكتروني

يجب أن تضمن المنصة حماية عمليات الدفع الرقمي من خلال توفير وسائل دفع آمنة، وإشراف مباشر على كل تحويل مالي، إلى جانب التعاون مع مؤسسات مالية موثوقة لضمان شفافية العمليات المالية وسهولة تتبعها .

ج-آليات الشكاوى وتسوية النزاعات

تأمين المنصة لا يتوقف على الحماية التقنية فحسب، بل يشمل أيضًا وجود آليات قانونية واضحة تمكّن الأطراف المتعاملة من تقديم الشكاوى وتسوية المنازعات بسرعة وشفافية، ما يزيد من ثقة المستخدمين بها.

ه-الامتثال للقوانين الدولية في حماية المستهلك

من المهم أن تلتزم هذه المنصات بالتشريعات الدولية المتعلقة بحقوق المستهلك، لا سيما من حيث حماية بياناته، ضمان جودة المنتجات، وتوفير شروط استرجاع عادلة في حال وجود خلل أو تلاعب.

و-التعاون مع سلطات الأمن السيبراني الدولية

لضمان استجابة سريعة لأي تهديد إلكتروني عابر للحدود، ينبغي أن تنسّق المنصات الكبرى مع الهيئات المختصة في الأمن الرقمي على المستوى الدولي، وتشارك في مبادرات التبليغ المشترك عن المخاطر والثغرات .وبفضل هذه الإجراءات، يمكن تعزيز مكانة التجارة الإلكترونية العابرة للحدود كخيار آمن وفعال للتبادل التجاري، وتوسيع دائرة المشاركة في الاقتصاد الرقمي العالمي، خصوصًا في ظل تزايد الاعتماد على التسوق الإلكتروني في مختلف أنحاء العالم[1].

5.تيسير العمليات الجمركية الرقمية

ا-تأمين أنظمة التخليص الجمركي الإلكتروني

يُعتبر التخليص الجمركي الإلكتروني من الأدوات الأساسية التي تسهل حركة التجارة الدولية وتختصر الوقت والجهد. يعتمد هذا النظام على استخدام البرمجيات والتقنيات الرقمية لتقديم البيانات الجمركية، دفع الرسوم، وتتبع الشحنات بشكل إلكتروني. ورغم المزايا العديدة لهذه الأنظمة، فإن تأمينها يشكل تحديًا كبيرًا نظرًا لأن أي اختراق قد يؤدي إلى فوضى في التعاملات التجارية. لذلك، يجب تعزيز أنظمة التخليص الجمركي الإلكتروني باستخدام تقنيات التشفير المتقدمة لضمان حماية البيانات المتبادلة بين جميع الأطراف المعنية، مثل الشركات المصدرة والمستوردة، والسلطات الجمركية، وبنوك الدفع .كما يجب استخدام أدوات تحليل سلوكي ذكي للكشف عن أي نشاط مشبوه أو تلاعب، مثل إدخال بيانات غير صحيحة أو محاولة

[1] سليمعلي؛**التجارة الإلكترونية الحديثة: الواقع والمستقبل**. بيروت: دار الفجر للنشر، 2016.

التهرب من الرسوم الجمركية. تعزيز هذه الأنظمة يعني ضمان التزام كل الأطراف بالمعايير القانونية وتعزيز الثقة في التجارة الدولية الرقمية .

ب-حماية وثائق الاستيراد/التصدير الرقمية

الوثائق الرقمية المتعلقة بالاستيراد والتصدير تمثل أساس عملية التحقق من صحة المعاملات التجارية. تشمل هذه الوثائق الفواتير الجمركية، شهادات المنشأ، إشعارات الشحن، وغيرها من الوثائق التي تُعتبر ضرورية لتأمين السلع المتداولة عبر الحدود. ولضمان حماية هذه الوثائق من التلاعب أو التسريب، يتم استخدام تقنيات التشفير الحديثة التي تُبقي البيانات مشفرة أثناء نقلها وتخزينها. إضافة إلى ذلك، تُستخدم أنظمة التوقيع الإلكتروني لضمان أن الوثائق المرسلة صحيحة وآمنة ولا يمكن تعديلها من قبل أطراف غير موثوقة .يجب على السلطات الجمركية التأكد من أن جميع الوثائق المقدمة مع الشحنات هي أصلية ومعتمدة، ما يساهم في تقليل مخاطر التلاعب ويزيد من موثوقية المعاملات الجمركية .

ج-منع تزوير الشهادات والتراخيص الدولية

تعد الشهادات والتراخيص الدولية، مثل شهادات المنشأ، تصاريح الاستيراد، شهادات الفحص، وغيرها، من العناصر الحيوية في ضمان توافق البضائع مع المعايير الصحية والبيئية والاقتصادية الخاصة بكل دولة. ومع ازدياد الاعتماد على العمليات الرقمية، أصبح تزوير هذه الوثائق يمثل تهديدًا كبيرًا لأمن التجارة الدولية. للتصدي لهذه المخاطر، يتم استخدام تقنيات متقدمة مثل التوقيع الرقمي الذي يُعد من أكثر الأساليب أمانًا في ضمان صحة الوثائق وتوثيقها. كما تُستخدم الرموز المائية(Watermarking) لمنع التلاعب بها. إضافة إلى ذلك، يمكن الاعتماد على تقنية البلوك تشين لتسجيل وتوثيق الشهادات والتراخيص بطريقة لا يمكن تعديلها أو تغييرها، ما يعزز من الشفافية والمصداقية في التجارة الدولية. باعتماد هذه التقنيات، يمكن تقليل التزوير بشكل كبير وضمان التحقق الفعّال من مصداقية الشهادات والتراخيص المعتمدة في التجارة عبر الحدود[1].

6حماية الملكية الفكرية في التبادل التجاري

ا-تأمين براءات الاختراع والتصاميم

[1]القيسي يحيى؛**التجارة الإلكترونية: المفاهيم والتطبيقات.**عمان: دار وائل للنشر، 2015. ص 89

براءات الاختراع والتصاميم الصناعية تمثل جزءًا أساسيًا من الملكية الفكرية التي تحمي الابتكارات والإبداعات من الاستنساخ غير القانوني. في عالم التجارة الدولية والتبادل التجاري الرقمي، تصبح حماية هذه البراءات والتصاميم أمرًا بالغ الأهمية، خاصة مع تزايد السرعة التي تُنقل بها المعلومات والمنتجات عبر الإنترنت. لحماية براءات الاختراع، يجب استخدام أنظمة تشفير متقدمة لتمكين نقل المعلومات المتعلقة بالبراءات بأمان، مع ضمان أن الأشخاص المصرح لهم فقط هم من يمكنهم الوصول إلى هذه البيانات الحساسة. علاوة على ذلك، يمكن استخدام تقنيات البلوك تشين لتوثيق براءات الاختراع، مما يوفر سجلًا ثابتًا وآمنًا يمكن الرجوع إليه عند الحاجة، ويمنع التلاعب في البيانات أو سرقتها. من خلال هذه الإجراءات، يتم ضمان أن حقوق الملكية الفكرية المتعلقة بالاختراعات والتصاميم محمية من الاستنساخ غير المشروع في الأسواق العالمية .

ب-حماية الأسرار التجارية أثناء النقل الرقمي

الأسرار التجارية مثل قواعد البيانات، استراتيجيات التسويق، صيغ المنتجات، وأي معلومات تعتبر قيمة وحساسة بالنسبة للمؤسسات التجارية، تحتاج إلى حماية صارمة أثناء نقلها عبر الإنترنت. استخدام التقنيات الأمنية المناسبة مثل التشفير من طرف إلى طرف يُعد أمرًا ضروريًا لضمان عدم اعتراض أو سرقة هذه الأسرار أثناء إرسالها عبر الشبكات الرقمية. يجب تطبيق أدوات تحقق متعددة الأطراف لضمان أن الأشخاص الذين يتعاملون مع هذه المعلومات هم فقط من يحق لهم الوصول إليها. إضافة إلى ذلك، يمكن للأنظمة القائمة على الذكاء الاصطناعي مراقبة الأنشطة المشبوهة بشكل فوري لاكتشاف أي محاولة للوصول غير المصرح به. بالتالي، فإن حماية الأسرار التجارية أثناء النقل الرقمي يُعتبر خطوة أساسية لضمان سرية المعلومات التجارية وحمايتها من السرقة أو التلاعب .

ج-مكافحة قرصنة المنتجات الرقمية

تعد قرصنة المنتجات الرقمية، مثل البرمجيات، الكتب الإلكترونية، الأفلام، والموسيقى، من القضايا البارزة في التجارة الرقمية. هذه القرصنة تؤثر سلبًا على حقوق الملكية الفكرية وتسبب خسائر كبيرة لأصحاب المنتجات الرقمية .لمكافحة هذه القرصنة، يمكن استخدام تقنيات مثل التشفير الرقمي لحماية المحتوى، مما يجعل من الصعب على أي شخص غير مصرح له الوصول إلى هذه المنتجات أو توزيعها بشكل غير قانوني. بالإضافة إلى ذلك، تتوفر أنظمة إدارة الحقوق الرقمية (DRM) التي تتيح لأصحاب المنتجات

الرقمية التحكم في كيفية توزيع واستخدام منتجاتهم عبر الإنترنت. من خلال هذه الأنظمة، يتم الحد من انتشار النسخ غير القانونية وحماية الملكية الفكرية للمنتجات الرقمية. كما يمكن تشجيع التعاون بين الشركات الكبرى والحكومات في إطار اتفاقيات مكافحة القرصنة على الإنترنت، مما يساهم في تحسين التشريعات وتطبيق القوانين الخاصة بحماية حقوق الملكية الفكرية في الفضاء الرقمي[1].

7.تعزيز الثقة بين الشركاء التجاريين

ا-أنظمة التحقق من الهوية الموثوقة

في ظل التحول الرقمي المتسارع في التجارة العالمية، أصبح من الضروري تعزيز الثقة بين الشركاء التجاريين عبر تأكيد الهوية الموثوقة للأطراف المتعاملة .أنظمة التحقق من الهوية تُعد من الوسائل الأساسية لضمان أن الأطراف التي تتعامل مع بعضها البعض هي كيانات حقيقية وصحيحة. في التجارة الإلكترونية، يتم اعتماد تقنيات مثل التحقق الثنائي (Two-Factor Authentication) أو التوثيق البيومتري لضمان مصداقية الهوية. من خلال هذه الأنظمة، يمكن التحقق من هوية الأشخاص أو المؤسسات عبر طرق متعددة، مثل كلمات المرور، الرموز المرسلة إلى الهاتف، أو حتى القياسات البيومترية مثل بصمة الأصبع أو الوجه .كما يمكن استخدام التوقيع الرقمي في المعاملات التجارية لضمان أن جميع الأطراف تقوم بالمعاملات بناءً على معلومات دقيقة وموثوقة. هذا يعزز الأمان ويقلل من مخاطر الاحتيال أو التلاعب في المعاملات التجارية، مما يعزز الثقة بين الشركات والأطراف المتعاملة .

ب-شهادات الأمان السيبراني للمؤسسات) مثل(ISO 27001

الشهادات السيبرانية مثل ISO 27001 تمثل معيارًا دوليًا معترفًا به لإدارة أمن المعلومات داخل المؤسسات. هذه الشهادات تُظهر التزام المؤسسة بحماية بيانات عملائها، وحفظ المعلومات بشكل آمن، وتطبيق أفضل الممارسات في مجال الأمن السيبراني. الحصول على شهادة ISO 27001 يعتبر خطوة هامة لتعزيز الثقة بين الشركاء التجاريين، حيث يُظهر للشركات المتعاملة أن هذه المؤسسة قد اتخذت جميع التدابير اللازمة لضمان حماية البيانات وحمايتها من الاختراقات أو الهجمات الإلكترونية. كما أن هذه الشهادات تساهم في إنشاء بيئة آمنة للعمل وتقلل من مخاطر الخروقات الأمنية التي قد تضر بسمعة الشركة

[1] الجندي فؤاد؛**أمن المعلومات في التجارة الإلكترونية.** القاهرة: دار العلوم للنشر، 2021 ص 41

أو تؤدي إلى خسائر مالية. من خلال اعتماد هذه الشهادات، يمكن للمؤسسات أن تضمن للعملاء والشركاء التجاريين مستوى عالٍ من الأمان في المعاملات والبيانات[1].

8.من الآثار الإيجابية للتطورات في التبادل التجاري الرقمي

ا-خفض تكاليف المعاملات الدولية بنسبة 25-40%

من أبرز الآثار الإيجابية لتطبيق الأنظمة الرقمية في التجارة الدولية هو خفض التكاليف المرتبطة بالمعاملات التجارية. عند اعتماد الأنظمة الرقمية للأعمال التجارية، يتم تقليل الحاجة إلى الإجراءات الورقية واليدوية المعقدة، مما يؤدي إلى تسريع العمليات وتقليل النفقات المتعلقة بالنقل، الطباعة، والتخزين. كما تساهم تقنيات مثل الذكاء الاصطناعي والبلوك تشين في تسريع الإجراءات المالية والتجارية، مما يؤدي إلى توفير الوقت والتكاليف المرتبطة بالتحقق من المعاملات وتنفيذها. بالإضافة إلى ذلك، يمكن تقليل عدد الوسطاء المشاركين في العمليات التجارية بفضل تحسين التواصل بين الأطراف المعنية. في النهاية، تساهم هذه التحسينات في تقليل التكاليف بنسبة تتراوح من 25% إلى 40%، مما يعزز القدرة التنافسية للشركات ويزيد من ربحيتها .

ب-تقليل حالات الاحتيال التجاري بنسبة 30-50%

التكنولوجيا الرقمية تقدم مجموعة من الأدوات التي تساهم في تقليل المخاطر المرتبطة بالاحتيال التجاري. باستخدام الأنظمة المتقدمة للتحقق من الهوية، التوقيع الرقمي، وتقنيات التشفير، يمكن تحسين الأمان وتقليل التلاعب أو التزوير في المعاملات التجارية. كما تساهم الأنظمة الذكية التي تعتمد على تحليل البيانات والذكاء الاصطناعي في اكتشاف الأنماط المشبوهة في وقت مبكر، مما يقلل من احتمالية حدوث عمليات احتيال. وقد أظهرت الدراسات أن الشركات التي تعتمد على الأنظمة الرقمية للتعامل مع المدفوعات والتحقق من المعاملات قد تمكنت من تقليل حالات الاحتيال بنسبة تتراوح بين30% و 50%. هذا بدوره يعزز الثقة بين الشركات التجارية ويحفز على إتمام المعاملات التجارية بأمان وفعالية.

ج-زيادة حجم التجارة الإلكترونية العالمية بشكل آمن

نعيمي عادل؛ **التجارة الإلكترونية وحماية البيانات الشخصية.** عمان: دار جروس للنشر، 2019 ص 200

التطورات الرقمية ساعدت على توسيع نطاق التجارة الإلكترونية على المستوى العالمي، إذ يُتوقع أن تستمر هذه التجارة في النمو بشكل متسارع مع توفير بيئة آمنة وموثوقة للمعاملات التجارية عبر الإنترنت. من خلال ضمان الأمان السيبراني، التحقق من الهوية، وحماية المعلومات الحساسة، يستطيع المشترون والبائعون من جميع أنحاء العالم تنفيذ المعاملات بأمان. هذا النمو يُترجم إلى زيادة في حجم التجارة الإلكترونية بشكل ملحوظ، مما يساهم في تحسين الاقتصاد العالمي. إضافة إلى ذلك، تتيح التجارة الإلكترونية الرقمية للأفراد والشركات في الأسواق الناشئة الوصول إلى أسواق أكبر، مما يعزز من تبادل السلع والخدمات ويزيد من فرص العمل. من خلال تقنيات التشفير وحماية البيانات، يمكن التأكد من أن المعاملات الإلكترونية تتم بطريقة آمنة، ما يحفز المزيد من الشركات للاستثمار في التجارة الإلكترونية[1].

المبحث الثاني

التداعيات السلبية للأمن السيبيراني على العلاقات الدولية

في ظل التحوّل الرقمي المتسارع، لم تعد التهديدات السيبرانية مجرّد اختراقات تقنية معزولة، بل أضحت أدوات استراتيجية ذات أبعاد جيوسياسية واقتصادية عميقة. لقد أفرزت الطفرة الرقمية بيئة جديدة من التفاعلات الدولية، تتداخل فيها المصالح وتشتد فيها حدة المنافسة، حيث بات الأمن السيبراني عاملًا حاسمًا في تشكيل ملامح العلاقات بين الدول .وقد كشف هذا الواقع عن مجموعة من التداعيات السلبية التي تتجاوز الأطر التقنية، لتطال جوهر العلاقات السياسية والدبلوماسية، من خلال حملات التجسس، والتأثير على العمليات الانتخابية، وتهديد السيادة الوطنية، فضلًا عن زعزعة الثقة بين الدول. كما لم تسلم العلاقات الاقتصادية الدولية من هذه التهديدات، حيث تأثرت سلاسل التوريد، وتعطّلت أنظمة الدفع العالمية، وتزايدت الهجمات على الملكية الفكرية، مما أدى إلى اختلالات في التجارة والاستثمار، وانخفاض ثقة الفاعلين الاقتصاديين .وعليه، يهدف هذا القسم إلى استعراض وتحليل هذه التداعيات في محورين رئيسيين: الأول يتناول الأثر السلبي للأمن السيبراني في المجال السياسي والدولي، والثاني يرصد الانعكاسات الاقتصادية لهذه التهديدات في السياق الدولي، مع تقديم أمثلة واقعية وموثّقة تبرز خطورة الظاهرة.

المطلب الأول

[1] قاسممصطفى؛**حماية البرمجيات الرقمية وبراءات الاختراع.** بيروت: دار الساقي للنشر، 2017. ص 83 -95

التداعيات السلبية للأمن السيبيراني في مجال العلاقات السياسية الدولية

في ظل تصاعد التهديدات السيبرانية عالميًا، بات الأمن السيبراني أحد أهم محاور التأثير في العلاقات السياسية الدولية، حيث أضحى يمثل أداة فعالة في الصراعات غير التقليدية بين الدول، ووسيلة لتحقيق أهداف سياسية دون اللجوء إلى المواجهات العسكرية المباشرة. لقد ساهم تطوّر أدوات الاختراق، والاعتماد المتزايد على الرقمنة في الأجهزة الحكومية والبنى التحتية، في تحويل الفضاء السيبراني إلى ساحة صراع سياسية بامتياز، تتجلى من خلالها مظاهر خفية من التدخل، والابتزاز، والتجسس، وتعطيل آليات التعاون الدولي.

الفرع الأول

التهديدات السيبيرانية وأثرها على سيادة الدول وعلاقاتها السياسية

أولًا :التدخل السيبراني في الشؤون الداخلية للدول

أصبح الفضاء السيبراني أداة استراتيجية بيد الدول والجهات الفاعلة غير الحكومية للتدخل في الشؤون الداخلية للدول الأخرى، بما يشكل تهديدًا صريحًا لمبدأ السيادة الوطنية الذي يعد أحد أسس النظام الدولي الحديث. لم يعد التدخل مقتصرًا على الأساليب التقليدية عبر الغزو العسكري أو الضغوط الاقتصادية والدبلوماسية، بل بات يتم من خلال وسائل رقمية متطورة يصعب كشفها وتتبع آثارها المباشرة.تتمثل أبرز مظاهر التدخل السيبراني في اختراق قواعد البيانات الحكومية، والتلاعب بالمعلومات الحساسة، واختراق شبكات الإعلام الرسمي وغير الرسمي بهدف التأثير على توجهات الرأي العام الداخلي. كما يشمل هذا التدخل بث حملات تضليل إعلامي عبر وسائل التواصل الاجتماعي لدعم جماعات معارضة، أو إثارة النزعات العرقية والطائفية، مما يؤدي إلى تقويض الاستقرار السياسي وزرع الفوضى داخل الدول المستهدفة .ويُعد التدخل في العمليات الانتخابية أحد أخطر أشكال التدخل السيبراني، حيث يتم التلاعب بسجلات الناخبين، أو اختراق أنظمة التصويت، أو نشر معلومات مضللة تؤثر على إرادة الناخبين. إضافة إلى ذلك، تقوم بعض الدول باستخدام الهجمات السيبرانية لتقويض الثقة في المؤسسات الوطنية وإظهار عجز السلطات المحلية عن حماية أمنها الداخلي .تُشكل هذه التدخلات تحديًا حقيقيًا للمجتمع الدولي، إذ يصعب إثبات المسؤولية المباشرة عنها بسبب الطابع غير المادي للهجمات الإلكترونية، وإمكانية استخدام تقنيات متقدمة لإخفاء هوية الفاعلين. كما أن غياب إطار قانوني دولي موحد ينظم السلوك في الفضاء السيبراني يزيد من تعقيد عملية التصدي لمثل هذه الاعتداءات، مما يدفع الدول إلى تطوير استراتيجيات

دفاعية وهجومية سيبرانية جديدة لضمان حماية أمنها الوطني .وإزاء هذه التهديدات، أكدت العديد من المواثيق والتقارير الدولية على ضرورة احترام مبادئ السيادة وعدم التدخل، حتى في الفضاء الرقمي. وقد دعت الأمم المتحدة عبر فريق الخبراء الحكوميين إلى اعتبار الهجمات السيبرانية التي ترقى إلى مستوى الإخلال بسيادة الدولة بمثابة أعمال عدوانية تتطلب ردا مناسبا في إطار الشرعية الدولية[1] .

ثانيًا :التجسس الإلكتروني واختراق الأنظمة الحكومية الحساسة

أصبح التجسس الإلكتروني أحد أبرز التهديدات التي تواجه الأمن السيبراني على مستوى العالم، ويشكل خطرًا متزايدًا على استقرار الدول وأمنها القومي. في عالمنا المعاصر، حيث أصبحت البيانات والمعلومات الحساسة تشكل رأس المال الاستراتيجي لكل دولة، يُعد اختراق الأنظمة الحكومية والحصول على هذه المعلومات سرًا من أسرار الحرب السيبرانية الحديثة. إن التجسس الإلكتروني لا يقتصر على سرقة المعلومات الحساسة فحسب، بل يتعداه ليشمل استهداف البنى التحتية للدولة بأكملها، بما في ذلك المؤسسات المالية، أنظمة الدفاع، الاتصالات، والخدمات الحيوية .إحدى أبرز سمات التجسس الإلكتروني هو استخدام أساليب متقدمة وأدوات متطورة، مثل البرمجيات الخبيثة (Malware) وبرامج التجسس(Spyware) ، التي يتم زرعها في الأنظمة الرقمية بهدف مراقبة البيانات المتداولة بين الجهات الحكومية، أو سحبها بشكل غير مرئي. تتخذ هذه الهجمات في بعض الأحيان شكل هجمات ممنهجة ومنسقة تستهدف جهات متعددة داخل الدولة المستهدفة في وقت واحد، مما يزيد من تعقيد عمليات الرد والملاحقة .من الأمثلة البارزة على هذا النوع من الهجمات هو هجومSolarWindsالذي وقع في عام 2020، حيث تم اختراق الشبكة الإلكترونية لشركةSolarWinds، وهي إحدى الشركات التي توفر حلول تكنولوجيا المعلومات للعديد من الوكالات الحكومية والشركات الكبرى في الولايات المتحدة. أدى هذا الهجوم إلى اختراق بيانات حساسة لعدة وكالات حكومية أمريكية، بما في ذلك وزارة الخزانة ووزارة الأمن الداخلي، مما أتاح للجهات المهاجمة الاطلاع على اتصالات حساسة ومعلومات استراتيجية يمكن أن تُستخدم في صياغة سياسات دولية أو لتوجيه مصالح اقتصادية وجيوسياسية .كما أن التجسس الإلكتروني يستهدف في بعض الأحيان الدول ذات الأنظمة السياسية المستبدة أو الضعيفة بغرض الحصول على معلومات استخباراتية حول السياسات الداخلية أو التفاعل مع الحركات المعارضة. يتم استخدام هذه البيانات لتوجيه استراتيجيات السياسة الخارجية، وللتأثير على الخيارات الاستراتيجية للدول المستهدفة في المحافل الدولية .علاوة على ذلك،

[1] محمد علي عمر؛**الأمنالسيبراني وانعكاساته على السيادة الوطنية**دار الفكر الجامعي، الإسكندرية، 2021، ص. 88-90.

يُستعمل التجسس الإلكتروني بشكل متزايد كأداة للحروب الاقتصادية، حيث تقوم بعض الجهات بشن هجمات سيبرانية بهدف سرقة أسرار صناعية أو تقنيات حساسة من الشركات الكبرى والمؤسسات البحثية. وهذا النوع من الهجمات يعكس تحولات كبيرة في مجال الأمن السيبراني، إذ أصبح يتداخل مع مجالات أخرى مثل الحرب الاقتصادية والتنافس الصناعي، مما يُزيد من تعقيد الأبعاد القانونية والسياسية لمكافحة هذه الظاهرة .تزداد التحديات أمام الدول في مجال التحقيق في هجمات التجسس الإلكتروني، لكون الفاعلين لا يكونون دائمًا واضحين، إذ يقومون باستخدام تقنيات لتخفي هويتهم، مثل استخدام الخوادم المخفية وتقنيات التمويه الرقمي. وبسبب هذه الصعوبة، غالبًا ما تواجه الدول صعوبة في تحديد الجهة المسؤولة عن الهجوم، مما يعرقل قدرة المجتمع الدولي على تنفيذ عقوبات مناسبة أو اتخاذ تدابير رادعة[1] .

ثالثًا :سرقة البيانات الدبلوماسية والأمنية وابتزاز الدول

تُعتبر سرقة البيانات الدبلوماسية والأمنية من أبرز صور الهجمات السيبرانية التي تهدد الأمن السيادي للدول. فالدول تعتمد بشكل متزايد على الأنظمة الرقمية لإدارة المعلومات الحساسة المتعلقة بالسياسات الأمنية، والخطط الدفاعية، والعلاقات الدولية، والاتفاقيات الاقتصادية والتجارية. وعليه، فإن سرقة هذه البيانات لا تُعدّ مجرد انتهاك للخصوصية أو للأمن السيبراني، بل هي بمثابة اختراق مباشر للسيادة الوطنية، يمكن أن يعرض الدولة لمخاطر استراتيجية هائلة .تشمل هذه الهجمات السيبرانية استهداف السفارات والبعثات الدبلوماسية في الخارج، وتهدف إلى الوصول إلى سجلات دبلوماسية ومراسلات سرية بين الحكومات أو بين الدول. هذه البيانات لا تقتصر على المواقف السياسية أو المفاوضات السرية فحسب، بل قد تشمل معلومات تتعلق بتحالفات استراتيجية أو اتفاقيات اقتصادية قد تُمثل تهديدًا إذا تم تسريبها أو استخدامها بشكل غير قانوني .على سبيل المثال، الهجوم الذي تعرضت له وزارة الخارجية الأمريكية في عام 2014، حيث استهدفت مجموعة قراصنة إلكترونيين مقرها في واشنطن، وتمكنوا من الوصول إلى البريد الإلكتروني للعديد من المسؤولين الدبلوماسيين. وعليه، تم تسريب معلومات حساسة عن المفاوضات والاتفاقات الدولية، مما أثر بشكل سلبي على العلاقات بين الولايات المتحدة وبعض الدول الشريكة.
وبالإضافة إلى ذلك، يُعتبر الابتزاز باستخدام هذه البيانات إحدى الأساليب السيبرانية الحديثة، حيث تقوم جهات غير حكومية أو حكومات معادية بسرقة معلومات حساسة تهدف إلى استخدامها لاحقًا كورقة ضغط على الدول. يمكن أن تتضمن هذه العمليات تهديدات بنشر هذه المعلومات في وسائل الإعلام الدولية أو

[1] خالد الزبيدي؛**الحروب السيبرانية: مخاطرها وأبعادها الإستراتيجية**لمركز العربي للأبحاث ودراسة السياسات، بيروت، 2022،ص 202-199

استخدامها في التفاوض على صفقات سياسية أو اقتصادية. هذا النوع من الابتزاز يمكن أن يعرض الدول المستهدفة لمخاطر كبيرة، خاصة إذا كانت المعلومات المُسربة تتعلق بشؤون دفاعية أو أمنية حساسة.في هذا السياق، تمثل هجمات مثل التي تعرضت لها العديد من المؤسسات الدفاعية في دول الاتحاد الأوروبي أو الهجمات التي استهدفت وكالات الاستخبارات الأمريكية في فترات سابقة، نموذجًا لما يمكن أن تؤدي إليه مثل هذه الهجمات من تدهور في العلاقات بين الدول وزيادة التوترات الدولية. من خلال هذه الهجمات، يمكن للأعداء أن يكتسبوا ميزة تنافسية، حيث يمكنهم استغلال هذه المعلومات في صياغة سياسات خارجية أو داخلية تهدف إلى إضعاف الدولة المستهدفة .تستمر الدول في تطوير استراتيجيات سيبرانية لحماية بياناتها الدبلوماسية والأمنية، مثل استخدام تشفير البيانات، وتعزيز أنظمة الدفاع الرقمي. ولكن على الرغم من هذه الإجراءات، تبقى عمليات سرقة البيانات واستخدامها لأغراض ابتزازية تهديدًا دائمًا يمكن أن يتسبب في انهيار الثقة بين الدول ويؤدي إلى تغييرات كبيرة في الديناميكيات السياسية الدولية[1]

رابعاً :التلاعب بالعمليات السياسية

التلاعب بالعمليات السياسية من خلال الهجمات السيبرانية أصبح من أبرز التحديات التي تواجه الدول في العصر الحديث. يشمل هذا التلاعب مجموعة متنوعة من الأنشطة التي تؤثر بشكل كبير على نزاهة الانتخابات والعمليات السياسية، وهو ما يؤدي إلى تهديد الاستقرار السياسي ويؤثر بشكل مباشر على العلاقات الدولية. وفيما يلي توسيع الشرح لهذا الموضوع :

1. اختراق الأنظمة الانتخابية:

الهجمات السيبرانية على الأنظمة الانتخابية تهدف إلى التأثير على سير العملية الانتخابية عن طريق اختراق نظم التصويت أو قواعد البيانات الانتخابية. هذه الهجمات قد تشمل :التلاعب في سجلات الناخبين: من خلال اختراق قواعد البيانات الخاصة بالناخبين، يمكن تغيير البيانات الشخصية أو حذف الأسماء أو إضافة أسماء وهمية بهدف التلاعب في النتائج أو تعطيل العملية الانتخابية .تعديل نتائج التصويت: يمكن للهجمات الإلكترونية أن تؤدي إلى تعديل نتائج التصويت في أماكن معينة من خلال اختراق أنظمة التصويت الإلكتروني أو التلاعب في الحسابات الآلية للنتائج .مثال على ذلك هو الهجوم السيبراني على الانتخابات الرئاسية الأمريكية في 2016، حيث كانت هناك محاولات اختراق لبعض أنظمة التصويت في الولايات الأمريكية بهدف التأثير على النتائج .

[1] محمود حسين،**تهديدات الأمن السيبراني: التحديات والعواقب القانونية** دار الجليل للنشر، عمان، 2021 ص 18 -20

2. التأثير على الرأي العام من خلال المعلومات المضللة:

تعتبر الوسائل الرقمية، مثل منصات التواصل الاجتماعي، أدوات قوية لنشر المعلومات المضللة (أو الأخبار الزائفة) بهدف التأثير على تصورات الناخبين والمواطنين حول القضايا السياسية. الهجمات السيبرانية قد تشمل :نشر أخبار كاذبة: يمكن للقراصنة السيبرانيين نشر قصص مفبركة أو معلومات مضللة عبر وسائل الإعلام الرقمية، مما يؤدي إلى تشويه الحقائق والتلاعب بآراء الجمهور .التأثير على انطباع الناخبين: هذه الحملات الإعلامية يمكن أن تؤثر على قرارات الناخبين، مما يجعلهم يصوتون بناءً على معلومات غير صحيحة أو مغلوطة .في الانتخابات الأمريكية 2016، استخدمت مجموعات مختلفة حسابات وهمية على وسائل التواصل الاجتماعي لنشر معلومات مغلوطة حول المرشحين والقضايا السياسية، مما أثار الشكوك حول نزاهة الانتخابات .

