

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 القبول: 2025/11/26

تاريخ الاستلام: 2025/06/07

ملخص:

يشكل الأمن السيبراني تحديًا فائق الأهمية لمواكبة الثورة التكنولوجية التي أسهمت في ميلاد عصر الذكاء الاصطناعي، وأمام تعدد الأدوار التي يؤديها استخدام الذكاء الاصطناعي بين اختراق وتهديد للأمن السيبراني وبين حماية وردع هذه التهديدات، تبحث هذه الورقة سبل واستراتيجيات خوارزميات الأمن السيبراني في ظل ترسانة من التقنيات التي يتحياها الذكاء الاصطناعي من التعلم الآلي والأمن السحابي وإدارة حماية الوصول والأنظمة والشبكات والتوقيع وغيرها، وهذه التحولات ارتبطت بضرورة حوكمة الأمن السيبراني بما يتناسب والفكر القيمي والأطر التشريعية الضابطة، ضمن تفعيل سياسات اليقظة الخوارزمية نحو تكريس مفاهيم وآليات هندسة الأمن السيبراني 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 خصوصاً في ظل الثورة الرقمية التي تشهدها المجتمعات الآن ساذجة، وأمام تعاضل أدوار التكنولوجيا وانخراط تقنيات الذكاء الاصطناعي AI في الصناعات الأمنية والتوظيفات العديدة لها في إدارة الهجمات والتهديدات المختلفة وهو الأمر الذي أبان عن سباق تسلح مدعوم بخوارزميات الذكاء الاصطناعي المختلفة مثل إنترنت 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 الميتافيزيقيا - فضاء المتسع واللامحدود افتراضيا وواقعيا، ما فتح المجال أمام الحديث عن إسقاط تصورات الخيال العلمي المنسوجة في فضاءات

الميتافيرس عن المستقبل القريب لمجتمعات الإذ سان وما بعد الإذ سان، بعد أن أصبحت الآلة شريكا في الحياة الاجتماعية وامتزجت التقنية لتكون امتدادا لأعضاء الإذ سان، 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 صدورها 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 باتت تشكل حتمية علمية لا مفرّ منها، ويفرض ضرورة تسريع وتيرة الترابط بين التخصصات لتجاوز الصور العلمية أو محدودية التأطير العلمي لتحويلات 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 الآليات والممارسات التي يتم توظيفها في عمليات الاختراق والجوسسة والتصيد والهندسة الاجتماعية وإدارة الذكاء الاصطناعي في الصراعات والحروب السيبرانية المختلفة، كما تعتمد الدراسة الحالية على بيان أهمية توظيف التقنيات الذكية في الجوانب الدفاعية مثل عمليات لحماية وحوكمة الأمن السيبراني، وبالاعتماد على السياقات الرشيدة التي توّطرها اليقظة الخوارزمية فإنه يمكن قولبة تصورات فكرية لما يمكن أن يشكل أفق اليقظة الخوارزمية في حوكمة وأخلاق تكنولوجيا الذكاء الاصطناعي AI في الفضاء السيبراني وتوطئتها في ميدان الأمن.

وتبرز أهمية الدراسة الحالية في كونها تتعاطى معرفيا مع أبرز القضايا الأمنية المرتبطة بحيثيات تطبيق تقنيات الذكاء الاصطناعي AI في مجال الأمن السيبراني ضمن بعدين أساسيين: 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 استتطاق الآليات التي من خلالها يمكن حوكمة الأمن السيبراني من خلال استراتيجيات وأدوات تستطيع فيها العمل على عقلنة خوارزميات الذكاء الاصطناعي AI وتوظيفها في مسار يخدم الأمن السيبراني، وتفتح أفق توطين مفاهيم اليقظة الخوارزمية وعمليات هندسة الأمن السيبراني على المدى البعيد مما يساهم في خلق نوعا من الاستقرار الآلي يضمن انخراط التقنية الذكية في مسار الاستعمالات الآمنة والرشيده وتفعيل المعايير والمبادئ القيمية والأخلاقية كأطر مرجعية تحتكم إليها توجهات هندسة الأمن السيبراني في ظل عصر الذكاء الاصطناعي.

ولمحاولة تحقيق أهداف هذا الدراسة، تم اعتماد المقاربة البحثية على المنهج التحليلي الذي يسعى إلى استعراض الأطر النظرية والمعرفية لبناء الهيكل النظري وفك التشابك الإجرائي بين المحاور الأساسية التي انطلقت منها هذه الدراسة، والمتعلقة بما بحث "الأمن السيبراني"، و"اليقظة الخوارزمية" و"تكنولوجيا الذكاء الاصطناعي" 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 الدراسة، وهي من المفاهيم الشائكة والمتداخلة المجالات، وبالتالي فإن محاولة تحديد إطار مفاهيمي دقيق يستعصي على هذه الدراسة، غير أن هذا لا يمنع من استعراض بعض المفاهيم التي تدخل في نطاق اهتمام هذه الدراسة ومجالها البحثي.

الأمن السيبراني:

يعرف الأمن السيبراني بأنه "حماية الأنظمة والشبكات والبرامج والمواقع الجغرافية من الهجمات الرقمية ومن أي شكل أو عائق أو هجمات إلكترونية تحول دون أداء عملها (بن مهدي وسعيد، 2022، ص 29).

إجرائياً؛ يمكن تعريفه بأنه نظام دفاع عالي الجاهزية يستهدف تحقيق أقصى قدر ممكن من حماية المواقع والبرمجيات والشبكات والأنظمة الحاسوبية وأنظمة الحماية من القرصنة والهجمات الإلكترونية والحروب الرقمية، ويعتبر من أهم المجالات التي تتطلب درجة عالية من الأهمية واليقظة نظراً 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 السيبرانية 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" (لمروس، 2019، ص 175)، أو "القدرة على تقييم الظروف الداخلية والخارجية بدقة وواقعية بطريقة تسهل بناء الأفكار المهمة" (أمين عثمان وقادر كرسو، 2021، ص 168)، ويؤسس هذا المفهوم في تحديد الأدوار الهامة لليقظة الاستراتيجية التي تسعى لإدارة عمليات التقييم ضمن المستويات المختلفة بغية بناء خطط استراتيجية وقائية استباقية أو نجيعة لاحقة.

