

## السيادة الرقمية والتحول الرقمي:

### التحديات والحلول الهيكلية

## Digital sovereignty and digital transformation: challenges and structural solutions

ط.د حميل مصطفى  
جامعة قاصدي مرباح ورقلة (الجزائر)  
hamil.moustafa@univ-ouargla.dz

### ملخص

في بداية القرن العشرين ، شهد العالم ثورة تكنولوجية رقمية هائلة ومذهلة ، أدت إلى تسارع وتدفق المعلومات وحركات التجارة والتعاملات الرقمية وظهور المدن والدول الرقمية والعملات الرقمية والدبلوماسية الرقمية حتى بدأ العالم يتحدث عن السيادة الرقمية ، والتي اتخذت بعداً رقمياً وفضاءً جغرافياً وهمياً بأشخاص وهميين ، والذين يتفاعلون في فضاء إلكتروني مفتوح على كل الأصعدة ، وليس له حدود وقوانين فعالة تؤطر هذا الأخير ، كل هذه التطورات والتفاعلات سمحت بظهور التهديدات السيبرانية ، والجرائم الإلكترونية ، والإرهاب السيبراني ، من خلال ما يسمى بالقرصنة الإلكترونية ، عن طريق نقل فيروسات فتاكة مثل حصان طروادة ، زومي ، ودوس وغيرها والتي غالباً ما تشل أجهزة الكمبيوتر وتسرق معلومات المستخدم ، بما في ذلك رسائل البريد الإلكتروني والمعلومات المصنفة سرية جداً في وقت يتحدث فيه العالم عن السيادة الرقمية ، والتي يصعب السيطرة عليها في ظل هذه التهديدات الجديدة المتعددة الأبعاد وذات انعكاسات شاملة على كل القطاعات، سعت العديد من الدول الى تفعيل نظام حماية ميكانيزم الإنذار المبكر، من أجل حامية سيادتها الرقمية من الاختراقات التي تؤدي إلى زعزعة امنها القومي.

**كلمات مفتاحية:** سيادة البيانات، الفضاء السيبراني، الأمن السيبراني، الحرب الإلكترونية، حوكمة الانترنت.

### Abstract

At the beginning of the twentieth century, the world witnessed a huge digital technological revolution, which led to the acceleration of the flow of information, digital trade movements, digital transactions, the emergence of digital cities, digital countries, digital currencies, and digital diplomacy until the world started talking about digital sovereignty, which took a digital dimension and an imaginary geographical space with people Fake, interacting in an open cyberspace that has no limits and effective laws framing the latter, all these developments and interactions allowed the emergence of cyber threats, cyber crimes, cyber terrorism, through the so-called pirates, by transmitting deadly viruses such as Trojan horse, zombie, DOS and others, Which often paralyze computers and steal user information, including emails and classified secret informations.

**Keywords:** ata sovereignty, cyberspace, electronic warfare, cyber security, Internet.



## رقمنة مجلة الدراسات الإعلامية والاتصالية

المجلد 02 | العدد 03  
ديسمبر 2022  
الصفحات 48 - 62

ردمك | ISSN-2773-4285  
EISSN | 2830-8417  
الإيداع القانوني | 07/2021  
العنوان | 11، طريق دودو مختار، بن عكنون،  
الجزائر العاصمة.  
الفاكس | 23 88 50 (023)  
الهاتف | 62 29 75 (0561)

تاريخ الاستلام 2022/10/17  
تاريخ القبول 2022/12/16  
تاريخ النشر 2022/12/31

ط.د حميل مصطفى  
جامعة قاصدي مرباح ورقلة (الجزائر)  
hamil.moustafa@univ-ouargla.dz



## 1. مقدمة:

غني عن البيان أن إتقان التقنيات كان دائماً مجاًلاً تمارس فيه القوة الاقتصادية والعسكرية والسياسية ومع ذلك من الشائع التقليل من أهمية الطبيعة الحاسمة لهذه السيطرة وإساءة تحديد التقنيات المعنية، إذا كان هناك اقتناع بأن إتقان تقنيات المعلومات "التفوق المعلوماتي" هو اليوم أحد المحددات العالمية للقوة، وإذا تم الإدراك بسهولة إن الإنترنت هو المكان والرافعة، فإن القليل هم من يهتمون بالديناميكيات المحددة لهذه التقنيات، والطريقة التي يتم بها نشرها في مجال الدول والأنظمة التنظيمية الدولية.

في الوقت الذي تقوم فيه جميع البلدان ببناء جزء متزايد من بنيتها التحتية الاقتصادية والاجتماعية والسياسية على الإنترنت، من الضروري أن يهتم عدد أكبر من الجهات الفاعلة بالطريقة التي يتم من خلالها مباشرة التقنيات التي تشكل بنية الإنترنت بأكملها. أو بشكل غير مباشر، تطور المجتمعات والعلاقات بين الدول من تنفيذ أنظمة القياسات الحيوية إلى تعليم الأشياء بواسطة الرقائق الذكية والاتصال، بما في ذلك الاستخدامات المتعلقة بأنظمة تحديد الموقع الجغرافي أو تطوير الإدارة الإلكترونية.

واليوم وصلت هذه النماذج التنظيمية الموروثة، من فترة كان فيها الإنترنت فقط ربط العلماء والباحثين وطرح مشاكل السيادة لعشاق الخيال العلمي حدودها، في عالم حيث الإنترنت على مفترق طرق لجميع الأنشطة البشرية، لم تعد القرارات التي توجه مستقبلها وتؤثر في استخداماتها تعتمد فقط على الفاعلين "التقنيين" في عصور ما قبل التاريخ الدول الأعضاء في الأمم المتحدة على تنظيم القمة العالمية لمجتمع المعلومات ولأول مرة، جمعت قمة للأمم المتحدة أطرافاً من القطاعات الرئيسية الثلاثة للإنترنت (الحكومات، والقطاع الخاص، والمجتمع المدني)، ومن ثم تم إضفاء الطابع المؤسسي على خصوصيات إدارة "شبكة الشبكات".

وفي نهاية المرحلة الأولى، وانطلاقاً من هذا المسار المقدماتي والمعطيات السابقة تطرح الإشكالية الرئيسية الآتية:

- ما هو واقع السيادة الرقمية، والتحول الرقمي في ظل التهديدات السبرانية الجديدة؟

للإجابة عن الإشكالية الرئيسية تطرح الفرضيتان الآتيتان:

1- السيادة الرقمية تطورت مع موجة الثورة التكنولوجية.

2- الأسلوب الوقائي وتكوين فرد يؤمن بالأمن القومي، والفضاء الإلكتروني الوطني والحذر من المنتج التكنولوجي

الغربي وتحقيق الاستقلالية التقنية من الأساليب الناجعة لتحقيق تحول رقمي وسيادة رقمية قوية.

ومن أجل التعمق الأمثل في فهم ودراسة الموضوع سيتم توظيف- مقارنة الأمن المعلوماتي- الخاص بالفضاء الإلكتروني، والتي تركز في تحليلها على تحليل ثلاث جوانب جوهرية، وهي الجانب الخاص بالمعلومات إضافة إلى الجانب الثالث والمتمثل في التطبيقات والبرامج الإلكترونية والتفاعلات الإلكترونية في الفضاء الجغرافي السبراني الوهمي، كما سيتم توظيف- المنهج

التحليلي الوصفي- الذي يرتبط في كثير من الأحيان بالأبحاث العلمية، ويستخدم المنهج الوصفي التحليلي عن طريق ملاحظة الباحث لمشكلة أو ظاهرة علمية، والشروع في وصفها بأسلوب علمي دقيق.

ويكتسي موضوع السيادة الرقمية أهمية بالغة، وخاصة سيادة البيانات لأن معظم المجالات مرتبطة بالانتقال أو التحول الرقمي فالتجارة والاقتصاد العالمي مرتبط بالجانب الرقمي، وتهدف الدراسة إلى تسليط الضوء على التحول الرقمي ومستقبل السيادة الرقمية للدول، في ظل التهديدات الجديدة.

## 2. تحديد المصطلحات:

### 2-1 مفهوم الأمن السيبراني:

تعتبر مهمة ضبط المفاهيم والمصطلحات تحدياً يواجه مختلف الباحثين والدارسين في مختلف التخصصات، وذلك لما يطرحه من إشكاليات تجعل من الصعوبة بمكان الاتفاق على تعريفات واضحة وشاملة وموحدة بين أعضاء المجتمع العلمي، ويعد الأمن السيبراني واحداً من المفاهيم المعقدة التي قدمت لها العديد من التعريف المختلفة وسيتم في الآتي التعرف والتدقيق والتعمق في هذا المصطلح.

