



الجمهورية الجزائرية الديمقراطية الشعبية
People's democratic republic of algeria

وزارة التعليم العالي والبحث العلمي

Ministray of higher education and scientific research

جامعة محمد البشير الإبراهيمي - برج بوعريرج

University of mohammed Al-bachir Al -Ibrahimi-BBA

كلية الحقوق والعلوم السياسية

Faculty of Law and Political Sciences



مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في الحقوق

تخصص: قانون اعلام آلى وأنترنت

الموسومة بـ:

القرصنة الالكترونية في الفضاء السيبراني (تهديد أمن الدول)

إشراف الأستاذ:

بوقرة عيسى

إعداد الطالب:

- داود زهرة

- رزيق نهلة

لجنة المناقشة

(اللقب والاسم)	(الرتبة)	(الصفة)
•		رئيسا
• بوقرة عيسى	أستاذ محاضر _ب_	مشرفا
•		ممتحنا

السنة الجامعية: 2025/2024



ملحق بالقرار رقم 10821 المؤرخ في 27 ديسمبر 2020
الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي
الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الأول)

أنا الممضي أسفله.

السيد(ة): د. **أود زهرة** الصفة: طالب. أستاذ. بالبحث
الحامل (ة) لبطاقة التعريف الوطنية رقم 41033988 والصادرة بتاريخ 2024/03/07
المسجل (ة) بكنية / معهد الحقوق والعلوم السياسية
والمكلف (ة) بإنجاز أعمال بحث (مذكرة التخرج. مذكرة ماستر. مذكرة ماجستير. أطروحة دكتوراه).
عنوانها: **القرصنة الإلكترونية في الفضاء السيبراني**
"تهديد أمن الدولة"
أصرح بشرفي أنني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية
المطلوبة في إنجاز البحث المذكور أعلاه.

التاريخ: 2025/5/19

توقيع المعني (ة)

شاهد لأجل التصديق

السيد: **الحسين**

بطاقة التعريف الوطنية رقم:

مستخرج بتاريخ:

الفاصل في:

07 جوان 2025

رئيس المجلس العلمي لبلدي ويتوقع منه

ضابط الحالة المدنية

حروز زهير





ملحق بالقرار رقم 1082/..... المؤرخ في 27 ديسمبر 2020
الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي
الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الثاني)

أنا الممضي أسفله.

السيد(ة): أريخا لعلة الصفة: طالب. أسكاذ. بالبحث
الحامل(ة) لبطاقة التعريف الوطنية رقم 144190437 والصادرة بتاريخ 2015/09/11
المسجل(ة) بكلية / معيد الحقوق والعلوم السامية قسم الحقوق
والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج. مذكرة ماستر. مذكرة ماجستير. أطروحة دكتوراه).
عنوانها: القرصنة الإلكترونية في الفضاء السيبراني
"تهديد أمن الدولة"
أصريح بشرفي أنني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية
المطلوبة في إنجاز البحث المذكور أعلاه.

التاريخ: 2025/05/08

توقيع المعني (ة)

شهود لأجل التصديق

السيد: الشيخ

بطاقة التعريف الوطنية رقم:

مستخرج بتاريخ:

العناصر في:

20 جوان 2025

الأبوس الجلس النعمي البلدي و بتقويف منه

ضابحة الحالة المدنية

حروف زهير



بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

شكر وتقدير

نحمد الله عز وجل الذي وفقنا في إتمام هذا البحث العلمي، والذي

ألهمنا الصحة والعافية والعزيمة فالحمد لله حمدا كثيرا

وبعد نتقدم بجزيل الشكر والتقدير إلى الأستاذ الدكتور المشرف

" عيسى بوقرة " على كل ما قدمه لنا من توجيهات و معلومات قيمة

ساهمت في إثراء موضوع دراستنا في جوانبها المختلفة

كما نتقدم بالشكر لمن سهروا على تربيتنا وتعليمنا بالجهد والمال

والدعوات إلى العائلتين العزيزتين

الشكر إلى رسل العلم الذين أشرفوا على تعليمنا وتكويننا كإطارات من

المرحلة الابتدائية إلى يومنا هذا

شكرا لكل من مر بين الأسطر وعجزت الكلمات على احتوائه فاعترفت

له بذلك بقولها عاجزة عن التعبير

الإهداء

"وأخر دعوانهم أن الحمد لله رب العالمين"

فالحمد لله عند البدء وعند الختام

لقد كانت طريقنا طويلة مليئة بالإحباطات والنجاحات فخورين بكفاحنا في تحقيق أحلامنا

أهدي هذا العمل إلى والدي العزيز الذي كان سندنا
ومعونا لي في كل مشواري ، إلى من كانت دعواتنا
الصادقة سر نجاحي أمي الغالية ، إلى إخوتي وأخواتي
الأشقاء أدامكم الله خلعاً ثابتاً لي وإلى كل أفراد
عائلتي إلى إخوة معرفتي بسم الحياة فكانوا رجب أخ لم
تلده أمك وهم أصدقائي وأخص بالذكر سارة زبيدي _
بوظفانية ساجدة _ أهواق قواسمي _ هيماء مختار . إلى
كل الأساتذة الأفاضل الذين قدموا لنا يد المساعدة

إلى كل هؤلاء أهدي هذا العمل وفقني الله وإياكم إلى

الخير

_ نهلة _

أهدي هذا العمل إلى عائلتي العزيزة ، أنتم
النور الذي أثار والدعم الذي لا ينضب فلكم
الفضل بعد الله في كل إنجاز وإلى أصدقائي
الذين كانوا السند والضحكة في أوقات التعب ،
وجودكم كان نعمة لا توصف هذا التخرج ثمرة
دعواتكم ومواقفكم الصادقة ، فشكرا من القلب
لكم جميعاً

أهدي هذا الانجاز لكم ، فهو منكم ولكم

_ زهرة _

مقدمة

شهد العالم تقدما تكنولوجيا هائلا ما يعرف اليوم بالثورة التكنولوجية خاصة في عالم الاتصالات والعلاقات الدولية واضحا العالم بفضلها قرية صغيرة، وأصبح الفضاء السيبراني يلعب دورا أساسيا في العلاقات الدولية وببدء تأثيره من تغيرات هيكلية تحتية إلى إحداث تغيرات كيفية في النظام الدولي بحيث أصبح العالم يشهد مخاطر أمنية مع التطور التكنولوجي وبذلك أصبحت قضية أمن الفضاء الإلكتروني من عمليات القرصنة الإلكترونية والهجمات السيبرانية والتي تؤثر على أمن الدول محطة اهتمام على صعيد الأمن الدولي وباتت العلاقة بين التكنولوجيا وأمن الدول علاقة وطيدة.

وكلما تطورت التكنولوجيا زادت المخاطر الإلكترونية وتعرض المصالح الإستراتيجية للدول، خاصة أن الفضاء الإلكتروني، أصبح مصدرا لأدوات الصراع الدولي والذي يعد اليوم الكيان الأول المهدد لأي دولة بالدمار والانهيار فالقرصنة الإلكترونية بمثابة نمط جديد من الصراع الدولي لأن المؤسسات الحكومية والعسكرية والشركات والمؤسسات المالية وباقي هياكل الدولة تقوم بمعالجة وتخزين كميات كبيرة من البيانات والمعلومات على دعائم إلكترونية.

هذا ما جعل الأمن السيبراني أمرا ذو أهمية بالغة مع نمو الهجمات الإلكترونية وتطورها زادت الحاجة إلى اتخاذ خطوات جديدة لحماية المعلومات الحساسة المتعلقة بأمن الدول واستقرارها التي يمكن أن ينتج عن الوصول لها والكشف عنها عواقب سلبية مدمرة، ولقد أفرزت هذه التهديدات واقعا جديدا أصبحت فيه الحدود الإلكترونية للدول لا تقل أهمية عن حدودها مما استدعي تطوير مفاهيم جديدة للأمن السيبراني.

وبهذا كشف الفضاء السيبراني عن مجال جديد للصراع بين الدول والفاعلين من غير الدول ممن يملكون القوة السيبرانية وأدركت هذه الأخيرة أن التفوق في الفضاء السيبراني جزءا

لا يتجزأ من قدرتها على حماية أمنها القومي من التهديدات السيبرانية، ومن أهم تجليات الفضاء الإلكتروني أنه أدى بالمجتمعات إلى الانتقال من مرحلة تبني النموذج القائم على مركزية دور الدولة في صنع سياسات إلى مشاركة أفراد في رسمها وصياغتها كما أثرت هذه الثورة التكنولوجية على أشكال الحروب والصراعات البشرية وهذه التهديدات أصبحت تهدد الأمن القومي للدول فقد غيرت من أشكال الحكومات ووظائفها مما استدعى مقاربة شاملة ومتكاملة لجميع التحديات التي يطرحها الفضاء السيبراني وتحد من مخاطر الفضاء السيبراني المتعددة.

وتعد دراسة موضوع القرصنة الإلكترونية في الفضاء السيبراني وتهديد أمن الدول من المواضيع البالغة الأهمية فمختلف الهجمات السيبرانية التي يتلقاها الفضاء الإلكتروني والتي أصبحت اليوم المهدد الأول لكيان الدولة بالدمار والانهيار وخلق صراعات دولية فيما بينها خاصة أن جل المجتمعات الحديثة أصبحت تعتمد بشكل متنامي على تكنولوجيات مما باتت القرصنة الإلكترونية تهدد الأمن السيبراني الذي يشكل جزءا أساسيا من أي سياسة أمنية دفاعية.

➤ أسباب إختيار الموضوع: تتراوح أسباب إختيار الموضوع بين أسباب ذاتية وأخرى موضوعية مقسمة على الشكل التالي:

أسباب ذاتية:

– ارتباط الموضوع بتخصص الدارسة قانون الإعلام الآلي والانترنت، مما يسمح بتطبيق المعارف النظرية على واقع عملي وطني.

الرغبة في التعمق في إشكاليات التهديدات السيبرانية في الفضاء السيبراني

أسباب موضوعية

- أرهنية الموضوع وأهميته البالغة في ظل التهديدات الجديدة التي تواجه الدول
- تزايد المخاطر السيبرانية التي تهدد أمن المعلومات، وضرورة تسليط الضوء عليها أكاديميا .
- محدودية الدراسات القانونية المحلية التي تناولت هذا النوع من الدراسات

➤ أهداف اختيار الموضوع

- تحليل التهديدات من خلال فهم أنواع مختلفة من الهجمات الإلكترونية وكيفية تأثيرها على الأمن السيبراني
- تطوير إستراتيجيات الدفاع من خلال وضع خطط لحماية البنى التحتية من الهجمات.
- البحث والتطوير لمكافحة القرصنة وتحسين الأمان.

الإشكالية:

أصبح العالم اليوم يشهد تطورا في المخاطر الأمنية مع تطور مراحل النضج التكنولوجي مع الانتقال من مرحلة النمو السريع إلى مرحلة الاستخدام الكثيف، وبذلك أصبحت قضية أمن الفضاء الإلكتروني من عمليات القرصنة الإلكترونية والهجمات السيبرانية والتي بدوها تؤثر على أمن الدول تلقى اهتماما متصاعدا على أجندة الأمن الدولي وذلك في محاولة لمواجهة تصاعد التهديدات الإلكترونية ودورها في التأثير على الطابع السلمي للفضاء الإلكتروني، وباتت العلاقة بين والتكنولوجيا وامن الدول علاقة طردية فبتطور التكنولوجيا تترادف إمكانية تعرض المصالح الإستراتيجية ذات الطبيعة الإلكترونية إلى أخطار الكترونية منها القرصنة الإلكترونية في الفضاء السيبراني الذي يمثل التهديد الأكبر لأمن الدول خاصة وان الفضاء الإلكتروني غدا وسيط ومصدر لأدوات جديدة

ومن خلال ما تم التطرق إليه تثار الإشكالية التالية:

ما هي إستراتيجيات والآليات التي يمكن تفعيلها لمواجهة تحديات القرصنة الإلكترونية في الفضاء السيبراني؟

وتندرج الإشكالية الرئيسية ضمن مجموعة من الأسئلة الفرعية تتمثل أساسا في:

- ما هي القرصنة؟ وما تأثيرها على الدول؟
- ما مدى علاقة القرصنة الإلكترونية بإحداث تغيرات في البيئة الأمنية السيبرانية؟
- كيف واجهت الدول هذه التهديدات؟

المنهج المتبع:

يقصد بالمنهج "خطة بحثية تعتمد على أسس علمية واضحة، تساعد الباحث على تحليل المشكلة البحثية والوصول إلى نتائج دقيقة، ولا يتم اختيار المنهج البحثي عشوائيا، بل تحدده طبيعة الموضوع وأهداف الدراسة، مما يجعل بعض المناهج أكثر ملاءمة من غيرها.

وانطلاقا من دراسة موضوع القرصنة الإلكترونية في الفضاء السيبراني وتهديد أمن الدول، تم الاعتماد على منهجين رئيسيين: أولا، المنهج الوصفي الذي استخدم في عرض المفاهيم الأساسية بالقرصنة الإلكترونية وأمن المعلومات، وكذا في توضيح الدلالات المفاهيمية للفضاء السيبراني وتهديد أمن الدول وثانياً، المنهج التحليلي، من خلال تحليل الآليات والاستراتيجية المنتهجة من طرف الدول في إطار مواجهة مختلف التهديدات.

صعوبات الدراسة :

بصدد إعدادي لهذه الدراسة صادفتنا جملة من الصعوبات تمثلت في:

- نقص المادة العلمية خاصة الكتابات الجديدة في هذا المجال
- هذا الموضوع لم يحض بالاهتمام الكافي من قبل الباحثين والدارسين
- صعوبة الحصول على المعلومات
- عراقيل إدارية واجهتنا من خلال اتصالنا بالمكتبات الجامعية قصد تحصيل المراجع

هيكلية الدراسة:

سعيًا للإجابة على الإشكالية المطروحة وتحقيق الأهداف المرجوة من هذه الدراسة، تم تقسيمها إلى فصلين رئيسيين:

تناولنا في الفصل الأول الإطار الإيتمولوجي المعرفي لمفاهيمي الدراسة، حيث قسم إلى ثلاثة مباحث: خصص المبحث الأول للجانب المفاهيمي الخاص بالقرصنة الإلكترونية، من خلال توضيح المفهوم وأهميته ومرتكزاته وخصائصه الأساسية، في حين تطرق المبحث الثاني إلى موضوع الفضاء السيبراني، من حيث المفهوم والدوافع والمهام المرتبطة به

أما الفصل الثاني، فقد خصص لدراسة القرصنة الإلكترونية وتهديدات الأمن السيبراني بين الإدارة والمواجهة ، وتم تقسيمه بدوره إلى ثلاثة مباحث؛ تناول المبحث الأول جدلية الصراع الإلكتروني في الفضاء السيبراني وبروز القوة الإلكترونية ، بينما خصص المبحث الثاني النماذج الحديثة للاختراقات السيبرانية خلال الفترة (2016_2020) ، أما المبحث الثالث فتناول المبحث الثالث: الجهود والدولية والأمنية في تحقيق الأمن السيبراني.

الفصل الأول: الاطار الإتيومولوجي

المعرفي لمفاهيم الدراسة

الفصل الأول: الإطار المفاهيمي والنظري للدراسة

يمثل تنفيذ تدابير الأمن السيبراني تحديا كبيرا اليوم نظرا لوجود عدد الأجهزة يفوق أعداد الأشخاص كما أصبح المهاجمون أكثر ابتكارا وطينا وإقليميا ودوليا بالقدر الذي يتركز على مدى امتلاكها لتكنولوجيا المعلومات وقدرتها على توظيفها لحماية حدود الفضاء السيبراني الإستراتيجي والأمر الذي يتطلب بتأكيد سياسة تشريعية ،أمنية قائمة على الدعم المؤسسي من أجل تأسيس منظومة شاملة للأمن السيبراني حيث أنه أصبح يشكل جزءا أساسيا من أي سياسة أمنية وطنية وأن سوء الاستغلال المتنامي للشبكات الإلكترونية لأهداف إجرامية تؤثر سلبا على سلامة البنى التحتية كمعلومات الوطنية الحساسة لاسيما على المعلومات الشخصية ، كما انتهت إلى وجود قصور قانوني وتشريعي في بعضها الأمني والإستراتيجي واعتمادها على آليات الردع ووضع إستراتيجية لنشر الوعي لدي مختلف شرائح المجتمع .

المبحث الأول: الفضاء السيبراني الدلالات المعرفية

لاشك أن ثورة المعلومات وتطور التكنولوجيا الرقمية وانتشارها كأداة في أيدي الدول والمنظمات والأفراد انعكست على موازين القوى في العلاقات الدولية وأحدثت نمطا جديدا في مقاربات الأمن القومي، تعتمد الفاعل الرقمي الذي يصف الطرق والأساليب والنماذج التي يتبعها اللاعبون الرقميون لانتهاج الخيارات المعلوماتية في خوض سباق التفوق الدولي ويحتم أيضا إعادة النظام في المفاهيم التقليدية للأمن والجريمة والحرب والصراع والقوة ، وهذا ما سنبينه في المطالب الآتية :

المطلب الأول: الفضاء السيبراني _ محاولة ضبط المفهوم

يتطلب التأصيل لمفهوم السيبرانية الانتقال من المفهوم الفني البحث لأمن المعلومات إلى الامتدادات التي فرضها التدرج المعرفي لهذا المفهوم كما سوف نعرضه في الفروع التالية:

الفرع الأول: تعريف الفضاء السيبراني

تختلف التعريفات حول الفضاء السيبراني على حسب طبيعة كل دولة أو كيان على مدي قدرته على تحديد رؤيته والإستراتيجية التعامل مع مجال الفضاء السيبراني بشقيه المدني والعسكري وكذلك مدي قدرته على استغلال المزايا ومواجهة المخاطر الكامنة في هذا المجال .فهناك من عرفه على انه عالم افتراضي يتشابك مع عالمنا المادي يتأثر به، ويؤثر فيه بشكل معقد حيث تقوم العلاقة بين العالمين على نظرة تكاملية تحمل بين طياتها مزايا ومخاطر لا تتوقف،وهناك من وصفه بذراع الرابعة للجيش الحديثة إلى جوار القوات الجوية والبحرية والبرية وخاصة أن الإنترنت شهد بداية الحديث عن المعارك الحقيقية تدور في هذا العالم الافتراضي¹

وهناك من يري أنه البعد الخامس للحرب كما يعرفه على أنه المجال المادي والغير المادي الذي يتكون من عناصر، هي أجهزة الكمبيوتر والشبكات والبرمجيات وحوسبة ومستخدمو كل هذه العناصر حيث تعد كل هذه العناصر العامل المشترك في جميع محاور استخدام الفضاء السيبراني سواء كانت الجهات المستخدمة القادرة على تعظيم قيمتها وقدرتها بما في ذلك رفع الكفاءة العنصر البشري أم كانت في مرحلة متأخرة. كما عرفته

¹ _نورة شلوش، القرصنة الإلكترونية في الفضاء السيبراني وتهديد أمن الدول، مجلة مركز بابل للدراسات الإنسانية 2018،

المجلد 8، العدد 2، ص 5، 6

الوكالة الفرنسية لأمن الأنظمة المعلوماتية أنه فضاء التواصل المشكل من خلال الربط العالمي لمعدات المعالجة آلية للمعطيات الرقمية¹

ويمكن تعريف الفضاء السيبراني انه عن حيز سوسيو مكاني أنتجه الدمج بين التكنولوجيات الوسائطية والانترنت ضمن مصفوفة تشابكية تتيح إنتاج وتبادل مختلف أشكال البيانات والمضامين النصية والسمعية البصرية والتفاعل بين المستخدمين بكيفيات محكومة بأطر الواقع الاجتماعي وأنظمتها الثقافية ورموزه التداولية ومحدداته، وهو تعريف يركز على البعد الفني في تحديد طبيعة مسمى الفضاء السيبراني بالتركيز على نفي مفهومي الزمان والمكان، نظير البعد السوسيو ثقافي لمستخدمي هذا الفضاء من أفراد المجتمع المعرفة المعلوماتية، ضمن حدود افتراضية لا يمكن تأمينها إلا من خلال تدخل تكنولوجيا المعلومات وامتلاك كافة الأدوات المعرفة الرقمية.²

ويعرف الفضاء السيبراني بأنه مجال عالمي داخل بيئة معلومات، يتكون من شبكة مترابطة من البنى التحتية لتكنولوجيا المعلومات، بما في ذلك الانترنت وشبكات الاتصالات وأنظمة الكمبيوتر والمعالجات ووحدات التحكم المدبجة، كما يشار إليه بوصفه ليس مكانا ماديا بل أنه يتحدى القياس في أي بعد مادي أو متواصل في الفضاء الزمني، فهو مصطلح مختصر يشير إلى بيئة التي تم إنشاءها عن طريق النقاء الشبكات التعاونية من أجهزة الكمبيوتر وأنظمة المعلومات والبنى التحتية للاتصالات التي يشار إليها عادة باسم شبكة الويب العالمية.³

¹ _دلاي الجيلالي، بالبشير يعقوب، رهانات الأمن السيبراني الوطني في ظل التحول الرقمي قراءة في التأصيل المعرفي وإستراتيجية المواجهة التشريعية، محاضرات مطبوعة موجهة لطلبة، كلية الحقوق جامعة بن بوعلي، شلف، الجزائر، بدون صفحة

² _المرجع نفسه، بدون صفحة

³ _بوطلاعة وداد، بوكورو منال، صراع الفضاء السيبراني وتأثيره على السلم والأمن الدوليين، مجلة العلوم القانونية والاجتماعية، المجلد السابع، العدد الرابع، جامعة الإخوة منتوري قسنطينة 01، الجزائر، تاريخ نشرها 01/12/2022

وما يمكن استنتاجه من جملة التعريفات هو أنها تدرجت بمفهوم الفضاء السيبراني وفق تراكم معرفي انتقل من منطلقات تقنية بحتة إلى ربطه بمفاهيم عابرة للتخصص المعرفي ذات أبعاد سوسيولوجية وسياسية وأمنية، لكنه لم يبتعد كثيرا عن مفهوم الفضاء المعلوماتي خصوصا عند رسم معالم حدود هذا الفضاء ومكوناته.¹

الفرع الثاني: أمن المعلومات

إن الأمن المعلومات هو مفهوم مركب من مصطلحين أمن والمعلوماتية ونحاول تفكيكه على النحو التالي:

أولا: تعريف الأمن

الأمن يعني التطور والتنمية سواء منها اقتصادية أو الاجتماعية أو السياسية في ظل حماية مضمونة، أو هو غياب التهديد بالحرمان الشديد من الرفاهية الاقتصادية²

ويعود هذا التعريف إلى مفهوم القوة والتهديد بالحرمان الشديد من الرفاهية بمفهومها المادي المحسوس، وهو الجانب الاقتصادي، مشيرا إلى أهمية القوة الاقتصادية كركيزة أساسية الأمن الوطني أما **جهولسن، وج. ويلبوك** فيؤكدان بأن الأمن الوطني قد يأخذ شكل أهداف تسعى الدولة لتحقيقها من خلال السياسات والبرامج ، والعمل على توسيع نفوذها في الخارج، ومحاولة التأثير على سلوك الدول الأخرى أو تغييره.³

ثانيا: تعريف المعلومات

المعلومات هي حقائق وأفكار، يتبادلها الناس في حياتهم العادية عبر وسائل الاتصال المختلفة من خلال مراكز ونظم المعلومات المختلفة في المجتمع والإنسان. فالمعلومة هي

¹ _دلاي الجيلالي، بالبشير يعقوب، مرجع سبق ذكره، بدون صفحة

² _المرجع نفسه، بدون صفحة

³ _المرجع نفسه، بدون صفحة

إذن تعبير يستهدف جعل الرسالة قابلة للتوصيل إلى الغير وتتطلب المعلومة بطبيعتها وجود وسط تخزين فيه.¹

ثالثا: تعريف أمن المعلومات

العلم الذي يبحث في النظريات وإستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها،ومن زاوية تقنية هو الوسائل والأدوات والإجراءات اللازمة توفرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية، ومن زاوية قانونية فإن الأمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة المحتوى وتوفر المعلومات ومكافحة الأنشطة الاعتداء عليها.أو استغلال نظمها في ارتكاب الجريمة وهو الهدف والغرض تشريعات حماية المعلومات من الأنشطة الغير المشروعة والغير القانونية،التي تستهدف المعلومات ونظمها.²

عرفه البعض انه مجموعة من الإجراءات والتدابير الوقائية التي تستخدم سواء في المجال التقني أو الوقائي، للحفاظ على المعلومات والأجهزة والبرمجيات،إضافة إلى الإجراءات المتعلقة بالحفاظ على العاملين في هذا المجال ويمكن التعبير عنه أكاديميا بأنه العلم الذي يهتم بدراسة طرائق حماية البيانات المخزونة ضمن الحاسوب وأنظمة الاتصالات والذي يتناول سبل التصدي للمحاولات الرامية إلى معرفة البيانات المخزونة ضمن الحاسوب بصورة غير مشروعة ، وإلى تلك التي ترمي إلى نقل أو تغيير أو تخريب برمجيات حماية البيانات .بأي وسيلة كانت اختراقا أم تصميميا لفيروسات،أم محاكاة برامج ، أم تدابير للنظم الرقمية.³

¹ _لتنيم فتيحة، الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة عنابة ص 239

² _ المرجع نفسه، ص 239

³ _دلالي الجيلالي، بالبشير يعقوب، مرجع سبق ذكره، بدون صفحة

ويعد مساسا أمن المعلومات كل فعل يهدد امن شبكات الحاسوب، أو نظام الرقمي الوطني، أو قواعد البيانات الخاصة، أو العامة، وهو ما يصطلح عليه بالجريمة الإلكترونية أو المعلوماتية التي يعرفها البعض بأنها "أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي، أو شبكة حاسوبية، أو داخل نظام حاسوبي، وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية".¹

ومما يلاحظ على هذه التعريفات أنها ركزت نظريا على الجمع بين مفهومي الأمن والمعلوماتية بشكل يبدو فيه التركيز واضحا على الجوانب الفنية والتكنولوجية المادية كعامل أساسي في ضبط المصطلح وتوظيفه معرفيا، وحتى مصطلح الجريمة الإلكترونية لم يبتعد كثيرا عن هذه الدائرة، ولعل الأمر يبقى مبررا إذا اعتبرنا أن النصوص التشريعية لم تتجح في تفكيك رموز التداخل بين ما هو إلكتروني وما هو سيبراني إلا في حدود ضيقة أو عندما يتعلق الأمر بربطه بسياسات الأمن والدفاع الخارجي، وحاجتها إلى توظيف تكنولوجيا المعلومات والأدوات السيبرانية.²