تعرفها المنظمة الفرنسية للتقييس (AFNOR) على أنها "الذ شاط الم مستمر 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 تقنياتها وأدواتها 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 الإنسان، ويتم ذلك عن طريق مجموعة من البرمجيات التي يتم تزويدها للحواسيب وتساعد على القيام بنفس العمليات الفكرية التي يقوم بها الإنسان مثل لغات الإنسان 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 القيام بمهام أعقد من ذلك (معهد الدراسات المصرفية، 2021، ص 3).

يقدم John McCarthy تعريفاً شاملاً 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 إجرائياً 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 لآخر أسهم في تجاوز قدرات الإنسان في التفكير على عمليات معقدة وشائكة وقدرات مذهلة في تحليل البيانات ومعالجة البيانات الضخمة وصولاً إلى إنتاج الروبوتات التي تحاكي الإنسان الممارسات الإنسانية".

الأمن السيبراني والجيل الخامس... تحولات بنوية

أثارت المخرجات التقنية للثورات التكنولوجية التي شهدتها الإنسان، تحولات مذهلة أثرت على الإنسان سنان بمختلف مجالاتها، امتد هذا الأثر ليقترن بالامتدادات المتعددة ومجالات ذات خصائص عالية من أهمها ميدان الأمن السيبراني ليدخل في ظل تقنيات الذكاء الاصطناعي AI أهم الميادين التي استقطبت توظيفات عالية الحساسية وشديدة العمق واهتمامات بالغة لأثار وتداعيات هذا الدمج الرقمي والذكي في الفضاء السيبراني.

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

الرقمية، والتي من خلالها يمكن بناء وإدارة دول منظمات حركات جيوش حروب و صراعات وتجارة واقتصاد وغيرها، ولكن بصفة رقمية بحتة، ولا يرتبط هذا الأمر بالإدارة فقط، بل يتعدى إلى إسقاط التحولات الافتراضية على البيئة الحقيقية، يمكن الاستدلال على ذلك بأحداث الهجوم ال سيبراني على كيبك التي سببت عطلا شاملا في شبكات التغذية الكهربائية لعاصمة أوكرانيا سنة 2015، الهجوم الذي استهدف منظومة قمر الاتصالات "كيبك" الخاص بشركة فيسات الأميركية عام 2022 والذي أدى إلى أضرار متعلقة بإمكانية الوصول وتصفح المواقع الإلكترونية في أوروبا.

وتعتمد المجتمعات بشكل متنام على تكنولوجيا الاتصالات والمعلومات المتصلة بالشبكة العنكبوتية، غير أن هذا الاعتماد المتزايد يرافقه مخاطر ناشئة ومحملة تهدد بشكل أساسي الشبكات وأمن المعلومات والمجتمع المعلوماتي وكيانه الهيكلي بصفة عامة، ويتوافق مع سوء الاستغلال أهداف إجرامية تؤثر على بنية المعلومات سيما الحساسية 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 اتخاذ صيغ فرقة خاصة 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 وسجلت أول هجمة سيبرانية على أنظمة المعلومات الخاصة بأوكرانيا سنة 2013 (شويرب و مراد، 2023، ص 161).

وأمام التحولات التي تعرفها التقنية ولوجها عالم الجيل الخامس وما ي صاحبه من توسع وانتشار وكفاءة الاتصالات وقدرته الفائقة الجودة والدقة والفعالية في الاستخدام الواسع النطاق لقواعد البيانات وكذا دعم ملايين الأجهزة التقنية وبأقل طاقة ممكنة، وهو الأمر الذي ينبئ بأن التحولات القادمة ستتم ضمن مستويات هيكلية وبنوية على حد سواء.

يمكن فهم عمق هذه التحولات في تكنولوجيا أنترنت الأشياء (IoT)، حيث تعتمد هذه الأخيرة على مشاركة البيانات، مما يعني تدفقا كبيرا وسريعا للبيانات والمعلومات أثناء عمليات التشارك ينتج عن هذا الأمر هشاشة منظومة الأمن المعلوماتي بالنظر لتركيز منتجي هذه الأجهزة على المزايا الذكية 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 أضرار مادية خصوصا فيما يتعلق بميدان الطاقة (روبدين، 2022)، أو ميدان صناعة المعدات والأسلحة الكيميائية أو النووية وهو ما ينذر بمخاطر وكوارث كبيرة في حال اختراقها والتحكم في أنظمتها. وفي ظل هذه التدفقات التكنولوجية من أنترنت الأشياء والروبوتات وتقنيات الجيل الخامس الفائقة الذكاء، تبرز الحاجة إلى دعم الأمن السيبراني، تتعلق هذه الحاجة بعمليات دمج المجتمعات الذكية مع آليات الذكاء الاصطناعي، تؤدي عمليات الاندماج إلى مجموعة من الإشكاليات مرتبطة بأمن البيانات وخصوصية الحسابات واستغلال الخبيث لمعلومات وبيانات الأشخاص خصوصا مع انتشار الأجهزة الاستشعارية الذكية القابلة للارتداء (راشد، 2020).