#### أ. لغة:

الأمن السيبراني مكوّن من لفظين أساسيين ومهمين وهما: الأمن والسيبرانية.

#### ب. اصطلاحاً:

هو نقيض الخوف، أي بمعنى السلامة، والأمن مصدر الفعل أَمِنَ أَمْنًا وَأَمَانًا وأمنة، أي اطمئنان النفس وسكون القلب وزوال الخوف، ويقال: أَمِنَ من الشر، أي سَلِمَ منه. وقد عرّفه قاموس بنغوين للعلاقات الدولية بأنه مصطلح يشير إلى غياب ما يهدد القيم النادرة.

### 2-2 السبرانية:

مصطلح السبرانية الآن هو واحد من أكثر المصطلحات تردداً في معجم الأمن وهو لفظ يوناني، مكون من كير-نيتس، وتعني الذي يدير ويتحكم في دفة السفينة، وتشير المقاربة الإيتيمولوجية للكلمة المتحكم. يعود الفضل في تطور السبرانية إلى الأب الروحي وعالم الرياضيات الأمريكي، نوربر وينر الذي ألف كتاب بعنوان السبرانية والتحكم في الاتصال بين الحيوان والآلة، ليستبدل مصطلح الآلة بعد الحرب العالمية الثانية بالحاسوب. (Op.ci)

هناك تعاريف أخرى قُدمت لمفهوم الأمن السيبراني، حيث يُعرّف بأنه، مجموعة من الإجراءات المتخذة في مجال الدفاع ضد الهجمات السيبرانية ونتائجها التي تشمل تنفيذ التدابير المضادة المطلوبة.

واعتبر الإعلان الأوروبي أن الأمن السيبراني هو قدرة النظام المعلوماتي على مقاومة محاولات الاختراق التي تستهدف البيانات، وهنا تجدر الإشارة إلى إن الأمن السيبراني مفهوم أوسع من أمن المعلومات، فالأمن السيبراني يهتم بأمن كل ما هو موجود على السايبر من غير أمن المعلومات، بينما أمن المعلومات لا يهتم بذلك، كما يمكن القول إن الأمن السيبراني هو مجموعة الآليات والإجراءات والوسائل والأطر تهدف إلى حماية البرمجيات وأجهزة الكمبيوتر من الاختراقات وكذلك حماية الأمن القومي للدول.

### 2-3 فضاء التواصل:

هو بيئة تفاعلية حديثة خلال الربط البيئي العالمي لمعدات المعالجة الآلية للمعطيات الرقمية مشكلة من عناصر مادية وغير مادية، مكون من مجموعة الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أ، مستعملين كما أنه الذراع الرابعة للجيش الحديثة. (op.ci).

## 4-2 الهجمات السيبرانية:

يمكن تعريفها بأنها استغلال نقطة ضعف معينة تُمكن المهاجم من التلاعب بالنظام.

## 5-2 الجريمة السيبرانية :

مجموعة الأفعال والأعمال غير القانونية، التي تتم عبر معدات أو أجهزة إلكترونية، أو شبكة الإنترنت أو تبث عبرها محتوياتها، وهي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي ونظم المعلومات.

## 6-2 القوة السيبرانية:

يعرفها جوزيف ناي بأنها القدرة على استخدام مصادر المعلومات المرتبطة بالفضاء السبراني لإيجاد مزايا للدولة، والتأثير على الأحداث المتعلقة بالبيئة التشغيلية.

تكمن أهمية الأمن السيبراني كقضية ناشئة في حقل العلاقات الدولية من خلال حداثة هذا المجال، فهناك تاريخ طويل من التخمينات حول دور التكنولوجيا الرقمية في الدراسات الأمنية وقد تم البحث في الموضوع من قبل أركلا وروفلدس منذ 1993 والحديث عن حرب إلكترونية. (EGE، 2020)

## 3-تطور السيادة من المفهوم التقليدي إلى الرقمي:

لتشريح مفهوم سيادة البيانات أو السيادة الرقمية، يجب أولاً تذكر الهيمنة التاريخية والسيطرة القوية على الخطاب خاصة في أوروبا، عبر قرون من الصراعات بين أنظمة السلطة ومناقشات السياسيين لمفهوم السيادة نفسه والتي ظهرت تدريجياً مع كتابات جان بودان، غروتوس، توماس هوبز، جون لوك، مونتسكيو روسو والذين يرون في السيادة بأنها التصرف بطريقة مستقلة، دون هيمنة أجنبية (Op.cit)، لقد تأثر المفهوم التقليدي للسيادة بشدة بالمنظر السياسي في القرن السادس عشر، حيث يعتقد جون بودان إن سلطة اتخاذ القرار النهائية والحق أُلحصر في استخدام القوة في الدولة يجب إن تكون بيد الحاكم، صاحب السيادة ثم في القرن الثامن عشر، أعلن الفيلسوف التنويري جان جاك روسو عن تغيير جذري في مفهوم السيادة من سيادة الحاكم إلى سيادة الشعب. مع تطور الديمقراطيات الحديثة، سادت فكرة إن الشعب، من وجهة نظره، يمتلك أعلى سلطة في الدولة، ولكن يمكنه إن يعهد بها إلى حكومة ذات سيادة ومنتخبة (مليح، 2021، الصفحات 225-228).

يرتبط مفهوم السيادة أيضاً ارتباطاً وثيقاً بمفهوم الدولة القومية المحددة، إقليمياً حيث تكون الدولة ذات سيادة إذا كان بإمكانها التصرف بطريقة مستقلة مع الدول الأخرى إلى حد كبير على المستوى السياسي والاقتصادي والمجتمعي (d'expert، 2022).

وفي نفس السياق تعني ضمناً ضمان قدرة مواطنيها على تقرير المصير بحقوقهم غير القابلة للتصرف، فهي تهدف إلى السماح لجميع الأفراد بالاحترام والتصرف في حقوقهم الشخصية بناءً على سلطتهم الخاصة. ويعتبر ضمان الشروط والأحكام الخاصة بذلك مسؤولية الدولة، لاسيما بالنظر إلى التحديات العديدة التي يفرضها التحول الرقمي على جميع مجالات المجتمع لذلك، أصبح مصطلح السيادة الرقمية أكثر شيوعاً في وسائل الإعلام وله مجموعة متنوعة من المعاني، أحد التفسيرات ونذكر منها:

- قدرة الدول على التحكم في البنية التحتية الرقمية الخاصة بها وبيانات مواطنيها. ومع ذلك، يرى إن المصطلح يستخدم بشكل متزايد في سياق أوسع حيث أصبحت التقنيات الرقمية ساحة معركة للمنافسة العالمية مثلما يحدث الآن من حرب إلكترونية معلوماتية بين الصين والولايات المتحدة الأمريكية (مليح، 2021، الصفحات 225-228).

- عندما برزت جائحة كورونا ظهر معها تحول رقمي هائل حيث انتقل الكثير من سكان العالم إلى الإنترنت نظراً لما فرضته الجائحة بالحجر الصحي ومنع الاحتكاك والعمل عن البعد.

- بدأ الأطفال الذين لديهم إمكانية الوصول إلى الإنترنت من المنزل في أخذ دورات التعليم عن بعد، وبدأ العديد من الموظفين في العمل من المنزل، واعتمدت العديد من الشركات نماذج الأعمال الرقمية للحفاظ على عملياتها والحفاظ على سمعتها وعلى

عمالها كما اعتمدت العديد من الشركات نماذج أعمال رقمية للحفاظ على العمليات والحفاظ على مصادر المعلومات والبيانات (مليح، 2021)، ومواكبة التعامل الرقمي الذي فرضته الجائحة، قامت العديد من محركات البحث ومواقع التواصل الاجتماعي، بالبحث عن أعراض الفيروس وتطور مجالات البحث عن اللقاحات ما أدى إلى تسارع وتيرة الانترنت بنسبة تصل إلى 11٪ بعد فترة وجيزة من انتشار الوباء، مما يؤكد التسارع الرقمي الذي أحدثه الوباء - أدى تسارع الوباء وتسارع وتيرة الرقمنة، إلى إبراز عدة فجوات رقمية بين الدول وأظهرت مدى تحكم الدول في سيادتها الرقمية ومواكبة التطور الهائل للتقنيات الحديثة ودول أخرى بقيت تصارع الوباء دون إحداث قفزة في مجال الرقمنة والتحكم في بياناتها وإنشاء قاعدة داتا للمرضى للإسراع في اللقاحات وتحقيق المناعة الجماعية (CAIRN، 2022)

#### 4-التحول الرقمي وأركانه:

قبل الخوض في التحول الرقمي، يجب شرح بعض المصطلحات التقنية المرتبطة بالتحول التكنولوجي الرقمي والدائرة في فلك الفضاء السبراني، والعالم الرقمي الجديد.

