السنة: الحادية عشرة المجلد: 11 العدد: 01 ص ص: 77- 110
EISSN 2676-1645 ISSN 2543-375X

هندسة الأمن السيبراني في عصر الذكاء الاصطناعي
قراءة في أدوار واستراتيجيات اليقظة الخوارزمية

Cybersecurity Engineering in the Age of Artificial Intelligence - Reading into the Roles and Strategies of Algorithmic Vigilance

خرفية جودي*، مخبر البحث في وسائل الإعلام،
الاستخدامات الاجتماعية والاتصال،
المدرسة الوطنية العليا للصحافة وعلوم الإعلام
Djoudi.kherfia@ensjsi.dz

تاريخ الاستلام: 2025/06/07 تاريخ القبول: 2025/11/26

ملخص:

يـ شكل الأمن الـ سيبراني تحدّيا فائق الأهمية لمواكبته الثّورة التّكنولوجيّة الّتي أ سهمت في ميلاد عـ صر الذّكاء الا صطناعي، وأمام تعدّد الأدوار الّتي يؤديها ا ستخدام الذّكاء الا صطناعي بين اختراق وتهديد للأمن السيبراني وبين حماية وردع هذه التهديدات، تبحث هذه الورقة سبل وا ستراتيجيات خوارزميات الأمن الـ سيبراني في ظل تر سانة من التقنيات التي يتحيها الذكاء الا صطناعي من التعلم الآلي والأمن الـ سحابي وإدارة حماية الو صول والأنظمة والـ شبكات والتوقيع وغيرها ، وهذه التحولات ارتبطت بضرورة حوكمة الأمن السيبراني بما يتنا سب والفكر القيمي والأطر التـ شريعية الـ ضابطة ، ضمن تفعيل سيا سات اليقظة الخوارزمية نحو تكريس مفاهيم وآليات هند سة الأمن الـ سيبراني على المدى الطويل بما يضمن جعل الأمن السيبراني من الأولويات القصوى التي يجب الاهتمام بها على مختلف الأصعدة.

* المؤلف المراسل

الكلمات المفتاحية: الأمن السيبراني – اليقظة الخوارزمية – الذكاء الاصطناعي – استراتيجيات – الأدوار.

Abstract:

Cybersecurity poses a critical challenge to keep pace with the technological revolution that contributed to the birth of the era of artificial intelligence and the multiplicity of roles that the use of artificial intelligence plays between a cybersecurity breakthrough and a cybersecurity threat and the protection and deterrence of such threats, This paper examines the ways and strategies of cybersecurity algorithms under an arsenal of technologies saluted by artificial intelligence from automated learning, cloud security, access protection management, systems, networks, signatures, etc. and these shifts were linked to the need for cybersecurity governance commensurate with value thinking and regulatory legislative frameworks, As part of the operationalization of algorithmic vigilance policies towards the long-term enshrinement of cybersecurity engineering concepts and mechanisms to ensure that cybersecurity is one of the highest priorities to be addressed at various levels.

Keywords: Cybersecurity, Algorithmic Vigilance, Artificial Intelligence, Strategies, Roles.

مقدمة:

يشكل الأمن السيبراني هاجسا أمنيا وتقنيا يعبر في فحواه عن تحديات ورهانات وإشكاليات شائكة خصوصا في ظل الثورة الرقمية التي تشهدها المجتمعات الإنسانية، وأمام تعاظم أدوار التكنولوجيات وانخراط تقنيات الذكاء الاصطناعي AI في الصناعات الأمنية والتوظيفات العديدة لها في إدارة الهجمات والتهديدات المختلفة وهو الأمر الذي أبان عن سباق تسلّح مدعوم بخوارزميات الذكاء الاصطناعي المختلفة مثل أنترنت الأشياء والذكاء الاصطناعي التوليدي والخوارزميات والروبوتات وغيرها والموظفة فيما يمكن تسميته بـ "الحرب السيبرانية."

استطاعت تقنيات الذكاء الاصطناعي AI نقل الصراع والحرب الهجينة والسيبرانية إلى الميتا- فضاء المتسع واللامحدود افتراضيا وواقعيا، ما فتح المجال أمام الحديث عن اسقاط تصورات الخيال العلمي المنسوجة في فضاءات

الميتافيرس عن المستقبل القريب لمجتمعات الإنسان وما بعد الإنسان، بعد أن أصبحت الآلة شريكا في الحياة الاجتماعية وامتزجت التقنية لتكون امتدادا لأعضاء الانسان، هذا التحول الأداتي والشبكي والفكري كشف عن سياقات مختلفة للصراعات السيبرانية ولآلاته المستقبلية، يؤدي هذا التحول على سرعته إلى نتائج لا يمكن التكهن بها ولا يمكن رصدها إجرائيا على الأقل، أما علميا فهو يفتح مجال التحاقل المعرفي بين الدراسات الأمنية من جهة والدراسات التقنية من جهة ثانية، فالمزاوجة بين هذه التخصصات العلمية بات يشكل حتمية علمية لا مفرّ منها، ويفرض ضرورة تسريع وتيرة الترابط بين التخصصات لتجاوز القصور العلمي أو محدودية التأطير العلمي لتحولات التكنولوجيا وتوظيفاتها على صعيد الأمن السيبراني.

انطلاقا مما سبق؛ تتأسس الفجوة البحثية لهذه الدراسة، في كونها تحاول استجلاء التصورات المعرفية المرتبطة باتجاهات توظيف اليقظة الخوارزمية، باعتبارها من أبرز مخرجات التزاوج بين الرقمية واليقظة، كسياسة واستراتيجية أمنية تحاول تقويض التهديدات السيبرانية، وتفعيل آليات الردع والتصدي والحماية.

وتسعى هذه الدراسة إلى استقصاء مختلف الأليات والممارسات التي يتم توظيفها في عمليات الاختراق والجوسسة والتصيد والهندسة الاجتماعية وإدارة الذكاء الاصطناعي في الصراعات والحروب السيبرانية المختلفة، كما تعمد الدراسة الحالية إلى بيان أهمية توظيف التقنيات الذكية في الجوانب الدفاعية مثل عمليات لحماية وحوكمة الأمن السيبراني، وبالاعتماد على السياسات الرشيدة التي تؤطرها اليقظة الخوارزمية فإنه يمكن قولبة تصورات فكرية لما يمكن أن يشكل أفق اليقظة الخوارزمية في حوكمة وأخلقة تكنولوجيا الذكاء الاصطناعي AI في الفضاء السيبراني وتوطينها في ميدان الأمن.

وتبرز أهمية الدراسة الحالية في كونها تتعاطي معرفيا مع أبرز القضايا الأمنية المرتبطة بحيثيات تطبيق تقنيات الذكاء الاصطناعي AI في مجال الأمن السيبراني ضمن بعدين أساسين: يرتبط البعد الأول في بيان مخاطر الاستخدام السلبي مثل الاحتيال؛ والتصيد؛ والاختراق؛ والفضاءات التي يقتحمها التزاوج بين الإرهاب والحرب السيبرانية وتقنيات الذكاء الاصطناعي، فيما تحاول هذا

الدراسة في البعد الثاني استنطاق الآليات التي من خلالها يمكن حوكمة الأمن الـ سيبراني من خلال ا ستراتيجيات وأدوات تـ ستطيع فيها العمل على عقلنة خوارزميات الذكاء الاصطناعي AI وتوظيفها في مسار يخدم الأمن السيبراني، وتفتح أفق توطين مفاهيم اليقظة الخوارزمية وعمليات هند سة الأمن الـ سيبراني على المدى البعيد مما يـ سهم في خلق نوعا من الا ستقرار الألي يـ ضمن انخراط التقنية الذكية في مـ سار الا ستعمالات الأمنة والر شيدة وتفعيل المعايير والمبادئ القيمـ ية والأخلاقية كأطر مرجعية تحتكم إليها توجهات هـ ند سة الأمن السيبراني في ظل عصر الذكاء الاصطناعي.

ولمحاولة تحقيق أهداف هذا الدرا سة، تم اعتماد المقاربة البحثية على المنهج التحليلي الذي يـ سعى إلى ا ستعرض الأطر النظرية والمعرفية لبناء الهيكل النظري وفك التـ شابك الإجرائي بين المحاور الأ سا سية التي انطلقت منها هذه ا لدرا سة، والمتعلـ قة بمـ با حث "الأمن الـ سيبراني"، و"اليقـ ظة الخوارزمـ ية" و"تكنولوجيا الذكاء الا صطناعي" ومحاولة إقامة التعالقات المعرفية الكفيلة بتحقيق رؤية استراتيجية تتأسس عليها أهداف الدراسة الحالية.

مفاهيم الدراسة:

قبل التطرق إلى المحاور النظرية وجب بيان الحمولة المفاهيمية التي تتكئ عليها هذه الدرا سة، وهي من المفاهيم الـ شائكة والمتداخلة المجالات، وبالتالي فإنّ محاولة تحديد إطار مفاهيمي دقيق يـ ستعـ صي على هذه الدرا سة، غير أن هذا لا يمنع من ا ستعراض بعض المفاهيم التي تـ دخل في نطاق اهتمام هذه الدراسة ومجالها البحثيّ.

الأمن السيبراني:

يعرف الأمن الـ سيبراني بأنه "حماية الأنظمة والـ شبكات والبرامج والمواقع الجغرافية من الهجمات الرقمية ومن أي مـ شكل أو عائق أو هجمات إلكترونية تحول دون أداء عملها (بن مهدي وسعيدي، 2022، ص 29).

إجرائيا؛ يمكن تعريفه بأنه نظام دفاع عالي الجاهزية يستهدف تحقيق أقصى قدر ممكن من حماية المواقع والبرمجيات والشبكات والأنظمة الحاسوبية وأنظمة الحماية من القرصنة والهجومات الإلكترونية والحروب الرقمية، ويعتبر من أهم المجالات التي تتطلب درجة عالية من الأهبة واليقظة نظرا لحجم التكنولوجيات الفائقة الذكاء والتي يمكن توظيفها في نواحي هجومية ودفاعية.

يتقاطع الأمن السيبراني مع عدة تخصصات علمية تقنية؛ فهو مرتبط بميدان التكنولوجيا الرقمية ووسائطها وبرمجياتها المتعددة، ويتقاطع مع ميدان العلوم الاستراتيجية في كونها يعتمد على آليات اليقظة في الكشف المبكر عن التهديدات المحتملة التي تشكل أخطار حقيقية يمكن تداركها، ويتقاطع مع علوم الاتصال والإعلام كأرضية يعمل من خلالها على توظيف الأدوات والوسائط في الدفاع وحماية الأمن السيبراني.