وأمام هذه المخاطر وغيرها أصبح الأمن السيبراني يمثل سوق استثماري متوسع، حيث بلغت قيمته الدفاعية العالمية 16,22 مليار دولار عام 2020، ويتوقع وصولها إلى 28,53 مليار بحلول سنة 2026م، ويعتبر إقليم آسيا الباسيفيك أسرع أسواق الأمن السيبراني نموا، فيما يعتبر إقليم أمريكا الشمالية أكبرها حجما، ويرجع نمو سوق الأمن السيبراني في منطقة الشرق الأوسط 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 أثر الميتافيرس:

تعرف الحرب السيبرانية بأنها قيام دولة أو فواعل من غير الدول بشن هجوم إلكتروني، يمثل أعمالاً 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 وأثارها يمكن صدورها على البيئة الواقعية والمتمثلة في استغلال البيانات وإحداث خسائر وزعزعة الأنظمة الحيوية وتعطيلها واختراق قواعد البيانات وغيرها من الآثار التي تحدثها الهجمات السيبرانية.

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

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

يمكن أن تتعرض هذه الطبقات للهجوم السيبراني، باستخدام مختلف الأسلحة على سبيل المثال، يمكن تدمير أجهزة الكمبيوتر فعلياً، 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 حرب العراق عام 2003، حيث تضررت شبكات الاتصالات ومرافق الكمبيوتر والاتصالات السلكية واللاسلكية أو دمرت (Sheldon, 2024).

تحدث الهجمات على الطبقة النحوية باستخدام الأسلحة الإلكترونية التي تدمر البرامج التي تعمل على تشغيل أنظمة الحاسوب أو تتداخل معها أو تقسد أو تراقبها أو تلحق الضرر بها، وتشمل هذه الأسلحة البرامج الضارة مثل الفيروسات وأحد صنعة طروادة وبرامج التجسس والديدان التي يمكن أن تدخل شفرة تالفة في البرامج الحالية، مما يتسبب في قيام الكمبيوتر بتنفيذ إجراءات أو عمليات غير مقصودة من قبل مشغله. تشمل الأسلحة السيبرانية الأخرى هجمات رفض الخدمة الموزعة (DDoS) (Sheldon, 2024)

تتلاعب الهجمات الإلكترونية الدلالية، والمعروفة باسم هجمات الهندسة الاجتماعية، بصورت المستخدمين البشريين وتفسيحاتهم للبيانات التي يتم إنشاؤها بواسطة الحاسوب من أجل الحصول على معلومات قيمة (مثل كلمات المرور والتفاصيل المالية والمعلومات الحكومية السرية) من المستخدمين من خلال وسائل احتيالية (Sheldon, 2024)

يشير التقرير العالمي لـ crowdstrike إلى زيادة عدد الهجمات السيبرانية حول العالم، يعزى هذا الأمر حسب التقرير إلى الاستخدام الواسع النطاق لتقنيات التدريب العملي أو التطفل التفاعلي والتي تنطوي على قيام الضوم بتنفيذ إجراءات نشطة على المضيف لتحقيق أهدافهم وهي على عكس البرامج الضارة التي تعتمد على نشر الأدوات والبرمجيات النصية الضارة، تعمل عمليات الاقتحام التفاعلية على تعزيز الإبداع ومهارات حل المشكلات لدى الضوم البشريين، يمكن لهؤلاء تقليد السلوك المتوقع للمستخدم والمسؤول مما يجعل من الصعب على المدافعين التمييز بين نشاط المستخدم المشروع والهجوم الإلكتروني، وقد رصدت منظمة crowdstrike زيادة بنسبة 60% في عدد حملات التطفل التفاعلية وزيادة بنسبة 75% في النصف الثاني (CROWDSTRIKE, 2024, p 10)

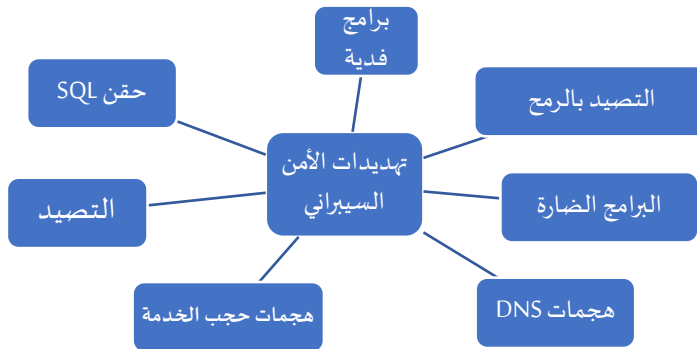
الشكل رقم 1: يوضح التكرار النسبي لعمليات التطفل التفاعلي في أهم 10 قطاعات صناعية وفي المناطق الجغرافية



المصدر: (CROWDSTRIKE، 2024، ص 10)

لقد استطاعت الحروب الـ سيبرانية إعادة ضبط مفاهيم واستراتيجيات الاشتباكات العسكرية والصراعات الاقتصادية، فهذا المنظور الـ سيبراني يتكئ على العدة التقنية في عمليات الـ صدام الـ إلكتروني وتنفيذ الاختراقات وإحداث خسائر مادية وبشرية وتقنية وأسرار البيانات والمعلومات وشل قدرات الخصم في وصوله للبيانات والمعلومات، وهي مفاهيم عملياتية تندرج ضمن سياق الهجمات الـ سيبراني في البيئة الرقمية. يمكن فهم أشكال التهديدات الـ سيبرانية على النحو التالي:

الشكل رقم 2: يوضح أبرز أنواع التهديدات التي يتعرض لها الأمن السيبراني



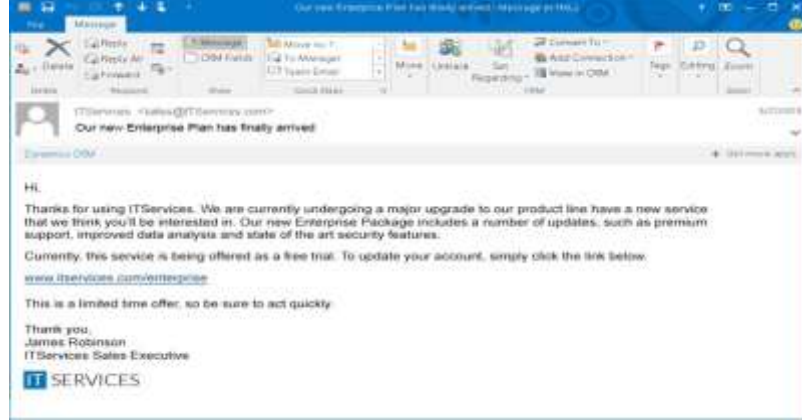
المصدر: من إعداد الباحثة

وتتعدد أشكال التهديدات والحروب الـ سيبرانية والتي يمكن استعراضها 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 متكرراً 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 تفاصيله باستخدام الرابط فوق ارتباط مرفق، مما يؤدي إلى تثبيت برامج ضارة على حاسوب الضحية.
 - رسائل البريد الإلكتروني للتصيد الاحتيالي غير شخصية ويتم إرسالها بشكل مجمع وغالباً 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 الجهات 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 مصدر قريبة من الهدف. يرسل مجرمو الإنترنت رسائل بريد إلكتروني مخدعة 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 للعمليات itservices.com، يدعي البريد

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

الشكل رقم 3: يوضح مثال لطريقة التصيد الاحتيالي



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

بعد النقر على الرابط، تتم إعادة توجيهه م مسؤول النظام إلى صفحة تسجيل الدخول على itservice.com، وهو موقع ويب مزيف مطابق لـ صفحة 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

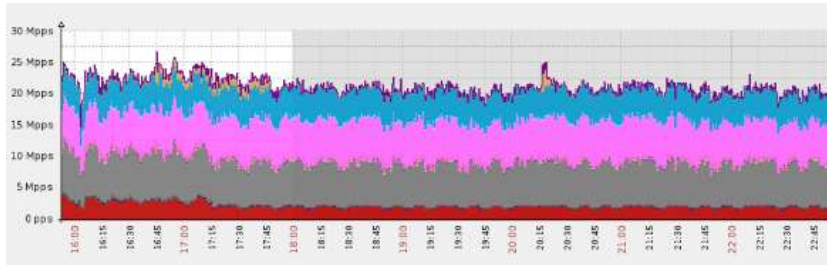
الأخرى من الهجمات الإلكترونية، لا تحاول هجمات DDoS اختراق محيط الأمان الخاص بالخادم. بدلا من ذلك، يهدف هجوم DDoS إلى جعل موقع الويب الخاص بالخادم وخوادمه غير متاحة للمستخدمين الشرعيين، يمكن أيضا استخدام DDoS كستار دخان للأنشطة الضارة الأخرى وإنزال الأجهزة الأمنية، وخرق المحيط الأمني للهدف.

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 رقم 4: 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 أو DDoS ، 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 إنترنت الأشياء وانتشار شبكات 5G ، والتي ستزيد من استخدام الأجهزة المتصلة، وهو ما يؤدي إلى زيادة في الهجمات عليها.

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

يمكن أن يتخذ الانتحال أشكالاً مختلفة، والتي تشمل:

أ. انتحال المجال: انتحال النطاق: هو شكل من أشكال التصيد الاحتمالي حيث ينتحل المهاجم شخصية نشطة تجاري معروف أو شخص لديه موقع ويب مزيف أو مجال بريد إلكتروني لخداع الأشخاص في الوثوق بهم. عادة، يبدو المجال شرعياً 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. نظراً لأن المرسلين يتلقون الرسائل في المرسلة المزعومة، فمن المرجح أن يفتح البريد الإلكتروني ويتفاعل مع محتوياته، مثل رابط أو مرفق ضار.

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

يمكن المتسلل 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 يوماً لتحديد الهوية، من الصعب للغاية اكتشاف الهجمات التي تعتمد على الهوية. عندما يتم اختراق بيانات اعتماد مستخدم صالح ويتنكر الخصم في زي هذا المستخدم، غالباً ما يكون من الصعب جداً التمييز بين سلوك المستخدم النموذجي وسلوك المتسلل باستخدام تدابير وأدوات الأمان التقليدية.

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

- Kerberoasting هي 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.

- هجومات الرجل في الوسط (MITM) هو نوع من الهجمات الإلكترونية التي يتصت 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 هجومات التجزئة (PtH) هو نوع من الهجومات 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. بدلاً من ذلك، يستخدم إصداراً مخزناً من كلمة المرور لبدء جلسة جديدة.

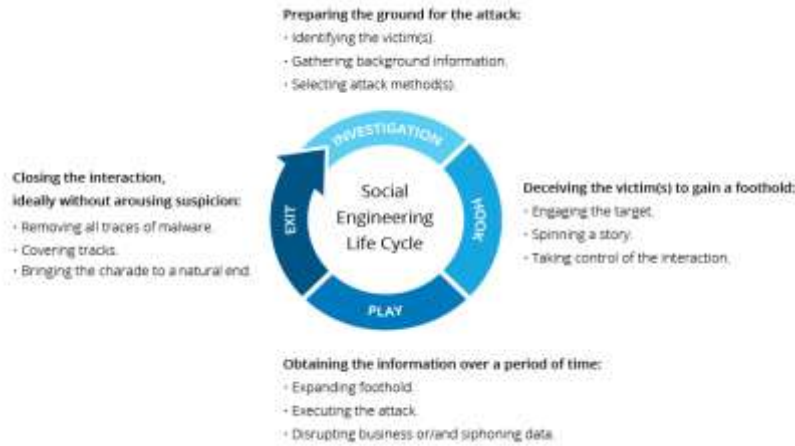
- هجومات التذكرة الذهبية: يحاول الخصوم الوصول غير المحدود إلى مجال المؤسسة عن طريق الوصول إلى بيانات المستخدم المخزنة في Microsoft Active Directory (AD) عن طريق استغلال الثغرات الأمنية في بروتوكول مصادقة الهوية Kerberos. هذا يسمح للخصوم بتجاوز طرق المصادقة.