##### 1-4 عنوان بروتوكول الإنترنت:

عنوان مخصص لأي جهاز اتصال بالإنترنت وهو رقم التعريف.

##### 2-4 الوكالة الوطنية لأمن نظم المعلومات:

وهي هيئة تم إنشاؤها في 7 جويلية 2009، في شكل خدمة ذات اختصاص، وطني تحت إشراف الأمانة العامة للدفاع الوطني في فرنسا، والتي تم وضعها نفسها مع، مكتب رئيس الوزراء، وولدت فكرة إنشاء الوكالة من كتاب الأبيض، حول الدفاع والأمن القومي الذي نُشر في 17 جوان 2008، والذي يسلط الضوء على أهمية التهديد السيبراني تقوم الوكالة بمهمة السلطة الوطنية فيما يتعلق بأمن نظم المعلومات وكذلك التنظيم والوقاية والخبرة ومساعدة إدارات وشركات الدولة الحيوية.

##### 3-4 هجوم رفض الخدمة أو دوس:

هذا هجوم من أقوى الهجمات والمقصود به منع المستخدمين- الشرعيين الوصول أو الولوج لخدمة الإنترنت واستخدامها، وكذلك يعمل الفيروس على تعطيل عمل الانترنت وحتى يمكن أن يؤدي إلى حظرها (Op.cit)، يعمل الهجوم على استهداف خادم وعنوان البريد الإلكتروني وإغراقه بالطلبات أو رسائل البريد الإلكتروني، ثم يتم إجبار الآلاف من المستخدمين للدخول والضغط على الإيميلات وصندوق البريد ما يؤدي إلى دخول الفيروس مباشرة وتعطيل الخادم وحتى سرقة البيانات الخاصة بالمستخدم والرسائل.

**4-4 بوت نت:** وهو ماكينات من الزومبي أو الفيروسات تتحكم في عدة خوادم وحواسيب تقوم بالتسلل فيها وتعطيلها وتصبح متصلة مباشرة بحاسوب القرصان أو الهاكر والذي يتمكن من سرقة بيانات المستخدمين ومنعهم من الاتصال بحواسيبهم وحساباتهم.

##### 5-4 فريق الاستجابة لطوارئ الكمبيوتر:

الكيان المسؤول عن الوقاية والاستجابة للحوادث الأمنية للشركات والإدارات وتتكون من فريق تقنيين ومختصين للوقاية من الفيروسات والتهديدات الإلكترونية.

#### 5-الهجمات الإلكترونية وتأثيراتها المتعددة الأبعاد:

أفضت التغيرات الرقمية التي تحدث اليوم بوتيرة سريعة، إلى إحداث آثار عميقة على الحياة بمجملها، ليتم تنفيذ معظم الأنشطة الاقتصادية والتجارية والثقافية والاجتماعية والسياسية، سواء بين الأفراد أو المؤسسات الحكومية أو الخاصة في الفضاء الإلكتروني ومن خلال الشبكة العنكبوتية (bitam، 2022) وأدى ما تقدم، إلى تسارع وتكثيف تبادل المعلومات، إلى الحد الذي تحول فيه الفضاء الإلكتروني، ليكون أحد مجالات التنافس والصراع بين القوى الدولية، ومكاناً لمواجهة بين الأفكار والإرادات، فاسحاً المجال أمام متسلي الشبكات لاختراق الحواسيب، وشن الهجمات في محاولة منهم إما لحجب

البيانات أو تعديلها أو سرقتها، ولأن مثل هذه الهجمات السيبرانية تحصل من خلال التحكم والسيطرة على الحواسيب والمعلومات، والشبكات الإلكترونية، والبنية التحتية للمعلوماتية، فإنها لا تقل خطورة عن الحروب التقليدية من حيث التهديد الذي تنطوي عليه، وحجم التدمير الذي يمكن أن تؤدي إليه، فضلاً عن سرعة حدوثها وانتشارها الواسع، إذ تُنقذ بأساليب يصعب تتبعها في كثير من الأحيان. وسيتم في هذه الدراسة تسليط الضوء على ماهية الهجوم السيبراني والتعرف على المنافسة السيبرانية بين الدول لتطوير إمكاناتها وقدراتها في الفضاء الإلكتروني، أو للقيام برد استباقي أو لشن هجوم مضاد، من خلال التعرف على إمكانات وقدرات بعض الدول، من بينها الولايات المتحدة الأمريكية والصين ودول أخرى. (El-djoundi, 2020)

لم تكن الزيادة في عدد القوى العاملة العالمية في مجال الأمن السيبراني التي نمت من 3.5 مليون عالمياً في عام 2020 إلى 4.2 مليون على مستوى العالم في عام 2021 كافية لملاءمة النقص، في ظل بقاء 2.7 مليون وظيفة شاغرة في هذا المجال (Op.cit). إن المنافسة السيبرانية والقوى الدولية تزيد اليوم من حدة المواجهة السيبرانية في ضوء تقاطع المصالح والتنافس على تعزيز المكانة الدولية، ومن منظور عسكري واستخباراتي، تتوافر بعض الدول على قدرات تؤهلها لشن هجمات سيبرانية مدمرة، الأمر الذي يثير المخاوف لجهة تحولها إلى صراع شامل في لحظة معينة بين دولتين أو أكثر، خاصة مع تصاعد وتيرة تلك الهجمات واتساع تأثيرها، في ظل امتلاك العديد من الدول البنية الوطنية السيبرانية المؤهلة للقيام بهجوم مسبق أو الرد على الهجوم، وبالمعنى نفسه، تضع حكومات الدول المختلفة الأمن السيبراني في صميم استراتيجيات الأمن القومي، بقصد تعزيز قدراتها التنافسية في عالم رقمي أخذ بالتطور المستمر. وتطبيق المبادئ التوجيهية المناسبة للاستخدام الآمن، وتنسيق التعاون بين الجميع في الفضاء السيبراني على مستوى الأفراد أو المؤسسات العامة والخاصة، ويعتقد جان لوك فيز، رئيس الأمن في المنتدى الاقتصادي العالمي والمدير العام السابق للمكتب الفيدرالي للشرطة في سويسرا، إن الهجمات الإلكترونية تشكل تهديداً خطيراً للغاية على حالة العالم، قائلاً بهذا الصدد «لقد أدت رقمنة المجتمع إلى تحقيق التقدم والتمكين، ولكن لها أيضاً جانب مظلماً للجرائم الإلكترونية والحرب الإلكترونية» (Op.cit)، وبحسب ما تقدم، يمكن إن يفضي الهجوم السيبراني الموجّه لدولة ما إلى عدد من العواقب لعل من أهمها:

- الإطاحة بنظام الحكم أو تهديد أمنها القومي
  - التمهيد لبدء الحرب التقليدية خلال المستقبل القريب
  - القيام بعمليات تخريب في قطاعات حيوية، تؤثر في حياة السكان
  - الإضرار بالعلاقات السياسية والدولية أو الإساءة إلى مكانتها.
  - التسبب بحدوث عدد من الإصابات البشرية أو إلحاق الضرر على الصحة والسلامة العامة.
  - نشر الفوضى الداخلية والاضطراب واسع النطاق.
  - تقويض ثقة الجمهور بمعتقداتهم الدينية والسياسية والقومية والعرقية.
  - إلحاق أضرار جسيمة بالاقتصاد الوطني
  - تدمير واسع النطاق أو تعطيل في أداء الأصول الإلكترونية الوطنية.
- إن تصاعد الهجمات في المجال السيبراني، يبرز تساؤلات، حول مدى جاهزية الدول لمواجهة مثل هذه الهجمات، والتصدي للحرب الإلكترونية وسيتم في الآتي عرض بعض الدول التي تمتلك برامج سيبرانية متطورة ذات أبعاد عسكرية على سبيل المثال لا الحصر ومن بينها الولايات المتحدة والصين وإسرائيل:

#### أ-الولايات المتحدة الأمريكية:

تُعتبر الولايات المتحدة، الدولة الأكثر تفوقاً في مجال امتلاك القدرات السيبرانية والعسكرية منها، ولديها قيادة سيبرانية موحدة هي وكالة الأمن السيبراني وأمن البنى التحتية بناءً على إستراتيجية وكالة الأمن القومي أو خطة السنوات الخمس لعام 2018 وتعتمد القيادة السيبرانية الأمريكية على خمس مكونات أساسية، هي: القيادة السيبرانية للجيش، وقيادة الأسطول السيبراني، والقيادة الإلكترونية للقوات الجوية، والقيادة الإلكترونية لقوات مشاة البحرية وخفر السواحل، إضافة إلى

