CJSP
ISSN-2536-0027

مجلة كامبريدج للبحوث العلمية

مجلة علمية محكمة تصدر
عن مركز كامبريدج للبحوث
والمؤتمرات في مملكة البحرين

العدد ـ ٣٤ ـ حزيران ـ ٢٠٢٤

CAMBRIDGE
RESEARCH AND CONFERENCES CENTER

صدر العدد بالتعاون مع
جامعة المشرق
العراق بغداد .طريق المطار الدولي

مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الرابع الثلاثون – حزيران ٢٠٢٤– ذي الحجة ١٤٤٥
ISSN–2536–0027

الذكاء الاصطناعي واستخداماته في المجال العسكري

م.م عبدالرحمن محمد عيسى
كلية العلوم السياسية/ جامعة النهرين
abdulrahman.mohammed@nahrainuniv.edu.iq

الملخص
شهدت تقنيات الذكاء الاصطناعي تطوراً سريعاً في السنوات الماضية حتى تعددت استخداماتها على المستوى العملي حتى باتت أنظمة الأسلحة الفتاكة المستقلة تُوصَف بالثورة الثالثة في الحرب بعد البارود والأسلحة النووية لما لها من قدرة على تحديد وتدمير أهداف مستقلة دون التدخل البشري المباشر على نحو يؤكد أهميتها في مجال الحروب لا سيما في ظل التغيرات المتوقعة في طبيعة المعارك المستقبلية ومع تعدد التهديدات التي يجب مواجهتها من خلال دفاعات عالية التقنية وأهمية استخدامها في عمليات الاستهداف التلقائي والتحليل الآلي للبيانات الاستخباراتية وتحسين اللوجستيات وغير ذلك.

Abstract
Artificial intelligence technologies have witnessed rapid development in the past years until their uses have multiplied on the practical level, to the point where lethal autonomous weapons systems are described as the third revolution in war after gunpowder and nuclear weapons, because of their ability to identify and destroy independent targets without direct human intervention, in a way that confirms their importance in the field of warfare. Especially in light of the expected changes in the nature of future battles and the multiplicity of threats that must be confronted through high-tech defenses and the importance of using them in automatic targeting operations, automated analysis of intelligence data, improving logistics, and so on.

المقدمة
ان للذكاء الاصطناعي استخدامات في مجالات واسعة من حياتنا المعاصرة، وقد كان أساس هذا العلم هي المحاولات الأولية لاستخدامه في السياق العسكري، حيث توجد إمكانية للاستفادة من قدرات الذكاء الاصطناعي في جميع الميادين (البرية والبحرية والجوية والفضائية)، وفي جميع مستويات الحرب السياسية والاستراتيجية والعملياتية والتكتيكية)، على سبيل المثال على المستويين السياسي والاستراتيجي، يمكن استخدام الذكاء الاصطناعي لزعزعة استقرار الخصم من خلال إنتاج ونشر كميات هائلة من المعلومات المزيفة في هذه الحالة من المرجح أن يكون الذكاء الاصطناعي أيضاً أفضل مرشح للدفاع ضد مثل هذه الهجمات على المستوى التكتيكي، يمكن للذكاء الاصطناعي تحسين التحكم المستقل جزئياً في الأنظمة غير المأهولة بحيث يمكن للمشغلين البشريين تشغيل الأنظمة غير المأهولة بكفاءة أكثر، وفي نهاية المطاف زيادة التأثير في ساحة المعركة.
ولقد أضحى الذكاء الاصطناعي يمارس دوراً حاسماً في جميع البرامج العسكرية للدول العظمى، كما أضحى استراتيجية رئيسية لوزارة الدفاع الأمريكية للحفاظ على التفوق التقني على الخصوم الأقران وشبه

مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الرابع الثلاثون – حزيران ٢٠٢٤– ذي الحجة ١٤٤٥
ISSN-2536-0027

الأقران، حاليا، تعتمد برامج الذكاء الاصطناعي على نماذج اللغات الكبيرة (LLMs)، والتي تستخدم مجموعات بيانات ضخمة لتشغيل أدوات مثل برامج الدردشة الآلية ومولدات الصور. ومع ذلك، غالبا ما يتم تقديم هذه الخدمات دون الكشف عن أعمالها الداخلية، مما يجعل من الصعب على المستخدمين فهم كيفية وصول التكنولوجيا إلى القرارات أو كيفية تحسنها بمرور الوقت.

تهدف التطورات التكنولوجية بالتطبيقات العسكرية إلى تقليل المخاطر على حياة الإنسان، وتنفيذ العمليات من مسافة آمنة. وسواء كان الأمر يتعلق بأسراب الطائرات بدون طيار أو دعم الذكاء الاصطناعي للطيارين المقاتلين، فإن الهدف هو تقليل الأضرار الجانبية مع تحسين خيارات الهجوم.

اهمية البحث: ان التنافس في المجال العسكري من أهم سمات النظام الدولي وهذه تتأثر بالتقدم التكنولوجي، سواء في مجال الأسلحة أو الأبحاث العسكرية أو النقل، وسيكون لسباق تسلح الذكاء الاصطناعي تأثير طويل الأمد، وسيشكل جزءاً رئيسياً من سباق التسلح في العالم في القرن الحالي، ويكشف هذا عن حرب رقمية باردة جديدة، ويضطلع الذكاء الاصطناعي أيضاً بدعم الأمن السيبراني للأفراد العاملين وشبكات الاتصالات، وعلى النقيض من ذلك يُستخدم في الهجمات السيبرانية لعرقلة أنظمة التسليح وإغلاق البنى التحتية الحيوية، لذلك فأن للذكاء الاصطناعي اهمية كبيرة في الاستخدام العسكري.

إشكالية البحث :

ينطلق البحث من إشكالية مفادها أن الذكاء الاصطناعي نقل علاقات القوى بين الوحدات الدولية والصراعات العالمية الى مرحلة جديدة ومختلفة ، حيث تطورت الجرائم السيبرانية بسرعة فائقة رغم حداثتها ترافق في ذلك سرعة انتشار التكنولوجيا الحديثة.

فرضية البحث

وبناء عليه فان البحث ينطلق من فرضية مفادها : كلما تمت الاستعانة بالعامل التكنولوجي كلما زاد من حالة عدم الاعتماد على العامل البشري في ادارة الحروب والصراعات الدولية وبداية الحروب غير تقليدية.

مناهج الدراسة: اعتمدت هذه الدراسة على مناهج متعددة من البحث العلمي، بغية الاحاطة بأكبر قدر ممكن من ابعاد هذه الدراسة، اذ تم الاعتماد على مناهج متعددة هي: المنهج الوصفي، والمنهج التحليلي النظمي، وعليه تم تقسيم البحث إلى المحاور الاتية :

اولاً: مفهوم الذكاء الاصطناعي وتطوره

يمثل الذكاء الاصطناعي كيانا متواجداً في شتى مجالات العصر وتقنياته فتجده في تطبيقات وخدمات الإنترنت في الطب وفي الصناعة والزراعة والهندسة والتعليم وغيرها من مجالات الحياة المختلفة وما لها من تقنيات متعددة تقوم الآن في جوهر صناعتها على الذكاء الاصطناعي[١].

يعتبر العالم الأمريكي (جون ماكارثي)[٢] هو الذي صك مصطلح الذكاء الاصطناعي في ١٩٥٦م وقد عرفه بأنه: (علم وهندسة صناعة الآلات الذكية أو هو فرع علوم الحاسوب الذي يهدف إلى إنشاء الآلات الذكية والذكاء Intelligence) ، ان الذكاء الاصطناعي كمفهوم يصعب تعريفه بدقة ويمكن اعتباره الجزء الحسابي الذي يعطينا القدرة على تحقيق الأهداف في العالم من حولنا ولدى الناس مختلف الدرجات من الذكاء.

يطلق الذكاء الاصطناعي القوي على الآله التي تحل محل الذكاء الانساني وتطبيق الاعمال حسب الخلفية المعرفية وبذلك بناء قدرات معرفية لا تختلف عن الكائن البشري فالأهداف العامة للذكاء الاصطناعي تقع في مناهج وهي تكرار الذكاء اللانساني ولايزال هدفاً بعيداً حل مشكلة المهام المكثفة للمعرفة عمل اتصال ذكي بين الادراك والفعل وتحسين الاتصال الانساني الإنساني والانساني الحاسوبي والحاسوبي الحاسوبي.

مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الرابع الثلاثون – حزيران ٢٠٢٤– ذي الحجة ١٤٤٥
ISSN-2536-0027

على الرغم من إمكانية استعمال التعريف الاصلي للذكاء الاصطناعي على أنه قدرة الآلة على التفكير أو التصرف مثل البشر، إلا أن هناك تعريفا أكثر دقة تم وضعة خلال العقد الأخير، ويتباين تعريف الذكاء الاصطناعي في المطبوعات المختلفة، حيث يعرفه قاموس (ميريام وبستر) على أنه:(فرع من فروع علم الحاسوب يتعلق بمحاكاة السلوك الذكي في أجهزة الحاسوب)

ويمكننا تعريف الذكاء الاصطناعي: هو دراسة كيفية جعل الحواسيب تقوم بأشياء يقوم بها الإنسان بشكل أفضل في الوقت الحالي، والذكاء الاصطناعي هو دراسة وتصميم العملاء الأذكياء(intelligent agents) اذ أن العميل الذكي هو نظام يدرك بيئته ويقدم أفعالا تزيد من فرصة نجاحه في أهدافه.

ثانياً: المجالات العسكرية للذكاء الاصطناعي

تتمثل تلك المجالآت بالآتي: [٣]

١. **المنظومات القتالية في الجيش:** تقوم القوات العسكرية من مختلف البلدان في العالم بتضمين الذكاء الاصطناعي في أسلحتها وأنظمتها الدفاعية والهجومية في مختلف الميادين البرية والبحرية والجوية وأن استخدام هذا المجال سيمكنهم من تطوير أنظمة حرب فعالة تكون أقل اعتمادًا على المدخلات البشرية ويمكن من تحسين أداءها السريع والدقيق النتائج مع الحاجة إلى صيانة أقل.