- حشو بيانات الاعتماد: تعمل هجمات حشو بيانات الاعتماد على فرضية أن الأشخاص غالباً 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 الأذ شطة 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 رقم 5: 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 المتصيد 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 الأعمال الإجرامية 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 الإلكتروني والوصول 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 الإنسان والقيم الديمقراطية والتنوع وتعزيز العدالة الاجتماعية (كاميزونو وكودا، 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 رقم 1: يوضح بعض البرمجيات المستخدمة في هجمات سيبرانية

اسم الفيروس	وظيفته
دودة Stuxnet	هاجمت هذه الدودة البرنامج النووي الإيراني، وهي من بين أكثر الهجمات الإلكترونية تطوراً في التاريخ، انتشرت هذه الدودة عبر أجهزة Universal Serial Bus واستهداف الوصول على البيانات وأنظمة التحكم الإشراقية، وقد أحدث الهجوم أضراراً خطيرة تهددت قدرات إيران على تصنيع أسلحة نووية حسب تقارير أمريكية.

<p>وجاء هجوم على شركة سوني بيكتشرز بعد إصدار فيلم "المقابلة"، الذي قدم صورة سلبية لكيم جونج 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.</p>	<p>Sony Pictures Hack <input type="checkbox"/></p>
<p>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.</p>	<p>Bronze Soldier <input type="checkbox"/></p>
<p>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 مما صابته 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.</p>	<p>Fancy Bear</p>

المصدر: (imperva، 2024)

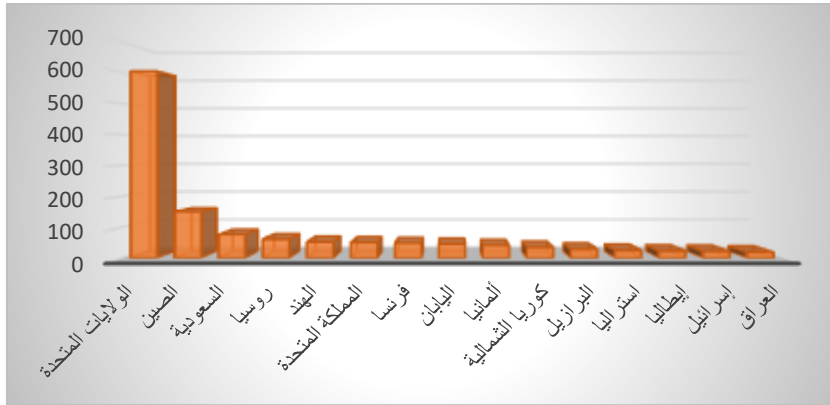
الحكومة السيبرانية... رؤية استراتيجية للتحويلات الرقمية:

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

الإمكانات التي يوفرها (الاستشعار عن بعد، والإدراك اللحظي للمتغيرات والمناورة واتخاذ القرار تحت الضغط) وضمن هذه التحولات التي أحدثها اندماج التقنية الذكية يمكن فهم الآثار الاستراتيجية 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 السيبراني في ترتيب أولويات الدول وهو الأمر الذي يوضح تخصيل ميزانيات عالية تهتم بتسليح المنظومة الدفاعية السيبرانية، وهو ما ترصده المؤشرات التالية :

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

الدفاع السيبراني



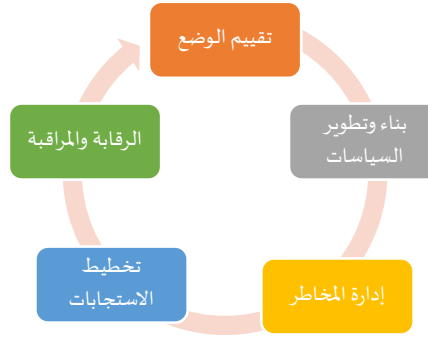
المصدر: من إعداد الباحثة وفقا لتقرير معهد الملكي للدراسات

الاستراتيجية IIS

وتشير حوكمة الأمن السيبراني إلى حوكمة التكنولوجيا المعلوماتية التي تسعى إلى إدارة أمن المعلومات وكذا وسائل تنظيم الأنظمة الأمنية المطبقة في المنظمة لتحقيق أهدافها، فهي عملية مستمرة وتشكل جزءا من ثقافة المنظمة وتدمج إدارة المخاطر وتتوافق استراتيجيا مع أهدافها، يحدد القواعد الأمنية التكتيكية والتشغيلية، مثل تنفيذ الضوابط المناسبة ولذلك فهي تضمن الامتثال للمعايير المعمول بها والالتزام بساق في تنفيذ الإطار المعياري سواء كانت تضع ل NIST 800-531 أو ISO270002 أو معيار أمان بيانات صناعة بطاقة الدفع PCIDSS ، ويجب على المنظمات الالتزام بمتطلبات 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 ال سيبراني وتجاوز المخاطر المحتملة والمحقة، وتحقيق الردع ال سيبراني 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 ال سيبرانية تمر عبر سبع مراحل أساسية هي (زمورة و بن عيسى، 2022، ص 418):

- تحديد الوضع الحالي: تقييم المخاطر الإلكترونية فهم الثغرات وإنشاء خارطة طريق لسد تلك الفجوات.
- إن شاء مراجعة وتحديث جميع ال سياسات ومعايير وعمليات الأمن ال سيبراني على مستوى هذه الخطوة ويجب أخذ الوقت الكافي لإنشاء هيكل وتوقعات حوكمة الأمن السيبراني.
- مقارنة الأمن السيبراني من منظور المؤسسة وتحديد ما هي البيانات التي يجب حمايتها وكيف تتماشى المخاطر ال سيبرانية مع إدارة أخطار المؤسسة وتحديد الأولوية الذسببية لا استثمار في الأمن السيبراني.
- زيادة الوعي والتدريب في مجال الأمن ال سيبراني: ربما ساهمت جائحة كوفيد 19 في بلورة هذا الاتجاه خاصة فيما يخص التدريب

مع وجود الكثير من الأشخاص الذين يعملون في المنزل والتعليم عن بعد، فمن الأهمية بمكان أن يعي الجميع أهمية الأمن السيبراني وأنه من مسؤوليتهم جميعاً وهذا المنقل يظهر ما يعرف بالنظافة السيبرانية.