وحدات الحرس الوطني. ويبلغ عدد الفرق السيبرانية في هذه القيادة، نحو 133 فريقاً (Op.cit) تضطلع بمهام مختلفة في مجال حماية الأمن السبراني، تقوم إستراتيجية الفضاء الإلكتروني الأمريكي على مبدأ «الدفاع المتقدم»، لذا ينظر البعض إلى القوة السيبرانية الأمريكية على أنها قوة هجومية في المقام الأول، تستند على دمج القدرات التكنولوجية في جميع مراحل العمليات التي تقوم به. (conflit, 2020)

#### ب-الصين:

بدأت الصين في عام 2003 بتنفيذ «مشروع الدرع الذهبي»، وهو برنامج للمراقبة الداخلية والرقابة على الإنترنت، أصبح يُعرف باسم جدار الحماية العظيم في الصين، في محاولة لممارسة السيطرة السيادية. وفي عام 2009 بذلت الصين جهوداً لحظر بعض تطبيقات البرامج بسبب تعارضها مع قوانين الرقابة على غرار اليوتيوب والفيسبوك وغيرها، حيث قامت بنشر أول إستراتيجية وطنية لأمن الفضاء السبراني في الصين في عام 2016 وتم دعمها من قبل أول قانون صيني للأمن السبراني في 2017، اين حددت الاستراتيجية تسع مهام أساسية، مع التركيز على السيادة وتقوية الدفاع الإلكتروني، وتهتم بكين بتطوير سبل الحرب السيبرانية التي تعتمد على تقنيات الذكاء الاصطناعي، حسب ما تقول وزارة الدفاع الأمريكية (Op.cit)، وتشير تقارير إلى إن الصين ربما تقوم بالفعل باستخدام الذكاء الاصطناعي في مجالات الروبوتات العسكرية وأنظمة توجيه الصواريخ، علاوة على مجالات الطائرات والزوارق الحربية المسيّرة على إن الصين تواصل تعزيز قوتها السيبرانية، وأوضحت تنصهر العالم في العديد من فئات هذه القوة، منها ما يتعلق بالمراقبة الإلكترونية، بالإضافة إلى تصدرها في مجال التجارة التي تفوقت فيها على قوة الولايات المتحدة الأمريكية.

#### ج-الكيان الصهيوني (إسرائيل):

تأسست سلطة الدفاع السبراني القومي الاسرائيلي عام 2016، تحت مسؤولية رئاسة الحكومة مباشرة، ووظيفتها الرئيسية هي إدارة جميع الجهود الدفاعية والعملياتية، في الفضاء السبراني وتشغيلها وتنفيذها الأمر الذي يتيح الرد الدفاعي الكامل والدائم على الهجمات السيبرانية، بما في ذلك التعامل مع تهديدات الفضاء السبراني والحوادث السيبرانية في وقت حقيقي، وصياغة تقدير للوضع الحالي، وجمع المعلومات الاستخباراتية والتدقيق فيها، والعمل مع المؤسسات ذات الاختصاص (Op.cit)، وفي يونيو 2015، تم تأسيس فرع سبراني مستقل يقود نشاط الجيش الاسرائيلي الدفاعي والهجوم في الفضاء السبراني، إذ يتولى الجيش الاسرائيلي المسؤولية عن قيادة الدفاع السبراني للدولة في زمن الحرب، وتستند الحرب السيبرانية إلى قدرات اسرائيلية مستقلة، تجمع بين الابتكار المحلي والتقنيات العالمية، كما إن المقاربات التي تتخذها اسرائيل تندمج في المتطلبات الثلاثة الأصلية الخاصة بمفهوم اسرائيل التقليدي بشأن الأمن القومي

- **الردع:** يمكن للقدرات السيبرانية المتقدمة إن تكون وسيلة فعالة لردع أعداء اسرائيل وكان أحد الأمثلة لذلك عملية ستاكسنت التي أدت إلى التي تنسب إلى الولايات المتحدة واسرائيل، والتي تعطيل أداء أجهزة الطرد المركزي الإيرانية.
- **الإنذار المبكر:** الاعتماد على التقنيات السيبرانية المتقدمة لجمع المعلومات الدقيقة بشأن نيات الخصم وخططه المستقبلية، وأن تمنع من الوصول إلى قواعد البيانات الخاصة بها في الوقت نفسه، وهكذا، يمكن لأجهزة اسرائيل الأمنية إن تقدم للمؤسسة الدفاعية إنذارات فعالة بشأن نيات الخصم بغية اتخاذ التدابير الضرورية ضده في اللحظة الصحيحة.

#### ■ الانتصار العملياتي الحاسم:

يمكن للجيش الاسرائيلي، باستعمال أدواته السيبرانية المتقدمة، أن يكسب أفضلية في القتال تمكّنه من قلب الميزان لمصلحته، وعلى سبيل المثال، جرى تعطيل أجهزة الرادار السورية خلال الهجوم على المفاعل النووي السوري عام 2007، والذي نُسب على نطاق واسع إلى اسرائيل، وذلك بواسطة رمز معادٍ يبدو أنه كان يبث إشارات عادية (Op.cit)، وهذا ما مكّن سلاح الجو الاسرائيلي من اختراق المجال الجوي السوري من دون إن يُكتشف، واستهداف المجمّع النووي وتدميره بالكامل، وما يظهر أيضا قوة اسرائيل في المجال السبراني والجوسسة، اختراع برنامج بيغاسوس الفتاك، والذي يعتبر من أخطر برامج

التجسس "وأكثرها تعقيداً"، وهو يستهدف بشكل خاص الأجهزة الذكية التي تعمل بنظام التشغيل "آي أو إس (iOS)" لشركة آبل، لكن توجد منه نسخة لأجهزة أندرويد تختلف بعض الشيء عن "آي أو إس".

وأوضحت شركة "كاسبرسكي المتخصصة في برامج الحماية من الفيروسات- إن "بيغاسوس" من نوع "البرامج الضارة المعيارية" أي أنه مؤلف من وحدات، حيث يقوم أولاً بعملية "مسح للجهاز المستهدف، ثم يثبت الوحدة الضرورية لقراءة رسائل المستخدم وبريده الإلكتروني، والاستماع إلى المكالمات، والتقاط صور للشاشة، وتسجيل نقرات المفاتيح، وسحب سجل متصفح الإنترنت، وجهات الاتصال، كما إن بإمكان "بيغاسوس"، الاستماع إلى ملفات الصوت المشفرة، وقراءة الرسائل المشفرة بفضل قدرته على تسجيل نقرات المفاتيح وتسجيل الصوت، حيث يسرق الرسائل قبل تشفيرها والرسائل الواردة بعد فك تشفيره. (https://political-encyclopedia.org/dictionary/%D8%A7، 2022)

إن الهجوم الإلكتروني، يحدث مثل نظيره العسكري، على ثلاث مراحل: الذكاء والتخطيط والتنفيذ فمرحلة الذكاء بالمعنى الواسع هي الأكثر أهمية لأنها تجعل من الممكن معرفة العيوب المختلفة القابلة للاستغلال من خلال هذه المرحلة على وجه الخصوص، يتم جمع المعلومات لسرقة الهوية وهذه العملية حدثت في فرنسا، والتي كانت 500 شركة فرنسية ضحية لها، مقابل خسارة 485 مليون يورو في خمس سنوات، إضافة إلى هذه الأعمال يأتي ما يسمى بالتجسس الاقتصادي للوصول إلى البيانات السرية لملفات العملاء، الأسعار، التوقعات، أسرار العمل والغرض منها هو زعزعة استقرار النشاط الاقتصادي لكيان ما بهدف جعل موقع ويب أو متجر على الإنترنت أو خدمة عملاء يتعذر الوصول إليه.

أما الطرق التقليدية فهي اغتصاب عنوان البريد الإلكتروني لأحد المدراء التنفيذيين في الشركة لتشجيع الرؤوس على أداء مهمة باستخدام تحويل نقدي سبيل المثال أو مشاركة المعلومات السرية، إذا لزم الأمر من أجل التلاعب بالسوق (El-djoundi, 2020)، هناك طرق أخرى يستعملها قراصنة الويب وهي السيطرة على شبكة الكمبيوتر ومطالبة المستخدمين بفدية مقابل تسريح الشبكة له، انتشر هذا النوع من الهجوم باستخدام برامج الفدية انتشر مع ظهور العملات المشفرة مما يجعل العملية غير قابلة للتعقب من قبل السلطات. ويقال إن هذه الهجمات بدأت بالانخفاض في الآونة الأخيرة. كما يجب الإشارة إلى نوع آخر من الهجمات الفتاكة ما يسمى ببوت نت والذي يهدف إلى تكوين جيش من الرقيق، ما يحدث شللاً في حواسيب المستخدمين والسيطرة عليها.