3. قرصنة وسائل الإعلام الرسمية:

يمكن أن تكون وسائل الإعلام الرسمية عرضة للهجمات السيبرانية التي تهدف إلى تغيير محتوى الأخبار أو استبدال تقارير حقيقية بأخرى مغلوطة. الهجمات قد تشمل :استيلاء على حسابات الصحف أو القنوات الإخبارية: الهجوم على الحسابات الرسمية للمنابر الإعلامية قد يسمح للقراصنة بنشر محتوى مزيف أو محرف يؤثر على الجمهور .تحريف الأخبار: قد يتم اختراق أنظمة الأخبار لتعديل أو تحريف تقارير هامة، مثل تقارير عن الانتخابات أو قضايا سياسية حساسة، مما يساهم في نشر معلومات مغلوطة تضر بالمصداقية العامة .مثال على ذلك هو الهجوم الذي تعرضت له وكالة الأنباء البريطانية "رويترز "في بعض الأحيان، حيث كانت هناك محاولات للتلاعب بالأخبار أو تسريب معلومات مغلوطة.

4. التلاعب بنتائج الانتخابات:

في بعض الحالات، يمكن للهجمات السيبرانية أن تؤدي إلى التلاعب المباشر في نتائج الانتخابات. يحدث هذا عندما يتم اختراق الأنظمة المخصصة لفرز الأصوات أو حتى التصويت الإلكتروني نفسه. تشمل هذه الأنشطة :تغيير نتائج التصويت: من خلال اختراق نظام التصويت الإلكتروني أو اختراق المراكز الانتخابية، قد يتم تغيير الأصوات لصالح مرشح معين .وقف العد أو تعطيل الأنظمة: في بعض الحالات، يمكن أن تؤدي الهجمات إلى تعطيل عملية العد أو تجميد الأنظمة، مما يتسبب في فقدان الثقة في نتائج الانتخابات .المثال الأبرز هو الهجوم الذي استهدف الانتخابات الرئاسية في 2000 في الولايات المتحدة،

حيث أدت بعض المشاكل التقنية في فرز الأصوات إلى حالة من الغموض والتوتر السياسي، رغم أنها لم تكن هجمة سيبرانية في ذلك الوقت. لكن الهجمات السيبرانية الحديثة قد تجعل مثل هذه الحوادث أكثر احتمالاً .

5. تهديد الأمن السياسي الداخلي:

التلاعب في العمليات الانتخابية لا يؤدي فقط إلى التأثير على نتائج الانتخابات، بل يمتد تأثيره إلى الأمن السياسي الداخلي. إذ قد تؤدي هذه الهجمات إلى :تفاقم الانقسامات السياسية: بعد التلاعب بالانتخابات أو نشر معلومات مضللة، تصبح هناك فجوات كبيرة في الثقة بين المواطنين والحكومة، مما يؤدي إلى تقسيم المجتمع حول نتائج الانتخابات .زيادة الاحتجاجات والاضطرابات: عندما يشعر المواطنون بأن نتائج الانتخابات قد تم التلاعب بها أو أن الأنظمة السياسية غير نزيهة، قد ينشأ غضب شعبي يؤدي إلى احتجاجات واسعة أو اضطرابات اجتماعية .الأثر على العلاقات الدولية :التلاعب بالعمليات السياسية له تأثير كبير على العلاقات بين الدول. على سبيل المثال :اتهامات بالتدخل في الشؤون الداخلية: عندما تكتشف دولة ما أن دولة أخرى قد تدخلت في انتخابات أو عمليات سياسية عبر الإنترنت، فقد تؤدي هذه الاكتشافات إلى توترات دبلوماسية واتهامات بالتدخل في السيادة الوطنية .العقوبات السياسية والاقتصادية: الدول المتهمة بالتلاعب بالانتخابات قد تواجه عقوبات اقتصادية أو دبلوماسية من دول أخرى، مما يزيد من حدة التوترات الدولية .فقدان الثقة بين الحكومات: الهجمات السيبرانية التي تستهدف العمليات السياسية تزيد من شكوك الدول في قدرة شركائها على حماية أمنهم السيبراني، مما قد يؤدي إلى تفكك التحالفات الدولية .في الختام، التلاعب بالعمليات السياسية عبر الهجمات السيبرانية أصبح تهديداً حقيقياً يؤثر على الدول الداخلية والدولية، حيث يهدد الأمن السياسي الداخلي ويزيد من التوترات الدبلوماسية ويؤثر على شرعية الحكومات.[1]

خامساً :العقوبات السيبرانية

أصبحت أداة متزايدة في الساحة الدولية، حيث تستخدم الدول هذه العقوبات في الرد على الهجمات الإلكترونية أو التهديدات السيبرانية التي تستهدف أمنها الوطني أو مصالحها الاستراتيجية. يتم فرض هذه العقوبات على الدول أو الكيانات أو الأفراد الذين يُعتقد أنهم مسؤولون عن الهجمات السيبرانية، ويمكن أن تتخذ هذه العقوبات أشكالاً متنوعة تؤثر بشكل كبير على العلاقات الدولية من هذه العقوبات نذكر:

[1] النعيميعادل؛الأمن السيبراني وتأثيراته على الأمن الوطنيدار الاكاديميون للنشر والتوزيع 2019 ص 65-80

1. فرض قيود تكنولوجية:

واحدة من أبرز أشكال العقوبات السيبرانية هي فرض قيود على التكنولوجيا. هذه القيود قد تشمل حظر الشركات أو المنتجات التكنولوجية التي يُعتقد أنها تشكل تهديدًا للأمن السيبراني لدولة معينة. على سبيل المثال :حظر الشركات التكنولوجية: من أبرز الأمثلة على ذلك هو الحظر الذي فرضته الولايات المتحدة على شركة "هواوي" الصينية في عام 2019، حيث اعتبرت الحكومة الأمريكية أن الشركة تشكل تهديدًا للأمن القومي بسبب علاقتها بالحكومة الصينية. هذا الحظر أثر بشكل كبير على قدرة هواوي على استخدام التقنيات الأمريكية في معداتها وأجهزتها .منع الوصول إلى تكنولوجيا متقدمة: قد تُفرض عقوبات على دول أو شركات لمنعها من الوصول إلى تقنيات معينة قد تُستخدم في شن هجمات سيبرانية، مثل تكنولوجيا الحوسبة السحابية أو البرمجيات المتقدمة .

2. تجميد الأصول:

عقوبة أخرى شائعة في السياسات السيبرانية هي تجميد أصول الأفراد أو الكيانات المتورطة في الهجمات الإلكترونية. يهدف هذا الإجراء إلى الحد من قدرة الأفراد أو الكيانات المستهدفة على استخدام أموالهم أو ممتلكاتهم في تنفيذ أعمال غير مشروعة، ويشمل :تجميد الأرصدة البنكية: تُفرض العقوبات على الأفراد أو الكيانات عبر تجميد أرصدتهم في البنوك أو منعهم من الوصول إلى أموالهم، مما يعطل أنشطتهم الاقتصادية .تجميد الأصول المملوكة للكيانات: قد تتضمن العقوبات تجميد الأصول المملوكة لشركات أو كيانات حكومية قد تكون مسؤولة عن الهجمات الإلكترونية .مثال على ذلك هو العقوبات التي فرضتها الولايات المتحدة والاتحاد الأوروبي على الكيانات الروسية في عام 2017 بعد الهجوم السيبراني على الديمقراطيات الغربية، مثل هجوم "نوتبيتيا" الذي استهدف أوكرانيا وانتشر ليؤثر على عدة دول أخرى.

3. حظر السفر على الأفراد:

في بعض الحالات، قد تشمل العقوبات السيبرانية منع الأفراد المسؤولين عن الهجمات السيبرانية من السفر إلى دول معينة. تهدف هذه العقوبات إلى معاقبة الأفراد المتورطين في الهجمات الإلكترونية ومنعهم من الاستفادة من السفر الدولي أو الوصول إلى الأنظمة المالية العالمية .تقييد حرية الحركة: قد تفرض الدول عقوبات على الأفراد المشتبه في تورطهم في هجمات سيبرانية عبر حظر دخولهم إلى أراضيها أو من خلال إلغاء تأشيرات السفر الممنوحة لهم .

4. عقوبات اقتصادية:

العقوبات السيبرانية قد تمتد إلى فرض عقوبات اقتصادية على الدول التي تُتهم بشن هجمات سيبرانية. قد تشمل هذه العقوبات فرض رسوم جمركية أو فرض قيود على التجارة بين الدول. الهدف من هذه العقوبات هو التأثير على الاقتصاد الوطني للبلد المستهدف وتعزيز الضغط عليه لقبول شروط معينة، مثل:فرض رسوم تجارية: قد تفرض بعض الدول رسوماً إضافية على السلع القادمة من دولة تمثل تهديدًا سيبرانيًا. حظر الصفقات التجارية: يتم فرض عقوبات تجارية لمنع الدول من إبرام صفقات تجارية مع كيانات تعتبرها الدولة المستهدفة منخرطة في الهجمات الإلكترونية.

5. التأثيراتالسلبية على العلاقات الدولية:

العقوبات السيبرانية قد تؤدي إلى توتر العلاقات بين الدول. عندما تفرض دولة عقوبات سيبرانية على دولة أخرى بسبب هجمات إلكترونية، يمكن أن يؤدي ذلك إلى تصعيد الخلافات السياسية والاقتصادية بين الدول، وهو ما يؤثر بشكل مباشر على التعاون الدولي في المجالات الأخرى مثل التجارة أو الأمن.زيادة التوترات الدبلوماسية: فرض العقوبات السيبرانية قد يؤدي إلى تصاعد التوترات بين الدول المعنية، مما يعيق التفاهم والتعاون في قضايا أخرى .الانتقام السيبراني: بعض الدول قد ترد على العقوبات السيبرانية من خلال شن هجمات إلكترونية على الدول التي فرضت هذه العقوبات، مما يؤدي إلى تزايد النزاعات السيبرانية بين الدول .في الختام، تعتبر العقوبات السيبرانية أداة هامة في مواجهة التهديدات السيبرانية، ولكنها قد تؤدي إلى تعقيد العلاقات الدولية وزيادة التوترات بين الدول، مما يستدعي اتخاذ إجراءات حذرة ومدروسة في استخدامها[1].

الفرع الثاني

تأجيج الصراعات والنزاعات السياسية (الإقليمية والدولية)

في العصر الحديث، أصبح الأمن السيبراني يشكل جزءًا أساسيًا من الصراعات الدولية والإقليمية، حيث يتم استخدام الفضاء الإلكتروني كأداة رئيسية لتأجيج النزاعات السياسية والصراعات بين الدول. لم يعد هذا المجال محصورًا في مسائل الحماية فقط، بل أصبح ساحة جديدة لشن الهجمات الإلكترونية التي تؤثر على الاستقرار السياسي والاقتصادي، وتؤدي إلى تعقيد العلاقات الدولية

[1] النعيميعادل. مرجع سابق ص 88

أولاً: الأمن السيبراني كسلاح سياسي جديد

لقد تطور الأمن السيبراني ليصبح سلاحًا سياسيًا غير مباشر تستخدمه الدول لتحقيق مصالحها السياسية والاقتصادية دون الحاجة إلى المواجهة العسكرية المباشرة. وأصبح يُنظر إلى الهجمات الإلكترونية كوسيلة فعالة للضغط على الخصوم في العديد من الأزمات السياسية. يمكن تقسيم هذه الظاهرة إلى عدة نقاط رئيسية :

1. **أداة للعدوان غير المباشر**: الهجمات السيبرانية أصبحت أداة فعالة للعدوان غير المباشر. الدول التي تستخدم الهجمات السيبرانية لا تحتاج إلى إرسال قوات عسكرية أو الدخول في مواجهات مفتوحة، بل يمكنها ضرب الأهداف الاستراتيجية عبر الفضاء الإلكتروني، ما يؤدي إلى تأثيرات كبيرة على مستوى الأمن القومي للدول المستهدفة.

هجمات إيران على منشآت النفط السعودية (2019-2022): في الفترة بين 2019 و2022، استهدفت إيران منشآت النفط السعودية عبر هجمات سيبرانية معقدة أثرت بشكل كبير على الإنتاج النفطي للملكة. تم استخدام هذه الهجمات كوسيلة للضغط على الحكومة السعودية في ظل التوترات الإقليمية بين البلدين. على الرغم من أن هذه الهجمات كانت إلكترونية ولم تجرِ المواجهة العسكرية المباشرة، إلا أن تأثيراتها الاقتصادية والسياسية كانت هائلة، حيث تم تعطيل جزء كبير من الإنتاج النفطي، وهو ما أثر في أسواق النفط العالمية. هذه الهجمات هي مثال على كيف يمكن للأمن السيبراني أن يكون أداة لتوجيه ضغوطات غير مباشرة ضد خصم سياسي واقتصادي .هجمات روسيا على البنية التحتية الأوكرانية قبل الغزو (2021-2022): قبل أن تبدأ روسيا هجومها العسكري على أوكرانيا في فبراير 2022، قامت بالعديد من الهجمات السيبرانية على البنية التحتية الأوكرانية الحيوية. شملت هذه الهجمات استهداف شبكات الكهرباء والماء والاتصالات، مما أدى إلى تدمير جزء كبير من البنية التحتية التي تعتمد عليها الحكومة الأوكرانية في إدارة شؤون البلاد. الهدف من هذه الهجمات كان إضعاف أوكرانيا قبل الغزو العسكري، وتحقيق نوع من الهيمنة الاستراتيجية على الدولة الأوكرانية. هذا النموذج يظهر كيف أن الأمن السيبراني يمكن أن يُستخدم كأداة حرب قبل أن تتحول الأمور إلى مواجهات عسكرية مباشرة.[1]

ثانياً: حروب بالوكالة عبر الأمن السيبراني

[1] سعيدجمال؛**الأمن السيبراني: التحديات والفرص في العلاقات الدولية**،دار الفكر العربي 2021 ص 75-88

في سياق الحروب الحديثة، أصبح الأمن السيبراني وسيلة أساسية للحروب بالوكالة. الدول لا تقتصر على شن الهجمات مباشرة، بل تقوم بدعم جماعات قراصنة إلكترونية لشن هجمات ضد خصومها، مما يجعل من الصعب تحديد المسؤول المباشر عن الهجوم ويصعب الرد عليه. هذا النوع من الهجمات أصبح شائعًا في الصراعات الإقليمية والدولية، حيث يتم تنفيذها تحت ستار من الإنكار الرسمي.

ا-استخدام جماعات قرصنة موالية: الدول التي لا ترغب في تحمل المسؤولية المباشرة عن الهجمات السيبرانية قد تستخدم جماعات قرصنة موالية لها أو جماعات مسلحة بالوكالة لتنفيذ الهجمات. هذه الجماعات قد تكون شبه حكومية أو تتلقى دعمًا غير مباشر من الحكومات، وبالتالي لا يمكن تحديد من يقف وراء الهجوم بسهولة.

جماعة APT 29 الروسية: تُعد جماعة) APT 29 المعروفة أيضًا باسم "دراجونفلاي") من أبرز أمثلة هذه الجماعات، وهي مجموعة قرصنة سيبرانية روسية موالية للحكومة الروسية. قامت هذه الجماعة بشن العديد من الهجمات السيبرانية ضد الحكومات الغربية، بما في ذلك الولايات المتحدة، حيث استهدفت وزارات حكومية وشركات كبيرة بهدف جمع المعلومات الاستخباراتية. من خلال هذه الهجمات، تسعى روسيا إلى تنفيذ أهداف سياسية بعيدة عن المواجهة العسكرية المباشرة، مما يعزز استخدامها للأمن السيبراني في تنفيذ استراتيجيات الحرب بالوكالة.

ب-تمويل قراصنة لتنفيذ هجمات "قابلة للإنكار": في بعض الحالات، تقوم الدول بتمويل قراصنة إلكترونيين لتنفيذ هجمات يمكن إنكارها علنًا، مما يجعل من الصعب إثبات تورط الدولة في هذه الهجمات. هذا يسمح للدول بتوجيه ضغوط على الخصوم دون أن تكون عرضة للعواقب السياسية أو العسكرية المباشرة.

هجمات كوريا الشمالية: كوريا الشمالية تعد من أبرز الدول التي تستخدم هذا التكتيك عبر دعم جماعات قراصنة لتنفيذ هجمات سيبرانية، مثل هجوم "رانسوم وير" الذي استهدف العديد من البنوك في أنحاء مختلفة من العالم، ومن بينها هجوم على بنك بنغلاديش في 2016. الهدف من هذه الهجمات هو الحصول على أموال طائلة لدعم الاقتصاد الكوري الشمالي، فضلًا عن تنفيذ ضغوط اقتصادية على الدول المستهدفة.

بالنظر إلى أن كوريا الشمالية تنفي دائمًا مسؤوليتها عن هذه الهجمات، فإنه يكون من الصعب على الدول المعنية الرد بشكل مباشر أو اتخاذ إجراء دبلوماسي ضدها[1] .

الفرع الثالث

تفويض التعاون الدولي في المجال السياسي

أولا : تفجير الأزمات الدبلوماسية التسريبات الموجهة:مثل تسريبات ويكيليكس، التي أثرت على علاقات أكثر من مائة دولة، مما أدى إلى أزمات ثقة بين الحلفاء .تسريب "الملفات البحرينية) "2021 :(والذي تسبب في توتر شديد في العلاقات بين دول مجلس التعاون الخليجي

ثانيا : تعطيل آليات الحوار الدبلوماسي استهداف المؤسسات الدولية :مثل الهجمات السيبرانية على مقرات منظمة الأمم المتحدة بجنيف عام 2021، واختراق أنظمة منظمة الصحة العالمية خلال جائحة كوفيد-19، ما أدى إلى إرباك العمليات الدبلوماسية والإنسانية .تعطيل القنوات الرسمية :من خلال استهداف أنظمة السفارات مثل الهجوم السيبراني على سفارة الولايات المتحدة في كينيا سنة 2023 .تشويش المؤتمرات الافتراضية الرسمية :عبر التدخلات الخبيثة في الاجتماعات والمؤتمرات الدبلوماسية الافتراضية لتعطيل سير المناقشات وتخريب مخرجاتها

ثالثاً: التلاعب بالسياسات الخارجية اختراق حسابات دبلوماسيين:كما حدث في "هجوم القرصان المزيف" سنة 2022، حيث تم إرسال رسائل مزيفة من حسابات دبلوماسية رسمية .تزوير الوثائق الدبلوماسية :كما في قضية تزوير الوثائق بين قطر والإمارات عام 2017، مما أدى إلى زيادة التوترات الإقليمية

رابعاً: تعقيد إدارة الأزمات الدولية التدخل في عمليات الوساطة:مثل اختراق مفاوضات السلام في اليمن سنة 2021 .تسريب مسودات اتفاقيات دولية :ما يؤثر سلباً على سير التفاوض وثقة الأطراف المعنية . تضليل صناع القرار :عبر تزويدهم بمعلومات استخباراتية مزورة .تزوير تحليلات استخباراتية مشتركة:

بما يؤدي إلى زعزعة الثقة بين الحلفاء .سرقة بيانات مشتركة بين أجهزة استخباراتية :ما يهدد الأمن القومي لدول عدة .زرع الشكوك بين الشركاء الاستراتيجيين :مما يؤدي إلى تفكك التحالفات وفشل التعاون الدولي

[1] حسن، عبد الله؛**السياسة السيبرانية: استراتيجيات الحروب الرقمية وأثرها في العلاقات الدولية**.دار العلوم للنشر بيروت 2022 ص 220

خامساً: استهداف المنظمات الإقليمية اختراق أنظمة الاتحاد الإفريقي) 2020-2023:(ما أضعف قدرته على تنسيق الجهود الإقليمية .الهجمات على أرشيف جامعة الدول العربية :بما يحمل من تهديد لتاريخ الدبلوماسية العربية ووثائقها الحساسة .سادساً: التداعيات الاستراتيجية ارتفاع تكاليف التعاون الدولي :بسبب الحاجة المتزايدة لتأمين قنوات الاتصال وحماية الأنظمة المعلوماتية .تباطؤ عمليات اتخاذ القرار المشترك : نتيجة فقدان الثقة وتزايد الحذر بين الدول .تحول في نمط العلاقات الدولية :مع تراجع الاعتماد على الدبلوماسية السرية لصالح القنوات غير الرسمية .زيادة الاعتماد على وسائل الاتصال غير الرقمية :لا سيما في الملفات الحساسة، كإجراء اللقاءات الشخصية المباشرة .تجزئة النظام الدولي :مع ظهور تحالفات سيبرانية متعارضة وتشكيل "حدائق سيبرانية مسيجة"، مثل التجارب الصينية والروسية[1].

المطلب الثاني

التداعيات السلبية في مجال العلاقات الاقتصادية الدولية

شهدت العلاقات الاقتصادية الدولية تحولات جوهرية بفعل تزايد الاعتماد على الفضاء الرقمي والتكنولوجي، غير أن هذه التحولات أفرزت تحديات أمنية أثرت سلبًا على النمو الاقتصادي والاستقرار التجاري. وتتمثل أبرز هذه التداعيات السلبية في: استخدام الأمن السيبراني كأداة للمنافسة الاقتصادية غير المشروعة، تآكل الثقة في الاقتصاد الرقمي العالمي، وتعطيل التجارة والاستثمار الدولي

الفرع الأول

استخدام الأمن السيبراني كأداة للمنافسة الاقتصادية غير العادلة

لقد أفرز التقدم التكنولوجي تطورًا نوعيًا في أساليب المنافسة الاقتصادية بين الدول والشركات، حيث أصبح الأمن السيبراني مجالًا استراتيجيًا تستخدمه بعض الأطراف كوسيلة غير عادلة لإضعاف المنافسين والاستيلاء على مزاياهم التقنية والتجارية. ويُلاحظ أن هذه الأفعال تتخذ عدة أشكال رئيسية نوضحها فيما يلي :

1. سرقة الملكية الفكرية والابتكارات التكنولوجية

[1] تقرير الأمن الدبلوماسي الأمريكي، 2023

تُعد سرقة الملكية الفكرية واحدة من أخطر مظاهر الهجمات السيبرانية التي تستهدف شركات التكنولوجيا والمؤسسات البحثية. إذ تقوم مجموعات مدعومة من بعض الدول بشن هجمات موجهة نحو ابتكارات الشركات الكبرى للحصول على معلومات سرية وتكنولوجيات متقدمة دون إذن أو ترخيص.ومن أبرز الأمثلة :تعرض شركة Google سنة 2009 لاختراق كبير نُسب إلى جهات صينية ضمن حملة تعرف بـOperation Aurora، استهدفت تقنيات متعلقة بمحركات البحث والبريد الإلكتروني .قيام مجموعة APT10بشن هجمات إلكترونية مكثفة على شركات الطيران والدفاع الأمريكية، لسرقة بيانات تتعلق بتصميمات أنظمة الطيران الحديثة .استهداف شركة Tesla سنة 2018 بهجمات تهدف إلى سرقة تصميمات سياراتها الكهربائية المتطورة .تعرض مختبرات الأدوية مثل Pfizer وModernaلهجمات خلال جائحة كوفيد-19، ما كشف عن محاولات لسرقة أبحاث اللقاحات الحيوية .سرقة بحوث متعلقة بالطاقة المتجددة من شركات أوروبية كبرى، وهو ما أثر على تنافسيتها الدولية.هذه السرقات تمنح الجهة الفاعلة ميزة تنافسية غير مشروعة، من خلال تفادي تكاليف البحث والتطوير وتحقيق سبق صناعي على حساب الشركات الضحية[1].

2. تعطيل سلاسل التوريد العالمية

يمثل تعطيل سلاسل التوريد العالمية أحد أبرز أساليب المنافسة الاقتصادية غير العادلة التي تتم عبر الهجمات السيبرانية .ومن الأمثلة البارزة على ذلك :هجوم سيبراني طال مصانع Samsung عام 2023، مما أدى إلى تعطيل أنظمة الإنتاج وتأخير توريد الأجهزة الإلكترونية إلى الأسواق العالمية.شل أنظمة الشحن اللوجستية لشركات تجارية كبرى، مما تسبب في اضطراب كبير في توزيع البضائع على المستوى العالمي .التلاعب بالبيانات التشغيلية للمصانع الذكية، مثل تغيير مواصفات المنتجات أثناء مراحل الإنتاج أو تزوير بيانات الجودة، مما يضعف سمعة الشركات المستهدفة ويزيد من نسبة المرتجعات والمنتجات المعيبة .هذه الأساليب تعرقل الإنتاج، وترفع التكاليف، وتؤثر سلبًا على العلاقات التعاقدية بين الشركات وموردیها وزبائنها[2].

3. التخريب الاقتصادي المباشر

[1]حسنين علي حسين«**الجريمة الإلكترونية وأثرها على الاقتصاد العالمي**» مجلة العلوم الاقتصادية والإدارية، العدد 8، 2021 ص 112
[2]عبد الله محمد العجمي«**التهديدات السيبرانية وأثرها على سلاسل الإمداد العالمية**» المجلة العربية للأمن السيبراني، العدد 3، 2022 ص 200

يتجسد التخريب الاقتصادي المباشر في شل القدرة التشغيلية للمؤسسات الاقتصادية الحيوية عبر هجمات الفدية والهجمات التخريبية .ومن أبرز هذه الحالات :هجوم 2021 على خط أنابيب الوقود الأمريكي Colonial Pipeline، الذي تسبب في أزمة وقود حادة أثرت على شرق الولايات المتحدة، وخسائر بالمليارات .شن هجمات إلكترونية على مستشفيات بهدف شل قدراتها التنافسية، مثل تعطيل أنظمة المعلومات في المستشفيات الكبرى مما أثر على قدرتها على تقديم الخدمات الطبية .التلاعب بالأسواق المالية عبر اختراق أنظمة التداول، مثل حادثة Flash Crash التي شهدها سوق NASDAQ سنة 2010، حيث تم توجيه الأسواق بشكل مصطنع مما أدى إلى خسائر فادحة .نشر معلومات مالية مزيفة للتأثير على أسعار الأسهم، بما يخل بمبدأ الشفافية والمساواة في الأسواق المالية العالمية[1] .

4. التجسس الاقتصادي والاستخبارات التجارية

تسعى بعض الدول والجهات الاقتصادية عبر التجسس السيبراني إلى جمع معلومات حساسة عن خطط الشركات واستراتيجياتها التفاوضية .وتتجلى أبرز الأساليب في :اختراق اجتماعات مجالس الإدارة عن بعد، مما يسمح بالحصول على قرارات استراتيجية سرية .التجسس على المفاوضات التجارية الحساسة بين الشركات أو بين الدول، بما يمنح جهة معينة أفضلية تفاوضية غير عادلة .هذا النوع من التجسس يخل بمبدأ السرية التجارية، ويؤدي إلى نتائج اقتصادية غير متوازنة[2].

5. دعم الشركات المحلية بشكل غير مشروع

تلجأ بعض الحكومات إلى استخدام الهجمات السيبرانية لدعم شركاتها الوطنية بشكل غير مشروع، عبر : توفير معلومات مسروقة عن منافسين أجانب لشركاتها المحلية، كما في حالة اتهام شركة Huawei بالحصول على تقنيات أجنبية بدعم حكومي صيني .تسريب تقنيات أجنبية إلى الشركات المحلية بأسعار زهيدة أو نقلها بطرق سرية .شل قدرة المنافسين الأجانب عبر شن هجمات على شركات التعدين الأسترالية. تعطيل أنظمة شركات الطيران المنافسة خاصة في منطقة الشرق الأوسط، لتقوية وضع شركات الطيران المحلية .مثل هذه التصرفات تضر بالتنافسية الدولية وتخالف قواعد منظمة التجارة العالمية[3] .

---

[1] سامي حسن العلي؛**الأمنالسيبراني في ظل العولمة الاقتصادية**،دار المنهل العربي، بيروت، 2021 ص 45-55

[2] ريم عبد الله أبو السعود **«التجسس الإلكتروني وأثره على العلاقات التجارية الدولية»**،المجلة العربية للعلوم السياسية، العدد 67، 2020 ص 12

[3] خالد عبد الرحمن الزهراني**«التنافس الاقتصادي الدولي وأثر الهجمات السيبرانية»** مجلة الدراسات الدولية، العدد 12، 2022 ص 18

الفرع الثاني

تفويض الثقة في الاقتصاد الرقمي العالمي

أصبح الاقتصاد الرقمي حجر الأساس في التبادلات التجارية والمالية عبر العالم. غير أن تصاعد الهجمات السيبرانية أدى إلى تآكل الثقة بين الأطراف الفاعلة في هذا الاقتصاد، وهو ما ألقى بظلال ثقيلة على المعاملات الرقمية وعلى بنية الاقتصاد العالمي عمومًا.

1. تآكل أسس الثقة الرقمية

تعتمد الثقة الرقمية على حماية البيانات وضمان سرية المعاملات، غير أن عدة حوادث سيبرانية أدت إلى تفكك هذه الثقة بشكل خطير :في حادثة Yahoo بين عامي 2013 و2014، تم اختراق حسابات أكثر من 3 مليار مستخدم، ما عرّض بياناتهم الشخصية للسرقة، وهز ثقة المستخدمين بالشركات الرقمية الكبرى. وفي عام 2018، تعرضت سلسلة فنادق Marriott لاختراق سيبراني أدى إلى تسريب بيانات حوالي 500 مليون نزيل، بما في ذلك معلومات جوازات السفر والبطاقات البنكية .إضافةً إلى ذلك، شهد العالم انتشارًا واسعًا لعمليات تزوير الهوية الرقمية، حيث ارتفعت حالات انتحال الشخصية بنسبة 113% منذ 2019، كما زادت عمليات تزوير شهادات- SSL التي تضمن أمان المواقع الإلكترونية- بمعدل نمو سنوي يقدر بـ30 .%هذه الحوادث قوضت الإيمان بالأمن الرقمي وأثرت على ممارسات المستهلكين والشركات على السواء[1] .

2. التأثيرات المباشرة على القطاعات الحيوية

لم يكن تأثير فقدان الثقة مقتصرًا على الأفراد، بل امتد إلى القطاعات الاقتصادية الحيوية، حيث ظهرت عدة آثار ملموسة :الخدمات المالية :انخفضت ثقة المستهلكين في الخدمات البنكية الرقمية بنسبة 28% عقب الهجمات السيبرانية الكبرى، مما أدى إلى عزوف فئات واسعة عن استخدام التطبيقات المصرفية عبر الإنترنت. وتشير التقديرات إلى أن قطاع التمويل الإسلامي الإلكتروني يسجل خسائر سنوية تقدر بـ1.4 مليار دولار نتيجة للهجمات .التجارة الإلكترونية :بسبب المخاوف الأمنية، 40% من المستهلكين يلغون عمليات الشراء عبر الإنترنت خوفًا من تسريب بياناتهم المالية أو الشخصية .المعاملات العابرة للحدود :

[1] محمد عبد الله العتيبي، «التحولات الأمنية في الاقتصاد الرقمي: تحديات الثقة» المجلة العربية للأمن المعلوماتي، العدد 5، 2021 ص 22

شهدت المعاملات الرقمية في الأسواق الناشئة تراجعًا بنسبة 15-20%، نتيجة مخاوف من المخاطر السيبرانية التي تهدد أمن البيانات التجارية والمالية .تؤدي هذه التأثيرات إلى تباطؤ نمو الاقتصاد الرقمي وفقدان الفرص الاستثمارية الهامة[1].

3. تداعيات إضافية على المعاملات والثقة الدولية

بفعل التهديدات المتزايدة، باتت الشركات العالمية تفرض إجراءات أمان أكثر صرامة، ما أدى إلى :زيادة التكاليف المرتبطة بحماية البيانات وتشفير المعاملات .بطء عمليات المصادقة والتحقق، مما يؤخر المعاملات التجارية الكبرى .اشتداد المنافسة حول من يملك بيئات رقمية أكثر أمانًا، ما خلق تفاوتات جديدة بين الشركات وحتى بين الدول .وقد دفع هذا الوضع ببعض الدول إلى سن تشريعات أكثر تشددًا لحماية البيانات، مثل قانون GDPR الأوروبي، لكن هذه التشريعات أضافت أعباء إضافية على الشركات الناشئة والأسواق النامية[2].