المطلب الثاني : خصائص الفضاء السيبراني

الفضاء السيبراني هو بيئة رقمية تنشأ من خلال تفاعل الشبكات وأجهزة الحاسوب والبرمجيات، ويعتبر من ابرز مكونات العصر الرقمي الحديث. يتميز بعدة خصائص أهمها

الفرع الأول: العالمية واللامركزية

يعتمد الفضاء السيبراني كمجال افتراضي على نظم الكمبيوتر وشبكات الإنترنت ومخزون هائل دون تقيد بالحدود الجغرافية وقد ظهر مصطلح الفضاء السيبراني في ثمانينات القرن

¹ _المرجع نفسه ،بدون صفحة

² _ المرجع نفسه

الماضي في احدي الروايات الخيال العلمي للكتاب الأمريكي الكندي وليام جيمس ويوصف العصر الحالي انه عصر رقمي فهو يتضمن تطورات تكنولوجية هائلة، تخدم جميع مناحي الحياة العامة والخاصة وينعكس على خدمة المجتمع الدولي بأكمله حيث بات العصر يتحرك من خلال تكنولوجيا المعلومات والاتصالات التي واكبتها حركة إجرامية كبيرة فانتشرت الجرائم المعلوماتية بشكل خطير في جميع دول العالم التي أصبحت عرضة للوقوع تحت تهديد هذه الجرائم باستخدام الفيروسات وبرامج التجسس وغيرها وهي الأدوات يمكن وصفها مجازا بالجرائم المستحدثة أو المختلفة.¹

الفرع الثاني:صعوبة الاكتشاف

تكن مخاطر هذا المجال في صعوبة تحديد هوية الكيان الذي نفذ الهجمات السيبرانية، في الكثير من حالات وكذلك غياب التشريعات الدولية والتي تضع الدول أو المؤسسات التي تقوم بمثل هذه الأنشطة تحت طائلة القانون الدولي. ما يعني عدم القدرة على ملاحقتها قانونيا على خلاف مجالات الحرب التقليدية²

كما يتميز بخصائص أخرى أن الفضاء السيبراني غير ملموس هو فضاء افتراضي لا يمكن رؤيته أو لمسه، بل يدار عبر أجهزة والبرمجيات. كما انه لا يخضع لسلطة مركزية واحدة بل يتوزع عبر شبكات متعددة ومستقلة جزئيا. تراجع دور الدول في ظل العولمة وانسحابها من بعض القطاعات الإستراتيجية مع تصاعد ادوار الشركات متعددة الجنسيات، خاصة العاملة في مجال التكنولوجيا كفاعل مؤثر في الفضاء السيبراني.³

¹ _نورة شلوش، مرجع سبق ذكره، ص 6

² _المرجع نفسه، ص 06

³ _شريعة كلاع، الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء الإلكتروني، مجلة الحقوق والعلوم الإنسانية، المجلد 15، العدد 01، جامعة الجزائر 3 ، تاريخ النشر 2022/04/27 ص 299

توظيف الفضاء السيبراني في تعظيم قوة الدول، من خلال ميزة أو تفوق أو تأثير في البيئات المختلفة، وبالتالي ظهر ما يسمى بالإستراتيجية السيبرانية للدول واتساع نطاق مخاطر الأنشطة العدائية التي يمارسها الفاعلون ، سواء من الدول أو من غير الدول في الحروب السيبرانية، فقد تشن الهجمات الإلكترونية عبر أجهزتها الأمنية الدفاعية، كما تلجأ إلى تجنيد القراصنة أو الموالين لشن هجمات ضد الخصوم دون أي ارتباط رسمي.¹

المطلب الثالث: أنواع الهجمات السيبرانية

في العصر الرقمي الحديث أصبحت الهجمات السيبرانية واحدة من أكبر التهديدات التي تواجه الأفراد، المؤسسات، الحكومات على حد سواء تهدف هذه الهجمات إلى اختراق الأنظمة المعلوماتية وسرقة البيانات أو تدميرها أو تعطيل الخدمات, حيث تتعدد أنواع الهجمات السيبرانية وتتنوع في أساليبها وأنواعها وهذا ما سنتطرق له في فروع التالية.

الفرع الأول: تعريف الهجمات السيبرانية

الهجمات السيبرانية في اللغة مصطلح بمعني القيادة والتحكم عن بعد²

أما في الاصطلاح فتعني:

تلك الإجراءات التي تتخذها الدولة من أجل الهجوم على نظم المعلومات للعدو ويهدف التأثير والإضرار فيها والدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة.³

ومن جهة أخرى هي التي يكون فيها النظام المعلوماتي وسيلة لارتكابها، إما ضد الأموال كالتحويل الإلكتروني غير المشروع للأموال، أو ضد الأشخاص كجريمة السب أو القذف عبر الإنترنت.¹

¹ _المرجع نفسه، ص 300

² _يحي ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، مجلة قانونية، ص 83

³ _المرجع نفسه، ص 84

وإذا شكلت الهجمات السيبرانية وتبعاً للظروف نزاعاً مسلحاً، فنكون أما مصطلح الحرب السيبرانية أو ما يعرف بالهجوم السيبراني وفقاً لقواعد القانون الدولي الإنساني بوصفه عملية إلكترونية سواء هجومية أو دفاعية يتوقع أن تتسبب في إصابة أو قتل أشخاص أو الإضرار بأعيان أو تدميرها وبالتالي فإن الهجمات السيبرانية يمكن أن تكون أوسع نطاقاً من الحرب السيبرانية وقد تحدث إطار خارج الحرب وقد تكون سبباً لبدء الحرب. بينما تبدو هجمات الفضاء الإلكتروني غير محددة المجال وغامضة الأهداف كونها تتحرك عبر شبكات المعلومات والاتصالات المتعدية للحدود الدولية، إضافة اعتمادها ما يمكن وصفه بأسلحة إلكترونية جديدة تتلاءم مع طبيعة السباق الإلكتروني لعصر المعلومات.²

الفرع الثاني : أنواع الهجمات السيبرانية

كل ما يعرض الأمن القومي والعسكري واقتصادي والاجتماعي ويهدد البنية التحتية للدول والأسواق، المال والقطاعات المصرفية والسلم الدولي والمنشآت النووية والمؤسسات الصحية والقطاعات النقل بكل أنواعها، وفي هذا الصدد يمكن الإشارة إلى أضخم العمليات التي شكلت الصورة من صور الاختراق والتهديد الأمني السيبراني عام 2016 والتي مازالت تتزايد وتتوسع بفعل عدم تركيز أدوات القوة السيبرانية في أيدي الدول وحدها، حيث يشير التقرير التحليلي الصادر من طرف المخابر المختصة لسنة 2016 إلى أن حالة انعدام فعالية الإجراءات الأمنية تسببت في تسجيل أكثر من 100 ألف و2260 اختراقاً في 82 دولة.³

¹ _دلالى جيلالى، بالبشير يعقوب، مرجع سبق ذكره، بدون صفحة

² _يحي ياسين سعود، مرجع سبق ذكره، ص 85

³ _دلالى الجيلالى، بالبشير يعقوب، مرجع سبق ذكره، بدون صفحة

المساس بسرية الاتصالات على الوسائط الإلكترونية وسرقة البيانات، الشخصية وتسريبها واستخدامها دون إذن والاعتداء على ملكية الفكرية.¹

1. الجرائم العادية التي تستخدم الإنترنت في تنفيذها كالسرقة والغش والخداع وتزوير لنشاطات مخالفة القانون.

2. سرقة كلمات المرور للمستخدمين للتسلل في النظام

3. هجمات رفض أداء الخدمة هجمات الدوس تستخدم لزيادة التحميل على الإنترنت والبنية التحتية للشبكات والخدمات، وهو يزج الشركات والمنظمات وهو على عكس من التقنيات التي يستخدمها مجرمو الإنترنت فهي تمنع المستخدمين الشرعيين من الوصول إلى منتجات والخدمات يمكن أن يرتكبها الفرد أو الجماعة²

قراصنة المعلومات:

تتمثل في هكرز، الكراكرز هما برمجيان قادرين على التعامل مع الكمبيوتر ومشاكله ويقدمون حلولاً للمشاكل البرمجية بشكل تطوعي³

6/البرمجيات الخبيثة:

هي برامج تهدف إلى إلحاق الضرر بالحاسوب أو تعطيله وجمع المعلومات والتجسس وعرقلة العمليات، وتتمكن بطريقة غير شرعية من عدوى نظام الحاسب بدون معرفة أو علم المستخدم من أجل اختراق جهازه و التجسس عليه ومن أنواع البرمجيات الخبيثة نذكر:

¹ _المرجع نفسه، بدون صفحة

² _نورة شلوش، مرجع سبق ذكره، ص 07

³ _المرجع نفسه، ص 07

أ/ **أحصنة طروادة:** وهي برامج تتضمن تعليمات خفية تهدف للتخريب وإلحاق الضرر بالنظام على الرغم من انه في ظاهرة يبدو كأنه يؤدي أعمالاً عادية، في توحى للمستخدم بأنها تقوم بعمل معين في حين أنها في واقع الأمر تؤدي عملاً آخر تخريبي في الغالب، فتقوم أحياناً بالتجسس ومتابعة كل ما يتم عمله من إجراءات وتسجيله من البيانات على الجهاز المصاب بها وتقوم أحياناً أخرى بإحداث أنواع أخرى من الأذى على الأجهزة المصابة مثل تشفير البيانات أو مسحها أو غير ذلك ولا تتمكن أحصنة طروادة من نسخ نفسها أو الالتصاق بالبرامج الأخرى ولكنها تؤدي عملاً معيناً تم تصميمها من أجله.¹

ب/ **القنابل المنطقية والقنابل الموقوتة:** هي من أنواع أحصنة طروادة وتعمل القنابل المنطقية عند شرط منطقي محدد مثل بلوغ الموظفين عدداً معيناً أو رفع اسم أحد الموظفين من كشف الرواتب، أو كتابة كلمة معينة أو عند تشغيل برامج معين لعدد محدد من المرات أما القنابل الموقوتة فتعمل وفقاً لتوقيت معين مثل ساعة محددة أو يوم محدد. هذه البرمجيات استخدمت في العديد من الهجمات على الدول من طرف دول أو المنظمات مختصة في السرقة، وكمثال تعرض إيران للعديد من هذه البرمجيات التي تستخدم للسرقة والإفساد في مفاعلاتها النووية وعرضتها لخسائر كبرى.²

7. **الاختراق:** يسمى باللغة العربية عملية التجسس أو القرصنة، حيث يقوم أحد الأشخاص غير المصرح لهم بدخول على نظام التشغيل في جهاز الحاسوب بطريقة غير شرعية ولأغراض غير مسموح بها مثل التجسس أو السرقة أو التخريب، حيث يتاح للشخص المتجسس {الهاكرز} أن ينتقل أو يسمح أو يضيف ملفات أو برامج، كما انه بإمكانه أن يتحكم في نظام التشغيل فيقوم بإصدار أوامر مثل إعطاء أمر الطباعة أو التصوير أو

¹ شعب قاسمي، فؤاد بالغيث، الإستراتيجيات الدولية في مكافحة الجريمة السيبرانية، مذكرة لنيل شهادة الماستر في العلوم السياسية والعلاقات الدولية، تخصص دراسات إستراتيجية أمنية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة

العربي تبسي، تبسه، ص 13

² _المرجع نفسه، ص 13

التخزين وبالتالي يكون المستهدف عرضة لسرقة معلوماته وبياناته سواء أكان فرداً أو منظمة أو دول لإلحاق الضرر المادي في بناها التحتية أو تهديد أمنها.¹

8. إتلاف المعطيات والبيانات المخزنة الرقمية أو تشويهاها، والتجسس على الشبكات، بالإضافة إلى تدمير الأصول والمعلومات بواسطة الأنظمة الخبيثة والفيروسية بأهداف إجرامية وإرهابية.²

9/ الإرهاب الإلكتروني: ويأخذ شكل التهديدات القائمة على مواجهة أنظمة الحواسيب بغرض الترويع أو الابتزاز أو إجبار الحكومات أو الأفراد على تحقيق أهداف سياسية أو دينية أو عقائدية ، وينبغي أن يكون الهجوم مدمراً أو تخريبياً لتوليد الخوف، بحيث يكون مشابهاً للأفعال المادية للإرهاب. التلاعب بالمعلومات الموجودة في النظام معين ، وتشويشها أو إتلافها سواء عبر الاقتحام اليدوي ، أو عبر إرسال برامج وفيروسات مخصصة بذلك، سرقة البيانات الشخصية وتسريبها واستخدامها دون إذن.³

¹ _المرجع نفسه، ص 14

² _دلالى الجيلالى، بالبشير يعقوب، مرجع سبق ذكره، بدون صفحة

³ _المرجع نفسه، بدون صفحة

المبحث الثاني: القرصنة الإلكترونية ضبط مفاهيمي

تعتبر القرصنة الإلكترونية مصدر تهديد حقيقي لاقتصاديات الدول، حيث أنها لم تعد تنحصر فقط على سرقة الأموال والبنوك والأفراد بل تطورت لتهدد أمن الدول. لذا سنتناول في هذا المبحث نشأة وتطور القرصنة الإلكترونية بالإضافة إلى مفهومها، وابرز مظاهرها.

المطلب الأول: كرونولوجيا القرصنة الإلكترونية

إن موضوع البحث في تاريخ القرصنة الإلكترونية يتضمن العديد من المحطات والتفاصيل التي تحتاج إلى البحث واسع ومطول. وسنحاول في هذا المطلب الوقوف على أهم عمليات القرصنة عبر التاريخ.

الفرع الأول: القرصنة الإلكترونية من 1903 إلى 1971

يستحيل بأي حال من الأحوال تحديد الفترة الزمنية لأول قرصنة وذلك لاتساع مفهوم القرصنة قديما ، حيث أنه لم يكن يشير إلى القرصنة الحواسيب والمواقع الإلكترونية فقط بل كان يرمي إلى السطو على أي جهاز لتحقيق أهداف خاصة ، أو جماعية.

- في عام 1903 كان الفيزيائي **جون أمبرز فلمنج** يستعد لعرض إحدى العجائب التكنولوجية المستجدة وهي نظام تلغراف لاسلكي بعيد المدى الذي ابتكره الإيطالي **جوليلمو ماركوني** في محاولة لإثبات أن رسائل شفرة **موريس** يمكن إرسالها لاسلكيا عبر مسافات طويلة، وكان ذلك أمام جمهور غفير في قاعة المحاضرات المعهد الملكي الشهير بلندن ،وقبل بدء العرض بدأ الجهاز ينقر مكونا رسالة كانت في بداية كلمة واحدة ثم تحولات إلي قصيدة ساخرة بشكل غير لائق تتهم **ماركوني** بخداع الجمهور فقد تم اختراق عرض **ماركوني** ، وكان المخترق هو الساحر والمخترع البريطاني **نيفيل ماسكلين**¹

¹ _ محمد أحمد عبد الغني، ملخص تاريخ القرصنة الإلكترونية وأشهر القراصنة، لمزيد من التفاصيل

- في 1932 تمكن الخبراء التشفير البولنديون ماريان ريجيوسكي وهنري وزيجلاسكي وجيرزيروزيكي من فك شفرة جهاز إنغيم الذي استخدمه بشكل خاص الألمان خلال الحرب العالمية لإرسال واستقبال رسائل سرية¹
- في ستينيات القرن العشرين كانت إحدى أولى عمليات الاختراق الشائعة والتي ارتبطت بالهواتف وهو عندما يستخدم الفرد صفارة أو أي صوت آخر عالي **Phreaking** والتي تعرف باسم النبرة لخداع الهاتف لتلقي أوامر تشغيلية وبالتالي تغيير سلوك النظام.²
- حوالي عام 1965 أدرك جون درابر الذي اشتهر باسم كابتن كراش بسبب تقنياته في التصنت ، أي أنه يستطيع استخدام صفارة لعبة لاستغلال المكالمات الهاتفية طويلة المسافة مجاناً. وقد وجد الصفارة في علبة حبوب الإفطار ومن هنا جاء لقبه، وبمساعدة الصفارة والتردد الصحيح لضوضاء كان قادراً على إجراء مكالمات هاتفية طويلة المسافة مجاناً. بدأ عالم القرصنة كما نعرفه اليوم في أوائل سبعينات القرن العشرين، بعد انتشار أجهزة الكمبيوتر المبتكرة، ومع استفادة الوكالات الحكومية من هذه التقنيات الجديدة³
- وقد مرت الجريمة الالكترونية في تطورها بعدة مراحل منذ رصدها في الإحصائيات لأول مرة في الفترة من 1971 إلى 1990 تضمنت أبرز الجرائم التي تم رصدها على نطاق العالم.⁴

¹ _المرجع نفسه

² _جاكوب فوكس، نبذة مختصرة عن تاريخ القرصنة الالكترونية كوبات، لمزيد من التفاصيل انظر [https:// www . Cobalt. Com](https://www.Cobalt.Com) (2025/3/6_12:35)

³ _المرجع نفسه، بدون صفحة

⁴ _ مدير البحوث والدراسات، الجريمة الالكترونية في المجتمع الخليجي وكيفية مواجهتها، مسابقة جائزة الأمير نايف بن عبد العزيز للبحوث الأمنية، مجمع البحوث والدراسات، أكاديمية السلطان قابوس لعلوم الشرطة، سلطنة عمان، 2016،

حيث قامت القوات الجوية بأول اختراق على الإطلاق لأنظمتها في عام 1971 أصبحت هذه الفرق من المتخصصين التقنيين للغاية تعرف باسم " فرق النمر" وكانت واحدة من أقدم أنواع القراصنة، بعد ظهور فرق النمر في سبعينيات القرن العشرين ،أصبح من الممكن رؤية أمثلة أخرى للاختراق بالمعني التقليدي مثل اختراع أول دودة كومبيوتر في العالم وبرامج مكافحة الفيروسات¹

الفرع الثاني : فجر القرصنة الحاسوبية 1981 إلى 2014

- عام 1981 تشكلت مجموعة قراصنة "نادي فوضي الحاسوب" في ألمانيا و " أسياذ البرامج" في أمريكا التي تتألف من عديد من المتسللين المراهقين ومخترقي الهاتف والمبرمجين والعديد من قراصنة الحاسوب الذين يعملون في الخفاء.²
- ليتخذ الكونجرس إجراءات من خلال إقرار قانون الاحتيال وإساءة استخدام الكومبيوتر، لقد لفتت أنشطة مجموعات القراصنة مثل نادي الكومبيوتر الفوضوي انتباه الرأي العام إلى أهمية الأمن السيبراني والعوائق المحتملة لإهماله ، غالبا ما كانت مجموعات القراصنة المبكرة هذه تعمل في المنطقة الرمادية ، وتوازن بين القراصنة الأخلاقية لاكتشاف العيوب والأنشطة الغير القانونية التي قد تسبب الضرر. دفعت أفعالهم المنظمات والحكومات إلى أخذ الأمن السيبراني على محمل الجد و الاستثمار في التدابير اللازمة لحماية أصولها الرقمية.³
- في عام 1988 ظهرت "دودة موريس" احدي أوائل الديدان الحواسيب المعروفة التي أثرت في البنية التحتية للانترنت وانتشرت في الحواسيب وعلى نطاق واسع داخل الولايات المتحدة، واستغلت الدودة نقطة ضعف في نظام يونيكس " ناون1" واستنسخت ذاتها

¹ _ جاكوب فوكس، مرجع سبق ذكره، بدون صفحة

² _ محمد أحمد عبد الغاني، مرجع سبق ذكره، بدون صفحة

³ _ جاكوب فوكس، مرجع سبق ذكره، بدون صفحة

بانتظام وتسبب بإبطاء أداء الحواسيب لدرجة عدم القدرة على استخدامها .وعند اعتقال مطور هذه الدودة روبرت تبان مورييس أصبح أول القرصان يدان تحت قانون " احتيال الحاسوب وإساءة الاستخدام" وهو الآن أحد القراصنة الأخلاقيين { أصحاب القبعات البيضاء}¹.

• أصابت دودة مورييس 6000 جهاز من أصل 60 ألف جهاز كان متصلا بالإنترنت وقتها أي نحو 10 بالمائة من إجمالي عددها، عدل مورييس بعد ذلك كود برمجته وجعل الدودة تنسخ نفسها على أجهزة الحواسيب التي تضربها، وتسبب هذا الكود الجديد في انتشارها بسرعة وقامت بنسخ نفسها على آلاف من الكمبيوترات في عدد محدود من الساعات.²

• وفي صيف عام 1994 تمكن قرصان روسي يدعي فلاديمير ليفين من اختراق "سيتي بنك" الأمريكي وتحويل عشرة ملايين دولار من حسابات عملاء إلى حساباته شخصية في فنلندا وإسرائيل مستخدما حاسوبه المحمول ، حكم عليه بعد اعتقاله بالسجن ثلاث سنوات واستعادت السلطات كافة المبلغ المسروق باستثناء أربعمئة ألف دولار. انونيموس تبنت مسؤولية العديد من الهجمات التي استهدفت مواقع الانترنت الإسرائيلية {غيتي}³.

التحول الرقمي سلاح ذو حدين للمؤسسات ، فمن جهة يحدث التغيرات التكنولوجية من خلال استخدام المؤسسة للتكنولوجيا الرقمية، ومن جهة أخرى يمثل عملية التغيير الشاملة التي تمس جميع أنشطة المؤسسة بما في ذلك ثقافتها ووظائفها ونماذج أعمالها.⁴

¹ _ المرجع نفسه، بدون صفحة

² _عبير حسين {دودة مورييس} أول قرصنة إلكترونية تعرفها الإنترنت، لمزيد من التفاصيل انظر

https:// www.alkhaleej.com (2025/2/2_12:55)

³ _ جاكوب فوكس، مرجع سبق ذكره، بدون صفحة

⁴ _ كريباش رحمة، التحول الرقمي في منظمات الأعمال بالاعتماد على برنامج hana / 4 saps مجلة نماء للاقتصاد

والتجارة، المجلد 08، العدد 01، 2024، ص413

"اختراقات القرن 21"

- في ديسمبر/كانون الأول 2006 أجبرت ناسا على حجب رسائل البريد الإلكتروني التي تأتي مع مرفقات قبل إطلاق المركبات الفضائية خشية اختراقها، وذكرت مجلة "بيزنس ويك" الأمريكية أن خطط إطلاق مركبات الفضاء الأمريكية الأخيرة حصل عليها مخترقون أجانب غير معروفين.¹
- في عام 2007 تعرضت شبكات الحاسوب الحكومة الإستونية لهجوم من نوع الحرمان من الخدمة من طرف المجهولين ،وذلك بعد جدال مع روسيا بشأن إزالة نصب تذكاري وتعطلت في الهجوم بعض الخدمات الحكومية الإلكترونية والخدمة المصرفية هجمات عبر الإنترنت وفي ذلك العام اخترق حساب بريد إلكتروني غير سري لوزير الدفاع الأمريكي من طرف مخترقين مجهولين ضمن سلسلة كبيرة من الهجمات للوصول إلى شبكات حاسوب البنتاغون²
- وفي صيف 2008 اخترقت قاعدة بيانات حملات المرشحين الجمهوريين و الديمقراطيين في الولايات المتحدة من قبل مجهولين قاموا بتحميل تلك البيانات، وفي اغسطس/أب اخترقت شبكة حواسيب في جورجيا من طرف مخترقين مجهولين خلال فترة صراعها مع روسيا.³
- شبكة حواسيب سوني بيكتشرز تعرضت لهجمة إلكترونية في يناير/كانون الثاني 2010 عطلت جماعة تطلق على نفسها اسم " الجيش الإيراني السيبراني " خدمة على الإنترنت لمحرك البحث الصيني الشائع "بايدو" وكان يتم تحويل مستخدمي محرك البحث إلى رسالة

¹ _ جاكوب فوكس، مرجع سبق ذكره، بدون صفحة

² _المرجع نفسه

³ _المرجع نفسه

سياسية إيرانية ، وكانت الجماعة ذاتها اخترقت "تويتر" في ديسمبر/كانون الثاني 2009 مع توجيه رسالة مشابهة¹ .

- ويعود ذلك إلى أن الانترنت لم تعد قاصرة على الباحثين وموظفي المؤسسات، وإنما طالت الأفراد والشركات الخاصة وأصبحت عصب عالم التجارة.²

-وفي أكتوبر/تشرين الأول 2009 اكتشف فيروس "ستكسنت" وهو برمجة خبيثة معقدة مصممة لتعطيل أنظمة التحكم الصناعية من إنتاج سمينر كالتى تستخدمها إيران وإندونيسيا إلى جانب الدول الأخرى الأمر الذي أثار تكهنات بأنها سلاح إلكتروني حكومي استهدف برنامج إيران النووي، في يناير/كانون الثاني 2011 أعلنت الحكومة الكندية تعرض وكالاتها لهجوم إلكتروني ضخم من بينها وكالة البحث والتطوير الدفاعي الكندية، وأجبرت الهجمات وزارة المالية ومجلس الخزانة الكنديين على فصل اتصالاتهما بالانترنت.³

- وفي يوليو/تموز 2011 أعلن نائب وزير الدفاع الأمريكي أن قرصنة الانترنت سرقوا 24 ألف ملف من وزارة الدفاع في عملية واحدة خلال مارس/آذار مضيافا أن الوزارة تعتقد أن وراء الهجوم دولة ليس أفرادا أو مجموعة قرصنة⁴

- في أكتوبر 2012 اكتشفت شركة أمن المعلومات الروسية "كاسبرسكي" هجوما إلكترونيا عالميا حمل اسم "أكتوبر الأحمر" وقالت أنه يجري منذ عام 2007 على الأقل ويعمل على جمع المعلومات من سفارات وشركات أبحاث ومؤسسات العسكرية وشركات الطاقة وغيرها ، مشيرة إلى أن أهداف الهجوم الرئيسية هي دول في أوروبا الشرقية ودول الاتحاد السوفياتي سابقا و آسيا الوسطى ، وبعض دول أوروبا الغربية وشمال أمريكا.وفي أواخر نوفمبر/تشرين

¹ _ أحمد عبد الغني مرجع سبق ذكره، بدون صفحة

² _ حورية بن سيدهم، رقية عواشيرة، الأمن الفضائي السيبراني "التحديات والحلول"، المجلة الجزائرية للأمن الإنساني،

المجلد 5، العدد2، السنة، 2020، ص 127

³ _ أحمد عبد الغاني، مرجع سبق ذكره، بدون صفحة

⁴ _ المرجع نفسه

الثاني 2014 تعرضت شبكة الحواسيب شركة سوني بيكتشرز اليابانية في الولايات المتحدة للهجوم إلكتروني عنيف¹ .