تعد الجرائم الإلكترونية وسيلة غير مشروعة أقل خطورة من الأنشطة الإجرامية التقليدية مثل الاتجار بالمخدرات أو الاتجار بالبشر أو الابتزاز قدمت شركة سيمونتيك في عام 2018 مخططاً للتهديدات الإلكترونية وهي كالتالي: ما بين عامي 2016 و 2017، شملت الهجمات: الصين بنسبة (21٪) والولايات المتحدة (11٪) والبرازيل (7٪)، روسيا (6٪)، الهند (5٪) وكل هذا رغم وجود تطبيقات وأجهزة حماية، ضد الفيروسات والهجمات الإلكترونية على غرار كاسبرسكي وسكورالست.

وجد باحثون من فريق تحليل البحوث العالمية على حقيقة أنه في عام 2017، كانت الحكومات هي الأكثر استهدافاً من قبل مجموعة معلومات التدريب على الذكاء الاقتصادي كما تعتبر البنوك والمؤسسات المالية، باعتبارها حراساً للثروة الشخصية والتجارية، أهدافاً رئيسية للجرائم الإلكترونية، تزداد محاولات الجرائم الإلكترونية المالية بشكل متزايد ومكلفة وناجحة، فوفقاً للمجموعة البحثية والاستشارية بالمملكة المتحدة، فهناك أكثر من 1.6 مليار جنيه إسترليني من خسائر الاحتيال غير المصرح بها في عام 2020، أي ما يقارب من 6.73 جنيه إسترليني في كل محاولة 10 جنهات إسترلينية. (Model behavior: Using AI to beat financial cybercrime، 2022)

زادت المكافحة ضد هذه الهجمات خاصة من قبل وحدة المعلومات والاستخبارات المالية التي قامت بحماية أكثر من 2.1 مليون رقم بطاقة مخترقة في عام 2020 (EGE، 2020)، استجابت المؤسسات المالية لمطالب عملائها لمزيد من المرونة والوصول من خلال التطبيقات والخدمات المصرفية عبر الإنترنت، مدفوعة بالحاجة إلى الحفاظ على قدرتها التنافسية ولكن لا ينبغي إن يأتي ذلك على حساب الأمان، سواء أثناء عملية الإعداد أو ضمن تفاعلات العملاء الحالية حيث تعد لوائح الامتثال التنظيمي ومتطلبات راحة المستهلك من الاعتبارات الأساسية ولكن في الوقت نفسه يؤدي هذا إلى استمرار تنامي الجرائم المالية، وجرائم الإنترنت بوتيرة متسارعة من خلال سرقة الهويات والمستندات والتلاعب بها، من خلال عمليات

الاحتيال على الاستيلاء على الحساب إلى التهديد المستمر بالاحتيال على البطاقة ، كل هذا جراء هشاشة نظام الأمن السيبراني ، في الواقع ، ترتبط الجريمة الإلكترونية والجريمة المالية الآن ارتباطاً وثيقاً ، مع تطور استراتيجيات جرائم الإنترنت على نطاق واسع كوسيلة لتوليد مدخلات للجرائم المالية سواء أكان الأمر يتعلق بسرقة الهويات بما في ذلك المستندات وصور الهوية أو أرقام بطاقات الائتمان ، إن الجهات الفاعلة السيئة تجمع هذه المعلومات بشكل روتيني وتستخدمها بشكل متكرر وفعال عبر الإنترنت لارتكاب مجموعة واسعة من الجرائم. (Op.cit) ، وتستخدمها بشكل متكرر وفعال عبر الإنترنت لارتكاب مجموعة واسعة من الجرائم. (Op.cit)

## 6- القرصنة الإلكترونية تحت البحار:

ظهرت القرصنة الإلكترونية تحت البحار بشكل مخيف خاصة مع هجوم القرصنة على سلك في البحر الأحمر في صيف 2016، ما أحدث خلا في خدمة الاتصالات السلكية واللاسلكية والويب، لأن الألياف الضوئية الآن تعتبر المتجه الرئيسي للاقتصاد العالمي متصلة بأعماق البحار وهي التي تغذي بالمعلومات الويب بنسبة 99٪ فتنتقل عن طريق شبكة تحت الماء ما أحدث ثورة اتصالية. تلعب البنية التحتية دوراً هاماً في نقل البيانات، خاصة ما يتعلق بالجانب التمويلي أو التجاري وكل أصناف الخدمات الأخرى، لقد أصبحت جميع الإدارات والجيش اليوم تستخدم طرق الإرسال عبر الأسلاك البحرية وأي هجوم عليها أو انقطاع سيؤدي إلى عواقب وخيمة جداً، ومن الأمثلة البارزة تأثر نظام الاتصالات التابع للبحرية الأمريكية سيا مي وي 3 بعد تمزق السلك البحري ما تسبب بخسارة مالية فادحة. (CAIRN، 2022)

## 7. تقنية التزييف العميق وكيفية مجابهتها:

أصبح التزييف العميق من الهجمات الفتاكة حيث يستفيد مجرمو الإنترنت من هذه التقنيات، لإنشاء هجمات متطورة للغاية، بالتالي فإن اكتشاف الهجمات الإلكترونية والوقاية منها أصبح تحدياً متزايداً للأفراد والشركات حيث يستخدم المتسللون أساليب أكثر ابتكاراً، أين يقوم محترفو الأمن السيبراني باختراق البيانات وإنشاء هجمات عبر برامج الفدية وعمليات التصيد الاحتيالي. ما يشكل تحدياً كبيراً بالنسبة الدول والأفراد هي التزييف العميق، وما يترتب عنه من انعكاسات جد وخيمة عبر نشر مقاطع فيديو مزيفة مظلمة (deep fake technology، 2022). وهناك عدة أمثلة ووقائع عن هجمات التزييف العميق، فلقد تم تسريب مقطع فيديو مزيف للرئيس السابق دونالد ترامب، ثم تبين أنه تم استخدام التقنية لتضليل الرأي العام.

لقد أدت قضايا التزييف العميق إلى سرقة أموال طائلة عبر اليوتوب في روسيا، كما تم خداع بنك مقره في هونغ كونغ بهجوم "صوت مزيف" مدعوم بالذكاء الاصطناعي حيث قام شخص ما باستنساخ صوت مدير ماثوق وطلب تحويل 35 مليون دولار (Op.cit).

أصبحت تقنية وهجوم التزييف العميق أكثر قوة في 2022 حيث تقوم الجهات الفاعلة باستعمال التهديد واستبدال صوت الشخص أو استخدام صورته لإنشاء محتوى مزيف أو نشر معلومات مظلمة، يستخدم بعض الأشخاص تقنية التزييف العميق لشن هجمات انتقامية أو تشويه سمعة شخصية عامة، فعلى سبيل المثال ، تفاجأت هيلين مورت ، الشاعرة والمذيعة المشهورة في المملكة المتحدة ، عندما قال أحد معارفها إن صوراً عارية لها نُشرت على الإنترنت وعبر منصات التواصل الاجتماعي حينها علمت مورت أن هؤلاء المجرمين استخدموا تقنية التزييف العميق لتحرير صورها وإطلاق حملة إباحية مزيفة ومحاولة تشويه سمعتها.

أصبح الاعتماد على الإنترنت من قبل الشركات والمنظمات في تزايد مستمر مما جعلها عرضة للتهديد الدائم من قبل القرصنة الذين يعتمدون إلى اختراق أنظمة الاتصالات وحسابات الشركات والأشخاص وتزييف الحقائق والاحتيال وطلب الفدية وسرقة حسابات وإيميلات الأشخاص والشركات عبر تقنية التزييف العميق، وهذا ما صعب وشكل تحدي كبير للأشخاص والشركات لردع هجمات التزييف العميق لأن الناس تميل إلى تصديق ما تراه دون استعمال عين الشك والتدقيق

لتحليل الظاهرة كل هذا أدى بالشركات المختصة، إلى تطوير نظام الحماية من التزييف العميق (Op.cit) وذلك عبر نظام وتقنية التشفير المائي واطر مارك الذي يمكن من وضع نظام حماية للصور والفيديوهات وغيرها ما يصعب مهمة اختراقها من قبل القراصنة ومجرمي الويب، كافحت الشركات عمليات الاحتيال المتعلقة بالهندسة الاجتماعية والهجمات الإلكترونية المتزايدة فهناك تقرير صادر في عام 2021 يشير إلى إن ، هناك زيادة بنسبة 50٪ في هجمات الأمن السيبراني أسبوعياً على شبكات الشركات مقارنة بعدد الهجمات في عام 2020.