الفرع الثالث

تعطيل التجارة والاستثمارات الدولية

تزايدت الهجمات السيبرانية على البنية التحتية التجارية والمالية للدول والشركات الكبرى، مما تسبب في تعطيل حركة التجارة العالمية وتدفق الاستثمارات الأجنبية، وأدى إلى ارتفاع التكاليف وتعقيد العمليات الدولية بشكل ملحوظ.

1. تعطيل سلاسل التوريد العالمية

تُعد سلاسل التوريد العالمية عصب التجارة الدولية، وقد أصبحت هدفًا رئيسيًا للهجمات الإلكترونية بسبب ما تمثله من أهمية استراتيجية :في عام 2021، تعرض ميناء روتردام، وهو أكبر ميناء في أوروبا، لهجوم إلكتروني عطل العمليات فيه لمدة 72 ساعة، مما تسبب في تأخير وصول آلاف الحاويات وحدوث خسائر تجارية ضخمة .كما تم تسجيل اختراقات لأنظمة الموانئ السعودية والإماراتية بين عامي 2022 و2023،

[1] عبد الرحمن مصطفى جابر؛ **الاقتصاد الرقمي والأمن السيبراني: بين التوسع والتحديات** دار الفكر العربي، القاهرة، ص852022-78

[2] فاطمة الزهراء شرف الدين، «الأمن السيبراني وعلاقته بالثقة الاقتصادية في البيئة الرقمية» مجلة بحوث السياسات العامة، العدد 15، 2023 ص 11-18

مما أدى إلى تعطيل شحنات استراتيجية وتأخير العمليات التجارية الحساسة .من جهة أخرى، أصبح التلاعب بأنظمة التتبع ظاهرة متنامية، حيث أدت الاختراقات إلى اختفاء شحنات بقيمة 2.3 مليار دولار سنويًا بسبب تغييرات وهمية في أنظمة التتبع الجمركي، بالإضافة إلى تزوير بيانات الجمارك الإلكترونية بنسبة 17% في التجارة عبر الحدود .هذا النوع من الهجمات ألحق ضررًا مباشرًا بتدفق السلع وأدى إلى زيادة تكلفة الاستيراد والتصدير وأضعف الثقة في الأنظمة اللوجستية العالمية[1].

2. التأثيرات المباشرة على تدفق الاستثمارات

نتيجة لعدم اليقين الذي أحدثته الهجمات السيبرانية، شهد العالم تدفقات استثمارية متذبذبة :سجلت الإحصاءات انخفاضًا بنسبة 12% في الاستثمار الأجنبي المباشر في القطاعات الرقمية الحساسة، مثل التكنولوجيا المالية والتجارة الإلكترونية .على صعيد آخر، ارتفعت شروط التأمين على المشاريع التقنية بنسبة 40%، مما زاد من الأعباء المالية على المستثمرين والشركات الناشئة، وأدى إلى إحجام بعض المستثمرين عن ضخ رؤوس أموالهم في المشاريع الرقمية المعرضة للمخاطر السيبرانية .النتيجة كانت بطء نمو الأسواق الرقمية الناشئة وتباطؤ التحول الرقمي في العديد من الدول النامية[2].

3. تعطيل أنظمة الدفع الدولية

تعتمد التجارة الدولية الحديثة بشكل كبير على أنظمة الدفع الإلكتروني السريع، مما جعل هذه الأنظمة هدفًا رئيسيًا للهجمات السيبرانية :تعرض نظامSWIFT ، الذي يستخدم لتحويل الأموال عبر الحدود، لهجوم في عام 2022 أدى إلى تعطيله لمدة 8 ساعات، مما أثر على مئات التحويلات الكبرى بين البنوك الدولية .وفي عام 2023، تم تنفيذ هجوم منسق على 37 بنكًا آسيويًا، مما أدى إلى شل عمليات التحويل وإرباك الأسواق المالية في عدة دول .هذه الهجمات أدت إلى فقدان الثقة في الأنظمة البنكية الرقمية، وإلى تعزيز النزعة نحو استخدام أنظمة دفع بديلة أو تقليدية[3].

4. ارتفاع تكاليف المعاملات

---

[1] سامي عبد الله الغامدي **«الأمن السيبراني وسلاسل التوريد العالمية: تهديدات وحلول»**مجلة الاقتصاد والأمن القومي، العدد 9، 2022 ص 32

[2] عبد القادر عموري؛**تداعيات الهجمات السيبرانية على مناخ الاستثمار الدولي**دار الهدى للنشر، الجزائر، 2023 ص 17

[3] ياسين بن موسى**«التحولات في بنية النظام المالي الدولي بسبب الهجمات السيبرانية»** مجلة الدراسات الاقتصادية الدولية، العدد 6، 2024 ص 15

بفعل تصاعد الهجمات وزيادة الحاجة إلى آليات تأمين إضافية :ارتفعت رسوم التحويلات الدولية بنسبة 15-20% لتغطية تكاليف الأمن والحماية من الاختراقات .كما تم إدخال مدة تأخير إضافية تقدر بـ12 ساعة للتحقق من المعاملات الكبرى العابرة للحدود، مما أثر على سرعة إنجاز الصفقات التجارية .هذا الوضع خلق بيئة تجارية أقل كفاءة، وزاد من التكاليف التشغيلية للشركات العاملة في التجارة الدولية[1] .

5. التأثيرات على الشركات المتعددة الجنسيات

الشركات الكبرى كانت من بين الأكثر تضررًا :تشير الإحصاءات إلى أن 43% من الشركات المتعددة الجنسيات تعرضت لتعطيلات بسبب الهجمات السيبرانية .بلغ متوسط تكلفة الخسائر لكل شركة حوالي 8.2 مليون دولار، نتيجة لتوقف العمليات، أو دفع الفديات، أو خسارة العملاء .هذه الخسائر دفعت العديد من الشركات إلى إعادة تقييم استراتيجياتها الرقمية، وزيادة استثماراتها في مجال الأمن السيبراني[2].

ملخص الفصل الأول

في ظل التطور التكنولوجي المتسارع الذي يشهده العالم اليوم، برز الأمن السيبراني كعامل مؤثر وحاسم في صياغة العلاقات الدولية، سواء على المستوى الاقتصادي أو السياسي. فقد أصبحت التهديدات السيبرانية تشكل خطرًا متزايدًا يهدد استقرار الدول ومصالحها الحيوية، مما أفرز تداعيات متعددة تتجاوز الجوانب التقنية لتلامس جوهر التفاعلات الدولية. وانطلاقًا من هذه الأهمية، يتناول هذا الفصل بالتحليل محورين أساسيين :يتناول المبحث الأول أبرز التداعيات السلبية للأمن السيبراني في المجال الاقتصادي، من خلال إبراز كيف تؤثر الهجمات السيبرانية على البنى التحتية الاقتصادية، وعلى بيئة الاستثمار والتجارة العالمية، وما تخلفه من خسائر مادية ومعنوية تمس الثقة في الاقتصاد الرقمي .أما المبحث الثاني، فيسلط الضوء على الانعكاسات السياسية للأمن السيبراني، من حيث دوره في زعزعة استقرار العلاقات بين الدول، وتأجيج الصراعات الرقمية، واستعماله كأداة للضغط أو التدخل في الشؤون الداخلية لدول أخرى، مما يهدد السيادة الوطنية ويعيد رسم خرائط التحالفات الدولية في عصر التقنية والمعلومات.

[1] محمد سعيد الإدريسي ؛**الجرائم الإلكترونية وأثرها على كفاءة التجارة الدولية**دار الإبداع الأكاديمي، القاهرة، 2023
[2] أسماء العلوي«**الحروب السيبرانية والتحديات الاقتصادية العالمية**» مجلة الأمن الرقمي العربي، العدد 8، 2024

الفصل الثاني

تحديات إدارة الامن السيبيراني وسبل مواجتها في مجال العلاقات الدولية

شهد العالم في العقود الأخيرة تحولات متسارعة في مجال التكنولوجيا والاتصالات، ما أدى إلى بروز الفضاء السيبراني كأحد الميادين الحيوية الجديدة التي أصبحت تمس مختلف مجالات الحياة، بما في ذلك العلاقات الدولية. ومع تزايد الاعتماد على الأنظمة الرقمية والبنى التحتية المعلوماتية، برزت إشكاليات أمنية معقدة باتت تشكّل تهديدًا مباشرًا على الأمن القومي للدول، وسلامة المؤسسات، واستقرار النظام الدولي ككل.

في هذا السياق، أصبح الأمن السيبراني من أولويات السياسات الدولية، حيث أضحت الهجمات السيبرانية أحد أخطر التحديات العابرة للحدود، نظرًا لقدرتها على التسلل إلى البنى الاستراتيجية، والتأثير على العمليات السياسية والاقتصادية، بل وحتى تهديد الأمن المجتمعي. وقد تجلت خطورة هذه التهديدات في عدد من الحوادث السيبرانية الكبرى التي طالت دولًا ومنظمات دولية، وأسهمت في تعميق التوترات بين الفاعلين الدوليين.

وبالرغم من إدراك الدول لأهمية إدارة الأمن السيبراني، إلا أن التعامل مع هذه التحديات لا يزال يواجه عراقيل متعددة، تتراوح بين الفجوات التقنية، وغياب الأطر القانونية الدولية الملزمة، وضعف التنسيق بين الدول، وتباين القدرات السيبرانية بين الشمال والجنوب. الأمر الذي يستدعي البحث في السبل الكفيلة بمواجهة هذه التحديات، سواء من خلال تطوير السياسات الوطنية، أو تعزيز التعاون الدولي، أو إرساء قواعد حوكمة فعالة للفضاء السيبراني.

وانطلاقًا من هذه الإشكالية، يتناول هذا البحث التحديات الرئيسية التي تواجه إدارة الأمن السيبراني في المجال الدولي، كما يسعى إلى استكشاف الاستراتيجيات والآليات المقترحة لمواجهتها، في ظل تعقيد البيئة الرقمية وتشابك المصالح الدولية.

المبحث الأول

تحديات إدارة الامن السيبراني في مجال العلاقات الدولية

يشهد العالم اليوم تحولات جذرية في طبيعة الاقتصاد العالمي نتيجة الاعتماد المتزايد على التكنولوجيات الرقمية والأنظمة المعلوماتية، مما جعل الفضاء السيبراني مكونًا حيويًا في دورة الحياة الاقتصادية. غير أن هذا الاعتماد الكبير صاحبه تصاعد في حجم التهديدات السيبرانية، التي باتت تشكل خطرًا مباشرًا على استقرار المعاملات الاقتصادية وأمن المؤسسات والشركات والدول.

المطلب الأول

التحديات الاقتصادية والتقنية

يشهد الاقتصاد العالمي تحولًا كبيرًا بسبب الاعتماد على التكنولوجيات الرقمية والأنظمة المعلوماتية، مما جعل الفضاء السيبراني جزءًا أساسيًا من المعاملات الاقتصادية. لكن هذا الاعتماد صاحبه زيادة في التهديدات السيبرانية التي تهدد استقرار المعاملات وأمن المؤسسات. لمواجهة هذه التهديدات، أصبحت الحاجة ملحة لتطوير استراتيجيات فعالة تشمل الحلول التقنية مثل التشفير والذكاء الاصطناعي، بالإضافة إلى تعزيز الوعي الأمني من خلال التعليم والتدريب، ووضع السياسات الأمنية على المستويين الوطني والدولي لضمان حماية الاقتصاد الرقمي.

الفرع الأول

التحديات الاقتصادية

تتمثل التحديات الاقتصادية للأمن السيبراني في التكاليف الباهظة الناتجة عن الهجمات الإلكترونية، مثل خسارة البيانات وتعطيل الأنظمة والإضرار بالثقة في الأسواق، مما يؤثر على ميزانيات الدول ويزيد من أعبائها في مجال الحماية الرقمية، خاصة في الدول النامية.

أولا –تحديات التكاليف والتمويل

إن التحديات الاقتصادية المتعلقة بالتكاليف والتمويل تمثل من أبرز القضايا التي تواجه الدول في العالم المعاصر، سواء كانت دولًا متقدمة أو نامية.

وهذه التحديات لا تقتصر على قضايا تمويل المشاريع التنموية، بل تمتد لتشمل القدرة على تحمل أعباء القروض، وإدارة الإنفاق العام، بالإضافة إلى التأثيرات العالمية التي قد تتسبب في زيادات غير متوقعة في التكاليف.

في هذا السياق، سنتناول هذه التحديات بشكل موسع في عدة محاور مهمة

1-ارتفاع الإنفاق الاستثماري

يشهد العالم في السنوات الأخيرة تزايدًا في حجم الإنفاق الاستثماري على مشروعات التنمية الكبرى، حيث تولي الحكومات اهتمامًا خاصًا ببناء البنية التحتية وتعزيز القطاعات الاقتصادية الحيوية مثل التعليم والصحة والطاقة.

لكن هذا الإنفاق يترافق مع مجموعة من التحديات :

ا-زيادة تكاليف الإنفاق بسبب التضخم:في السياق الاقتصادي العالمي المعاصر، تشهد العديد من الاقتصادات الكبرى معدلات تضخم مرتفعة تؤثر بشكل مباشر على تكاليف الإنفاق الاستثماري. على سبيل المثال، في مشروعات البناء الكبرى مثل الطرق السريعة، السكك الحديدية، أو محطات الطاقة، يؤدي التضخم إلى زيادة أسعار المواد الأساسية مثل الأسمنت، الحديد، وغيرها من المواد الأولية، مما يجعل التكاليف ترتفع بسرعة[1]

ب-تحديات تمويل المشروعات من خلال الاقتراض :تزداد مشكلة تمويل المشروعات الاستثمارية في الدول التي تعتمد بشكل كبير على الاقتراض سواء من أسواق المال المحلية أو الدولية. فالتوسع في الاقتراض يؤدي إلى زيادة في الديون العامة، مما يعزز من خطر العجز المالي. في حالات الأزمات

[1]عباسي، محمد؛**التحديات الاقتصادية في العالم المعاصر :التكاليف والتمويل.** الاقتصاد الدولي, 2020ص 43

الاقتصادية، يصبح الوصول إلى التمويل أكثر صعوبة، وتجد الحكومات نفسها مجبرة على إعادة جدولة الديون أو اللجوء إلى تمويلات بأسعار فائدة مرتفعة .

ج-[1]ضغط التمويل على الميزانيات الحكومية:في حال كانت مشاريع الإنفاق الاستثماري بحاجة إلى أموال ضخمة، يؤدي ذلك إلى زيادة الضغط على الميزانيات الحكومية. وفي العديد من الحالات، قد يتطلب الأمر تقليص الإنفاق في القطاعات الأخرى مثل التعليم أو الصحة من أجل تمويل المشروعات الأساسية، مما يؤثر سلبًا على رفاهية المواطنين[2] .

2-**تفاوت القدرات المالية بين الدول** واحدة من أكبر التحديات الاقتصادية التي تواجه العالم هي التفاوت الكبير في القدرات المالية بين الدول. الدول المتقدمة تتمتع بقدرة مالية هائلة تمكنها من تمويل مشاريعها التنموية بسهولة، بينما تواجه الدول النامية تحديات كبيرة في جمع التمويل المحلي والدولي. هذا التفاوت يعكس نفسه بشكل كبير في قدرات الدول على مواجهة الأزمات الاقتصادية وتنفيذ الإصلاحات الهيكلية.

ا-الدول المتقدمة وقدرتها على التمويل :الدول المتقدمة مثل الولايات المتحدة، وكندا، والعديد من الدول الأوروبية تتمتع بأنظمة مالية قوية واقتصادات متنوعة تتيح لها القدرة على جمع الأموال بسهولة. تعتمد هذه الدول بشكل كبير على الأسواق المالية الداخلية التي توفر لها سيولة كافية لتمويل المشاريع الكبرى. بالإضافة إلى ذلك، تُعد هذه الدول مستفيدًا رئيسيًا من تدفق الاستثمارات الأجنبية المباشرة التي تدعم نموها الاقتصادي. كما أن التمويل المحلي عبر البنوك التجارية يعتبر جزءًا أساسيًا من النمو الاقتصادي في هذه الدول[3] .

ب-النامية وصعوبة التمويل :في المقابل، تواجه الدول النامية تحديات أكبر في جمع الأموال بسبب الضعف النسبي في أنظمتها المالية. غالبًا ما تعاني هذه الدول من ارتفاع معدلات الفقر، انخفاض العائدات الضريبية، والافتقار إلى بنية تحتية مالية قادرة على جذب الاستثمارات. وبالتالي، تعتمد هذه الدول بشكل كبير على الاقتراض الخارجي، والذي يكون مصحوبًا بشروط معقدة قد تضر باقتصاديات هذه الدول على المدى البعيد. بالإضافة إلى ذلك، قد تكون الدول النامية عرضة للتقلبات الاقتصادية العالمية مثل ارتفاع أسعار الفائدة، مما يزيد من تعقيد وضعها المالي.[4]

---

[1]سامي، فاطمة ،**دور التمويل الدولي في النمو الاقتصادي :التحديات والفرص**. دوريات التنمية الاقتصادية، العدد 32،2019 ص 19-33

[2]عباسي محمد.مرجع سابق ص 123-135.

[3]الجمعية العربية للاقتصاد والتنمية،المصادر المستدامة للتمويل في الدول النامية. دراسات اقتصادية دولية 2018، الجزء الثاني ص 198

[4]الجمعية العربية للاقتصاد والتنمية مرجع سابق ص 220-230

ج-الديون الخارجية وأثرها على الاقتصاد :الديون الخارجية تعد واحدة من أبرز المشاكل التي تواجهها الدول النامية .فالديون تمثل عبئًا كبيرًا على ميزانيات الدول، حيث تخصص الحكومات نسبة كبيرة من ميزانيتها لتسديد فوائد الديون، مما يحد من قدرتها على تخصيص الأموال لتمويل مشاريع تنموية أخرى. هذا العبء المالي يترتب عليه أيضًا تزايد الاعتماد على القروض الخارجية، ما يزيد من حجم الدين العام على مر الزمن[1] .

3-**التحديات في التمويل الدولي في سياق** التمويل الدولي، هناك العديد من التحديات التي قد تؤثر بشكل كبير على قدرة الدول في الحصول على الأموال اللازمة لتنفيذ مشروعاتها التنموية .في حين أن التمويل الدولي يشكل أداة أساسية للنمو الاقتصادي في العديد من الدول، إلا أن هناك العديد من الصعوبات التي يجب التغلب عليها .تقلبات الأسواق المالية العالمية :تعتبر التقلبات المستمرة في الأسواق المالية أحد التحديات الكبرى التي تواجه التمويل الدولي. في فترات الأزمات المالية العالمية، تتراجع سيولة الأسواق، مما يؤدي إلى صعوبة الحصول على تمويل بشروط ميسرة. أيضًا، تؤدي التقلبات في أسعار الفائدة إلى زيادة تكلفة الاقتراض، مما يجعل من الصعب على الدول التخطيط المالي بعيد المدى[2].

.ا-**المخاطر السياسية في التمويل الدولي:**يتعرض التمويل الدولي للمخاطر السياسية التي قد تؤدي إلى توقف المشروعات أو خسائر مالية كبيرة. من هذه المخاطر التغيرات في الحكومات، السياسات الاقتصادية الجديدة التي قد تفرضها الحكومات المحلية، إضافة إلى الحروب والنزاعات السياسية التي تؤثر على استقرار الاقتصاد.

ب-**الدول التي تواجه عدم استقرار سياسي** قد تجد صعوبة كبيرة في جذب الاستثمارات الأجنبية المباشرة أو الحصول على تمويل دولي[3] .

ج-**البحث عن حلول تمويلية مستدامة** من أجل تجاوز هذه التحديات، يجب على الحكومات والمؤسسات المالية أن تبحث عن حلول تمويلية مستدامة وطويلة الأجل. ويمكن تلخيص بعض هذه الحلول في النقاط التالية :تنويع مصادر التمويل :يجب على الدول السعي لتنويع مصادر تمويل مشاريعها، من خلال التنويع بين التمويل المحلي، التمويل الدولي، والتوجه نحو أدوات مالية مبتكرة مثل السندات الخضراء. هذا التنويع يقلل من المخاطر المترتبة على الاعتماد على مصدر تمويل واحد. كما يمكن للدول النامية

[1] سامي، فاطمة ,مرجع سابق ص 219
[2] عبلسي، محمد. مرجع سابق ص 45
[3] الجمعية العربية للاقتصاد والتنمية. مرجع سابق ص 50-65

الاستفادة من التمويل الرقمي، مثل القروض الجماعية أو التمويل عبر العملات الرقمية، والتي بدأت تنمو بشكل سريع في السنوات الأخيرة[1]

.**د-تعزيز الشراكات بين القطاعين العام والخاص** :من خلال تعزيز الشراكات بين القطاعين العام والخاص، يمكن تقليل العبء المالي على الحكومات وتحقيق أقصى استفادة من الموارد المتاحة. هذه الشراكات توفر أيضًا فرصًا للقطاع الخاص للمساهمة في تمويل مشروعات حيوية، مثل البنية التحتية والمشاريع البيئية[2]

ثانيا-لتحديات التجارة الإلكترونية

تواجه التجارة الإلكترونية تحديات متعددة تمس الجوانب التقنية والمالية والتنظيمية، مما يؤثر على أدائها واستدامتها. وهذه التحديات تتطلب من المؤسسات مرونة كبيرة واستثمارات مستمرة لتجاوزها. نعرض فيما يلي أبرز هذه التحديات

ا-تكاليف الامتثال المتزايدة تُعد الالتزامات القانونية والتنظيمية أحد أكبر العوائق التي تواجه التجارة الإلكترونية في العصر الحديث. مع تنامي النشاط الرقمي عبر الحدود، أصبح لزامًا على الشركات أن تواكب تشريعات مختلفة في كل دولة تعمل فيها .على سبيل المثال، تختلف قوانين الضرائب الرقمية من دولة لأخرى؛ فبعضها يفرض ضرائب على القيمة المضافة، بينما تفرض دول أخرى ضرائب على أرباح المنصات الأجنبية. وهذا يُجبر الشركات على توظيف مختصين في الضرائب الدولية، أو شراء برمجيات محاسبية متطورة لمواكبة هذه الفروقات .كما تفرض تشريعات حماية البيانات (مثل اللائحة العامة لحماية البيانات GDPR في الاتحاد الأوروبي) التزامات معقدة، تتضمن الحصول على موافقة المستخدمين، وتخزين بياناتهم بطرق آمنة، وإبلاغهم في حالة حدوث خرق أمني .ويتطلب ذلك فرقًا متخصصة في أمن المعلومات، مع تكاليف إضافية في البنية التحتية السحابية وبرامج التشفير .من جهة أخرى، يجب على المؤسسات الامتثال لقوانين التجارة العادلة التي تلزمها بالشفافية في الإعلانات، وضمان جودة المنتجات، وإتاحة سياسات استرجاع واضحة للمستهلكين. كل هذه المتطلبات تؤدي إلى ارتفاع التكاليف القانونية والتقنية واللوجستية للشركات[3] .

ب-. مخاطر سلسلة التوريد تتسم سلاسل التوريد في التجارة الإلكترونية بتعدد المراحل وتعدد الجهات الفاعلة، مما يجعلها عرضة لمخاطر داخلية وخارجية. فالشركات تعتمد غالبًا على موردين وموزعين

[1] الجمعية العربية للاقتصاد والتنمية.مرجع سابق ص 218

[2] عباسي محمدمرجع سابق ص 123-135.

[3] زينب، سارة؛التحديات الضريبية في التجارة الإلكترونية: دراسة تطبيقية,2021 ,ص 29

في بلدان مختلفة، مما يعقد عمليات التنسيق والمراقبة .أحد المخاطر الأساسية هو ضعف التكامل بين أنظمة الموردين، حيث تختلف أدوات تتبع الشحنات والفوترة والتخزين من طرف لآخر، مما يؤدي إلى تضارب البيانات وتأخير في التسليم .كما أن أزمات الشحن العالمية مثل جائحة كوفيد-19 أو النزاعات الجيوسياسية قد تؤدي إلى توقف أو تباطؤ حركة السلع، مما يؤثر على الوفرة في السوق ويُحدث ضغطًا على علاقات العملاء .بالإضافة إلى ذلك، فإن التكاليف المرتفعة للنقل والتخزين، خاصة في ظل تقلب أسعار الوقود ورسوم الجمارك، تؤثر على هوامش الربح. وقد يُجبر ذلك الشركات على رفع الأسعار أو تقليص خدمات التوصيل المجاني .أيضًا، تُمثل المخاطر الجيوسياسية مثل الحرب التجارية بين الولايات المتحدة والصين تهديدًا مباشرًا لاستيراد المكونات الإلكترونية، ما قد يؤدي إلى بطء الإنتاج، أو توقف بعض المنصات عن خدمة مناطق معينة[1] .

ثالثا -تحديات الاستثمار الأجنبي

يُعد الاستثمار الأجنبي عنصرًا بالغ الأهمية لدفع عجلة التجارة الإلكترونية، فهو يُسهم في إدخال رؤوس الأموال، ونقل التكنولوجيا، وخلق فرص العمل. غير أن هذا النوع من الاستثمار يواجه العديد من التحديات التي تُقلّص من قدرته على تحقيق أهدافه التنموية، وتؤثر على مدى جاذبية الدول، خصوصًا النامية منها، لاستقطاب الشركات متعددة الجنسيات. وفيما يلي التحديات الرئيسة بالتفصيل:

1-**تجزئة الأسواق التكنولوجية** تتمثل هذه المشكلة في غياب توحيد المعايير التقنية والتشريعية بين الدول، مما يُعيق الاستثمار الأجنبي في التجارة الإلكترونية. فالشركات العابرة للحدود تضطر إلى تعديل أنظمتها الداخلية وخدماتها لتتماشى مع كل سوق، ما يزيد من التكاليف التشغيلية ويقلّل من الكفاءة .مثال: شركة عالمية مثل "أمازون" قد تجد نفسها مطالَبة بتعديل بوابة الدفع الخاصة بها لتتوافق مع أنظمة دفع محلية، أو تقيد تقديم بعض خدماتها مثل "Amazon Prime"في بعض الدول التي لا تسمح ببث المحتوى الرقمي الأجنبي .يُضاف إلى ذلك الحظر المفروض على بعض التطبيقات والمنصات في دول معينة، مما يمنع المستثمرين من العمل بحرية، مثل حظر "بايبال" في بعض الدول العربية، أو تقييد عمل "علي بابا" في أسواق غربية .كما أن بعض الحكومات تفرض قوانين صارمة لحوكمة البيانات، مثل اشتراط حفظ بيانات المستخدمين محليًا، وهو ما يجبر الشركات على إنشاء مراكز بيانات وطنية مكلفة

[1] المنصور، أحمد؛**أثر تقلبات أسعار الشحن على التجارة الإلكترونية**،2021ص 31

2-. **بيئة تنظيمية غير مستقرة**: أحد أبرز عوائق الاستثمار الأجنبي هو عدم استقرار الأطر القانونية والتنظيمية. فالتعديلات المفاجئة على قوانين التجارة الإلكترونية، الضرائب، شروط الملكية الأجنبية، أو الجمارك الإلكترونية، تُربك خطط المستثمرين وتُفقدهم الثقة في السوق.مثال: في عام 2020، فرضت الهند قيودًا جديدة على الاستثمارات الأجنبية من الصين، ما أدى إلى انسحاب العديد من الشركات الرقمية الصينية. كما أن بعض الدول تضع سقوفًا للملكية الأجنبية في شركات التكنولوجيا، مما يُجبر المستثمر الأجنبي على الدخول في شراكات قد لا تكون مربحة. إضافة إلى ذلك، عدم وجود آليات مستقرة لحل النزاعات، أو تأخر إصدار الرخص الرقمية، يجعل بيئة الاستثمار غير جاذبة، خاصة عندما يكون المستثمر مضطرًا للانتظار عدة أشهر لتسجيل شركته أو تفعيل أنظمة الدفع

3-**ضعف البنية التحتية الرقمية واللوجستية** تُعد البنية التحتية الرقمية واللوجستية الأساس الذي تُبنى عليه التجارة الإلكترونية. إلا أن العديد من الدول النامية تعاني من تردي جودة الإنترنت، ضعف مراكز البيانات، غياب خدمات التخزين السحابي المحلية، وبطء خدمات البريد والتوصيل. هذه الفجوات تجعل من الصعب على المستثمرين بناء نماذج عمل فعالة في هذه الأسواق. فمثلًا، إذا كانت سرعات الإنترنت منخفضة، فإن المستخدم سيواجه صعوبات في تصفح الموقع أو تحميل التطبيقات، مما يؤثر على رضا العملاء ومعدل التحويل .في الجانب اللوجستي، قلة شركات الشحن المتخصصة بالتجارة الإلكترونية، وغياب العنونة الدقيقة للأحياء، يجعل من التوصيل عملية مكلفة وبطيئة، وهو ما لا يتماشى مع معايير الشركات العالمية التي تعتمد على خدمات التوصيل السريع والدقيق

4-**انعدام الحماية القانونية وضعف الثقة المؤسسية**غالبًا ما تواجه الشركات الأجنبية عقبات قانونية تتعلق بغياب تشريعات واضحة في مجال التجارة الإلكترونية. فبعض الدول لا تزال تُجرم المعاملات الرقمية أو لا تعترف قانونيًا بالتوقيع الإلكتروني .كما أن غياب قوانين لحماية حقوق الملكية الفكرية الرقمية يجعل المستثمرين عرضة للقرصنة أو النسخ غير المشروع لمنتجاتهم. مثال: في بعض الدول، قد يتم تقليد موقع إلكتروني لشركة أجنبية وتقديم خدمات باسمها دون إمكانية فعالة لملاحقة الفاعلين قانونيًا .أما على صعيد الثقة المؤسسية، فغالبًا ما يعاني المستثمر

الأجنبي من البيروقراطية، الفساد الإداري، والمحسوبية، ما يجعل الاستثمار مغامرة غير مضمونة العواقب[1].

رابعا- تحديات الموارد البشرية

يُعد العنصر البشري من الركائز الأساسية في قطاع التجارة الإلكترونية، كونه المحرك الرئيسي لعمليات التطوير، التسيير، والصيانة التقنية، وخدمة العملاء. لكن بالرغم من التقدم التكنولوجي، لا تزال الموارد البشرية تُشكل أحد أهم التحديات التي تُواجه هذا القطاع، خصوصًا في الدول النامية. وفيما يلي تفصيل لأبرز هذه التحديات:

1-**الفجوة العالمية في المهارات الرقمية** تعتبر الفجوة الرقمية في المهارات أحد التحديات الجوهرية التي يواجهها قطاع التجارة الإلكترونية، إذ تمثل حاجزًا كبيرًا أمام التوسع والنمو السريع في هذا المجال. في الوقت الذي يشهد فيه قطاع التجارة الإلكترونية نموًا متسارعًا على مستوى العالم، فإن وجود فجوة واسعة في المهارات الرقمية على مستوى العمالة يشكل تهديدًا حقيقيًا لتنفيذ استراتيجيات ناجحة. يمكن تحديد هذا التحدي في عدة أبعاد

ا-الفرق بين الدول المتقدمة والدول النامية:الدول المتقدمة، مثل الولايات المتحدة ودول الاتحاد الأوروبي، قد تمكنت من توجيه استثمارات ضخمة في تدريب وتعليم القوى العاملة في مجالات التكنولوجيا الحديثة، مثل التسويق الرقمي، البرمجة، تحليل البيانات، و الذكاء الاصطناعي. بينما في الدول النامية، لا تزال التحديات الاقتصادية والبنية التحتية التعليمية تشكل عائقًا أمام تدريب القوى العاملة على استخدام الأدوات التكنولوجية الحديثة .ففي دول مثل الهند والصين، رغم أن هناك تقدمًا ملحوظًا في مجالات التدريب على التجارة الإلكترونية، فإن الفجوة تبقى كبيرة مقارنةً بالدول الغربية، حيث يتم تدريب الجيل الجديد على المهارات التقنية بشكل مبكر جدًا .