- فجميع شاشات الحواسيب الموجودة في الشركة أصبحت تعرض صورة واحدة فقط . صورة مخيفة إلى أقصى حد قاتمة الألوان تظهر هيكل عظمي أحمر كأنه قادم من أعماق الجحيم يتطلع إليك عبر شاشة نظرة مخيفة، ويمد يداه العظيمنتان كأنه يستعد للإمساك بك. ولكن ليس هذا هو المخيف فقط بل أنها رسالة المكتوبة على الصورة.²
- نتجت عنه سرقة عدد من الأفلام السينمائية الحديثة التي لم يكن بعضها قد عرض بعد، وتسريب مئات الألف رسائل بريد الإلكتروني والبيانات الشخصية لحسابات معروفة، ووصفت بعض تلك الرسائل بالمرحجة وبشكل عام تكبدت الشركة نتيجة هذا الهجوم الذي نسب إلى كوريا الشمالية أو المتعاطفين معها خسائر قدرت بنحو مائة مليون دولار³

المطلب الثاني: مفهوم القرصنة الإلكترونية

قبل دراسة القرصنة الإلكترونية لابد من الإشارة إلى الجريمة المعلوماتية وهي كل فعل غير مشروع يتم بوسيلة إلكترونية عن طريق شبكة الانترنت. تعتبر جريمة القرصنة الإلكترونية من أكثر الجرائم الإلكترونية انتشارا في القرن الواحد والعشرين حيث أصبحت مصدرا لتهديد أمن الدول. لذا سنتطرق في هذا المطلب لتحديد تعريف القرصنة الإلكترونية من حيث اللغة والاصطلاح، وأسباب ارتكابها.

¹ _المرجع نفسه

² _اختراقات سوني بيكتشرز، القصة كاملة، لمزيد من التفاصيل أنظر

<https://arabhardwre.net> (2025/3/8_14:30)

³ احمد عبد الغني، مرجع سبق ذكره، بدون صفحة

الفرع الأول: تعريف القرصنة الإلكترونية

أولاً: التعريف اللغوي

القرصنة لغة هي: الاسم من القرصان وهم لصوص البحر، ويجعلها بعض الكتاب لفظة مفردة يجمعونها على قرصنة وهي كلمة إيطالية، كما عرفت أيضاً س لغة "السطو على الحقوق الملكية الفكرية أو الأدبية أو الفنية قرصنة حقوق المؤلفين، القرصنة في مجال التسجيلات الموسيقية.¹

ثانياً: التعريف الاصطلاحي

اختلفت تعريفات القرصنة الإلكترونية باختلاف الميادين والمجالات التي تتعرض للقرصنة الإلكترونية. فنذكر على سبيل المثال مجال الملكية الفكرية كونه من أكثر الميادين عرضة للقرصنة.

1. التعريف الفقهي: عرفه الفقهاء القرصنة الإلكترونية في مجال الملكية الفكرية على " أنها الاستيلاء أو النسخ غير المشروع على ملك الغير بدون ترخيص من المالك ومن دون أي سند قانوني، فهي اختراق للتدابير التقنية عبر شبكة الإنترنت من خلال أشخاص أو أطراف قرصنة متمكنين في هذا المجال عن طريق استخدام التقنيات الحديثة لتحايل على التدابير التقنية، أو عن طريق الغش أو يمكن أن تنفذ على المصنفات عن طريق استعمال كلمة السر بواسطة برامج معدة لهذا الغرض من أجل اختراق الأعمال الفكرية والإبداعية والنفوذ إليها ونسخها بصورة غير مشروعة²

¹ _ داودي منصور، مرابط حمزة، التشفير كآلية لحماية المصنفات الرقمية الإلكترونية، مجلة الحقوق والعلوم السياسية

جامعة خنشلة، المجلد 10، العدد 01، 2022، الجزائر، ص 30_31

² _ المرجع نفسه، ص 31، 32

2. التعريف القانوني: عرفت اتفاقية بوايست في المادة 6 منها تحت مصطلح التدخل في البيانات حيث: جاء في نصها تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمداً، وبغير حق، إتلاف، محو، أو إفساد أو تعديل، أو تدمير بيانات الموجودة على كومبيوتر وأضافت مصطلح التدخل غير المشروع في منظومة وذلك في مادة 5 منها.¹

كما عرفت اتفاقية تريبس القرصنة الإلكترونية بقولها "إن السلع أو المواد المقرصنة هي كل سلعة تشكل نسخة نسخت من دون الحصول على موافقة صاحب الحق، سواء تصنيف بصورة مباشرة أو غير مباشرة". كما نصت الاتفاقية العربية لمكافحة الجرائم التقنية للمعلومات على تعريف جريمة الدخول غير المشروع في مادة 06 بقولها "أن الدخول أو البقاء وكل اتصال غير مشروع مع كل جزء من تقنية المعلومات أو الاستمرار به" أما المادة 07 من الاتفاقية السالفة فعرّفت جريمة الاعتراض غير المشروع بقولها "الاعتراض التعمد بدون وجه حق لخط سير البيانات بأي من الوسائل التقنية وقطع البث أو استقبال بيانات تقنية المعلومات"²

أما المشرع الجزائري وعلى غرار التشريعات المقارنة لم يعرفه أيضاً. و لكن بالرجوع إلى قانون العقوبات الجزائري فقط نص على تجريم القرصنة الإلكترونية في القسم السابع مكرر المعنون بالمساس بأنظمة المعالجة الآلية للمعطيات حيث نصت المادة 394 مكرر "يعاقب بالحبس من ثلاثة {3} أشهر إلى سنة {1} وبغرامة من 50.000 إلى 1000.000 دج كل من

¹ _دحو نجا، أولاد علي فاطمة، جريمة القرصنة الإلكترونية في التشريع الجزائري، دراسة لنيل شهادة الماستر، تخصص قانون جنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية قسم الحقوق، جامعة غرداية، الجزائر 2021، 2022 ص 09

² _داودي منصور، مرابط حمزة، مرجع سبق ذكره، ص 33

يدخل أو يبقى عن طريق الغش في كل جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك . تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.¹

كما استحدث المشرع الجزائري نص تشريعي جديد متخصص في الجرائم المرتكبة في بيئة رقمية، من خلال القانون 04-09 المتضمن قواعد الخاصة للوقاية من جرائم متصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.²

يشير مفهوم القرصنة الإلكترونية إلى استخدام وسائل الاتصال وتكنولوجيا المعلومات الحديثة في ممارسات غير مشروعة تستهدف لتحايل على أنظمة المعالجة الآلية للبيانات، لكشف البيانات الحساسة أو تغييرها والتأثير على سلامتها أو حتى إتلافها ، بعبارة أخرى القرصنة ما هي سوى عملية دخول غير مصرح به إلى أجهزة الغير وشبكاتهم الإلكترونية أي أن توجه هجمات إلى معلومات الكمبيوتر أو خدماته ،بقصد المساس بالسرية أو المساس بسلامة المحتوى والتكاملية، أو تعطيل القدرة والكفاءة للأنظمة للقيام بأعمالها .³

والجزائر كغيرها من الدول التي لم تسلم هي الأخرى من ما يسمى بالقرصنة الإلكترونية ، أو من الجرائم الإلكترونية ككل، حيث لم تسلم مواقع التواصل الاجتماعي وفضاء تبادل المعلومات من عملية السطو على الصور والبيانات الشخصية واستعمالها كوسيلة ابتزاز والمساومة والتشهير وناهيك عن استغلال بيانات الحسابات الشخصية بالإضافة للاعتداء على أنظمة المعلومات ، وحسب المصدر الموثوق لجريدة الفجر، فقط تم

¹ _ القانون رقم 04-15، المؤرخ 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات ، ج، عدد 71 الصادر في 10 نوفمبر 2004، المادة 394 مكرر

² _داودي منصور، مرابط حمزة، مرجع سبق ذكره، ص 34

³ _بوديسة إيمان، مكافحة الجريمة الإلكترونية في القانون الجزائري، مذكرة لنيل شهادة الماستر، في القانون العام تخصص قانون جنائي والعلوم الجنائية، جامعة ألكلى محمد أو لحاج بوييرة، الجزائر 2019، 2020 ص 08

تسجيل أكثر من 500 جريمة إلكترونية في الجزائر سنة 2016 وهذا ما يستدعي تضافر الجهود من اجل التصدي لهذا الخطر والمتمثل في الردع السيبراني¹

الفرع الثاني: خصائص القرصنة الإلكترونية

تتحلى القرصنة الإلكترونية بجملة من الخصائص التي تتشابه إلى حد كبير من مميزات الجريمة المعلوماتية.

أولاً: أسلوب ارتكاب القرصنة

الجرائم المعلوماتية تبرز بصورة أكثر وضوحاً في أسلوب ارتكابها وطريقتها ، فإذا كانت الجريمة التقليدية تتطلب نوعاً من الأسلوب العضلي الذي قد يكون في صورة الخلع أو الكسر كما هو حال في جريمة السرقة وتحتاج كذلك إلى وجود شبكة المعلومات الدولي الإنترنت مع وجود مجرم يوظف خبرته التوجه النظري والإطار المنهجي للدراسة أو اختراق خصوصيات الغير لتعزيز قدراته على التعامل مع الشبكة للقيام بجرائم مختلفة كالتجسس بالقاصرين كل ذلك دون الحاجة لسفك الدماء.²

فهي جرائم مغرية للمرتكبين لما كانت الإنترنت جرائم سريعة التنفيذ، إذا غالباً ما تنفذ بوسائل سهلة سريعة وإمكانية تنفيذها عن بعد.³

¹ _نورة شلوش، مرجع سبق ذكره، ص 201

² _عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة مقدمة لنيل شهادة الماستر المهني الطور الثاني، تخصص علوم تسير، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة قاصدي مرباح، ورقلة، الجزائر 2019، ص 10

³ _دبابنة شرين، الجرائم الإلكترونية القرصنة الإلكترونية، مجلة الدراسات المالية والمصرفية، دار المنظومة، المجلد 23، العدد 01، 2015، ص 10

ثانيا: الضرر الناجم من الجرائم الإلكترونية غير قابل للقياس

ثالثا: السطو على المؤلفات والأعمال الفكرية للغير واستخدامها بغير ترخيص¹

رابعا: القرصنة الإلكترونية صعبت الاكتشاف والإثبات

تتسم الجرائم الناشئة عن استخدام الإنترنت بأنها خفية ومستترة في أغلبها، لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجودها على الشبكة، لأن الجاني يتمتع بقدرات فنية تمكنه من ارتكاب جريمته بدقة مثلا عند إرسال الفيروسات وسرقة الأموال والبيانات الخاصة أو إتلافها والتجسس وسرقة المكالمات وغيرها من الجرائم والتجسس وسرقة المكالمات وغيرها من الجرائم.²

كما أن وسيلة تنفيذها تتميز في أغلب الأحيان بالطابع التقني الذي يضيف عليها الكثير التعقيد بالإضافة إلى الأحجام عن تبليغ عنها في حالة اكتشافها لخشية المجني عليه فقدان عملاتهم فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل إثبات في مدة تقل عن الثانية،³ وما يترتب على حدوث تلك الجريمة أثار عملية هامة تتمثل في انتهاك حقوق الأفراد بما يشمل الاعتداء على حرمة الحياة الخاصة.⁴

فلجريمة المعلوماتية تتم في بيئة غير تقليدية حيث تقع خارج إطار الواقع المادي الملموس، لتقوم أركانها في بيئة الحاسوب والإنترنت مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن، وأجهزة التحقيق والملاحقة، ونظرا لما تتطلبه هذه الجرائم من تقنية لارتكابها

¹ داودي منصور، رابط حمزة، مرجع سبق ذكره، ص 34

² _عمار حشمان، مرجع سبق ذكره، ص 10

³ _المرجع نفسه

⁴ _إسلام مصطفى جمعة مصطفى، جريمة اختراق الالكترونية وحماية استخدام البيانات والمعلومات في القانون المصري،

المجلة القانونية مجلة متخصصة في الدراسات والبحوث القانونية مجلة علمية ومحكمة، كلية الحقوق جامعة القاهرة،

فهي تتطلبها لاكتشافها والبحث عنها ،وتستلزم أسلوب خاص في التحقيق والتعامل ،الأمر الذي لم يتحقق في الجهات الأمنية والقضائية لدينا، نظرا لنقص المعارف وهو ما يتطلب تخصص في التقنية لتحسين الجهاز الأمني والقضائي ضد هذه الظاهرة، حيث لم تعد القوانين التقليدية قادرة على مواجهة تطور الجريمة المعلوماتية في ظل السرعة الهائلة للتطورات التكنولوجية¹

خامسا: الجريمة المعلوماتية المتعدية للحدود"عابرة للوطنية"

ومعنى ذلك أن هذه القرصنة الإلكترونية غير المحصورة بالحدود الجغرافية أو المكانية للدول² فلجريمة المعلوماتية بهذا الشكل لا تعترف بالحدود بين الدول وهي بذلك شكل جديد من أشكال الجرائم العابرة للحدود الإقليمية بين دول العالم كافة، ذلك أن قدرة تقنية المعلومات على اختصار المسافات وتعزيز الصلة بين مختلف أنحاء العالم انعكست على طبيعة الأعمال الإجرامية التي يعتمد فيها المجرمون إلى استخدام هذه التقنيات في خرقهم للقانون،وهو ما يعنى أن مسرح الجريمة المعلوماتية لم يعد محليا بل أصبح عالميا .³

فقط ترتكب الجريمة بواسطة الحاسب الآلي عن طريق الشبكات الدولية وتحقق نتيجتها الإجرامية في دول أخرى من العالم مروجاً بمزود خدمة أو قنوات الاتصال في إقليم دولة ثالثة ،ويترتب على البعد الوطني للجريمة المعلوماتية عدة إشكاليات مشابهة لتلك المرتبطة بالجرائم ذات الطابع عبر الوطنية أهمية إصدار إجراءات التحقيق وضبط المتهمين وملاحقتهم بمبدأ السيادة الوطنية لدولة وخاصة في الجرائم التي تتطلب إتحاد إجراء من

¹ _عمار حشمان، مرجع سبق ذكره، ص 10، 11

² _داودي منصور، مرابط حمزة، مرجع سبق ذكره، ص 11

³ _بوديسة إيمان، مرجع سابق الذكر، ص19

إجراءات التحقيق في إقليم دولة أجنبية ،وبذلك إشكالية الاختصاص القضائي وإشكالية تحديد القانون واجب التطبيق.¹

إذا أن الفاعل لا يتواجد على مسرح الجريمة بل يرتكب جريمته عن بعد،وهو ما يعني عدم تواجد المادي للمجرم للمعلوماتي في مكان الجريمة ومن ثم تتباعد المسافات بين الفعل الذي يتم من خلال جهاز الكمبيوتر الفاعل وبين المعلومات محل الاعتداء ،فقط يوجد الجاني في بلد ما يستطيع الدخول إلى ذاكرة الحاسوب الآلي الموجود في بلد آخر،وهو بهذا السلوك قد يضر شخصا آخر موجود في بلد ما ثم يتم نسخ هذا في بلد ثالث، أو القيام بإعداد أحد البرامج الخبيثة في بلد ما يتم نسخ هذا البرنامج ويرسل إلى دول مختلفة من العالم²

الفرع الثالث: أسباب القرصنة الإلكترونية

بعد دراسة مفهوم القرصنة الإلكترونية بين التعريف والخصائص نتطرق الآن لمعرفة أسباب هذه الجريمة

¹ ين مالك أسمهان، خصائص الجريمة المعلوماتية وأسباب ارتكابها، محاضرات مقدمة لطلبة السنة أولى ماستر، قسم

الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعرييج، ص 116

² يوديسة إيمان، مرجع سبق ذكره، ص 19

أولا: الدوافع الشخصية

1/ حب التعلم:

يعتبر حب التعلم والاستطلاع من الأسباب الرئيسية التي تدفع إلى ارتكاب مثل هذه الجرائم، لأن المخترق يعتقد أن أجهزة الحاسوب والأنظمة هي ملك للجميع ويجب ألا تبقى المعلومات حكرا على أحد أي أن للجميع الحق في التعرف والاستفادة من هذه المعلومات¹

2/ المحيط:

يعتبر محيط الإنسان والبيئة التي يعيش فيها من العوامل المؤثرة في سلوكه وتصرفاته هـ.وغالبا ما تدفع مشاكل العمل إلى رغبة في الانتقام ووجود أنظمة إلكترونية تسهل له القيام برغباته، فيبعث بمحتوياتها إلى درجة التخريب،أو يكون الدافع التحدي وإثبات الجدارة أمام الآخرين بحيث يفتخر هذا الشخص بأن في استطاعته اختراق أي حاسوب أو في أي نظام ولا يستطيع احد الوقوف في وجهه²

3/ الاستيلاء على المعلومات:

الإقدام على ارتكاب هذا الجرم بواسطة تقنية المعلومات بهدف الحصول على معلومة بذاتها والاستيلاء عليها والتصرف فيها يتمثل ذلك في الحصول على المعلومة المحفوظة في الحاسب الألى أو المنقولة أو تغييرها أو حذفها أو إلغائها نهائيا من النظام ويختلف الدافع لهذا التصرف فقط يكون دافع تنافسي أو سببه الإبتزاز أو الحصول على مزايا ومكاسب اقتصادية كثيرة ما يكون هدف هذه الجرائم ذو طابع سياسي أو اقتصادي³

¹ بن شريف أحلام، بوغرة الصالح، القرصنة الإلكترونية أنواعها أشكالها وطرق التصدي لها، ، مجلة الجزائرية للعلوم السياسية والعلاقات الدولية، جامعة تيارت، مجلد 5، العدد 1، جوان 2012، ص 39

² نفس المرجع ص 39

³ - مدير مجموعة البحوث والدراسات، مرجع سابق الذكر، ص28

ثانيا: الدوافع المادية

1/المنفعة المادية:

قد تكون محاولات الكسب السريع، وجني الأرباح الطائلة دون تعب، ولا رأس مال من الأسباب التي تدفع إلى اختراق الأنظمة الإلكترونية كالتي تستخدمها المصرف عن طريق الدخول إلى الحسابات المصرفية، والتلاعب فيها أو استخدام غير مشروع لبطاقة الائتمان¹

2/ إلحاق الأذى بأشخاص أو جهات:

بعض المجرمين الذين يقدمون على ارتكاب الجريمة عبر شبكة المعلومات العالمية وتقنية المعلومات بصورة عامة يتركز الدافع من ورائها على إلحاق الأذى بأشخاص محددين أو جهات معينة، وغالبا ما تكون تلك جرائم مباشرة تتمثل في صورة ابتزاز أو تهديد أو تشهير كما حصل في القضية التي تم ضبطها بإمارة دبي بدولة الإمارات العربية المتحدة عندما أقدم الجاني ويلقب " بقرصان صور الفتيات" بالسطو على البريد الإلكتروني لمجموعة من الفتيات بتلك الدولة والاستيلاء غير مشروع على صورهن الشخصية وتعتمد نشرها على موقع خاص بالشبكة الأنترنت².

¹ _ين شريف أحلام، بوغرة الصالح، مرجع سبق ذكره، ص 39

² _ مدير مجمع البحوث والدراسات، مرجع سبق ذكره، ص 29

3/ تهديد الأمن القومي والعسكري للدول:

بعض الجرائم الإلكترونية الهدف منها أسباب ودوافع سياسية كتهديد الأمن القومي والعسكري ومن ذلك ظهر ما يعرف بالتجسس الإلكتروني والإرهاب الإلكتروني والحرب المعلوماتية كما هو الحاصل بين الدول المتقدمة إلكترونياً.¹

المطلب الثالث: مظاهر القرصنة الإلكترونية

انتشرت القرصنة الإلكترونية بشكل رهيب مؤخراً حيث سنقوم في هذا المطلب بدراسة مظاهر القرصنة الإلكترونية بشكل عام ثم نتطرق لنتحدث عن القرصنة الإلكترونية بشكل خاص في الجزائر. وقد ظهرت القرصنة الإلكترونية في عدة أشكال

أ/ **تقليد برامج الحاسوب:** يقصد بتقليد برامج الحاسوب محاكاة برنامج معين يصنع أو إنتاج نسخ على مثاله بحيث تبدو عند تسويقها كالأصل.²

ب/ **نسخ برامج الحاسوب:** وتعد هذه المصورة أهم صور القرصنة على البرامج وتتمثل في عملية النسخ الكلي أو الجزئي سواء عن طريق المحاكاة أم النسخ المباشر، حيث تقوم بعض الشركات بنسخ البرامج وبيعها دون ترخيص الشركات المنتجة، ويتم كذلك سرقة البرنامج الأصل عن طريق إزالة معالم و تغيير هيئته و إعادة تجهيزه على نحو يبدو كمنتج جديد.³

هناك نوعان يمكن أن يراد بها نسخ البرامج هما النسخ المباشر أو ما يطلق عليه النسخ الحرفي، ويقصد به قيام مرتكب هذا الفعل بنسخ البرنامج بصفة كاملة أو بيعه دون

¹ _المرجع نفسه، ص 30

² _عباسة فاروق، عيوب خديجة، القرصنة الإلكترونية في الجزائر وأثرها على المستخدم، ريبورتاج مصور لنيل شهادة الماستر في علوم إعلام واتصال تخصص سمعي بصري و فضاءات عمومية، شعبة علوم الإعلام والاتصال، قسم علوم إنسانية، كلية العلوم الاجتماعية جامعة عبد الحميد ابن باديس، مستغانم، الجزائر، بدون صفحة

³ _بوديسة إيمان، مرجع سابق الذكر ص 10

الحصول على ترخيص بذلك من الجهات المعنية، كما تشمل القرصنة النسخ غير القانوني للبرامج ويقصد به كل استخدام غير مسموح به للبرامج.¹

ج/أسلوب الهندسة العكسية: يقصد به قيام بعض الشركات المتخصصة في تصنيع و إنتاج أجهزة لأداء وظائف معينة تؤديها أجهزة أخرى موجودة في الأسواق، حيث تكون الطريقة المتبعة في تصنيع و إنتاج الأجهزة الجديدة مختلفة عن طريقة تصنيع أو إنتاج الأجهزة الأصلية.²

أولا : حول العالم

هناك حوالي 80 % من أعمال الجريمة الإلكترونية تنشأ في شكل من أشكال النشاط المنظم، مع سوق الجرائم الإلكترونية الأسود، على شكل عمل دورة البرمجيات الخبيثة، و فيروسات الكمبيوتر ، و إدارة الروبوتات، و حصاد البيانات المالية ،و بيع البيانات و قبض ثمن المعلومات المالية حيث لم يعد يحتاج مجرمو الجرائم الإلكترونية مهارات أو تقنيات معقدة، على الصعيد العالمي تظهر أفعال الجريمة الإلكترونية انتشارا واسعا عبر أعمال مدفوعة ماليا وأعمال ذات صلة بمحتوى الكمبيوتر، وكذلك العمل ضد السرية و السلامة و الوصول إلى أنظمة الكمبيوتر.³

حاليا لا تمثل إحصاءات الجريمة المسجلة لدى الشرطة أساسا سليم للإجراء مقارنات عبر الوطنية على الرغم من أن هذه الإحصاءات غالبا ما تكون هامة لرسم السياسات على المستوى الوطني، يرى ثلثي الدول أن أنظمتها غير كافية لإحصاءات الشرطة في تسجيل

¹ _عباسة فاروق، عيوب خديجة، مرجع سابق الذكر، بدون صفحة

² _بوديسة إيمان، مرجع سابق الذكر، ص 10_11

³ _دحو نجا ، أولاد علي فاطمة ، مرجع سابق الذكر، ص11

الجريمة الإلكترونية، وترتب سجلات الشرطة للجريمة مع مستويات الدولة التنموية و قدرة الشرطة المتخصصة.¹

ثانيا: الولايات المتحدة

ففي الولايات المتحدة مثلا تمت جريمة قرصنة أرقام بطاقات الدفع المغناطيسية بما يقارب 1.7 مليون بطاقة دفع مقرصنة ، مما أدى إلى خسائر قدرت ب4,3 مليون دولار وقد ارتفعت الخسارة الناجمة عن الجرائم المعلوماتية مقارنة بالجرائم العادية إذ حسب تقرير المركز الوطني للبيانات(NCCCD)أنه في21جوان1999للباحث Pernard D Standlar أن إجمالي الخسائر الناجمة في الشهر بلغت حوالي 810000 دولار أي مايساوي800 بليون دولار سنويا، وتوصل مكتب التحقيقات الفيدرالي FBI إلى أن متوسط الخسارة التي تخلفها الجريمة المعلوماتية يبلغ حوالي 500000 دولار في حين لا تزيد الخسارة التي تخلفها جرائم السرقة العادية عن 3500 دولار.²

المبحث الثالث: السيادة الرقمية والأمن السيبراني علاقة التزامن من السيادة التقليدية إلى السيادة الرقمية

السيادة الرقمية والأمن السيبراني هما مفهومان حديثان مرتبطان بتطور التكنولوجيا في العصر الرقمي، بينما ترتبط السيادة التقليدية بالتحكم والسلطة على الأراضي والشعوب ضمن حدود جغرافية معينة، فإن السيادة الرقمية تتعلق بالتحكم في الفضاء الرقمي{البيانات،الأنظمة،المعلومات،والسياسات الرقمية} التي تؤثر على الأفراد والدول والشركات في العالم الرقمي.فالسيادة التقليدية هي القدرة القانونية والسياسية لدولة معينة على

¹ _ المرجع نفسه ص 11 _ 12

² _ المرجع نفسه، ص 12

ممارسة سلطتها داخل حدودها الجغرافية، بما في ذلك تطبيق القانون ،حماية الحدود،وضمان الأمن الداخلي والخارجي .