حقق الذكاء الاصطناعي تطورات كبيرة في تحليل الصور والصوت والفيديو عبر هذه التقنية أين يتم تحليل المحتوى وحتى فك تشفير مقاطع الفيديو والأصوات المزيفة عن طريق تقنية أبل وال كما تم تطوير نظام قادر على اكتشاف التزييف العميق عبر منصات التواصل الاجتماعي على غرار الفايستوك عبر تطبيق الهندسة العكسية لتحديد للكشف عن مصدر الهجوم وإدارته بشكل فعال (Op.cit).

قامت عدة شركات بالتفكير في استخدام طرق المصادقة المختلفة لمحاربة هجمات التزييف العميق فبعد التحقق من أي محتوى تمت مشاركته داخل المؤسسة أو خارجها والمصادقة عليه أمراً بالغ الأهمية في إحدى الطرق الفعالة في عالم التشفير، إضافة إلى تكثيف البرامج الوقائية والتطبيقات السليمة ذات مصداقية والتي لا تحمل معها أغراض الجوسسة أو إلحاق الضرر بجهاز المستخدم وجعله هشاً وغرضه للقرصنة، إضافة إلى كل هذا هنالك تقنية طلب إثبات هوية منفذ الهجوم وتأكيداها قبل نشر المحتوى ومشاركته وعدم المصادقة عليه للكشف عنه وردعه مباشرة (Op.cit).

وهناك تقنية أخرى أكثر نجاعة لردع هجمات القراصنة، خاصة التزييف العميق وهي توعية الموظفين بأفضل ممارسات حول الأمن السيبراني، فقد يبدو الأمر وكأنه سهل ولا يحتاج إلى تفكير، ولكن من الضروري تثقيف الموظفين حول التزييف العميق وتشجيعهم على استخدام أفضل ممارسات الأمن السيبراني فيعد إعطاء الأولوية لتعليم المستخدم أفضل دفاع للشركة لأن العديد من الانتهاكات الأمنية أسبابها أخطاء بشرية بسيطة، من غير المرجح أن يقع الموظفون المتعلمون ضحية للهجمات الإلكترونية الشائعة لأنهم يعرفون ما الذي يبحثون عنه وعادة ما يكون لديهم مستوى معين من الشك عند التعامل مع المحتوى أو مراجعة رسائل البريد الإلكتروني المشبوهة بالتالي يمكن إن يساعد التدريب على رصد التزييف العميق وقضايا الأمن السيبراني الأخرى الشركات على تجنب الوقوع كضحايا لهجمات التزييف العميق.

## 8-البرامج الضارة ، طرق الكشف عنها وردعها:

مع قيام المزيد من المؤسسات بنقل أصولها إلى السحابة كلود ، يوجه موزعو البرامج الضارة انتباههم إلى السحابة أيضاً، وهنا يجدر طرح سؤال جوهري مهم وهو كيف تجد البرامج الضارة طريقها إلى الأصول السحابية، في العالم الداخلي؟. تعتمد نواقل العدوى الرئيسية على الإجراءات المتعلقة بالمستخدم مثل، المرفقات الضارة برسائل البريد الإلكتروني أو الروابط الخبيثة في رسائل البريد الإلكتروني أو التنزيلات من المواقع شبه الشرعية، يختلف الأمر قليلاً في عالم السحابة ، حيث يبحث المهاجمون عن نوع مختلف من سلوك "المستخدم" غير الأمن مثل الأصول غير الخاضعة للإدارة والحسابات التي تم تكوينها بشكل خاطئ فالمستخدمون هنا هم أصحاب السحابة، تعتمد نواقل الهجوم الأكثر شيوعاً في السحابة على العثور على الأصول ذات المصادقة السهلة مثل كلمات المرور الضعيفة أو المسربة، ونقاط الضعف القابلة للاستغلال والاستعمال المفرط والخطير للإنترنت (cyber-security، 2022).

إن انتشار القرصنة والفيروسات بات في تزايد مستمر فهناك العديد من الفيروسات الفتاكة والأكثر انتشاراً على غرار حصان طروادة المعروف بانتشاره الكبير من خلال البريد الإلكتروني ومرغقاته، كما تصيب بخلل نظام التشغيل المعروف بالوندوز هناك أيضاً ما يسمى بهجوم نات واير والذي يستهدف الكلمات السرية في الحسابات والتحكم بالأجهزة، أما هجمات دوس فهي جد خطيرة فهي تعمل على شل الحواسيب ونظام التشغيل.

وكانت الجزائر من الدول التي أرادت استعمال نظام الإمداد النفطي والغازي عبر التحكم بالبيب لاین والأنابيب بالتقنيات الحديثة ولكن لم تقم بها خوفاً من قرصنة نظامها ما سيحدث خسائر فادحة للاقتصاد الجزائري، إن الهجوم الذي نفذته

القرصنة بتوظيف برنامج درك سايد بعد تشفير بيانات الشركة البترولية الأمريكية وسرقة البيانات السرية والقيام بابتزاز الشركة وإفشاء أسرار الشركة مكن القرصنة من طلب فدية حيث قامت الشركة بدفعها للمهاجمين لفك الشفرة وعدم إفشاء البيانات السرية للشركة. ولعل مجموعة برامج الفدية المستخدمة دارك سايد قامت بابتزاز العديد من المشاهير عبر سرقة واختراق بياناتهم مثل مادونا وليدي غاغا وطلب الفدية منهم.

لقد وصلت هجمات القرصنة، ذروتها خاصة مع استهداف العملات المشفرة وهذا كلها بسبب الهشاشة المركزية والقدرة للوصول إليها بطريقة سهلة لعدم وجود تشفير فعال، هناك العديد من الطرق لتنفيذ التعليمات البرمجية الضارة في قاعدة البيانات، فكل ما يحتاجه المهاجم هي ثغرة أمنية أو تكوين خاطئ ويمكن تنفيذ هجوم على الفور، يقوم المهاجمون بفحص الإنترنت باستمرار بحثًا عن قواعد البيانات بعدها وبعد وقت طويل من البحث وإيجاد الثغرة يقومون بتنفيذ الهجوم.

ولتجنب البرامج الضارة في البيئة السحابية، يجب إتباع ثلاثة مبادئ أساسية أولاً هو عدم الإفراط في استخدام الإنترنت، فالبرامج الضارة في السحابة تأتي في الغالب من مهاجمين خارجيين فالأصول المعرضة للإنترنت هي نقطة الدخول للمهاجمين فيجب التأكد من كشف الأصول التي يجب كشفها فقط والحفاظ على البيانات والأشياء السرية في أمان وبعيداً عن وصول عامة الناس الخطة التالية، هي التأكد من أن الأصول السحابية مؤمنة ومصححة بشكل صحيح، حيث يتم فحص الأصول التي تواجه الإنترنت من قبل جهات ضارة طوال الوقت وستجعل كلمات المرور الضعيفة أو نقاط الضعف طريقها أسهل بكثير، في الأخير يجب التدقيق في كل دور وأصل في السحابة (Op.cit).

تعتبر الحوسبة السحابية بمثابة تقدم تقني في تكنولوجيا المعلومات كان هذا التقدم مدفوعاً للعديد من المنظمات للاستعانة بمصادر خارجية لبياناتها واحتياجاتها الحاسوبية هذه المنصات مطلوبة للوفاء بمبادئ الأمان الأساسية مثل السرية والتوافر والنزاهة.

تقدم الحوسبة السحابية خدمات افتراضية وقابلة للتطوير بمستوى عالٍ من المرونة وتكاليف صيانة منخفضة للمستخدمين النهائيين، قد تحتوي البنية التحتية والبروتوكولات الكامنة وراء الحوسبة السحابية على أخطاء ونقاط ضعف، يتم استغلال هذه الثغرات الأمنية من قبل المهاجمين، مما يؤدي إلى شن هجمات، ولعل من بين أكثر الهجمات المبلغ عنها في الحوسبة السحابية هجمات رفض الخدمة الموزعة دوس يتم تنفيذ هجمات ما يسمى بهجمة دوس، عن طريق إرسال العديد من حزم على البيانات إلى البنية على البنى التحتية المستهدفة مما يؤدي إلى استهلاك معظم النطاق الترددي للشبكة ووقت الخادم، ويؤدي إلى رفض الخدمة لهذا تم اقتراح العديد من الطرق وتجربتها للكشف المبكر عن الهجوم يستخدم النهج المقترح في 2022 مجموعة من المصنفات المعتمدة على اكتشاف الهجمات وتم دراسة 32000 حالة هجوم بما في ذلك 8450 حالة هجوم حميدة وتم الكشف عن 98,65 من الهجمات (repulic, 2020).