اليقظة الخوارزمية:

تتعدد المفاهيم التي تلامس وتفكك مفهوم اليقظة في أبعاده المختلفة السياسية والاقتصادية والثقافية والاستراتيجية، ولكنها تشترك في كونها تمثل الآلية فهي "سيرورة إرشادية من جمع ومعالجة المعلومات ذات الصلة ببيئة المؤسسة من أجل التحكم فيها، فهي سيرورة من خلال تسلسل مراحلها، وإرشادية من خلال تحديد أنواع المعلومات التي لها صلة مباشرة باتخاذ إقرار والجمع وهي عملية الحصول على المعلومات، المعالجة من خلال تحليل المعلومات والتحكم في المعلومات لاتخاذ القرار السليم" (لمروس، 2019، ص 175) ، أو "القدرة على تقييم الظروف الداخلية والخارجية بدقة وواقعية بطريقة تسهل بناء الأفكار المهمة" (أمين عثمان و قادر كرسو، 2021، ص 168) ، ويسهم هذا المفهوم في تحديد الأدوار الهامة لليقظة الاستراتيجية التي تسعى لإدارة عمليات التقييم ضمن المستويات المختلفة بغية بناء خطط استراتيجية وقائية استباقية أو نجعية لاحقة.

تعرفها المنظمة الفرنسية للتقييس (AFNOR) على أنها "النشاط المستمر والمتكرر إلى حد كبير للمراقبة الفعالة بهدف استباق التغييرات الطارئة في المحيط التكنولوجي، التجاري، المجتمعي... إلخ"(عياط وحاكم، 2016، ص 6)، ويعتمد هذا المنظور على عمليات مراقبة التغييرات التي تحدث في المحيط وبناء خطط لمتابعتها والتنبؤ باتجاهاتها وإتاحة القدرة على اتخاذ القرارات الصائبة.

تعرف كذلك بأنها "مجموعة عمليات تستهدف البحث عن المعلومات ومعالجتها ومن ثم نشرها وحمايتها لتكون تحت تصرف الشخص المناسب وفي الوقت المناسب بغية اتخاذ القرارات الصائبة في الوقت المناسب"، وبالتالي فاليقظة تمثل الأسلوب الأمثل لإدارة العمليات واتخاذ القرار المناسب.

وتعتبر اليقظة الخوارزمية آلية تعتمد على خوارزميات الذكاء الاصطناعي AI بمختلف تقنياته وأدواته في إدارة العمليات وأتمتة القرارات وبناء التنبؤات المختلفة بناء على تحليل البيانات الضخمة التي تتيحها الوفرة المعلوماتية والتقنية والبرمجية لتكنولوجيات الذكاء الاصطناعي.AI

وتمثل اليقظة الخوارزمية من أكثر الأطر العملية التي ارتبطت بعمليات دمجت مفاهيم اليقظة الاستراتيجية في بيئة الذكاء الاصطناعي AI ضمن مجالات ذات استخدامات بالغة الأهمية مثل ميدان الأمن السيبراني والمخاطر والتحديات التي تحيط به.

الذكاء الاصطناعي:

يشير مفهوم الذكاء الاصطناعي AI إلى قدرة الآلة مثل الحواسيب على التفكير المنطقي مثل الانسان، ويتم ذلك عن طريق مجموعة من البرمجيات التي يتم تزويدها للحاسوب وتساعده على القيام بنفس العمليات الفكرية التي يقوم بها الإنسان مثل لغات الانسان أو الترجمة وغيرها (مجدي، 2020، ص 5) .

ويفسر عمل الذكاء الاصطناعي بالقدرة على محاكاة العقل البشري وطريقة عمله، مثل قدراته على التفكير والاستكشاف ومع التطورات الهائلة للحواسيب تبين أن باستطاعته القيان بمهام أعقد من ذلك (معهد الدراسات المصرفية، 2021، ص 3).

يقدم John McCarthy تعريفا شاملا للذكاء الاصطناعي AI عام 2004 حيث يقول إنه علم وهندسة صنع الآلات الذكية وخاصة برامج الكمبيوتر الذكية، وهي على ارتباط بالمهمة المشابهة لاستخدام أجهزة الكمبيوتر لفهم الذكاء البشري" (بن الصغير، 2023، ص 115).

يمكن تعريف الذكاء الاصطناعي إجرائيا بأنه "مجموعة من البرمجيات التي تؤدي سلوكيات معينة تحاكي فيها أنظمة البشر في التفكير والاستكشاف وحل المشكلات، غير أن التطورات التي عرفها الذكاء الاصطناعي AI من جيل لأخر أسهم في تجاوز قدرات الانسان في التفكير على عمليات معقدة و شائكة وقدرات مذهلة في تحليل البيانات ومعاجلة البيانات الضخمة و صولا إلى إنتاج الروبوتات التي تحاكي الإنسان الممارسات الإنسانية".

الأمن السيبراني والجيل الخامس... تحولات بنيوية

أثارت المخرجات التقنية للثورات التكنولوجية التي شهدها الإنسان، تحولات مذهلة أثّرت على الإنسان بمختلف مجالاتها، امتد هذا الأثر ليقتحم الاستعمالات المتعددة ومجالات ذات خصوصية عالية من أهمها ميدان الأمن السيبراني ليشكل في ظل تقنيات الذكاء الاصطناعي AI أهم الميادين التي استقطبت توظيفات عالية الحساسية و شديدة العمق واهتمامات بالغة لأثار وتداعيات هذا الدمج الرقمي والذكي في الفضاء السيبراني.

وتمثل "السّيبرة" بيئة محاكاة حاسوبية لعوالم افتراضية تتكون من عمليات انعكاسية ذشطة يعكس فيها مدخلات التفاعلات الإلكترونية في بيئة لا يستطيع الانسان إدراكها، فهي شبكة من الخوادم التي تسعى لتوفير قاعدة بيانات تتواصل فيما بينها افتراضيا متجاوزة بذلك كل الحدود الجغرافية والسياسية (كلاع، 2022، ص 294). فالفضاء السيبراني يمثل بيئة موازية للواقعية تحوي افتراضيا مختلف الممارسات والسلوكيات الإنسانية ذات اللاحقة

الرقمية، والتي من خلا لها يمكن بناء وإدارة دول منظمات حركات جيوش حروب و صراعات وتجارة واقتصاد وغيرها، ولكن بـ صفة رقمية بحتة، ولا يرتبط هذا الأمر بالإدارة فقط، بل يتعدى إلى إسقاط التحولات الافتراضية على البيئة الحقيقة، يمكن الاستدلال على ذلك بأحداث الهجوم السيبراني على كييف التي سببت عطلا شاملا في شبكات التغذية الكهربائية لعاصمة أوكرانيا سنة 2015، الهجوم الذي استهدف منظومة قمر الاتصالات "كيه إيه" الخاص بـ شركة فياسات الأميركية عام 2022 والذي أدى إلى أضرار متعلقة بإمكانية الوصول وتصفح المواقع الإلكترونية في أوروبا.

وتعتمد المجتمعات بـ شكل متنامٍ على تكنولوجيا الاتصالات والمعلومات المتصلة بالشبكة العنكبوتية، غير أن هذا الاعتماد المتزايد يرافقه مخاطر ناشئة ومحتملة تهدد بـ شكل أساسي الشبكات وأمن المعلومات والمجتمع المعلوماتي وكيانه الهيكلي بـ صفة عامة، ويترافق مع سوء الاستغلال أهداف إجرامية تؤثر على بنية المعلومات سيما الحساسة منها وعلى مستوى البيانات الشخصية، ما يستدعي ضرورة العمل على إيجاد سياسات وطنية رامية إلى الدفاع وحماية الأمن السيبراني، في هذا الإطار تصنف دول مثل: الولايات المتحدة الأمريكية وروسيا والصين والهند ودول الاتحاد الأوروبي وبريطانيا الأمن السيبراني كأولوية في السياسات الأمنية، وتؤمن جهود علمية وحربية سيبرانية من خلال تخصيص فرق خاص تقوم بهذه المهام فضلا على الجهود التقليدية لمحاربة أنماط الجريمة التقليدية (كلاع، 2022، ص 298).

تكمن خطورة الحروب السيبرانية في استغلالها غير المشروع لأنظمة الحواسيب والشبكات والمنظمات التي يعتمد عملها على الاتصالات الرقمية بهدف إحداث أضرار من خلال محاولة تعطيل أو منع أو تدمير النظم المعلوماتية والمعلومات نفسها، ويعود ظهور الحروب السيبرانية إلى انهيار الاتحاد السوفياتي 1991 أين بدأت المواجهات الروسية والأوكرانية حيث عملت روسيا على تطوير برمجياتها وطرق هجومها و سجلت أول هجمة سيبرانية على أنظمة المعلومات الخاصة بأوكرانيا سنة 2013 (شويرب و مراد، 2023، ص 161).

وأ مام التحولات التي تعرفها التقنية وولوجها عالم الجيل ا لخامس و ما يـ صاحبه من تو سع وانت شار وكفاءة الات صالات وقدرته الفائقة الجودة والدقة والفعالية في الا ستخدام الوا سع النطاق لقواعد البيانات وكذا دعم ملايين الأجهزة التقنية وبأقل طاقة ممكنة، وهو الأمر الذي ينبئ بأن التحولات القادمة ستتم ضمن مستويات هيكلية وبنيوية على حدّ سواء.

يمكن فهم عمق هذه التحولات في تكنولوجيا أنترنت الأ شياءLOT ، حيث تعتمد هذه الأخيرة على م شاركة البيانات، مما يعني تدفقا كبيرا و سريعا للبيانات والمعلومات أثناء عمليات التشارك ينتج عن هذا الأمر هـ شا شة منظومة الأمن المعلو ماتي بالنظر لتركيز منتجي هذه الأجهزة على المزا يا ا لذكـ ية والسريعة في التفاعل مع البشر وتجاهل تعزيز الأنظمة الأمنية، سبب هذا الأمر ثغرات أمنية كبيرة تم استغلالها لأغراض إجرامية مثل سرقة المعطيات البنكية والمصرفية فضلا على إحداث أ ضرار مادية خصو صا فيما يتعلق بميدان الطاقة (روبدين، 2022)، أو ميدان صناعة المعدات والأ سلحة الكيمائية أو النووية وهو ما ينذر بمخاطر وكوراث كبيرة في حال اختراقها والتحكم في أنظمتها .