٢. **الأمن الالكتروني والسيبراني:** لم تعد أغلب المنظومات العسكرية في العالم ميكانيكية العمل فقط بل تحولت في أغلبها الى أنظمة هجينة الكتروميكانيكة أو تعتمد على أجهزة الكومبيوتر بشكل كبير وبالتالي باتت عرضة أكثر للهجمات الإلكترونية ما سيؤدي حتماً الى إلحاق الضرر بهذه المنظومات والى فقدان المعلومات العسكرية السرية والمهمة لذلك يمكن للأنظمة المجهزة بالذكاء الاصطناعي تفير الحماية لهذه المنظومات من خلال حماية الشبكات وأجهزة الكمبيوتر والبرامج والبيانات بشكل مستقل من أي نوع من الوصول غير المصرح به، كما يمكن لأنظمة أمان الانترنت المدعومة بالذكاء الاصطناعي تسجيل أنماط الهجمات الإلكترونية بهدف تطوير أدوات للهجوم المضاد لمعالجتها[٤].

٣. **النقل والدعم:** يمارس الذكاء الاصطناعي دورًا حاسمًا في قطاع اللوجستيات العسكرية والنقل خاصة وأن النقل الفعال للقوات والأسلحة والمعدات والذخيرة والدعم المختلف يشكل ركناً أساسياً في نجاح العمليات العسكرية، لذا يمكن أن يؤدي دمج الذكاء الاصطناعي في هذا المجال إلى خفض تكاليف النقل وتقليل الجهود التشغيلية البشرية كما ويمكّن القوات العسكرية من اكتشاف مكامن الخلل بسهولة والتنبؤ بسرعة قبل وقوع أي حدث مفاجئ.

٤. **التعرف على الأهداف**: يعتبر هذا التطبيق من أهم ما يعمل عليه حالياً في كل الميادين حيث يتم تطوير تقنيات الذكاء الاصطناعي لتعزيز دقة التعرف على الهدف في بيئات قتال معقدة ما يساعد الجنود او المنظومات على التعرف على الأهداف وتحسين قدرتهم على تحديد مواقعها بسرعة من أجل تحييدها بدقة.

٥. **الاستغناء عن الوجود البشري:** كما يعتبر هذا التطبيق أيضاً من أكثر المجالات استخداماً حيث يعتمد على الروبوتات في تنفيذ العمليات العسكرية الخطيرة مثل تصوير مناطق جغرافية معينة أو تفكيك الألغام أو حتى قصف وقنص أهداف محددة في أماكن مكشوفة كما تقوم بعض الدول بدمج الذكاء الاصطناعي مع الأنظمة الجراحية الروبوتية والمنصات الأرضية الروبوتية لتوفير الدعم الجراحي عن بُعد وأنشطة الإخلاء.

مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الرابع الثلاثون – حزيران ٢٠٢٤– ذي الحجة ١٤٤٥
ISSN-2536-0027

٦. **محاكاة ساحات القتال والتدريب:** تعد منظومات المحاكاة والتدريب من أقدم المنظومات التي تستخدم تقنيات الذكاء الاصطناعي حيث توفر للجنود الفرصة في التعرف والتدرب واتقان استخدام أنظمة القتال المختلفة من خلال أنظمة ميكانيكية وتكنولوجية معقدة تحاكي الواقع الميداني.(٥)

٧. **الرصد والانذار المبكر:** يمكن تشغيل الأنظمة غير المأهولة المستخدمة (روبوتات طائرات بدون طيار) لتنفيذ مهام الرصد والاستخبارات عن بُعد أو إرسالها على طريق محدد مسبقً، الامر الذي سيساعد الوحدات العسكرية من تأمين مراقبة متطورة للتهديدات وتوفير الإنذار المبكر والمعلومات الميدانية الدقيقة.

ثالثاً: الحروب السيبرانية كأحد مهددات الذكاء الاصطناعي في المجال الامني

ترتبط نشأة الحروب السيبرانية بحدثين مهمين يتعلق الأول باستحداث أجهزة الكمبيوتر في منتصف الخمسينيات من القرن المنصرم كأداة لمعالجة وحفظ المعلومات رقمياً رافقته تضافر جهود عدد من الشركات الخاصة والعامة توج بتطوير وحدة المعالجة المركزية (CPU) وذلك لتسهيل المهام الموكلة له وقد تطور ذلك بصورة جذرية في العقود اللاحقة حتى أصبح جهاز الكمبيوتر أساساً في عمل الكثير من المؤسسات الخاصة والعامة فضلاً عن الحياة اليومية للأفراد أما الحدث الثاني فهو يظهور الشبكة العنكبوتية (الانترنت) والذي احدث انقلاباً مثيراً في حياة البشرية من خلال التواصل ونقل المعلومات بسرعة فائقة عن طريق سيل من البيانات المرسلة عبر الأثير.

١- نشأة الحرب السيبرانية

أحدثت الثورة التكنو معلوماتية ثورة في المجال الإلكتروني وأصبح الفضاء الإلكتروني تبعاً لذلك مرشحاً بقوة لأن يكون ساحة جديدة لصراعات وحروب تدار بأسلحة وأدوات مختلفة تماماً بالشكل والمضمون عن تلك الحروب التي تعتمد على الأسلحة التقليدية وهنا جاء ظهور مسمى الحروب السيبرانية او ما يسمى بحروب القضاء الإلكتروني والتي أصبح لها قواعد اشتباك خاصة مختلفة عن تلك الموجودة في الحروب التقليدية وقد غيرت حروب القضاء الإلكتروني من طبيعة الحرب ذاتها فهي لا تستهدف في غاياتها تدمير الآلات والمعدات العسكرية والقوات البشرية للعدو ولا تهدف للاستيلاء على أرض العدو واحتلالها وإنما الحاق الضرر البالغ بالبنى التحتية بأقل كلفة ممكنة. (٦)

لقد سارعت الدول في وتيرة استخدام الكمبيوتر لتحقيق قفزات نوعية في المجال الأمني والعسكري وذلك في مطلع التسعينيات من القرن المنصرم حتى أطلق البعض عليها مصطلح الحرب السيبرانية الباردة (Cyber Cold War) أو سباق التسلح السيبراني Cyber arms race ولم يكن للهجمات السيبرانية صدى على المستوى الدولي، ونشأت الجريمة السيبرانية أولا على هيئة جرائم طالت المؤسسات المالية والمصرفية فضلاً عن الشركات المتخصصة ببرمجة نظم الاتصالات وقد دأبت الدول على اتخاذ التدابير التشريعية لتجريم الأفعال وتحديد العقوبات.

وقد عالجت الدول ومنها العربية كالعراق و الإمارات و عمان والأردن وسوريا الجرائم السيبرانية من خلال تشريعات جزائية وأخرى تنظيمية في تجريم الدخول غير المشروع إلى المواقع الالكترونية والأنظمة المعلوماتية المملوكة من الغير. (٧)

ان الأثر المترتب في اللجوء إلى الحروب السيبرانية يختصره الخبير الروسي ديمتري كريجوروف بأنه يتجسد في التهديد على المستوى العسكري والسياسي فضلاً عن التهديدات الإجرامية والإرهابية التي يمكن

مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الرابع الثلاثون – حزيران ٢٠٢٤– ذي الحجة ١٤٤٥
ISSN-2536-0027

لمجموعات من غير الدول تبنيها لأجل الحصول على مزايا سياسية أو اقتصادية لقد تنبه إلى هذا الموضوع الكثير من المختصين فركزوا عليه بالبحث والتحليل في نطاق النزاعات المسلحة عموماً.

٢- تعريف الحروب السيبرانية

سنتطرق في هذا المحور الى الجهود الفكرية لعدد من المعنيين بدراسة حروب القضاء الإلكتروني منها ما تقدم به (جون أركويلا وديفيد رون) اللذان عرفا حروب القضاء الإلكتروني بأنها: إجراء أو استعداد لإجراء عمليات عسكرية بالاعتماد على المبادئ والآليات المعلوماتية ما يعني تعطيل أو تكمير نظم المعلومات والاتصالات في الدولة العدو، كما عرفتها (ماريا روزاريا تاديو) الباحثة في معهد أكسفورد للإنترنت بأنها: حرب تركز على استخدامات معينة لتكنولوجيا المعلومات والاتصالات ضمن استراتيجية عسكرية هجومية أو دفاعية أقرتها الدولة وتهدف إلى التعطيل الفوري أو السيطرة على موارد العدو والتي تشن داخل بيئة المعلومات مع أهداف تتراوح ما بين الصعيد المادي والمجالات غير المادية والتي قد يختلف مستوى الدمار فيها حسب طبيعة وحجم الهجوم،[٨] وعرفها (عبد القادر محمد فهمي): بأنها هجمات تستخدم فيها المنظومة الشبكية والأجهزة الحاسوبية للدولة أو الفاعلين من غير الدول لتعطيل كفاءة السيطرة والقدرة على التحكم في منظومة أجهزة أو شبكات الحاسوب وما تتضمنه من بيانات ومعلومات للفاعلين الآخرين من الدول وغير الدول أو تقليلها أو حتى تدميرها سواء كان ذلك على مستوى البنية التحتية الوطنية للدولة أو على مستوى منظومات قوتها العسكرية وبالشكل الذي يعرض الأمن القومي للدولة إلى تهديد جسيم، وقدعرفت وزارة الدفاع الامريكية الحروب السيبرانية بانها توظيف القدرات السيبرانية وذلك بهدف تحقيق غرض أساسي يتمثل في تحقيق الأهداف أو الآثار العسكرية في الفضاء السيبراني أو من خلاله.[٩]

يمكن الاستدلال بان الحروب السيبرانية لها أدوات جديدة ومسرح جديد و ميدان جديد هو الفضاء الإلكتروني والذي يمكن تعريفه بأنه المجال الخامسة للحرب يُضاف إلى المجالات التقليدية الأربعة البحر اليابسة الجو الفضاء وهو يشير إلى البيئة التي أنشأها التقاء الشبكات التعاونية لأجهزة الحاسوب والبنى التحتية للاتصالات المستخدمة لربطها وكل ما يتصل بهذه الشبكات من معدات وأجهزة يتم التحكم بها من خلالها.