أما السيادة الرقمية فتتعلق بالقدرة على التحكم في الفضاء السيبراني {إنترنت،شبكات،بيانات} وفي هذا السياق السيادة الرقمية تعني قدرة الدولة على فرض قوانينها وتنظيمات الأمنية على الأنترنت، ضمان حماية البنية التحتية الرقمية وضمان خصوصية وحماية البيانات.فالانتقال من السيادة التقليدية، إلى سيادة الرقمية يضع ضغطا على الدول لتطوير إستراتيجيات أمن السيبراني قوية لضمان حماية معلوماتها، بينما تدير التحديات جديدة مرتبطة بالتهديدات الرقمية والفضاء السيبراني .

المطلب الأول: أبعاد الأمن السيبراني

يرتبط الأمن السيبراني بمجالات مختلفة سياسية،عسكرية،اقتصادية ،قانونية،اجتماعية بهدف تحقيق منظومة أمن متكاملة تعمل على الحفاظ على الأمن القومي للدولة من أي تهديدات سيبرانية محتملة ،ويمكن توضيح ذلك من خلال ما يلي:

الفرع الأول: تعريف الأمن السيبراني

الأمن السيبراني هو عبارة عن مجموعة من الوسائل التقنية والإدارية التي يتم استخدامها لمنع الاستخدام من قبل غير المصرح له على الشبكات الكمبيوتر،أو سوء استغلال واستعادة المعلومات الإلكترونية التي تحتويها بهدف ضمان واستمرارية عمل نظم المعلومات،وتأمين حماية وسرية خصوصية البيانات الخاصة بقواعد الفضاء السيبراني وعليه فهو المجال المتعلق بالإجراءات ومقاييس ومعايير الحماية المفروض اتخاذها. أو الالتزام بها،لمواجهة التهديدات ومنع التعديات أو للحد من أثارها في أقصى وأسوء الأحوال.¹

¹ _دلاي الجيلالي، بالبشير يعقوب، مرجع سبق ذكره، بدون صفحة

وبحسب تعريف الإتحاد الدولي للاتصالات في تقريره حول اتجاهات الإصلاح في الاتصالات للعام 2011, 2010 فإنه مجموعة من المهمات مثل تجميع وسائل وسياسات والإجراءات الأمنية، ومبادئ توجيهية ومقاربات لإدارة المخاطر، وتدريبات وممارسات فضلى وتقنيات يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات و المستخدمين . وهو مفهوم نفسه تقريبا الذي أخذت به وكالة الأمن الرقمي الأوربية في تشريع أصدرته في هذا الشأن سنة 2001 فهو قدرة النظام المعلوماتي على مقاومة محاولات الاختراق أو الحوادث الغير المتوقعة ،التي تستهدف البيانات المتداولة أو المخزنة وفق إطار توافقي تنتظم فيه الأدوات القانونية والسياسات الأمنية ووسائل الدفاع الإلكتروني لتحقيق أهداف الأمان السيبراني المنشودة وطنيا، إقليميا ،دوليا.¹

فالأمن السيبراني هو سلاح إستراتيجي بيد الحكومات والأفراد لاسيما أن الحرب السريانية أصبحت جزءا لا يتجزأ من التكتيكات الحديثة للحروب وهجمات بين الدول. الأمن السيبراني هو الوسائل والأدوات والسياسات الدفاعية لمواجهة مختلف التهديدات السيبرانية ومختلف العمليات القرصنة، من أجل حماية البيئة السيبرانية. الأمن السيبراني يضمن إمكانية للحد من الخسائر والأضرار والحيلولة دون الوصول هذه الأضرار إلى خسائر دائمة و احتوائها في أسرع وقت ممكن.²

الفرع الثاني: أبعاد الأمن السيبراني

في ضل التطور السريع لتكنولوجيا والتحول الرقمي في جمع مجالات الحياة أصبح الأمن السيبراني حجر الأساس لحماية الأفراد والمؤسسات من التهديدات الإلكترونية المتزايدة

¹ _المرجع نفسه

² _شعيب قاسمي, فؤاد بالغيث، مرجع سبق ذكره، ص 26

ولا يقتصر على حماية البيانات فقط , بل يشمل مجموعة من الأبعاد لضمان بيئة رقمية آمنة ومن ابرز هذه الأبعاد:

1/ البعد العسكري: تكمن الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء الإلكتروني. بما يسمح بسهولة تبادل المعلومات وتدفقها وبسرعة إعطاء الأوامر العسكرية والقدرة على إصابة الأهداف عن بعد وتدميرها، وقد تتحول هذه الميزة إلى نقطة ضعف إن لم تكن الشبكة الإلكترونية المستخدمة في ذلك مؤمنة جيدا من أي اختراق قد يتسبب في شن الهجمات الإلكترونية، مضادة على شبكات القوة المسلحة وأجهزة الاستخبارات ومن تم تدمير قواعد البيانات العسكرية وتعطيل قدرة الدولة على النشر السريع لقدراتها وقواتها أو قطع أنظمة الاتصال بين الوحدات العسكرية وتعطيل شبكات الكمبيوتر.¹

2/ البعد الإقتصادي: يرتبط الأمن السيبراني ارتباطا وثيقا بالاقتصاد، فتلازم واضح بين اقتصاد المعرفة وتوسيع استخدام تقنيات المعلومات والاتصالات كما بالقيمة التي تمثلها البيانات، والمعلومات المتداولة والمخزنة ومستخدم على كل المستويات، كما تتيح تقنيات المعلومات والاتصالات تعزيز التنمية الاقتصادية لدول كثيرة عبر إفادتها من فرص الاستخدام التي تقدمها الشركات الدولية والشركات الكبرى التي تبحث في إدارة كلفة إنتاجها بأفضل شروط يضاف إلى ذلك دخول العالم عصر المال الإلكتروني ضمن بيئة تقنية متحركة بعد إطلاق الخدمات الإلكترونية إذ تتزايد الاستثمارات المصاريف والمؤسسات المالية في مجال المال الرقمي.²

¹ _ نفس المرجع ص 26, 27

² _ نفس المرجع ص 27

3/ البعد السياسي :

يتمثل البعد السياسي للأمن السيبراني بشكل أساسي في حق الدولة في حماية نظامها السياسي وكيانها ومصالحها الاقتصادية التي تعني حقها وواجبها في السعي إلى تحقيق رفاة شعبها في وقت تؤثر موازين القوى داخل المجتمع نفسه، حيث أصبح بإمكان الفرد أن يتحول إلى لاعب أساسي في اللعبة السياسية كما أصبح بإمكانه الإطلاع على خلفيات ومبررات و القرارات السياسية التي تتخذها حكومته عبر الكم الهائل من المعلومات التي يمكنه الوصول إليها. بالمقابل لا يتوانى العاملون في الشأن السياسي من الاستفادة مما تقدمه هذه التقنيات للوصول إلى أكبر شريحة ممكنة، من الأفراد والترويج لسياستهم في العالم، ومدى تأثير الذي يتركه هذا الأمر بغض النظر عن صحة السياسات والمبادئ.¹

4/ البعد الاجتماعي: لقد جاء في تقرير الإتحاد الدولي للاتصالات بشأن البعد الاجتماعي للأمن السيبراني أن الثورة الرقمية، غيرت كيفية التعامل التجاري، وكيفية عمل الحكومات وأدت العولمة والتقدم التكنولوجي إلى إضعاف البنية التحتية وبالتالي جعلتها هدف محتملا للهجمات إرهابية حيث تواجه البلدان مخاطر حقيقية للأعداء أن يستغلوا المواطن ضعف التي تعاني منها أنظمة المعلومات الدقيقة، فهم يسعون إلى تعطيل البنية التحتية والموارد الأساسية من أجل تهديد الأمن القومي واستحداث، الجرائم السيبرانية وزيادة معدلاتها وتسهيل سبل التجسس الاقتصادي، وتؤثر على عمليات الحكومة مثل الفيروسات، وهجمات منع خدمة ، سرقة البيانات والرسائل الاقتحامية ، وتهديم القيم الأخلاقية من خلال تدني المستوى وارتفاع نسبة الممارسات الإجرامية كالإباحية و الدعارة و الإرهاب، وتجنيذ لقضايا تمس الأمن والسلام الدوليين²

¹ نفس المرجع ص 27

² إسلام فوزي، الأمن السيبراني الأبعاد الاجتماعية و القانونية، تحليل سيكولوجي، مجلة الاجتماعية القومية، المجلد

5/ البعد القانوني: غياب الأمن القومي في تناقض الأحكام والقوانين وتنازع الأنظمة القانونية فيؤدي إلى ارتفاع منسوب للمخاطر مع انعدام ملاحقة الفاعلة تتلاءم وطبيعة الأعمال والجرائم والاعتداءات السيبرانية ، العابرة للحدود وللأنظمة القانونية ، بحيث تطل أي مواطن في أية بقعة من الأرض بما يطل الدول وأمنها و استقرارها .وتعد المخاطر التي تتعرض لها الأفراد والدول مخاطر هائلة وغير مقيدة بالاطر القانونية الجارية التي لاستوعب العصر السيبراني بالقدر الكافي، وهناك حاجة عاجلة إلى الخطر السريعة التي تقيم بها البلدان القيادات السيبرانية وتوسع قدراتها العسكرية لتشمل النزاع السيبراني ويجب إن تتوازن بعدم تعارض للقوانين والتشريعات .¹

المطلب الثاني: الإختراقات الرقمية والفئات المستهدفة

كثير انتشار مصطلح الاختراقات الرقمية أو ما يعرف بالهجمات السيبرانية لذا سنتطرق في هذا المطلب إلى تحديد مفهوم هذه الاختراقات وما هي الفئات التي تستهدفها .

الفرع الأول : الإختراقات الرقمية :

إن الاستعمال المتزايد للفضاء السيبراني أدى وبالضرورة إلى وجود مشكلات رقمية أو ما يعرف بالاختراقات الرقمية لذا سنتعرف في هذا الفرع على المقصود بالاختراق الرقمي.

أولاً: تعريف الاختراقات الرقمية:

هو هجوم يشن على الأجهزة الرقمية عن طريق الفضاء الإلكتروني واختراق بيانات شخصية أو مؤسسية أو حتى رسمية أو عسكرية لأسباب مختلفة. عادة ما تهدف هذه الهجمات الإلكترونية إلى الوصول إلى المعلومات الحساسة والبيانات وسرقتها

¹ _المرجع نفسه، ص 114

أو تغييرها أو تدميرها أو حتى ابتزاز المال من المستخدمين والمؤسسات. على مستوى فردي، يمكن أن يؤدي هجوم الأمن السيبراني إلى عدة تداعيات مثل سرقة الهوية أو محاولات الابتزاز أو حتى فقدان البيانات المهمة والصور.¹

بعبارة بسيطة الهجمات الإلكترونية عبارة عن هجوم يتم شنه من أحد أجهزة الكمبيوتر أو مجموعة من الأجهزة على جهاز كمبيوتر آخر أو عدة أجهزة كمبيوتر أو شبكات يمكن تقسيم الهجمات الإلكترونية إلى نوعين على النحو التالي:

هجمات يكمن الهدف من ورائها إلى تعطيل جهاز الكمبيوتر المستهدف وهجمات يكون الغرض منها الوصول إلى بيانات جهاز الكمبيوتر المستهدف وربما الحصول على امتياز المسئول عنه²

الفرع الثاني: الفئات المستهدفة

أولاً: اختراق حساب الأفراد خلال جائحة كوفيد19 ما أحدثه انتشار فيروس كوفيد19 هو الكشف عن العديد من الثغرات في أنظمة الأمن والبنى التحتية الحيوية في جميع أنحاء العالم، وهشاشة الميكانيزمات المتبعة لاحتواء الأخطار المحيطة والمهددة لهذه الأبعاد في الوقت نفسه، برزت الأهمية المتزايدة لقدرة الانترنت إلى جانب أهمية الذكاء الاصطناعي في الرفع من حدة التحديات والالتزامات الموجودة سلفاً أمام الدول لتحقيق التوازن بين مطالب أمن الدولة والصحة العامة والاقتصاد.³

¹ شركة أمنية، ملا تعرفه عن الأمن السيبراني أكتوبر لمزيد من التفاصيل أنظر

<https://Ar.Wikipedia.org> (2025/4/7_22:30)

² مؤسسة دعائم التقنية للحاسب الآلي، ما معنى الهجمات الالكترونية وأشهر الهجمات السيبرانية؟ظن لمزيد من التفاصيل

أنظر <https://www.it.pillars.com> (2025/4/7_22:40)

³ وفاء مطروح، ابتسام لونيس، تداعيات جائحة كوفيد19 وتأثيرها على الأمن السيبراني في الجزائر، مجلة دولية

الاتصالات الاجتماعي، جامعة عبد الحميد بن باديس، مستغانم، المجلد 9، العدد 2، الجزائر، 2022، ص 230، 231

وهو ما أدى إلى أن المعلومات الشخصية التي كانت منعزلة ومتفرقة يصعب التوصل إليها غدت مجمعة ومتوافرة بشكل يتيح الوصول إليها واستخدامها بسهولة، بطريقة مشروعة وغير مشروعة، فالبيانات الشخصية الموجودة في قواعد البيانات المرتبطة بالأجهزة الذكية المتصلة بشبكة الإنترنت تكون هدفا سهلا لعمليات القرصنة التي تتم عبر النظم المعلوماتية، بحيث يمكن الولوج إلى تلك القواعد وسرقة البيانات الشخصية الموجودة فيها واستخدامها بشكل غير مشروع أو بيعها لجهات أخرى والاستفادة منها كلما كان تأمين تلك القواعد ضعيفا.¹

الدخول على الأنظمة وما تحتويه من بيانات ومعلومات دون إذن والتجسس على الاتصالات والحد من سلامة المعلومات، نتيجة التلاعب، والتعديل عليها، وإتلافها، وهذا يعد اعتداء بحد ذاته على الحريات والحقوق الشخصية.²

ومن المخاطر التي تتعرض لها البيانات الشخصية إمكانية الإطلاع على البيانات السرية من قبل الغير دون وجود تصريح بذلك.³

تتطلب التحولات التي فرضها انتشار فيروس كوفيد19 أن تعترف الدول بالأخطار المحدقة بالطبيعة المتعدد للأمن القومي وترابطه وتداخله مع الأمن الدولي، حيث يجب معالجة كليهما بشكل كلي، وألا يطرح أي حل نفسه بمعزل عن الآخر.⁴

¹ إيمان خميس اليحيائي، عدنان إبراهيم سرحان، الآثار القانونية لجائحة كورونا كوفيد19 على حماية البيانات الشخصية، مجلة الحقوق، العدد 4، الجزء 2، 2021، ص 465

² طمطامي سالم، الصحافة الإلكترونية والأمن السيبراني، مذكرة لنيل شهادة الماستر في الإعلام والاتصال، جامعة أحمد دراية، كلية العلوم الإنسانية والاجتماعية والعلوم الإسلامية، قسم العلوم الإنسانية، تخصص صحافة، ولاية أدرار، الجزائر، 2021، 2022، ص 23

³ إيمان خميس اليحيائي، عدنان إبراهيم سرحان، مرجع سبق ذكره، ص 465

⁴ وفاء مطروح، إبتسام أونيس، مرجع سبق ذكره، ص 230

ثانيا: قرصنة بيانات المؤسسات الاقتصادية

في الوقت الذي أصاب فيه فيروس كوفيد19 قرابة 200 دولة حول العالم وما فرضه من عزلة اجتماعية كانت في بعض الأحيان بصفة كلية مما أضطر الأفراد، الشركات والمؤسسات في هذه الدول لتبني نمط التواصل، العمل والتعليم عن بعد بالاعتماد على تكنولوجيا الاتصال والإنترنت¹

ولكن الفضاء الرقمي لا يخلو من المخاطر، حيث يقوم القراصنة الإلكترونيين باختراق بيانات الشركات وتشفيرها، ثم يطلب القراصنة بعد ذلك مبالغ ضخمة من هذه الشركات مقابل استرجاع البيانات مرة أخرى، ولكن أحيانا نجد القراصنة يعملون لصالح الشركات المنافسة²

أضف إلى ذلك المخاطر المتمثلة في أن المعلومات الرقمية ليس لها وقت نهائي فهي لا تتقادم ولا تنتهي، وهو ما يمكنها من معاودة الظهور في أي وقت لاحق.³

ثالثا: تهديد أمن ورموز الدولة

إن التهديدات الناتجة عن التجسس وقرصنة المعلومات لا تتوقف عند المؤسسات الاقتصادية أو قرصنة المعلومات الشخصية للمواطنين، وإنما تتجاوز ذلك من خلال كشف أسرار أمن الدول واختراق مواقع المؤسسات الحكومية والبريد الإلكتروني لرؤساء بعض دول العالم فقد شهد هذا الأخير في العشر سنوات الأخيرة تسريبات غير مسبقة تتسم بالطابع السري وبأدق التفاصيل حول شخصيات دولية مستهدفة قصد الإطاحة بها أو خلق مشاكل واضطرابات داخل الدول التي ينتمون إليها. ومن بين المواقع التي سربت هذه المعلومات

¹ _المرجع نفسه، ص 219

² _يعوني ليلي، التهديدات في الفضاء السيبراني وانعكاساتها على السيادة الرقمية، القرصنة الإلكترونية نموذجاً، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة الجزائر 3، العدد 16، السداسي الثاني، 2021، ص 17

³ _إيمان خميس اليحيائي، عدنان إبراهيم سرحان، مرجع سبق ذكره، ص465

نجد موقع ويكيليكس لصاحبه الأسترالي "جوليان بول اسانج" والذي قدم معلومات في غاية من السرية لوسائل الإعلام الدولية، ما تسبب في أزمات دبلوماسية واضطرابات في العلاقات الدولية بسبب الاتهامات بين العديد من الفاعلين الدوليين.¹

وعموما فإن هذه التهديدات السيبرانية او الهجمات السيبرانية هي التي تهدد امن المجتمع وامن الاقتصاد الوطني والجانب الأمني والعسكري للدول، كما أن للتهديدات السيبرانية أهداف مسطرة حيث تمس كلا من الجانب المعنوي والجانب المادي وعلى جميع الأصعدة، ولكن ما يتوجب على الدول المعرضة لتلك التهديدات وضع خطط إستراتيجية من أجل مكافحتها والتخلص منها.²

والهجمات الإلكترونية تمثل في سرقة أو تغيير معلومات أو تدمير النظام أو إيقاف عمل الشبكات وباستخدام الشفرات الخبيثة أو تعطيل الوظائف أو إيقاف عمل الشبكات وباستخدام هذه الوسائل يمكن للقائمين بالهجوم بالإضرار بالمؤسسات الحكومية والمستشفيات وغيرها من الكيانات التي تعتمد بشكل كبير على أجهزة الحاسب الآلي في القيام بأعمالها الرئيسية وهو ما يترتب عليه تعطيل المحركات الرئيسية لاقتصاد الدولة والإضرار بمواطنيها وتهديد أمنها القومي بشكل عام ولذلك تكون التداعيات الدولية لتلك الهجمات خطيرة وواسعة النطاق وتتخطى حيز الدولة لتؤثر في الأمن العالمي ككل.³

¹ يعوني ليلي، مرجع سبق ذكره، ص18

² طمطامي سالم، مرجع سبق ذكره، ص 23

³ _عجاتي سهيلة، راهم أميرة، الهجمات السيبرانية وأثارها على تهديد السلم والأمن الدوليين، مذكرة لنيل شهادة الماستر في القانون، جامعة 8 ماي 1945، كلية الحقوق والعلوم السياسية، قسم الحقوق، تخصص قانون عام، 2023، 2024،
قائمة، الجزائر، ص 60

ملخص الفصل الأول

نلخص في ختام هذا الفصل أن القرصنة الإلكترونية واحدة من أخطر التهديدات التي تواجه الأمن القومي للدول في العصر الرقمي ، حيث أصبح الفضاء السيبراني ساحة جديدة للصراعات والجريمة المنظمة ، تستهدف الهجمات السيبرانية البنى التحتية وأنظمة الاتصالات وحتى المؤسسات المالية والعسكرية لذا يمكننا تعريف الفضاء السيبراني انه بيئة رقمية شاملة تنشأ من خلال تفاعل بين شبكات الحواسيب،أنظمة المعلومات عبر الإنترنت ويمتلك الفضاء السيبراني مجموعة من الخصائص من خلال سهولة الوصول،التطور المستمر والتهديدات الأمنية كما أبرزنا أنواع الهجمات كالبرمجيات الخبيثة وهجمات الفدية، التصنت ،و تم التطرق إلى تطور القرصنة الإلكترونية حيث مرت بعدة مراحل من بداية السبعينات إلى يومنا هذا وتبيان أهم أسبابها كالتجسس،وحب التعلم والشهرة والتحدي، كما تم توضيح الأمن السيبراني وأهم أبعاده منها الاقتصادية والقانونية والاجتماعية، وتفسير الاختراقات الرقمية هي الدخول غي المصرح به إلى أنظمة المعلومات بهدف التلاعب بالمعلومات إلكترونيا وأهم فئاتها المستهدفة الشركات والحكومات والأفراد والمنظمات العسكرية.يمكننا القول أن القرصنة والاختراقات مظاهر حادة لهذه الصراعات في الفضاء السيبراني.

**الفصل الثاني: القرصنة الالكترونية
وتهديدات امن الدول بين الادارة
والمواجهة**

الفصل الثاني: القرصنة الالكترونية وتهديدات امن الدول بين الادارة والمواجهة

صار السلم السيبراني والأمن في الفضاء المعلوماتي اليوم أحد رهانات الدول في الحفاظ على أمنها القومي وضمان سيادتها الوطنية وسيطرتها على مجالها السيبراني بالشكل الذي يحقق أكبر قدر من الحصانة للدفاعات الإلكترونية من جهة، ومن جهة أخرى يضمن لها القدرة الكافية على تطوير إمكاناتها الرقمية وتعزيز منظومتها السيبرانية حتى تكون رقما أساسيا في المعادلة السيبرانية الأمنية وطنيا وإقليميا ودوليا في ظل احتدام الصراعات والحروب السيبرانية. وإذا كان الأمن الإلكتروني يعني بالحماية وغياب التهديد لقيم المجتمع الأساسية وغياب الخوف من خطر تعرض هذه القيم للهجوم، فإن الفضاء السيبراني قد فرض إعادة التفكير في مفهوم الأمن، والذي يتعلق بدرجة تمكن الدولة من أن تصبح في مأمن من خطر التعرض للهجوم، والإجراءات الحماية ضد تعرض المنشآت الحيوية والبنى التحتية للتهديد خلال استخدام السيئ لتكنولوجيا الإيصال والمعلومات، كما فرض أيضا إعادة النظر في المفاهيم التقليدية للحرب والقوة والسيادة .