ب-محدودية فرص التعليم الرقمي المتخصص:يعد التعليم الرقمي المتخصص أحد الركائز الأساسية لتطوير الكوادر البشرية في مجال التجارة الإلكترونية. إلا أن العديد من الدول النامية لا توفر برامج تعليمية متخصصة أو تدريبية في تقنيات التجارة الإلكترونية الحديثة. كما أن الجامعات والمعاهد التعليمية في هذه الدول تفتقر إلى برامج محدثة تواكب التغيرات السريعة في هذا المجال .حتى في الدول التي توفر بعض البرامج الرقمية، تظل جودة التعليم منخفضة بسبب نقص الإمكانيات، مما يؤدي إلى

[1] زينبسارة.مرجع سابق ص 29

تخريج طلاب لا يمتلكون المهارات الكافية لدخول السوق الرقمي، سواء من حيث إدارة المنصات الإلكترونية، أو استخدام أدوات التحليل المتقدم .

ج-تأثير هذا على الشركات الصغيرة والمتوسطة:من أكبر تداعيات الفجوة الرقمية هو تأثيرها المباشر على الشركات الصغيرة والمتوسطة(SMEs) ، التي لا تستطيع منافسة الشركات الكبرى التي تمتلك فرقًا مؤهلة من المتخصصين في التجارة الإلكترونية. هذه الشركات غالبًا ما تعتمد على استراتيجيات تقليدية في التسويق أو البيع، مما يُقلل من قدرتها على الاستفادة من تقنيات مثل الذكاء الاصطناعي، التحليلات البيانية، والتسويق الرقمي المدعوم بالبيانات .إن الشركات الصغيرة والمتوسطة التي لا تواكب التحول الرقمي تجد نفسها غير قادرة على تنفيذ استراتيجيات تجارة إلكترونية مبتكرة، كما يواجه موظفوها صعوبة في إدارة العمليات التقنية بشكل فعال، مما يؤثر في النهاية على القدرة التنافسية للمؤسسة في السوق .ارتفاع الطلب على المهارات المتقدمة :من الملاحظ أن العديد من الشركات العالمية تسعى بشكل متزايد للحصول على مهارات متقدمة في مجالات التحليلات الرقمية، الأتمتة، التجارة عبر الأجهزة المحمولة، والأمن السيبراني، وهي مجالات تفتقر إلى عدد كبير من المحترفين في الأسواق النامية. وبالتالي، تظهر منافسة شديدة على توظيف المهارات المتقدمة، مما يجعل الشركات المحلية في هذه الدول غير قادرة على توظيف هذه المهارات المتخصصة

2-أزمة "هجرة العقول :"في الأسواق النامية، تعتبر هجرة العقول الرقمية من أكبر التحديات. الشباب المؤهلون في مجالات التكنولوجيا الحديثة غالبًا ما يبحثون عن فرص في الدول المتقدمة التي تقدم لهم بيئة تقنية متقدمة وأجورًا مغرية. هذه الهجرة تؤدي إلى نقص حاد في المواهب الرقمية في الدول النامية، مما يعيق قدرة هذه البلدان على المنافسة في سوق التجارة الإلكترونية العالمي

3-الآثار السلبية للفجوة في المهارات:بطء التوسع في التجارة الإلكترونية: المؤسسات التي تفتقر إلى الكفاءات الرقمية تجد صعوبة في التوسع السريع والابتكار .ارتفاع التكاليف: الاعتماد على فرق خارجية لتنفيذ المهام التقنية يؤدي إلى زيادة التكاليف التشغيلية .تأثير على تجربة العملاء:

نقص المهارات التقنية يؤدي إلى ضعف القدرة على تحسين تجارب المستخدمين، مما يؤثر على مستوى رضا العملاء[1] .

[1]العربيمنير مرجع سابق ص92–95.

4-نقص برامج التدريب والتكوين المتخصص تُعد برامج التدريب والتكوين المتخصص حجر الزاوية لتطوير المهارات اللازمة في مجال التجارة الإلكترونية، إذ تساهم بشكل رئيسي في تمكين الأفراد من التعامل مع التقنيات الحديثة واحتياجات السوق المتزايدة. ورغم الأهمية الكبيرة لهذه البرامج، إلا أنها ما زالت تواجه العديد من التحديات التي تقف عائقًا أمام تحقيق أقصى استفادة منها في العديد من الدول النامية. هذه التحديات تشمل الفجوة بين المهارات المكتسبة في البرامج الأكاديمية والاحتياجات الفعلية في السوق، فضلاً عن تطور التكنولوجيا بشكل يفوق سرعة البرامج التدريبية المتاحة.في هذا السياق، تتعدد الأسباب التي تساهم في نقص برامج التدريب المتخصص في التجارة الإلكترونية، وفيما يلي بعض أبرز تلك الأسباب :عدم توافق البرامج التدريبية مع المتطلبات العملية :على الرغم من وجود عدد من برامج التدريب، إلا أن معظمها يظل نظريًا أو محدودًا في نطاق المهارات الأساسية فقط، مثل التسويق عبر الإنترنت أو التصميم على المنصات. ومع تزايد الحاجة إلى مهارات تقنية متقدمة، مثل تحليل البيانات الضخمة، تقنيات الذكاء الاصطناعي، أمن المعلومات، والتفاعل مع أنظمة التجارة الإلكترونية المتقدمة، تبقى برامج التدريب التقليدية غير قادرة على تلبية هذه المتطلبات. إن الفجوة بين ما يُدرّس في الجامعات والمعاهد من جهة، وما يحتاجه سوق العمل الرقمي من جهة أخرى، تجعل الخريجين غير قادرين على تلبية احتياجات الشركات أو التكيف مع بيئة العمل المتغيرة[1].

نقص التدريب المستمر والتحديث الدوري للمهارات :في مجالات التجارة الإلكترونية، لا تقتصر الحاجة على تعلم المهارات في بداية المشوار المهني، بل على الاستمرار في تطوير هذه المهارات بشكل دوري لمواكبة تطورات التكنولوجيا المتسارعة. لكن في العديد من الدول النامية، لا تتوفر برامج تدريبية مستمرة، ما يؤدي إلى توقف العاملين عن تحديث مهاراتهم بعد اكتسابهم الخبرات الأولى. بهذا الشكل، تفقد الشركات جزءًا من قدرتها على الابتكار والمنافسة. التغييرات المستمرة في اللوائح، أساليب التسويق، وتحسين تجربة المستخدم، تتطلب من العاملين أن يظلوا على دراية بالتحديثات بشكل دائم، وهو ما يعجز العديد من البرامج التدريبية عن تقديمه

التدريب والتأهيل غير الكافي :بالرغم من أهمية تدريب فرق خدمة العملاء على التعامل مع الاستفسارات الرقمية واحتياجات العملاء عبر الإنترنت، فإن معظم الشركات لا تُخصص موارد كافية لتدريب موظفيها في هذا المجال. بالإضافة إلى ذلك، فإن البرامج التدريبية التي تُقدم في بعض الحالات لا تكون مُحدثة بما يتناسب مع التقنيات الحديثة مثل الذكاء الاصطناعي، أنظمة الدعم الآلي، أو أدوات

[1] العربي منير. مرجع سابق ، ص91–108

تحليل البيانات المتعلقة بتجربة العملاء. وهذا يؤدي إلى حالة من الارتباك لدى العاملين في هذه الأقسام، مما يُعطل قدرتهم على توفير خدمة عالية الجودة

5-القصور في التخصصات الحديثة:تعد التجارة الإلكترونية ميدانًا دائم التغيير، حيث تظهر تقنيات جديدة بشكل مستمر، مثل الذكاء الاصطناعي، الحوسبة السحابية، والبلوكشين. ومع ذلك، فإن معظم برامج التدريب الموجودة في الدول النامية تفتقر إلى التخصصات المرتبطة بهذه التقنيات الحديثة. في العديد من المؤسسات التعليمية، يتم تعليم الطلاب بعض المهارات الأساسية، مثل كيفية استخدام بعض المنصات أو التطبيقات التجارية، دون أن يشمل ذلك المفاهيم الأكثر تخصصًا والمتطورة مثل "التسويق الذكي" أو "إدارة البيانات في الزمن الحقيقي". وهذا يعرض العاملين إلى صعوبة في التكيف مع التحولات السريعة في القطاع

ا-التكاليف المرتفعة والصلات المحدودة بالمناطق الريفية :من بين التحديات التي تواجهها برامج التدريب في التجارة الإلكترونية، نجد أيضًا تكاليف التدريب المرتفعة التي قد تكون عائقًا أمام الأفراد أو الشركات الصغيرة والمتوسطة التي لا تملك الميزانية الكافية للاستثمار في برامج تدريب متخصصة. بالإضافة إلى ذلك، يعاني العديد من الموظفين في المناطق الريفية أو غير الحضرية من صعوبة الوصول إلى هذه البرامج بسبب قلة المراكز التدريبية المتخصصة في هذه المناطق أو ارتفاع تكاليف السفر للمشاركة في الدورات التدريبية. وهذا يؤدي إلى تقليص الفرص أمام فئات كبيرة من الشباب والعمال في هذه المناطق لتطوير مهاراتهم

.6-الدور المحدود للتعليم الأكاديمي في التكوين المتخصص :في العديد من البلدان، تُركز الجامعات على تقديم برامج تعليمية أساسية ولا تتضمن التقنيات الحديثة التي تتطلبها التجارة الإلكترونية. نتيجة لذلك، يتخرج الطلاب مع مجموعة من المعارف العامة التي لا تتماشى مع احتياجات السوق الرقمي. علاوة على ذلك، تفتقر المؤسسات التعليمية إلى شراكات قوية مع الشركات أو الهيئات الصناعية، مما يحد من قدرة الجامعات على تصميم برامج أكاديمية ومهنية تُلبي متطلبات سوق العمل. كما أن جزءًا كبيرًا من المناهج الدراسية يكون قديمًا وغير ملائم لمواكبة تطورات الصناعة[1] .

7-مستوى الوعي والتفاعل مع صناعة التجارة الإلكترونية :إن العديد من المؤسسات والأفراد قد لا يدركون تمامًا حجم التغيرات التي فرضتها التجارة الإلكترونية على الاقتصاد الرقمي. كما أن هناك

[1]العربي، منير مرجع سابق ، ص91–108

بعض المقاومات للتحول الرقمي في الشركات التقليدية التي لا تشجع على تدريب الموظفين أو استثمار الوقت والمال في تطوير المهارات الرقمية. في بعض الأحيان، يُعتبر التدريب على التجارة الإلكترونية مجرد "تدريب إضافي"، ولا يُنظر إليه على أنه استثمار حقيقي في تطور الشركات والموظفين

8-. **نقص الكفاءات في خدمة العملاء الرقمية** تُعتبر خدمة العملاء الرقمية أحد العوامل الرئيسية التي تحدد نجاح أو فشل أي مؤسسة تجارية إلكترونية، حيث تلعب هذه الخدمة دورًا مهمًا في تعزيز تجربة المستخدم، وبناء الولاء للعلامة التجارية، وزيادة رضا العملاء. ومع ذلك، فإن الكثير من الشركات تواجه صعوبة في توفير كفاءات مدربة بشكل جيد في هذا المجال، الأمر الذي يُعرقل فعالية العمليات ويؤثر بشكل سلبي على سمعة الشركات في السوق. هذه المشكلة تتفاقم بشكل خاص في الدول النامية، حيث يتطلب الأمر اهتمامًا بالغًا لتطوير هذه الكفاءات والتغلب على التحديات المرتبطة بها .نقص المهارات المتخصصة في خدمة العملاء الرقمية :أحد أبرز التحديات التي تواجه العديد من الشركات في الدول النامية هو نقص المهارات المتخصصة في خدمة العملاء الرقمية. في حين أن العديد من الموظفين في أقسام خدمة العملاء قد يمتلكون مهارات تقليدية في التعامل مع العملاء شخصيًا أو عبر الهاتف، إلا أنهم يفتقرون إلى المعرفة التقنية اللازمة للتفاعل مع العملاء عبر منصات الدردشة الرقمية، البريد الإلكتروني، أو شبكات التواصل الاجتماعي. هذه التقنيات تتطلب مهارات متقدمة في إدارة التفاعل الرقمي، تحليل سلوك العملاء، واستخدام أنظمة إدارة علاقات العملاء (CRM) الرقمية بفعالية

9-**نقص الكفاءات في خدمة العملاء الرقمية** تُعد خدمة العملاء الرقمية من العوامل الأساسية التي تساهم في تعزيز نجاح الشركات في عالم التجارة الإلكترونية، حيث أن تفاعل العملاء مع الشركة وتلبية احتياجاتهم بشكل فعال يعكس صورة المؤسسة أمام الجمهور. في ظل التحول الرقمي، أصبحت الخدمة عبر الإنترنت، سواء من خلال البريد الإلكتروني أو المحادثات الفورية، أو حتى عبر منصات التواصل الاجتماعي، ضرورة لا غنى عنها. ومع ذلك، لا تزال العديد من الشركات تواجه تحديات كبيرة في توفير كفاءات قادرة على إدارة هذه الخدمات بطريقة مهنية وفعالة. هذا النقص في الكفاءات المتخصصة في خدمة العملاء الرقمية يؤدي إلى ضعف في التواصل مع العملاء، وبالتالي ينعكس سلبًا على سمعة الشركات في السوق الرقمي .التحديات الأساسية التي يواجهها قطاع خدمة العملاء الرقمية :نقص التدريب على أدوات التواصل الرقمي المتقدمة تعتبر أدوات التواصل الرقمي من أساسيات خدمة العملاء الحديثة. ففي عالم التجارة الإلكترونية، يتعين على الموظفين أن يكونوا على دراية باستخدام أدوات الدردشة المباشرة، أنظمة إدارة علاقات العملاء(CRM) ، وبرامج الذكاء الاصطناعي الخاصة

بالمساعدة الآلية. وفي العديد من الشركات، لا يتم توفير التدريب الكافي على هذه الأدوات، مما يجعل التواصل مع العملاء غير فعال وأحيانًا يسبب تأخيرات في الاستجابة. كما أن التدريب على هذه الأدوات يكون غالبًا غير مستمر أو محدود في نطاقه، ما يجعل الموظفين غير قادرين على التعامل بكفاءة مع الاستفسارات المعقدة أو الشكاوى المتقدمة

كما ان ضعف الخبرة في إدارة بيانات العملاء وتحليلها التحليلات الدقيقة لبيانات العملاء أصبحت أحد العوامل الجوهرية في نجاح أي عمل تجاري إلكتروني. باستخدام تقنيات مثل الذكاء الاصطناعي وتحليل البيانات الكبيرة(Big Data) ، يمكن للمؤسسات تحديد احتياجات العملاء بشكل أكثر دقة وتقديم حلول مخصصة لهم. ومع ذلك، يواجه العديد من الشركات تحديات في تدريب موظفيهم على كيفية جمع وتحليل البيانات ذات الصلة بشكل مناسب. نقص الكفاءات في هذا المجال يؤدي إلى فقدان فرص هائلة لتحسين تجربة العميل وزيادة ولائه للعلامة التجارية

.**10-الصعوبة في التعامل مع شكاوى العملاء عبر منصات متعددة** في عصر التجارة الإلكترونية، يمتلك العملاء العديد من القنوات الرقمية التي يمكنهم استخدامها للتواصل مع الشركات، مثل البريد الإلكتروني، وسائل التواصل الاجتماعي، المحادثات المباشرة، أو حتى المراجعات عبر الإنترنت. يتطلب الأمر وجود كفاءات قادرة على التنقل بين هذه المنصات بشكل فعال دون التأثير على جودة الخدمة المقدمة. وفي كثير من الأحيان، لا يملك الموظفون الخبرة الكافية للتعامل مع الشكاوى عبر هذه المنصات المتعددة أو تقديم حلول مرضية وسريعة. هذا يؤدي إلى تراكم الشكاوى مما يزيد من درجة الاستياء لدى العملاء ويضر بسمعة الشركة

الافتقار إلى التعامل الاحترافي مع الشكاوى الرقمية :أحد التحديات الأخرى في هذا السياق هو ضعف القدرة على التعامل مع الشكاوى الرقمية أو الحالات المعقدة التي قد تظهر على منصات التواصل الاجتماعي أو المواقع الإلكترونية. في بيئة التجارة الإلكترونية، يُعد التعامل السريع والفعال مع الشكاوى أمرًا بالغ الأهمية للحفاظ على سمعة العلامة التجارية. ولكن الكثير من الموظفين لا يمتلكون التدريب الكافي للتعامل مع هذه الشكاوى بشكل احترافي ومؤثر، مما قد يؤدي إلى زيادة الاستياء لدى العملاء وفقدانهم للثقة في العلامة التجارية

11-**المقاومة الداخلية للتغيير الرقمي في الشركات** من التحديات التي تواجهها العديد من الشركات في تطوير كفاءات خدمة العملاء الرقمية هو مقاومة بعض الموظفين لتبني التقنيات الرقمية الجديدة.

خصوصًا في المؤسسات التقليدية التي لم تدمج التكنولوجيات الحديثة بعد، قد يرفض الموظفون استخدام أدوات الدردشة الرقمية أو منصات التواصل الاجتماعي لخدمة العملاء، ويعتبرونها تهديدًا لوظائفهم. هذه المقاومة للتغيير يمكن أن تبطئ من التحول الرقمي في المؤسسات وتجعل عملية تطبيق الأنظمة الرقمية في خدمة العملاء غير فعالة

12-**التأثير على الولاء والثقة في العلامة التجارية**تُعتبر خدمة العملاء الرقمية هي الواجهة الأولى التي يتفاعل معها العملاء مع الشركات على الإنترنت. عندما تكون هذه الخدمة غير فعالة أو تفتقر إلى الكفاءات المهنية، تتأثر سمعة الشركة بشكل مباشر. العميل الذي لا يحصل على استجابة سريعة أو حل مناسب لمشكلته عبر القنوات الرقمية قد يفقد الثقة في العلامة التجارية ويقرر الانتقال إلى منافس آخر يقدم تجربة أفضل. لذا، فإن نقص الكفاءات في خدمة العملاء الرقمية يؤثر سلبًا على ولاء العملاء وعلى المدى الطويل يؤثر على أرباح الشركة[1] .

الفرع الثاني

التحديات التقنية

تتمثل التحديات التقنية في سرعة تطور أدوات الهجوم الإلكتروني، وتفاوت القدرات التكنولوجية بين الدول، إلى جانب الحاجة المستمرة لتحديث البنية التحتية الرقمية وتطوير الكفاءات الفنية، مما يعرقل جهود بناء دفاعات إلكترونية فعّالة على المستوى الدولي.

أولا -تحديات البنية التحتية الرقمية

تُعتبر البنية التحتية الرقمية من المرتكزات الأساسية لقيام فضاء سيبراني آمن وفعّال، فهي تتكوّن من مجموعة متكاملة من الأنظمة والتقنيات والموارد التي تتيح الاتصال، وتبادل البيانات، وتشغيل المنصات الرقمية والخدمات الإلكترونية. وتشمل هذه البنية: مراكز البيانات، شبكات الاتصالات، الكابلات البحرية، أجهزة الحوسبة، نظم التشغيل، برمجيات الأمان، السيرفرات، الأقمار الصناعية، والمستشعرات الذكية. ورغم التقدم الهائل في المجال الرقمي خلال العقود الأخيرة، فإن البنية التحتية الرقمية لا تزال تواجه تحديات هيكلية وتقنية عميقة تهدد استقرار وأمن الفضاء السيبراني، وتزداد خطورتها مع تعقّد الاعتماد على هذه البنية في كل نواحي الحياة الاقتصادية، والسياسية، والتعليمية، والصحية .

[1]العربي، منير مرجع سابق ، ص91–108

1-**تفاوت القدرات التقنية والبنية التحتية بين الدول** تُبرز الدراسات الحديثة وجود فجوة رقمية متنامية بين الدول المتقدمة والدول النامية. ففي الوقت الذي تبني فيه الدول الصناعية بنى رقمية متطورة، ومحمية جيدًا، ومرتبطة بنظم سيادة رقمية متكاملة، تعاني معظم الدول النامية من هشاشة في الهياكل التحتية الرقمية، ونقص في الكوادر البشرية المؤهلة، فضلاً عن ضعف التمويل الحكومي الموجه لقطاع الأمن السيبراني. هذا التفاوت يُنتج واقعًا مزدوجًا :

الواقع الأول: دول تمتلك سيادة رقمية كاملة، وقدرة على رصد ومعالجة أي تهديد إلكتروني بسرعة وفعالية، وتشارك في وضع المعايير العالمية .الواقع الثاني: دول تعتمد على تقنيات مستوردة، وبنية هشّة، ولا تمتلك الحد الأدنى من الدفاع الرقمي الذاتي، مما يجعلها عرضة للاستغلال، ومواقع انطلاق للهجمات العابرة للقارات .والأخطر من ذلك أن هذا التفاوت يجعل من بعض الدول نقاط ضعف استراتيجية في النظام الرقمي العالمي، بحيث يمكن للمهاجمين استغلال ضعف البنية التحتية في إحدى الدول لشن هجمات على دول أخرى من خلالها، وهو ما يجعل الأمن السيبراني مسألة ذات بعد دولي وجماعي، لا مجرد شأن داخلي.

2-**تعدد وتضارب المنصات والتقنيات** في عالم يزداد تعقيدًا من حيث تقنيات التشغيل، والأجهزة، والأنظمة الرقمية، أصبحت البنية التحتية مكوّنة من عدد هائل من المنصات المختلفة، والتي غالبًا ما تكون من تطوير شركات عالمية كبرى تحت أنظمة تشغيل متباينة (مثلWindows، Linux، IOS، Android)، مما يجعل من التنسيق الأمني مهمة شاقة. هذا التعدد ينتج عنه عدة مشكلات :عدم التوافق (Incompatibility):أي أن الأنظمة لا يمكنها التواصل أو التفاعل بشكل مباشر أو سلس، مما يصعّب تطوير منظومات حماية أو رقابة موحدة .تعدد الثغرات الأمنية: مع كثرة الأنظمة وتنوعها، تزداد احتمالية وجود ثغرات غير مكتشفة أو غير مصححة، وهو ما يُعرف بـ "الثغرات الصفرية" (Zero-day vulnerabilities)التي يستغلها القراصنة بشراسة .صعوبة التحديث الموحد: تحتاج كل منصة إلى صيانة وتحديثات خاصة، ما يعني أن المؤسسات تحتاج إلى فرق متعددة من المتخصصين لإدارة كل نظام على حدة، وهو أمر مكلف ومعقد .تضارب المعايير الأمنية: فكل شركة تستخدم بروتوكولات تشفير، وإدارة هوية، وأدوات تحقق مختلفة، ما يُصعب توحيد الرؤية الأمنية الوطنية أو الدولية .

3-**مركزية البنية التحتية وغياب التوزيع الجغرافي العادل** تتركّز معظم البنية التحتية للإنترنت (مثل الكابلات البحرية ومراكز البيانات العملاقة) في مناطق جغرافية معينة في أمريكا الشمالية وأوروبا، مما يمنح هذه الدول هيمنة تقنية واستراتيجية على حركة البيانات، ويُضعف من قدرة باقي الدول على فرض

سيادتها على فضائها الرقمي. كما أن ذلك يعرض حركة البيانات العابرة للدول للرقابة أو القرصنة، ويزيد من الاعتماد البنيوي على القوى الرقمية الكبرى، بما يخل بالتوازن الدولي في مجال الأمن السيبراني .

4-ضعف آليات الصيانة والطوارئ تتطلب البنية التحتية الرقمية صيانة مستمرة، وتحديثات عاجلة، وخطط طوارئ فعالة في حال حدوث كوارث رقمية مثل الانقطاع أو الاختراق أو التخريب. إلا أن: كثيرًا من المؤسسات لا تمتلك أنظمة نسخ احتياطي فعالة .يوجد غياب واضح لبروتوكولات الطوارئ أوفرق الاستجابة السريعة في دول ومؤسسات عديدة .هناك نقص حاد في التنسيق بين القطاعين العام والخاص، مما يُطيل من زمن الاستجابة للحوادث ويُضاعف الخسائر[1] .

ثانيا -تحديات حماية البيانات تعتبر حماية البيانات من أبرز التحديات التي تواجه الأمن السيبراني في العلاقات الدولية، ويعود ذلك بشكل رئيسي إلى تعدد الأطراف المعنية، وتعقيد التكنولوجيات الحديثة المستخدمة في جمع وتخزين وتحليل البيانات. ومع تزايد التحولات الرقمية في مختلف أنحاء العالم، أصبحت حماية البيانات أمرًا بالغ الأهمية، حيث يُمكن أن تؤثر تسريبات أو اختراقات البيانات بشكل كبير على الأمن السياسي والاقتصادي وحتى الاجتماعي للدول. سنستعرض في هذا السياق أبرز التحديات التي تواجه حماية البيانات من خلال النظر في جوانب متعددة تشمل إدارة البيانات العابرة للحدود، التشفير، التشريعات، الهجمات السيبرانية، والوعي المجتمعي.

1-**إدارة البيانات العابرة للحدود** أصبح التعامل مع البيانات العابرة للحدود أحد التحديات الأساسية في مجال الأمن السيبراني. في الوقت الذي تزداد فيه كمية البيانات المتبادلة عبر الحدود بشكل غير مسبوق، تتعرض الدول لمشكلة حوكمة هذه البيانات عند نقلها أو تخزينها في خوادم خارج أراضيها. إذ لا يمكن للدولة أن تفرض قوانينها الخاصة بحماية البيانات على خوادم تقع في دول أخرى، ما يؤدي إلى فقدان السيطرة على المعلومات الحساسة مثل بيانات المواطنين، المؤسسات المالية، وحتى البيانات العسكرية. علاوة على ذلك، تعاني بعض الدول من مشكلة تفاوت القدرات التقنية في التعامل مع البيانات بشكل آمن، ما يجعلها عرضة للاستغلال من قبل أطراف خارجية، سواء كانت دولًا أو شركات متعددة الجنسيات .على سبيل المثال، من الممكن أن يتم استغلال هذه البيانات لأغراض تجسسية أو تجارية، مما يعرض أمن الدول للخطر .فيما يتعلق بالإجراءات الدولية، على الرغم من وجود اتفاقيات

[1] مصطفى عبد الحميد ؛**الأمن السيبراني كأولوية وطنية في العالم العربي**دار الفكر العربي للنشر والتوزيع القاهرة 2021 ص 121

مثل اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي، إلا أن هناك تفاوتًا كبيرًا في مدى تطبيق هذه التشريعات بين الدول. هذا التفاوت يشكل عقبة أمام التعاون الدولي في حماية البيانات ويسمح بوجود مناطق رمادية حيث تُحفظ البيانات في بيئات غير آمنة

2-**تحديات التشفير وحماية الخصوصية** التشفير يُعد من أدوات الحماية الأساسية التي تعتمد عليها الدول والشركات لضمان سرية المعلومات وحمايتها من الوصول غير المصرح به. إلا أن تقنيات التشفير تواجه تحديات متعددة، أبرزها "أبواب الخلفية" التي تطالب بعض الحكومات بإدخالها إلى أنظمة التشفير لتسهيل الوصول إلى البيانات في حالات معينة، مثل مكافحة الإرهاب. هذا النوع من "التساهل" في تطبيق أساليب التشفير قد يؤدي إلى فتح ثغرات في الأنظمة الأمنية تُستغل لاحقًا من قبل قراصنة أو جهات غير موثوقة. على سبيل المثال، قد تُستخدم تقنيات التشفير ضعيفة أو قديمة من قبل بعض الدول النامية، ما يسهل اختراق البيانات من قبل القراصنة .إضافة إلى ذلك، تتفاوت مستويات التشفير بين الشركات والدول، ما يعكس مشكلة أخرى تتعلق بغياب معايير موحدة على المستوى العالمي. هذا يؤدي إلى حالة من انعدام الأمان النسبي عندما يتم نقل البيانات بين دول أو مؤسسات تستخدم أنظمة تشفير غير متوافقة. وإذا كانت الشركات التي تخزن بيانات المستخدمين تفتقر إلى فهم كافٍ حول كيفية تطبيق سياسات الخصوصية بشكل فعال، فإنها تضع جميع الأطراف في خطر

3-**ضعف التشريعات وعدم نضج الأطر القانونية** على الرغم من الجهود التي بذلتها بعض الدول لتطوير قوانين لحماية البيانات، إلا أن العديد من الدول ما تزال تفتقر إلى تشريعات متكاملة تتعلق بالأمن السيبراني وحماية البيانات. في بعض الأحيان، قد تكون التشريعات المحلية غير قادرة على مواكبة التطورات السريعة في تكنولوجيا المعلومات، ما يسبب فجوات قانونية. علاوة على ذلك، تفتقر العديد من الدول إلى الأطر القانونية اللازمة لمواجهة الجرائم السيبرانية العابرة للحدود، وهو ما يعوق التعاون الدولي في هذا المجال .وتبرز أيضًا مسألة التحديات القانونية في بعض الاتفاقيات الدولية التي تفتقر إلى معايير موحدة تُنظم كيفية معالجة البيانات بين الدول. كما أن الحوكمة العالمية لهذه البيانات تعد قضية صعبة نظرًا لاختلاف القوانين في جميع أنحاء العالم. غياب مثل هذه الأطر الموحدة يُشجع بعض الأطراف على استغلال هذا الضعف في اللوائح القانونية لصالحها، مما يجعل حماية البيانات أكثر تعقيدًا

4-**الاستهداف المباشر للبيانات في الهجمات السيبرانية** تزداد الهجمات السيبرانية تطورًا وتخصيصًا مع مرور الوقت، حيث لم تعد هذه الهجمات تقتصر فقط على تعطيل الأنظمة أو تدمير البنية التحتية، بل

أصبحت تستهدف البيانات بشكل مباشر. يعتمد القراصنة اليوم على تقنيات متقدمة مثل الذكاء الاصطناعي وتحليل البيانات لاختراق الأنظمة وجمع أكبر قدر من المعلومات القيمة. الهجمات على قواعد البيانات الحكومية أو الشركات المالية أصبحت شائعة، حيث يسعى القراصنة إلى سرقة البيانات الشخصية، المالية أو التجارية .تتزايد هذه الهجمات بسبب غياب بعض الأنظمة المتقدمة للحماية في المؤسسات الصغيرة والمتوسطة التي قد لا تمتلك القدرة على تكثيف الدفاعات الإلكترونية بما يكفي للتصدي لهذه الهجمات. مع تقدم التكنولوجيا، أصبح من السهل على المهاجمين استغلال ثغرات في الأنظمة لاستهداف المعلومات الحساسة بشكل سريع ومنظم، مما يجعل من الضروري تحديث أساليب الحماية بشكل مستمر

5-**تحدي الوعي المجتمعي والمؤسسي الوعي بالأمن السيبراني وحماية البيانات** هو العامل المحوري في تعزيز قدرة الأفراد والشركات على التعامل مع التهديدات الأمنية. ورغم الجهود المبذولة، فإن العديد من الأفراد والمؤسسات ما زالوا يجهلون أساليب حماية بياناتهم الشخصية أو المعلومات الخاصة بالشركات. الكثير من الأفراد لا يتخذون تدابير الأمان الأساسية مثل استخدام كلمات مرور معقدة أو تحديث الأنظمة بانتظام .على المستوى المؤسسي، يعاني العديد من الشركات من ضعف التدريب والتوجيه فيما يخص أساليب الحماية، ما يجعلها عرضة للتهديدات. بالإضافة إلى ذلك، لا تلتزم بعض الشركات بتطبيق بروتوكولات حماية البيانات على أكمل وجه، مما يؤدي إلى تسريبات أو اختراقات. لذلك، أصبح من الضروري تنفيذ برامج تدريبية دائمة لتعزيز الوعي داخل المؤسسات والأفراد بشأن أهمية حماية البيانات وكيفية التعامل مع التهديدات[1].