إن التحديات كثيرة ومتنوعة فعلى المستوى القانوني والسياسي، تظهر على عدة مستويات على المستوى الوطني، الدول هي الخاسر الأكبر اعتماداً على الأدوات التكنولوجية، تكافح من أجل إنفاذ سياساتها الضريبية وقوانينها على الشبكات (الكشف عن البيانات الحساسة)، وتكييف القوانين المتعلقة بالنشر استطلاعات الرأي أو الألعاب عبر الإنترنت، أو إساءة استخدام حرية التعبير في النقاش، أو حول قوانين "مكافحة المعلومات المزيفة" أو مكافحة الكراهية على الإنترنت)، يجب عليها أيضاً التكيف مع التهديدات الجديدة (الجرائم الإلكترونية، القرصنة)، التجسس، برامج الفدية، إن غياب الحوكمة في الفضاء الرقمي يفسح المجال أمام تنظيم شبكي لامركزي، إلى حد كبير إشراك الجهات و الفواعل غير دولية في تشارك السلطة في الفضاء السبراني، ما يعرض الدول وحقوق الأفراد وسيادة البيانات إلى الخطر.

سيضمن تقرير المصير المعلوماتي حق الأفراد، للتحكم في استخدام ومستقبل البيانات الشخصية المقدمة، وكذلك "الآثار" التي خلفها النشاط الرقمي فلقد تم بالفعل تكريس بعض الحقوق المستمدة منها، ولا سيما على المستوى الأوروبي، من خلال اللائحة العامة لحماية البيانات الشخصية، التي دخلت حيز التنفيذ في 2018، أو من قبل محكمة العدل التابعة للاتحاد الأوروبي (الحق في النسيان)، وإلغاء المرجع، وإمكانية نقل البيانات، والموافقة، والمعلومات والتصحيح، وما إلى ذلك، أصبحت أوروبا الآن أكثر يقظة، بعد أن اعتمدت منذ فترة طويلة، في مواجهة نهب بيانات مواطنيها والمساومة عليها،

"نفس نظام الدفاع أنها تستفيد من أحد الأصول الرئيسية المستهلكون الأوروبيون هم السوق الاقتصادي الرائد للعمالقة الرقميين، على المستوى الدولي ، يجب بلا شك إصلاح حوكمة العالم الرقمي ، حيث إنه غير متعدد الأطراف وديمقراطي وشفاف بشكل غير كافٍ، يُعهد بوظيفة التقييس إلى جهات فاعلة خاصة ، أو منظمات غير معروفة جيداً ، أو مجموعات غير رسمية لا يتم ضمان شرعيتها واستقلاليتها في مواجهة القوى العظمى على غرار، الولايات المتحدة ، ومجموعات المصالح بسبب عدم تقاسم المسؤوليات ، قامت القوى العظمى الأكثر قوة من الناحية الاقتصادية أو التكنولوجية و إلى إنشاء "إنترنت منفصل" ، وهو أمر مقلق بالنسبة لمستقبل الشبكات، بالنسبة للأوروبيين (Op.cit) ، لأنه بحسبهم يغيب دورهم في إدارة الشبكات وتعزيز قيمهم فيها وتكريس الديمقراطية والشفافية التي ناضلت من أجلها، الحكومات المنتخبة والخاضعة للمساءلة والشفافة والملزومة بالعمل من أجل المصلحة العامة والخضوع للمساءلة ومع ذلك ، فإن هذه الحكومات تتنافس مع هيئات إدارة جديدة مهمة لا تخضع لأي من هذه القيود والمتطلبات، لهذا السبب يفكر البعض في إضفاء الطابع الرسمي ، في "ميثاق" مع دعوة عالمية ، إلى المبادئ الأساسية التي يجب إن توجه تطوير التقنيات (الحياد ، حرية التعبير ، التنوع اللغوي ، حماية الخصوصية ، إلخ)، هناك قضايا أخرى تتعلق القضايا الأخرى بأنماط التعبير عن المواطنة ، وتمكين الأفراد ، الذين تمت دعوتهم لاستعادة جزء من سيادتهم ، من أجل تجربة أكثر نشاطاً في المواطنة، إذا لم يرغبوا في الخضوع للتغيير التكنولوجي ، فيجب على الأجيال الشابة تعلم إتقان الأدوات الرقمية ، ومعرفة حقوقهم وحررياتهم والتأكيد عليها ، والاهتمام ببناء وحماية "هويتهم الرقمية" ، الناتجة عن كل الآثار التي تركت طواعية أم لا على الشبكات ، إضافة إلى كل التحديات المذكورة سالفا هناك تحدي أكبر وهو اعتماد الاقتصاد العالمي على القطاع الرقمي إذ يتيح استغلال كتلة البيانات التي تم جمعها (البيانات الضخمة) ، المجمع والمعالجة بواسطة الخوارزميات (Op.cit)، إمكانية توقع - حتى توجيه - سلوك المستهلكين والعملاء ، مما يفتح آفاقاً هائلة حول تكييف العرض التجاري في الوقت الفعلي ، وثورة في مناهج الإعلان والتسويق ، ومقارنة الأسعار ، وإدارة المخزون، وما إلى ذلك (Op.cit).

ويتطلب التحول الرقمي وتحقيق الأمن السبراني اتباع، نهجا أكثر استباقية أولاً تحولاً زلزالياً في منظور الإدارة، لرؤية الأمن كوظيفة أساسية لحماية ما قامت الشركات ببنائه على مدى سنوات عديدة، و "الانتصار" في المواجهة المستمرة مع القراصنة. لكن الواقع الذي تواجهه جميع الشركات هو على الدوام "" من عدم الاستعداد للتحدي الذي يجب عليهم مواجهته، وغير مدركين للتجليات العديدة للتهديد لذلك ليس من المستغرب أنهم يجدون صعوبة في فهم الشكل الذي يبدو عليه نموذج الأمان الدائم وذات الصلة، ناهيك عن كيفية تنفيذه، يتطلب الأمن الاستباقي إتباع نهجاً معقداً ومتكاملاً أو "مقارناً" يتضمن عناصر الأمن البشرية والمادية بقدر أمن تكنولوجيا المعلومات لتوفير "أمان المعلومات".

تميل الإخفاقات البشرية والالتزام الباهت بممارسات الأمان الجيدة إلى تفسير العديد من الانتهاكات الأمنية وعصر إدخال الموظفين أجهزتهم الخاصة في مكان العمل يؤدي إلى تفاقم المخاطر التي تواجهها الشركات، يمكن للمهندسة الاجتماعية والتخريب والتطفل المستهدف والتسلل إن تعرض تكنولوجيا أمن المعلومات للتهديدات من داخل "المحيط" ، بالنسبة لمعظم المنظمات ، يتطلب علاج المشكلات البشرية والجسدية قيادة وتغييراً ثقافياً يصعب عليهم تبنيها ، بسبب برنامج التوعية المكثف المطلوب لدعم سياسات وإجراءات أكثر صرامة، في حين إن هناك قبول ضمني للمشكلة ، إلا إن الرغبة الإدارية غير كافية للتفكير في حل هادف لذلك في حالة عدم وجود إدارة استباقية ومستنيرة ، يتم تخصيص ميزانيات أكبر للأنظمة الاستباقية ، لضمان نظام الدفاع والأمن (Op.cit).

يستنتج من كل هذا إن أمن المعلومات يثبت أنه مفهوم ثابت في الطريقة التي يتم تنفيذه بها حتى على أنه "أمان استباقي". يُظهر نهج "المحيط" المستمر المعتمد بشكل شائع "أعراض الوهم" التي ابتليت بها المفاهيم الأمنية منذ بناء جدار هادريان حتى خط ماجينو، وهم يقللون من شأن خصمهم بشكل خطير، إن حقيقة الممارسات الثابتة الحالية هي أنها تفشل فالمسألة أقل بكثير عن طبيعة مفهوم الأمن وأكثر عن "العقيدة" التي تتبناها الشركات لمكافحة التهديدات.