المبحث الأول: جدلية الصراع الإلكتروني في الفضاء السيبراني و بروز القوة الإلكترونية

تعكس التحولات الكبيرة في كيفية ممارسة القوة والنفوذ في العصر الرقمي، مع تطور التكنولوجيا أصبح الفضاء السيبراني ساحة جديدة للصراعات بين الدول والمنظمات والأفراد، تستخدم الهجمات السيبرانية كأداة من أدوات السياسة الخارجية، حيث تسعى الدول لاختراق أنظمة خصومها للحصول على معلومات إستراتيجية أو لتعطيل قدراتهم وبالتالي هذا الصراع يعكس تعقيدات العلاقات الدولية في العصر الرقمي، و بروز القوة الإلكترونية كعنصر أساسي في السياسة الدولية يتطلب فهما عميقا للتحديات والفرص التي تقدمها، بالإضافة إلى تطوير استراتيجيات فعالة لمواجهة التهديدات السيبرانية، وهذا ما سنتناوله في المطالب التالية:

المطلب الأول: عصر الصراع الإلكتروني في الفضاء السيبراني

بعد أحداث 11 ديسمبر 2001 بدأ التركيز على الفضاء الإلكتروني كتهديد أمني جديد بفعل أحداث دولية كان أبرزها استخدام تنظيم قاعدة له كساحة قتال ضد الولايات المتحدة، وفي عام 2008 برز بوضوح الفضاء الإلكتروني كمجال جديد في العمليات العدائية في الصراع بين استونيا وروسيا وذلك عن طريق إغراق المواقع الإلكترونية بسيل من البيانات غير اللازمة، حيث وجهت ما يقارب من مليون حاسبة من عدة نقاط في العالم، واستهدفت المواقع الحكومية والصحف والجامعات والمستشفيات والمصارف وخدمات الإطفاء والإسعاف وذلك بهدف إسقاط وشل الحكومة الإستونية، إذا يستطيع أحد أطراف الصراع أن يوقع خسائر فادحة بالطرف الآخر ويتسبب في شل منظومة المعلومات الخاصة به من خلال قطع أنظمة الاتصال بين الوحدات العسكرية بين بعضها البعض أو تضليل معلوماتها أو سرقة المعلومات سرية عنها من خلال التلاعب بالبيانات الاقتصادية والمالية.¹

وجاء الهجوم الإلكتروني بفيروس "ستاكسنت" على برنامج إيران النووي عام 2010 ليمثل نقله هامة بالتطور في مجال الأسلحة الإلكترونية، وعلى الرغم من الدور السياسي الذي لعبته شبكات التواصل الاجتماعي في حالة الثورات العربية في مطلع عام 2011 إلا أنها مثلت نقطة هامة لدعم الاهتمام الدولي بأمن الفضاء الإلكتروني، وبرزت محاولات للسيطرة عليها بعد تصاعد الاحتجاجات في أكثر البلدان ديمقراطية وهي بريطانيا والولايات المتحدة، وخلال العقد الأخير شهد المجتمع الدولي صعود قضايا الأمن الإنساني المشترك والتغير في المجال الاقتصادي والاعتماد المتبادل وضعف دور الدولة وبرز الفاعلين من غير الدول.²

¹ - دليلة العوفي، الحرب السيبرانية في عصر الذكاء الاصطناعي ورهانات على الأمن الدولي، مجلة الحكمة للدراسات الفلسفية، المجلد 9، العدد 02، جامعة الجزائر 3، تاريخ النشر 2021/10/7، ص 787،

² - نورة شلوش، مرجع سبق ذكره، ص 192

الفرع الأول: التهديدات التي يواجهها الفضاء الإلكتروني في البيئة الأمنية

في ظل التطور المتسارع لتكنولوجيا أصبح الفضاء الإلكتروني جزءاً لا يتجزأ من البنية التحتية للدول والمؤسسات مما جعله بيئة حيوية وحساسة تتعرض لتهديدات متزايدة ومعقدة وهذه التهديدات هي:

- ارتباط العالم المتزايد بالفضاء الإلكتروني بما عمل على زيادة خطر تعرض البنية التحتية الكونية للمعلومات لهجمات الإلكترونية.
- انسحاب الدولة من القطاعات الإستراتيجية لصالح القطاع الخاص وخاصة بالمنشآت الحيوية.
- تأثير مواجهة الحرب الإلكترونية على حرية استخدام الفضاء الإلكتروني
- إشكالية التعامل الدول مع الشركات التكنولوجية متعددة الجنسيات والتي أصبحت تفوق قدراتها مثل مواقع الشبكات الاجتماعية كالفيسبوك وتويتر واليوتيوب الذين أصبحوا فاعلين دوليين.¹

حيث تعتبر الدولة فاعل محوري في تسيير الفضاء الإلكتروني انطلاقاً من إمكاناتها المادية والبشرية والقانونية، وذلك لابد للدولة التحكم في مجال الفضاء السيبراني ، وهو الفضاء الذي يزاحمها فيه العديد من الفواعل الأخرى، التي قد تصل حد تهديد مصالح الدولة نفسها .وقد أوضح تقرير المؤسسة العالمية المستقلة في مجال استشارات المخاطر السياسية، الأمنية أن نسبة الزيادة في إعداد الهجمات السيبرانية ذات الدوافع السياسية خلال عام 2015 بلغت 56 بالمائة وتوقع تقرير أن أعداد الدول القومية القادرة على شن الهجمات الإلكترونية ذات التأثير الشديد خلال عام 2016 بلغت حوالي 45 دولة مقارنة

¹ _المرجع نفسه ، ص 788

بحوالي 10 دول فقط مقارنة بعام 2014 وتشكل القدرات الدفاعية والهجومية الإلكترونية للدول في أغلب الأحيان من الجنود والمحاربين السيبرانيين.¹

الفرع الثاني: الفضاء الإلكتروني ساحة جديدة لصراع بشكله التقليدي ذو طابع إلكتروني

يعكس النزاعات التي تخوضها الدول أو الفاعلين من غير الدول على خلفيات دينية أو عرقية أو إيديولوجية أو اقتصادية أو سياسية. ويتمدد الصراع الإلكتروني بداخل شبكات الاتصال والمعلومات متجاوزا الحدود التقليدية وسيادة الدول، ويؤثر ذلك في امتداد مجاله وتداعياته أو آثاره، وأضافت عملية تعدد استخدام والفاعلين والمصالح لتنوع أشكال الصراع وأهدافه. ولأن الصراعات الفعلية تستعمل شتي أنواع الأسلحة التدمير الاقتصادية والإلكترونية والسياسية والإعلامية، فإنها لم تتوان عن استخدام الفضاء الإلكتروني، بماله من تأثير أمني وعسكري لتزحف جبهات القتال التقليدية بشكل مواز لها إلى ساحة الفضاء الإلكتروني.²

وكانت روسيا قد تعرضت لهجمات أيضا خلال استضافتها لبطولة كأس العالم عام 2018 حيث واجهت روسيا خلالها حوالي خمسة وعشرين مليون هجوم إلكتروني على البنية التحتية لتكنولوجيا المعلومات، وفي مواجهة أخرى شهد عام 2019 صرح نعيم شعار، الضابط في وحدة الدفاع الإلكتروني التابعة للجيش الإسرائيلي لوكالة بلومبيرغ الأمريكية بأن وحدة أحبطت عملية اختراق إيرانية استهدفت نظام التنبيه ضد الصواريخ في إسرائيل، وبين شعار أن هذه المحاولات الإيرانية بدأت منذ فترات تعود لعام 2017 مبينا أن التقنيين الإسرائيليين رصد وبرمجيات خبيثة تحاول الدخول لمنظومة التنبيه التي تعمل على إطلاق

¹ _ غريب حكيم، شرقي صبرينة، تداعيات الحرب الإلكترونية على العلاقات الدولية، مجلة دفا تر السياسة والقانون، المجلد

12 العدد 02، المدرسة الوطنية العليا للعلوم السياسية، الجزائر، ص 98

² _ نورة شلوش، مرجع سبق ذكره، ص 193

الفصل الثاني القرصنة الإلكترونية وتهديدات امن الدول بين الادارة والمواجهة

تحذير في المدن الإسرائيلية عند حصول هجمات صاروخية التي تمنع المخترقين من الوصول إلى أنظمة التحكم.¹

وتجدر الإشارة إلا أن التحديات في الفضاء السيبراني تتطلب مواكبة التحولات الحديثة في تكنولوجيا ومفاهيم امن المعلومات، وأدوات الصراع الإلكتروني غير المرئية، مما يستلزم إعادة النظر في فهم حقيقة مفهوم الأمن الشامل، فالسلوك البشري يعد أمراً ضروريا لفهم طبيعة السباق وأدوات الحرب وأهدافها، واتجاه موازين القوة السياسية والعسكرية والتكنولوجية إقليمياً ودولياً.²

وتقوم عقيدة الناتو العسكرية على تحقيق المرونة وسلامة السيبرانية والكشف المبكر للهجمات السيبرانية والتعامل معها واعتبار الفضاء السيبراني ميدان جديد للعمليات العسكرية أيضاً تبني مفهوم الدفاع السيبراني الوقائي، وحق في اللجوء إلى استعمال القوة في الدفاع عن النفس في الفضاء السيبراني كما اعتبرت الدفاع السيبراني جزء مهم من الدفاع الجماعي أما في الولايات المتحدة الأمريكية فقد أعدت الإدارات المتعاقبة على البيت الأبيض في إطار التصدي للتهديدات السيبرانية المتنوعة. من خلال السعي لشن هجمات وإتباع أسلوب الدفاع من خلال ضرب مصادر التهديد خارج حدود الولايات المتحدة الأمريكية قبل أن تؤثر في قدرة وزارة الدفاع الأمريكية على الاستجابة والدفاع عن المصالح الوطنية.³

وتعدد الفاعلين في الفضاء السيبراني كالجماعات الإرهابية والأفراد وشركات متعددة الجنسيات، يمتلك بعضها قدرات التفوق الدول كجوجل فيسبوك مايكروسوفت تمتلك قواعد

¹ _صلاح حيدر عبد الواحد، حروب الفضاء الإلكتروني دراسة في مفهومها وخصائصها وسبل مواجهتها، رسالة مكملة لمتطلبات الحصول على درجة الماجستير في العلوم السياسية، كلية الآداب والعلوم، جامعة الشرق الأوسط، تموز 2021، ص 33

² _دلالي الجيلالي، بالبشير يعقوب، مرجع سبق ذكره، بدون صفحة

³ _بوظلاعة وداد، بوكورو منال، مرجع سبق ذكره، بدون صفحة

الفصل الثاني القرصنة الالكترونية وتهديدات امن الدول بين الادارة والمواجهة

بيانات ضخمة من خلالها تستكشف وتستغل السوق العالمية للتأثير على اقتصاديات الدول وثقافة مجتمعاتها، والمنظمات الإجرامية والتي تختص بعمليات السطو السيبراني على المصارف وتحويل الأموال كما تستعمل الإنترنت أيضا لأغراض الاتجار بالمخدرات والأسلحة والبشر، لأغراض ربحية تبلغ التكلفة جرائمها مليارات الدولارات.¹

حيث أصبح أطراف الصراع يتسبب في شل البنية التحتية المعلوماتية وهو ما يسبب خسائر عسكرية أو تضليل معلوماتها أو سرقة معلومات سرية عنها أو من خلال التلاعب بالبيانات الاقتصادية والمالية وتزييفها أو مسحها من أجهزة الحواسيب أمام هذا الوضع دفع بالدول إلى حشد جيوشها من الخبراء المعلوماتيين لضمان امن وسلامة أنظمتها المعلوماتية ومواجهة مختلف الاختراقات التي قد تحدث حيث تعمل على تنفيذ عمليات التجسس وإدارة الهجمات الإلكترونية بالإضافة إلى شن الحروب المعلوماتية في وسائل الإعلام ومواقع التواصل المختلفة.²

المطلب الثاني: المخاطر والتهديدات في الفضاء السيبراني

إن التطور الدائم والمتزايد لتكنولوجيا أدى بالضرورة إلى اتساع الفضاء السيبراني. فبرغم من إيجابيات الانترنت وسهولة استخدامها إلا أن هذا الأخير أدى إلى العديد من المخاطر التي هددت أمن الدول وأثرت على استقرارها نتطرق إليها في الفروع التالية:

الفرع الأول: مخاطر اجتماعية وثقافية واقتصادية

إن التطور الدائم والمتزايد لتكنولوجيا المعلومات أدى بالضرورة إلى اتساع الفضاء السيبراني . فبرغم من إيجابيات الإنترنت وسهولة استخدامها إلا أن هذا الأخير أدى إلى

¹ _المرجع السابق.

²دليلة العوفي، مرجع سبق ذكره، ص 792

العديد من المخاطر التي هددت أمن الدول وأثرت على استقرارها نتطرق إليها في الفروع التالية :

تهديد القيم والأخلاق: ومن الأبعاد الاجتماعية الحامية من تدمي المستويين القيمي والأخلاقي فالمحتويات غير المشروعة والغير مرغوب بها ذات التأثير السلبي على أخلاقيات المجتمع وزيادة نسبة الممارسات الإجرامية كالإباحية، والترويج للاتجار بالممنوعات، والدعارة، والإرهاب، والتجنيد لقضايا تمس الأمن السيبراني، قادر على التعامل مع قواعد السلامة ومدرک للعواقب القانونية التي يمكن أن تترتب على التعرض لسلامة الأفراد والمؤسسات ورؤوس الأموال.¹

التجارة باستخدام الهندسة الاجتماعية: هي أسلوب يستخدمه الخصوم لاستدراجك للكشف عن المعلومات الحساسة. يمكنهم طلب الحصول على دفع نقدي أو الوصول إلى بياناتك السرية. ويمكن دمج الهندسة الاجتماعية مع أي من التهديدات.²

هجمات الفدية: الهجوم الذي يتضمن تشفير البيانات على النظام المستهدف والمطالبة بفدية مقابل السماح للمستخدم بالوصول إلى البيانات مرة أخرى³ لقد أصبحت المعلومات في عصرنا الحالي مصدر قوة نادر وهام لمن يمتلكها، سلاح هجوم وسلاح دفاع. فمعرفة المعلومات ذات القيمة عن الخصم لا تقدر بثمن وخاصة في وقت الأزمات.⁴

¹ _ إسلام فوزي، مرجع سبق ذكره، ص112

² _ إسلام مصطفى، جمعة مصطفى، جريمة اختراق الأمن السيبراني و حماية استخدام البيانات والمعلومات في القانون المصري، المجلة الاجتماعية القومية، المجلد 26، العدد 2، القاهرة، مايو 2019 ص 726_727

³ _ هيئة الإعلام، الأمن السيبراني، قسم الدراسات والاتصال والعلاقات العامة 2021 _ص12

⁴ _ عبد الحفيظ ديب الاختراق الأمني، الاختراق الأمني للدولة الوطنية في عصر ثورة المعلومات، كلية العلوم السياسية والإعلام، جامعة الجزائر 03، ص217

1. **تهديد البنية التحتية:** لا يشمل مفهوم الحرب السيبرانية استهداف القدرات والأنظمة العسكرية وحسب، ولكن أيضا استهداف البنية التحتية الحيوية للمجتمع بما في ذلك الشبكات الذكية وشبكات المراقبة الشرفية وحياسة البيانات التي تسمح لها بالعمل والدفاع عن نفسها ومن ثم يتمخض النزاع السيبراني عن عواقب تُهدد الحياة إذا تم إفساد البنية التحتية للمعلومات.¹

ولعل من أهم المخاطر الاقتصادية التي تتحقق من خلال التنظيمات الإرهابية:

- اختراق النظام المصرفي وإلحاق الضرر بأعمال البنوك وأسواق المال العالمية
- تعطيل عمليات التحويل المالي، مما يلحق الأذى بالاستثمار الأجنبي وبالثقة بالاستثمار عامة، وإلحاق الأذى بالاقتصادي الوطني²

ويستخدم وسطاء التهديد معرفتهم بالثغرات لإنتاج تهديدات جديدة ضد أحد الأصول وبالنسبة لأصول المعلوماتية فإن التعديل على شفرة البرمجيات لمعالجة الثغرات يعرف بـ "التصحيح الأمني" وأفادت إدارة الأمن الداخلي لقاعدة بيانات الثغرات الوطنية الأمريكية بوجود 3532 ثغرة في عام 2011 أي بمعدل 10 ثغرات جديدة تكتشف كل يوم. وهذا في الواقع يعد تحسنا مقارنة بأرقام عام 2009 وعام 2010³

رغم التقدم الكبير الذي أحرزته الثورة التكنولوجية والفضاء الإلكتروني حول العالم في التقارب الزماني والمكاني، وجعلت العالم قرية صغيرة ترتبط بعضها البعض من خلال هذه

¹ _إسلام فوزي، مرجع سبق ذكره، ص112

² _ غجاتي سهيلة، راهم أميرة، مرجع سبق ذكره، ص32

³ _ أمن المعلومات، البرمجيات الخبيثة وأمن الحواسيب، لمزيد من التفاصيل أنظر

<https://darajat.ly> (26/5/2025_21 :14)

التكنولوجيا الجديدة، إلا أن هناك العديد من المخاطر التي أثرت على العديد من النواحي سواء كانت الاجتماعية أو الثقافية أو الاقتصادية أو البيئية...الخ.¹

الفرع الثاني: المخاطر السياسية والأمنية:

لم تعد الهجمات الإلكترونية مصدرا لتهديد الأفراد فقط بل تعدت ذلك لتهدد أمن الدول من خلال المخاطر السياسية والأمنية

التجسس الإلكتروني: CyberEspionage يعد أحد أنواع التجسس التقليدي ، باستخدام وسائل التكنولوجيا الفائقة، ومعظم الهجمات السيبرانية المتطورة التي تقع ضمن هذه الفئة حيث يتم الحصول على معلومات سرية بطرق غير مشروعة بهدف الحصول على أفضلية اقتصادية، أو إستراتيجية أو عسكرية باستخدام تقنيات إلكترونية أو الشبكات السلكية أو الأقمار الاصطناعية.²

2. الهجمات السيبرانية: هي استغلال الحاسبات وتكنولوجيا المعلومات في تخريب وتدمير البنية المعلوماتية للخصوم ، بل وتعطيل شبكات الدفاع الجوي واختراق أنظمة المعلومات للبريد الإلكتروني لمكاتب رؤساء الدول والتجسس عليهم وفق خطة ممنهجة.³

تقوم الدولة المعتدية باستخدام الفضاء السيبراني لتنفيذ الهجوم السيبراني من أجل تدمير البيانات التي تحتوي عليها الأجهزة، وغير ذلك من الأسباب كنقل المعلومات للاستفادة منها للتفوق على الدولة المعتدى عليها أو لتعطيل تلك الأجهزة أو التقليل من كفاءة تشغيلها، وقد تلجأ الدول المعتدية إلى ارتكاب تلك الهجمات قبل شن الحروب على ساحة الاقتتال

¹ _عجاتي سهيلة، راهم أميرة، مرجع سبق ذكره، ص 32

² _ طماطي سالم، مرجع سبق ذكره، ص22

³ _ إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، كلية الحقوق والعلوم السياسية، جامعة العربي تبسي، تبسة / الجزائر، ص108

لإضعاف القوة العسكرية للدولة المُعتدى عليها أو يتزامن الهجوم أثناء الضربات الجوية من أجل تعطيل أجهزة الدفاع وصد هذه الضربات¹

التنصت: يعرف التنصت بعبارات شائعة مثل استطلاع الشبكات واكتشاف الحزم. يمكن أن يستخدم التنصت لاكتشاف الهجمات على الشبكات. ومن الأمثلة على البيانات القابلة للتأثر بالتنصت النسخة الأولى من بروتوكول (snmp) الذي يرسل نص التعريف (community string) بالنص الواضح غير المشفر. ويستطيع القرصان الماكر تشغيل أدوات تنصت على بروتوكول (snmp) وجمع معلومات قيمة عن معدات الشبكة وطرق إعداد كل منها. ومن البروتوكولات التي تقبل التنصت بروتوكول (tip/ IP) حيث يتم مراقبة الحزم والتقاط كلمات المرور وأسماء المستخدمين عند مرورها بالشبكة وبيانات بطاقات الائتمان والبيانات الشخصية والكثير من البيانات المختلفة التي تقود لتسهيل الوصول إلى شبكة الضحية ودخول أجهزة الخادم المتوفرة فيها.²

إتلاف المعلومات أو تعديلها: وهي هجمات تهدف إلى الوصول لمعلومات الضحية عبر شبكة الانترنت أو الشبكات الخاصة، والقيام بعملية تعديل البيانات الهامة دون أن يكتشف الضحية ذلك، فالبيانات تبقى موجودة لكنها مضللة، وقد تؤدي إلى نتائج كارثية خاصة إذا تمثلت البيانات في معلومات أمنية أو مواعيد أو خرائط سرية أو خاصة بالصناعات الحساسة لاسيما الصناعات العسكرية.³

¹ _ وسام محمود عرفان، سبل مكافحة الهجمات السيبرانية دولياً، مجلة الدراسات القانونية والاقتصادية، المجلد 10، العدد 3، سبتمبر 2024، ص 2994

² _ إوراغ كريم، الاختراق الالكتروني في الفضاء السيبراني وأفضل الطرق للحماية منه، مجلة التطوير العلمي للدراسات والبحوث، المجلد 2، العدد 4، الجزائر، 2020، ص 35

³ _ يعوني ليلي، مرجع سبق ذكره، ص 12

العرضية للكابلات البحرية :تعد الكابلات submarine cable جزء هام لتوفير خدمة الاتصالات بين دول العالم في مجال الإنترنت، وشبكات الكمبيوتر وغيرها، فمنذ عام 2005 أصبحت الكابلات البحرية مأهولة على مجال الاتساع والانتشار ، كما تعرضت تلك الكابلات إلى عدد من المشاكل التي تؤثر سلبا على أعمال البنى التحتية بالضرر، حيث تقع في مياه المحيط العميق.¹

هجمات الحرمان من الخدمة: ويتم فيها إطلاق حزمة كبيرة من الطلبات والمهمات على خوادم الضحية بصورة تفوق قدرة الخادم أو الجهاز على معالجتها والاستجابة لها ، مما يؤدي إلى توقفه بشكل جزئي أو كلي أو إبطاء عمله ،وهذا ما ينتج عنه ضررا للمستخدم النهائي، وتستعمل هذه الهجمات بكثرة ضد مواقع الانترنت أو البنوك أو المؤسسات بهدف التأثير عليها أو لدفع فدية مالية.²

المطلب الثالث: القوة الإلكترونية للدول وأثارها

أصبحت القوة الإلكترونية للدول من أهم عناصر القوة الوطنية للدول في العصر الرقمي حيث تتجلى هذه القوة من خلال القدرة على حماية البنى التحتية الرقمية ، تنفيذ الهجمات الإلكترونية عند الضرورة والتأثير على الرأي العام عبر وسائل الإعلام الرقمية

الفرع الأول: القوة الإلكترونية

يعد الهدف الأسمى للأمن السيبراني هو القدرة على مقاومة التهديدات المعتمدة وغير المعتمدة الاستجابة والتعافي ، وبالتالي التحرر من الخطر أو الأضرار الناجمة عن تعطيل أو إتلاف تكنولوجيا المعلومات والاتصالات أو بسبب إساءة استخدام تكنولوجيا المعلومات والاتصالات ويتطلب حماية الشبكات وأجهزة الكمبيوتر، والبرامج والبيانات من الهجوم أو

¹ _ طماطي سالم، مرجع سبق ذكره، ص 22

² _ يعوني ليلي، مرجع سبق ذكره، ص 12

الفصل الثاني القرصنة الالكترونية وتهديدات امن الدول بين الادارة والمواجهة

الضرر أو الوصول غير المصرح به ، ونتيجة لأهمية الأمن السيبراني في واقع مجتمعات اليوم فقد جعلته العديد من الدول على رأس أولوياتها ، خاصة بعد الحروب الإلكترونية التي بدأت تظهر تجلياتها بين بعض الدول الكبرى.¹

التي تندرج تحت إطار الصراع الإلكتروني بشكل يختلف عن مسمى الحرب الإلكترونية والذي يشير إلى تطبيقات عسكرية للفضاء الإلكتروني ويتم الإشارة إليه بالهجوم الإلكتروني عندما يتم اعتباره نمطا من الهجوم يتم شنه من قبل الدولة أو الفاعلين من غير الدول والتي يكون لها تداعيات على الأمن القومي للدول والأمن العالمي. ويقدم جوزيف ناي مصطلح القوة الإلكترونية لفهم الدور الذي تلعبه الإنترنت في تشكيل قدرة الأطراف المؤثرة، والتي تعد من أبرزها الأطراف الدولية والدول الناشئة، لتحقيق أهدافها وبأن العصر الإلكتروني قد قلل من صعوبات الدخول وأعطى أطراف القدرة والقوة ولكن القوة الإلكترونية في الوقت نفسه فرضت تحديات كبرى على هؤلاء الأطراف.²

ويكشف أن مفهوم القوة الإلكترونية تختلف عن ما يسمى الحرب الإلكترونية التي تقتصر على التطبيقات العسكرية للفضاء الإلكتروني ويتم الإشارة إليه بالهجوم الإلكتروني ويقول إذا كانت ثروة المعلومات لها تأثير على تطوير الجوانب العسكرية للدول فإن لذلك أبعاد سياسية، اجتماعية، حيث ازدادت القدرات التدميرية للأسلحة. كما تؤكد الدراسات أن ممارسة القوة عبر الإنترنت تعد إرهابا إذا صاحبها دوافع سياسية مثل التأثير على القرارات الحكومية أو الرأي العام ويتم ذلك من خلال أبعاد فالبعد الأول يتمثل في توفير المعلومات عن الأهداف المنشودة لتنفيذ العمليات الإرهابية التقليدية.³

هذا الوضع أدى إلى تغيير في مفهوم القوة الوطنية للدولة ، فبات بالإمكان تعريفها بأنها مجموعة الوسائل ، والطاقت، والإمكانات المادية وغير المادية المنظورة وغير

¹ _ عيش مرسى، خيمود محمد، مرجع سبق ذكره، ص 98

² _نورة شلوش، المرجع السابق، ص 198

³ _ محمد الحمامصي، القوة الإلكترونية عنصر أساسي مؤثر في النظام العالمي، مقال، 22 أوت 2014، بدون صفحة

المنظورة التي بحوزة الدولة ، ويستخدمها صانع القرار في فعل مؤثر يحقق مصالح الدولة و تؤثر في سلوك الوحدات السياسية الأخرى.¹

أما البعد الثاني فيستخدم فيه الفضاء الالكتروني للتأثير على المعتقدات مثل تحريض على بث الكراهية وحرب الأفكار، أما البعد الثالث فيتم في صورة رقمية حيث تقوم جماعات المتطرفة على اختلاف أشكالها باستغلال مزايا الفضاء الالكتروني كعنصر حيوي لدعم وتحقيق أهدافها ومنفذ لوجيستي داعم وحاضن لنشاطها الإعلامي في مناطق مختلفة من العالم.²

الفرع الثاني: أثر الفضاء الالكتروني على مفهوم القوة في العلاقات الدولية

من الأمور المستقلة في العلاقات الدولية أن مصادر قوة الدولة وأشكالها تتغير، فإلى جانب القوة الصلبة ممثلة في القدرات العسكرية والاقتصادية يتزايد الاهتمام بالبعد غير المادية للقوة ، ومن ثم بروز القوة الناعمة التي تعتمد على جاذبية النموذج والإقناع ، ومع ثورة المعلومات ظهر شكل جديد من أشكال القوة وهي القوة الالكترونية التي لها تأثير كبير على المستوى الدولي والمحلي، فمن ناحية أدت إلى توزيع وانتشار القوة بين عدد اكبر من الفاعلين مما جعل قدرة الدولة على السيطرة موضع شك ، ومن ناحية أخرى منحت الفاعلين الأصغر قدرة أكبر على ممارسة كل من القوة الصلبة والقوة الناعمة عبر الفضاء الالكتروني وهو ما يعني تغيراً في علاقات القوى في السياسة الدولية³

وقد حدد جوزيف ناي ثلاث أنواع من الفاعلين الذين يمتلكون القوة الالكترونية:

¹ _ عيش موسى، خيمود محمد، مرجع سبق ذكره، ص98

² _ محمد الحماسي، مرجع سبق ذكره، بدون صفحة

³ _ محمود علي عبد الرحمان، الفضاء الإلكتروني وأثره على مفاهيم القوة والأمن والصراع في العلاقات الدولية، مجلة كلية السياسة والاقتصاد، المجلد16، العدد15، يونيو2022، ص429

1. **الدول:** الدول التي لديها القدرة على تنفيذ هجمات إلكترونية وتطوير البنية التحتية وممارسة السلطات داخل حدودها

2. **الفاعلين من غير الدول:** يستخدم هؤلاء الفاعلون القوة الالكترونية لأغراض هجومية بالأساس، إلا أن قدرتهم في تنفيذ أي هجوم إلكتروني مؤثر تتطلب مشاركة ومساعدة الأجهزة الاستخباراتية متطورة ولكن يمكن اختراق المواقع الالكترونية واستهداف الأنظمة الدفاعية

3. **الأفراد "القرصنة":** الذين يمتلكون معرفة تكنولوجيا عالية والقدرة على توظيفها، وعادة ما تكون هناك صعوبة في الكشف عن هوياتهم، ومن الصعب ملاحقتهم.¹

4. **شركات متعددة الجنسيات:** تمتلك بعض الشركات التكنولوجيا موارد القوة تفوق قدرة بعض الدول، ولا تقتصر سوى شرعية ممارسة القوة التي مازلت حkra على الدول، فخدام شركات مثل، فيسبوك، ميكروسوفت، تسمح لها بامتلاك قواعد البيانات العملاقة التي من خلالها تستكشف وتستغل الأسواق، وتؤثر في اقتصاديات الدول وفي ثقافة المجتمعات وتوجهاتها وهذا ما حدث في الأزمة بين شركة جوجل والصين حول المحتوى أو ل فضيحة تسريب البيانات مستخدم فيسبوك لصالح شركة "كامبردج أناليتيكا" التي تم الاستعانة بها لصالح حملة المرشح الجمهوري ترامب.²