6-**تحديات التنسيق التقني** يواجه التنسيق التقني بين الأنظمة المختلفة تحديات كبيرة في ظل التطورات السريعة والمتنوعة في مجال الأمن السيبراني والتكنولوجيا الرقمية. تتطلب مواجهة هذه التحديات تنسيقًا مستمرًا بين الجهات الفاعلة المختلفة، مثل الحكومات، الشركات، والمنظمات الدولية، حيث أن الفجوة التكنولوجية بين الأطراف يمكن أن تؤثر بشكل مباشر على فعالية السياسات والإجراءات المتخذة في مواجهة الهجمات السيبرانية.

ا-**عدم توافق الأنظمة** مشكلة عدم توافق الأنظمة هي من أبرز التحديات التي تواجه التنسيق التقني، خاصة في بيئة رقمية تتسم بتنوع الأنظمة والتقنيات. كل منظمة أو حكومة قد تعتمد على مجموعة من الأدوات والبرمجيات المختلفة، ولا توجد دائمًا آلية موحدة للتفاعل بين هذه الأنظمة. في بعض

[1] مصطفى عبد الحميد،مرجع سابق، ص .48-53

الحالات، قد تستمر المؤسسات في استخدام أنظمة قديمة لا تتوافق مع أنظمة الأمان الحديثة، مما يجعلها عرضة للاختراقات .المشاكل التي تنشأ عن عدم توافق الأنظمة تتراوح من صعوبة في تبادل البيانات بشكل آمن، إلى تأخير في الاستجابة للهجمات السيبرانية. على سبيل المثال، في حالة حدوث هجوم سيبراني معقد، قد لا تكون الأنظمة القديمة قادرة على الاتصال بالأنظمة الحديثة التي تم تطويرها للتعامل مع مثل هذه الهجمات، مما يؤدي إلى وجود فجوات في الاتصال وتخلف في اتخاذ الإجراءات الأمنية اللازمة.

ب- صعوبة التفاعل مع البيانات :بالإضافة إلى ذلك، فإن التنوع الكبير في التقنيات والمعايير المستخدمة بين الشركات والدول يؤدي إلى صعوبة في التفاعل مع البيانات بشكل فعال. قد يتعين على كل طرف إجراء تحديثات وصيانة مستمرة لضمان أن الأنظمة الخاصة بهم متوافقة مع المعايير الدولية أو مع أنظمة الأطراف الأخرى .مثال على ذلك، قد تكون دولة معينة قد تبنت أنظمة تقليدية في مجال الحماية السيبرانية، بينما تعتمد دولة أخرى على أنظمة متقدمة وحديثة، مما يؤدي إلى ضعف التنسيق بينهما في مواجهة الهجمات السيبرانية العابرة للحدود. يتطلب التنسيق الفعّال بين هذه الأنظمة تنسيقًا دائمًا بين مختلف الأطراف وتوحيد المعايير التقنية المتبعة في كل مرحلة

ثانيًا: نقص الأدوات المشتركة

نقص الأدوات المشتركة يمثل أحد التحديات الكبرى التي تواجه التنسيق بين الأنظمة المختلفة. رغم أن الأدوات الأمنية الحديثة توفر العديد من الإمكانيات لحماية البيانات والمعلومات الحساسة، فإن غياب معايير موحدة للأدوات المستخدمة يجعل التنسيق بين الأنظمة المختلفة معقدًا. تختلف الشركات والدول في اختيار أدوات الحماية الخاصة بها، مما يؤدي إلى وجود فجوات في التنسيق بين هذه الأدوات .فعلى سبيل المثال، قد تستخدم بعض الشركات حلولاً خاصة بها لمراقبة الشبكة وتحليل التهديدات، بينما قد تعتمد أخرى على برامج أخرى تتسم بكفاءات مختلفة. في حال وقوع هجوم سيبراني معقد، ستكون هذه الأدوات غير قادرة على التفاعل مع بعضها البعض في بعض الحالات، مما يؤدي إلى تباين في الاستجابة وتباطؤ في الإجراءات الوقائية. يزداد الأمر تعقيدًا عندما تكون البيانات الحساسة مخزنة في أنظمة مختلفة يستخدمها مزودون مختلفون، مما يجعل تأمينها وتنسيق الوصول إليها أمرًا صعبًا .العدد الكبير من الأدوات الأمنية المتاحة في السوق يعني أن كل منظمة أو دولة قد تتبنى حلولًا خاصة بها وفقًا لاحتياجاتها التقنية، مما يؤدي إلى عدم الاتساق بين الأدوات. في العديد من الحالات، قد تكون الحلول الخاصة بكل طرف غير متوافقة مع الحلول الأخرى التي يتعين عليها العمل معها. يؤدي هذا

إلى وجود حاجة مستمرة لإجراء التحديثات على هذه الأدوات لجعلها أكثر توافقًا مع أنظمة الأمان المتطورة .أيضًا، فغالبًا ما تحتاج هذه الأدوات إلى قدرات فنية عالية من فرق العمل لضمان تكاملها بشكل مناسب ضمن بيئة العمل، وهذا يزيد من العبء على المؤسسات في سبيل الحفاظ على الأمن السيبراني الفعّال. وعليه، فإن توحيد الأدوات الأمنية في جميع الأطراف يمكن أن يساهم في تحسين التنسيق، لكنه يتطلب تعاونًا دوليًا وشركات خاصة للموافقة على استخدام الحلول المشتركة

ثالثًا: تحديات التنسيق بين الجهات المختلفة

التنسيق بين الجهات المختلفة يعد من أكبر التحديات في عالم الأمن السيبراني. على الرغم من أن التنسيق بين المؤسسات الكبرى أو الحكومات المحلية قد يكون أسهل إلى حد ما، إلا أن التنسيق بين أطراف دولية أو بين الحكومات والشركات الخاصة في بعض الأحيان قد يكون معقدًا جدًا. غالبًا ما تواجه الحكومات والشركات تحديات كبيرة في تحديد كيفية تبادل المعلومات حول التهديدات السيبرانية، خاصة إذا كانت تلك المعلومات تتعلق بأمن البيانات أو الهجمات العابرة للحدود .في كثير من الأحيان، لا تتفق الدول أو حتى الشركات الكبرى على سياسات حماية البيانات المتبعة، مما يؤدي إلى تعارض في طرق التعامل مع المعلومات المشتركة. هذا التنوع في السياسات ينعكس على صعوبة التنسيق بين الأطراف المختلفة في حال وقوع هجوم سيبراني. على سبيل المثال، قد تتبنى دولة ما سياسة أمنية صارمة للغاية بخصوص البيانات الشخصية، بينما قد تكون سياسة دولة أخرى أكثر مرونة أو قد لا تتوفر لديها قوانين حماية البيانات بقدر كافٍ .إضافة إلى ذلك، فإن التنسيق بين الحكومات والشركات قد يواجه صعوبة خاصة عندما تكون الشركات الخاصة هي التي تمتلك البنية التحتية الرقمية الأساسية. في بعض الأحيان، قد تكون الشركات غير مستعدة للتعاون الكامل مع الحكومات في تبادل المعلومات الأمنية، مما يعرقل الاستجابة الفعّالة للهجمات .الجهود المبذولة لتحسين التنسيق بين الجهات المختلفة تشمل تحسين التعاون بين القطاع العام والخاص من خلال منصات مشتركة لتبادل المعلومات، وتطوير استراتيجيات تعاون دولية لتعزيز الأمن السيبراني. لكن رغم هذه الجهود، فإن التباين في السياسات والأهداف بين الدول والشركات يعوق التنسيق الفعّال في معظم الحالات

رابعًا: تحديات الحوسبة السحابية الحوسبة السحابية تمثل تقنية ثورية في كيفية تخزين البيانات ومعالجتها، إلا أنها أيضًا تثير عددًا من التحديات التقنية عندما يتعلق الأمر بالتنسيق بين الأنظمة المختلفة. هذه التقنية تتيح للعديد من الشركات والدول تخزين ومعالجة البيانات على خوادم بعيدًا عن مواقعها الأصلية، مما يسمح بالوصول إلى البيانات من أي مكان في العالم. لكن في المقابل، تفتح

الحوسبة السحابية أبوابًا لمجموعة من المخاطر الأمنية .أحد أكبر التحديات في الحوسبة السحابية هو ضمان أمان البيانات المخزنة عبر منصات سحابية متعددة. في حال تم تخزين البيانات عبر عدة مزودين سحابيين، تصبح عملية التنسيق بين هذه الأنظمة أكثر تعقيدًا، حيث قد تختلف استراتيجيات الأمان المتبعة من مزود لآخر. هذا التنوع في حلول الأمان يرفع من احتمال وجود ثغرات يمكن استغلالها من قبل المهاجمين .إضافة إلى ذلك، تتعرض البيانات المخزنة في السحابة إلى تهديدات قد تكون أقل وضوحًا من تلك التي يمكن التعرف عليها في الأنظمة التقليدية. فالهجمات التي تستهدف البنية التحتية السحابية يمكن أن تؤدي إلى اختراق واسع النطاق للبيانات الحساسة، خاصة إذا كانت أنظمة الأمان غير متوافقة بين مختلف مزودي الخدمات السحابية .العديد من المؤسسات التي تعتمد على الحوسبة السحابية تواجه صعوبة في ضمان أن أنظمتها الأمنية متوافقة مع الإجراءات الأمنية التي يتبعها مزودو الخدمات السحابية. هذا التنسيق بين الشركات والمزودين السحابيين يتطلب جهدًا إضافيًا في تحديد معايير الأمان التي يتم تطبيقها على مستوى جميع المنصات السحابية المستخدمة، لضمان عدم تعرض البيانات للاختراق[1]

خامسا-تحديات التقنيات الناشئة تمثل التقنيات الناشئة محورًا حيويًا في تطور البيئة الرقمية، إذ تفتح آفاقًا جديدة للإبداع، لكنها في المقابل تفرز تهديدات مستحدثة قد تتجاوز القدرات التقليدية للأنظمة الأمنية. ومن أبرز هذه التقنيات: إنترنت الأشياء، الذكاء الاصطناعي، والحوسبة السحابية، التي سنفصل تحدياتها كما يلي

1-إنترنت الأشياء:إن إنترنت الأشياء عبارة عن منظومة ضخمة من الأجهزة الذكية المرتبطة بالشبكة، والتي تقوم بجمع ومعالجة وتبادل البيانات دون تدخل بشري مباشر .وتشمل هذه الأجهزة مختلف أنواع الحساسات، الكاميرات، عدادات الكهرباء، الثلاجات، وحتى نظم المراقبة في المصانع أو البنايات الذكية .تكمن أبرز التحديات في هذه التقنية في أن أغلب الأجهزة المدمجة بإنترنت الأشياء تُصمم لتكون منخفضة التكلفة وذات قدرات معالجة محدودة، ما يعني أنها غالبًا ما تُطرح في الأسواق بخصائص أمان ضعيفة أو شبه معدومة، مثل غياب التشفير أو كلمات مرور افتراضية يمكن اختراقها بسهولة. على سبيل المثال، يمكن للمهاجمين استخدام جهاز منزلي بسيط، مثل كاميرا مراقبة متصلة بالإنترنت، كنقطة دخول إلى الشبكة المنزلية بأكملها، ومنها إلى الحواسيب أو البيانات الشخصية. وتزداد الخطورة حينما تُستخدم هذه الأجهزة ضمن أنظمة البنى التحتية الحرجة (مثل شبكات المياه أو الكهرباء)، حيث قد يؤدي اختراقها إلى شلل جزئي أو كامل في هذه الخدمات .أضف إلى ذلك أن غياب معايير موحدة دوليًا

[1] مصطفى عبد الحميد مرجع سابق ص 121

لتصميم وتحديث هذه الأجهزة يُعقّد من مهمة الجهات التنظيمية، كما يجعل من الصعب تنفيذ عمليات التصحيح أو التحديث الأمني عبر جميع الأجهزة المنتشرة عالميًا، والتي قد تبلغ الملايين، وهو ما يؤدي إلى تشكل "شبكات زومبي (Botnets) "يُستخدم بعضها في تنفيذ هجمات ضخمة مثل هجوم"Mirai" الشهير

2-الذكاء الاصطناعي:الذكاء الاصطناعي يُعد ثورة فكرية وتقنية بامتياز، إذ أصبحت النماذج الذكية تُستخدم في التنبؤ بالهجمات السيبرانية، وتقييم المخاطر، بل حتى في إدارة أنظمة الدفاع الإلكتروني بشكل آلي. غير أن نفس الأدوات تُستخدم أيضًا في الجانب المعاكس، أي من قِبل المهاجمين.من أبرز التحديات ما يُعرف بهجمات الاصطناع العكسي(Adversarial Attacks) ، وهي هجمات يُدخل فيها المهاجم بيانات مزيفة أو معدّلة بخبث ضمن بيانات التدريب الخاصة بالنموذج الذكي، ما يجعله يتخذ قرارات خاطئة. مثلاً، قد يتم التلاعب بخوارزمية للتعرف على الصور لتصنيف فيروس على أنه ملف آمن .كما أن أنظمة الذكاء الاصطناعي قد تعتمد على "صندوق أسود"، أي أنها تُصدر نتائج دون أن تكون هناك طريقة واضحة لفهم كيف توصلت إليها، مما يعيق عمليات التدقيق والمراجعة القانونية أو التقنية في حال وقوع خلل أو خطأ. وهذا يشكل تهديدًا كبيرًا، خاصة إذا تم استخدام الذكاء الاصطناعي في التحكم الآلي بالطائرات، أو تحليل بيانات المراقبة الأمنية، أو حتى اتخاذ قرارات سياسية واقتصادية .وفي سياق آخر، يشكّل الذكاء الاصطناعي تحديًا للخصوصية، حيث يتم جمع وتحليل كم هائل من البيانات الشخصية لتدريب الخوارزميات، ما يطرح تساؤلات حول الجهة التي تملك هذه البيانات، وكيفية حمايتها من التسريب أو الاستخدام التعسفي

3-**الحوسبة السحابية** (Cloud Computing) الحوسبة السحابية غيّرت جذريًا مفهوم إدارة البيانات، حيث أصبحت المؤسسات تُخزن بياناتها وتشغّل تطبيقاتها على خوادم افتراضية موجودة في مواقع بعيدة، ما قلّل من الحاجة إلى البنية التحتية الداخلية. ومع ذلك، فإن هذا التحول جلب مجموعة من التحديات :

ا-السيادة على البيانات: عندما تكون البيانات مخزنة في سحابات تقع خارج الحدود الوطنية، فإنها قد تخضع لقوانين بلد الشركة المستضيفة، وهو ما يعقّد المسائل القانونية والأمنية. فمثلًا، قد تُطالب جهة حكومية أجنبية بالوصول إلى بيانات محفوظة على خوادم شركة سحابية، حتى لو كانت هذه البيانات تعود لمؤسسة وطنية في بلد آخر.

ب-الهجمات على البنية التحتية السحابية: مثل هجمات "استغلال تكوينات خاطئة " (Misconfiguration Exploits)، حيث تؤدي أخطاء بسيطة من طرف المستخدم إلى فتح الثغرات أمام المهاجمين. كما أن وجود آلاف المستخدمين في نفس بيئة الحوسبة السحابية يخلق خطر "الهجمات بين المستأجرين(Cross-Tenant Attacks) "، حيث يمكن لمستخدم ضار اختراق بيانات مستخدمين آخرين.

ج-فقدان السيطرة المباشرة: بما أن البيانات لم تعد في الخوادم المحلية، يصبح من الصعب تتبع من يملك حق الوصول الفعلي إليها أو مدى الالتزام بالسياسات الأمنية. كما أن هناك صعوبة في تنفيذ خطط الطوارئ في حال انقطاع الخدمة أو تعرض السحابة لهجوم.

د-التحديات التقنية للتكامل: في بعض الأحيان، يصعب على المؤسسات دمج أنظمتها القديمة (Legacy Systems)مع أنظمة السحابة الحديثة، ما يُحدث فجوات في الأمان ويزيد من كلفة التحديث والتكيّف التكنولوجي[1].

و-تحديات الاستجابة للحوادث السيبرانية

تُعد الاستجابة للحوادث السيبرانية من أكثر المراحل حساسية في منظومة الأمن السيبراني، وتُبرز بشكل واضح مدى كفاءة البنية التحتية، وسرعة التنسيق، ومدى نضج المؤسسات المكلفة بحماية الفضاء الرقمي. الحوادث السيبرانية، بما في ذلك الهجمات على الشبكات، تسريب البيانات، عمليات الاحتيال الكبرى، والهجمات على البنى التحتية الحيوية، تستدعي تدخلًا فوريًا ومنسقًا، إلا أن هذا التدخل يُواجه عدة تحديات بنيوية وتقنية وتنظيمية. وفيما يلي تفصيل موسّع لأبرز هذه التحديات:

*صعوبة الإسناد (Attribution) تُعتبر صعوبة الإسناد من أعقد الإشكالات التي تُواجه فرق الاستجابة، حيث لا يمكن بسهولة تحديد الجهة التي نفّذت الهجوم. يرجع ذلك إلى أن الفضاء السيبراني يُتيح للجهات المهاجمة التخفي واستعمال شبكات متعددة لإخفاء مصدر الهجوم، مثل الشبكات الافتراضية الخاصة(VPN) ، والخوادم الوسيطة (Proxies)، وتقنيات إخفاء الهوية مثل TOR.كل هذه الوسائل تُربك أدوات التحليل وتجعل من الصعب تتبع المسارات الرقمية .وتزداد

[1]أحمد أبو راس«**التقنيات الناشئة والأمن السيبراني: تحديات الحماية الرقمية في بيئة متغيرة**»، مجلة الدراسات التكنولوجية، العدد 15، جامعة القاهرة، 2022، ص. 112–125

المسألة تعقيدًا باستخدام تقنيات "الراية الزائفة(False Flag) "، حيث يقوم المهاجم بإدراج إشارات توحي بأن جهة أخرى هي المسؤولة. مثلًا، يُمكن زراعة شفرة خبيثة مكتوبة بلغة برمجية تُستخدم عادة في منطقة جغرافية معينة، أو تزييف توقيعات رقمية توحي بأن الهجوم نُفذ من عنوان

تابع لدولة معينة. كما يُمكن إدخال نصوص تحتوي على عبارات بلغة معينة ضمن البرمجيات الخبيثة لتضليل فرق التحليل .عدم القدرة على الإسناد يُعيق الاستجابة الفعالة، لأن تحديد المسؤول شرط أساسي لاتخاذ إجراءات مضادة، سواء كانت تقنية أو دبلوماسية أو قانونية .وتبقى هذه الصعوبة قائمة حتى في ظل التعاون الدولي، نظرًا لغياب إطار قانوني عالمي يُنظم قواعد الإسناد السيبراني ويُحدد معاييره وحدوده

*تنسيق الاستجابة في كثير من الأحيان، تؤدي الحوادث السيبرانية إلى ارتباك داخل المؤسسات المعنية، نتيجة غياب التنسيق الفوري. تنسيق الاستجابة يتطلب عملًا جماعيًا متكاملًا بين وحدات الأمن السيبراني، السلطات الأمنية، الهيئات القضائية، وفرق الطوارئ الفنية. غير أن هذا التنسيق يصطدم غالبًا بعدة معيقات، مثل عدم وجود خريطة واضحة للجهات المسؤولة، أو تضارب الصلاحيات بينها .على المستوى الوطني، تعاني بعض الدول من غياب فرق استجابة وطنية مُنظمة (CERT)، أو من ضعف قدرة هذه الفرق على اتخاذ قرارات عاجلة دون الرجوع إلى مستويات إدارية عليا، مما يُؤخر التدخل. كما أن غياب بروتوكولات الاستجابة المعيارية يجعل كل حادثة تعامل وكأنها حالة جديدة تمامًا، مما يضيع الوقت والجهد .أما على المستوى الدولي، فالأمر أشد تعقيدًا. في حالات الهجمات العابرة للحدود، يصبح التعاون مع جهات خارجية ضرورة، لكن معوقات اللغة، واختلاف القوانين، والتباين في المصالح، كلها تُقلل من فاعلية هذا التعاون. كما أن بعض الدول ترفض تسليم بيانات أو التعاون لأسباب تتعلق بالسيادة أو الحساسيات الجيوسياسية

*ضعف الجاهزية المؤسساتية والبشرية لا يمكن الحديث عن استجابة فعالة للحوادث السيبرانية في ظل ضعف الموارد البشرية وعدم تدريب العاملين على سيناريوهات الطوارئ. كثير من المؤسسات تعتمد على كوادر غير متخصصة أو غير مدربة على التعامل مع الحوادث المعقدة، خصوصًا في المؤسسات الحيوية مثل الموانئ، المطارات، والمستشفيات .كما أن ضعف الوعي العام داخل المؤسسة حول كيفية الإبلاغ عن حادثة، أو الإجراءات التي يجب اتخاذها عند الشك بوجود اختراق، يؤدي إلى تأخر في رصد الحوادث ويمنح المهاجمين وقتًا أكبر للتمدد داخل الأنظمة. وتُبرز التجارب الدولية أن الدقائق الأولى بعد اكتشاف الحادثة هي الأكثر حسمًا في تقليص

الخسائر، ومع ذلك فإن العديد من المؤسسات تُضيّع هذه الفرصة بسبب الارتباك أو ضعف الإجراءات الداخلية.

*تأخر الوصول إلى المعلومات الحيوية تواجه فرق الاستجابة كثيرًا من العوائق في الحصول على المعلومات الفنية الدقيقة المرتبطة بالحادثة. في بعض الحالات، تكون السجلات أو "Logs" غير مفعّلة أو محفوظة بشكل سيء، أو يتم حذفها تلقائيًا، مما يُفقد المحققين القدرة على تحليل آثار الهجوم. وفي حالات أخرى، ترفض بعض الشركات، خصوصًا تلك المتعددة الجنسيات، التعاون الفوري لأسباب قانونية أو للحفاظ على سمعتها .يُضاف إلى ذلك أن الحوادث الكبيرة تستدعي تعاونًا مع مزودي الخدمات التقنية، مثل الشركات المالكة للبنية التحتية للحوسبة السحابية أو لمشغلي الإنترنت. وفي غياب اتفاقات مسبقة أو آليات واضحة لتبادل المعلومات في حالات الطوارئ، تُصبح هذه العمليات بطيئة أو غير فعالة

*نقص الاستثمار في أدوات الاستجابة العديد من الدول، خاصة النامية، لا تُخصص ميزانيات كافية لتطوير أدوات وتقنيات الاستجابة السريعة. وتبقى الاستجابة محدودة بالأدوات اليدوية أو البرمجيات المجانية، التي لا تتيح دائمًا كشف الهجمات المتطورة. كما أن الاعتماد على مزودي خدمات خارجيين دون وجود فرق محلية يُضعف من سرعة ودقة الاستجابة .النقص في الاستثمار لا يشمل فقط الأدوات التقنية، بل يتعداه إلى غياب سيناريوهات محاكاة للأزمات السيبرانية، والتي تُعد ضرورية لاختبار الجاهزية. فبدون تمارين دورية، يصعب على الفرق المعنية معرفة نقاط الضعف أو التنسيق الفعلي المطلوب في حالات الضغط[1]

المطلب الثاني

التحديات القانونية والأمنية

[1]الهيئة الوطنية للأمن السيبراني". **تقرير حول جاهزية الاستجابة للحوادث السيبرانية"**. الرياض: المركز الوطني للاستجابة للطوارئ الإلكترونية2023.ص. 42–85.

-

أحدثت التكنولوجيا الرقمية والأنظمة المعلوماتية تحولًا جذريًا في الاقتصاد العالمي، مما جعل الفضاء السيبراني جزءًا حيويًا من المعاملات الاقتصادية .لكن هذا التحول صاحبه زيادة في التهديدات السيبرانية التي تؤثر على استقرار المعاملات وأمن المؤسسات. وللتصدي لهذه التهديدات، أصبح من الضروري تطوير استراتيجيات فعالة تشمل استخدام حلول تقنية مثل التشفير والذكاء الاصطناعي، بالإضافة إلى تعزيز الوعي الأمني من خلال التعليم والتدريب، ووضع السياسات الأمنية على المستويين الوطني والدولي لحماية الاقتصاد الرقمي ومن هذه التهديدات ما يتعلق بالجانب القانوني في حين يتعلق الجانب الاخر من هذا المطلب بالحروب السيبرانية تفاقم الجرائم الرقمية العابرة للحدود وغيرها

الفرع الأول

التحديات القانونية

يواجه الإطار القانوني تحديات كبيرة في مواكبة تطور الجريمة السيبرانية، خاصة بسبب الطبيعة العابرة للحدود للهجمات الإلكترونية، وصعوبة تحديد المسؤولية القانونية في البيئة الرقمية. كما تُعاني التشريعات الوطنية من قصور في التعاريف والمفاهيم، فيما يشهد التعاون الدولي بطئًا وتفاوتًا بين الدول في تنظيم الحقوق والواجبات الرقمية، ما يُضعف من فعالية المواجهة القانونية الشاملة.

أولا-تضارب القوانين واختصاص القضاء

التباين الحاد في التشريعات الوطنية الخاصة بالأمن السيبراني يُعدّ الاختلاف الجذري بين النظم القانونية الوطنية في مجال الأمن السيبراني

1-من أبرز المعوقات أمام تشكيل منظومة قانونية دولية متجانسة قادرة على مواجهة التهديدات الرقمية العابرة للحدود. فمع تصاعد المخاطر الناجمة عن الاستخدامات غير المشروعة لتكنولوجيا المعلومات والاتصالات، سارعت معظم الدول إلى سنّ تشريعاتها الخاصة بالأمن السيبراني بشكل أحادي يعكس مخاوفها الداخلية، دون مراعاة لمبدأ الانسجام أو التكامل القانوني مع باقي الدول، ما أدى إلى نشوء حالة من التشظي القانوني الدولي .فعلى سبيل المثال، يعتمد الاتحاد الأوروبي على أطر قانونية صارمة مثل توجيه NIS(أمن الشبكات والمعلومات) واللائحة العامة لحماية البياناتGDPR،

والتي تُعد الأكثر تطورًا من حيث حماية خصوصية الأفراد وتنظيم سلوك الشركات فيما يتعلق بجمع ومعالجة البيانات الشخصية. ويُلزم هذا النظام الشركات داخل وخارج الاتحاد الأوروبي باتباع معايير مشددة، ويمنح سلطات الدول الأعضاء حق فرض غرامات ضخمة على المخالفين .أما في المقابل، فإن الولايات المتحدة الأمريكية لا تتبنى إطارًا موحدًا على المستوى الفيدرالي، بل تعتمد على خليط من القوانين الفيدرالية مثل CISA (قانون تبادل المعلومات السيبرانية) و) CLOUD Actقانون الوصول إلى البيانات السحابية)، بالإضافة إلى قوانين محلية تختلف من ولاية إلى أخرى، ما يخلق حالة من عدم الاتساق القانوني حتى داخل الدولة الواحدة. كما يُعدّ قانون CLOUD Act مثار جدل كبير دوليًا، لأنه يمنح السلطات الأمريكية صلاحيات لطلب بيانات مخزنة في خوادم خارج الولايات المتحدة إذا كانت مملوكة لشركات أمريكية، ما يتعارض مع قوانين الحماية في دول أخرى مثل الاتحاد الأوروبي.أما الصين وروسيا، فتعتمدان نهجًا سياديًا مغلقًا في تنظيم الفضاء السيبراني، حيث تفرضان على الشركات الأجنبية والمحلية تخزين بيانات المستخدمين محليًا، ومنعها من نقلها إلى الخارج دون إذن مسبق من السلطات .وتُجبر الصين الشركات على التعاون مع أجهزة الأمن القومي، وفقًا لقانون الأمن السيبراني لسنة 2017، وهو ما يتعارض تمامًا مع المفهوم الليبرالي الأوروبي لحماية الخصوصية.هذا التباين في الرؤى القانونية، لا يُعيق فقط تنسيق الاستجابة للهجمات السيبرانية، بل يخلق بيئة غير مواتية للاستثمار الرقمي والتبادل التجاري، إذ تجد الشركات متعددة الجنسيات نفسها أمام التزام مزدوج أو متناقض أحيانًا، مما يرفع التكاليف القانونية ويفرض قيودًا تعجيزية على الامتثال التنظيمي

2-**تنازع الاختصاص القضائي وصعوبات تحديد المسؤولية القانونية** تطرح الطبيعة اللامادية والعابرة للحدود للفضاء السيبراني تحديات غير مسبوقة أمام الأنظمة القضائية التقليدية، التي تعتمد أساسًا على معايير جغرافية لتحديد الاختصاص القضائي. ففي عالم تتنقل فيه البيانات والمعلومات بسرعة الضوء عبر خوادم موزعة جغرافيًا، لم يعد بالإمكان تطبيق قواعد الاختصاص القضائي بمعناها الكلاسيكي. فعلى سبيل المثال، يمكن لهجوم سيبراني أن ينطلق من دولة "أ" باستخدام أدوات وتقنيات مستضافة في خوادم بدولة "ب"، ويستهدف منشآت أو مؤسسات في دولة "ج". في هذه الحالة، من هي الدولة صاحبة الحق في التحقيق والمقاضاة؟ وهل يمكن المطالبة بتعاون قضائي من دولة لا تعترف أصلاً بوجود ضرر على أرضها أو لا تملك اتفاقية تسليم مجرمين مع الدولة المتضررة؟ هذا السيناريو ليس افتراضيًا بل يتكرر في الواقع، مثلما حدث في هجومNotPetyaالذي ضرب شركات وبنى تحتية غربية، وتبين لاحقًا أن مصدره خوادم روسية عبر أوكرانيا، دون أن تستطيع أي دولة إثبات المسؤولية المباشرة

بشكل قانوني ملزم .إضافة إلى ذلك، تزداد تعقيدات تحديد الاختصاص حينما ترتبط الهجمات السيبرانية بجهات فاعلة غير حكومية، أو بجماعات مدعومة من قبل دول بشكل غير مباشر، مما يُصعّب إثبات العلاقة القانونية بين الفاعل والدولة، ويجعل من عملية "الإسناد "Attribution واحدة من أعقد التحديات القانونية والتقنية في هذا المجال. كما أن كثيرًا من الدول تفتقر أصلًا إلى البنية القانونية والفنية اللازمة لتحليل الأدلة الرقمية وتقديمها أمام المحاكم، بسبب غياب الخبراء، وضعف تجهيزات فرق التحقيقات الرقمية، وعدم وجود آليات توثيق إلكتروني معترف بها قضائيًا .علاوة على ذلك، فإن تعاون الدول في التحقيقات غالبًا ما يتوقف عند حدود المصالح الجيوسياسية. فبعض الدول ترفض التعاون في تحقيقات لا تخدم أهدافها أو تشكّل تهديدًا لمصالحها الاستراتيجية، وتستخدم غموض الفضاء الرقمي كغطاء للإنكار أو التضليل. هذا ما يجعل من الفضاء السيبراني ساحة مثالية للحروب الرمادية التي يصعب فيها فرض المسؤولية القانونية أو حتى إثباتها[1].

ثانيا -نقص الإطار القانوني الدولي الموحد

يمثّل غياب إطار قانوني دولي موحد ينظم الأمن السيبراني إحدى أبرز المعضلات التي تعرقل الجهود الدولية الرامية إلى تأمين الفضاء الرقمي ومكافحة التهديدات السيبرانية العابرة للحدود. فعلى الرغم من الطابع العالمي لهذا الفضاء الذي لا يعترف بالحدود الجغرافية التقليدية، إلا أن المجتمع الدولي لم ينجح حتى الآن في التوصل إلى معاهدة شاملة تنظم سلوك الدول والجهات الفاعلة غير الحكومية في هذا المجال.لقد أدى هذا النقص إلى وجود فراغ قانوني يسمح للدول بالتصرف بشكل منفرد أو متعارض أحيانًا، ويمنح الفاعلين الخطرين (سواء دولًا أو جهات خاصة أو منظمات إجرامية) حرية المناورة في بيئة تفتقر إلى القواعد الملزمة والآليات الموحدة للمساءلة. ويرجع هذا العجز إلى عدة عوامل متداخلة، من بينها الخلافات الجيوسياسية، والتباين في المفاهيم القانونية، وتضارب المصالح الاستراتيجية بين القوى الكبرى
محدودية الاتفاقيات الدولية القائمة وضعف فعاليتها أبرز محاولة لتنظيم الفضاء السيبراني دوليًا تمثلت في اتفاقية بودابست بشأن الجريمة السيبرانية (2001)، والتي تمثل المرجع الأساسي في مكافحة الجرائم الإلكترونية على المستوى الدولي. ورغم أهميتها، إلا أن فعاليتها تبقى محدودة جدًا لعدة أسباب

1-لم توقّع عليها قوى دولية رئيسية مثل الصين وروسيا والهند، بسبب تحفظات سياسية وسيادية، خصوصًا فيما يتعلق بمسألة "الولاية القضائية عبر الحدود

[1] علي، ناصر.**«القانون الدولي والأمن السيبراني: إشكاليات الاختصاص والسيادة في الفضاء الرقمي »**.مجلة البحوث القانونية والاقتصادية، العدد 18، 2022، ص.190–155 .