عرفت وزارة الدفاع الأمريكية الحرب السيبرانية بأنها: توظيف القدرات السيبرانية حيث يكون الغرض الأساسي هو تحقيق الأهداف والآثار العسكرية في القضاء السيبراني أو من خلاله" يضيف تقرير خدمة أبحاث الكونغرس لعام ٢٠٠١ يمكن استخدام مصطلح الحرب السيبرانية لوصف الجوانب المختلفة للدفاع، ومهاجمة شبكات المعلومات والحواسيب في الفضاء السيبراني فضلاً عن حرمان الخصم من القدرة على العمل.[١٠]

ووفق القرار الصادر عن مجلس الأمن الدولي مؤخرا الحرب السيبرانية في استخدام أجهزة الحاسوب و الوسائل الرقمية من قبل حكومة أو معرفة أو موافقة صريحة من تلك الحكومة ضد دولة أخرى أو ملكية خاصة داخل دولة أخرى بما في ذلك الوصول المتعمد أو اعتراض البيانات أو نمو البلية التحتية الرقمية والحج وتوزيع الأجهزة التي يمكن استخدامها لتحريب النفط المحلي، وتعني ايضاً تشاط متماثل أو غير متماثل دفاعي أو هجومي على الشبكة الرقمية من قبل فواعل دولية او غير دولية يهدف لـ الحاق الضرر بالبنية التحتية الحيوية الوطنية والأنظمة العسكرية" والتأثير على إرادة وقدرات صنع القرار في القيادة السياسية العلم والقوات المسلحة، أو مواقف السكان المدنيين في مسرح العمليات على مستوى نظم المعلومات.[١١]

٣- خصائص الحروب السيبرانية

مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الرابع الثلاثون – حزيران ٢٠٢٤– ذي الحجة ١٤٤٥
ISSN-2536-0027

جاء التحول المتزايد من قبل الدول والفاعلين السياسيين نحو الاعتماد بصورة متزايدة على خيار المواجهة في الفضاء الإلكتروني سبب ما تتمتع به من خصائص ويأتي في مقدمتها انخفاض تكلفة المواجهة فيها نسبيا بالمقارنة مع الحروب التقليدية فهي لا تحتاج المعدات وجيوش مجهزة كما أن احتمالية وقوع الضحايا والخسائر البشرية في صفوف القوة المهاجمة تكون منعدمة وبالتالي فإن التوجه المتزايد نحوها يأتي من مبدأ السعي لتحمل أقل كلفة مع إلحاق أكبر ضرر، تتضمن هذه الهجمات تحقيق مبدأ إخلاء المسؤولية وذلك بالنظر إلى صعوبة تحديد الجهة والمكان الذي صدر منه الهجوم وكذلك إمكانية التلاعب والتمويه العالية فيما يتعلق بمصدر ومكان توجيه وشن الهجوم الإلكتروني إضافة إلى إمكانية استخدام سلسلة من الوكلاء في شن الهجوم بما يبدد أي احتمالية تتبع مباشر للدولة صاحبة القرار في شن الهجوم من ناحية أخرى.(١٢)

استدعت الحروب السيبرانية حدوث تغيرات على مستوى الأهداف وعلى مستوى الفاعلين من ناحية الأهداف فإن هذه الحروب تتجه نحو استهداف متنوع من الأهداف فهي تستهدف البنى التحتية المدنية ولا تقتصر على العسكرية، والأساس في الهدف بالنسبة لها هو أن يكون مرتبطاً بشبكات المعلومات وهو ما بات يتوافر بشكل متزايد في شتى مناحي الحياة والمصالح الحيوية حول العالم وذلك بفعل التحول المتسارع نحو الرقمنة المختلف الأنشطة والمنشأت بحيث باتت التعاملات التجارية معتمدة على الفضاء الإلكتروني وكذلك الصحة والتعليم وصولاً حتى شبكات المياه والكهرباء وكذلك المؤسسات والمعاملات الحكومية.

ان ذلك ادى إلى توسعة بنك الأهداف المتاحة أمام هجمات أسلحة الفضاء الإلكتروني وجعل من مخاطرها متعدية للمواقع العسكرية إذا تتعداها إلى استهداف البنى التحلية والحساسة في البلدان المستهدفة وهو أمر أصبح واقعاً في نقل القدرة على استهداف شبكات الكهرباء والمياه والطاقة وشبكات النقل والنظام المالي والمنشآت الصناعية بواسطة فيروس يمكنه إحداث أضرار مادية حقيقية تؤدي إلى وقوع انفجارات أو دمار هائل وكمثال على ذلك، هجوماً على أنظمة التحكم بشبكات المواصلات قادر على إيقاع حوادث تصادم القطارات والسيارات وبحيث تكون خسائرها البشرية والمادية كبيرة كذلك الهجوم على أنظمة التحكم الجري إذ بالإمكان أن يؤدي إلى إسقاط الطائرات من الجو أو الهجوم على منشأت الطاقة حيث يمكن أن يؤدي إلى إيقاع حوادث كبرى والهجوم على محطات تزويد الكهرباء والمياه يمكن أن يؤدي إلى تعطيل خدمات المياه والكهرباء عن مدن بأكملها وكل ذلك يتم دون إطلاق رصاصة واحدة ما يمكن اعتباره بمثابة عملية تدمير صامتة وخلفية. (١٣)

تصاعدت خطورة مثل هذه الهجمات مع تحوّل معظم قطاعات الاقتصاد نحو الرقمنة وبحيث باتت تعتمد على التكنولوجيا من البنوك والتعاملات المالية إلى قطاع الاتصالات إلى قطاع التجارة الإلكترونية المتنامي وكذلك مع الاعتماد والانتشار المتزايد للمعلومات وتداولها عبر الشبكات حيث بات بإمكان الدولة المهاجمة بث الفوضى المعلوماتية في البلد المستهدف عبر نشر معلومات مغلوطة قد تكون ذات تأثيرات وارتدادات سياسية بالغة كما قد يحصل مثلاً في فترة الانتخابات. (١٤)

تركت حروب القضاء الإلكتروني تأثيرات هامة في طبيعة المواجهات حيث بات بالإمكان أن يكون هناك أطراف فاعلة من غير الدول إذ أن الأسلحة المستخدمة في هذه الحروب ليست حكراً بين الدولة، اذ بات يتردد وصف حروب الفضاء الإلكتروني بأنها حروب غير تناظرية وذلك عائد إلى التكلفة المتدنية نسبياً للأدوات اللازمة لشن هكذا حروب، فمن اجل انخراط طرف من غير الدول فليس هناك حاجة لأن يقوم بتصنيع اسلحة مكلفة جداً مثل حاملات الطائرات والمقاتلات المتطورة لتفرض تهديداً خطيراً وحقيقياً على الاطراف الأخرى وإنما يكفي تطوير البرمجيات اللازمة وامتلاك الأجهزة الحاسوبية وهكذا بات بإمكان

مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الرابع الثلاثون – حزيران ٢٠٢٤– ذي الحجة ١٤٤٥
ISSN-2536-0027

وصف المجال الإلكتروني للمواجهات باعتباره ليس حكراً على الدول فقط ولكن أيضاً تنخرط فيه الجهات الفاعلة من غير الدول.

تعتبر نماذج الردع المعروفة في الحروب التقليدية والحروب غير التقليدية (النووية والبيولوجية والكيميائية) تفشل في هذه الحروب فهي غير ممكنة في العالم المعلوماتي إذ يتعذر إظهار القوة الإلكترونية المهاجمة بحيث يتم ردع العدو عن الهجو فالردع بالانتقام أو العقاب لا ينطبق على هذه الحروب على عكس الحروب التقليدية حيث ينطلق الصاروخ المهاجم على سبيل المثال من أماكن محددة يتم رصدها ومن ثم يكون بالإمكان الرد على الجهة المهاجمة. خلافاً لما هو الحال عليه في حروب الفضاء الإلكتروني. (١٥)

يكون من الصعوبة بمكان بل ومن المستحيل في كثير من الأحيان تحديد مصدر الهجمات الإلكترونية وحتى إذا ما تم تتبع مصدر الهجمات الإلكترونية وتبيّن أنها تعود إلى دول محددة أو فاعلين غير حكوميين فإنه في هذه الحالة لن يكون لديهم قواعد أو فضاءات مادية حتى يتم الرد إليها عبر استهدافها كما أن بعض الهجمات قد تتطلب أشهراً لرصدها وهو ما يلغي مفعول الردع بالانتقام عبر توجيه ضربة تالية للضربة الأولى التي وجهها الطرف البادئ بالهجوم.