- تحليل المخاطر السيبرانية؛ كيف يتم وضع نماذج تهديدات والمخاطر وتقييمها عند إذ شاء نموذج المخاطر يجب الأخذ بعين الاعتبار جميع المخاطر التي تتعرض لها المنظمة سواء الداخلية أو الخارجية.
- المراقبة والقياس والتحليل والإبلاغ والتدسين: والقيام ببرمجة فترات تقييم منتظمة، والقيام بقياس ما يهمهم ومن ثم تحليل البيانات وإذ شاء خطة تدسين مع تقديم تقرير إلى متخذي القرار حول الوضع السيبراني وموقف المخاطر السيبرانية.
- القيادة مهمة؛ من خلال جعل الأمن السيبراني وحوكمة الأمن السيبراني أولوية لدى القيادة العليا وجعل السياسات والمعايير والعمليات تعمل على موائمة حوكمة الأمن السيبراني مع أولويات الأمن السيبراني.

تخفف حوكمة الأمن السيبراني من التعرض للمخاطر باستخدام مجموعة من المعايير والضوابط والإجراءات والتي يمكن بلورتها فيما يلي (زمورة وبن عيسى، ص ص 424، 425):

- السياسات: وترسم من طرف أصحاب القرار ويتم تصميمها للتأثير على القرارات وتوجيه المنظمة لتحقيق النتائج المرجوة، ويتم فرضها من خلال المعايير وكذلك من خلال إجراءات لتحديد متطلبات قابلة للتنفيذ وخاضعة للمساءلة، وتحدد التقنية كيفية تنفيذ هذه السياسات، وعادة ما توضع السياسات لتلبية مطالب خارجية (مثل القوانين واللوائح وحتى التعاقدات).
- أهداف التحكم: هي الأهداف أو الشروط المرغوب الوصول إليها بمعنى آخر تصف ما يجب تحقيقه كنتيجة عند تطبيق المنظمة لعنصر التحكم، وهو يهدف المعيار إلى معالجته لاحقاً، ترتبط

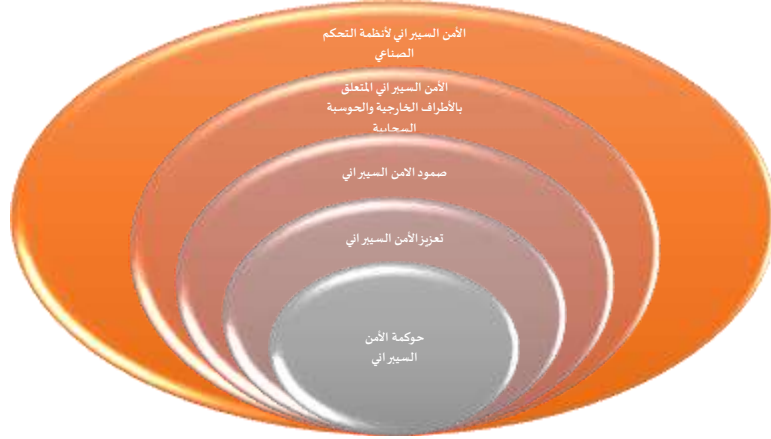
- أهداف التحكم ارتباطا بما شرا مع الممارسة ال صحية لموائمة الأمن السيبراني والخصوصية مع الممارسات المقبولة.
- المعايير: وهي متطلبات إلزامية فيما يتعلق بالعمليات والإجراءات والإعدادات المصممة لتلبية أهداف التحكم، يقصد بالمعايير أن تكون دقيقة وإلزامية لإذ شاء الحد الأدنى من متطلبات الأمن والتي تضمن تصميم وتشغيل الأنظمة والتطبيقات والعمليات لتشمل الأمن السيبراني وحماية الخصوصية.
 - التوجيهات: وهي عبارة عن ممارسات موصى بها تستند إلى ممارسات آمنة معترف بها في كل المجالات، تساعد الإرشادات على زيادة المعايير عندما يكون التقدير مسموحا به، على عكس المعايير تسمح التوجيهات للمستخدمين بتطبيق حرية التصرف، أو مجال واسع لتفسيرها، أو تنفيذها، أو استخدامها.
 - الضوابط: وتعتبر الرابط المستخدم لإدارة المخاطر من خلال منع أو اكتشاف أو تقليل تهديد معين على التأثير سلبا على العمليات تطبق عناصر التحكم بشكل مباشر على المعايير، ويستخدم اختبار التحكم بشكل روتيني في اختبار ما قبل التطبيق للتحقق من أي نظام قد استوفى الحد الأدنى من مستوى الأمان قبل أن يسمح باستخدامه في البيئة الحقيقية، غالبا ما يتم إجراء الاختبارات المتكررة على ضوابط معينة للتحقق من الامتثال للالتزامات القانونية والتنظيمية وحتى التعاقدية.
 - الإجراءات وهي مجموعة موثقة من الخطوات اللازمة لأداء مهمة أو عملية محددة وفقا لمعايير قابلة للتطبيق، وتساعد في معالجة مسألة كيفية قيام المنظمة بتشغيل سياسة أو معيار أو عنصرتحكم، الإجراءات بشكل عام هي مسؤولية السلطات التنفيذية، ولكن تحت إشراف متخذي القرار لضمان معالجة متطلبات الامتثال المعمول بها.