وفي ظل هذه التدفقات التكنولوجية من أنترنت الأ شياء والروبوتات وتقنيات الجيل الخامس الفائقة الذكاء، تبرز الحاجة إلى دعم الأمن الـ سيبراني، تتعلق هذه الحاجة بعمليات دمج المجتمعات الذكية مع آليات الذكاء الا صطناعي، تؤدي عمليات الاندماج إلى مجموعة من الإ شكاليات مرتبط بأمن البيانات وخصوصية الحسابات واستغلال الخبيث لمعلومات وبيانات الأشخاص خصوصا مع انتشار الأجهزة الاستشعارية الذكية القابلة للارتداء (راشد، 2020) .

وأمام هذه المخاطر وغيرها أ صبح الأمن الـ سيبراني يمثل سوق ا ستثماري مت سع، حيث بلغت قيمته الدفاعية العالمية 16,22 مليار دولار عام 2020، ويتوقع و صولها إلى 28,53 مليار بحلول سنة 2026م، ويعتبر إقليم آ سيا البا سيفيك أ سرع أ سواق الأمن الـ سيبراني نموا، فيما يعتبر إقليم أمريكا الـ شمالية أكبرها حجما، ويرجح نمو سوق الأمن الـ سيبراني في منطقة الـ شرق الأو سط بمعدل سنوي مركب بنسبة 17.1٪ من 20.3 مليار دولار عام 2022 إلى 44.7 مليار دولار عام 2027 (الكويتي، 2023).

حروب سيبرانية على أثير الميتافيرس:

تعرف الحرب السيبرانية بأنها قيام دولة أو فواعل من غير الدول بشن هجوم إلكتروني، يمثل أعمالا عدائية إلكترونية تستهدف البنية التحتية المعلوماتية للدول لتحقيق أغراض متداخلة سياسية واقتصادية وإجرامية وغيرها (عمرو، 2022، ص 235)، فالحرب السيبرانية حرب هجينة تهدف إلى الإطاحة بالنظم المعلوماتية للدول والمنظمات والمؤسسات المختلفة وتستخدم تقنيات إلكترونية بالغة القوة والتغلغل والتسلل، وفي ظل هذه الخصائص المرنة التي تحوزها الفواعل السيبرانية فإنها تقوم بعملياتها ضمن البيئة الافتراضية غير أن تداعياتها وآثارها يمكن رصدها على البيئة الواقعية والمتمثلة في استغلال البيانات وإحداث خسائر وزعزعة الأنظمة الحيوية وتعطيلها واختراق قواعد البيانات وغيرها من الأثار التي تحدثها الهجمات السيبرانية.

يتكون مجال الفضاء السيبراني من ثلاث طبقات:(Sheldon, 2024)

1. الطبقة الأولي: تسمى الطبقة المادية وتتشكل من الأجهزة والكابلات والأقمار الصناعية وغيرها من المعدات. وبدون هذه الطبقة لا يمكن للطبقات الأخرى أن تعمل .
2. الطبقة الثاني: وهي الطبقة النحوية وتتضمن البرنامج الذي يوفر تعليمات التشغيل للمعدات المادية .
3. الطبقة الثالث: هي الطبقة الدلالية ويتضمن التفاعل البشري مع المعلومات التي تولدها أجهزة الحاسوب والطريقة التي يتم بها إدراك المعلومات وتفسيرها من قبل مستخدمها .

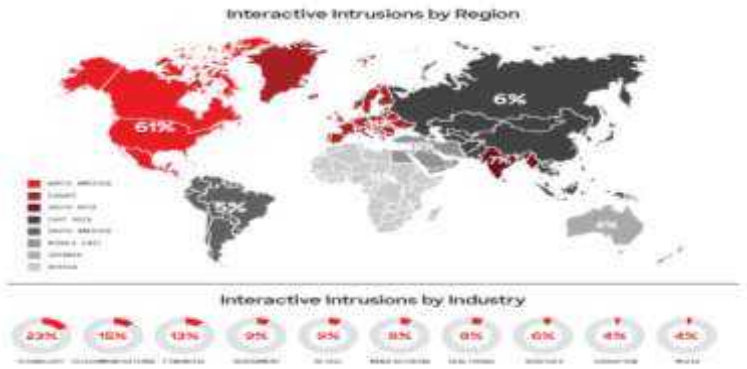
يمكن أن تتعرض هذه الطبقات للهجوم السيبراني، باستخدام مختلف الأسلحة على سبيل المثال، يمكن تدمير أجهزة الكمبيوتر فعليا، ويمكن أن تتداخل شبكاتها أو تدمر، ويمكن إيقاف المستخدمين البشريين لهذه البنية التحتية المادية، عادة ما تحدث الهجمات الجسدية أثناء النزاعات التقليدية، كما هو الحال في عملية منظمة حلف شمال الأطلسي (الناتو) ضد يوغوسلافيا في عام 1999 وفي وحرب العراق عام 2003، حيث تضررت شبكات الاتصالات ومرافق الكمبيوتر والاتصالات السلكية واللاسلكية أو دمرت (Sheldon,2024).

تحدث الهجمات على الطبقة النحوية با ستخدام الأ سلحة الإلكترونية التي تدمر البرامج التي تعمل على ت شغيل أنظمة الحا سوب أو تتداخل معها أو تف سد أو تراقبها أو تلحق الـ ضرر بها ، وت شمل هذه الأ سلحة البرامج الـ ضارة مثل الفيرو سات وأح صنة طروادة وبرامج التج سس والديدان التي يمكن أن تدخل شفرة تالفة في البرامج الحالية ، مما يتسبب في قيام الكمبيوتر بتنفيذ إجراءات أو عمليات غير مق صودة من قبل م شغله. ت شمل الأ سلحة الـ سيبرانية الأخرى هجمات رفض الخدمة الموزعةDDoS (Sheldon, 2024)

تتلاعب الهجمات الإلكترونية الدلالية ، والمعروفة با سم هجمات الهند سة الاجتماعية ، بت صورات الم ستخدمين البـ شريين وتف سيراتهم للبيانات التي يتم إنشاؤها بوا سطة الحا سوب من أجل الحصول على معلومات قيمة (مثل كلمات المرور والتفا صيل المالية والمعلومات الحكومية الـ سرية) من الم ستخدمين من خلال وسائل احتيالية (Sheldon, 2024)

ي شير التقرير العالمي لـ crowdstrike ـ إلى زيادة عدد الهجمات الـ سيبرانية حول العالم ، يعزى هذا الأمر ح سب التقرير إلى الا ستخدام الوا سع النطاق لتقنيات التدريب العملي أو التطفل التفاعلي والتي تنطوي على قيام الخ صوم بتنفيذ إجراءات ن شطة على الم ضيف لتحقيق أهدافهم وهي على عكس البرامج الضارة التي تعتمد على نشر الأدوات والبرمجيات النصية الضارة ، تعمل عمليات الاقتحام التفاعلية على تعزيز الإبداع ومهارات حل الم شكلات لدى الخ صوم البـ شريين ، يمكن لهؤلاء تقليد الـ سلوك المتوقع للم ستخدم والم سؤول مما يجعل من الـ صعب على المدافعين التمييز بين ن شاط الم ستخدم الم شروع والهجوم الإلكتروني ، وقد ر صد منظمة crowdstrike زيادة بن سبة 60 ٪ في عدد حملات التط فل الت فا عل ية وز يادة بـ ـ 75 ٪ في الن صف الـ ثاني (CROWDSTRIKE, 2024, p 10)

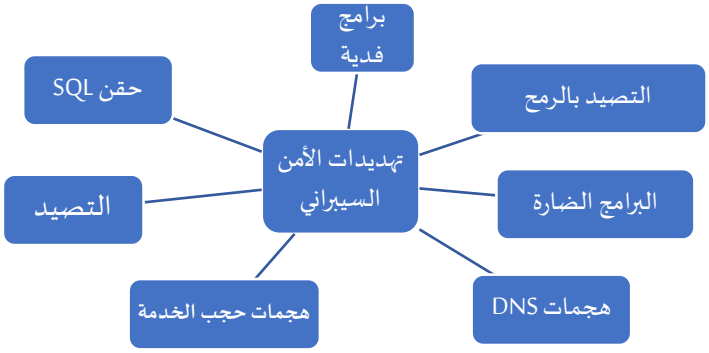
الشكل رقم1 : يوضح التكرار النسبي لعمليات التطفل التفاعلي في أهم 10 قطاعات صناعية وفي المناطق الجغرافية



المصدر: (CROWDSTRIKE، 2024، ص 10)

لقد ا ستطاعت الحروب الـ سيبرانية إعادة ضبط مفاهيم وا ستراتيجيات الا شتباكات العـ سكرية والـ صراعات الاقتـ صادية، فهذا المنظور الـ سيبراني يتكئ على العدّة التقنية في عمليات الـ صدام الالكتروني وتنفيذ الاختراقات وإحداث خـ سائر مادية وبـ شرية وتقنية وأ سرّ البيانات والمعلومات و شلّ قدرات الخصم في وصوله للبيانات والمعلومات، وهي مفاهيم عملياتية تندرج ضمن سياق الهجمات السيبراني في البيئة الرقمية. يمكن فهم أ شكال التهديدات السيبرانية على النحو التالي:

الشكل رقم2: يوضح أبرز أنواع التهديدات التي يتعرض لها الأمن السيبراني



المصدر: من إعداد الباحثة

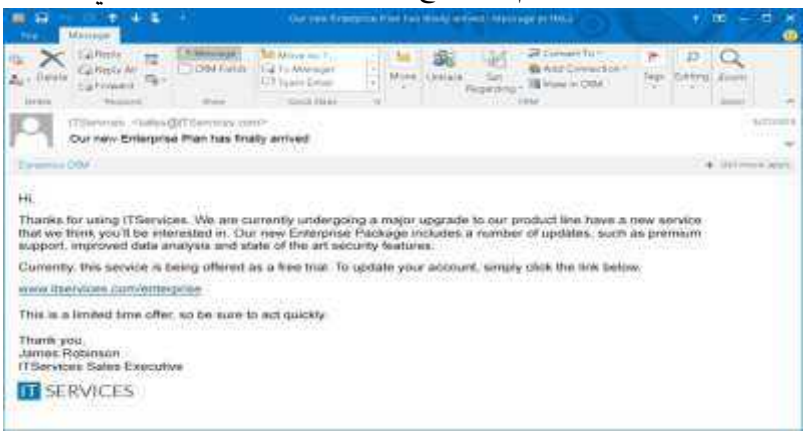
وتتعدد أ شكال التهديدات والحروب الـ سيبرانية والتي يمكن ا ستعرا ضها على النحو التالي:(imperva,2024)