يقترن بهذه الخاصية خاصية أخرى تميز حروب القضاء الإلكتروني من الحروب التقليدية وهي أنه لا توجد حدود جغرافية واضحة في هذه الحروب كما لا يتواجد مفهوم المبادلاء بمعناه السالك في العالم الواقعي بحيث يتم منع الأطراف الأخرى من الدخول إلى المناطق الخاضعة لسيادة دولة ما مثلاً بل إنه بالإمكان وصف الحدود في القضاء الإلكتروني بأنها حدود مانعة وبالأحرى فإنه لا توجد حدود في العالم الافتراضي. (١٦)

الحدود للداخل مع بعضها حيث أن كل الدول صغيرة وكبيرة تشترك في نفس الشبكات التي يمكن اعتبارها بمثابة سحابة واحدة وحتى خوادم الشبكات تكون في كثير من الأحيان موجود في بلدان أخرى غير البلدان المستخدمة لها والمشغلة لها وبالتالي فإنه بالإمكان التأكيد على أن مفهوم السيادة في العالم الإلكترونية مفهوم مانع وذلك مما يقتضيه طبيعة العالم الافتراضي المتداخلة، تتمتع هذه الحروب من خصائص و مميزات جعلتها ذات طبيعة مختلفة من المواجهات في الحروب التقليدية فإن قواعد الاشتباك فيها لا تنطبق على قواعد الاشتباك المتبعة في الحروب التقليدية وبالحديث عن قواعد الاشتباك في العالم الافتراضي فإنه بالإمكان الحديث عن مراحل تسير وفقها وهي:

أ. **مرحلة التحضير للحرب:** يسود فيها عمليات التجسس والاستطلاع وجمع المعلومات وتطوير البرمجيات وتجديد المخترقين.

ب. **مرحلة التصعيد:** يجري فيها الهجوم على الأهداف ضمن هجمات متفرقة ومتباعدة سواء أكانت شخصيات أو مؤسسات والتي تتم وفق ما تم إعداده وجمعه أثناء تحضير بنك الأهداف الإلكترونية والتي تتنوع ما بين استهداف أنظمة القطاع الخاص أو استهداف أنظمة القطاع العام والمرافق العامة وفي هذه المرحلة تتخذ الهجمات شكل عمليات الاختراق للمواقع الإلكترونية وقواعد البيانات المستهدفة ومن ثم المباشرة في تخريبها أو مسحها أو سرقة المعلومات منها أو التجسس عليها أو تعطيل المواقع جملة والعبث بما يرتبط بها من أنظمة وحسابات.

ج. **مرحلة الحرب الالكترونية:** يكون هناك تنظيمات معترفة ومدربة تدريبا جيداً ولديها الموارد والأماكن المجهزة والأجهزة والمعدات والبرمجيات اللازمة والتي تقوم بتوفيرها الدول المنخرطة فيها وفي هذه المرحلة تستخدم الأسلحة الإلكترونية بغرض الحاق أضرار مادية

مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الرابع الثلاثون – حزيران ٢٠٢٤– ذي الحجة ١٤٤٥
ISSN-2536-0027

بالغة بمنشأت العدو بما في تلك المدانية والعسكرية منها بحيث يكون هناك أضرار مادية واسعة وملموسة تنجم عن الهجمات الإلكترونية وعادة ما تكون هذه المرحلة موازية لحرب ومواجهة عسكرية تقليدية لتكون بمثابة موالية من الميدان الافتراضي للميدان العسكري. (١٧)

اما فيما يخص طبيعة الأسلحة والأدوات المستخدمة وأنواعها في الحرب الإلكترونية فإن القوة الإلكترونية تعمد بصفة أساسية على الأجهزة والجامع الأجهزة تشتمل على أنظمة الحاسوب مثل وحدة المعالجة المركزية(CPU) أو محرك الألتراس العضونية (CD Drive) أو لوحة المفاتيح أو الثنائية وكذلك الكابات والأقمار الصناعية، اما البرامج فهي الصياغات البرمجية المستخدمة لتوجيه عمليات الحاسوب وفي هذه الحروب يتم استخدام البرامج الضارة والفيروسات مثل لغة الاستعلام الميكانية (SQL) وهي مجموعة من التعليمات المستخدمة للتفاعل مع قواعد البيانات وعمليات الحقن الإلكتروني عبر إدخال برمجيات ضارة في الأنظمة الحاسوبية المستهدفات أو البرمجة النصية للمواقع لتشويه صفحات الويب الخاصة بالعدو واتلافها، يستحوذ هذا الشكل من الفيروسات على الموقع لبضع ساعات أو أيام ويقوم بعرض صور ونصوص تهدد الضحية وتسيء له كما حصل في الهجوم الإلكتروني الروسي على إستونيا إثر نزاع الجندي البرونزي عام ٢٠٠٧ عندما هاجم قراصنة روس مواقع تابعة للحكومة الإستونية على إثر قرارها بإزالة تمثال جندي يرمز للحقبة السوفيتية وذلك ضمن أساليب ناعمة يكون لها آثار نفسية كبيرة.(١٨)

تبرز الاختراقات كأحد أهم أساليب الهجوم في الحرب الإلكترونية وهي تعتمد على برامج فعالة السرقة المعلومات الحساسة كذلك هناك تكتيك الحرمان من خدمة الموزع ويؤدي هذا النوع من الهجمات دوراً رئيسياً عبر محاولة جعل مورد الحاسوب غير متوفر للمستخدمين المقصودين به وتتنوع البرمجيات المستخدمة في عمليات التسلل والاختراق ومن أهمها: القنابل المنطقية والتي هي عبارة عن هو قطع من التعليمات البرمجية المدرجة عمداً في نظام برمجي يقوم بإطلاق وظيفة ضارة عند استيفاء شروط محددة والفيروسات والديدان الحاسوبية. (١٩)

نظراً إلى كونها أدوات جديدة وتتطور بسرعة وباستمرار فإنّ ذلك يجعل من يزيد من تعذر إسناد الهجمات الإلكترونية إلى جهات فاعلة إذ أن البرامج المستجدة تحتاج باستمرار إلى التعرف عليها وفك شيفرتها هذا بالإضافة إلى القيود التقنية المتضمنة في البرامج ذاتها والتي تمنع ضحية الهجوم الإلكتروني من التعرف على المهاجم.

يمكن الاستدلال بان الحرب السيبرانية يسود فيها حالة من ضباب الحرب وعدم القدرة على ردع المعتدل المحتمل (مجهول الهوية) ما يستدعي تطوير مقاربات جديدة للخطط والاستراتيجية العسكرية وان جوهر العقيدة العسكرية في الفضاء السيبراني تقوم على أساس السعي لكسب الحروب من خلال ضرب القلب الاستراتيجي للهياكل الالكترونية للخصم وذلك مع الاستمرار في تطوير استراتيجيات وقدرات للحماية عبر تطوير أنظمة الدفاع السيبراني والدروع.

ثالثاً: الإرهاب السيبراني وتهديد المنظومة العسكرية للدول

١. مفهوم الارهاب السيبراني

ينطلق تعريف الارهاب السيبراني من تعريف الارهاب حيث لا يختلف كلاهما الا في نوعية الاداة أو الوسيلة المستخدمة لتحقيق العمل الارهابي . وكانت بداية استخدام مصطلح الإرهاب الالكتروني Cyber Terrorism في فترة الثمانيات على يد باري كولين Barry Collin) والتي خلص فيها إلى صعوبة تعريف شامل للإرهاب التكنولوجي. ولكنه تبنى تعريفاً للإرهاب الالكتروني مقتضاه ، بأنه هجمة الكترونية غرضها تهديد الحكومات أو العدوان عليها، سعياً لتحقيق أهداف سياسية أو دينية أو أيديولوجية، وأن الهجمة

مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الرابع الثلاثون – حزيران ٢٠٢٤– ذي الحجة ١٤٤٥
ISSN-2536-0027

يجب أن تكون ذات أثر مدمر وتخريبي مكافئ للأفعال المادية للإرهاب. ويعرفه **جيمس لويس** (James Lewis) على أنه " استخدام أدوات شبكات الحاسوب في تدمير أو تعطيل البنى التحتية الوطنية المهمة مثل : الطاقة والنقل والعمليات الحكومية، أو بهدف ترهيب حكومة ما أو مدنيين.[٢٠]

أما دورثي دينينغ Dorothy Denningg وهي من أبرز الباحثين في مجال الأمن الالكتروني ، ترى أن الإرهاب الالكتروني هو الهجوم القائم على مهاجمة الحاسوب وأن التهديد به يهدف إلى الترويع أو إجبار الحكومات أو المجتمعات لتحقيق أهداف سياسية أو دينية أو عقائدية وينبغي أن يكون الهجوم مدمراً وتخريبياً ، لتوليد الخوف بحيث يكون مشابه للأفعال المادية للإرهاب.[٢١]

فالإرهاب الالكتروني هو احد الاستخدامات الغير سلمية للفضاء الالكتروني وهو نتيجة لتفاعل العالم المادي مع العالم الافتراضي ، لذا من الصعب الوصول الى تعريف محدد لظاهرة الارهاب الالكتروني فهو يمثل استخدام الفضاء الالكتروني كأداة لألحاق الضرر بالبنية التحتية للدول سواء كانت طاقة او خدمات حكومية أو منشآت سيادية ، فهي هجمات تستخدم ضد الاقتصاد والحكومات بأهداف أغلبها سياسية من اجل تدمير نظم المعلومات لدى الخصم وافقاده القدرة على التواصل مع اعضائه عن طريق تدمير مواقعه الالكترونية واختراق شبكات معلوماته الرسمية في الوزارات والحكومات بغرض الحصول على معلوماته السرية. [٢٢]

ويمكن تعريف الارهاب السيبراني بأنه هجمة الكترونية غرضها تهديد الحكومات أو العدوان عليها سعياً لتحقيق اهداف سياسية أو دينية أو ايدلوجية ونتج عنا آثار تخريبية مدمرة مكافئة لآثار الافعال المادية للإرهاب، عُرف الارهاب السيبراني بأنه هجمات غير مشروعة أو تهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزونة الكترونياً توجه من اجل الانتقام أو الابتزاز أو اجبار أو التأثير في الحكومات أو الشعوب أو المجتمع الدولي باسره لتحقيق اهداف سياسية أو دينية أو اجتماعية معينة نخلص من كل ما تقدم بأن الارهاب السيبراني هو: هجمات غير مشروعة ضد الحاسبات والشبكات أو المعلومات المخزونة توجه من اجل الانتقام أو التأثير في الحكومات بدوافع سياسية أو دينية أو اجتماعية.[٢٣]