وتعد روسيا والصين والولايات المتحدة من اكبر القوى في مجال الاستحواذ على القوة الالكترونية القادرة على توفير أقصى درجات الأمن الالكتروني، وهو ما فرض على الدول وجود إجراءات حماية عبر تبني سياسات دفاعية ، تتضمن عمليات الحماية والتطوير لإجراءات الدفاع ضد الأخطار المحتملة وحماية نظم المعلومات ، ومنع تعرضها لعمليات

¹ _ المرجع نفسه، ص 431

² _ المرجع نفسه، ص 432

الفصل الثاني القرصنة الالكترونية وتهديدات امن الدول بين الادارة والمواجهة

هجومية معادية، وتعزيز الأمن الالكتروني بأبعاده المتعلقة بالبرمجيات والبنية التحتية ، ومنع استغلاله في الحرب النفسية .من أجل ضمان أمن وسلامة الفضاء الالكتروني إلى جانب تبني سياسات هجومية في الفضاء الالكتروني عبر اتخاذ إجراءات لمهاجمة مصادر التهديد وتعقب الفاعلين في الهجوم¹

فتناول **ميشل فاتيس** بعض حالات الصراع السياسي الذي أدى إلى هجمات على أنظمة الدول الالكترونية مثل الصراع بين الهند وباكستان حول إقليم **كشمير** ، والصراع الإسرائيلي الفلسطيني وتدخل منظمة حلف الشمال الأطلسي الناتو في حرب كوسوفو، والصراع بين الولايات المتحدة الأمريكية والصين على خلفية اصطدام طائرة مقاتلة صينية بطائر الاستطلاع الأمريكية انتهت بشن الهجمات الالكترونية على الولايات المتحدة²

وير جوزيف ناي أن الدولة سوف تظل هي الفاعل المهيمن على الفضاء الالكتروني ولكن هناك فواعل أخرى سوف تشارطها في هذا الفضاء الالكتروني وسوف نجد صعوبة في السيطرة عليه فالحكومات قلقة في حالة تسرب المعلومات وتدفقها وصعوبة السيطرة عليها، ويرى أيضا أن القوى الكبرى ليست مساحة نفسها التي يمكن من خلالها السيطرة على الفضاء الالكتروني مقارنة بقدرتها على السيطرة على الإقليم البري والجوي إن الكيانات الافتراضية التي تنشأ عبر الانترنت.³

ويؤكد أن الفضاء الالكتروني لن يزيل سيادة الدول أو حدودها الجغرافية ولكن سوف يؤثر على مفاهيم القوة وتحولات القوة وأدواتها ويضيف أن الدول الكبرى التي تمتلك القوة

¹ _ نورة شلوش، مرجع سبق ذكره، ص 199، 200

² _ إيهاب خليفة، القوة الالكترونية "كيف يمكن أن تدير شؤونها في عصر الإنترنت، العربي للنشر والتوزيع، القاهرة،

2017، ص 19

³ _ المرجع نفسه، ص 25

الناعمة والصلبة قبل الولايات المتحدة الأمريكية وجدت نفسها تواجه مشاكل في السيطرة على حدودها على الانترنت¹

المبحث الثاني: النماذج الحديثة للاختراقات السيبرانية خلال الفترة (2016_2020)

إن انتشار الشبكات الحاسوبية واعتماد المؤسسات العامة والخاصة عليها، فإن أي خلل يصيبها قد يؤثر على عمل المؤسسات وتعطيل أعمالها في خدمة المواطنين، ومع سوء استخدام الانترنت والأخطار المترتبة على ذلك أصبح التحدي الأساسي للدول هو إمكانية مواجهة التهديدات التي هيا تتزايد وتتطور مع تطور التكنولوجيا، فقد تعرضت الدول لعدة اختراقات الكترونية خلال الحروب السيبرانية، لذا سنقف في هذا المبحث على أهم الاختراقات الالكترونية في العصر الحديث .

المطلب الأول: اختراق مركز التحكم الرئيسي بكيف - أوكرانيا عام 2016

شهدت الحرب السيبرانية بين أوكرانيا وروسيا عدة اختراقات إلكترونية، ويعتبر اختراق مركز التحكم الرئيسي بكيف من أهم محطات الاختراق الإلكتروني في العصر الحديث، وسنتعرف في هذا المطلب لمعرفة مركز التحكم الرئيسي وكيف تم اختراقه.

الفرع الأول: مركز التحكم الرئيسي

هو المركز المشترك للسيطرة والتنسيق بشأن وقف إطلاق النار واستقرار خط ترسيم الحدود، والمختصر **jccc** وهو منظمة تتألف من ضباط عسكريين أوكرانيين وروس، ودورهم هو المساعدة في تنفيذ اتفاقيات مينسك لوقف إطلاق النار وضمان سلامة مراقبي منظمة

¹ _ المرجع نفسه، ص 26

الأمن والتعاون في أوروبا في الحرب الروسية الأوكرانية ،تم تأسيسه في 26 سبتمبر 2014¹.

أما فيما يخص "اتفاقية مينسك الثانية" فإنه كان هناك تخوف في أواسط الأطراف بأن اتفاق "مينسك الثاني" يذهب أبعد من الاتفاق الأول الذي نص بدوره على وقف إطلاق النار ،وسحب الأسلحة الثقيلة .²

أقامت اللجنة المشتركة للتعاون العسكري مقرها في سوليدار في منطقة دونيتسك الأوكرانية .في أكتوبر 2014 ، انتقلت إلى ديبالت سيف في 21 يناير 2015 ،عادت الوحدة الروسية إلى سوليدار بسبب تدهور الوضع ، في الأول من فبراير أصابت عدة صواريخ مقر ديبالت سيف وبعد ذلك انتقل الأوكرانيون إلى سوليدار.³

الفرع الثاني: اختراق مركز التحكم الرئيسي

باتت أوكرانيا تنشر الخبراء السيبرانيين على الخطوط الأمامية للحرب ،يتبارزون مع نظرائهم الروس في نوع جديد من المعارك ألا وهي معركة التقنيات العالمية .⁴ ما يشهده العالم من هجمات إلكترونية مختلفة قد ينقلنا إلى نموذج جديد من الحروب يطلق عليه الحرب السيبرانية ، وهو ما استخدمته روسيا بجدارة في أكثر من دولة وأكثر من

¹ _مركز مشترك للتحكم والتنسيق، لمزيد من التفاصيل

انظر (<https://www.en.m.wikipedia.org>8/5/2025_18:30)

39_أسماء حداد، الحروب الهجينة :الأزمة الأوكرانية أنموذجا، مجلة مدارات سياسية، عدد ديسمبر 2017، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر 3، الجزائر، 2017، ص123

³ _ مركز مشترك للتحكم والتنسيق، مرجع سبق ذكره، بدون صفحة

⁴ _ غوردن كوريرا، هل أصبحت الحرب الروسية الأوكرانية معركة التقنيات المتقدمة، لمزيد من التفاصيل انظر (18:45_

<https://www-bbc.com.cnd.ampproject.org> (2025/5/8)

الفصل الثاني القرصنة الإلكترونية وتهديدات امن الدول بين الادارة والمواجهة

حالة فالقيادة الروسية عملت في السنوات القليلة الماضية بشكل دؤوب على تنمية قدرات روسيا في المجال السيبراني وتطويرها بشكل كبير.¹

كان أول هجوم سيبراني ناجح على شبكة كهرباء في ديسمبر 2015 حيث تم اختراق شبكة الكهرباء في المنطقة الغربية "ايفانو فرانكوفسك" مما أدى إلى الانقطاع التام في التيار الكهربائي على عموم المنطقة وفي العام التالي تكرر الاختراق لشبكة الطاقة الأوكرانية من قبل محترفين روس ، قامت أوكرانيا على الصعيد الآخر في 9 ماي من 2016 بشن تسع عمليات اختراق ناجحة لمواقع مجموعة "جمهوريات دونيتسك الشعبية" الانفصالية وأيضا اخترقت مواقع روسية للدعاية المناهضة لأوكرانيا بالإضافة لشركات عسكرية روسية² سنوات متتالية من الشد والجذب بين روسيا و أوكرانيا ، وشهدت العلاقات توترا متصاعدا حيث عبرت الحكومة الأوكرانية خلال عامي 2017، 2016 في تصريحات لوزارة الخارجية عن غياب العلاقات الدبلوماسية مع روسيا³

ففي عام 2016 تم اختراق المنظومة الإلكترونية الخاصة لمحطة التحكم الرئيسية بمدينة كييف في أوكرانيا والتي تتبعها أكثر من 60 محطة فرعية ،حيث تم اختراق حسابات العاملين في إدارة المحطة ومن ثم استغلال كلمات السر الخاصة بهم للدخول عن بعد والتحكم في المحطات الفرعية والوصول إلى الانقطاع التام للتيار الكهربائي وقد ترتب عن

¹ _أمني عصام، استخدام روسيا للقوة السيبرانية في إدارة تفاعلاتها الدولية، كلية التجارة وإدارة الأعمال، جامعة حلوان، 2021، لمزيد من التفاصيل انظر (2025/5/8_17:50) [https:// www.jpsssa.journals.ekb.eg](https://www.jpsssa.journals.ekb.eg)

² _المركز الديمقراطي، العمليات السيبرانية بين روسيا وأوكرانيا :قراءة في الأسباب والنتائج، 2024، لمزيد من التفاصيل انظر (2025/5/8_16:30) [https:// www.Democraticac.de.com](https://www.Democraticac.de.com)

³ _العابد نائلة، تداعيات الحرب الروسية الأوكرانية على العلاقات الدولية، مخبر القانون البنكي والمالي، المجلد 27، العدد 1، 2023، الجزائر، ص493

هذا الانقطاع لساعات طويلة العديد من الأضرار على كافة القطاعات سواء العسكرية أو المدنية¹.

تعد الحرب الروسية على أوكرانيا إحدى أكبر الأزمات التي تعيشها القارة الأوروبية منذ الحرب العالمية الثانية والتي ستكون لها حتما انعكاسات متعددة الأوجه على النظام العالمي برومته نتيجة المسار الذي اتخذته أبعاد الحرب والتوتر التي أعقبتها وطبيعة القوة الفاعلة لصياغة ملامحها الاقتصادية والعسكرية والسياسية وذلك أن شظايا الحرب ومخلفاتها والعقوبات التي طالت روسيا بما يشبه قنبلة نووية اقتصادية ستعكس أثارها وتنتظير شظاياها لتمس كل الدول التي تتقاطع مصالحها مع الجانبين الروسي والأوكراني²

المطلب الثاني: اختراق وزارة الصحة البريطانية 2017

في عام 2017 تعرضت وزارة الصحة البريطانية لهجوم إلكتروني واسع النطاق ، كان هذا الهجوم عبارة عن برنامج فدية، انتشر بسرعة في أنظمة الحواسيب حول العالم .

الفرع الأول: دراسة تحليلية للاختراق

في مايو 2017 تم استهداف وزارة الصحة البريطانية بفيروسات الفدية وتم تشفير الخوادم الرئيسية العاملة بالمنظومة الصحية وقواعد البيانات والتطبيقات التابعة لها وقد أدى ذلك إلى شلل المنظومة الالكترونية بالكامل كنتيجة لذلك تعطلت كافة الخدمات الصحية في نطاق واسع من المملكة المتحدة مما كان له بالغ الأثر في إحداث أضرار جسيمة على

¹ حسن هاني، حسن محمود، أثر التهديدات السيبرانية على الأمن القومي، دراسة حالة ماليزيا 2022، 2015 المركز الديمقراطي العربي، لمزيد من التفاصيل أنظر (19:05_ 2025/5/8) <https://www.denaticon.com>

² دمان ديبج محمد رشدي، الحرب الروسية الأوكرانية في الإعلام الرقمي دراسة تحليلية لمضامين موقع+aj عربي، مذكرة مقدمة لنيل شهادة الماستر، تخصص صحافة مكتوبة وإلكترونية، قسم الصحافة، كلية الإعلام والاتصال والسمعي البصري، جامعة صالح بوينيدر قسنطينة3، 2022،

الجزائر، ص25

الفصل الثاني القرصنة الالكترونية وتهديدات امن الدول بين الادارة والمواجهة

خدمات الصحية بالمستشفيات ومراكز الرعاية الصحية وهو ما مثل تهديدا خطيرا على حياة المواطنين المتواجدين أو المترددين على المستشفيات .¹

كشف تقرير جديد عن تمكن مجموعة من الهاكرز اليوم من اختراق ما لا يقل عن 16 مستشفى مختلفة في جميع أنحاء إنجلترا ، ما أدى إلى إصابة هيئة الصحة البريطانية NHS بحالة من الفوضى بعدما هددتهم الهاكرز بضرورة دفع فدية أو سيتم حذف الملفات الطبية الخاصة بالمرضى ، مما دفع الهيئة إلى العمل حاليا على تحويل المرضى في حالة طوارئ إلى مناطق أخرى حيث تضررت المستشفيات في لندن ،توتنغهام ، بلاكبيرن ،هيرتفورد شاير ، وكوم بريا ، ووفقا لما نشره البريطاني indelendent ، فأدت الهجمات إلى إصابة نظم تكنولوجيا المعلومات في الهيئة الوطنية لرعاية الصحية البريطانية .²

بفيروسات الفدية وهي عبارة عن برمجيات خبيثة تؤدي إلى إغلاق أنظمة الكمبيوتر ، ولن يتمكن أصحابها من استخدامها مرة أخرى إلا عند دفع مبلغ من المال ، حيث تكشف الرسالة الواردة من الهاكرز أنه يمكن استيراد الملفات ولكن فقط بشرط أن يحصلوا على 300 دولار من عملات البيتكوين ،محذرين من الارتفاع هذا المبلغ مع مرور الوقت أو أنهم قد يحذفون الملفات في نهاية المطاف ، من جهتها قالت الهيئة الوطنية للصحة العامة في بيان لها " أن عددا من منظمات الصحة الوطنية أبلغت شركة بأنها تأثرت بهجوم الفدية "³ موضحة أن الأمن السيبراني الوطني البريطاني يعمل حاليا على التحقيق في الحادث ، والذي تسببت فيه قطعة من البرمجيات الخبيثة تسمى " وأنا دكريبتور " فينا قالت هيئة

¹ _حسن هاني، حسن محمود، مرجع سبق ذكره، 10ماي 2025، 10:43

² _إكرام قصاص، اختراق هيئة الرعاية الصحية البريطانية، للمزيد من التفاصيل أنظر <https://www.Youm7.com> (2025/5/10_11:09)

³ _ المرجع نفسه

الصحة الوطنية البريطانية المتضررة أنه تم إغلاق جميع أنظمة تكنولوجيا المعلومات من أجل حمايتها ، وهذا ما يعني أن جميع أنظمة في وضع عدم الاتصال وأن تتمكن المستشفيات من قبول المكالمات الواردة مطالبة المواطنين بعدم حضور إلى الطوارئ في المستشفيات العمومية ، ولكن بدلا من ذلك يقوموا بالاتصال ب111 و999 في حالة الطوارئ القصوى . ويذكر أن المستشفيات شرق وغرب هيرتفورد التابعة لأمانة هيئة الرعاية الصحية قد تأثرت أيضا وقالت إنها تعاني من أعطال في نظم الكمبيوتر والهواتف .¹

الفرع الثاني: الخسائر المادية ناتجة عن الاختراق

كشفت شركة هادون بوساطة التأمين أن الهجمات الالكترونية كلفت الشركات البريطانية نحو 44 مليار جنيه إسترليني (ما يعادل 55.08 مليار دولار) من الإيرادات المفقودة على مدى السنوات الخمس الماضية . وأشارت إلى أكثر من 52 بالمائة من شركات القطاع الخاص أبلغت عن تعرضها لهجوم إلكتروني واحد على الأقل خلال هذه الفترة ، وأظهرت البيانات أن هذه الهجمات تكلف الشركات في المتوسط 1.9 بالمائة من إيرادات تزيد عن 100 مليون جنيه ، الأكثر عرضة لهذه الهجمات ، ما يعكس حجم التحدي الذي تواجهه الشركات الكبرى بسبب بنيتها الرقمية المعقدة واعتمادها الكبير على التكنولوجيا.²

أوضحت الشركة أسباب الأكثر شيوعا للهجمات الالكترونية هي :

- اختراق رسائل البريد الالكتروني لواقع 20 بالمائة
- سرقة البيانات بنسبة 18 بالمائة من الحالات

¹ _المرجع نفسه

² _مونت كارلو الدولية، الهجوم الالكتروني، لمزيد من التفاصيل أنظر

[https:// www.mc.Doualiya.com](https://www.mc.Doualiya.com)(2025/5/10_12:15)

وأبلغت الشركات المالية عن خسائر مباشرة كبيرة بلغ مجموعها ما يقارب 2.5 مليار دولار، خاصة المؤسسات المالية في اقتصاديات المتقدمة وخاصة في الولايات المتحدة.¹

المطلب الثالث: اختراق شركة "winds Solar" عام 2020

سنتعرف في هذا المطلب عن شركة "سولار ويندز" وكيف تم اختراقها من خلال الفرعين التاليين:

الفرع الأول: شركة سولار ويندز

• **corporation winds Solar**: هي شركة أمريكية تطور برامج للشركات للمساعدة في إدارة شبكاتها وأنظمتها والبنية التحتية لتكنولوجيا المعلومات. يقع مقرها في أوستن بولاية تكساس ، ولها مكاتب مبيعات وتطوير في عدد من المواقع في الولايات المتحدة والعديد من البلدان الأخرى. تمتد أول الشركة علنا من مايو 2009 حتى نهاية عام 2015 ومرة أخرى من أكتوبر 2018. كما استحوذت على عدد من الشركات الأخرى، لا تزال تعمل تحت أسماءها الأصلية بما في ذلك **Loggly. Papertrail. Pingdom** ، كان لديها حوالي 3000000 عميل تقريبا وحوالي **fortune500** اعتبارا من ديسمبر 2020 بما في ذلك جميع شركات وكالات الحكومة الفدرالية الأمريكية.²

"سولار ويندز": هي شركة بورتوريكو الرائدة في مجال إدارة الشبكات بما في ذلك برنامج **"Orion Platform"** هذا البرنامج يستخدمه العديد من العملاء حول العالم لتكنولوجيا

¹ _ الجزيرة، خسائر متزايدة للشركات في العالم جراء العجلات الالكترونية، لمزيد من التفاصيل أنظر (2025/5/10_13:15) <https://www.aljazeera.net>

² _ solarwinds، مقالة شركة تكنولوجيا المعلومات، لمزيد من التفاصيل انظر <https://en.m.wikipedia.org> (2025/5/7_10:50)

الفصل الثاني القرصنة الالكترونية وتهديدات امن الدول بين الادارة والمواجهة

شبكاتهم ، في أو آخر عام 2020 اكتشف ابتكار أن نسخة معينة من هذا البرنامج على باب خلفي يسمح للمبدعين بالوصول إلى العملاء ¹.

باعتبارها نظاما لمراقبة تكنولوجيا المعلومات، يتمتع **Winds Orion Solar** بامتياز الوصول إلى أنظمة تكنولوجيا المعلومات للحصول على بيانات السجلات وأداء النظام. هذا الامتياز وانتشارها الواسع جعل **solarwinds** هدفا مريحاً وجذاباً ².

الفرع الثاني: اختراق شركة Solar Winds

شهد عام 2020 هجوماً سيبرانياً لم يتضامن معه وأطلق عليه اسم " هجوم سولارويندز" ³

كشف باحثوا الأمن النقيب عن أسوأ خروقات البيانات في التاريخ الحديث ، وكانت حملة قرصنة مدعومة من الكرملين أدت إلى اختراق خوادم مزود إدارة الشبكة سولار ويندز، ومن هناك اخترقت شبكات تضم عملاء كبار لهذه الشركة ، بما في ذلك 9 وكالات فدرالية أمريكية ⁴

في هذا الاختراق تمكن قراصنة يشتبه في انتمائهم لدول ، والذين حددتهم ميكروسوفت بمجموعة تعرف باسم " نوبليوم" وغالباً ما يطلق عليهم باحثون آخرون اسم "قرصنة سولار ويندز " من الوصول إلى شبكات وأنظمة وبيانات آلاف عملاء سولار ويندز . يعد نطاق

¹ _هجوم سولار ويندز: اختراق عميق في قلب البنية التحتية الرقمية،

² _ شهيد أولديميجي، شون مايكل كيرنر، كل ما تحتاجه لمعرفة اختراق solarwinds، لمزيد من التفاصيل انظر (2025/5/6_9:20) <https://www.techtarget.com>

³ _خالد المسعود، هجوم سولار ويندز: اختراق عميق في قلب البنية التحتية الرقمية، مقال تحليل البرمجيات الضارة، لمزيد من التفاصيل أنظر (2025/5/8_14:55) <https://cyberhub.sa>

⁴ _قرصنة سولارويندز مجموعة كاملة من الحيل الجديدة لهجمات شرسة، لمزيد من التفاصيل أنظر (2025/5/8_14:53) <https://www.aljazeera.net>

الاختراق غير مسبوق، وهو من أكبر عمليات الاختراق، إن لم يكن الأكبر من نوعه على الإطلاق.¹

قالت شركة ميكروسوفت إن الجهة التي نفذت هجوم سولار ويندز عبر الانترنت تستهدف حاليا وكالات حكومية ومؤسسات بحثية وشركات استشارات ومنظمات غير حكومية ، وأضافت ميكروسوفت في منشور على مدونتها " شهدنا هذا الأسبوع هجمات إلكترونية عبر الانترنت من نوبليوم استهدفت وكالات حكومية ومؤسسات بحثية واستشارية ومنظمات غير حكومية " وبعد اكتشاف هذا الاختراق أعلنت شركة **solarwinds** أن هناك 18000 من عملاءها قد تعرضوا لهذا الاختراق ومنهم شركة ميكروسوفت والتي بدورها لاحقا عن تعرض 30.000 من عملاء نظام الحوسبة السحابية لديها للاختراق بالتبعية.²

كانت هجومية سولار ويندز واحدة من أكبر الشركات السيبرانية في التاريخ . لقد كشفت عن نقص البيانات ونقاط الاتصال الخاصة بشبكة الإنترنت الرقمية العالمية ، وأحد المشاهير إلى إعادة تقييم المعلومات الخاصة بها . من المتوقع أن تستمر الهجمات السيبرانية في التطور ، مما يتطلب بذل الجهود المستمرة لدعمنا ونظمنا.³

وهذا الاختراق يأتي ضمن قائمة طويلة من الهجمات الالكترونية التي يشتبه بأن روسيا قامت بشنها (**Reuters**)، معتقدين أن سبب الاقتحام يمكن أن يكون ببساطة حالة تجسس من حكومة تحاول فهم ما يفعله خصمها.⁴

¹ _ شهيد أولديجي، مرجع سابق

² _ شركة ميكروسوفت، من نفذوا هجوم سولار ويندز يستهدفون حاليا وكالات، لمزيد من التفاصيل أنظر (2025/5/8_14:45) <https://www.cnbcarabia.com>

³ _ خالد آل مسعود، مرجع سابق الذكر

⁴ _ إيمان نجة، أمال بن أعراب، الأمن المعلوماتي واختراق خصوصية المؤسسات الاقتصادية، مجلة الدراسات الإعلامية والاتصالية، المجلد 3، العدد 1، الجزائر، 2023، ص 35

المبحث الثالث: الجهود الدولية والأمنية في تحقيق الأمن السيبراني

إن الخسائر التي أفرزتها الحروب السيبرانية جعلت من الأمن السيبراني أمرا مهما نظرا للانتشار الواسع للإنترنت والتقنيات الحديثة ، حيث أدى التحول الرقمي والاعتماد المتزايد على تكنولوجيا الإعلام والاتصال وواقع النمو المتزايد للتهديدات السيبرانية إلى وجوب تضافر الجهود وضرورة التعاون في الحد من مخاطر الأمن السيبراني .سواء على المستوى الأمم أو على المستوى الإقليمي للدول وسنتعرف في هذا المبحث المقسم إلى ثلاثة مطالب عن جهود هيئة الأمم المتحدة في ردع الهجمات السيبرانية وكذا الجهود الإقليمية للدول بالإضافة المؤتمرات والقمة الدولية في تحقيق الأمن السيبراني.

المطلب الأول: الجهود الدولية والأمنية في تحقيق الأمن السيبراني

باعتبار الإجرام الالكتروني يتمتع بالطابع الدولي فهي جرائم لا تعترف بالمكان حيث أنها ترتكب على دعامة افتراضية غير محدودة لذا سنتطرق في هذا المطلب إلى دراسة الجهود المبذولة من طرف الهيئات الدولية في تحقيق الأمن السيبراني .

الفرع الأول: الجهود الأمنية

بذلت الأمم المتحدة جهوداً كبيرة في سبيل العمل على مكافحة الإجرام السيبراني ، وذلك لم تسببه هذه الجرائم من أضرار بالغة وخسائر فادحة بالإنسانية جمعاء ، وإيماناً منها بأن منع هذه الجرائم ومكافحتها يتطلبان استجابة دولية في ضوء الطابع والأبعاد الدولية لإساءة استخدام الكمبيوتر والجرائم المتعلقة به.¹

تعمل هيئات الأمم المتحدة مع مختلف الاتحادات ذات الصلة ، منها الأعمال التي جمعتها مع الاتحاد الدولي للاتصالات في مجال حماية المعلومات ، وكذا أعمالها مع

¹ _ مراد مشوش، الجهود الدولية لمكافحة الإجرام السيبراني، مجلة الوحدات للبحوث و الدراسات، المجلد12، العدد 2،

الفصل الثاني القرصنة الالكترونية وتهديدات امن الدول بين الادارة والمواجهة

الاتحاد الدولي للملكية الفكرية في حماية براءات الاختراع و الحقوق¹ المترتبة على الأعمال الفنية المنصفة ، بالإضافة إلى الشراكة التي تجمعها مع اتحاد الشركات و الكيانات الاقتصادية في مجال حماية أمنها الالكتروني¹.