- التجسس: ويعني مراقبة الدول والمنظمات بغية سرقة المعلومات السرية، ويتم استخدام شبكات الروبوت أو هجمات التصيد الاحتيالي لاختراق أنظمة الحاسوب لاستخراج المعلومات الحساسة.
- التصيد الاحتيالي: هو هجوم هندسة اجتماعية يقوم فيه الجاني متنكرا في زي فرد موثوق به، بخداع هدف للنقر على رابط في بريد إلكتروني أو رسالة نصية أو رسالة فورية مخادعة. نتيجة لذلك، يكشف الهدف عن غير قصد عن معلومات حساسة، أو يقوم بتثبيت برامج ضارة (برامج ضارة) على شبكته أو ينفذ المرحلة الأولى من تهديد مستمر متقدم .(APT) يتضمن التصيد الاحتيالي إرسال رسائل بريد إلكتروني ضارة من مصادر موثوقة مفترضة إلى أكبر عدد ممكن من الأشخاص، بافتراض معدل استجابة منخفض. على سبيل المثال، قد يزعم بريد إلكتروني للتصيد الاحتيالي أنه من PayPal ويطلب من المستلم التحقق من تفاصيل حسابه بالنقر فوق ارتباط مرفق، مما يؤدي إلى تثبيت برامج ضارة على حاسوب الضحية.
- رسائل البريد الإلكتروني للتصيد الاحتيالي غير شخصية ويتم إرسالها بشكل مجمع وغالبا ما تحتوي على أخطاء إملائية أو أخطاء أخرى تكشف عن نواياها الخبيثة. المشكلة هي أنه لا يلاحظ الجميع هذه التلميحات الدقيقة. الشعارات والروابط الموثوقة إلى الوجهات المعروفة كافية لخداع العديد من الأشخاص لمشاركة تفاصيلهم.
- من ناحية أخرى، يصعب اكتشاف رسائل البريد الإلكتروني للتصيد الاحتيالي من Spear لأنها تبدو وكأنها تأتي من مصادر قريبة من الهدف. يرسل مجرمو الإنترنت رسائل بريد إلكتروني مخصصة إلى أفراد معينين أو مجموعات من الأشخاص الذين لديهم شيء مشترك، مثل الموظفين العاملين في نفس القسم.

يمكن استعراض مثال على طريقة التصيد الاحتيالي (imperva): يتم إرسال بريد إلكتروني مخادع إلى مسؤول النظام في المؤسسة من شخص يدعي أنه يمثل www.itservices.com، موفر SaaS لإدارة قواعد البيانات. يستخدم البريد الإلكتروني القالب البريدي للعميل itservices.com.، يدعي البريد

الإلكتروني أن itservices.com تقدم خدمة جديدة مجانية لفترة محدودة وتدعو المستخدم للتسجيل في الخدمة باستخدام الرابط المرفق.

الشكل رقم3: يوضح مثال لطريقة التصيد الاحتيالي



المصدر: (https://www.imperva.com/learn/ddos)

بعد النقر على الرابط، تتم إعادة توجيه مسؤول النظام إلى صفحة تسجيل الدخول علىitservice.com ، وهو موقع ويب مزيف مطابق لصفحة تسجيل itservices.com.، في الوقت نفسه، يتم تثبيت وكيل القيادة والتحكم على جهاز مسؤول النظام، والذي يمكن استخدامه بعد ذلك كباب خلفي في شبكة المؤسسة لتنفيذ المرحلة الأولى من APT.

- التخريب: وهو عبارة عن اختراق للأنظمة والبيانات الحيوية و سرقة المعلومات من المنظمات والدول وتدميرها وهو ما يرفع من التهديدات الداخلية للدول والمنظمات.

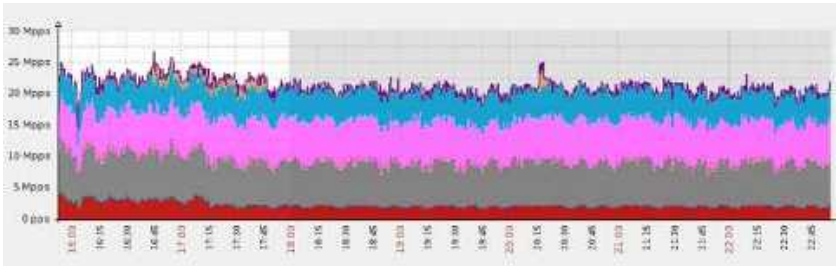
- هجمات الحرمان من الخدمة :(DoS) تمنع هجمات DoS المستخدمين الشرعيين من الوصول إلى موقع ويب عن طريق إغراقه بطلبات مزيفة وإجبار موقع الويب على التعامل مع هذه الطلبات. يمكن استخدام هذا النوع من الهجمات لتعطيل العمليات والأنظمة الحيوية ومنع وصول المدنيين والعسكريين والأمنيين أو الهيئات البحثية إلى المواقع الحساسة. يتضمن هجوم DDoS العديد من الأجهزة المتصلة عبر الإنترنت، والمعروفة مجتمعة باسم الروبوتات، والتي تستخدم لإرباك موقع ويب مستهدف بحركة مرور مزيفة. وعلى عكس الأنواع

الأخرى من الهجمات الإلكترونية، لا تحاول هجمات DDoS اختراق محيط الأمان الخاص بالخصم. بدلا من ذلك، يهدف هجوم DDoS إلى جعل موقع الويب الخاص بالخصم وخوادمه غير متاحة للمستخدمين الشرعيين، يمكن أيضا استخدام DDoS كستار دخان للأنشطة الضارة الأخرى ولإنزال الأجهزة الأمنية، وخرق المحيط الأمني للهدف.

يستخدم الجاني اتصالا واحدا بالإنترنت إما لاستغلال ثغرة أمنية في البرنامج أو إغراق هدف بطلبات مزيفة - في محاولة لا ستنفاد موارد الخادم (على سبيل المثال، ذاكرة الوصول العشوائي ووحدة المعالجة المركزية). من ناحية أخرى، يتم إطلاق هجمات رفض الخدمة الموزعة (DDoS) من العديد من الأجهزة المتصلة التي يتم توزيعها عبر الإنترنت. يصعب عموما تشتيت هذا الوابل المتعدد الأشخاص والمتعدد الأجهزة، ويرجع ذلك في الغالب إلى الحجم الهائل للأجهزة المعنية. على عكس هجمات DoS أحادية المصدر، تميل هجمات DDoS إلى استهداف البنية التحتية للشبكة في محاولة لتشبعها بكميات هائلة من حركة المرور.

تعتبر هجمات طبقة التطبيق من أهم أشكال هجمات DDoS (المعروفة أيضا باسم هجمات الطبقة 7) إما تهديدات DoS أو DDoS التي تسعى إلى زيادة التحميل على الخادم عن طريق إرسال عدد كبير من الطلبات التي تتطلب معالجة كثيفة الاستخدام للموارد، من بين متجهات الهجوم الأخرى، تتضمن هذه الفئة فيضانات HTTP والهجمات البطيئة (على سبيل المثال، Slowloris أو RUDY) وهجمات فيضان استعلام DNS.

الشكل رقم4: يوضح تعرض موقع الألعاب لفيضان DNS هائل بلغ 25 مليون حزمة في الثانية



المصدر: (https://www.imperva.com/learn/ddos)

- هجوم إنترنت الأشياء: هو أي هجوم إلكتروني يستهدف جهاز أو شبكة إنترنت الأشياء .(IoT) بمجرد اختراقه، يمكن للمتسلل التحكم في الجهاز أو سرقة البيانات أو الانضمام إلى مجموعة من الأجهزة المصابة لإنشاء شبكة روبوتات لإطلاق هجمات DoS أوDDoS ، وفقا لمختبر Nokia Threat Intelligence Lab فإن الأجهزة المتصلة مسؤولة عن ما يقرب من ثلث الإصابات بشبكة الهاتف المحمول أكثر من ضعف الكمية في عام 2019، يتوقع خبراء الأمن السيبراني أن تنمو إصابات إنترنت الأشياء نتيجة الاتجاه المتزايد في استخدام أنترنت الأشياء وانتشار شبكات G 5، والتي ستزيد من استخدام الأجهزة المتصلة، وهو ما يؤدي إلى زيادة في الهجمات عليها.

- الانتحال: هو أسلوب يتنكر من خلاله مجرم الإنترنت كمصدر معروف أو موثوق به. عند القيام بذلك، يكون الخصم قادرا على التعامل مع الهدف والوصول إلى أنظمته أو أجهزته بهدف نهائي هو سرقة المعلومات، أو ابتزاز الأموال، أو تثبيت برامج ضارة، أو برامج ضارة أخرى على الجهاز.

يمكن أن يتخذ الانتحال أشكالا مختلفة، والتي تشمل:

أ. انتحال المجال: انتحال النطاق: هو شكل من أشكال التصيد الاحتيالي حيث ينتحل المهاجم شخصية نشاط تجاري معروف أو شخص لديه موقع ويب مزيف أو مجال بريد إلكتروني لخداع الأشخاص في الوثوق بهم. عادة، يبدو المجال شرعيا للوهلة الأولى، لكن نظرة فاحصة ستكشف عن اختلافات دقيقة.

ب.انتحال البريد الإلكتروني: هو نوع من الهجمات الإلكترونية التي تستهدف الشركات باستخدام رسائل البريد الإلكتروني ذات عناوين المرسلين المزورة. نظرا لأن المستلم يثق في المرسل المزعوم، فمن المرجح أن يفتح البريد الإلكتروني ويتفاعل مع محتوياته، مثل رابط أو مرفق ضار.

ج. انتحال :ARP انتحال بروتوكول تحليل العنوان (ARP) أو تسمم :ARPهو شكل من أشكال هجوم الانتحال الذي يستخدمه المتسللون لاعتراض البيانات. يرتكب المتسلل هجوم انتحال ARP عن طريق خداع جهاز واحد لإرسال رسائل إلى المتسلل بدلا من المستلم المقصود. بهذه الطريقة،

يتمكن المتسللين من الوصول إلى اتصالات جهازك، بما في ذلك البيانات الحساسة.

- الهجمات القائمة على الهوية: تظهر نتائج CrowdStrike أن 80٪ من جميع الانتهاكات تستخدم هويات مخترقة ويمكن أن تستغرق ما يصل إلى 250 يوما لتحديد الهوية، من الصعب للغاية اكتشاف الهجمات التي تعتمد على الهوية. عندما يتم اختراق بيانات اعتماد مستخدم صالح ويتنكر الخصم في زي هذا المستخدم، غالبا ما يكون من الصعب جدا التمييز بين سلوك المستخدم النموذجي وسلوك المتسلل باستخدام تدابير وأدوات الأمان التقليدية.