2-تقتصر الاتفاقية على الجرائم السيبرانية ذات الطابع الجنائي (مثل الاختراق، الاحتيال، القرصنة، المحتوى غير القانوني)، لكنها لا تتناول بشكل مباشر القضايا المتعلقة بالأمن القومي، أو الهجمات السيبرانية التي قد تُشن من دول ضد دول أخرى .ثالثًا، تفتقر الاتفاقية إلى آليات تنفيذ قوية تُلزم الدول بالتعاون الفعلي، حيث تظل مسألة تبادل المعلومات والأدلة خاضعة لإرادة سياسية أكثر منها التزامًا قانونيًا .إضافة إلى ذلك، سعت بعض المنظمات الدولية إلى إطلاق مبادرات جزئية مثل مجموعة العمل المفتوح التابعة للأمم المتحدة (OEWG) ومجموعة الخبراء الحكوميين(GGE) ، لكنها لم تُفضِ إلى نتائج ملموسة بسبب الانقسامات الحادة بين المعسكرين الغربي والشرقي. ففي حين تدعو الدول الغربية إلى حرية تدفق البيانات واحترام حقوق الإنسان الرقمية، تتمسك دول مثل روسيا والصين بمبدأ السيادة الرقمية وتقييد حرية الإنترنت باسم الأمن القومي

ثالثا –إشكالية الإسناد القانوني والردع في الهجمات السيبرانية

يُعدّ تحديد المسؤولية القانونية عن الهجمات السيبرانية (الإسناد) من أبرز التحديات التي يُواجهها القانون الدولي. فعلى عكس الحروب التقليدية، يصعب تحديد الجهة التي تقف وراء هجوم سيبراني بدقة، نظرًا لاعتماد المهاجمين على تقنيات التخفي، والخوادم الوسيطة، والهويات المزيفة، وشبكات VPN، مما يجعل عملية الإسناد محفوفة بالشكوك .ويُبرز ذلك معضلة أساسية: هل يمكن تحميل دولة معينة مسؤولية قانونية عن هجوم سيبراني انطلق من أراضيها دون دليل مادي قطعي؟ وهل يُمكن اعتبار الهجمات السيبرانية شكلًا من أشكال العدوان الذي يبرّر اللجوء إلى الدفاع المشروع بموجب المادة 51 من ميثاق الأمم المتحدة؟ في هذا السياق، يثور جدل قانوني كبير حول المعايير التي يجب توفرها لتفعيل قواعد القانون الدولي الإنساني على الهجمات الرقمية. فمثلًا، هجومNotPetyaالذي نُسب إلى روسيا وخلّف أضرارًا بمليارات الدولارات على مستوى العالم، لم يُقابل بأي رد قانوني رسمي بسبب عدم وجود دليل قاطع ومُلزم. وهذا يفتح الباب أمام الإفلات من العقاب الرقمي، ويقوّض مبدأ الردع القانوني .كما أن غياب اتفاق دولي حول تعريف "الهجوم السيبراني" أو "العمل الحربي الرقمي" يجعل من الصعب على الدول تبرير إجراءاتها الدفاعية أو الردعية قانونيًا، ويزيد من احتمال استخدام التدخلات السيبرانية كأداة للحرب الرمادية دون إعلان رسمي أو رقابة قانونية

رابعا -ضعف القدرات القانونية والفنية على مستوى الدول النامية

يُضاف إلى ما سبق ضعف البنية التحتية القانونية والفنية في عدد كبير من الدول، خاصة النامية منها، حيث تعاني هذه الدول من نقص حاد في الكفاءات المتخصصة في الجرائم السيبرانية، وغياب

القوانين الوطنية الحديثة المواكبة للتطورات الرقمية، فضلًا عن افتقارها للمختبرات الرقمية الجنائية والمحاكم المتخصصة .هذا التفاوت في القدرات يخلق بيئة غير متوازنة على المستوى الدولي، حيث تبقى الدول الضعيفة عرضة للاستغلال الرقمي دون القدرة على حماية سيادتها أو ملاحقة المهاجمين. كما أن هذه الدول غالبًا ما تُستبعد من مفاوضات الاتفاقيات التقنية الكبرى، مما يكرّس فجوة رقمية قانونية بين الشمال والجنوب[1]

الفرع الثاني

التحديات الأمنية

اصبحت الحروب السيبرانية من أبرز التحديات الأمنية التي تهدد استقرار الدول في العصر الرقمي، حيث تعتمد على استهداف الأنظمة الحساسة والمعلومات الحيوية بطرق خفية ومعقدة. وتكمن خطورة هذه الحروب في صعوبة اكتشاف مصدر الهجمات وسرعة تنفيذها، مما يجعل من التصدي لها أمرًا بالغ التعقيد. وتُطرح تحديات أمنية متعددة أبرزها ضعف البنية التحتية السيبرانية، وقلة الكفاءات المتخصصة، وتنوع دوافع الهجمات التي قد تكون سياسية أو اقتصادية أو استخباراتية. إن مواجهة هذه التحديات تتطلب يقظة مستمرة وتطويرًا دائمًا للقدرات الدفاعية السيبرانية.

أولا -الحروب السيبرانية والصراعات بين الدول:أصبحت الحروب السيبرانية أحد أخطر وجوه الصراع في القرن الحادي والعشرين، إذ انتقلت المواجهة بين الدول من الميدان العسكري إلى ميدان غير مرئي: الفضاء الرقمي. وتكمن خطورة هذه الحروب في طابعها اللا متماثل، حيث يمكن لدولة صغيرة أو حتى مجموعة غير حكومية أن تُحدث أضرارًا جسيمة بقوة عظمى باستخدام أدوات رقمية فقط

1-**مفهوم الحروب السيبرانية:**تعرف الحروب السيبرانية بأنها أعمال عدائية تُنفذ عبر الفضاء الرقمي بهدف تعطيل أو إتلاف أو التأثير على البنية التحتية الحيوية أو الأنظمة المعلوماتية لدولة ما، وغالبًا ما تنفذها دول أو كيانات مدعومة من دول .وتُعد هذه الهجمات جزءًا من استراتيجية أوسع تسمى بـ"الردع الرقمي" أو "الهجوم الوقائي السيبراني

[1]منصور هدى.«**الفراغ التشريعي الدولي في مواجهة الهجمات السيبرانية: دراسة في ضوء القانون الدولي العام**.».مجلة الدراسات القانونية والسياسية، العدد 12، 2021، ص. 88–112.

2-**دوافع الحروب السيبرانية:**تشمل الدوافع الأساسية لهذه الحروب أهدافًا استخباراتية واقتصادية وسياسية وعسكرية. فمن الناحية الاستخباراتية، تسعى الدول إلى الحصول على معلومات سرية حول القدرات الدفاعية أو العلاقات الدولية للدول الأخرى. أما على المستوى الاقتصادي، فغالبًا ما تستهدف الهجمات أسرار الابتكار الصناعي والملكية الفكرية. وفي الجانب السياسي، تهدف هذه الهجمات إلى زعزعة استقرار الدول، سواء بتسريب معلومات محرجة أو بالتأثير على الرأي العام. وأخيرًا، يُستخدم الفضاء السيبراني عسكريًا لتعطيل أنظمة القيادة والسيطرة قبيل العمليات الهجومية التقليدية

من أبرز الحوادث السيبرانية بين الدول: نذكريُعتبر هجوم "Stuxnet" ضد إيران سنة 2010 أول هجوم إلكتروني هجومي معروف، حيث استُخدم فيروس متطور لاستهداف أجهزة الطرد المركزي النووي وتعطيلها، ما ألحق أضرارًا بالغة بالبرنامج النووي الإيراني دون تدخل عسكري مباشر. هذا الهجوم بيّن أن الحروب الرقمية يمكن أن تُحدث تأثيرات ميدانية حقيقية .وفي السياق ذاته، استخدمت روسيا منذ 2014 سلسلة من الهجمات السيبرانية ضد أوكرانيا، استهدفت بها البنية التحتية للكهرباء، حيث انقطعت الطاقة عن آلاف السكان خلال الشتاء. كما انتشر فيروسNotPetyaالذي بدأ في أوكرانيا وامتد عالميًا، مسببًا خسائر اقتصادية تقدر بالمليارات، ومسًا خطيرًا بشبكات المؤسسات المالية والتجارية. وظهر دور مجموعة APT 29 المعروفة بـ"Cozy Bear" ، والتي ارتبطت بالاستخبارات الروسية، في شن هجمات على أهداف حكومية أمريكية وأوروبية، بما في ذلك اختراق اللجنة الوطنية للحزب الديمقراطي الأمريكي خلال انتخابات 2016، وتسريب بيانات حساسة .

3-**استهداف البنية التحتية الحيوية:**لم تعد أهداف الحروب السيبرانية محصورة في المؤسسات الأمنية والعسكرية، بل اتسعت لتشمل قطاعات مدنية شديدة الحساسية، مثل الصحة والطاقة والاتصالات والنقل. ومن أبرز الأمثلة على ذلك، هجوم"Colonial Pipeline"سنة 2021 الذي استهدف شركة توزيع وقود رئيسية في الولايات المتحدة، مما أدى إلى توقف إمدادات الوقود لعدة ولايات أمريكية وأثار حالة من الذعر. كما أن الهجمات التي استهدفت مستشفيات خلال جائحة كوفيد-19 كشفت عن خطورة استخدام البرمجيات الخبيثة في توقيتات حرجة، بما قد يعرّض حياة آلاف المدنيين للخطر .

4-**التأثيرات الاستراتيجية:**تخلق الحروب السيبرانية حالة من "الردع الرقمي المتبادل" بين القوى العالمية، حيث يتخوف كل طرف من الرد العكسي إذا شن هجومًا مباشرًا. وتؤدي هذه الحروب إلى تقويض سيادة الدول على فضائها الرقمي، كما تعزز من هشاشة الأنظمة الديمقراطية نتيجة لاستغلال

الثغرات لنشر الفوضى المعلوماتية أو التدخل في العمليات الانتخابية. كما تضطر الدول إلى تخصيص ميزانيات ضخمة لتعزيز قدراتها الدفاعية السيبرانية، ما يؤثر على أولوياتها التنموية[1] .

ثانيا -انتشار الجريمة السيبرانية العابرة للحدود

في عصرنا الحالي، حيث أصبح العالم مرتبطًا بشبكة الإنترنت بشكل متزايد، ظهرت الجريمة السيبرانية كأحد أخطر التهديدات التي تواجه الأمن الدولي. ومن بين أخطر صور هذه الجريمة، تأتي الجريمة السيبرانية العابرة للحدود التي تنطوي على تهديدات واسعة النطاق تشمل العديد من الدول في وقت واحد، وتسبب في أضرار جسيمة للمجتمعات، الاقتصاد، وحتى الأمن الوطني للدول. إذ تعد الجرائم التي ترتكب عبر الإنترنت من أكثر الجرائم تعقيدًا وصعوبة في الملاحقة، خاصةً عندما تكون هذه الجرائم عابرة للحدود وتنفذ من خلال شبكات معقدة تضم العديد من الجهات الفاعلة

1-**استخدام عصابات إجرامية في الفضاء السيبراني** أصبح الفضاء السيبراني مجالًا خصبًا لأنواع متعددة من الجرائم التي ترتكبها عصابات إجرامية منظمة. تتيح التقنيات الحديثة لهذه العصابات تنفيذ عمليات معقدة عبر الإنترنت، مما يجعل ملاحقتها أكثر صعوبة. هجمات الفدية (Ransomware) تُعد من أكثر الأنواع الشائعة للجريمة السيبرانية التي تنفذها العصابات الإجرامية عبر الإنترنت. ففي هذه الهجمات، يتمكن المهاجمون من اختراق الأنظمة الإلكترونية الخاصة بالمؤسسات، ثم يقومون بتشفير البيانات الهامة أو تعطيل الأنظمة الحيوية، ويطالبون الفدية مقابل فك تشفير هذه البيانات أو إعادة الأنظمة للعمل .هجوم :"WannaCry"كان هجوم"WannaCry"الذي وقع في مايو 2017 من أشهر الهجمات في هذا السياق. استهدف هذا الهجوم مستشفيات ومرافق طبية في المملكة المتحدة وعدد من المؤسسات في دول أخرى. وتمكن المهاجمون من تشفير البيانات الهامة على أجهزة الكمبيوتر وطلبوا فدية لفك تشفيرها. هذا الهجوم أدى إلى تعطيل الأنظمة الطبية، مما أسفر عن تأخير العديد من العمليات الطبية وخلق فوضى كبيرة في المستشفيات .أثر هجمات الفدية: إن الهجمات مثل"WannaCry"لم تقتصر على الخسائر المالية فحسب، بل ألحقَت أيضًا أضرارًا جسيمة على الصحة العامة. فعلى سبيل المثال، تأخرت العمليات الجراحية في بعض المستشفيات، وتم نقل المرضى إلى مستشفيات أخرى بسبب تعطل الأنظمة، مما أسفر عن تأثيرات بشرية صعبة

[1] بوحوشوليد.**«الحروب السيبرانية وأثرها على الأمن الدولي. مجلة الدراسات السياسية والدولية»**. جامعة الجزائر 3، العدد 18، 2022، ص. 135–160.

2-**غسيل الأموال الرقمية** يعتبر غسيل الأموال أحد الأنشطة غير القانونية الأخرى التي يُسهلها الفضاء السيبراني، وذلك بفضل استخدام العملات الرقمية التي توفر مستوى عالٍ من الخصوصية. تتيح هذه العملات مثل البيتكوينوالإيثريوم للمجرمين إخفاء مصدر الأموال غير المشروعة وتحويلها عبر شبكات معقدة من المعاملات التي يصعب تتبعها. تعتبر هذه العملات الرقمية أداة قوية للجماعات الإجرامية التي تسعى إلى إخفاء أنشطتها غير القانونية .التحديات القانونية في مكافحة غسيل الأموال: يمثل غسيل الأموال عبر الإنترنت تحديًا كبيرًا للهيئات القانونية الدولية. فالدول لم تضع بعد تشريعات موحدة لمكافحة غسيل الأموال المرتبط بالعملات المشفرة، كما أن العديد من البورصات الرقمية تعمل في بيئات قانونية غير واضحة، مما يسهل على المجرمين إخفاء أموالهم وتحويلها إلى أصول مشروعة في نظر الأنظمة المالية .هجوم :"REvil" في 2019، استهدفت مجموعةREvilالمهاجمين قطاع الأعمال من خلال تنفيذ هجمات فدية مشفرة تطلب من الشركات دفع الفدية بعملة البيتكوين.وقد استخدم المهاجمون هذه الأموال لتمويل عمليات غسيل الأموال عبر منصات غير مراقبة. هذا النوع من الجرائم يعزز قدرة المجرمين على تجاوز الحدود القانونية ويعطيهم فرصة لتمويل أنشطة غير مشروعة مثل التجارة في المخدرات والأسلحة .

3-خصائص الجريمة السيبرانية العابرة للحدود

الجريمة السيبرانية العابرة للحدود تتميز بعدد من الخصائص التي تجعلها فريدة وصعبة الملاحقة. من أبرز هذه الخصائص :

ا-العالمية: تمتد تأثيرات الجريمة السيبرانية عبر الحدود الجغرافية، مما يجعل الجريمة السيبرانية ليست قاصرة على دولة معينة. يمكن للمهاجم أن يكون في قارة معينة بينما يكون هدفه في قارة أخرى. هذا يعقد عملية التحقيقات القانونية والتعاون الدولي في ملاحقة الجرائم

ب-التخفي والتشفير: يتنكر المهاجمون باستخدام تقنيات مثل شبكاتVPN وتطبيقات التور (TOR) التي تساعد في إخفاء هويتهم والموقع الجغرافي الذي ينفذون منه الهجوم. هذا يجعل ملاحقتهم من قبل السلطات أمرًا في غاية الصعوبة .السرعة العالية: تتميز الجريمة السيبرانية بقدرتها على التنفيذ السريع، حيث يمكن للمهاجم تنفيذ هجوم ضخم خلال دقائق معدودة. هذا يتيح له التأثير على عدد كبير من الأهداف في وقت واحد، وهو ما يعقد من مسألة الاستجابة

ج-القدرة على التطور المستمر: ما يجعل الجريمة السيبرانية تتسم بالخطورة هو قدرتها المستمرة على التطور. فالمهاجمون يتطورون باستمرار في أساليبهم وتقنياتهم لتجاوز الأنظمة الأمنية والحماية الإلكترونية، مما يستدعي تحديث مستمر في التقنيات المستخدمة في الحماية والملاحقة

-أمثلة إضافية على الجريمة السيبرانية العابرة للحدود بجانب هجمات الفدية وغسيل الأموال، هناك العديد من الأنشطة الإجرامية التي تُنفذ عبر الإنترنت وتسبب تأثيرات واسعة. من بين هذه الأنشطة

*الاحتيال المالي الإلكتروني: يعد الاحتيال الإلكتروني أحد أكثر الجرائم شيوعًا عبر الإنترنت. حيث يستخدم المهاجمون أساليب مختلفة مثل التصيد الاحتيالي(Phishing) ، التي يتم فيها إرسال رسائل مزيفة تدعي أنها من مؤسسات مالية أو حكومية بهدف سرقة المعلومات الشخصية والمالية للأفراد

*التجارة غير المشروعة: في الفضاء السيبراني، تتنوع الأنشطة التجارية غير المشروعة، حيث يتم بيع المخدرات، الأسلحة، والبيانات المسروقة عبر الإنترنت باستخدام الشبكات المظلمة(Dark Web). هذه الأنشطة تساهم في تمويل العمليات الإرهابية والجماعات المسلحة.

*الابتزاز الجنسي والسياسي: في ظل الانفتاح الرقمي، أصبح الابتزاز أحد الأساليب التي تُستخدم لإجبار الأفراد أو المؤسسات على دفع مبالغ مالية أو التنازل عن معلومات حساسة، مثل الصور الشخصية أو الوثائق السرية، مقابل عدم نشرها.

د-**صعوبات ملاحقة الجريمة السيبرانية العابرة للحدود** تواجه الدول والهيئات القضائية العديد من التحديات التي تجعل ملاحقة الجريمة السيبرانية العابرة للحدود أمرًا معقدًا :

و-التباين في الأنظمة القانونية: لا توجد اتفاقات دولية شاملة لمكافحة الجريمة السيبرانية العابرة للحدود. بعض الدول لا توفر تشريعات واضحة لملاحقة المجرمين السيبرانيين، مما يعوق التعاون بين الهيئات القضائية في الدول المختلفة

هالقدرة التقنية المحدودة: لا تمتلك العديد من الدول قدرات فنية كافية لمكافحة الجريمة السيبرانية. فالمهاجمون يستخدمون تقنيات متطورة لتخفي هويتهم، مما يتطلب استخدام أدوات تحليلية معقدة لرصد وتتبع الهجمات

رغم وجود بعض الاتفاقيات الدولية مثل اتفاقية بودابست 2001، إلا أن التنسيق بين الدول لا يزال ضعيفًا، مما يجعل التعاون في مكافحة الجريمة السيبرانية مسألة صعبة[1]

المبحث الثاني

سبل مواجهة هذه التحديات

في ظل تصاعد التهديدات السيبرانية وتزايد تأثيرها على الاقتصاد الرقمي العالمي، بات من الضروري التفكير في حلول استراتيجية تضمن حماية الفضاء السيبراني وتعزيز الثقة في المعاملات الاقتصادية الرقمية. ويُعد الاستثمار في الشركات التكنولوجية المتقدمة خطوة أساسية لتقوية البنية التحتية الرقمية وتطوير أدوات الحماية السيبرانية، بما يضمن مواجهة الهجمات بكفاءة وفعالية. في المقابل، لا يمكن تحقيق أمن سيبراني شامل دون وجود إطار قانوني دولي موحد وملزم، يحدد المسؤوليات، ويُعزز التعاون بين الدول. بناءً على ذلك، سيتم تناول هذا الجانب من خلال مطلبين رئيسيين: الأول يتعلق بأهمية الاستثمار في الشركات التكنولوجية المتقدمة، والثاني يركز على ضرورة اعتماد إطار قانوني دولي ملزم لمواجهة التحديات السيبرانية العابرة للحدود.

المطلب الأول

الاستثمار في الشركات التكنولوجية المتقدمة

امام الطابع العابر للحدود الذي تتسم به التهديدات السيبرانية، لم يعد بالإمكان الاعتماد على الجهود الفردية للدول، بل أصبحت الحاجة ملحة لتعزيز العمل الجماعي والتعاون الدولي لمواجهة هذه المخاطر بشكل شامل ومنسق. كما أن مجابهة التحديات المعقدة التي يفرضها الفضاء السيبراني تتطلب كفاءات بشرية عالية التأهيل ومواكِبة لأحدث التطورات التكنولوجية. وعليه، سيتم تناول هذا الجانب من خلال فرعين رئيسيين: يُعنى الأول بسبل تعزيز التعاون الدولي في مجال الأمن السيبراني، بينما يركّز الثاني على تطوير الكفاءات البشرية على المستوى الدولي كركيزة أساسية لحماية البنية التحتية الرقمية وتحقيق أمن سيبراني مستدام

الفرع الأول

[1] عبدالرحمن محمد؛ **الجريمة الإلكترونية وأثرها على الأمن الدولي**. دار النشر الجامعي. 2020 ص 99-105

تعزيز التعاون الدولي

أمام تصاعد الهجمات السيبرانية واتساع نطاقها العابر للحدود، أصبح تعزيز التعاون الدولي في مجال الأمن السيبراني ضرورة استراتيجية لا يمكن تجاهلها .فالتحديات الأمنية المعقدة لم تعد محصورة ضمن حدود الدول، بل تتطلب تنسيقًا عالميًا شاملاً لمواجهتها بفعالية. وفي هذا السياق، برزت أهمية إنشاء التحالفات السيبرانية، وتوقيع الاتفاقيات الثنائية والمتعددة الأطراف، وتفعيل شراكات الابتكار في مجال الأمن الرقمي، إلى جانب تبادل الخبرات التقنية بين الدول. كما يشكل إطلاق مشاريع مشتركة في البحث والتطوير، وتوحيد معايير الحماية، خطوة محورية لبناء جبهة دفاعية متماسكة في مواجهة التهديدات الإلكترونية العالمية.

اولًا :إقامة شراكات استراتيجية بين الدول في عصر تتسارع فيه وتيرة التحول الرقمي، لم يعد بإمكان أي دولة بمفردها أن تواجه تحديات الأمن السيبراني المعقدة والمتطورة. إذ أن التهديدات الإلكترونية تتجاوز الحدود الجغرافية والسيادية، وهو ما يجعل من إقامة شراكات استراتيجية بين الدول أمرًا حتميًا وليس خيارًا .

1. إنشاء تحالفات أمنية سيبرانية

يُعد إنشاء التحالفات الأمنية في الفضاء السيبراني من أبرز أشكال التعاون الدولي. هذه التحالفات تهدف إلى بناء استجابة جماعية للتهديدات المتنامية، من خلال تنسيق السياسات، وتبادل المعلومات الاستخباراتية، وتنفيذ مناورات مشتركة لمحاكاة الهجمات السيبرانية. ومن أبرز هذه التحالفات :تحالف الأمن السيبراني العالمي: يضم مجموعة من الدول تتعاون لمجابهة الهجمات السيبرانية المنظمة، من خلال تبادل آليات الكشف المبكر والاستجابة السريعة .مبادرة الناتو السيبرانية: تهدف إلى حماية البنية التحتية الحيوية للدول الأعضاء من الهجمات الرقمية، وتطوير أطر تشريعية مشتركة .الاتحاد الأوروبي للأمن السيبراني (ENISA):يمثل تجربة رائدة في تنسيق جهود الأمن السيبراني داخل الفضاء الأوروبي، ويمتد بتأثيره إلى دول الجوار من خلال برامج التعاون والتوأمة .تكمن أهمية هذه التحالفات في تعزيز السيادة الرقمية المشتركة، وتوحيد الجهود البحثية، وتقوية القدرات الوطنية في مواجهة تهديدات معقدة مثل الهجمات على الأنظمة المالية، أو البنى التحتية للطاقة، أو أنظمة الاتصالات .

2. شراكات الابتكار التكنولوجي بين الدول المتقدمة والدول الناشئة

الهوة الرقمية بين الشمال والجنوب العالمي لا يمكن ردمها إلا من خلال بناء شراكات تكنولوجية عادلة. فالدول المتقدمة تمتلك الموارد والمعرفة، بينما تمتلك الدول الناشئة الديناميكية السكانية والحاجات المتزايدة للبنية الرقمية .ومن أبرز مجالات هذه الشراكات :نقل التكنولوجيا: عبر اتفاقيات تسمح بتوطين التقنيات الحديثة كأنظمة التشفير، والحوسبة السحابية، والحماية من الفيروسات المتطورة .إنشاء مراكز بحثية مشتركة: تُقام هذه المراكز في الدول الناشئة بتمويل مشترك، وتُدار بكفاءات محلية بدعم من خبراء دوليين. برامج الابتكار المشتركة: مثل مبادرة "Digital Africa" التي تمولها فرنسا لدعم الابتكار التكنولوجي في القارة الإفريقية .تكمن أهمية هذه الشراكات في تحقيق تنمية رقمية شاملة، وتحسين الجهوزية الرقمية للدول النامية، بما يضمن حمايتها من الاستغلال الرقمي والاختراقات السيادية.

3. تبادل الخبرات والتقنيات

يمثل تبادل الخبرات التقنية حجر الزاوية في التعاون الدولي. إذ تسهم الدورات التدريبية، وورش العمل، والتوأمة بين الإدارات السيبرانية في نقل المعرفة بشكل فعّال وسريع. وتشمل هذه المبادرات :التكوين المشترك لأطر الأمن السيبراني: عبر برامج تعليمية بتمويل مشترك بين حكومات ومؤسسات دولية .تبادل قواعد البيانات وأساليب التحليل السيبراني: لتطوير آليات الإنذار المبكر واكتشاف البرمجيات الخبيثة .تبادل أدوات البرمجيات الأمنية مفتوحة المصدر: مثل أدوات فحص الشبكات ومراقبة الاختراقات، وهو ما يساهم في تعزيز القدرات الذاتية للدول .هذه الآليات تُفضي إلى بناء ثقة استراتيجية بين الدول، كما تُعدّ خطوة ضرورية لتقليل الفجوة التقنية.

4. مشاريع بحثية مشتركة

ترتكز المشاريع البحثية الدولية على تطوير حلول تقنية لمشاكل سيبرانية عالمية، من خلال فرق علمية متعددة الجنسيات. وتغطي هذه المشاريع عادة :تطوير خوارزميات أمنية جديدة: خاصة في مجالات الذكاء الاصطناعي والبلوك تشين .بحوث حول حماية البيانات الشخصية: تُمثل أهمية خاصة في سياق القوانين الدولية مثل اللائحة العامة لحماية البيانات .(GDPR) أبحاث في الأمن الكمومي: نظرًا لتأثير الحوسبة الكمية المرتقب على تقنيات التشفير التقليدية .وتوفر هذه المشاريع منصة لتطوير حلول رقمية تتسم بـ"الحياد

التكنولوجي"، وتُعزز الاستقلال الرقمي الجماعي، وتقلل من الاعتماد على القوى العظمى في المجال السيبراني[1]

ثانيًا :تمويل مشاريع الابتكار التكنولوجي المشتركة يشكل التمويل حجر الأساس لأي جهد دولي لتعزيز الأمن السيبراني وتطوير التقنيات الحديثة، لا سيما في ظل التكاليف الباهظة المرتبطة بالبحث والتطوير، والتكوين، وبناء البنية التحتية الرقمية. ولهذا، تتجه الدول والمؤسسات الدولية إلى إنشاء آليات تمويلية متعددة لدعم الابتكار التكنولوجي عبر الحدود، خصوصًا في الدول النامية أو تلك التي تمر بمرحلة انتقال رقمي .

1. الصناديق الاستثمارية الدولية

تلعب الصناديق الدولية دورًا محوريًا في تمويل المبادرات التكنولوجية المشتركة، خصوصًا في الميادين ذات الطابع الأمني والابتكاري. وتندرج تحت هذه الفئة :صندوق الأمن السيبراني العالمي: يموّل مشاريع تطوير البرمجيات الدفاعية، ويدعم البنى التحتية الحيوية في البلدان النامية .صندوق الشراكة الرقمية الأوروبية – المتوسطية: يهدف إلى تمويل مشاريع رقمية بين دول الاتحاد الأوروبي ودول جنوب المتوسط، مع تركيز خاص على الأمن الرقمي .صندوق الأمم المتحدة للتنمية التكنولوجية: يقدم منحًا للدول منخفضة الدخل من أجل تطوير حلول تكنولوجية محلية تتماشى مع المعايير الدولية .هذه الصناديق تمثل أداة فعالة لتحقيق العدالة التكنولوجية وتجاوز الحواجز المالية التي تعيق تطوير منظومات الأمن السيبراني في العديد من البلدان .

2. تقديم منح مشتركة للباحثين والمطورين

يُعد تقديم المنح المشتركة أحد أبرز أشكال دعم البحث العلمي المشترك في المجالات التكنولوجية الحديثة، خصوصًا تلك التي تتعلق بالتقنيات الناشئة .وتشمل :منح الذكاء الاصطناعي التعاونية: تمنحها مؤسسات دولية كالاتحاد الأوروبي بالتعاون مع جامعات في إفريقيا وآسيا .برامج الابتكار المفتوح: التي تجمع باحثين ومطورين من خلفيات ثقافية مختلفة لتصميم حلول مبتكرة لأزمات الأمن الرقمي .منح خاصة للبحوث في البلوك تشين والتقنيات الكمية: نظرًا لحساسية هذه المجالات وارتباطها المباشر بأمن المعلومات

[1] خليفة عادل.؛**التعاون الدولي في مجال الأمن السيبراني: الإطار النظري والتجارب العالمية**دار الكتب العلمية، بيروت،2022ص. 143–152

والمعاملات .تُشجع هذه المنح على ظهور ما يُعرف بـ"الابتكار المتضامن"، الذي يقوم على تبادل المنافع المعرفية والتقنية بين الدول .

3. تحفيز الشركات متعددة الجنسيات على الاستثمار في الابتكارات الأمنية عبر الحدود

يُعد القطاع الخاص، لاسيما الشركات التكنولوجية الكبرى، فاعلًا رئيسيًا في تطوير أدوات الأمن السيبراني، مما يجعل تحفيزه على الاستثمار في مشاريع دولية ضرورة ملحة. وتشمل وسائل التحفيز :الإعفاءات الضريبية في حال استثمار الشركات في إنشاء مراكز بحثية في الدول النامية .ضمانات قانونية لحماية الملكية الفكرية وتسهيل إجراءات نقل التكنولوجيا .اتفاقيات تبادل المنافع: حيث تساهم الشركات بخبرتها في مقابل تسهيلات سوقية أو دخول أسواق جديدة .وتُعد هذه الاستراتيجية فعالة جدًا لتحقيق نقل تكنولوجي واقعي، وتحفيز القطاع الخاص على لعب دور في التنمية الرقمية المستدامة عالميًا .