توصلت الجمعية العام للأمم المتحدة نتيجة جهودها على المسار القانوني و التنفيذي إلى اعتماد إستراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب عام 2006 فلقد قامت الجمعية العامة للأمم المتحدة بإصدار بعض التوصيات والقرارات ذات الصلة بالأمن الإلكتروني ، كان لها دور كبير في دفع الدول الأعضاء لإدراك أهميته و ما يرتبط به من تحديات تتطلب مجهودات تعاونية مشتركة لمواجهته . كما ظهر الاهتمام بالبعد الإلكتروني في أغلب الأجهزة التابعة للأمم المتحدة و أبرزها المجلس الاقتصادي والاجتماعي، وجهاز مكافحة الجرائم².

و تتم معظم الجهود في مكافحة الجرائم السيبرانية من خلال تدابير أمنية تقنية ، مثل مكافحة الفيروسات و تصفية البريد العشوائي و التشفير هذا يمنع الهجمات الإلكترونية من النجاح حيث تكون هذه الإجراءات الأمنية كافية ، لكنها لا تمنع مجرمي الإنترنت من العثور على أهداف مناسبة في مكان آخر ، و يحتمل أن يكون أفضل وسيلة يتم القضاء على هجمات مجرمي الإنترنت تمامًا عن طريق حبس الجاني³.

أكدت الجمعية العامة للأمم المتحدة ، علاوة على ذلك ، أن حقوق الأشخاص خارج الفضاء السيبراني ، يجب أن تحظى بالحماية أيضا داخله وهذا ما تضمنه تقرير المفوضة

¹ _ بولفيح محمد السعيد، أطر التعاون الدولي للتصدي لتهديدات السيبرانية، مجلة الدراسات القانونية التطبيقية، جامعة الإخوة منتوري قسنطينة، 2024، الجزائر، بدون صفحة

² _ غجاتي سهيلة، راهم أميرة، مرجع سبق ذكره، ص71

³ _ قطاف سليمان، مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية، مجلة البحوث القانونية والاقتصادية، المجلد 5 العدد2، الجزائر، 2022، ص 75

الفصل الثاني القرصنة الالكترونية وتهديدات امن الدول بين الادارة والمواجهة

السامية من خلال اعتماد القرار 167 / 68 ،حيث طلبت الجمعية العامة من المفوضة السامية لحقوق الإنسان إعداد تقرير عن الحق في الخصوصية في العصر الرقمي ، إذ تناول التقرير بالبحث ، وفق النص القرار " حماية الحق في الخصوصية وتعزيزه في سياق المراقبة الداخلية و الخارجية للاتصالات الرقمية و / أو اعتراضها و جمع البيانات الشخصية. " حيث قدم التقرير إلى مجلس حقوق الإنسان في دورته السابعة و العشرين و إلى الجمعية العامة في دورتها التاسعة و الستين¹

وكذا القرار رقم 211 / 64 الصادر عام 2010 ، الذي يدعو الدول إلى تحديث تشريعاتها بشأن الجرائم الإلكترونية ، والخصوصية، والبيانات الشخصية، و نحو ذلك و أيضا اعتماد اتفاقيات إقليمية بهذا الشأن القرار رقم 65 / 41 و الذي صادقت عليه الجمعية العامة للأمم المتحدة في يناير 2011، الذي دعا فيه على تقرير فريق الخبراء الحكوميين في مجال المعلومات و الاتصالات السلكية و اللاسلكية في سياق الأمن الدولي . و تضمنت استنتاجات فريق الخبراء من بينها ما ذكرته من أن هناك دول تستحدث تكنولوجيا المعلومات و الاتصال كوسائل للحرب و الاستخبارات.²

عقدت كذلك الأمم المتحدة المؤتمر الثاني عشر لمنع الجريمة و العدالة الجنائية بالبرازيل أيام 12 إلى 19 أبريل 2010 ، حيث ناقشت فيه الدول الأعضاء ببعض التعمق مختلف التطورات الأخير في استخدام التكنولوجيا من طرف المجرمين و السلطات المختصة في مكافحة الجريمة ، حيث تبقى منظمة الأمم المتحدة الإطار الأمثل لمكافحة الإجرام السيبراني حيث وضعت مجموعة من القواعد الموضوعية و الإجرائية 7 لمواجهة

¹ _ منزر رابح، درويش السعيد، الطبيعة القانونية للهجمات السيبرانية التي تقع بين الدول، مجلة صوت القانون، المجلد الثامن، العدد1، الجزائر، 2021، ص549

² _ وسام محمود عرفان، سبل مكافحة الهجمات السيبرانية دوليا، مجلة الدراسات القانونية والاقتصادية، المجلد 10، العدد 3، 2024، ص3005

هذه النوعية من الجرائم¹. ربما تكون أفضل إستراتيجية طويلة الأجل لمكافحة الجريمة السيبرانية هي من خلال الاتفاقيات الدولية التعاون في تقديم مرتكبي جرائم الكمبيوتر إلى العدالة².

أو لا :القواعد الموضوعية

تتضمن هذه القواعد النص على قائمة الحد الأدنى للأفعال المتعين تجريمها واعتبارها من قبيل الإجرام السيبراني و تحديثها دوريا و المتضمنة :جريمة الاحتيال أو الغش المرتبط بالكمبيوتر و يشمل ذلك الإدخال و الإتلاف و المحو لمعطيات الكمبيوتر أو برامجها و القيام بأية أفعال تؤثر بمجرى المعالجة الآلية للبيانات وتؤدي إلى إلحاق الخسارة أو فقدان الحياة أو ضياع ملكية شخص و ذلك بقصد جني الفاعل منافع اقتصادية له أو للغير.³ وجريمة التزوير التي تطل برامج الكمبيوتر أو التزوير المعلوماتي وجريمة تخريب وإتلاف الكمبيوتر، وجريمة الدخول غير المصرح بيه وجريمة الاعتراض غير المصرح بيه.⁴

- **جريمة تخريب و إتلاف الكمبيوتر:** و يشمل ذلك إدخال أو الإتلاف أو التخريب أو أي فعل آخر بقصد تعطيل وظيفة من وظائف الكمبيوتر أو نظام الاتصالات والشبكات.

- **جريمة الدخول غير المصرح به:** وهو التوصل أو الولوج دون تصريح إلى نظام أو مجموعة نظم عن طريق انتهاك إجراءات الأمن.
- **جريمة الاعتراض غير المصرح به:** وهو الاعتراض عن طريق وسائل فنية-

¹ _مراد مشوش مرجع سبق ذكره، ص707

² _يولفيح محمد السعيد، مرجع سبق ذكره، بدون صفحة

³ _مراد مشوش، مرجع سبق ذكره، ص707_708

⁴ _ سينا علي محمود، التحديات الأمنية للدول في الفضاء السيبراني، مقال، العدد80، 2025، ص325

للاتصال توجه لنظام كمبيوتر أو عدة نظم أو شبكة اتصالات¹.

ثانيا: القواعد الإجرائية

أما القواعد الإجرائية فتنضمن بعض الأسس الواجب أخذها في الاعتبار من أبرزها وجوب تحديد السلطة المعنية بإجراء التفتيش و الضبط في بيئة تكنولوجيا المعلومات، ووجوب التعاون الفعال بما يتيح التنسيق و التعاون للأغراض القضائية في حل الجرائم ، و السماح للسلطات العامة باعتراض الاتصالات داخل البيئة المعلوماتية مع استخدام الأدلة التي يمكن أن يتحصل عليها ، و كذلك إدخال بعض التعديلات التشريعية في حالة الضرورة بما يتماشى مع طبيعة الإجرام السيبراني داخل القانون الوطني و كذلك القواعد القائمة في مجال الإثبات الالكتروني من حيث مصداقية الأدلة وما يمكن أن تنثيره من مشاكل عند تطبيقها.² يجب أن يوضع في الاعتبار كل المسائل المرتبطة ببيئة تكنولوجيا المعلومات، مثل ضياع فرصة اقتصادية، التجسس، انتهاك حرمة الحياة الخاصة، مخاطر الخسارة الاقتصادية، كلفة إعادة بناء قواعد البيانات كما كانت و إعادتها إلى الوضع السابق قبل إجراء أي تفتيش أو تحقيق.³

كما دعت لجنة منع الجريمة والعدالة الجنائية في البند 42 من تقرير هذا المؤتمر، النظر والدراسة الشاملة لمشكلة الجرائم الالكترونية وردود فعل الدول الأعضاء عليها ، وطلب من المجتمع الدولي والقطاع الخاص بتبادل المعلومات بشأن التشريعات الوطنية ، والمساعدة التقنية والتعاون الدولي يهدف إلى دراسة الخيارات الوطنية والاستجابات للجرائم الالكترونية.⁴

¹ _ مراد مشوش مرجع سابق الذكر، ص708

² _ سينا علي محمود، مرجع سابق الذكر، ص325

³ _ مراد مشوش، مرجع سابق الذكر، ص708

⁴ _ بيدي أمال، جهود الأمم المتحدة في مكافحة الجريمة السيبرانية، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 8،

العدد 1 الجزائر، 2022، ص309

المطلب الثاني: الجهود على المستوى الإقليمي

أصبح من الضروري اتخاذ تدابير تشريعية لمكافحة الجريمة السيبرانية وأضرارها المدمرة على الدول والمجمعات خاصة في ظل شيوع شبكة المعلومات والتطور الواسع لأنظمة الحاسوب وتدفق المعلومات ، وسنتعرف على أبرز الجهود المبذولة من طرف الدول والمنظمات لردع الجريمة المعلوماتية من خلال الفروع التالية:

الفرع الأول: المجلس الأوروبي "اتفاقية بودابست" والتعاون الثنائي

• اعتمد المجلس الأوروبي اتفاقية بودابست بشأن الجرائم السيبرانية كإطار قانوني لمكافحة بعض الجرائم السيبرانية ، توفر الاتفاقية أحكاماً قانونية نموذجية يمكن للدول تكييفها لتناسب احتياجاتها الوطنية ، وتركز الاتفاقية على جرائم مثل النفاذ غير القانوني (القرصنة) و اعتراض الاتصالات ، ومع ذلك، فإنها لا تشمل بعض التهديدات السيبرانية الأكثر تطوراً ، مثل التجسس الإلكتروني و التخريب، و على الرغم من أنها تُشجع التعاون الدولي من خلال تجريم الجرائم السيبرانية الأساسية، إلا أن قوتها الإلزامية محدودة نظراً لتجنبها مخالفة التشريعات الوطنية لبعض الدول، جدير بالذكر أن الاتفاقية، التي فُتح باب التوقيع عليها في نوفمبر 2001 ، صُدمت عليها من قبل ثلاثين دولة فقط، بما في ذلك دولة واحدة فقط من خارج أوروبا.¹

• تهدف اتفاقية الجريمة الإلكترونية بودابست 2001 إلى رفع هذا التحدي، مع إبداء الاحترام الواجب لحقوق الإنسان في مجتمع المعلومات الجديد.²

• كما قد طرح مشروع الاتفاقية للعامة ووزع على مختلف الجهات وأطلق ضمن مواقع عديدة أوروبية و أمريكية على شبكة الإنترنت لجهة التباحث وإبداء الرأي، وتعكس

¹ _ سيناء غلي محمود، مرجع سبق ذكره، ص 327

² _ منزر رابح، درويش السعيد، مرجع سابق الذكر، ص 550

الفصل الثاني القرصنة الالكترونية وتهديدات امن الدول بين الادارة والمواجهة

الاتفاقية الجهد الواسع و المميز للاتحاد الأوروبي و لجان الخبراء فيهما المنصبة على مسائل جرائم الكمبيوتر وأغراضها منذ أكثر من عشرة أعوام.¹

• كما تعد الاتفاقية الوحيدة المتعددة الأطراف المعنية بمكافحة الجرائم التي تتم باستخدام أو ضد الكمبيوتر وباستخدام شبكة الانترنت، وهي تمثل ركيزة أساسية منذ دخولها حيز النفاذ، في الأول من جويلية لعام 2004 على مستوى الدول أعضاء مجلس الاتحاد الأوروبي وكما سبق الإشارة ، فلقد وقعت عليها العديد من الدول من غير أعضاء مجلس أوروبا مثل كندا واليابان وجنوب إفريقيا، كما صادقت عليها الولايات المتحدة الأمريكية.²

بالإضافة إنشاء صندوق الصين-إسرائيل بين شنغهاي وهونج كونج و تل أبيب (GEOC) عام 2013، يهدف الصندوق إلى الاستثمار في شركات التكنولوجيا المتقدمة، بما في ذلك علوم الحياة، الطابعات ثلاثية الأبعاد، والأمن السيبراني.³

الفرع الثاني: منظمة حلف الناتو والاتحاد الدولي للاتصالات

أنشأ حلف الناتو هيئة خاصة بإدارة الدفاع السيبراني ، بالإضافة إلى فريق للاستجابة للحوادث الحاسوبية بهدف تقديم دعم سريع للبلدان الأعضاء التي تتعرض لهجمات سيبرانية، كما أسس الحلف مركزا للتميز في مجال الدفاع السيبراني التعاوني، مقره في استونيا، يضم هذا المركز خبراء متخصصين في البحث والتدريب في مجال الأمن السيبراني.⁴

أدت تداعيات الهجمات السيبرانية التي استهدفت البنية التحتية الرقمية لاستونيا عام 2007 وأيضا منه جورجيا خلال نزاعها المسلح مع روسيا عام 2008، إلى سعي حلف شمال الأطلسي (الناتو) للتصدي لتلك الهجمات و ذلك من خلال نشر دليل يعرف باسم

¹ _ مراد مشوش، مرجع سبق ذكره، ص 712

² _ قطاف سليمان مرجع سبق ذكره، ص 79

³ _ سيناء علي محمود، مرجع سبق ذكره، ص 328

⁴ _ سيناء علي محمود، مرجع سبق ذكره، ص 327

الفصل الثاني القرصنة الالكترونية وتهديدات امن الدول بين الادارة والمواجهة

دليل تالين **Manuel de Tallin** الذي يعتبر وثيقة غير ملزمة تنظم قواعد الاشتباك عبر الانترنت وقد تم صدور إصدارين¹

الإصدار الأول عام 2013: قواعد دليل تالين (le manuel de Tallin) لعام 2013
المتعلق بقواعد القانون الدولي المطبقة على الحروب السيبرانية، أعد هذا الدليل من مجموعة خبراء في القانون الدولي بدعوة من منظمة حلف شمال الأطلسي (OTAN)، وبحضور اللجنة الدولية للصليب الأحمر الدولي "CICR"، يتكون هذا الدليل الذي يعد الوثيقة القانونية الوحيدة التي تحكم مثل هذه الاعتداءات التي تتم بين الدول، من 95 قاعدة استمدت في مجمله امن أحكام القانون الدولي المختلفة كميثاق الأمم المتحدة وقواعد القانون الدولي الإنساني... وغيره.²

الإصدار الثاني عام 2017 المعروف باسم "Tallinn20" و يتكون من 154 قاعدة قانونية ويركز على الوضع القانوني لمختلف أنواع القرصنة والهجمات السيبرانية الأخرى التي تحدث يومياً وقت السلم ويوضح دليل تالين، قوانين الدولة التي يمكن تطبيقها على الحرب السيبرانية وهو سيمثل على كل من مبدأ حق اللجوء إلى الحرب ومبدأ سلوكيات الحرب، لما يعالج هذا الدليل كلا من النزاعات المسلحة الدولية و غير الدولية و يجمع الفقهاء في ضوء دليل تالين، بأن النزاع المسلح الدولي يحصل متى ما قامت دولة ذات سيطرة بحملة على مجموعة من الأفراد بتوجيه تلك المجموعة لتنفيذ هجمات سيبرانية ضد دولة، أما إذا كانت لا تملك إلا سيطرة فعالة على تلك المجموعة فعندئذ تلك الهجمات لا تبلغ مستوى النزاع المسلح الدولي.³

الاتحاد الدولي للاتصالات: اعتمد المؤتمر العالمي لتنمية الاتصالات لعام 2006 القرار رقم 45 الذي دعا فيه مدير مكتب تنمية الاتصالات إلى تنظيم اجتماع بشأن الأمن

¹ _عجاتي سهيلة، راهم أميرة، مرجع سبق ذكره، ص73

² _منزر رابح، درويش السعيد، مرجع سبق ذكره، ص547

³ _عجاتي سهيلة، راهم أميرة، مرجع سبق ذكره، ص 73

الفصل الثاني القرصنة الالكترونية وتهديدات امن الدول بين الادارة والمواجهة

المعلوماتي و مكافحة الرسائل الاقتحامية، وتقديم تقرير يتضمن نتائج الاجتماع إلى مؤتمر المندوبين المفوضين العام 2006 ، وقد تمت بني مجموعة من التوصيات في مجال الأمن المعلوماتي و الرسائل الاقتحامية، كما أطلق الأمين العام للاتحاد في أيار 2007 ، جدول أعمال الأمن المعلوماتي العالمي لوضع إطار لمواجهة التحديات المتزايدة لأمن الإنترنت.¹ و لإيجاد حلول لتعزيز الشقة و الأمن في مجتمع المعلومات، وفي أكتوبر 2007 أنشأ فريق من الخبراء رفيع المستوى HLEG ضم أكثر من مائة خبير قدموا التقارير والتوصيات في حزيران 2008 حيث نشرت الإستراتيجية العالمية في 12 / 11 / 2008 وقد اشتملت الإستراتيجية على المجالات التالية :التدابير القانونية والتدابير التقنية و الإجرائية ، والهيكل التنظيمية وبناء القدرات، والتعاون الدولي.²

المطلب الثالث: المؤتمرات والقمم الدولية

ساهمت الولايات المتحدة من خلال تنظيم مؤتمرات و قمم دولية في تعزيز الجهود العالمية لمواجهة التهديدات السيبرانية المتزايدة وسعت إلى بناء تعاون دولي فعال لمكافحة الجرائم إلكترونية ومن ابرز هذه الجهود :

أو لا: مؤتمر هافانا 1990

خلال المؤتمر الثامن للأمم المتحدة حول منع الجريمة ومعاملة المجرمين ، الذي عقد في هافانا عام 1990 ، أقر قانون خاص بالجرائم المرتبطة بالحاسوب ، ويشكل هذا القانون

¹ _قطاف سليمان، مرجع سبق ذكره، ص76

² _قطاف سليمان، مرجع سبق ذكره، ص77

خطورة رائدة في توجيه الجهود الدولية لتنظيم التعامل مع الجرائم السيبرانية ووضع إطار قانوني لها .¹

وعمم هذا المؤتمر معلومات عن شبكات الحاسوبية الخاصة بالعدالة الجنائية ، والأحكام المتعلقة بحجز العائدات المالية الجريمة المنظمة وفحص سجلات المصرفية ، وثاني الخيرات في مجال صلة مكافحة الجريمة بالتنمية الاجتماعية ، الاقتصادية ، استعرض أيضا تطوير منع الجريمة القائمة على المستوى المحلي ، وأوصى بالجمعية بأن تعتمد صكوكا دولية أكثر من جرائم الحاسوب دعا فيه الدول الأعضاء إلى النظر في عدد من التدابير منها تحسين الأمن الحاسوبي واتخاذ تدابير وقائية ، أخذه بعين الاعتبار المشاكل المتصلة بالحماية الحرة الشخصية ومراعاة حقوق الإنسان وحياته الأساسية أي آليات تنظيمية تتعلق باستخدام الحواسيب .²

أوصى هذا المؤتمر بعقد قمة في باريس تؤدي إلى إنشاء لجنة حكومية دولية بشأن الجريمة والعدالة الجنائية تكون هيئة الرئيسية لصنع السياسات في الأمم المتحدة وتحسين التصدي للجريمة داخل الدول وفيما بينها .³

ثانيا: لجنة منع الجريمة والعدالة الجنائية أبريل 2010

في الدورة الثانية عشر للجنة الأمم المتحدة منع الجريمة والعدالة الجنائية ، تم الإعلان عن إنشاء فريق خبراء حكومي دولي متخصص لدراسة الجريمة السيبرانية، الهدف من هذا

¹ _سيناء علي محمود، مرجع سبق ذكره، ص325

² _بانكوك، مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية، لمزيد من التفاصيل أنظر

(2025/5/11 _10:47) <https://digitallibarg.un.org>

³ _ مكتب الأمم المتحدة بالمخدرات والجريمة، لمزيد من التفاصيل أنظر

(2025/5/11_10:59) <https://unis.univenna.org>

الفريق هو تحليل أبعاد المشكلة السيبرانية على الصيد الدولي ، وتقديم توصيات حول كيفية صياغة إستجابات فعالة وشاملة لمكافحة هذا النوع من الجرائم¹.

ثالثا: جلسة المجلس الاقتصادي والاجتماعي للأمم المتحدة 2010

تهدف هذه المنظمة إلى تحقيق أعلى مستويات النمو الاقتصادي وتناغم التطور الاقتصادي مع التنمية الاجتماعية، بدأت هذه الاهتمام بالجريمة السيبرانية منذ عام 1978 ، حيث وضعت مجموعة من الأدلة وقواعد إرشادية تتصل بتقنية المعلومات ، ويعد الدليل المتعلق بحماية الخصوصية وقواعد البيانات من أول الأدلة التي تم تبنيها من قبل مجلس المنظمة في عام 1980 مع توصية الأعضاء بالالتزام بها وأصدرت تقريرا بعنوان الجرائم المرتبطة بالحاسوب وتحليل السياسة القانونية الجنائية ، حيث تضمن التقرير الحد الأدنى من أفعال سوء استخدام الحاسوب والتي على الدول تجريمها.²

رابعا: إنشاء الشركات التعددية ضد التهديدات السيبرانية

في إطار البناء المؤسسي أطلقت الأمم المتحدة مبادرة الشراكة التعددية ضد التهديدات السيبرانية عام 2009 ، وتعد هذه المنظمة أول كيان مدعوم من الأمم المتحدة يعمل على الدعم الأمن السيبراني من خلال توفير منصات التعاون الدولي ، وتقديم المساعدة التقنية للدول الأعضاء لمواجهة الهجمات السيبرانية³

خامسا: قرار مجلس الأمن رقم 2341 (2019)

دعا فيه جميع الدول إلى تعزيز تعاونها من أجل حماية الهياكل الأساسية الحيوية من الهجمات الإرهابية ، بما في ذلك ربط الإقليم وما يتصل به من هياكل أساسية عابرة الحدود، وكان مجلس الأمن قد عقد مناقشة مفتوحة اليوم بشأن حماية الهياكل الأساسية الحيوية من الهجمات الإرهابية ،تحت بدء الأخطار التي تهدد السلام والأمن الدوليين جراء الأعمال

¹ _ سناء علي محمود، مرجع سبق ذكره، ص 326

² _ مراد مشوش، مرجع سبق ذكره، ص 709

³ _ سناء علي محمود، مرجع سبق ذكره، ص 326

الفصل الثاني القرصنة الالكترونية وتهديدات امن الدول بين الادارة والمواجهة

الإرهابية، وفي هذا الشأن قال **بافلو كليمكين** وزير خارجية أوكرانيا ،الذي ترأس المجلس خلال الشهر الحالي ، وأشار أن الهجمات الإرهابية التي تطال هذه المرافق والخدمات يمكن أن تترك بشكل كبير حياة المجتمعات وتسبب قدرا كبيرا من المعاناة البشرية ¹.

سادسا: اعتماد قرار الأمم المتحدة رقم 247/74 (2019)

جرى إنشاء هذه الآلية بمبادرة من روسيا الاتحادية بمشاركة 46 دولة بناء على قرار الجمعية العامة للأمم المتحدة رقم 247/74 في عام 2019 وهدفها تطوير أول اداة دولية في تاريخ مكافحة جرائم الكترونية المعلومات والاتصالات .ولعبت روسيا طوال العملية دور الملهم لعملية التفاوض وقائدها ، تهدف هذه اللجنة إلى تعزيز التعاون الدولي وتطوير إطار قانوني دولي يواجه التحديات الناشئة عن الجرائم السيبرانية ².

سابعا : اعتماد الأمم المتحدة لمكافحة الجريمة السيبرانية 2024

اعتمدت الأمم المتحدة معاهدة لمكافحة الجريمة السيبرانية ، هي أول نص من نوعه تقره المنظمة ، رغم معارضة شديدة من الناشطين الحقوقيين حذروا من أخطار قد تترتب عليها ووصفها بعضهم بأنها أدبت للمراقبة ، وتهدف اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، بما في ذلك تعزيز التعاون الدولي وتوفير الدعم الفني وبناء القدرات ، خاصة إلى الدول النامية ، واعتبرت أن اعتماد الاتفاقية يشكل خطوة بالغة الأهمية نحو تعزيز الجهود لمكافحة الجرائم ، بما في ذلك الاعتداء الجنسي على الأطفال عبر الانترنت والاحتيال الالكتروني المعتقد وغسل الأموال وسيتم فتح الاتفاقية لتوقيع في حفل رسمي تستضيفه فينتام عام 2025 على أن تدخل حيز التنفيذ بعد 90 يوم من تصديق الدولة الأربعين عليها ³.

¹ ريك باغورناس، مجلس الأمن للأمم المتحدة، للمزيد من التفاصيل أنظر

<https://www.un.org/ar/sc> (2025/5/11_12:28)

² وزارة الخارجية روسيا الاتحادية، للمزيد من التفاصيل أنظر <https://www.med.ru>. (2025/5/11_13:07)

³ إكرام القصاص، الأمم المتحدة تعتمد اتفاقية لمكافحة الجريمة السيبرانية، لمزيد من التفاصيل أنظر

[https:// www.youn7.cim](https://www.youn7.cim) (2025/5/11 _13:57)

ملخص الفصل:

من خلال العرض الذي قدمناه حول القرصنة الالكترونية في الفضاء السيبراني وتهديد امن الدول رأينا أن جميع الدول قامت بوضع العديد من إستراتيجيات لمواجهة هذه التهديدات ومن خلال ما سبق توصلنا إلى النتائج التالية :

مع التطور التكنولوجي ظهرت الجريمة الالكترونية والتي انتشرت بشكل كبير وأصبحت تشكل خطرا على أمن الدول والهيئات والمنظمات بوضع العديد من القوانين التي تجرم هذه العملية

أصبح الفضاء السيبراني ساحة جديدة لصراع ولم يعد مقتصرًا على البر، والبحر، بل أصبح ساحة خامسة للحرب حيث استخدم مختلف الهجمات الالكترونية للتجسس وتعطيل البنى التحتية والتأثير على الرأي العام .