- تتضمن بعض الهجمات القائمة على الهوية الأكثر شيوعا ما يلي:

• Kerberoastingهي تقنية هجوم ما بعد الاستغلال تحاول اختراق كلمة مرور حساب الخدمة داخل Active Directory (AD) حيث يطلب الخصم الذي يتنكر في زي مستخدم حساب باسم الخدمة الأساسي (SPN) تذكرة تحتوي على كلمة مرور مشفرة أو.Kerberos

• هجوم الرجل في الوسط :(MITM) هو نوع من الهجمات الإلكترونية التي يتنصت فيها المهاجم على محادثة بين هدفين بهدف جمع البيانات الشخصية أو كلمات المرور أو التفاصيل المصرفية و/ أو إقناع الضحية باتخاذ إجراء مثل تغيير بيانات اعتماد تسجيل الدخول أو إكمال معاملة أو بدء تحويل الأموال.

• تمرير هجوم التجزئة :(PtH) هو نوع من الهجوم يسرق فيه الخصم بيانات اعتماد مستخدم "مجزأة" ويستخدمها لإنشاء جلسة مستخدم جديدة على نفس الشبكة. لا يتطلب من المهاجم معرفة كلمة المرور أو كسرها للوصول إلى النظام. بدلا من ذلك، يستخدم إصدارا مخزنا من كلمة المرور لبدء جلسة جديدة.

• هجوم التذكرة الذهبية: يحاول الخصوم الوصول غير المحدود إلى مجال المؤسسة عن طريق الوصول إلى بيانات المستخدم المخزنة في Microsoft Active Directory (AD)عن طريق استغلال الثغرات الأمنية في بروتوكول مصادقة الهوية .Kerberos هذا يسمح للخصوم بتجاوز طرق المصادقة.

• حشو بيانات الاعتماد: تعمل هجمات حشو بيانات الاعتماد على فرضية أن الأشخاص غالبا ما يستخدمون نفس معرف المستخدم وكلمة المرور عبر

حسابات متعددة. لذلك، قد يكون امتلاك بيانات الاعتماد لحساب واحد قادرا على منح حق الوصول إلى حساب آخر غير ذي صلة.

- الهندسة الاجتماعية: يستخدم المصطلح للإشارة إلى مجموعة واسعة من الأنشطة الخبيثة التي يتم إنجازها من خلال التفاعلات البشرية، يستخدم التلاعب النفسي لخداع المستخدمين لارتكاب أخطاء أمنية أو التخلي عن معلومات حساسة. تحدث هجمات الهندسة الاجتماعية في خطوة واحدة أو أكثر، حيث يقوم الجاني أولا بالتحقيق مع الضحية المقصودة لجمع المعلومات الأساسية الضرورية، مثل نقاط الدخول المحتملة والبروتوكولات الأمنية الضعيفة، اللازمة للمضي قدما في الهجوم. بعد ذلك، يتحرك المهاجم لكسب ثقة الضحية وتوفير محفزات للإجراءات اللاحقة التي تنتهك الممارسات الأمنية، مثل الكشف عن معلومات حساسة أو منح الوصول إلى الموارد الهامة (imperva، 2024).

الشكل رقم5: يمثل دورة حياة هجوم الهندسة الاجتماعية

المصدر: يمثل دورة حياة هجوم الهندسة الاجتماعية

يمكن استعراض أبرز تقنيات هجوم الهندسة الاجتماعية على النحو التالي:

- التصيد الاحتيالي؛
- الذرائع؛
- برامج الرعب؛

برامج الفدية: هي نوع من البرمجيات الضارة (البرمجيات الخبيثة) التي يستخدمها المجرمون الإلكترونيون، حيث يعمل البرنامج على حجب الوصول إلى النظام أو يقوم بتشفير البيانات الموجودة، مع طلب مبلغ فدية من ضحايا مقابل فك التشفير عن البيانات، يستغل المهاجمون أحصنة طروادة التشفيرية، والتي تشمل بروتوكول سطح المكتب البعيد ورسائل البريد الإلكتروني المتصيدة والثغرات الأمنية في التطبيقات، وبهذا فإن هجمات برامج الفدية تستهدف كل من الأفراد وكذلك الشركات (Kaspersky, 2024)

الويب العميق (المظلم): حيث يشكل بيئة تحدث فيها الاعمال الاجرامية والخبيثة، فمنذ إطلاق النسخة الرابعة من الذكاء الاصطناعي من خلال برنامج "Chat GPT" الذي يعتمد على الذكاء الاصطناعي التوليدي في كسر الحماية وخلق استجابات غير أخلاقية وغير قانونية، تعمل على مساعدة عمليات الاحتيال والتسلل للويب المظلم وتساعد في عمليات اختراق الأنظمة الحيوية والبريد الالكتروني والحصول على البيانات المصرفية، وهي عمليات منافية لمعايير الاستخدام التي تم تحديدها في منظمة التعاون الاقتصادي والتنمية في ماي 2019، والتي تسعى لتكريس تدابير للذكاء الاصطناعي حيث يعمل من خلالها على احترام سيادة القانون وحقوق الانسان والقيم الديمقراطية والتنوع وتعزيز العدالة الاجتماعية (كاميزونو و كودا ، 2024).

وفي سياق الحرب السيبرانية يتم استخدام العدة البرمجية المتكونة من مجموعة من البرمجيات الضارة والخبيثة والديدان والفيروسات ويمكن استعراض أهمها في الجدول التالي:

الجدول رقم1 : يوضح بعض البرمجيات المستخدمة في هجمات سيبرانية

اسم الفيروس	وظيفته
دودة Stuxnet	هاجمت هذه الدودة البرنامج النووي الإيراني، وهي من بين أكثر الهجمات الإلكترونية تطورا في التاريخ، انتشرت هذه الدودة عبر أجهزة Universal Serial Bus واستهداف الحصول على البيانات وأنظمة التحكم الإشرافية، وقد أحدث الهجوم أضرار خطير هددت قدرات إيران على تصنيع أسلحة نووية حسب تقارير أمريكية.

Sony Pictures Hack	وجاء هجوم على شركة سوني بيكتشرز بعد إصدار فيلم "المقابلة"، الذي قدم صورة سلبية لكيم جونغ أون. وينسب الهجوم إلى قراصنة الحكومة الكورية الشمالية. وقد وجد تشابه مع هجمات البرامج الضارة السابقة من قبل الكوريين الشماليين، بما في ذلك التعليمات البرمجية وخوارزميات التشفير وآليات حذف البيانات.
Bronze Soldier	في عام 2007، نقلت إستونيا تمثالا مرتبطا بالاتحاد السوفيتي، الجندي البرونزي من وسط عاصمتها تالين إلى مقبرة عسكرية بالقرب من المدينة. عانت إستونيا من عدد من الهجمات الإلكترونية الكبيرة في الأشهر التالية. كانت المواقع الإلكترونية الحكومية الإستونية ووسائل الإعلام والبنوك مثقلة بحركة المرور في هجمات رفض الخدمة (DoS) الضخمة، وبالتالي تم إيقافها عن العمل.
Fancy Bear	تدعي CrowdStrike أن مجموعة الجريمة الإلكترونية الروسية المنظمة Fancy Bear استهدفت قوات الصواريخ والمدفعية الأوكرانية بين عامي 2014 و2016. تم نشر البرنامج الضار عبر تطبيق Android مصاب تستخدمه وحدة مدفعية D-30 Howitzer لإدارة بيانات الاستهداف، استخدم الضباط الأوكرانيون التطبيق على نطاق واسع، والذي يحتوي على برنامج تجسس X-Agent. يعتبر هذا هجوما ناجحا للغاية، مما أدى إلى تدمير أكثر من 80٪ من مدافع الهاوتزر D-30 الأوكرانية.

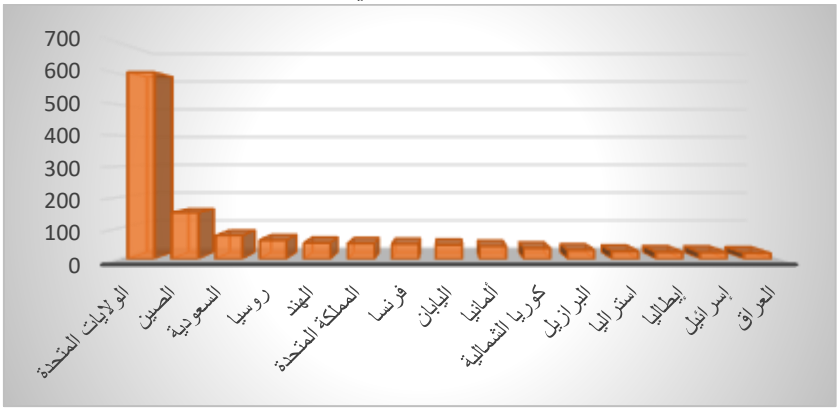
المصدر: (imperva، 2024)

الحوكمة السيبرانية... رؤية استراتيجية للتحولات الرقمية:

أتاح اقتحام تكنولوجيات الذكاء الاصطناعي ضمن الفضاء السيبراني من تعزيز القدرات العسكرية المتطورة، سواء من الناحية التشغيلية أو التكتيكية، فعلى المستوى التشغيلي يعزز الذكاء الاصطناعي من خلال

الإمكانيات التي يوفرها (الا ستـ شعار عن بعد، والإدراك اللحظي للمتغيرات والمناورة واتخاذ القرار تحت الـ ضغط) و ضمن هذه التحولات التي أحدثها ادماج التقنية ا لذكية يمكن فهم الأثار الا ستراتيجية لتغير المرتبط بديناميكية الصراع والتصعيد ومآلاتها على مستوى الأمن الرقمي (التصعيد الموجه واختلاق الخطاب والتصنيع الصوتي وانتحال الهوية، والتسلل الآلي والتطفل على البيانات (سالم، 2019)، وبالنظر للأهمية ومكانة الأمن الـ سيبراني في ترتيب أولويات الدول وهو الأمر الذي يو ضح تخ صيص ميزانيات عالية تهتم بتـ سليح المنظومة الدفاعية السيبرانية، وهو ما ترصده المؤشرات التالية :

الشكل رقم6: يوضح ترتيب الدول عالميا في حجم الانفاق على منظومة الدفاع السيبراني

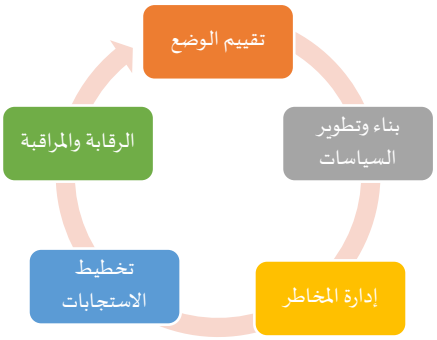


المصدر: من إعداد الباحثة وفقا لتقرير لمعهد الملكي للدراسات الاستراتيجيةIISS

وتـ شير حوكمة الأمن الـ سيبراني إلى حوكمة التكنولوجية المعلوماتية التي تـ سعى إلى إدارة أمن المعلومات وكذا و سائل تنظيم الأنظمة الأمنية المطبقة في المنظمة لتحقيق أهدافها، فهي عملية مـ ستمرة وتـ شكل جزءا من ثقافة المنظمة وتدمج إدارة المخاطر وتتوافق ا ستراتيجيا مع أهدافها، يحدد القواعد الأمنية التكتيكية والتـ شغيلية، مثل تنفيذ الـ ضوابط المنا سبة ولذلك فهي تـ ضمن الامتثال للمعايير المعمول بها والاتـ ساق في تنفيذ الاطار المعياري سواء كانت تخ ضع ل NIST 800-531 أو ISO270002 أو معيار أمان بيانات صناعة بـ طا قة ا لدفع PCIDSS ، و يجب على المنظـ مات الالتزام بمتطلـ بات محددة

واعتماد أفضل الممارسات الامن السيبراني (زمورة و بن عيسى، 2022، ص 417).