٢. التجسس السيبراني

اكتسبت الصراعات السياسية والعسكرية والاقتصادية بين الدول بعدا إلكترونيا بحيث يصعب التنبؤ بحجمها وتأثير الها بل أن الحروب التي تدور رحاها في الفضاء السيبراني أكثر أهمية من الأحداث التي تجري على أرض الواقع ذلك أن الإنجازات المذهلة للتجسس السيبراني أظهرت المكاسب الكبيرة لعمليات احتراق أجهزة الكمبيوتر مقارنة بارتفاع أشكال التجسس التقليدية التي تتطلب ذكاء بشري وارتفاع نسبة الخطورة مما جعل التجسس السيراني على الساحة العالمية مصدر قلق للدول على أمنها الوطني، ان التجسس السيبراني يعني تلك المحاولات المتعمدة لاختراق أجهزة الكمبيوتر والمواقع الإلكترونية التابعة للدولة المناولة أو الخصم بهدف سرقة معلومات سرية ويهدف للحصول على بنك معلومات هائلة عن المنظومات والأسرار العسكرية والسياسية والأمنية والاقتصادية والصناعية والتي تعتمد بشكل كامل في عملها على وسائل ومنظومات التواصل والاتصال التكنولوجي الحديث داخل الدول.[٢٤]

التجسس المعتمد على المجال السيبراني يؤثر سلبا على المعلومات وأنظمة المعلومات مما يتيح إمكانية تسريب أسرار ومعلومات حساسة للدول الأخرى وتجدر الإشارة إلى أن أجهزة الاستخبارات السيبرانية لا يقتصر على وجهة النظر الرسمية للدول والحكومات بل يتعدى ذلك لدور الأفراد في إنتاج المعلومات وترويجها وفي توفير كم كبير للملفات السياسية والاقتصادية مع تعدي الحدود الدولية عكفت أجهزة استخبارات الدول للحصول عليها أولا والبحث فيها ثانيا وتوظيف نتائجها ثالثا. [٢٥]

مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الرابع الثلاثون – حزيران ٢٠٢٤– ذي الحجة ١٤٤٥
ISSN–2536–0027

يتمثل أحد الأمثلة على التجسس العسكري في قيام هاكرز بالتسلل إلى جهاز أحد المتعاقدين مع الجيش الأمريكي وسرقة آلاف الملفات الخاصة بالمقاتلة أف - ٣٥ وتتمثل المعلومات الاقتصادية التي يتم عادة استهدافها في براءات الاختراع وحقوق الملكية الفكرية أو المواقف التفاوضية للدول وتجدر الإشارة أيضا إلى حالات تجسس أخرى يذكر منها في هذا الإطار ما تناولته مجلة دير شبيغل الألمانية في ١٧ أوت ٢٠١٤ من أن الاستخبارات الألمانية قد تجسست أكثر مرة على محادثات وزير الخارجية الأمريكية في تلك الفترة، بينما تجسست على تركيا لعدة سنوات ونشرت معلومات حول قيام وكالة الأمن القومي الأمريكية بالتجسس على نحو ٣٥ من القادة على مستوى العالم وأكثر من ٦٠ مليون مكالمة هاتفية في دول مختلفة من بينها دول أوروبية وهي حادثة كشفت عن أن التجسس لم يعد يشمل قاطني الدولة بل يمتد إلى قاطني دول أخرى وقادتهم الذين هم بالأساس حلفاء مع الدولة مما يزيد من عدم الثقة بين الحفاء.[٢٦]

أعلن أمين مجلس الأمن الروسي نيكولاي باتروشيف في ٢٦ أوت ٢٠١٥ على العثور على برامج تابعة للاستخبارات الأجنبية في نظم المعلومات للمؤسسات الحكومية الروسية وأكد على تزايد حالات التجسس على نظم المعلومات الحكومية وفي واقعة مماثلة قامت شبكة دولية ضخمة للتجسس السيبراني تعمل تحت إشراف وكالة الأمن القومي الأمريكية بالتعاون مع أجهزة الاستخبارات في كندا وبريطانيا وتجدر الإشارة إلى أنه لا يقتصر الرصد على المحطات الموجهة إلى الأقمار الصناعية والشبكات الدولية بل يشمل الاتصالات التي تجري عبر أنظمة الاتصالات الأرضية.[٢٧]

يُذكر في هذا المقام ما تناولته فضيحة برنامج بيغاسوس (Pegasus Project) الذي طورته شركة Group NSO الإسرائيلية والذي استخدمته أنظمة سياسية عدة حول العالم ضد خصومها ومعارضيها وهو برنامج احتراق وتجسس تم تسويقه الى حكومات دول العالم ولديه القدرة على احتراق مليارات الهواتف التي تعمل بأنظمة تشغيل IOS أو أندرويد (Android).

ازدادت قدرات برنامج بيغاسوس تقدما وأصبح بإمكانه الوصول إلى أهدافه عن طريق ما يسمى الهجمات الخالية من النقر (zero-click) التي لا تتطلب أي تفاعل من مالك الهاتف ليتمكن من اختراقه وغالبا ما تستغل هذه الهجمات ثغرات الفحمات دون انتظار (zero day) وهي عيوب أو أخطاء في نظام التشغيل لا تكون الشركة المصنعة للهاتف المحمول قد اكتشفتها وبالتالي لا تتمكن من إصلاحها وقد بذلت شركة NSO Group جهودا كبيرة حتى تجعل برنامجها صعب الكشف وأصبح من الصعب جدا الآن التعرف على هجمات بيغاسوس.[٢٨]

كشف تقرير نشرته عدة وسائل إعلام غربية كبيرة في العام ٢٠٢١ أن ناشطين وصحافيين وسياسيين حول العالم قد تعرضوا لعمليات تجسس بواسطة برنامج بيغاسوس ويستند التقرير إلى قائمة حصلت عليها منظمتا فوربيدن ستوريز والعفو الدولية[٢٩] حيث أظهر عن تسرب بيانات ٥٠٠٠٠ من أرقام الهواتف التي كان أصحابها مستهدفين للمراقبة منذ سنة ٢٠١٦ ومن بين المستهدفين لهذا التجسس رؤساء دول نشطاء وصحفيون بما في ذلك عائلة الصحفي السعودي جمال خاشقجي ومن خلال البيانات المسربة والتحقيقات التي أجرتها منظمة القصص المحظورة وشركاؤها الإعلاميون أمكن لهم تحديد العملاء المحتملين المجموعة شركة Group NSO في ١١ بلدا هي أذربيجان والبحرين والبحر والهند وكازاخستان والمكسيك والمغرب ورواندا والسعودية وتوغو والإمارات العربية المتحدة.[٣٠]

فضلاً عن ان مصطلح الاستغلال السيبراني له علاقة بالجوسسة والذي يشير إلى الأنشطة المتعمدة المصممة لاحتراق أنظمة أو شبكات الحاسوب التي يستخدمها الخصم وذلك بقصد الحصول على معلومات موضوعة على هذه الأنظمة والشبكات أو يجري تداولها من خلالها ولا يسعى الاستغلال السيراني إلى تعطيل التشغيل

مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الرابع الثلاثون – حزيران ٢٠٢٤– ذي الحجة ١٤٤٥
ISSN-2536-0027

المعتاد النظام أو شبكة حاسوب من وجهة نظر المستخدم وإنما أفضل استغلال سيبراني هو الاستغلال الذي لا يلاحظه المستخدم أبدا والمعلومات المطلوبة هي بوجه عام المعلومات التي يريد الخصم أن لا يتم الكشف عنها.

تقوم الدولة بعمليات استغلال سيبراني لجمع معلومات استخباراتية قيمة مثلما قد تنشر جواسيس من البشر لأداء هذه المهمة كما وقد تسعى إلى الحصول على معلومات من شبكة حاسوب شركة في بلد آخر لتستفيد منها شركة منافسة محلية في ذلك البلد ومن بين المعلومات التي لها أهمية كبيرة تلك التي تتيح للبلد إجراء مزيد من الاختراقات لأنظمة أو شبكات حاسوب أخرى بغية جمع معلومات إضافية أما بالنسبة للفاعلين الذين قد يقومون بمثل هذه العمليات فإنه نظرا لطبيعة تكنولوجيا المعلومات فإن نطاق الفاعلين سواء على المستوى الوطني الفعلي أو الدولي قد يكونوا من الفاعلين الدول أو الأفراد (القراصنة) أو الوكلاء السيبرانيون أو جماعات إرهابية تعمل بشكل منفرد أو القطاع الخاص المدني.[٣١]

ان الهجوم السيبراني ليس غاية في حد ذاته ولكنه وسيلة قوية لمجموعة متنوعة من الغايات من الدعاية إلى التجسس ومن تعطيل الخدمات إلى تدمير البنية التحتية الحيوية وتجدر الإشارة إلى أنه لم يحدث تغير في طبيعة التهديد للأمن الوطني إلا أن الأنترنت قد وفرت آلية جديدة يمكنه من زيادة سرعة الهجوم وحجمه وقوته ذلك أن انتشار الأنترنت وتزايد اعتماد العالم عليه سيترتب على الإضرار به تداعيات سياسية واقتصادية وعسكرية ملموسة سيما بعد التطور اللافت للهجمات السيبرانية كنتيجة طبيعية للنزاعات في العالم الحقيقي سيؤدي دوراً رئيسيا في النزاعات المستقبلية.[٣٢]

رابعاً: التحديات الامنية للدول في مواجهة مخاطر الذكاء الاصطناعي

١- استهداف البنى التحتية للدولة

يتم استهداف البنية التحتية للدول سواء كانت مدنية أو عسكرية لهجمات إلكترونية بما يؤدي إلى شلل أنظمتها وتدمير أنظمة التشغيل الخاصة بها والتأثير على تدفق المعلومات بما يؤدي إلى إرباك عمل البنية التحتية الحيوية وينشأ عن مثل هذه الهجمات تعطيل العديد من مرافق الحياة في الدول وسيادة الفوضى مثل استهداف محطات الطاقة والوقود والخدمات المالية والمصرفية ونظم الاتصالات والمواصلات ومن أبرز الأمثلة على ذلك تعرض أوكرانيا خلال شهر جوان ٢٠١٧ لهجمة إلكترونية شملت محطات الطاقة.