تطورت الاختراقات السيبرانية تنوعت أشكالها وتعددت أثارها وانعكاساتها لتشمل جميع المجالات وعليه أصبحنا أمام جرائم حقيقية مست الأمن السيبراني للدول وأثرت عليه .

خاتمة

خاتمة:

من خلال ما سبق نستنتج أن الفضاء السيبراني لم يعد مجرد فضاء افتراضي تقني محصور في تداول المعلومات أو الاتصالات الرقمية ، بل أصبح ميدانا للصراع والتنافس بين الدول والجهات الفاعلة بحيث بات الفضاء السيبراني مجالا استراتيجيا يمس سيادة الدول وأمنها القومي . فمع الانتشار الواسع لتكنولوجيا المعلومات وما تحمله من مخاطر وتهديدات تمس الأمن القومي ، والسيادة الرقمية للدول وكثرة الاعتماد عليها في إدارة شؤون الأفراد والمؤسسات ، أصبحت التهديدات السيبرانية والقرصنة الالكترونية تشكل خطرا مباشرا ومتزايدا يفرض تحديات غير مسبقة تتطلب تضافر الجهود الدولية والوطنية لمواكبة التطور التكنولوجي . كما تناولنا الجوانب المفاهيمية والنظرية للفضاء السيبراني من خلال تعريفه وتوضيح خصائصه ، وأهم المخاطر المترتبة عليه خصوصا في ظل الاعتماد الواسع على الأنظمة الرقمية في جميع الميادين المختلفة وعليه فإن مواجهة هذه الظاهرة تتطلب الحاجة إلى الوعي المجتمعي وتعزيز الثقافة الأمنية الرقمية وتطوير أدوات الدفاع السيبراني على جميع الأصعدة ، بالإضافة إلى أننا تطرقنا إلى مفهوم الأمن السيبراني وأبعاده المتعددة ،الاقتصادية ، القانونية ، العسكرية ، السياسية ، والاجتماعية ودوره المحوري في ردع التهديدات السيبرانية ، بمقاربات شاملة توازن بين الحرية الرقمية ومتطلبات الأمن .ومما لاشك فيه أن تعاون المجتمع الدولي أصبح ضروريا من أجل التصدي لهذه الجرائم ، حيث أن القوانين التقليدية لم تعد تتفع للاختلاف الواسع بين الجرائم التقليدية والجرائم السيبرانية التي تعود إلى أساسها الافتراضي بسبب التطور العلمي الحاصل .

النتائج

_ الفضاء السيبراني أصبح ميدانا للحروب والصراع بين الدول ،ولم يبق مجرد فضاء افتراضي تقني .

القراصنة الالكترونية بل هي تحدي حضاري يمس سيادة الدول وحقوق الأفراد ، واستقرار المجتمعات .

لم يعد السعي نحو تحقيق أمن سيبراني فعال خيارا بل أصبح ضرورة حتمية تفرضها طبيعة العصر الرقمي المتجدد باستمرار

الجهود الدولية والوطنية لمكافحة الجرائم السيبرانية تبقى قاصرا نظرا للتطور السريع لتكنولوجيا المعلومات .

التوصيات:

استنادا لم تم عرضه يمكن تقديم بعض التوصيات التي من شأنها تحقيق الأمن السيبراني .

✓ إعداد إطار قانوني عالمي موحد: من خلال تحديث القوانين الوطنية لمواكبة التطور التكنولوجي، بالإضافة إلى تشجيع التعاون الدولي في سن تشريعات موحدة تحارب جميع أشكال الجرائم المعلوماتية وسد الثغرات القانونية المستغلة من طرف القراصنة.

✓ تعزيز القدرات الوطنية في الأمن السيبراني : ضرورة دعم المؤسسات الأمنية والمختصة في مكافحة الجرائم السيبرانية ،من خلال توفير الإمكانيات المادية والبشرية ،وتدريب الكفاءات الوطنية في مجالات الأمن السيبراني والتحقيقات الالكترونية .

✓ إطلاق حملات توعية وتنقيفية برفع الوعي المجتمعي

✓ تعزيز التعاون الدولي: إذ أن الجرائم المعلوماتية ذات مجال افتراضي عابر للحدود فمن المهم وجود آليات التعاون المشترك بين دول العالم، من أجل تبادل المعلومات وردع الهجمات التي تتجاوز الحدود الجغرافية بشكل منسق وفعال.

✓ تشجيع البحث العلمي : دعم الأبحاث والدراسات التي تساهم في تحقيق الأمن السيبراني

✓ تمكين الأطر المؤسسية الرقمية : بضرورة دمج الأمن السيبراني في سياسة الأمن القومي، وإنشاء مراكز مستقلة ومتخصصة في الاستجابة لمتطلبات الأمن الدولي .

قائمة المصادر والمراجع

قائمة المصادر والمراجع:

قائمة المراجع

أولاً: الكتب

_ إيهاب خليفة ، القوة الإلكترونية ، كيف يمكن أن تدير الدول شؤونها في عصر الأنترنت، القاهرة ،العربي النشر والتوزيع 2017

ثانياً: المجالات والدوريات

_ أسماء حداد، الحروب الهجينة، الأزمة الإلكترونية نموذجاً، مجلة مدارات سياسية ديسمبر 2017 كلية العلوم السياسية وعلاقات الدولية جامعة الجزائر 03

- إدريس عطية ،مكانة الأمن السيبراني ،مجلة الدراسات القانونية والاقتصادية ،المجلد 10 العدد 3سنة سبتمبر 2024

- إسلام فوزي ، امن السيبراني ،الأبعاد الاجتماعية و قانونية تحليل سيكولوجي ، مجلة اجتماعية قومية المجلد 56، العدد 2

- إسلام مصطفى ، جمعة مصطفى ، جريمة الاختراق الإلكترونية وحماية استخدام البيانات والمعلومات في القانون ، مجلة قانونية ،كلية الحقوق، جامعة القاهرة

- إوراغ كريم ،الاختراق الإلكتروني ، مجلة التطوير العلمي مجلد 2، العدد 4الجزائر 2020

- إيمان خميس اليحياني ، عدنان إبراهيم سرحان ، أثار القانونية لجائحة كورونا كوفيد 19 على حماية البيانات الشخصية ، مجلة الحقوق العدد 4الجزء 2

- إيمان نعجة، آمال بن عراب ، الأمن المعلوماتي واختراق خصوصية المؤسسات الاقتصادية ، مجلة الدراسات الإعلامية واتصالية المجلد 3، العدد 1الجزائر 2023
- بعوني ليلي ، التهديدات في الفضاء السيبراني وانعكاساتها على السيادة الرقمية ، القرصنة الإلكترونية نموذجاً ، مجلة عددها 16، كلية العلوم اقتصادية جامعة الجزائر 03
- بن شريف أحلام ، بوغرة الصالح، القرصنة الإلكترونية أنواعها أشكالها وطرق التصدي لها ، مجلة الجزائرية للعلوم السياسية والعلاقات الدولية ، جامعة تيارت العدد 1 المجلد 5، جوان 2012
- بوطلاعة و داد ، بوكورو منال ، صراع الفضاء السيبراني وتأثيره على السلم والأمن الدوليين ، مجلة العلوم القانونية والاجتماعية ، المجلد 7، العدد 4، جامعة الإخوة منتوري قسنطينة 01
- بولفيح محمد السعيد ، أطر التعاون الدولي لتصدي التهديدات السيبرانية ، مجلة الدراسات القانونية والتطبيقية ، جامعة الإخوة منتوري قسنطينة 2024
- بيدي آمال ، جهود الأمم المتحدة في مكافحة الجريمة السيبرانية ، مجلة البحوث في الحقوق والعلوم السياسية ، المجلد 8، العدد 1الجزائر 2022
- حورية بن سيدهم ، رقية عواشيرة، الأمن الفضائي السيبراني للتحديات والحلول ، مجلة الجزائرية للأمن الإنساني المجلد 5، العدد 2، سنة 2020
- داودي منصور ، مرابط حمزة ، التشفير كألية لحماية المصنفات الرقمية الإلكترونية ،مجلة الحقوق والعلوم السياسية ، جامعة خنشلة ، المجلد 23، العدد 1سنة 2020
- دبابنة شرين ، الجرائم المعلوماتية ، القرصنة الإلكترونية.مجلة الدراسات المالية والمصرفية ، دار المنظومة المجلد 23، العدد 1، سنة 2015

- دليلة العوفي ، الحرب السيبرانية في عصر الذكاء الاصطناعي ورهانات الأمن الدولي،
مجلة الحكمة للدراسات الفلسفية ، المجلد 9، العدد 2، الجزائر 3

- شريفة كلاع ، الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر
الفضاء الإلكتروني ، مجلة الحقوق والعلوم الإنسانية ، المجلد 15، العدد 1، جامعة الجزائر
03

- غريب حكيم ، شرقي صبرينة ، تداعيات الحرب الإلكترونية على العلاقات الدولية ،
مجلة دفاتر السياسة والقانون ، المجلد 12، العدد 02، المدرسة الوطنية العليا للعلوم
السياسية الجزائر

- قطاف سليمان ، مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية ، مجلة البحوث
القانونية والاقتصادية ، المجلد 5، العدد 2، الجزائر 2022

- كراش رحمة ، التحول الرقمي في منظمات الأعمال بالاعتماد على برنامج ، مجلة نماء
للاقتصاد والتجارة ، المجلد 08، العدد 1، سنة 2024

- لتييم فتيحة، الأمن المعلوماتي للحكومة الإلكترونية وإرهاب والقرصنة ،مجلة المفكر، كلية
الحقوق والعلوم السياسية ، جامعة عنابة

- محمود علي عبد الرحمان، الفضاء الإلكتروني وأثره على مفاهيم القوة والأمن والصراع في
العلاقات الدولية، مجلة كلية السياسة و الاقتصاد المجلد 16، العدد 15 ،يونيو 2022

- مراد مشوش ، الجهود الدولية لمكافحة الإجرام السيبراني ، مجلة الوحدات للبحوث
والدراسات ، المجلد 12، العدد 2، الجزائر 2019

- منزر رابح، درويش السعيد ، الطبيعة القانونية للهجمات السيبرانية التي تقع بين الدول ،
مجلة صوت القانون ، المجلد 8، العدد 1، الجزائر 2021

- نورة شلوش ، القرصنة الإلكترونية في الفضاء السيبراني وتهديد امن الدول ، مجلة مركز بابل للدراسات الإنسانية ، 2018 المجلد 8، العدد 2
- وسام محمود عرفان، سبل مكافحة الهجمات السيبرانية دوليا، مجلة الدراسات القانونية والاقتصادية ، المجلد 10، العدد 03، سبتمبر 2024
- وفاء مطروح ، إبتسام لونيس ، تداعيات جائحة كوفيد 19 على حماية البيانات الشخصية ، مجلة الحقوق العدد 4، الجزء 2021، 2،
- يحي ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني ، مجلة قانونية

ثالثا: المذكرات والرسائل الجامعية

- بوديسة إيمان ، مكافحة الجريمة الإلكترونية في القانون الجزائري ، مذكرة لنيل شهادة الماستر في القانون العام ، تخصص قانون جنائي ، جامعة أكلي محمد اولحاج بويرة ، الجزائر 2019,2020
- دحو نجا ، أولاد علي فاطمة ، جريمة القرصنة الإلكترونية في التشريع الجزائري ، دراسة لنيل شهادة الماستر ، تخصص قانون جنائي والعلوم الجنائية ، كلية الحقوق جامعة غرداية ، الجزائر 2021,2022
- دمان دبيح محمد رشدي ، الحرب الروسية الأوكرانية في الإعلام الرقمي ، مذكرة مقدمة لنيل شهادة الماستر ، تخصص صحافة مكتوبة وإلكترونية ، كلية الإعلام والاتصال والسمعي البصري ، جامعة صالح بوبنيدر قسنطينة 03 سنة 2022

- شعيب قاسمي ،فؤاد بالغيث ، الإستراتيجيات الدولية في مكافحة الجريمة السيبرانية ، مذكرة لنيل شهادة الماستر في العلوم السياسية و علاقات الدولية ، كلية الحقوق والعلوم السياسية ، قسم الحقوق ، جامعة العربي تبسي - تبسة-
- صلاح حيدر عبد الواحد ، حروب الفضاء الإلكتروني ،دراسة في مفهوما وخصائصها وسبل مواجهتها ، رسالة مكملة لمتطلبات الحصول على شهادة الماجستير في العلوم السياسية ،كلية الآداب والعلوم، جامعة الشرق الأوسط ،تموز 2021
- طمطامي سالم ،الصحافة الإلكترونية والأمن السيبراني ، مذكرة لنيل شهادة الماستر في الإعلام والاتصال ، جامعة أحمد دراية ،ولاية أدرار ،قسم العلوم الإنسانية 2021,2022
- عمار حشمان ، الجريمة المعلوماتية في التشريع الجزائري ،مذكرة مقدمة لنيل شهادة الماستر المهني ، الطور الثاني ،تخصص علوم تيسير ، كلية العلوم التجارية ،جامعة قاصدي مرياح ورقلة ،الجزائر 2جويلية 2019
- غجاتي سهيلة، راهم أميرة ، الهجمات السيبرانية وآثارها على تهديد السلم والأمن الدوليين ، مذكرة لنيل شهادة الماستر ،في القانون ،جامعة 8ماي 1945، كلية الحقوق ، تخصص قانون عام ، قالمة 2023,2024
- عبابسة فاروق ، عيوب خديجة ، القرصنة الإلكترونية في الجزائر وآثارها على المستخدم ريبورتاج مصور لنيل شهادة الماستر في علوم إعلام والاتصال ،تخصص سمعي بصري ، قسم العلوم الإنسانية ، كلية العلوم الاجتماعية ،جامعة عبد الحميد بن باديس ، مستغانم ، الجزائر

رابعاً: الملتقيات علمية

- بن مالك أسمهان ، خصائص الجريمة المعلوماتية وأسباب إرتكابها ، محاضرات مقدمة لطلبة السنة الأولى ماستر ،قسم الحقوق ، جامعة محمد البشير الإبراهيمي، برج بوعرييج
- ديلالي جيلالي ، بالبشير يعقوب ، رهانات الأمن السيبراني الوطني في ظل التحول الرقمي قراءة في التأصيل المعرفي و إستراتيجية المواجهة التشريعية ، محاضرات مطبوعة موجهة لطلبة كلية الحقوق ،جامعة بن بوعلي ، شلف ، الجزائر
- سيناء علي محمود ،التحديات الأمنية للدول في الفضاء السيبراني ، مقال العدد 80 سنة 2025
- عبد الحفيظ ديب الاختراق الأمن السيبراني للدولة الوطنية في عصر ثورة المعلومات ، محاضرة مطبوعة ، كلية العلوم السياسية ، جامعة الجزائر 03
- محمد الحماسي ، القوة الإلكترونية عنصر أساسي مؤثر في النظام العالمي ،مقال الجمعة 22 اغسطس 2014

خامساً: القوانين

- القانون رقم 15-04 المؤرخ 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 156-56، المتضمن قانون العقوبات عدد 71، الصادر في 10 نوفمبر 2004 المادة 394 مكرر

سادساً: المواقع الإلكترونية

- أكرم قصاص ،الأمم المتحدة تعتمد اتفاقية لمكافحة الجرائم السيبرانية لمزيد من التفاصيل انظر 13:57 (11/05/2025), <https://www.youn7.cin>

- أماني عصام ، استخدام روسيا القوة السيبرانية في إدارة تفاعلها الدولية، كلية التجارة لمزيد من التفاصيل انظر <https://www-bbc.com- org>
- المركز الديمقراطي لعمليات السيبرانية بين روسيا وأوكرانيا لمزيد من التفاصيل انظر [https:// www- Denorcrticac.com\(08/05/2025\)16:30](https:// www- Denorcrticac.com(08/05/2025)16:30)
- اختراقات سوني بيكتشرز لمزيد من التفاصيل انظر [https://www .arabhard wne-net\(08/03/2025\)14:30](https://www .arabhard wne-net(08/03/2025)14:30)
- بانكوك مؤتمر الأمم المتحدة ،الحادي عشر لمنع جريمة لمزيد من التفاصيل انظر [https:// digitallibrahg.un.org\(11/05/2025\) 10:47](https:// digitallibrahg.un.org(11/05/2025) 10:47)
- جاكوب فوكس ، نبذة مختصرة عن تاريخ القرصنة لمزيد من التفاصيل انظر [https:// www cobalt.com\(06/03/2025\) 12:35](https:// www cobalt.com(06/03/2025) 12:35)
- حسن هاني ،حسن محمود أثر التهديدات السيبرانية على الأمن القومي دراسة حالة ماليزيا 2015.2022،المركز الديمقراطي العربي لمزيد من التفاصيل انظر [https:// www.dendicon.com\(08/05/2025\)](https:// www.dendicon.com(08/05/2025))
- خالد المسعود هجوم سولار ويندز لمزيد من التفاصيل انظر [https://cyberhub.sa \(06/05/2025\)9:20](https://cyberhub.sa (06/05/2025)9:20)
- ريك باغورناس، مجلس الأمن للأمم المتحدة لمزيد من التفاصيل انظر [https://www.un.org/ar/sc\(11/05/2025\)12;28](https://www.un.org/ar/sc(11/05/2025)12;28)
- شركة امنية مالا نعرفه عن الأمن السيبراني لمزيد من التفاصيل انظر [https:// ar.wikipedia.org\(7/04/2025\)22:30](https:// ar.wikipedia.org(7/04/2025)22:30)

- شركة مايكروسوفت من نفذ هجوم سولار وينذر لمزيد من التفاصيل انظر [https://www.chbcahabia.com\(08/05/2025\)14:45](https://www.chbcahabia.com(08/05/2025)14:45)
- شهيد أولديميجي ،كل ما تحتاجه لمعرفة الاختراق لمزيد من التفاصيل انظر [https://www-techtahget.com\(06/05/2025\)9:20](https://www-techtahget.com(06/05/2025)9:20)
- عبير حسين أول قرصنة تعرفها الأنترنت لمزيد من التفاصيل انظر [https://www.alkhaleej.com\(2/2/2025\)12:55](https://www.alkhaleej.com(2/2/2025)12:55)
- غوردن كوريرا ،هل أصبحت الحرب الروسية الأوكرانية معركة التقنيات لمزيد من التفاصيل انظر [https://www-bbc.com.cnd-ampphobject.org\(08/05/2025\)18:45](https://www-bbc.com.cnd-ampphobject.org(08/05/2025)18:45)
- قراصنة سولار وينذر مجموعة كاملة من الحيل الجديدة لهجمات سرية لمزيد من التفاصيل انظر [https://cybernub.sa\(08/05/2025\)14:55](https://cybernub.sa(08/05/2025)14:55)
- مؤسسة الدعائم التقنية للحاسب الآلي لمزيد من التفاصيل انظر [https://www.itpillars.com\(7/04/2025\)22:40](https://www.itpillars.com(7/04/2025)22:40)
- محمد احمد عبد غني ،ملخص تاريخ القرصنة الإلكترونية لمزيد من التفاصيل انظر [https://www.hooobook.com\(06/03/2025\)14:55](https://www.hooobook.com(06/03/2025)14:55)
- مركز مشترك للتحكم والتنسيق لمزيد من التفاصيل انظر [https://www.en-wiki-pedai.org\(08/05/2025\)18:30](https://www.en-wiki-pedai.org(08/05/2025)18:30)
- مقلة شركة سولار وينذر لتكنولوجيا المعلومات لمزيد من التفاصيل انظر [https://en.wikipedia.org\(7/05/2025\)10:56](https://en.wikipedia.org(7/05/2025)10:56)

- مكتب الأمم المتحدة للجريمة ومخدرات للمزيد من التفاصيل انظر

[https:// uns.unvemma.org/](https://uns.unvemma.org/)(11/05/2025)10:59

- وزارة الخارجية روسيا الاتحادية للمزيد من التفاصيل انظر

[https:// www.ned.ru/](https://www.ned.ru/)(11/05/2025)13:0

فهرس المحتويات

فهرس المحتويات:

Contenu

1	مقدمة:
1	الفصل الأول: الاطار الإتيومولوجي المعرفي لمفاهيم الدراسة
6	الفصل الأول: الإطار المفاهيمي والنظري للدراسة
6	المبحث الأول: الفضاء السيبراني الدلالات المعرفية
7	المطلب الأول: مفهوم الفضاء السيبراني
7	الفرع الأول: تعريف الفضاء السيبراني
9	الفرع الثاني: أمن المعلومات
11	المطلب الثاني : خصائص الفضاء السيبراني
11	الفرع الأول: العالمية واللامركزية
12	الفرع الثاني: صعوبة الاكتشاف
13	المطلب الثالث: أنواع الهجمات السيبرانية
13	الفرع الأول: تعريف الهجمات السيبرانية
13	الهجمات السيبرانية في اللغة مصطلح بمعنى القيادة والتحكم عن بعد
14	الفرع الثاني : أنواع الهجمات السيبرانية
18	المبحث الثاني: القرصنة الإلكترونية ضبط مفاهيمي
18	المطلب الأول: كرونولوجيا القرصنة الإلكترونية
18	الفرع الأول: القرصنة الإلكترونية من 1903 إلى 1971

20.....	الفرع الثاني : فجر القرصنة الحاسوبية 1981 إلى 2014
24.....	المطلب الثاني: مفهوم القرصنة الإلكترونية
25.....	الفرع الأول: تعريف القرصنة الإلكترونية
28.....	الفرع الثاني: خصائص القرصنة الإلكترونية
31.....	الفرع الثالث: أسباب القرصنة الإلكترونية
34.....	المطلب الثالث: مظاهر القرصنة الإلكترونية
	المبحث الثالث: السيادة الرقمية والأمن السيبراني علاقة التزامن من السيادة التقليدية إلى
36.....	السيادة الرقمية
37.....	المطلب الأول: أبعاد الأمن السيبراني
37.....	الفرع الأول: تعريف الأمن السيبراني
38.....	الفرع الثاني: أبعاد الأمن السيبراني
41.....	المطلب الثاني: الإختراقات الرقمية والفئات المستهدفة
41.....	الفرع الأول : الإختراقات الرقمية :
42.....	الفرع الثاني: الفئات المستهدفة
46.....	ملخص الفصل الأول
1	الفصل الثاني: القرصنة الإلكترونية وتهديدات امن الدول بين الادارة والمواجهة
45.....	الفصل الثاني: القرصنة الإلكترونية وتهديدات امن الدول بين الادارة والمواجهة
45.....	المبحث الأول: جدلية الصراع الإلكتروني في الفضاء السيبراني وبروز القوة الإلكترونية .
46.....	المطلب الأول: عصر الصراع الإلكتروني في الفضاء السيبراني
47.....	الفرع الأول: التهديدات التي يواجهها الفضاء الإلكتروني في البيئة الأمنية

الفرع الثاني: الفضاء الإلكتروني ساحة جديدة لصراع بشكله التقليدي ذو طابع إلكتروني.	48
المطلب الثاني: المخاطر والتهديدات في الفضاء السيبراني	50
الفرع الأول: مخاطر اجتماعية وثقافية واقتصادية	50
الفرع الثاني: المخاطر السياسية والأمنية:	53
المطلب الثالث: القوة الإلكترونية للدول وأثارها	55
الفرع الأول: القوة الإلكترونية	55
الفرع الثاني: أثر الفضاء الإلكتروني على مفهوم القوة في العلاقات الدولية.	57
المبحث الثاني: النماذج الحديثة للاختراقات السيبرانية خلال الفترة (2016_2020)	60
المطلب الأول: اختراق مركز التحكم الرئيسي بكيف - أوكرانيا عام 2016	60
الفرع الأول: مركز التحكم الرئيسي	60
الفرع الثاني: اختراق مركز التحكم الرئيسي	61
المطلب الثاني: اختراق وزارة الصحة البريطانية 2017	63
الفرع الثاني: الخسائر المادية ناتجة عن الاختراق	65
المطلب الثالث: اختراق شركة "winds Solar" عام 2020	66
الفرع الأول: شركة سولار ويندز	66
الفرع الثاني: اختراق شركة Solar Winds	67
المبحث الثالث: الجهود الدولية والأمنية في تحقيق الأمن السيبراني	69
المطلب الأول: الجهود الدولية والأمنية في تحقيق الأمن السيبراني	69
الفرع الأول: الجهود الأمنية	69

74	المطلب الثاني: الجهود على المستوى الإقليمي.....
74	الفرع الأول: المجلس الأوربي "اتفاقية بودابست" والتعاون الثنائي.....
75	الفرع الثاني: منظمة حلف الناتو والاتحاد الدولي للاتصالات
77	المطلب الثالث: المؤتمرات والقمم الدولية.....
81	ملخص الفصل :
83	خاتمة:
86	قائمة المصادر والمراجع.
96	فهرس المحتويات

المخلص:

القرصنة الإلكترونية في الفضاء السيبراني تُعد من أخطر التهديدات المعاصرة التي تواجه أمن الدول. فمع تطور التكنولوجيا واعتماد الحكومات على الأنظمة الرقمية، أصبحت هذه الأنظمة هدفاً سهلاً للهجمات السيبرانية. يشمل ذلك التجسس، سرقة البيانات الحساسة، تعطيل البنى التحتية الحيوية مثل الطاقة والاتصالات، وحتى التأثير في العمليات السياسية. تستخدم جهات معادية أو منظمات إجرامية تقنيات متقدمة لاختراق الشبكات وسرقة المعلومات أو تدميرها. وتكمن الخطورة في أن هذه الهجمات قد لا تُكتشف فوراً، مما يمنح القراصنة وقتاً أطول لتحقيق أهدافهم. لذا، تسعى الدول إلى تعزيز قدراتها الدفاعية السيبرانية والتعاون الدولي لمواجهة هذه التهديدات المتنامية.

Abstract

Cyber piracy in cyberspace is considered one of the most serious contemporary threats to national security. With the advancement of technology and governments' reliance on digital systems, these systems have become easy targets for cyberattacks. This includes espionage, theft of sensitive data, disruption of critical infrastructure such as energy and communications, and even interference in political processes. Hostile entities or criminal organizations use advanced techniques to infiltrate networks and steal or destroy information. The danger lies in the fact that these attacks may not be detected immediately, giving hackers more time to achieve their goals. Therefore, countries are working to enhance their cyber defense capabilities and promote international cooperation to confront these growing threats.