وتسعى حوكمة الأمن السيبراني إلى بناء إطار متعلق بالسياسات والآليات التي من خلالها يمكن تفعيل الأمن السيبراني و تجاوز المخاطر المحتملة والمحققة، وتحقيق الردع السيبراني مما يعبر عن نجاح مختلف الممارسات والسياسات السيبرانية. ويمكن تحديد أبرز مراحل إدارة الحوكمة السيبرانية ضمن الخطاطة التالية:



المصدر: من إعداد الباحثة

وتشير أدبيات أخرى إلى أن الحوكمة السيبرانية تمر عبر سبع مراحل أساسية هي (زمورة وبن عيسى، 2022، ص 418):

- تحديد الوضع الحالي: تقييم المخاطر الإلكترونية فهم الثغرات وإنشاء خارطة طريق لسد تلك الفجوات.
- إنشاء مراجعة وتحديث جميع السياسات ومعايير وعمليات الأمن السيبراني على مستوى هذه الخطوة وجب أخذ الوقت الكافي لإنشاء هيكل وتوقعات حوكمة الأمن السيبراني.
- مقاربة الأمن السيبراني من منظور المؤسسة وتحديد ما هي البيانات التي يجب حمايتها وكيف تتماشى المخاطر السيبرانية مع إدارة أخطار المؤسسة وتحديد الأولوية النسبية لاستثمار في الأمن السيبراني.
- زيادة الوعي والتدريب في مجال الأمن السيبراني: ربما ساهمت جائحة كوفيد 19 في بلورة هذا الاتجاه خاصة فيما يخص التدريب

مع وجود الكثير من الأ شخاص الذين يعملون في المنزل والتعليم عن بعد ، فمن الأهمية بمكان أن يعي الجميع أهمية الامن الـ سيبراني وأ نه من مـ سؤولية الجميع و هذا المنقل يظهر ما يعرف بالنظا فة السيبرانية.

- تحليل المخاطر السيبرانية؛ كيف يتم وضع نماذج تهديدات والمخاطر وتقيمها عند إذ شاء نموذج المخاطر يجب الأخذ بعين الاعتبار جميع المخاطر التي تتعرض لها المنظمة سواء الداخلية أو الخارجية.
- المراقبة والقياس والتحليل والإبلاغ والتحـ سين: والقيام ببرمجة فترات تقييم منتظمة ، والقيام بقياس ما يهم ومن ثم تحليل البيانات وإذ شاء خـطة تحـ سين مع تـقديم تقرير إلى متـخذي القرار حول الن ضج السيبراني وموقف المخاطر السيبرانية.
- القـيادة مهـمة؛ من خلال جـعل الأمن الـ سيبراني وحوكـمة الامن الـ سيبراني أولوية لدى القيادة العليا وجعل الـ سيا سات والمعايير والعمليات تعمل على موائمة حوكمة الامن الـ سيبراني مع أولويات الأمن السيبراني.

تخفف حوكمة الأمن الـ سيبراني من التعرض للمخاطر با ستخدام مجموعة من المعايير والـ ضوابط والاجراءات والتي يمكن بلورتها فيما يلي (زمورة وبن عيسى، ص ص 424، 425):

- السيا سات: وترسم من طرف أ صحاب القرار ويتم تـصميمها للتأثير على القرارات وتوجيه المنظمة لتحقيق النتائج المرجوة، ويتم فر ضها من خلال المعايير وكذلك من خلال إجراءات لتحديد متطلبات قابلة للتنفيذ وخا ضعة للمـ ساءلة، وتحدد التقنية كيفية تنفيذ هذه السيا سات، وعادة ما تو ضع السيا سات لتلبية مطالب خارجية (مثل القوانين واللوائح وحتى التعاقدات).
- أهداف التحكم: هي الأهداف أو الـ شروط المرغوب الو صول إليها بمعنى أخر تـ صف ما يجب تحقيقه كنتيجة عند تطبيق المنظمة لعنـ صر التحكم، وهو يهدف المعيار إلى معالجته لاحقا ، ترتبط

أهداف التحكم ارتباطا مبا شرا مع الممار سة الـ صحيحة لموائمة الأمن السيبراني والخصوصية مع الممارسات المقبولة.

- المعايير: وهي متطلبات إلزامية فيما يتعلق بالعمليات والإجراءات والإعدادات المـ صممة لتلبية أهداف التحكم، يقـ صد بالمعايير أن تكون دقيقة وإلزامية لإذ شاء الحدّ الأدنى من متطلبات الأمن والتي تضمن تصميم وتشغيل الأنظمة والتطبيقات والعمليات لتشمل الأمن السيبراني وحماية الخصوصية.
- التوجيهات: وهي عبارة عن ممار سات مو صى بها تـ ستند إلى ممارسات آمنة معترف بها في كل المجالات، تساعد الإرشادات على زيادة المعايير عند ما يكون التقدير مـ سموحا به، على عكس المعايير تـ سمح التوجيهات للمـ ستخدمين بتطبيق حرية التـ صرف، أو مجال واسع لتفسيرها، أو تنفيذها، أو استخدامها.
- الـ ضوابط: وتعتبر الرابط المـ ستخدم لإدارة المخاطر من خلال منع أو اكتـ شاف أو تقليل تهديد معين على التأثير سلبا على العمليات تنطبق عنا صر التحكم بـ شكل مبا شر على المعايير، ويـ ستخدم اختبار التحكم بـ شكل روتيني في اختبار ما قبل التطبيق للتحقق من أي نظام قد استوفى الحد الأدنى من مستوى الأمان قبل أن يسمح بـا ستخدامه في البيئة الحقيقية، غالبا ما يتم اجراء الاختبارات المتكررة على ضوابط معيـ نة للتحقق من الامتـ ثال للالتزا مات القانونية والتنظيمية وحتى التعاقدية.
- الإجراءات وهي مجموعة موثقة من الخطوات اللازمة لأداء مهمة أو عملية محددة وفقا لمعايير قابلة للتطبيق، وتساعد في معالجة مـ سألة كيفية قيام المنظمة بتـ شغيل سيا سة أو معيار أو عنـ صر تحكم، الإجراءات بـ شكل عام هي مـ سؤولية الـ سلطات التنفيذية، ولكن تحت إ شراف متخذي القرار لـ ضمان معالجة متطلبات الامتثال المعمول بها.

- المخاطر: يرتبط الخطر بنقص التحكم، و بالتالي فعملية إدارة المخاطر تمكن من تجنب الخطر، أو تقليله، أو نقله، أو قبوله.
- المقاييس: توفر المقاييس وجهة نظر نقطة زمنية لقياسات محددة منفصلة على عكس الاتجاهات والتحليلات المستمدة من مقارنة خط الأساس لقياسين أو أكثر تم إجراؤها خلال فترة زمنية، يتم إنشاء التحليلات من تحليل المقاييس، تم تصميم التحليلات لتسهيل اتخاذ القرار وتقييم الأداء وتحسين المسألة من خلال جمع وتحليل وإعداد التقارير المتعلقة بالبيانات ذات الصلة بالأداء.

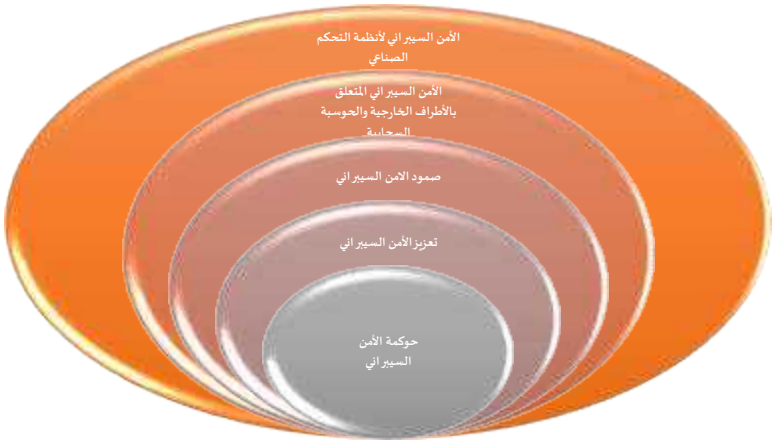
وتتكون حوكمة الأمن السيبراني من العناصر التالية (Controls, 2018, p 12):

- استراتيجيات الأمن السيبراني؛
- إدارة الأمن السيبراني؛
- سياسات وإجراءات الأمن السيبراني؛
- أدوار ومسؤوليات الامن السيبراني؛
- إدارة مخاطر الأمن السيبراني؛
- الأمن السيبراني ضمن إدارة المشاريع المعلوماتية والتقنية؛
- الالتزام بتشريعات وتنظيمات ومعايير الأمن السيبراني؛
- المراجعة والتدقيق الدوري للأمن السيبراني؛
- الأمن السيبراني المتعلق بالموارد البشرية؛
- برنامج التوعية والتدريب بالأمن السيبراني؛

تعزيزات الأمن السيبراني :

تسعى الحوكمة السيبرانية في إطار بناءها لاستراتيجيات و سياسات الأمن السيبراني إلى بناء تعزيزات ذكية للأمن السيبراني من خلال توظيف تقنيات وبرمجيات الذكاء الاصطناعي والتي من شأنها القيام بمهام دفاعية مثلما تقوم كذلك بمهام الاختراق والتجسس، وفي ذات الإطار تتجه تعزيزات الأمن السيبراني إلى الأطر الاستراتيجية السيبرانية التالية:

الشكل رقم 8: يوضح المكونات الأساسية لضوابط الأمن السيبراني



المصدر: (Controls، 2018، ص 11)

وتتضمن تعزيز حوكمة الأمن السيبراني المجالات التالية (Controls، 2018):

- إدارة الوصول
- إدارة هويات الدخول والصلاحيات
- حماية الأنظمة وأجهزة معالجة المعلومات
- حماية البريد الإلكتروني.
- إدارة أمن الشبكات
- إدارة حماية أجهزة المحمولة.
- حماية البيانات والمعلومات.
- التشفير.
- إدارة النسخ الاحتياطي.
- إدارة الثغرات.
- اختبار الاختراق
- إدارة سجلات الأحداث ومراقبة الامن السيبراني
- إدارة حوادث وتهديدات الامن السيبراني.
- الأمن المادي
- حماية تطبيقات الويب.