إضافة إلى البنية التحتية المؤسسات المالية والمؤسسات العسكرية مثل محطات الطاقة النووية كما هو الحال في قيام فيروس ستاكسنت (Stuxnet) بتعطيل حوالي ألف من أجهزة الطرد المركزي في منشأة لتخصيب اليورانيوم في مفاعل تاتيانز في وسط إيران في العام ٢٠١٠ فضلا عن تعرض أنظمة الكمبيوتر لشركة كوريا الجنوبية للطاقة المائية والنووية التي تديرها الدولة لهجمات إلكترونية في شهر ديسمبر ٢٠١٤ واتهمت الولايات المتحدة الأمريكية روسيا بالتورط في شن هجمات إلكترونية على شبكات الكمبيوتر في عدة محطات طاقة نووية.

لقد ربطت انقطاعات الكهرباء المتعددة في البرازيل بهجمات سيبرانية أيضا ففي عام ٢٠٠٨ تمكن القراصنة من الدخول إلى الموقع الشبكي للحكومة والسيطرة عليه لمدة تزيد عن أسبوع حيث توضح انقطاعات الكهرباء في البرازيل الاتساع المحتمل للأنواع الجديدة من الهجمات السيرانية وجاء في التقارير تشبيه المشهد بفيلم من أفلام الخيال العلمي حيث توقفت تماما قطارات الأنفاق وإشارات المرور وثاني أكبر محطة إنتاج قوى كهربائية وهو سد إيتابيو وتأثر أكثر من ٦٠ مليون شخص جراء ذلك.[٣٣]

تعرضت شبكات الكهرباء في الولايات المتحدة الأمريكية أيضا لمثل هذه الهجمات في شهر ف يالعام ٢٠٠٩[٣٤] وتجدر الإشارة أيضا إلى أحمد الهجمات السيبرانية الشائعة والمعروفة على البنية التحتية الحيوية

مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الرابع الثلاثون – حزيران ٢٠٢٤– ذي الحجة ١٤٤٥
ISSN-2536-0027

والمتمثلة في الهجوم على خط أنابيب النفط التركي في العام ٢٠٠٨ والذي اشتعلت فيه النيران بطريقة غامضة دون إطلاق أي مستشعرات أو إنذارات على الرغم من أن الانفصاليين الأكراد زعموا بأنهم من تسبب بالهجوم إلا أن عدد من مسؤولي المخابرات الأمريكية قد أدانوا روسيا التي عارضت إنشاء خط أنابيب الغاز باكو – تبليسي – جيهان لأنه خارج الأراضي الروسية ومن شأنه تقويض قدرتها على التحكم في تدفق الطاقة باتجاه أوروبا.[٣٥]

كما هاجم فيروس الصخرة الدوارة سنة ٢٠١٧ السعودية من طرف قراصنة إيرانيين حيث استهدف قطاع الطيران والبتروكيماويات وقد أحدث هذا البرنامج الخبيث تأثيرات كبيرة على شركات الطيران وشركات البتروكيماويات في السعودية وفي سنة ٢٠١٩ تم تنفيذ هجمات سيبرانية متقدمة مستمرة تدعى أي بي تي وهي هجمات بالغة التأثير مارسها قراصنة سيرانيون إيرانيون لاستهداف شبكات المعلومات وبنيتها التحتية في كل من قطر الكويت السعودية الإمارات والبحرين خلال مدة زمنية متطاولة لضمان بلوغ أهدافها وتعميق مستويات تأثيرها.

٢- اختراق الأنظمة العسكرية وتدميرها

خلال قيام قراصنة محترفين أو حيوش نظامية إلكترونية ووكلاء سيبرانيين بشن هجمات إلكترونية بغرض السيطرة على نظم القيادة والسيطرة عن بعد الأمر الذي يؤدي إلى إخراج بعض منظومات الأسلحة عن سيرة القيادة المركزية وإعادة توجيهها نحو أطراف داخلية أو ضد دول صديقة، يمكن أيضا السيطرة على الطائرات من دون طيار أو الغواصات النووية في أعماق البحار أو السيطرة على الأقمار الصناعية العسكرية في الفضاء الخارجي وإخراجها عن سيطرة الدولة التابعة لها هذه الأسلحة والمعدات إذ تزداد خطورة مثل هذه الهجمات إثر التطور التكنولوجي واعتماد اللوجستيات ونظم القيادة والتحكم وتحديد الأهداف وإصابتها على برامج الكمبيوتر وشبكات الاتصال.

تقوم الهجمات السيبرانية بتدمير أنظمة إلكترونية لمنشآت حيوية عسكرية وتعطيل أو إتلاف شبكات الدفاع العسكرية عن بعد واختراق أو تعطيل أو تدمير شبكات القطاع الخاص ذا الصلة بالقطاع العسكري وكذا التدخل في سلامة البيانات العسكرية الداخلية لدول أخرى والقيام بمحاولات الإرباك والتشويش على أجهزتها.

تحدث الهجومات السيبرانية من أجل سرقة تصميمات الأسلحة العسكرية والتقنيات التكنولوجية الحديثة حيث قام قراصنة صينيون بشن هجمات على شركة لوكهيد مارتين الأمريكية وسرقة معلومات عن تكنولوجيا تصنيع المقاتلة أف – ٣٥ التي استخدمتها الصين فيما بعد لدى تصميم وتصنيع مقاتلة تي ٢٠ الصينية وشملت الهجمات السيبرانية أيضا مقاولين لدى وزارة الدفاع الأمريكية يعملون على صناعة وتطوير الطائرات من دون طيار الأمريكية بهدف سرقة معلومات حول هذه الطائرات وكيفية صناعتها وتطويرها.[٣٦]

٣- سرقة المعلومات العسكرية والتلاعب بها

ويتم ذلك عبر اختراق قواعد البيانات العسكرية وسرقتها او تزييفها او تدميرها الكترونيا اذ تسعى الهجمات الالكترونية في هذه الحالة الى اختراق الشبكات الخاصة بالمؤسسات العسكرية بهدف سرقة خرائط أنظمة التسليح أو التصميمات الخاصة بالمعدات العسكرية وتجدر الإشارة إلى أنه قد انطلقت واحدة من أخطر الهجمات ضد أنظمة حواسب الجيش الأمريكي سنة ٢٠٠٨، خلال وصلة (USB) كانت متصلة بجهاز كمبيوتر محمول تابع للجيش الأمريكي في قاعدة عسكرية موجودة في الشرق الأوسط ولم يتم اكتشاف انتشار برامج التجسس في كل الأنظمة السرية وغير السرية في الوقت المناسب مما شكل ما يشبه جسرا

مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الرابع الثلاثون – حزيران ٢٠٢٤– ذي الحجة ١٤٤٥
ISSN-2536-0027

رقميا تم من خلاله نقل آلاف الملفات من البيانات إلى خوادم خارجية(Servers) وبالمثل تم استهداف أكثر من ٧٢ شركة من بينها ٢٢ مكتبا حكوميا و ١٣ من مقاولي قوات الدفاع بهدف سرقة معلومات حول الخطط والمباني العسكرية.

تعرض العراق في ٢٦ و٢٧ سبتمبر ٢٠١٩ إلى هجوم سيبراني من قبل قراصنة طالت قرابة ٣٠ موقعا حكوميا أبرزها مواقع وزارة الدفاع والداخلية والخارجية والأمن الوطني والصحة وقد استغل المهاجمون بعض الثغرات فعملوا على تطبيق التغييرات على بيانات مواقع البحث التي من شأنها توجيه المستخدمين إلى صفحة بحث مختلفة وعلى الرغم من أن الجهات الحكومية العراقية قد نجحت في استعادة سريعة لبعض المواقع إلا أن بعضها استغرق وقتا أطول علما أن المهاجمين تمكنوا من الدخول إلى أجهزة الحواسيب الحكومية واختراق قواعد بيانات من المفروض أن تكون محمية بشكل جيد مما سمح لهم بأخذ معلومات كثيرة. [٣٧]

يتضح من خلال ما تقدم ان الهجمات السيبرانية متعددة ويمكن ان تشمل التجسس السيبراني وإغلاق النظم المعلوماتية واستهداف أنظمة معلومات الخصم سواء المدنية أو العسكرية ويمكن أن تشمل أيضًا التلاعب بأنظمة توجيه الأسلحة التي قد تتسبب في إطلاق النار بعيدًا عن الأهداف المستهدفة التي قد تشمل: البنية التحتية الحيوية المدنية كشبكة الكهرباء وأسواق الأوراق المالية وقواعد البيانات المالية وخطوط تنقية المياه وغيرها، يشكل كل ذلك خطرًا شديدًا على الدول القومية سواء على اقتصاداتها أو بنيتها التحتية الحيوية أو أنظمتها السرية التي تعتمد على نظم المعلومات. كما يؤثر ذلك سلبًا في القدرات العسكرية للدول خاصة أن الهجمات السيبرانية من شأنها أن تقوم بجمع وتحليل معلومات استخبارية موثوق بها عنها. ولذا فإن ردع تلك الهجمات لا بد أن يكون من أولويات الردع السيبراني.

الخاتمة

شهدت تقنيات الذكاء الاصطناعي تطوراً سريعاً في السنوات الماضية حتى تعددت استخداماتها على المستوى العملي حتى باتت أنظمة الأسلحة الفتاكة المستقلة تُوصَف بالثورة الثالثة في الحرب بعد البارود والأسلحة النووية لما لها من قدرة على تحديد وتدمير أهداف مستقلة دون التدخل البشري المباشر على نحو يؤكد أهميتها في مجال الحروب لا سيما في ظل التغيرات المتوقعة في طبيعة المعارك المستقبلية ومع تعدد التهديدات التي يجب مواجهتها من خلال دفاعات عالية التقنية وأهمية استخدامها في عمليات الاستهداف التلقائي والتحليل الآلي للبيانات الاستخباراتية وتحسين اللوجستيات وغير ذلك.