- المخاطر: يرتبط الخطر بنقص التحكم، و بالتالي فعلية 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 خطط الأساس لقياسات سابقة أو أكثر تم إجراؤها خلال فترة زمنية، يتم إنشاء التحليلات من تحليل المقاييس، تم تصميم التحليلات لتسهيل اتخاذ القرار وتقييم الأداء وتحسين الممارسات من خلال جمع وتحليل وإعداد التقارير المتعلقة بالبيانات ذات الصلة بالأداء.
- وتتكون حوكمة الأمن السيبراني من العناصر التالية (Controls, p 12, 2018):

- استراتيجيات الأمن السيبراني؛
 - إدارة الأمن السيبراني؛
 - سياسات وإجراءات الأمن السيبراني؛
 - أدوار ومسؤوليات الأمن 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 وسياسات 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 ال سيبراني 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 الألى نحو أتمتة الأمن السيبراني:

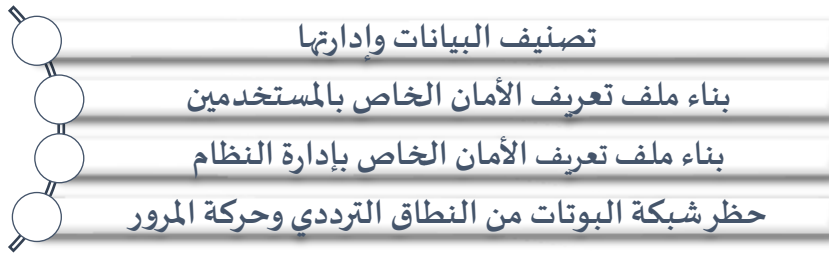
يتمثل الدور المثالي للذكاء الاصطناعي في الأمن السيبراني في تفسير الأنماط التي تحددها خوارزميات التعلم الآلي، حيث تعتمد هذه الأخيرة على "الدقة" في تعاملها مع البيانات، وتأطيرها، وتصنيفها باستخدام قواعد محددة مسبقاً، لتعيين فئات لنقاط البيانات، وهذا التصنيف يساهم في بناء ملف تعريف للهجمات السيبرانية، كما يحدد نقاط قوتها وضعفها، وهو ما يعزز الأمن الاستباقي ويخلق فرص نجاح كبرى بين دمج التعلم الآلي والأمن السيبراني (kaspersky,2024).

يتزايد الترابط بين الأمن السيبراني والذكاء الاصطناعي AI، حيث يلعب هذا الأخير دوراً مهماً في تعزيز تدابير الأمن السيبراني. وهذا التكامل ليس جديداً، ولكنه تطور مع مرور الوقت مع تقدم التكنولوجيا والتحديات السيبرانية التي أصبحت أكثر تعقيداً. حيث تركزت الاستخدامات الأولية للذكاء الاصطناعي في مجال الأمن السيبراني على بعض البرمجيات المرتبطة بجدران الحماية وبرامج مكافحة الفيروسات، مع بداية تسعينيات القرن الماضي تم اللجوء إلى الذكاء الاصطناعي في لعب دور في أنظمة كشف التسلل (IDS)، وذلك باستخدام تقنيات لتحليل أنماط حركة مرور الشبكة واكتشاف الحالات الشاذة التي قد تشير إلى حدوث خرق أمني، وشهد العقد الأول من القرن الحادي والعشرين أيضاً زيادة في استخدام تقنيات التعلم الآلي في الأمن السيبراني، وتطبيق الخوارزميات لتحليل أنماط البيانات وتحديد التهديدات المحتملة. اكتسب التحليل السلوكي، وهو أحد أشكال الذكاء الاصطناعي، أهمية كبيرة في اكتشاف البرامج الضارة والتهديدات السيبرانية الأخرى من خلال فهم السلوك الطبيعي وتحديد الانحرافات عن القاعدة (Nigro, 2024)

فيما يتعلق بتدابير وبروتوكولات أمن البيانات، تعتبر خوارزميات الذكاء الاصطناعي واحدة من أفضل التقنيات لضمان تحسین أمنها، من خلال بروتوكولات تشفير البيانات المتعددة، وهذا المجال يعتبر من أهم المجالات التي يحقق فيها الذكاء الاصطناعي عمليات تشفير عالية الدقة وبمهارات كبيرة (Pawankumar، Bibhu، Meraj، و Nikhitha، 2022، ص 83)

تتمثل إحدى الفرص المتاحة لفرق الأمن الـ سيبراني في تطوير طرق جديدة ومبتكرة لاكتشاف التهديدات والاستجابة لها. يمكنهم استخدام الذكاء الاصطناعي لأتمتة المهام الأمنية وإنشاء المزيد من الحلول الأمنية التكيفية الخاصة ومن خلال تعزيز بيئة تعزيز 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 لتصنيف القواعد المحددة مسبقاً ووضعها في مجموعات "مجمعة" من البيانات ذات السمات المشتركة أو الخصائص الفردية، كما تعمل مسارات العمل الموصى بها من الإجراءات الاستباقية لنظام أمن التعلم الآلي حيث تستند إلى مجموعة من التحذيرات على أنماط السلوك والقرارات السابقة وتوفر مسارات عمل مقترحة بشكل طبيعي، وهذا ما يجعل القرارات المتخذة في إطاره بمثابة عمل استراتيجي تكيفي قائم على أبرام العلاقات المنطقية ما يعني قدرة فائقة على الاستجابة للتهديدات وتخفيف المخاطر، وضمن هذا النطاق يسمح توليف الاحتمالات بتوليف إمكانيات جديدة قائمة على دخلات من بيانات جديدة غير مألوفة، ويمنح التعلم الآلي بعلميات التقدير التنبؤي وهو الأكثر العملية التفكيرية المستقبلية وهي ميزة ذكية تسمح بتحقيق التوقع والتنبؤ لبناء نماذج التهديد وتحديد أنماط الاحتيال وحماية من اختراق البيانات (Kaspersky, 2024)، يمكن فهم الآلية 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):

- تأمين 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 رقم 10: 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 ال سيبراني وخوارزميات الذكاء الاصطناعي، يتم من خلال هذه التقنية كشف الهجمات الالكترونية والبرامج الضارة من خلال الرموز المتاحة بالاعتماد على خوارزميات الذكاء يتم مطابقة التوقيع في هذه الرموز مع قواعد البيانات مع يمنح لخبراء الامن ال سيبراني ميزة إضافية تمكنهم من إيقاف الهجمات ال سيبرانية واكتشافها، وتحفظ هذه التقنية بالتوقيعات البرامج الضارة ضمن القائمة السوداء ويتم اكتشاف الهجمات باستخدام التعلم الالي في تتبع والتعرف على توقيعات جديدة ومطابقتها مع القائمة السوداء في حال تغيير أنماط الهجوم (Bibhu ، Meraj ، Pawankumar ، و Nikhitha ، 2022 ، ص 84).