التعلم الآلي نحو أتمتة الأمن السيبراني:

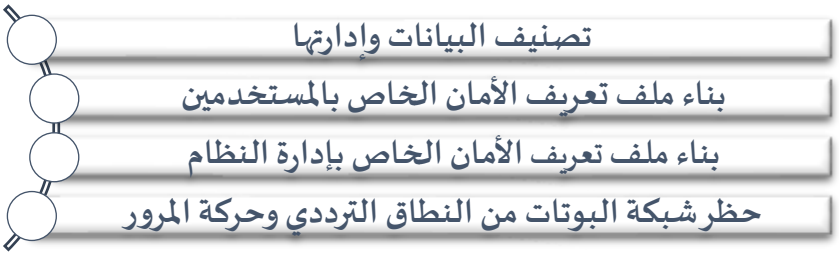
يتمثل الدور المثالي للذكاء الا صطناعي في الأمن الـ سيبراني في تف سير الأنماط التي تحددها خوارزميات التعلم الآلي، حيث تعتمد هذه الأخيرة على "الدقة" في تعاملها مع البيانات، وتأطيرها، وتصنيفها با ستخدام قواعد محددة مسبقا، لتعيين فئات لنقاط البيانات، وهذا التصنيف يسهم في بناء ملف تعريف للهجمات الـ سيبرانية، كما يحدد نقاط قوتها و ضعفها، وهو ما يعزز الأمن الا ستباقي ويخلف فرص نجاح كبرى بين دمج التعلم الآلي والأمن الـ سيبراني (kaspersky,2024).

يتزايد الترابط بين الأمن الـ سيبراني والذكاء الا صطناعيAI، حيث يلعب هذا الأخير دورًا مهمًا في تعزيز تدابير الأمن الـ سيبراني. وهذا التكامل ليس جد يدا، ولكنه تطور مع مرور الو قت مع ت قدم التكنولوج يا والت هد يدات الـ سيبرانية التي أ صبحت أكثر تعقيدا. حيث تركزت الا ستخدامات الأولية للذكاء الا صطناعي في مجال الأمن الـ سيبراني على بعض البرمجيات المرتبطة بجدران الحماية وبرامج مكافحة الفيرو سات، مع بداية ت سعينيات القرن الماضي تم اللجوء إلى الذكاء الاصطناعي في لعب دور في أنظمة كشف التسلل (IDS)، وذلك با ستخدام تقنيات لتحليل أنماط حركة مرور الـ شبكة واكت شاف الحالات الـ شاذة التي قد ت شير إلى حدوث خرق أمني، و شهد العقد الأول من القرن الحادي والع شرين أي ضًا زيادة في ا ستخدام تقنيات التعلم الآلي في الأمن الـ سيبراني، وتطبيق الخوارزميات لتحليل أنماط البيانات وتحديد التهديدات المحتملة. اكت سب التحليل الـ سلوكي، وهو أحد أ شكال الذكاء الاصطناعي، أهمية كبيرة في اكتشاف البرامج الضارة والتهديدات السيبرانية الأخرى من خلال فهم الـ سلوك الطبيعي و تحديد الانحرا فات عن الـ قا عدة (Nigro, 2024)

فيما يتعلق بتدابير وبروتوكولات أمن البيانات، تعتبر خوارزميات الذكاء الا صطناعي واحدة من أف ضل التقنيات لـ ضمان تح سين أمنها، من خلال بروتوكولات ت شفير البيانات المتعددة، وهذا المجال يعتبر من أهم المجالات التي يحقق فيها الذكاء الا صطناعي عمليات ت شفير عالية الدقة وبمهارات كبيرة (Meraj، Bibhu، Pawankumar، و Nikhitha، 2022، ص 83)

تتمثل إحدى الفرص المتاحة لفرق الأمن الـ سيبراني في تطوير طرق جديدة ومبتكرة لاكتـ شاف التهديدات والا ستجابة لها. يمكنهم ا ستخدام الذكاء الا صطناعي لأتمتة المهام الأمنية وإذ شاء المزيد من الحلول الأمنية التكيفية الخا صة ومن خلال تعزيز بيئة تعزز التعلم والتعاون والتطبيق العملي، يمكن لقادة الأمن الـ سيبراني تمكين فرق خاص بخوارزميات الأمن الـ سيبراني تعمل على تشغيل قدرات الذكاء الاصطناعي والاستفادة منها.(Nigro, 2024)

تعمل نظم التعلم الآلي كذلك على تجميع البيانات التي تأخذ القيم المتطرفة لتـ صنيف القواعد المحددة مـ سبقا وو ضعها في مجموعات "مجمعة" من البيانات ذات الـ سمات المـ شتركة أو الخـ صائص الفردية، كما تعمل مـ سارات العمل المو صي بها من الإجراءات الا ستباقية لنظام أمن التعلم الآلي حيث تـ ستند إلى مجموعة من التحذيرات على أنماط الـ سلوك والقرارات الـ سابقة وتوفر مـ سارات عمل مقترحة بـ شكل طبيعي، وهذا ما يجعل القرارات المتخذة في إطاره بمثابة عمل ا ستنتاجي تكيفي قائم على أبرام العلاقات المنطقية ما يعني قدرة فائقة على الا ستجابة للتهديدات وتخفيف المخاطر، و ضمن هذا النطاق يـ سمح توليف الاحتمالات بتوليف إمكانيات جديدة قائمة على دخلات من بيانات جديدة غير مألو فة، ويمح التعلم الآلي بعمل يات التـ قدير التنبؤي وهو الأكثر العمل ية التفكيرية المـ ستقبلية وهي ميزة ذكية تـ سمح بتحقيق التوقع والتنبؤ لبناء نماذج التهديد وتحديد أنماط الاحتيال وحماية من اختراق البيانات (Kaspersky، 2024)، يمكن فهم الآل ية التي يوظف فيها التعلم الآلي في مجال الأمن السيبراني من خلال الشكل التالي:



المصدر: من إعداد الباحثة بناء على معطيات برنامج الحماية kaspersky

ويعتبر الأمن السحابي من أهم مجالات الامن السيبراني يعمل على تأمين أنظمة الحوسبة السحابية ويتضمن الحفاظ على خصوصية البيانات وأمانها عبر البنية التحتية والتطبيقات والأنظمة الأساسية القائمة على الأنترنت، ويبدأ تأمين الخدمات السحابية بفهم ما يتم تأمينه من خلال تطوير الواجهة الخلفية من الثغرات الأمنية، ويتم ذلك على مستوى (kaspersky، 2024):

- تامين الشبكات المادية ومنها أجهزة التوجيه والطاقة الكهربائية والكابلات وأجهزة التحكم في المناخ.
- حماية البيانات المخزنة والمعدلة والتطبيقات.
- حماية خوادم البيانات
- تأمين أطر المحاكاة الافتراضية مثل برامج الآلة الافتراضية والأجهزة المضيفة وأجهزة الضيف.
- تأمين أنظمة التشغيل OS وإدارة واجهة برمجيات التطبيقات API.
- حماية بيئات التشغيل
- حماية المستخدم النهائي وأجهزة المستخدم وأجهزة أنترنت الأشياء.

ويستخدم الأمن السيبراني السحابي مجموعة من الأدوات يمكن تلخيصها على النحو التالي:

الشكل رقم10: يوضح أدوات الأمن السيبراني السحابي

المصدر: من إعداد الباحثة بناء على معطيات Microsoft

تقنية التوقيع Signature based technique:

تعتبر هذه التقنية من مخرجات التكامل بين الأمن الـ سيبراني وخوارزميات الذكاء الا صطناعي، يتم من خلال هذه التقنية كـ شف الهجمات الالكترونية والبرامج الـ ضارة من خلال الرموز المتاحة بالاعتماد على خوارزميات الذكاء يتم مـ طاب قة التوقيع في هذه الرموز مع قوا عد البـ يا نات مع يمنح لخبراء الامن الـ سيبراني ميزة إ ضافية تمكنهم من إيقاف الهجمات الـ سيبرانية واكتـ شافها، وتحتفظ هذه التقنية بالتوقيعات البرامج الـ ضارة ضمن القائمة الـ سوداء ويتم اكتشاف الهجمات باستخدام التعلم الالي في تتبع والتعرف على توقيعات جديدة ومطابقتها مع القائمة السوداء في حال تغيير أنماط الهجوم (Meraj، Bibhu ، Pawankumar، و Nikhitha، 2022، ص 84).

يـ شكل الاعتماد المتزايد على ا ستخدام الذكاء الا صطناعي في الامن الـ سيبراني فر صة ا ستثمارية كبيرة تفرض تحولات كبرى في ميدان الـ صناعة التكنولوجية الذكية، هذا الامر تفـ سره أرقام نمو سوق الذكاء الا صطناعي في مجال الأمن السيبراني والتي يوضحها الجدول التالي:

الجدول رقم2: يوضح الاتجاه الاستشرافي لاستخدامات تقنيات الذكاء الاصطناعي في مجال الأمن السيبراني

حجم سوق	سعر السوق بالدولار الأمريكي
حجم سوق 2018	9.8 مليار دولار أمريكي
حجم سوق 2021	14.9 مليار دولار أمريكي
حجم سوق 2025	36.6 مليار دولار أمريكي
حجم سوق 2030	8133 مليار دولار أمريكي

المصدر (Meraj، Bibhu، Pawankumar، و Nikhitha، 2022، ص 85)

□

خاتمة

فر ضت التحولات الرقمية على ثورة الذكاء الا صطناعي تغييرات لام ست المفاهيم الا ستراتيجية لليقظة والأمن الـ سيبراني ومكنتها من الاذ سياب ضمن الأقنية التي أتاحتها ووفرتها تقنيات التعلم الآلي والحو سبة الـ سحابية والذكاء الا صط ناعي التول يدي وغير ها من أ نماط ومخر جات الثورة التكنولوج ية الذكية.