يجب إن يؤخذ النهج المتقدم للدفاع الإلكتروني في الاعتبار و تبني نهج وقائي ، وموقف دفاعي أكثر نشاطاً، فكلأهما بحاجة لأن يُنظر إليهما على أنهما نهجان "قائمان على العقيدة، يفترض النهج الوقائي إن التدابير الفعالة ستوقع التهديدات

الحالية وتكون مستعدة لصمد الهجمات ، بناءً على معلومات التهديد ذات الصلة ، وإعداد واختبار تدابير الاستجابة ، وكجزء من عقيدة "مطورة" للكشف والاستجابة فبمجرد إنشاء الدفاع المعقد بشكل مناسب ، يتم بناء هذا النهج على مبادئ استباق الفشل المحتمل ، من خلال محاكاة ما يحتاج الدفاع إلى تحقيقه ، وكيفية تحقيقه ، وفي ظل أي ظروف سيفشل ، ثم يتم تحديد ذلك مقابل أنواع التهديد التي تواجهها المنظمة وإبلاغ أي تعزيز للقدرات المطلوبة، إنه يضمن حالة عالية من "الاستعداد" للتعامل مع ما يمكن توقعه بشكل معقول، ويحافظ على فعالية القدرات التي تمتلكها الشركة نظرًا لأنه من المقبول عمومًا إن معظم الشركات غير قادرة على حل هجوم إلكتروني، فإن هذا النهج له فوائد عديدة؛ ليس أقلها أنه يدفع المنظمات إلى تحقيق التوازن بين تركيزها بين الوقاية والاستجابة، علاوة على ذلك ، وبسبب تخصيص القليل من الاستثمار والتخطيط للاستجابة في الوقت الفعلي ، فإن النهج الوقائي يحفز وعيًا محددًا يؤدي إلى مزيد من التحضير والاستثمار في الاستجابة ، حتى لو كان يقتصر في البداية على الاستعانة بمصادر خارجية للاستجابة لحوادث الإنترنت الموثوقة (d'expert, 2022).

بالنسبة للمنظمات التي لديها تسامح شبه معدوم مع فقدان الملكية الفكرية وفشل الأمن بشكل عام، لا يزال النهج الوقائي لا يفي بالمتطلبات الأساسية لـ "الدفاع" لأنه لا يوفر لهم فرصة كافية لاعتراض محاولات الخروقات والتغلب عليها. لها خصائص متعددة الأوجه ، واستخدمت خداعًا معقدًا ضدهم كما أنها توفر عامل ردع ضعيف لذلك يجب العمل على بناء الدفاع النشط الذي يفترض إن الدفاع الفعال يتطلب خطة نشطة معدة مسبقًا لردع التهديدات أو "التصدي لها" أو الاشتباك معها كجزء من عقيدة دفاعية (Op.cit) ، مع تزايد مجموعة الأدلة حول مخاطر التجسس الإلكتروني والتوسع السريع في سطح الهجوم ، فقد ثبت بشكل متزايد عدم جدوى الاعتماد على أي محيط ، يحتاج المدافعون إلى البدء في تطوير "التكتيكات" ، والمزيد من المفاهيم العسكرية مثل "السيطرة على ساحة المعركة" ، وتطوير "مناطق القتل" (Op.cit)، واستخدام الحيلة والشرك والتمويه، هذه مهمة معقدة من الناحية المفاهيمية لأن النهج والأساليب تختلف اختلافًا جوهريًا عن الموقف الأمني التقليدي ، والمهارات المطلوبة أكثر تقدمًا.

يعد استخدام استراتيجيات الخداع داخل العقيدة الدفاعية أمرًا محوريًا لعقيدة الدفاع المسبق لأنها تضيف التعقيد إلى ساحة المعركة، مما يوفر الوقت و "المساحة" وخيارات الاشتباك، كما يؤدي تقديم الخداع أيضًا إلى إنشاء "مجاهيل" يتعين على المهاجمين معالجتها، ويزيد من احتمالية فشل الهجوم، في بعض الحالات ، يمكن إن يكون لـ "إظهار القوة" أو تقديم إشارات تدل على وجود خطة خداع عامل رادع ضد بعض المهاجمين.

كان الخداع دعامة أساسية للحرب منذ العصور التوراتية، والتاريخ مليء بالأدلة على القيمة الاستراتيجية للخداع في العالم التجاري، يمكن إن يوفر استخدام الخداع جانبًا منخفض التكلفة وفعالًا للدفاع عن المعلومات، وذلك باستخدام طرق لإرباك المهاجمين أو تظليلهم أو خداعهم للاعتقاد بأنهم لم يتم اكتشافهم أو الوصول إلى بيانات حقيقية أو إن أساليبهم فعالة. من خلال التوقيت الدقيق والتسلسل الدقيق لـ "مسرحيات" الخداع، يمكن للمدافعين تقديم حالة من عدم اليقين حيث من المرجح إن تفيد المدافع، وتعزيز ثقة المهاجم حيث لا يوجد ما يبرر ذلك.

## 9. الخلاصة :

خلصت الدراسة لما يلي:

- شهد العالم ثورة تكنولوجية هائلة ادت الى تسارع وتيرة الرقمنة.
- السيادة الرقمية تطورت بشكل كبير مع ظهور التهديدات الامنية اللاتماثلة الجديدة على غرار كوفيد 19
- اهتمت الكثير من الدول الرائدة على غرار الصين والولايات المتحدة وروسيا وإيران بالسيادة الرقمية، والتحول الرقمي، عبر تفعيل نظام الحماية والانداز المبكر لصمد التهديدات الالكترونية الجديدة

- ارتبط التحول الرقمي والسيادة الرقمية ارتباطا وثيقا بالاقتصاد والتجارة والأمن القومي لذلك سعت الدول، حتى النامية مثل تونس وتشاد ومالي والجزائر لبلورة نظام الأمن السيبراني لحماية أمنها القومي.
- أزمة كورونا فعلت وزادت من التحول الرقمي للعديد من الدول خاصة دول الشرق الاوسط والقرن الافريقي.
- تكوين طاقم بشري في مجال الامن السيبراني، وتحسيس المجتمع بمخاطر ومزايا التحول الرقمي من اساسيات نجاح وتقوية السيادة الرقمية للدول.
- الوقاية خير من العلاج وصفة وعلاج لكل المشكل لذلك من الجيد الحذر من التطبيقات والإيميلات المشبوهة، لمنع الجوسسة والاختراقات وسرقة المعلومات السرية الخاصة بالمستخدم والشركات والدول.
- الاستقلالية التكنولوجية وحوكمة الانترنت، والمواقع المحلية من المکانزمات الفعالة لبسط السيطرة على البيانات ومنع الاختراقات.
- التهديدات في تزايد مستمر وتقنيات المجاهبة في تطور أيضا، وهذا ما يشكل تحدي كبير لمستقبل الدول في تحقيق التحول الرقمي المنشود وتحقيق فضاء سيبراني آمن.
- لا يوجد تحول رقمي، إدارة إلكترونية فعالة وناجحة، بدون تكوين وتحسيس، والامام بالعالم الجيوبولتيكي الافتراضي.
- الإدارة الالكترونية الجيدة تعتمد على الفصل بين حواسيب العمل والاستعمالات الشخصية وقطع أي صلة بالعالم الافتراضي والمنصات الاجتماعية لتفادي تسرب البيانات الحساسة للدول والشركات.

## 10. قائمة المراجع:

- CAIRN. (2022, 07 17). *Léxique de la souveraineté numérique*. تم الاسترداد من <http://www.revue-cairn-lexique-espace-cybernetique-geo-politic-and-digital-sovereignty.cyber-security.deep-fake-technology.review,c-s>
- EGE. (2020, 5 15). *info-guerre*. تاريخ الاسترداد 2022، من <http://www.infoguerre-souv-numerique-htm>
- El-djoundi. (2020, 07 6). *تطور الامن السيبراني*. تاريخ الاسترداد 2022، من <https://www.aljundi.ae/%D8%A7>
- https://political-encyclopedia.org/dictionary/%D8%A7*. (2022, 07 06). تاريخ الاسترداد 2022، من <https://political-encyclopedia.org/dictionary/%D8%A7>
- Model behavior: Using AI to beat financial cybercrime. (2022, 05 10). *review, c-s*. تاريخ الاسترداد 2022
- Op.ci. (بلا تاريخ).
- Op.cit. (بلا تاريخ).
- p d'expert. (2022, 5 6). *souveraineté numérique*. تم الاسترداد من <https://www.vie-publique.fr/parole-dexpert/276125-definition-et-enjeux-de-la-souverainete-numerique>

conflit .r (28 07 ,2020). *cyber-puissance*. تاريخ الاسترداد 2022، من  
./https://www.revueconflits.com/comparatif-cyberpuissances  
.riverpublishers .digital sovereignty (2020). repulic  
bitam (s.) (s.) (04 17 ,2022). *https://www-samira-bitam-impact-tranformation-digital-htm-*. تاريخ  
الاسترداد 2022، من *https://www-samira-bitam-impact-tranformation-digital*.  
ياسين مليح. (أكتوبر، 2021). السيادة الرقمية تحدياتها وممكنات تحقيقها بالمغرب. *مجلة العمال الدولية*.