دفع تعدد استخدامات الذكاء الاصطناعي نحو صعود نهج جديد للحرب يُعرف باسم الحرب الذكية أو الحرب القائمة على الذكاء الاصطناعي، وقد شهدت الحروب بالتوازي مع ذلك تغيرات جذرية على صعيد مهام الاستطلاع والمراقبة والاستهداف والاستخبارات وتوثيق وقائع العمليات العسكرية والدعم اللوجستي لتدفع بعض التحليلات بتعدد المفاهيم العملياتية الجديدة التي تتواكب مع جيل جديد من الحروب بعد أن أضحى المجال المعرفي هو ميدان الحروب في المستقبل لا سيما في ظل التطور التكنولوجي المستمر.

تتعدد مجالات توظيف الذكاء الاصطناعي في الحروب الحديثة حيث يساعد الذكاء الاصطناعي في تحسين جمع المعلومات الاستخبارية والعمليات المستقلة ودعم اتخاذ القرار وربما يقلل التكلفة البشرية الناجمة عن انخراط الدول في صراعات مسلحة، تبين لنا ما لهذه الجريمة من ضرر كبير على المجتمع من خلال استخدام الجماعات الإرهابية أساليب غير تقليدية من اجل ارعاب وتهديد الامن وكذلك القصور التشريعي في معالجة هذي الظاهرة الجرمية الحديثة مما جعلها أكثر صعوبة لما تتصف بها من خصوصية.

مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الرابع الثلاثون – حزيران ٢٠٢٤– ذي الحجة ١٤٤٥
ISSN-2536-0027

ان القوة العسكرية تتعلق في نهاية المطاف بالأشخاص والمنظمات أكثر من الأدوات ويظهر التاريخ أنه حتى الجيوش الأكثر نجاحاً تحتاج إلى دمج قدرات جديدة في خططها إذا أرادت الفوز في ساحة المعركة ومع عودة الحرب التقليدية كما في أوكرانيا ستحتاج الولايات المتحدة إلى التكيف وإعادة هيكلة جيشها من أجل المستقبل.

التوصيات

١. استخدام الذكاء الاصطناعي في عمليات جمع المعلومات من خلال مراقبة اتصالات الخصم، وكذلك يمكن الاعتماد على الأتمتة (التشغيل الآلي) والذكاء الاصطناعي لتحسين الوصول إلى المعلومات ومعالجة وتحليل صور الأقمار الصناعية وتحويل بيانات الاستشعار التي تجمعها أجهزة الاستخبارات ومختلف الكيانات الحكومية والعسكرية إلى منتجات استخباراتية قابلة للاستخدام.

٢. دعم القوات البحرية باستخدام الخرائط الذكية اذ يلعب الذكاء الاصطناعي دوراً في دعم القوات البحرية وتعزيز الأمن البحري من خلال تعزيز الردع والوعي بالمجال البحري باستخدام الخرائط الذكية والأقمار الصناعية وشاشات المراقبة التفاعلية، وهذاما تمارس فيه المسيرات البحرية دوراً مهماً بجانب المركبات المسيرة الغائصة تحت سطح البحر والمركبات غير المأهولة بهدف تنفيذ عدد من دوريات الحراسة وتعزيز قوة الردع ورصد أي نشاط مزعزع لاستقرار الممرات المائية الحيوية إذ يمكن لتلك المسيرات إلى جانب الطائرات من دون طيار أن تقدم رؤية أفضل للمياه لأغراض الاستطلاع في إطار شبكة دفاع إقليمية محتملة.

٣. توظيف الطباعة الثلاثية الأبعاد في الصناعات العسكرية بشكل مباشر حيث يمكن توظيف الطباعة الثلاثية الأبعاد لإنتاج بزات وجلد اصطناعي لمعالجة جرحى الحروب وهو الأمر الذي يفسر كثافة الاستثمارات الأمريكية في هذا المجال.

٤. القيام بمهام التجسس والمراقبة حيث يمكن توظيف الذكاء الاصطناعي في عميات التجسس على نطاق واسع ذلك أن استخدام التكنولوجيات الرقمية الحديثة المتصلة بالشبكات حولتها إلى أدوات هائلة للمراقبة والسيطرة وهو ما يتجلى – على سبيل المثال – في أدوات الاختراق الحاسوبي كبرامج التجسس مثلاً وهو الأمر الذي تتزايد أهميته في تتبع معلومات الخصم العسكرية والكشف عن خططه الميدانية.

٥. توقع اندلاع الحروب المستقبلية تتزايد الأبحاث العلمية الرامية إلى توظيف الذكاء الاصطناعي في التنبؤ بالحروب المستقبلية من خلال إنشاء قواعد بيانات ضخمة تضم بيانات تفصيلية عن الدول وتاريخها ودرجة تسليحها وذلك من بين بيانات أخرى. وبعبارة ثانية يتم استخدام الذكاء الصناعي حالياً في المجال العسكري لوضع سيناريوهات محددة في زمن محدد وجغرافيا محددة وبناءً على توافر معطيات محددة يتم ضبط حدودها للخوارزمية للوقوف على نتيجة تثبت فرضية محددة أو تنفيها ما يعني إمكانية التنبؤ بالحروب قبل وقوعها.

٦. يمكن إدارة عمليات الهجرة واللجوء حيث تتزايد أهمية توظيف الذكاء الاصطناعي في توقع موجات الهجرة واللجوء ذات الصلة بتداعيات الحروب العسكرية وذلك من خلال جمع البيانات وتحليلها بهدف توقُّع الدول المصدِّرة للمهاجرين والطرق التي سيسلكونها بجانب إدارة عمليات استقبال واندماج اللاجئين على نحو أفضل وتخصيص الموارد على الحدود على نحو أفضل والاستعانة بخبرات اللاجئين في الوظائف المتاحة على نحو أمثل.

مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الرابع الثلاثون – حزيران ٢٠٢٤– ذي الحجة ١٤٤٥
ISSN-2536-0027

المصادر

اولاً: الكتب العربية والمترجمة

١. ساري محمد الخالد، اتجاهات في امن المعلومات وامانها: أهمية تقنيات التعمية – التشفير، مكتبة العبيكان، الرياض، ٢٠١٨.
٢. عباس بدران، الحب الالكترونية: الاشتباك في عالم المعلومات، مركز دراسات الحكومة الالكترونية، بيروت، ٢٠١٠.
٣. عبد القادر محمد فهمي، المدخل الى دراسة الاستراتيجية، دار مجدلاوي للنشر والتوزيع، عمان، ٢٠١٤.
٤. هربرت لين، النزاع السيبراني والقانون الدولي الإنساني، مختصرات من المجلة الدولية للصليب الأحمر، مجلد (٩٤)، ٢٠١٢.
٥. احمد الرشيدي ود. نضال عودة، مفهوم الارهاب وحق الشعب الفلسطيني في المقاومة، التقرير الاستراتيجي، مركز دراسات الشرق الاوسط، عمان، بدون سنة نشر.
٦. د. معراج احمد إسماعيل، الحماية الجنائية لحقوق ضحايا الجريمة الارهابية دراسة مقارنة، دار الفكر الجامعي، الاسكندرية، ٢٠١٨.
٧. مستشارية الأمن الوطني، امانة سر اللجنة الفنية العليا لأمن الاتصالات والمعلومات، استراتيجية الامن السيبراني العراقي، بلا تاريخ.
٨. المعجم الوسيط، صادر عن مجمع اللغة العربية بجمهورية مصر العربية، ط٤، مكتبة الشروق الدولية.

ثانياً: الرسائل والاطاريح:

٩. عمر عباس خضير العبيدي، الإرهاب الإلكتروني في نطاق القانون الدولي، رسالة ماجستير، كلية الحقوق، جامعة تكريت، ٢٠١٩.

ثالثاً: البحوث والدراسات

١٠. سميرة معاشي، ماهية الجريمة المعلوماتية، مجلة منتدى القانون، العدد ١٠، جامعة محمد خضير-بسكرة، ٢٠١٠.
١١. كرار عباس متعب، الحرب السيبرانية: دراسة في استراتيجية الهجمات السيبرانية بين الولايات المتحدة الامريكية وايران، مجلة حمورابي للدراسات، العدد (٤٠)، مركز حمورابي للدراسات، ٢٠٢١.
١٢. عادل عبد الرزاق، القوة الالكترونية: أسلحة الانتشار الشامل في عصر الفضاء الالكتروني، مجلة السياسة الدولية، العدد (١٨٨)، كلية العلوم السياسية، جامعة بغداد، ٢٠١٢.
١٣. مصطفى إبراهيم سلمان الشمري، الأمن السيبراني واثره في الامن الوطني العراقي، مجلة العلوم القانونية والسياسية، العدد (١)، ٢٠٢١.
١٤. ياسمين بلعسل بنت نبي، التهديدات الالكترونية والامن السيبراني في الوطن العربي، مجلة نوميروس الاكاديمية، العدد (٢)، ٢٠٢١.
١٥. غادة محمد عامر، عبدالله النجار الحمادي، دور الذكاء الاصطناعي في التطبيقات العسكرية، المركز الديمقراطي العربي، مجلة الدراسات الاستيراتيجية والعسكرية، المانيا (برلين)، العدد١٩.