وإذا كان اتجاه ا ستخدام هذه التقنيات ضمن الف ضاء الـ سيبراني قد اتخذ سارات سلبية تتمثل في انخراطه في الهجمات والتهديدات والحروب الـ سيبرانية بالنظر لليونة الا ستخدام العالية التي يوفرها الذكاء الا صطناعي لم ستخدميه و قدر ته على الغوص في ظل مات الو يب العميق، وتوفيره الـ عدة التقن ية من فيرو سات وديدان وبرمجيات في عمليات التج سس والت صيد والاحتيال واختراق والأنظمة واحتجاز البيانات والمعلومات ذات الح سا سية العالية والهند سة الاجتماعية والتي تشكل مخاطر حقيقة ومؤكدة تؤدي إلى ظواهر مثل الإرهاب الـ سيبراني وإحداث الـ صدام والـ صراع ف ضلا على اقتحامه ميدان الحروب الهجينة.

وأمام تهديدات تكنولوجيا الذكاء الا صطناعي للف ضاء الـ سيبراني، تبرز الحاجة إلى إعادة ضبط خارطة الممار سات الرقمية وتدعيمها على المـ ستوى التقني والاجرائي بالاعتماد على ا ستراتيجيات اليقظة الخوارزمية أو اليقظة الـ سيبرانية التي تعمل على إتاحة البرمجيات اللازمة لت صدي والردع الـ سيبراني ف ضلا على كونها تمثل الجانب الأكثر كفاءة وفعالية و سرعة كمخرجات عملية لحوكمة الأمن الـ سيبراني، وت سعى اليقظة الخوارزمية لتوظيف عمليات الأتمتة وأنشطة التعلم الآلي وبرمجيات الذكاء الا صطناعي التوليدي واستغلال الخوارزميات في عمليات التتبع والإدارة والت صنيف والحماية والت صدي والتنبؤ بالأنشطة الخبيثة والحركات المريبة ضمن الفضاء السيبراني.

وتؤطر اليقظة الخوارزمية ممار سات الذكاء الا صطناعي التوليدي فهي تعمل على صعيد مؤ سـ ساتي يعكف على بناء منظومة متكاملة تجمع في فحواها الجانب البرمجي والتقني بالإ ضافة إلى الإطار القانوني والت شريعي

كضامن أساسي ومقيد لانفلات الذكاء الاصطناعي نحو العمل الاجرامي فضلا على دعوتها للاحترام البعد الأخلاقي في ممارسات الذكاء الاصطناعي.

ويتجاوز عمل اليقظة الخوارزمية في الضبط القانوني والمؤسساتي والأخلاقي لنشاط الذكاء الاصطناعي ضمن الفضاء السيبراني والاستخدامات الإيجابية في عمليات الدفاع والردع السيبراني إلى بناء آليات هندسة الأمن السيبراني من خلال عمليات تطويع وإدارة الأمن السيبراني، ويتاح هذا الأمر بالعمل على تصميم وبناء شبكات الأنظمة الحيوية عالية الدقة ومؤتمتة وترتكز على تكنولوجيا الذكاء الاصطناعي التوليدي والتعلم الآلي، توظيف الأمن السحابي وتعزيزه وهو الذي يضمن حماية قصوى للبيانات والمعلومات الحساسة وأمن المستخدم وأنظمة الوصول وغيرها من الميادين التي تقع ضمن نطاق الأمن السحابي السيبراني.

أتاح الدمج التقني والبرمجي المتكامل للذكاء الاصطناعي في الفضاء السيبراني، ما توفر لليقظة الخوارزميات إمكانيات عالية متعلقة بإدارة الحماية السيبرانية والامتثال للمعايير وبرتوكولات الأمان وحل المشكلات وتحليل المواقف والتنبؤ بالمخاطر والتهديدات المحتملة والسيطرة عليها قبل وقوعها فضلا على تحقيق السرعة والأنية والتفاعلية في تجاوز المخاطر والتهديدات وتحقيق الميزة الابتكار والإبداع والتنافسية مع ضمان شرط الحماية السيبرانية، وهو من التوجهات الاستراتيجية الأمنية الشديدة الاهمية التي ينبغي للدول والمنظمات والأشخاص العمل بها وتفعيلها ضمن أولويات تحقيق الأمن السيبراني.

يشكل التحول نحو تفعيل هندسة الأمن السيبراني رؤية استراتيجية تسهم في إتاحة فرص تكوين متخصصين في مجالات الفضاء والحماية السيبرانية وتطبيقات الذكاء الاصطناعي، وهو الأمر الذي يعد بتحول رقمي في مجال البحث العلمي الأكاديمي ويتيح تجاوز الفجوة الرقمية وتحقيق الاشباع التكنولوجي من خلال العمل على بناء اتجاهات علمية تؤسس معيارية مهنية مستقبلية ترتبط بتحقيق الأمن السيبراني من جهة وتأطير المسارات العلمية ضمن أولويات استراتيجية متكاملة تمكنها السياسات العامة لليقظة الخوارزمية.

قائمة المراجع:

- بن الصغير. يعقوب. (2023). المسألة الرقمية وفتوحات الذكاء الاصطناعي: نصوص فكرية في ضوء الراهن الاجتماعي التواصلي. الجلفة: فهرنهايت 541 للنشر والتوزيع.
- مجدي. نرمين. (2020). الذكاء الاصـــطناعي وتعلم الآلة. أبو ظبي: صـــندوق النقد العربي.
- معهد الدراسات المصرفية. (2021). إضاءات: الذكاء الاصطناعي. الكويت: معهد الدراسات المصرفية.
- الهيئة الوطنية للأمن السيبراني. (2018). الضوابط الأساسية للأمن السيبراني. الرياض: الهيئة الوطنية للأمن السيبراني.
- أمين عثمان. م. وقادر كرسو. ك. (2021). دور اليقظة الاستراتيجية في تحقيق النجاح الاستراتيجي- دراسة استطلاعية لآراء عينة من القيادات الادارية في جامعة جيهان أربيل. مجلة العلوم الإنسانية لجامعة زاخو (1).184 -167 .
- جيلالي شويرب، وفائزة مراد. (2023). مفهوم الحروب السيبرانية والأمن السيبراني. مجلة الحقوق والحريات (1)، الصفحات 157-178.
- سعاد عياط، وأسماء حاكم. (2016). اليقظة الاستراتيجية وضمان الامن الاقتصادي للمؤسسات -دراسة نظرية-, ورقة بحثية مقدمة لأشغال ملتقي حول: أداء المنظمات والحكومات والأمن الاقتصادي (الصفحات 1-15). الجزائر: جامعة طاهيري محمد بيشار.
- زمورة. جمال وبن عيسى. ليلي. (2022). أهمية حوكمة الأمن السيبراني لضمان تحول رقمي آمن للخدمات العمومية في الجزائر. مجلة البحوث الاقتصادية، 2.
- شريفة كلاع. (2022). الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني. مجلة الحقوق والعلوم الانسانية، الصفحات 292-314.
- مريم لمروس. (2019). سياسة اليقظة الاستراتيجية في الجزائر. مجلة دراسات اقتصادية (38)، الصفحات 173- 188.
- أنترنت الأشياء: الحماية من التهديدات السيبرانية، مقال في موقع روبدين نشر بتاريخ: 29 نوفمبر 2022، متاح على الرابط: https://robodin.com/iot-cyber-security/ تم الاطلاع عليه يوم: 2024/05/13.
- سارة عبد العزيز سالم. (20019). تأثير الذكاء الاصطناعي في سباق التسلح العالمي. تاريخ الاسترداد 13 5, 2024، من المستقبل للأبحاث والدراسات المتقدمة: https://2u.pw/kwNtyrLx
- سعادة محمد الكويتي. (26 جانفي, 2023). الأمن السيبراني في 2023: تحولات وتحديات عصر الذكاء الاصطناعي. تم الاسترداد من ترينذ للبحوث والاستشارات: https://trendsresearch.org/ar/insight/%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A-%D9%81%D9%8A-2023-%D8%AA%D8%AD%D9%88%D9%84%D8%A7%D8%AA-%D9%88%D8%AA%D8%AD%D8%AF%D9%8A%D8%A7%D8%AA-%D8%B9%D8%B5
- طارق راشد. (28 ديسمبر, 2020). الدفاع السيبراني في عصر الذكاء الاصطناعي والمجتمعات الذكية والإنسانية المُعززة. تم الاسترداد من ترينذ للابحاث والاستشارات: https://trendsresearch.org/ar/insight/%d8%a7%d9%84%d8%af%d9%81%d8%a7%d8%b9-%d8%a7%d9%84%d8%b3%d9%8a%d8%a8%d8%b1%d8%a7%d9%86%d9%8a-%d9%81%d9%8a-%d8%b9%d8%b5%d8%b1-%d8%a7%d9%84%d8%b0%d9%83%d8%a7%d8%a1-%d8%a7%d9%84%d8%a7%d8%b5%d8%b7%d9%86
- عمرو، أحمد (2022)، ما بعد الإنسانية: العوالم الافتراضية وأثرها على الإنسان، أفاق المعرفة للنشر والتوزيع، الرياض.

- ماساكي كاميزونو، وساتورو كودا. (2024). الجانب المظلم للذكاء الاصطناعي: ما هي أبرز تحديات الأمن السيبراني مع التقدم المذهل للذكاء الاصطناعي؟ تاريخ الاسترداد 14 5, 2024، من اليابان بالعربي: https://www.nippon.com/ar/in-depth/d00948
- CrowdStrike. (2024). Global Threat Report | CrowdStrike.
- Farheen Ansari Meraj ،Dash Bibhu ،Sharma Pawankumar و ، Yathiraju Nikhitha. (2022). The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review. International Journal of Advanced Research in Computer and Communication Engineering. p. 81- 90 . doi:10.17148/IJARCCE.2022.11912
- Imperva. (15 5, 2024). What is an NTP amplification attack تاريخ ؟ الاسترداد 2024، من imperva: https://www.imperva.com/learn/ddos/ntp-amplification/
- John B. Sheldon. (14 5, 2024). cyberwar تاريخ الاسترداد 2024، من Encyclopedia Britannica.: https://www.britannica.com/facts/cyberwar
- Kaspersky. (2024). https://me.kaspersky.com تم الاسترداد من ./ https://me.kaspersky.com/
- Meraj , Farheen Ansari; Bibhu , Dash; Pawankumar, Sharma; Nikhitha , Yathiraju, (2022), The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review, International Journal of Advanced Research in Computer and Communication Engineering, 81- 90.
- Pam Nigro. (15 1, 2024). The intersection of cybersecurity and artificial intelligence تاريخ الاسترداد 15 5, 2024، من security: https://2u.pw/CBwjdfxG