4. الشراكة مع القطاع الخاص العالمي

تعتمد هذه الشراكة على إنشاء تحالفات تنفيذية بين الحكومات والشركات التقنية الرائدة مثلMicrosoft و IBMو Ciscoوغيرها، لتطبيق حلول أمنية متقدمة في دول الجنوب. وتشمل هذه الشراكات :برامج التدريب المهني الرقمي: التي تُشرف عليها هذه الشركات وتُنفذ بالتعاون مع الوزارات المحلية .إنشاء مختبرات مشتركة للأمن السيبراني: تُستخدم لتطوير أدوات كشف الهجمات والاستجابة لها .تزويد المؤسسات العمومية بأدوات الحماية الرقمية: في قطاعات مثل التعليم والصحة والطاقة .يُسهم هذا النموذج من الشراكة في دمقرطة التكنولوجيا وتعميم الأمن الرقمي، دون احتكار المعرفة أو تبعية رقمية[1] .

الفرع الثاني

تطوير الكفاءات البشرية في مجال الامن السيبراني على المستوى الدولي

[1]خليفة، عادل. مرجع سابق ص. 167.

في ظل التهديدات السيبرانية المتصاعدة، برزت الحاجة الملحة إلى تطوير الكفاءات البشرية كأحد المحاور الأساسية لتعزيز الأمن السيبراني عالميًا .ويُعدّ الاستثمار في التعليم الأكاديمي والتدريب المتخصص من أبرز السبل لتحقيق هذا الهدف، إذ أن بناء قاعدة من الخبراء المؤهلين يتطلب مناهج تعليمية حديثة، وبرامج دراسية متكاملة تواكب تطور التهديدات وأساليب الحماية. كما يكتسي التدريب المستمر أهمية بالغة في تزويد العاملين بالمهارات التقنية المتقدمة، والاستجابة الفعالة للهجمات المعقدة. لذا، فإن تعزيز التعليم العالي في مجالات الأمن السيبراني، إلى جانب تنظيم ورشات عمل ودورات تخصصية، يشكلان حجر الزاوية في تكوين مورد بشري قادر على حماية الفضاء الرقمي بكفاءة عالية وعلى نطاق دولي.

أولا تعزيز التعليم الأكاديمي والتدريب المتخصص

1-تطوير المناهج الأكاديمية

إدراج برامج جامعية متخصصة في الأمن السيبراني: تسعى العديد من الجامعات الرائدة إلى تقديم برامج دراسات بكاليروس، ماجستير، ودكتوراه في مجال الأمن السيبراني. على سبيل المثال، تقدم جامعة الملك سعود برنامج بكالوريوس في الحوسبة التطبيقية مع مسار في الأمن السيبراني، يهدف إلى تأهيل الكوادر البشرية لمواجهة الهجمات السيبرانية وحماية الفضاء السيبراني .تعاون مع جامعات مرموقة: تسعى بعض المؤسسات التعليمية إلى التعاون مع جامعات عالمية مرموقة مثل جامعة ستانفورد لتطوير المحتوى الأكاديمي وتبادل الخبرات.

أ - توحيد المناهج وفق معايير عالمية مثلNICE ، ISO 27032يُعد توحيد المناهج الأكاديمية في مجال الأمن السيبراني أمرًا بالغ الأهمية لضمان جودة التعليم وتوافقه مع المعايير الدولية .من بين هذه المعايير :إطار عمل القوى العاملة للأمن السيبراني (NICE Framework)يوفر هذا الإطار لغة مشتركة لوصف وظائف الأمن السيبراني والمهارات والمعرفة المطلوبة لكل دور وظيفي .يُستخدم هذا الإطار على نطاق واسع في القطاعات العامة والخاصة والأكاديمية لتطوير القوى العاملة في مجال الأمن السيبراني.
معيار :ISO/IEC 27032 يُركز هذا المعيار على توفير إرشادات لإدارة الأمن السيبراني، بما في ذلك حماية المعلومات الشخصية والأنظمة الإلكترونية .يساعد هذا المعيار المؤسسات على تطوير استراتيجيات فعّالة لمواجهة التهديدات السيبرانية .من خلال اعتماد هذه المعايير، يمكن للمؤسسات التعليمية تطوير مناهج دراسية متوافقة مع

الاحتياجات العالمية، مما يُعزز من كفاءة الخريجين ويُسهل عليهم الاندماج في سوق العمل الدولي

ب -**إنشاء مراكز تدريب متقدمة أو مراكز تميز مثل**: المركز الوطني للأمن السيبراني، برامج تدريب دولية في الاختراق الأخلاقي، الاستجابة للحوادث، الذكاء الاصطناعي تُعتبر مراكز التدريب المتقدمة أو مراكز التميز في الأمن السيبراني من الركائز الأساسية لتطوير المهارات العملية للمتخصصين في هذا المجال .تُقدم هذه المراكز برامج تدريبية متخصصة تشمل :الاختراق الأخلاقي :(Ethical Hacking) تُركز هذه البرامج على تعليم المتدربين كيفية اكتشاف الثغرات الأمنية في الأنظمة بطريقة قانونية وأخلاقية، مما يُساعد المؤسسات على تعزيز أمنها السيبراني .الاستجابة للحوادث (Incident Response):تُعد هذه البرامج ضرورية لتدريب الفرق على كيفية التعامل مع الحوادث الأمنية بسرعة وفعالية، مما يُقلل من الأضرار المحتملة .الذكاء الاصطناعي في الأمن السيبراني: تُستخدم تقنيات الذكاء الاصطناعي لتحليل البيانات واكتشاف التهديدات السيبرانية بشكل أسرع وأكثر دقة .على سبيل المثال، تم إنشاء مركز الأمن السيبراني في تكساس بالتعاون مع جامعة تكساس في سان أنطونيو، والذي يُعتبر من أكبر مراكز الأمن السيبراني في الولايات المتحدة، ويُقدم برامج تدريبية متقدمة في هذا المجال

ج- منح شهادات مهنية عالمية مثل: أخصائي أمن معتمد(CISSP) ، مدير أمن المعلومات المعتمد(CISM) ، اختبار الاختراق الأخلاقي (CEH) تُعد الشهادات المهنية العالمية في مجال الأمن السيبراني من الأدوات الفعّالة لتأكيد كفاءة الأفراد في هذا المجال .من بين هذه الشهادات :أخصائي أمن نظم معلومات معتمد :(CISSP) تُقدم هذه الشهادة من قبل[2](ISC) ، وتُعتبر من أكثر الشهادات شهرة في مجال أمن المعلومات، حيث تُغطي مجالات متعددة مثل إدارة المخاطر، أمن الشبكات، والتشفير .مدير أمن المعلومات المعتمد :(CISM) تُقدم هذه الشهادة من قبلISACA ، وتركز على إدارة أمن المعلومات وتطوير السياسات والإجراءات الأمنية داخل المؤسسات .اختبار الاختراق الأخلاقي المعتمد :(CEH) تُقدم هذه الشهادة من قبل EC-Council، وتُركز على تعليم المتدربين كيفية التفكير والتصرف كقراصنة أخلاقيين لاكتشاف الثغرات الأمنية .الحصول على هذه الشهادات يُعزز من فرص الأفراد في الحصول

على وظائف مرموقة في مجال الأمن السيبراني، ويُعطي الثقة لأصحاب العمل في كفاءة الموظفين[1]

المطلب الثاني

اعتماد اطار قانوني دولي ملزم

نظرًا لتزايد خطورة التهديدات السيبرانية وامتدادها إلى كافة الأبعاد السياسية، الاقتصادية، والقانونية، أصبحت الحاجة ملحة لوضع أطر تنظيمية ومؤسساتية دولية شاملة. فمن جهة، بات من الضروري تطوير منظومة تشريعية دولية متكاملة تعالج مختلف أوجه الجرائم السيبرانية كالتجسس، والتخريب، والقرصنة، وتُرسّخ مبدأ المساءلة القانونية للدول والجهات غير الحكومية، مع العمل على توحيد المعايير الفنية والقانونية بين الدول. ومن جهة أخرى، فإن فعالية هذه المنظومة التشريعية تتطلب دعمًا مؤسساتيًا يتمثل في إنشاء هيئات رقابية دولية متخصصة سياسية، قانونية، وتنفيذية. وعليه، سيتم تناول هذه الرؤية من خلال فرعين رئيسيين: يُعنى الفرع الأول بتطوير منظومة تشريعية دولية خاصة بالأمن السيبراني، بينما يتناول الفرع الثاني ضرورة إنشاء هيئات رقابية متخصصة قادرة على تطبيق القوانين وحسم النزاعات السيبرانية بفعالية وعلى نحو دولي موحد.

الفرع الأول

تطوير منظومة تشريعية دولية خاصة بالأمن السيبراني

لقد بات من الضروري في العصر الرقمي أن تتبنى الدول إطارًا تشريعيًا دوليًا موحدًا لمواجهة التحديات الأمنية في الفضاء السيبراني. ويشمل هذا التطوير عدة جوانب رئيسية:

أولًا: معاهدة دولية خاصة بالجرائم السيبرانية

تُعَدّ الجرائم السيبرانية من أخطر التهديدات العابرة للحدود في العصر الرقمي، نظرًا لقدرتها على اختراق النظم الحيوية للدول، والتأثير على الاقتصاد، والأمن القومي، واستقرار المجتمعات. وتتنوع أشكال هذه الجرائم بين القرصنة(Hacking) ، التخريب المعلوماتي(Cyber Sabotage) ، التجسس

[1] علي، م. ع. ح؛ **الأمنالسيبراني وأساسياته.** دار المناهج للنشر والتوزيع. 2024 ص 73

الإلكتروني(Cyber Espionage)، الابتزاز الرقمي(Ransomware) ، وسرقة الهوية والمعلومات الشخصية. ونظرًا لتطور أساليب هذه الجرائم بشكل سريع، أضحى من المستحيل معالجتها اعتمادًا على القوانين الوطنية وحدها، مما يفرض ضرورة وجود معاهدة دولية شاملة ومُلزِمة تُوحِّد الجهود القانونية والأمنية عالميًا .

1. حاجة المجتمع الدولي إلى إطار قانوني موحّد

إن تفاوت التشريعات الوطنية في تعريف الجريمة السيبرانية، وطرق التحقيق فيها، والعقوبات المقررة، يخلق فراغًا قانونيًا تستغله المجموعات الإجرامية للهروب من الملاحقة أو التمركز في دول تتساهل مع هذه الجرائم. لذا فإن معاهدة دولية تُوحِّد هذه المفاهيم وتضع نظامًا عالميًا للتصنيف والتجريم تعتبر أداة أساسية لتحقيق العدالة الرقمية .

2. محتوى المعاهدة المقترحة

يجب أن تتضمن المعاهدة البنود التالية :تعريف الجرائم السيبرانية: وضع تعريف دقيق ومفصل لكل نوع من أنواع الجرائم الإلكترونية، مثل :القرصنة: أي دخول غير مشروع إلى نظام معلوماتي بنية الإضرار أو التلاعب .التخريب: إتلاف أو تعطيل الأنظمة أو البيانات .التجسس: جمع معلومات سرية أو حساسة بوسائل غير مشروعة .الابتزاز السيبراني: استخدام البيانات المسروقة للضغط على الأفراد أو المؤسسات لدفع فدية .آليات التحقيق والتعاون القضائي: النص على إنشاء قنوات فورية لتبادل المعلومات بين الدول، والسماح بالتحقيق المشترك في قضايا الجرائم العابرة للحدود .تسليم المجرمين السيبرانيين: إدراج بنود ملزمة بشأن تسليم مرتكبي الجرائم السيبرانية، مع ضمان احترام حقوق الإنسان .تدابير الحماية السيبرانية: إلزام الدول الأعضاء بوضع أنظمة وطنية للحماية من الجرائم السيبرانية، وتوفير التكوين المستمر للشرطة والقضاة في هذا المجال .

3. تجربة معاهدة بودابست كنموذج أولي

تمثل اتفاقية بودابست لعام 2001 خطوة أولى في هذا الاتجاه، حيث نصّت على الجرائم المتعلقة بالحواسيب والأنظمة المعلوماتية ووفرت آليات للتعاون القضائي الدولي. لكنها واجهت انتقادات من دول عديدة

(كالصين وروسيا) بسبب غلبة الطابع الغربي في صياغتها، وغياب التوازن في احترام سيادة الدول وحقوق المستخدمين. ومن ثمّ، فإن الحاجة قائمة لتوسيع هذه الاتفاقية أو إبرام معاهدة جديدة أكثر شمولية وتعددية.

4. تحديات وصعوبات إبرام المعاهدة

من أبرز التحديات التي تواجه إنشاء معاهدة دولية للجرائم السيبرانية :الخلاف السياسي بين القوى الكبرى حول تعريف الجرائم السيبرانية، وتحديد المسؤولية، وحدود التدخل الدولي في الفضاء السيبراني .اختلاف البنية التشريعية والتقنية بين الدول المتقدمة والنامية، مما يصعّب التوصل إلى معايير موحدة .التحفظات المرتبطة بسيادة الدولة، حيث تخشى بعض الدول من التدخل في شؤونها السيادية تحت ذريعة مكافحة الجرائم الرقمية .

5. أهمية المعاهدة في بناء أمن سيبراني جماعي

إن إبرام معاهدة دولية ملزمة من شأنه أن :يخلق منظومة ردع قانوني دولية فعالة ضد مرتكبي الجرائم السيبرانية .يعزز التعاون التقني والقضائي بين الدول في التحقيق والاستجابة .يُرسيأسس الشفافية والثقة في الفضاء الإلكتروني، بما يخدم الأمن العالمي[1].

ثانيًا:ترسيخ مبدأ المساءلة القانونية للدول والجهات غير الحكومية مع ازدياد التهديدات السيبرانية العابرة للحدود

لم يعد من الممكن تجاهل مسألة المساءلة القانونية كأحد الأسس التي لا غنى عنها لضمان أمن واستقرار الفضاء الرقمي الدولي. إن مبدأ المساءلة القانونية يُمثل حجر الزاوية في أي نظام قانوني عادل، ويجب أن يمتد ليشمل كل من الدول، والجهات الفاعلة غير الحكومية، وحتى الأفراد الذين يشاركون أو يسهلون الهجمات السيبرانية .

1. مسؤولية الدول في القانون الدولي السيبراني

بموجب قواعد القانون الدولي التقليدي، تكون الدول مسؤولة عن الأفعال التي تُنسب إليها مباشرة، وكذلك تلك التي تقع على أراضيها أو بمساعدتها وتسبب ضررًا لدول أخرى. وفي السياق السيبراني، يجب أن

[1]القمري، ع. م«**الجرائم الإلكترونية في القانون الدولي. مجلة العلوم القانونية**»، جامعة الجزائر1 2020 ، (12)، ص 45–67

تُحمّل الدولة المسؤولية عندما :تتورط مؤسساتها أو أجهزتها الاستخباراتية أو العسكرية في هجمات إلكترونية تستهدف البنية التحتية الحيوية لدول أخرى .تتقاعس عن منع مجموعات إجرامية رقمية (cybercriminal groups)تنشط انطلاقًا من أراضيها .توفر ملاذًا آمنا للمنصات والمخترقين (hackers)دون اتخاذ إجراءات فعالة ضدهم .ولتحقيق ذلك، تُطالب بعض المنظمات الدولية بوضع "مبدأ العناية الواجبة (Due Diligence) "كقاعدة قانونية تلزم الدول بمراقبة نشاط الإنترنت داخل حدودها ومنع الأعمال التي تُهدد الأمن السيبراني الدولي .

2. مساءلة الجهات غير الحكومية والشركات

لا يقتصر التهديد السيبراني على الدول، بل أصبحت الجهات غير الحكومية – من مجموعات هاكرز إلى شركات خاصة توفر أدوات التجسس أو برامج الاختراق – تلعب دورًا متزايدًا. ومن هنا، تبرز الحاجة إلى تحميل هذه الكيانات مسؤولية قانونية عند :تنفيذ أو تسهيل أعمال اختراق إلكترونية مدفوعة أو موجهة .إنتاج وتوزيع أدوات هجومية مثل برامج الفدية أو الفيروسات الموجهة .الامتناع عن حماية بيانات المستخدمين أو الإبلاغ عن الثغرات الأمنية .كما يجب فرض مساءلة على شركات التكنولوجيا الكبرى (مثل شركات استضافة البيانات أو شبكات التواصل الاجتماعي) عندما ترفض التعاون في التحقيقات الدولية، أو تسمح باستخدام منصاتها لنشر البرمجيات الخبيثة أو المحتوى التحريضي الإلكتروني.

3. آليات تنفيذ المساءلة القانونية

لتفعيل هذا المبدأ على المستوى الدولي، من الضروري إنشاء أو تعزيز هياكل وآليات قانونية خاصة، مثل: محكمة دولية للجرائم السيبرانية: تتولى التحقيق والمحاكمة في القضايا الكبرى التي تشمل فاعلين من دول متعددة، على غرار المحكمة الجنائية الدولية .هيئة رقابية دولية مستقلة: ترصد مدى امتثال الدول والجهات الفاعلة للمعايير الأخلاقية والقانونية في الفضاء السيبراني .آلية عقوبات رقمية: تفرض إجراءات مثل حظر استخدام بعض البروتوكولات أو الشبكات، أو إدراج كيانات في "قائمة سوداء سيبرانية" تمنع من التعامل معها دوليًا .

4. التحديات التي تعيق ترسيخ المساءلة السيبرانية

رغم أهمية هذا المبدأ، إلا أن تطبيقه يواجه عقبات معقدة، منها :صعوبة تحديد مصدر الهجمات (Attribution Problem):فقد يتم استخدام تقنيات تمويه عالية تجعل تتبع الجهة المسؤولة شبه مستحيل. الاختلافات في تفسير السيادة الرقمية: حيث تعتبر بعض الدول أن الفضاء السيبراني جزء لا يتجزأ من سيادتها ولا تقبل التدخل الخارجي .تضارب المصالح السياسية والاقتصادية: خاصة عندما تكون الشركات المتورطة تابعة لقوى كبرى تملك نفوذًا على الساحة الدولية .

5. نحو مسؤولية رقمية عالمية مشتركة

في النهاية، لا يمكن تحقيق أمن سيبراني عالمي دون ترسيخ مبدأ "المسؤولية المشتركة والمتفاوتة"، بحيث تتحمل كل دولة وكل جهة فاعلة مسؤوليتها وفقًا لقدراتها وموقعها في البنية الرقمية العالمية. ويجب أن يُدرج هذا المبدأ ضمن أي اتفاقية دولية قادمة لضمان التوازن بين الحقوق الرقمية والواجبات القانونية[1].

ثالثًا: توحيد المعايير الفنية والقانونية) ضمن إطار عمل مرن مثل NIST CSF :أو (ISO 27001

1. أهمية توحيد المعايير في الفضاء السيبراني العالمي

في عصر العولمة الرقمية، لم تعد التهديدات السيبرانية حبيسة المجال الوطني، بل أصبحت تمتد وتتوسع لتطال مؤسسات دولية وأنظمة مالية وصحية وعسكرية في مختلف أرجاء العالم. هذا الواقع المتغير يُحتم على المجتمع الدولي السعي الحثيث نحو توحيد المعايير الفنية والقانونية الخاصة بالأمن السيبراني. ذلك أن غياب التنسيق أو اختلاف القواعد بين دولة وأخرى يولد ثغرات كبيرة تسمح للهجمات الإلكترونية بالنجاح والتكاثر .التوحيد لا يعني فرض نموذج واحد صارم، بل هو توجه نحو صياغة أطر مرنة وعامة تكون قابلة للتكييف بحسب خصوصية كل دولة أو مؤسسة، لكنها في الوقت ذاته تضمن الحد الأدنى من التكامل والتفاهم السيبراني بين مختلف الأطراف الدولية .

2. الأطر الفنية المعيارية: تعمل الأطر الفنية المعيارية بأسلوب مرن يتدرج من التنوع الى التماثل ومن بين اهم هذه الأطر نذكر

[1] زروقي، ل..**« المسؤولية القانونية عن الهجمات السيبرانية في القانون الدولي العام.»**. مجلة دراسات قانونية وسياسية، جامعة باتنة 2021 ، (15)، ص 89–110.

أ. **إطارNIST CSF** صدر عن المعهد الوطني الأمريكي للمعايير والتكنولوجيا (NIST) عام 2014، وتم تحديثه عام 2018. يتميز هذا الإطار بمرونته وكونه قائمًا على خمسة محاور أساسيةIdentify :(تحديد): تحديد الأصول الرقمية والبيئة المعلوماتية والمخاطر المرتبطة بهاProtect .(الحماية): وضع إجراءات الحماية التقنية والإداريةDetect .(الكشف): آليات اكتشاف الهجمات ومحاولات الاختراقRespond . (الاستجابة): الخطوات العملية للاستجابة للحوادث السيبرانيةRecover .(التعافي): ضمان استعادة الأنظمة واستمرار الأعمال بعد الهجوم .هذا الإطار لا يفرض إجراءات تقنية محددة، بل يوجه المؤسسات لاختيار الحلول المناسبة بناءً على قدراتها وظروفها، مما يجعله قابلاً للتطبيق في الدول المتقدمة والنامية على حد سواء

ب. **معيارISO/IEC 27001** يُعد هذا المعيار الدولي من أشهر المعايير في مجال إدارة أمن المعلومات، وقد تبنته آلاف المؤسسات عبر العالم. يهدف إلى :إنشاء نظام متكامل لإدارة أمن المعلومات .(ISMS) تحديد وتحليل المخاطر وتقييمها ومعالجتها .حماية سرية وتكامل وتوافر المعلومات .التحسين المستمر من خلال دورات التدقيق والمراجعة .ما يميز ISO 27001 هو قابلية المؤسسة للحصول على شهادة دولية تؤكد التزامها بالمعايير الأمنية، مما يُعزز الثقة مع الشركاء المحليين والدوليين.

3. التوحيد القانوني: الحاجة إلى تقارب تشريعي عالمي

رغم التقدم الحاصل في المجال الفني، إلا أن الجوانب القانونية المتعلقة بالأمن السيبراني ما تزال تشهد تفاوتًا كبيرًا بين الدول، وهو ما يُعرقل ملاحقة مرتكبي الجرائم الإلكترونية، خصوصًا حين تكون الهجمات عابرة للحدود. لذا فإن توحيد المصطلحات والمفاهيم القانونية يُعد شرطًا ضروريًا لتفعيل التعاون الدولي. بعض جوانب التوحيد المقترحة :تحديد قانوني دقيق لمصطلحات مثل: "القرصنة"، "الهجوم السيبراني"، "البيانات الحساسة"، و"البنية التحتية الرقمية الحيوية ."توحيد الإجراءات المتعلقة بتبادل الأدلة الرقمية، وحمايتها، وتقديمها أمام القضاء .صياغة قوانين مشتركة لحماية الخصوصية الرقمية، خاصة في ما يتعلق باستخدام البيانات البيومترية أو الصحية أو المالية .تفعيل اتفاقيات قضائية ثنائية أو متعددة الأطراف تُمكن من تسليم المجرمين السيبرانيين .

4. أبعاد التحدي: تباين القدرات والخصوصيات السيادية

يبقى التحدي الأبرز في توحيد المعايير هو التفاوت الكبير في القدرات التكنولوجية والتشريعية بين الدول. فالدول المتقدمة تمتلك بنية تحتية إلكترونية متطورة، وأجهزة أمنية مختصة، ومختبرات رقمية عالية الكفاءة، بينما تعاني الدول النامية من نقص في الكفاءات والموارد. هذا التفاوت يجعل بعض الدول تتحفظ على تبني معايير موحدة خشية المساس بسيادتها أو كشف نقاط ضعفها .من جهة أخرى، تطرح بعض الدول، مثل روسيا والصين، تحفظات على الأطر الغربية، وتدعو إلى اعتماد أطر دولية تكون برعاية الأمم المتحدة بدل المعاهدات الإقليمية أو الثنائية، لضمان الشفافية والتوازن .

5. فوائد التوحيد على المدى البعيد

رغم التحديات، إلا أن التوحيد التدريجي للمعايير الفنية والقانونية سيحقق مكاسب كبرى، من أهمها:تعزيز الثقة الرقمية بين الدول والشركات .تسهيل التعاون الفني والقضائي في مواجهة الهجمات .خفض التكاليف الاقتصادية الناجمة عن الاختراقات .تعزيز قدرات الدول النامية من خلال آليات المساعدة والتدريب .تحقيق العدالة الدولية في مكافحة الجريمة السيبرانية .

6. نحو هيئة دولية معيارية

يقترح الباحثون إنشاء هيئة دولية متخصصة بالأمن السيبراني، تحت مظلة الأمم المتحدة، تُكلف بما يلي: تحديث وتطوير المعايير الفنية .اقتراح نماذج تشريعية مرنة للدول .مراقبة التزام الدول الكبرى بالمعايير الأخلاقية والتقنية .إصدار تقارير سنوية حول المخاطر السيبرانية العالمية[1].

الفرع الثاني

إنشاء هيئات رقابية متخصصة (سياسية، قانونية، تنفيذية)

أصبح الأمن السيبراني يشكل اليوم أحد المحاور الأساسية في بنية العلاقات الدولية المعاصرة، حيث لم تعد التهديدات السيبرانية محصورة في أبعاد تقنية ضيقة، بل أصبحت تنطوي على أبعاد سياسية، قانونية، وأمنية بالغة التأثير. ومن ثمّ، فإن مواجهة هذه التهديدات تتطلب أكثر من مجرد تقنيات دفاعية؛ بل تحتاج إلى هيئات رقابية متخصصة تُشرف على سن التشريعات، فض النزاعات، وتفعيل التعاون التنفيذي

أولاً: إنشاء منظمة دولية للأمن السيبراني في عصر الثورة الرقمية

[1]International Organization for Standardization. (2013). ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements. ISO

أصبح الفضاء السيبراني ساحة رئيسية للتفاعل بين الدول، الشركات، والأفراد. ومن دون إطار قانوني وتنظيمي دولي موحد، يمكن أن تتفاقم تهديدات الهجمات السيبرانية بشكل سريع، مما يُشكل تهديدًا حقيقيًا للأمن والسلم الدوليين. بناءً على ذلك، تُعتبر فكرة إنشاء منظمة دولية للأمن السيبراني خطوة هامة لضمان إدارة أكثر فعالية للفضاء الرقمي وتعزيز التعاون بين الدول في مواجهة التهديدات السيبرانية.

1. الحاجة إلى إنشاء منظمة دولية

تُعاني العديد من الدول من تحديات متزايدة في إدارة الأمن السيبراني بسبب التنوع في الأنظمة التقنية والقانونية. الهجمات السيبرانية المعقدة التي يمكن أن تعبر الحدود بسرعة، مثل الهجمات على البنية التحتية الحيوية، سرقة البيانات الشخصية، والقرصنة الإلكترونية، تتطلب استجابة منسقة وموحدة من قبل المجتمع الدولي. غير أن التعامل مع هذه التهديدات يتطلب منظمة دولية تتمتع بالقدرة على تنظيم الجهود الدولية، وتقديم الدعم الفني للدول، والمساعدة في صياغة قوانين سيبرانية موحدة.

2. مهام المنظمة الدولية المقترحة

المهام الأساسية التي قد تقوم بها المنظمة الدولية للأمن السيبراني تشمل :تنسيق الجهود الدولية لمواجهة التهديدات السيبرانية: تسعى المنظمة إلى أن تكون منصة تُنسق من خلالها الدول جميع الجهود لمكافحة الجرائم السيبرانية، بدءًا من التحقيقات الجنائية الرقمية وصولًا إلى التصدي للهجمات السيبرانية العالمية. وضع معايير سيبرانية عالمية: أحد الأدوار الرئيسية للمنظمة هو وضع معايير دولية تتعلق بالأمن السيبراني، بما في ذلك الاستجابة للهجمات، تعزيز الأمن المعلوماتي، والوقاية من التهديدات. المعايير يمكن أن تشمل جوانب تقنية (مثل تقنيات التشفير) وكذلك إدارية (مثل إدارة المخاطر السيبرانية) .تقديم الدعم الفني والتدريبي للدول النامية: كثير من الدول النامية تفتقر إلى الموارد المالية والتقنية لتطوير قدراتها في مجال الأمن السيبراني. ومن ثم، يمكن أن تُقدم المنظمة دورات تدريبية و ورش عمل و استشارات تقنية لمساعدتها على رفع مستوى قدرتها على مواجهة الهجمات .إرساء أسس التعاون الدولي: من خلال عملها كحلقة وصل بين الدول والمؤسسات الدولية، يمكن للمنظمة تسهيل إنشاء اتفاقيات متعددة الأطراف، مثل تبادل المعلومات الرقمية، أو آليات تسليم المجرمين السيبرانيين .مراقبة التزام الدول بالمعايير الدولية: أحد المهام الهامة للمنظمة هو إنشاء آلية مراقبة دولية تتابع التزام الدول بتطبيق المعايير الخاصة بالأمن

السيبراني. في حال اكتشاف أي انتهاك، يمكن للمنظمة تقديم تقارير أو إجراءات تصحيحية وفقًا لما يقرره الأعضاء .

3. الهيكل التنظيمي للمنظمة الدولية

من أجل أن تكون المنظمة فعّالة في تحقيق مهامها، يجب أن تمتلك هيكلًا تنظيميًا مرنًا وقويًا في نفس الوقت. الهيكل يمكن أن يشمل :الهيئة التنفيذية: الهيئة التي تكون مسؤولة عن تنفيذ القرارات والإشراف على عمليات المنظمة .اللجنة الاستشارية التقنية: تتكون من خبراء في مجالات الأمن السيبراني، التحقيقات الجنائية الرقمية، و التشريعات السيبرانية، تقدم استشارات فنية وتنظيمية .المجلس التشريعي: يتكون من ممثلين عن الدول الأعضاء ويعمل على وضع السياسات والقوانين التي تحكم عمل المنظمة.المنتدى العام: يمثل منصة تجمع كل الأطراف المعنية، بما في ذلك الحكومات، الشركات، والقطاع المدني، من أجل تبادل الخبرات و التعاون المشترك .

4. التحديات المرتبطة بتأسيس منظمة دولية للأمن السيبراني

رغم أهمية إنشاء منظمة دولية، إلا أن هناك عدة تحديات قد تعرقل إرساء مثل هذه الهيئة، من أبرزها: الاختلافات القانونية والسياسية بين الدول: تختلف القوانين والأنظمة السيبرانية بين الدول، مما يجعل الاتفاق على معايير موحدة أمرًا صعبًا. بعض الدول قد تتردد في الانضمام إلى معاهدات دولية بسبب مخاوف من التحكم الخارجي أو المساس بسيادتها الرقمية .القدرة المالية واللوجستية: إنشاء منظمة دولية يتطلب موارد ضخمة من حيث التمويل والإدارة. العديد من الدول قد تواجه صعوبة في المساهمة في هذه الجهود المالية. الحاجة إلى آلية فرض العقوبات: بدون آلية فعّالة لفرض العقوبات على الدول أو الكيانات التي ترفض التعاون، قد تظل التهديدات السيبرانية تنتشر دون رادع .التهديدات المتطورة والمتغيرة: الطبيعة المتغيرة والمبتكرة للهجمات السيبرانية تجعل من الصعب على أي منظمة أن تظل على رأس آخر التطورات التقنية، وبالتالي تصبح هناك حاجة دائمًا إلى تحديث المعايير والإجراءات بشكل دوري.

5. الفوائد المتوقعة من إنشاء منظمة دولية للأمن السيبراني

إنشاء مثل هذه المنظمة يفتح الباب أمام عدد من الفوائد الكبيرة التي ستعود على العالم بشكل عام، من أهمها: تعزيز التعاون بين الدول: يوفر إطارًا منظمًا للتعاون الأمني والتقني بين الدول.تقليل تأثير الهجمات

السيبرانية: بوجود هيكل مرن، ستتمكن الدول من الاستجابة بشكل أسرع وأكثر فعالية.دعم الدول النامية: ستتيح الدول النامية فرصًا لتطوير قدراتها في المجال الرقمي مما يساعدها على حماية بنيتها التحتية الحيوية .تحقيق العدالة العالمية: من خلال إنشاء آليات للعدالة والمساءلة على المستوى الدولي[1]

ثانيًا:إنشاء هيئات قضائية دولية للفصل في منازعات الأمن السيبراني

إن تزايد التهديدات السيبرانية التي تستهدف الأفراد والدول والشركات على حد سواء قد فاقم الحاجة إلى وجود هيئات قضائية دولية مختصة بالفصل في النزاعات المتعلقة بالأمن السيبراني. فالأمن السيبراني لا يعترف بالحدود الجغرافية أو السياسية، مما يجعل من الضروري إيجاد آلية قضائية دولية تتعامل مع الجرائم السيبرانية التي تؤثر على أكثر من دولة في وقت واحد. وفي ظل غياب آليات قضائية فعالة على المستوى الدولي، تتعرض الحقوق الرقمية للأفراد والكيانات في الدول المختلفة للخطر .