رابعاً: شبكة المعلومات الدولية (الانترنيت)

ISSN–2536–0027

١٦. حسين باسم عبد الأمير. تحديات الامن السيبراني، مركز الدراسات الاستراتيجية، جامعة كربلاء، تمت زيارة الموقع بتاريخ ٢٠٢٣/٨/٢٦، على الرابط: http://kerbalacss.uokerbala.eA/
١٧. صلاح حيدر عبد الواحد، حروب الفضاء الالكتروني دراسة في مفهومها وخصائصها وسبل مواجهتها، تمت زيارة الموقع بتاريخ ٢٠٢٣/٨/٢٤ على الرابط: https://meu.edu.jo/libra%D ٪٨A.pdf
١٨. صلاح حيدر عبد الواحد، حروب الفضاء الالكتروني دراسة في مفهومها وخصائصها وسبل مواجهتها، تمت زيارة الموقع بتاريخ ٢٠٢٣/٩/٢٥ على الرابط: https://meu.edu.jo/libraryTh.pdf
١٩. ايهاب شوقي، الارهاب السيبراني وجرائمه، تمت زيارة الموقع بتاريخ ٢٠٢٣/٩/٢٧ على الرابط: http://www.Annt..tv/showsubject.aspxpid=١٢١٠٦٢
٢٠. منظمة العفو الدولية، تسرب هائل للبيانات يكشف عن استخدام برمجيات التجسس لمجموعة ان اس او الإسرائيلية، تمت زيارة الموقع بتاريخ ٢٠٢٣/٩/٢٦ على الرابط: https://www.amnesty.org/ar/t/
٢١. عبد الله ذيبان، اوخنتيك الروسية اخطر درونز عسكرية، المادين نت، تمت زيارة الموقع ٢٠٢٣/٩/٣٠م على الرابط: https://www.almayadeen.net/technology/%D٨٪A٣٪D%D٨٨A%D٨٪A٩

---

(١) هربرت لين. النزاع السيبراني والقانون الدولي الإنساني، مختصرات من المجلة الدولية للصليب الأحمر، مجلد (٩٤)، ٢٠١٢ ، ص٥١٦.
(٢) فهد ال قاسم. الذكاء الاصطناعي، مدخل مبسط في أهم مواضيع علم الذكاء الاصطناعي، تمت زيارة الرابط بتاريخ ٢٠٢٣/٩/٢٣ على الرابط: http://www.myreaders.info/html/artificence.html
(٣) عادل عبد الرزاق، القوة الالكترونية: أسلحة الانتشار الشامل في عصر الفضاء الالكتروني، مجلة السياسة الدولية، العدد (١٨٨)، كلية العلوم السياسية، جامعة بغداد، ٢٠١٢، ص٣٠.
(٤) نضال ناجي بدوي بريوش، الصراع السيبراني مع العدو الصهيوني، رسالة ماجستير (غير منشورة)، اكاديمية دراسات اللاجئين، فلسطين، ٢٠١٩، ص١٤.
(٥) شادي عبد الوهاب منصور، حروب الجيل الخامس: أساليب التفجير من الداخل على الساحة الدولية، العربي للنشر والتوزيع، القاهرة، ٢٠١٩، ص١٠٦.
(٦) عبد القادر محمد فهمي، المدخل الى دراسة الاستراتيجية، دار مجدلاوي للنشر والتوزيع، عمان، ٢٠١٤، ص٢٠.
(٧) قانون التوقيع الالكتروني والمعاملات الالكترنية العراقي. رقم (٧٨) لسنة ٢٠١٢.
٨ شادي عبد الوهاب منصور، مصدر سبق ذكره، ص٣٦.
(٩) صلاح حيدر عبد الواحد، حروب الفضاء الالكتروني دراسة في مفهومها وخصائصها وسبل مواجهتها، تمت المعاينة بتاريخ ٢٠٢٣/٥/٢٤ بالساعة ١٣٠٠ على الرابط: https://meu.edu.jo/libra%D ٪٨A.pdf .
(١٠) المصدر نفسه
(١١) نضال ناجي بدوي بريوش، مصدر سبق ذكره، ص٤٧.
(١٢) ريتشارك كلارك وكنيك روبرت، حرب الضاء الالكتروني: الخطر القادم على الامن القومي وسبل مواجهته، مركز الامارات لدراسة السياسات، أبو ظبي، ٢٠١٣، ص٢٨٦.
(١٣) صلاح حيدر عبد الواحد، حروب الفضاء الالكتروني دراسة في مفهومها وخصائصها وسبل مواجهتها، تمت زيارة الموقع بتاريخ ٢٠٢٣/٥/٢٥ على الرابط: https://meu.edu.jo/libraryTh.pdf .
(١٤) ساري محمد الخالد، اتجاهات في امن المعلومات وامانها: أهمية تقنيات التعمية – التشفير، مكتبة العبيكان، الرياض، ٢٠١٨، ص٧٠.

مجلة كامبريدج للبحوث العلمية: مجلة علمية محكمة
تصدر عن مركز كامبريدج للبحوث والمؤتمرات–العدد الرابع الثلاثون – حزيران ٢٠٢٤– ذي الحجة ١٤٤٥
ISSN-2536-0027

(١٥) المصدر نفسه، ص٧١.
(١٦) غادة محمد عامر، عبدالله النجار الحمادي، دور الذكاء الاصطناعي في التطبيقات العسكرية، المركز الديمقراطي العربي، مجلة الدراسات الاستيراتيجية والعسكرية، المانيا (برلين)، العدد، ١٩ص٢٤٠.
(١٧) ساري محمد الخالد، مصدر سبق ذكره، ص٧٠.
(١٨) غادة محمد عامر، عبدالله النجار الحمادي، مصدر سبق ذكره، ص٢٤٤.
(١٩) ريتشارك كلارك وكنيك روبرت، حرب الفضاء الالكتروني: الخطر القادم على الامن القومي وسبل مواجهته، مركز الامارات لدراسة السياسات، أبو ظبي، ٢٠١٣، ص٢٨٦.
(٢٠) عبد الرحمن المسند ، وسائل الإرهاب الالكتروني ، حكمها في الإسلام وطرق مكافحتها ، السجل العلمي لمؤتمر موقف الإسلام من الإرهاب ، الجزء الأول ، الرياض ، ٢٠٠٤، ص٣٤.
(٢١) عادل عبد الصادق هل يمثل الارهاب الالكتروني شكلا جديدا من اشكال الصراع الدولي الاهرام الاستراتيجي، العدد ١٥٦ مركز الدراسات السياسية والاستراتيجية ، ٢٠٠٧، ص ١٨.
(٢٢) جمال علي الدهشان، الإرهاب في العصر الرقمي الإرهاب الإلكتروني صوره –مخاطره- آليات مواجهته، المجلة الدولية للبحوث في العلوم التربوية، العدد ٣ ، مصر، ٢٠١٨، ص ٩٢.
(٢٣) حسن تركي عمير، سلام جاسم عبد الله، الإرهاب الالكتروني ومخاطره في العصر الراهن، مجلة العلوم القانونية والسياسية، جامعة ديالى، ٢٠١٣، ص ٥٦.
(٢٤) جمال علي الدهشان، مصدر سبق ذكره، ص٧٣.
(٢٥) شادي عبد الوهاب منصور، حروب الجيل الخامس: أساليب التفجير من الداخل على الساحة الدولية، العربي للنشر والتوزيع، القاهرة، ٢٠١٩، ص١٠٦.
(٢٦) إيهاب خليفة، القوة الالكترونية: كيف يمكن ان تدبر الدول شؤونها في عصر الانترنت، العربي للنشر والتوزيع، القاهرة، ٢٠١٧، ص١٠١.
(٢٧) اميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، العدد (٣)، ٢٠٢٠، ص٤١٥.
(٢٨) ما هو برنامج بيغاسوس الإسرائيلي للتجسس.. ولماذا يعد اقوى نظام لاختراق الهواتف في العالم. موقع عربي بوست، شبكة المعلومات الدولية (الانترنت)، تمت زيارة الموقع بتاريخ ٢٠٢٣/٥/٢٥ على الرابط: https://arabicpost.net/%D٨٪A ٨٪AC%D٨٪B٣/
(٢٩) فضيحة بيغاسوس، شركة إسرائيلية تجسست على صحافيين وقادة دول ومعارضين، موقع جريدة الجريدة، تمت زيارة الموقع بتاريخ ٢٠٢٣/٥/٢٥ على الرابط: https://www.aljarida.com/articles/
(٣٠) منظمة العفو الدولية. تسرب هائل للبيانات يكشف عن استخدام برمجيات التجسس لمجموعة ان اس او الإسرائيلية، تمت زيارة الموقع بتاريخ ٢٠٢٣/٥/٢٦ على الرابط: https://www.amnesty.org/ar/t/
(٣١) غادة محمد عامر، عبدالله النجار الحمادي، مصدر سبق ذكره، ص٢٤٨.
(٣٢) مصطفى إبراهيم سلمان الشمري، الأمن السيبراني واثره في الامن الوطني العراقي، مجلة العلوم القانونية والسياسية، العدد (١)، ٢٠٢١، ص١٦٦.
(٣٣) حمدون توريه، البحث ع السلام السيبراني، الاتحاد الدولي للاتصالات، جنيف، ٢٠١١، ص٧.
(٣٤) حسين باسم عبد الأمير، تحديات الامن السيبراني، مركز الدراسات الاستراتيجية، جامعة كربلاء، تمت المعاينة بتاريخ ٢٠٢٣/٥/٢٦ بالساعة ١٤٠٠ على الرابط ، على الرابط: http://kerbalacss.uokerbala.eA/
(٣٥) ياسمين بلعسل بنت نبي، التهديدات الالكترونية والامن السيبراني في الوطن العربي، مجلة نوميروس الاكاديمية، العدد (٢)، ٢٠٢١، ص١٧١.
(٣٦) كرار عباس متعب، الحرب السيبرانية: دراسة في استراتيجية الهجمات السيبرانية بين الولايات المتحدة الامريكية وايران، مجلة حمورابي للدراسات، العدد (٤٠)، مركز حمورابي للدراسات، ٢٠٢١، ص١٩٨.
(٣٧) إيهاب خليفة. مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الراعة على الامن القومي، العربي للنشر والتوزيع، القاهرة، ٢٠١٩، ص١١٤.