يشكل الاعتماد المتزايد على استخدام الذكاء الاصطناعي في الامن ال سيبراني فرصة استثمارية كبيرة تفرض تحولات كبرى في ميدان الصناعة التكنولوجية الذكية، هذا الامر تفسره أرقام نمو سوق الذكاء الاصطناعي في مجال الأمن السيبراني والتي يوضحها الجدول التالي:

الجدول رقم 2: يوضح الاتجاه الاستراتيجي 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 (Bibhu ، Meraj ، Pawankumar ، و Nikhitha ، 2022 ، ص

(85)



خاتمة

فر ضت التحولات الرقمية على ثورة الذكاء الاصطناعي تغييرات لامست المفاهيم الاستراتيجية لليقظة والأمن السيبراني ومكنتها من الأذسياب ضمن الألفية التي أتاحها ووفرتها تقنيات التعلم الآلي والحواسبة السحابية والذكاء الاصطناعي التوليدي وغيرها من أنماط ومخرجات الثورة التكنولوجية الذكية.

وإذا كان اتجاه استخدام هذه التقنيات ضمن الفضاء السيبراني قد اتخذ سارات سلبية تتمثل في انخراطه في الهجمات والتهديدات والحروب السيبرانية بالنظر لليونة الاستخدام العالية التي يوفرها الذكاء الاصطناعي لمستخدميه وقدرته على الغوص في ظلمات الويب العميق، وتوفيره العدة التقنية من فيروسات وديدان وبرمجيات في عمليات التجسس والتصيد والاحتيال واختراق والأنظمة واحتجاز البيانات والمعلومات ذات الحساسية العالية والهندسة الاجتماعية والتي تشكل مخاطر حقيقة ومؤكدة تؤدي إلى ظواهر مثل الإرهاب السيبراني وإحداث الصدام والصراع فضلا على اقتحامه ميدان الحروب الهجينة.

وأمام تهديدات تكنولوجيا الذكاء الاصطناعي للفضاء السيبراني، تبرز الحاجة إلى إعادة ضبط خارطة الممارسات الرقمية وتدعيمها على المستوى التقني والاجرائي بالاعتماد على استراتيجيات اليقظة الخوارزمية أو اليقظة السيبرانية التي تعمل على إتاحة البرمجيات اللازمة لتصدي والردع السيبراني فضلا على كونها تمثل الجانب الأكثر كفاءة وفعالية وسرعة كمخرجات عملية لحوكمة الأمن السيبراني، وتسعى اليقظة الخوارزمية لتوظيف عمليات الأتمتة وأنشطة التعلم الآلي وبرمجيات الذكاء الاصطناعي التوليدي واستغلال الخوارزميات في عمليات التتبع والإدارة والتصنيف والحماية والتصدي والتنبؤ بالأنشطة الخبيثة والحركات المريبة ضمن الفضاء السيبراني.

وتؤطر اليقظة الخوارزمية ممارسات الذكاء الاصطناعي التوليدي فهي تعمل على صعيد مؤسساتي يعكف على بناء منظومة متكاملة تجمع في فحواها الجانب البرمجي والتقني بالإضافة إلى الإطار القانوني والتشريعي

كضامن أ س ا سي ومقيد لانفلات الذكاء الاصطناعي نحو العمل الاجرامي فضلا على دعوتها للاحترام البعد الأخلاقي في ممارسات الذكاء الاصطناعي. ويتجاوز عمل اليقظة الخوارزمية في الضبط القانوني والمؤسسي 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 الخوارزمية 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 الأهمية 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 الابتكار التكنولوجي من خلال العمل على بناء اتجاهات علمية تؤسس معايير مهنية مستقبلية ترتبط بتحقيق الأمن السيبراني من جهة وتأطير الممارسات العلمية ضمن أولويات استراتيجية متكاملة تمكنها من مساهمة 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 الاصطناعي وتعلم الآلة. أبو ظبي: صندوق 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 البيقظة الاستراتيجية في تحقيق النجاح الاستراتيجي- دراسة استطلاعية لأراء عينة من القيادات الادارية في جامعة جيهان أربيل. مجلة العلوم الإنسانية لجامعة زاخو (1). 167- 184 .
- جيلالي شويرب، وفائزة مراد. (2023). مفهوم الحروب السيبرانية والأمن السيبراني. مجلة الحقوق والحريات (1)، الصفحات 157-178.
- سعاد عياط، وأسماء حاكم. (2016). البيقظة 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 البيقظة 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 5 13 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 تريند 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 المعززة. تم الاسترداد من تريند للبحوث 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، أفق 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/IJARCCCE.2022.11912
- Imperva. (15 5, 2024). What is an NTP amplification attack تاريخ الاسترداد 14 5, 2024، من <https://www.imperva.com/learn/ddos/ntp-amplification/>
- John B. Sheldon. (14 5, 2024). cyberwar من تاريخ الاسترداد 14 5, 2024، من <https://www.britannica.com/facts/cyberwar>
- Kaspersky. (2024). <https://me.kaspersky.com/> من تاريخ الاسترداد 14 5, 2024، 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 من تاريخ الاسترداد 15 5, 2024، من <https://2u.pw/CBwjdfxG>