1. هيئات تحكيم دولية للأمن السيبراني

تُعد الهيئات التحكيمية الدولية إحدى الحلول المطروحة لحل المنازعات في مجال الأمن السيبراني. هذه الهيئات تقوم على التحكيم الدولي بين الأطراف المتنازعة، مما يسمح بحل القضايا خارج إطار المحاكم التقليدية، ما يقلل من التوترات بين الدول ويسرع من إجراءات الفصل في النزاعات .أهمية هذه الهيئات تشمل :توفير حل سريع وفعال: حيث يمكن أن تُساعد في حل النزاعات المرتبطة بالجرائم السيبرانية بسرعة وكفاءة، دون الحاجة إلى المرور بالإجراءات المعقدة التي قد تستغرق وقتًا طويلاً .المرونة في القوانين: يُمكن للهيئات التحكيمية أن تضع قواعد خاصة بها تتناسب مع طبيعة النزاعات السيبرانية، بعيدًا عن القيود التي قد تفرضها الأنظمة القضائية التقليدية .حماية حقوق الأطراف التجارية: كثير من الشركات الدولية تواجه تهديدات سيبرانية في معاملاتها العابرة للحدود. الهيئات التحكيمية يمكن أن تقدم حلولًا لهذه النزاعات بين الشركات أو بين الشركات والحكومات .

2. محكمة جنائية سيبرانية دولية

بالنسبة للجرائم السيبرانية التي تنطوي على أضرار جسيمة على الأمن الدولي، مثل الهجمات الإلكترونية التي تؤثر على البنية التحتية الحيوية أو أنظمة الدفاع الوطنية، فإنه من الضروري إنشاء محكمة جنائية سيبرانية دولية لتكون مكلفة بمحاكمة مجرمي الإنترنت الذين يرتكبون هذه الجرائم.تتخصص هذه المحكمة

[1]Kello, L. The Virtual Weapon and International Order. Yale University Press 2017

في محاكمة المجرمين السيبرانيين الدوليين الذين يشنون هجمات على نطاق واسع، مما يؤثر على الدول والشعوب بشكل كبير. في هذا السياق، سيكون دور المحكمة هو تقديم العدالة للضحايا، ومنع الإفلات من العقاب .أهداف إنشاء المحكمة :محاكمة الأفراد والكيانات: خاصة في الجرائم السيبرانية الكبرى مثل الهجمات الرقمية على البنية التحتية الوطنية، الأنظمة الحكومية، أو الانتخابات الرقمية .تطبيق العقوبات المناسبة: مثل السجن أو الغرامات المالية على الأفراد أو الكيانات التي تُنتهك منها الأمن السيبراني

أ- الدور المتوقع :يمكن أن تكون محكمة جنائية سيبرانية دولية مسؤولة عن محاكمة مجرمي الإنترنت الذين ينفذون هجمات تهدد الاستقرار السياسي والاقتصادي في دول معينة. قد تشمل القضايا التي تتم محاكمتها: الجرائم ضد الأمن القومي: مثل الهجمات على الأنظمة الحكومية أو البنية التحتية العسكرية .الاختراقات المالية: مثل الهجمات على البنوك أو الأنظمة المالية التي تؤدي إلى خسائر مالية ضخمة .التلاعب بالانتخابات: من خلال هجمات سيبرانية تُنفذ للتأثير على العملية الانتخابية في الدول الديمقراطية

ب-تحديات إنشاء محكمة جنائية سيبرانية دولية ورغم الأهمية الكبيرة لهذه المحكمة، فإن إنشاء محكمة جنائية سيبرانية دولية يواجه عدة تحديات :

-الاختلافات القانونية بين الدول: كل دولة تتمتع بتشريعاتها الخاصة التي قد تختلف فيما يتعلق بقضايا التحقيقات السيبرانية أو العقوبات المفروضة على الجرائم السيبرانية.

-الاعتبارات السيادية: بعض الدول قد تتردد في الانضمام إلى محكمة جنائية سيبرانية دولية بسبب المخاوف من فقدان سيادتها القضائية.

-صعوبة تتبع المهاجمين: في الهجمات السيبرانية، غالبًا ما يتخذ المهاجمون إجراءات إخفاء متطورة مثل استخدام تقنيات إخفاء الهوية (VPN) أو الهجمات المجهولة

-الاختصاص القضائي: في الجرائم السيبرانية العابرة للحدود، يصبح تحديد الاختصاص القضائي معقدًا بسبب الطبيعة غير المحددة للفضاء الرقمي.

3. الحاجة إلى تحالفات دولية لتعزيز دور الهيئات القضائية

من أجل ضمان نجاح الهيئات القضائية الدولية في التعامل مع القضايا السيبرانية، يجب تعزيز التعاون بين الدول، وذلك من خلال إنشاء اتفاقيات دولية تتيح تبادل الأدلة الرقمية، وتبادل المعلومات حول الجرائم السيبرانية، وتسليم المجرمين عبر الحدود .تحالفات محتملة :إجراءات تسليم المجرمين: مثل الاتفاقات الثنائية أو الإقليمية التي تسهل تسليم المجرمين السيبرانيين من دولة إلى أخرى .تبادل الأدلة الرقمية: عبر

إطار قانوني يحدد كيفية التعامل مع الأدلة السيبرانية، مع ضمان حماية حقوق الأفراد .تعزيز التعاون مع منظمات دولية: مثل الإنتربول أو اليوروبول لتنسيق الجهود بين الدول لمكافحة الجرائم السيبرانية.[1]

ثالثًا :إيجاد آلية تنفيذية قانونية سريعة

في ظل التهديدات المتنامية في الفضاء السيبراني، لم يعد الاكتفاء بوضع تشريعات دولية كافيًا لمواجهة التحديات المعقدة التي تفرضها الجرائم الإلكترونية، بل أصبح من الضروري إرساء آليات تنفيذية فعّالة وسريعة الاستجابة، قادرة على مواجهة التطورات التقنية وتجاوز الحواجز التقليدية للسيادة الوطنية والاختصاص القضائي .

1. تعزيز التعاون الدولي الفعّال

من أبرز الركائز في أي آلية تنفيذية ناجعة، وجود شبكات دولية متكاملة تربط بين مختلف الجهات الفاعلة على المستوى العالمي، سواء كانت دولًا، أو منظمات أمنية، أو كيانات خاصة. وتتمثل أهمية هذا التعاون في :الاستجابة الفورية للهجمات: عبر قنوات اتصال دبلوماسية وتقنية مستعدة لتبادل المعلومات حول الحوادث السيبرانية بمجرد وقوعها .تشكيل فرق طوارئ مشتركة: مثل فرق الاستجابة للطوارئ السيبرانية (CERTs)العابرة للحدود، التي تتمتع بصلاحيات تدخل سريعة عبر الدول الأعضاء .إنشاء مراكز قيادة عمليات سيبرانية دولية تعمل على تنسيق الجهود الفنية والاستخباراتية لمواجهة الهجمات المتزامنة.

2. منح صلاحيات فورية للجهات المختصة

تحتاج الدول إلى إصلاحات قانونية داخلية تسمح للأجهزة المختصة، مثل أجهزة مكافحة الجريمة الإلكترونية، باتخاذ إجراءات سريعة ومرنة، على غرار :إجراءات تحفظية فورية (تجميد الحسابات، حجز الخوادم، تعطيل المواقع المشبوهة .(أوامر ملاحقة دولية إلكترونية تصدر في وقت قياسي لتتبع مرتكبي الجرائم داخل أو خارج البلاد .تطبيق نماذج إنذار مبكر سيبراني يُبلغ السلطات عند رصد نشاط غير طبيعي أو محاولة اختراق كبرى .

3. إعادة تعريف مفهوم "الاختصاص القضائي

[1] علياً،**الأمنالسيبراني: التحديات القانونية والأمنية في العصر الرقمي.**مركز البحوث القانونية، القاهرة 2021 ص 22-33

الطبيعة غير الإقليمية للفضاء السيبراني تفرض على المنظومة القانونية أن تعيد النظر في الأسس التقليدية للاختصاص. لذا تقترح المبادرات الدولية :مبدأ "الاختصاص المستند إلى الضرر": بحيث يمكن لدولة ما أن تتدخل قانونيًا إذا تعرضت بنيتها التحتية للضرر، حتى لو كان مصدر الهجوم خارجيًا .اختصاص تعاوني متعدد الجنسيات: حيث يتم التحقيق والحكم بناءً على لجنة قانونية مختلطة تمثل عدة دول معنية بالقضية.

4. دمج الذكاء الاصطناعي والأدوات الرقمية في الإجراءات القانونية

تتطلب آلية تنفيذية فعّالة توظيف أحدث الأدوات التقنية في مجال التحقيق السيبراني، مثل :خوارزميات التعلم الآلي لتحليل الأنماط السلوكية للمهاجمين والتنبؤ بتحركاتهم .أنظمة تتبع العملات الرقمية لتحديد تمويل الجرائم السيبرانية مثل الفدية الإلكترونية .(ransomware) نظم محاكاة افتراضية تُستخدم لمحاكاة الهجمات واستكشاف الثغرات واستباق الأخطار .

5. تسريع إصدار وتنفيذ الأحكام القضائية

واحدة من العقبات الكبرى في ملاحقة مجرمي الإنترنت هي البطء الإجرائي. لذلك، تقترح بعض الدول والمنظمات :إنشاء محاكم متخصصة في الجرائم السيبرانية تعمل على مدار الساعة، وتستفيد من البنية التحتية الرقمية للتعامل مع القضايا بشكل سريع .تفعيل آليات التحكيم السيبراني كبديل لحل النزاعات الإلكترونية بين الدول والشركات والأفراد .إنشاء قوائم سوداء دولية تشمل القراصنة والمجموعات السيبرانية، ويتم تحديثها بشكل دوري لتسهيل التعقب والمحاسبة .

6. إطار عمل دولي ملزم للتنفيذ

رغم وجود اتفاقيات مثل "نداء باريس"، إلا أن فعاليتها تبقى محدودة في غياب إلزام قانوني، لذا من المقترح أن يتم :الربط بين الاتفاقيات الدولية ومنظمة التجارة العالمية أو مجلس الأمن لجعل الامتثال لهذه الآليات شرطًا للاستفادة من التعاون الدولي .فرض عقوبات سيبرانية دولية ضد الدول أو الكيانات التي ترفض التعاون أو توفر ملاذًا آمنًا لمجرمي الإنترنت .إشراف لجنة تنفيذية عالمية تتمتع بصلاحيات فرض ومراقبة تنفيذ القوانين والجزاءات في إطار الأمم المتحدة .

7. مراعاة التوازن بين الحريات العامة والأمن

من المهم أن تكون هذه الآليات التنفيذية مصممة بما يضمن :حماية خصوصية الأفراد وعدم التعدي على حرية التعبير .توفير آليات رقابة ومساءلة قانونية تضمن عدم استغلال التدخلات السيبرانية من قبل الحكومات أو الشركات لأغراض غير مشروعة .إنشاء هيئة أممية لمراقبة شرعية التنفيذ، تعمل على التدقيق في حالات التدخل ومنح التصاريح الدولية للتنفيذ[1].

ملخص الفصل الثاني

يتناول الفصل الثاني من مذكرة "تأثير الأمن السيبراني على العلاقات الدولية" التحديات الكبرى التي تواجه إدارة الأمن السيبراني على الصعيد الدولي، من بينها التحديات الاقتصادية الناتجة عن هشاشة البنى التحتية الرقمية، والتقنية المتقدمة التي تستغلها الهجمات السيبرانية، بالإضافة إلى التحديات القانونية بسبب غياب إطار دولي موحد يُنظّم الفضاء السيبراني، وصعوبة تحديد المسؤولية القانونية في الجرائم العابرة للحدود. كما يشير الفصل إلى التحديات السياسية والدبلوماسية، حيث أصبح الأمن السيبراني أداة جديدة في الصراع بين الدول والتدخل في شؤونها الداخلية. ويقترح الفصل سبلًا لمواجهة هذه التحديات، من أبرزها تعزيز التعاون الدولي من خلال التحالفات وتبادل المعلومات، وتطوير تشريعات دولية موحدة، إلى جانب بناء قدرات وطنية لمجابهة الهجمات وتحقيق "المرونة السيبرانية" التي تضمن استمرارية الأنظمة والمؤسسات في ظل التهديدات المتزايدة.

[1] العجالعبد الحكيم.: **العدالة الجنائية في مواجهة الجرائم السيبرانية: دراسة قانونية مقارنة**دار الجامعة الجديدة، الإسكندري 2022ة ص 66-55

خاتمة

لقد شكّل الأمن السيبراني في العقود الأخيرة أحد أهم التحديات التي فرضت نفسها بقوة على الساحة الدولية، نظرًا لتنامي استخدام الفضاء الرقمي في كافة مناحي الحياة، بما فيها العلاقات السياسية، والاقتصادية، والعسكرية، وحتى الثقافية والدبلوماسية. ومع تصاعد الهجمات السيبرانية، وازدياد قدراتها التخريبية، بات من الضروري الوقوف عند هذه الظاهرة تحليلاً وتفكيكًا، بهدف فهم أبعادها، وآثارها، والآليات الممكنة لمواجهتها من منظور دولي شامل .لقد انطلقت إشكالية هذا البحث من التساؤل الجوهري: ما هو تأثير الأمن السيبراني على العلاقات الدولية، وكيف يمكن مواجهته ضمن أطر قانونية وتعاونية دولية؟ وقد حاول البحث من خلال مباحثه المختلفة أن يستعرض أبرز التهديدات السيبرانية التي طالت الدول والمجتمعات، وكشفت هشاشة البنى التحتية التكنولوجية، وعرّت الثغرات القانونية والمؤسساتية على المستوى العالمي، مما جعل الأمن السيبراني ليس مجرد مسألة تقنية، بل قضية استراتيجية ذات أبعاد قانونية، سياسية، وأمنية.كما أظهر البحث أن الأمن السيبراني قد أضحى من أبرز العوامل المؤثرة في هندسة العلاقات الدولية، حيث لا يقتصر تأثيره على الأمن القومي للدول فقط، بل يمتد ليشمل إعادة تشكيل موازين القوى، وأنماط التحالفات، ومستويات الثقة المتبادلة بين الفاعلين الدوليين. إن تصاعد الأعمال العدائية في الفضاء السيبراني بين الدول، مثل عمليات التجسس الإلكتروني، وزرع البرمجيات الخبيثة، واختراق الانتخابات، أدى إلى توتر العلاقات، وتهديد السلم العالمي، لا سيما في ظل غياب إطار قانوني دولي ملزم وشامل .ورغم التحديات، فإن الأمن السيبراني يمكن أن يكون أيضًا أداة لتعزيز التعاون الدولي، إذا ما تم تبنّي مقاربات تشاركية قائمة على الشفافية، وبناء الثقة الرقمية، وتوحيد المفاهيم القانونية والممارسات التقنية. وهنا تظهر أهمية العمل متعدد الأطراف، وتعزيز دور المنظمات الدولية، وإقامة اتفاقيات دولية متخصصة .وانطلاقًا من ذلك،

نعرض فيما يلي النتائج المستخلصة من البحث، متبوعة بأبرز التوصيات والاقتراحات العملية التي يمكن أن تساهم في صياغة سياسة دولية أكثر فعالية واستدامة في مواجهة تهديدات الأمن السيبراني

النتائج المستخلصة

-تحول الأمن السيبراني إلى عنصر مركزي في العلاقات الدولية، حيث لم يعد شأنًا داخليًا للدول، بل مسألة عالمية تتجاوز الحدود والسيادات التقليدية.

-الهجمات السيبرانية تمثل تهديدًا مباشرًا للأمن القومي والسيادة الرقمية، خاصة عند استهداف البنى التحتية الحيوية أو التأثير على العمليات الديمقراطية كالإنتخابات.

-غياب إطار قانوني دولي موحد ينظم الفضاء السيبراني يؤدي إلى فوضى قانونية، واستغلال الثغرات لصالح القوى الكبرى.

-وجود تفاوت كبير بين الدول في القدرات السيبرانية، مما يكرس الهيمنة الرقمية ويعمّق الفجوة التكنولوجية بين الدول المتقدمة والنامية.

-التعاون الدولي في مجال الأمن السيبراني ما زال محدودًا وضعيف التنسيق، رغم تنامي التهديدات العابرة للحدود.

التوصيات

-صياغة اتفاقية دولية شاملة للأمن السيبراني، تحت إشراف الأمم المتحدة، تتضمن تعريفات موحدة، وآليات للمساءلة، وأطرًا للتعاون التقني والقانوني.

-إنشاء هيئة دولية دائمة للأمن السيبراني تشبه الوكالة الدولية للطاقة الذرية، تُعنى بمراقبة الأنشطة في الفضاء الرقمي وتقييم التهديدات.

-إدماج الأمن السيبراني في سياسات العلاقات الخارجية والدبلوماسية الوقائية، من خلال تعزيز الثقة الرقمية وآليات فض النزاعات السيبرانية.

-تعزيز قدرات الدول النامية في المجال السيبراني من خلال برامج التكوين ونقل التكنولوجيا، وتقليص الفجوة الرقمية بين الشمال والجنوب.

-توسيع التعاون الإقليمي والدولي بين الحكومات، والقطاع الخاص، والمجتمع المدني لبناء بيئة رقمية أكثر أمنًا واستقرارًا.

-إطلاق حملات توعية رقمية دولية حول مخاطر الهجمات السيبرانية، وحماية البيانات، والدفاع الرقمي الأخلاق

قائمة المصادر و المراجع

1-المصادر والمراجع بالعربية

أ,ولا- المصادر

1-التقارير الدولية

منظمة التعاون والتنمية الاقتصادية؛ تقرير حول حماية البنى التحتية الرقمية الحيوية، ترجمة مركز دراسات الوحدة العربية، بيروت 2018، ص 46-55

تقرير الأمن الدبلوماسي الأمريكي، 2023 الهيئة الوطنية للأمن السيبراني، تقرير حول جاهزية الاستجابة للحوادث السيبرانية، الرياض: المركز الوطني للاستجابة للطوارئ الإلكترونية، 2023، ص 42–85

ثانيا- المراجع

1-الكتب

أ. الكتب العامة

عبد الله الجلود؛ الاقتصاد الرقمي والابتكار التكنولوجي، مكتبة الرشد، الرياض، 2021، ص 113-119 عبد العزيز اللويحق؛ مستقبل التقنيات الناشئة: الذكاء الاصطناعي، البيانات الضخمة، والميتافيرس، مركز الملك عبد الله للدراسات، 2022، ص 28-

36 عبد العظيم حسام؛ التجارة الإلكترونية: النظرية والتطبيق، القاهرة: دار الكتب العلمية، 2018، ص 220-

225 نبيل صلاح العربي؛ الاقتصاد الرقمي: المبادئ والتطبيقات، القاهرة: مكتبة النهضة المصرية، 2017، ص 180-200

عبد الحافظ أحمد؛ أمن المعلومات وحمايتها في التجارة الإلكترونية، القاهرة: دار الفكر الجامعي، 2019، ص 44-54

زكريا عماد؛ أمن المعلومات وحماية الخصوصية في التجارة الإلكترونية، القاهرة: مكتبة الشروق الدولية، 2020، ص 188

سليم علي؛ التجارة الإلكترونية الحديثة: الواقع والمستقبل، بيروت: دار الفجر للنشر، 2016 القيسي يحيى؛ التجارة الإلكترونية: المفاهيم والتطبيقات، عمان: دار وائل للنشر، 2015، ص 89

الجندي فؤاد؛ أمن المعلومات في التجارة الإلكترونية، القاهرة: دار العلوم للنشر، 2021، ص 41

نعيمي عادل؛ التجارة الإلكترونية وحماية البيانات الشخصية، عمان: دار جروس للنشر، 2019، ص 200

قاسم مصطفى؛ حماية البرمجيات الرقمية وبراءات الاختراع، بيروت: دار الساقي للنشر، 2017، ص 83-95

محمود حسين؛ تهديدات الأمن السيبراني: التحديات والعواقب القانونية، دار الجليل للنشر، عمان، 2021، ص 18-20

سعيد جمال؛ الأمن السيبراني: التحديات والفرص في العلاقات الدولية، دار الفكر العربي، 2021، ص 75-88

حسن عبد الله؛ السياسة السيبرانية: استراتيجيات الحروب الرقمية وأثرها في العلاقات الدولية، دار العلوم للنشر، بيروت، 2022، ص 220

خالد الزبيدي؛ الحروب السيبرانية: مخاطرها وأبعادها الإستراتيجية، المركز العربي للأبحاث ودراسة السياسات، بيروت، 2022، ص 199-202

سامي حسن العلي؛ الأمن السيبراني في ظل العولمة الاقتصادية، دار المنهل العربي، بيروت، 2021، ص 45-55

عبد الرحمن مصطفى جابر؛ الاقتصاد الرقمي والأمن السيبراني: بين التوسع والتحديات، دار الفكر العربي، القاهرة، 2022، ص 78-85

عبد القادر عموري؛ تداعيات الهجمات السيبرانية على مناخ الاستثمار الدولي، دار الهدى للنشر، الجزائر، 2023، ص 17

محمد سعيد الإدريسي؛ الجرائم الإلكترونية وأثرها على كفاءة التجارة الدولية، دار الإبداع الأكاديمي، القاهرة، 2023 عباسي محمد؛ التحديات الاقتصادية في العالم المعاصر: التكاليف والتمويل، الاقتصاد الدولي، 2020، ص 43

سامي فاطمة؛ دور التمويل الدولي في النمو الاقتصادي: التحديات والفرص، دوريات التنمية الاقتصادية، العدد 32، 2019، ص 19-33

الجمعية العربية للاقتصاد والتنمية؛ المصادر المستدامة للتمويل في الدول النامية، دراسات اقتصادية دولية 2018، الجزء الثاني، ص

198 زينب سارة؛ التحديات الضريبية في التجارة الإلكترونية: دراسة تطبيقية، 2021، ص 29

المنصور أحمد؛ أثر تقلبات أسعار الشحن على التجارة الإلكترونية، 2021، ص 31

مصطفى عبد الحميد؛ الأمن السيبراني كأولوية وطنية في العالم العربي، دار الفكر العربي للنشر والتوزيع، القاهرة، 2021، ص 121

ب. الكتب الخاصة

سامي حسن العلي؛ الأمن السيبراني في ظل العولمة الاقتصادية، دار المنهل العربي، بيروت، 2021، ص 45-55 محمد علي عمر؛ الأمن السيبراني وانعكاساته على السيادة الوطنية، دار الفكر الجامعي، الإسكندرية، 2021، ص 88-90

خالد الزبيدي؛ الحروب السيبرانية: مخاطرها وأبعادها الإستراتيجية، المركز العربي للأبحاث ودراسة السياسات، بيروت، 2022، ص 199-202

سعيد جمال؛ الأمن السيبراني: التحديات والفرص في العلاقات الدولية، دار الفكر العربي، 2021، ص 75-88

النعيمي عادل؛ الأمن السيبراني وتأثيراته على الأمن الوطني، دار الأكاديميون للنشر والتوزيع، 2019، ص 65-80

سامي حسن العلي؛ الأمن السيبراني في ظل العولمة الاقتصادية، دار المنهل العربي، بيروت، 2021، ص 45-55

مصطفى عبد الحميد؛ الأمن السيبراني كأولوية وطنية في العالم العربي، دار الفكر العربي للنشر والتوزيع، القاهرة، 2021، ص 121

عبد الحافظ أحمد؛ أمن المعلومات وحمايتها في التجارة الإلكترونية، القاهرة: دار الفكر الجامعي، 2019، ص 44-54

خالد عبد الرحمن الزهراني؛ التنافس الاقتصادي الدولي وأثر الهجمات السيبرانية، مجلة الدراسات الدولية، العدد 12، 2022، ص 18

محمد عبد الله العتيبي؛ التحولات الأمنية في الاقتصاد الرقمي: تحديات الثقة، المجلة العربية للأمن المعلوماتي، العدد 5، 2021، ص 22

فاطمة الزهراء شرف الدين؛ الأمن السيبراني وعلاقته بالثقة الاقتصادية في البيئة الرقمية، مجلة بحوث السياسات العامة، العدد 15، 2023، ص 11-18

سامي عبد الله الغامدي؛ الأمن السيبراني وسلاسل التوريد العالمية: تهديدات وحلول، مجلة الاقتصاد والأمن القومي، العدد 9، 2022، ص 32

علي مروان؛ التحولات الرقمية ومكافحة الجريمة السيبرانية في العلاقات الدولية، المجلة العربية للعلوم السياسية، العدد 58، 2023، ص 45

علي حسن الجابري؛ أمن المعلومات والأمن السيبراني: تحديات الواقع واستراتيجيات المواجهة، مجلة دراسات قانونية وسياسية، جامعة باتنة، العدد 13، 2022، ص 218

يوسف الحوامدة؛ الحوكمة الأمنية السيبرانية وتحديات التعاون الدولي، المجلة الأردنية للأمن والحماية، 2021 أحمد عبد العزيز شقير؛ الجريمة الإلكترونية والتحديات القانونية المعاصرة، دار الجامعة الجديدة، الإسكندرية، 2021، ص 142-145

محمد الرويني؛ أمن المعلومات في المؤسسات الاقتصادية، دار الفكر الجامعي، الإسكندرية، 2020، ص 218

فوزي بن خليل؛ التهديدات السيبرانية وتأثيرها على الأمن الاقتصادي للدولة، المجلة الجزائرية للدراسات الأمنية، العدد 5، 2021، ص 211

حسن عبد الكريم؛ الأمن السيبراني والتحولات في العلاقات الدولية المعاصرة، المركز العربي للأبحاث ودراسة السياسات، 2022، ص 45-52

2- المجلات

ريم عبد الله أبو السعود؛ التجسس الإلكتروني وأثره على العلاقات التجارية الدولية، المجلة العربية للعلوم السياسية، العدد 67، 2020، ص 12

عبد الله محمد العجمي؛ التهديدات السيبرانية وأثرها على سلاسل الإمداد العالمية، المجلة العربية للأمن السيبراني، العدد 3، 2022، ص 200

علي، ناصر؛ القانون الدولي والأمن السيبراني: إشكاليات الاختصاص والسيادة في الفضاء الرقمي، مجلة البحوث القانونية والاقتصادية، العدد 18، 2022، ص 155-

190 منصور هدى؛ الفراغ التشريعي الدولي في مواجهة الهجمات السيبرانية: دراسة في ضوء القانون الدولي العام، مجلة الدراسات القانونية والسياسية، العدد 12، 2021، ص 88-112 ب

وحوش وليد؛ الحروب السيبرانية وأثرها على الأمن الدولي، مجلة الدراسات السياسية والدولية، جامعة الجزائر 3، العدد 18، 2022، ص 135-160

عبد الرحمن محمد؛ الجريمة الإلكترونية وأثرها على الأمن الدولي، دار النشر الجامعي، 2020، ص 99-105

علي م. ع. ح؛ الأمن السيبراني وأساسياته، دار المناهج للنشر والتوزيع، 2024، ص 73 القمري ع. م؛ الجرائم الإلكترونية في القانون الدولي، مجلة العلوم القانونية، جامعة الجزائر 1، 2020، (12)، ص 45-67

زروقي ل؛ المسؤولية القانونية عن الهجمات السيبرانية في القانون الدولي العام، مجلة دراسات قانونية وسياسية، جامعة باتنة، 2021، (15)، ص 89-110

أحمد أبو راس؛ التقنيات الناشئة والأمن السيبراني: تحديات الحماية الرقمية في بيئة متغيرة، مجلة الدراسات التكنولوجية، العدد 15، جامعة القاهرة، 2022، ص 112–125

2المصادر والمراجع باللغة الإنجليزية

International Organization for Standardization. (2013). ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements. ISO

Kello, L. The Virtual Weapon and International Order

فهرس المحتويات

الملخص

تناولت مذكرة "تأثير الأمن السيبراني على العلاقات الدولية" بالدراسة والتحليل مدى تأثير الفضاء السيبراني على طبيعة التفاعلات بين الدول، في ظل التحول الرقمي المتسارع الذي يشهده العالم. وقد قسمت المذكرة إلى فصلين رئيسيين؛ حيث تناول الفصل الأول التداعيات المختلفة للأمن السيبراني على العلاقات الدولية، مبرزاً الجانبين الإيجابي والسلبي. فمن الجانب الإيجابي، ساهم الأمن السيبراني في تحسين الاستقرار الدولي من خلال تعزيز التعاون بين الدول، وإطلاق اتفاقيات ثنائية ومتعددة الأطراف تهدف إلى الحد من النزاعات السيبرانية. كما ساهم في حماية البنى التحتية الحيوية مثل الطاقة، الصحة، والمصارف، وساعد في دعم الابتكار والنمو الاقتصادي العالمي عبر توفير بيئة رقمية آمنة. أما من الجانب السلبي، فقد برز الأمن السيبراني كأداة جديدة للصراع، من خلال الهجمات السيبرانية الموجهة، واستخدام الفضاء الرقمي في التجسس، ونشر المعلومات المضللة، والتدخل في الانتخابات، مما أدى إلى تصاعد حدة التوترات السياسية بين الدول وزيادة حدة الصراعات غير التقليدية. في حين ركز الفصل الثاني على التحديات التي تعيق إدارة الأمن السيبراني دولياً، مثل غياب إطار قانوني موحد، وتباين تشريعات الدول، وصعوبة تتبع المهاجمين، فضلاً عن نقص الكفاءات التقنية في الدول النامية. كما تناول سبل المواجهة، عبر دعم التحالفات الأمنية السيبرانية، وتبادل المعلومات عبر منصات متخصصة، ووضع مدونات سلوك دولية لتنظيم الفضاء الرقمي، مع تعزيز بناء القدرات الوطنية لمجابهة التهديدات وتعزيز المرونة السيبرانية. وخلصت المذكرة إلى أن الأمن السيبراني لم يعد مسألة تقنية فقط، بل أصبح ركيزة جوهرية في حفظ السيادة الوطنية والاستقرار الدولي، ويستوجب تضافر الجهود الدولية لصياغة أطر قانونية وتنظيمية موحدة، والعمل المشترك من أجل بناء فضاء سيبراني آمن ومستقر يخدم مصالح الشعوب ويُجنب العالم مخاطر النزاعات الرقمية المتزايدة

abstract

The thesis titled “The Impact of Cybersecurity on International Relations” explores the growing influence of cyberspace on the nature of interactions between states in the era of rapid digital transformation. The study is divided into two main chapters. The first chapter addresses the various implications of cybersecurity on international relations, highlighting both the positive and negative aspects. On the positive side, cybersecurity has contributed to enhancing global stability by fostering cooperation among states and launching bilateral and multilateral agreements aimed at limiting cyber conflicts. It has also played a key role in protecting critical infrastructure such as energy, healthcare, and banking systems, while supporting innovation and global economic growth by providing a secure digital environment. On the negative side, cybersecurity has emerged as a new tool of conflict, with cyberattacks, digital espionage, disinformation campaigns, and election interference becoming sources of increasing political tensions and unconventional conflicts among states. The second chapter focuses on the challenges that hinder the management of cybersecurity at the international level, including the absence of a unified legal framework, differing national legislations, the difficulty of tracing cyber attackers, and the lack of technical expertise in developing countries. It also discusses potential solutions, such as supporting cyber defense alliances, sharing information through specialized platforms, establishing international codes of conduct for cyberspace governance, and strengthening national capabilities to confront threats and enhance cyber resilience. The thesis concludes that cybersecurity is no longer merely a technical issue but a fundamental