مجلة الحكمة للدراسات الفلسفية
Eissn :2602-5264 Issn : 2353-0499
المجلد 9 /العدد: 02 (2021)، ص ..- ..

الحرب السيبرانية في عصر الذكاء الاصطناعي و رهاناتها على الأمن الدولي

Cyber war in the age of artificial intelligence and its challenges on international security

د. دليلة العوفي

جامعة الجزائر 3(الجزائر) ،laoufi.dalila@univ-alger3.dz

تاريخ الاستلام: 2021/07/01 تاريخ القبول: 2021/07/05 تاريخ النشر: 2021/10/07

ملخص:

أدى ظهور الذكاء الاصطناعي و انترنت الأشياء و الحوسبة الحسوبية والبيانات الضخمة إلى ظهور مؤشرات جديدة في العلاقات الدولية ، حيث تغيرت موازين القوى عالميا و أصبحت قوة الدول تعتمد على التكنولوجيا مع التحكم في تطبيقاتها و ذلك في بيئة أمنة.

هذا الوضع أفرز صراعا بين الدول أطلق عليه " الحرب السيبرانية "، تقودها دول و جيوش بهدف مهاجمة أجهزة الحاسوب أو شبكات المعلومات في دول أخرى و الإضرار بها . كما يمكن التحكم في نظم دفاع الدول المستهدفة أو التشويش عليها و شل منظومة أسلحتها المتطورة.

مما جعل الدول تعيد النظر في استراتيجياتها التي أصبحت تركز أساسا على القوة السيبرانية ، و في حالة تأهب قصوى استعدادا لأي حرب سيبرانية محتملة مستقبلا مما أثر على مفهوم الأمن الدولي .

الكلمات المفتاحية : الذكاء الاصطناعي ، الحرب السيبرانية، أنترنت الأشياء ،الحوسبة السحابية

Abstract

The emergence of artificial intelligence, Internet of things, computer, computing and big data, has led to the appearance of new indicators in international relations.

Therefore, the balance of power has changed internationally and the power within countries has become dependent on the technology and its wide use, with the control of its applications in a secure environment.

This situation has created a conflict between countries named “The cyber war”, commanded by states and armies with the objective of attacking computer devices or information networks in other countries, in order to harm them.

This led countries to reconsider their strategies, starting to focus principally on the cyber power, and become in a high state of alert, to be prepared for any possible cyber war in the future.

This state of facts has affected the concept of international security.

Key words:; Artificial intelligence, Cyber War, Internet of things , Cloud Computing

المؤلف المرسل: د. دليلة العوفي

1. مقدمة:

أدت أنظمة الاتصال السريعة و المتطورة باستمرار إلى تحويل الحروب من واقعها التقليدي إلى الفضاء الرقمي ،مما جعل الدول تعيد النظر في مفهوم الحروب ، "حروب المستقبل" باعتبارها جزءا من استراتيجياتها الأساسية للدفاع الوطني .

فمع ظهور ما يسمى " المجتمع الخامس" Fifth Society أو " مجتمع ما بعد المعلومات " و هو المجتمع الذي تندمج فيه المعلومة و الآلة مع عقل الإنسان ، أعادت الدول النظر في تسطير استراتيجيات جديدة تتلاءم مع هذا العصر لتحافظ على تطورها على الأقل أو تستطيع مواجهة تلك التي سبقتها تكنولوجيا و تفرض بذلك قوتها الدولية.

و نقصد بالدول القوية تلك الدول التي تستثمر في التكنولوجيا و في الابتكارات التكنولوجية التي أزاحت كثيرا من عناصر القوة عن مواقعها التي شملت حيزا كبيرا لفترة طوية ، حيث ذاب المفهوم التقليدي للقوة الذي كان يعتمد في أساسه على القدرات العسكرية و الاقتصادية Hard Power ، ليصبح اليوم ، موجها للقوة السيبرانية Cyber Power الذي فرض نفسه كمفهوم جديد في العلاقات الدولية .

فلا وجود لدولة قوية أخرى ضعيفة إلاّ وفقا لهذا المنظور، مما أفرز صراعا من نوع جديد بين الدول و هو صراع قائم على التكنولوجيا و التحكم فيها و تأمينها من مختلف المخاطر و الاعتداءات التي قد تهددها في فضاء رقمي مفتوح علي مصراعيه.

إذا أفرز مجتمع ما بعد المعلومات الذي يسيطر عليه الذكاء الاصطناعي ، مفهوما جديدا للحروب أطلق عليه أهل الاختصاص " بالحروب السيبرانية " ، فمن الصعب تخيل صراع عسكري أو حرب عسكرية دون أن يتضمن أبعادا إلكترونية ، بل أصبحت في صلب اهتمامات الدول في أنظمتها الدفاعية أو الهجومية المحتملة حدوثها مستقبلا.

فلم تعد تقتصر الحرب السيبرانية أو " الحرب الرقمية أو " الحرب الإلكترونية" على مهاجمة المرافق الخدماتية و الاعتداء عليها ، و إنما تعدى ذلك إلى التحكم في نظام دفاع العدو و التشويش على أقماره الاصطناعية و يمكن حتى شل منظومة أسلحتها المتطورة.

و قد أدى ظهور الذكاء الاصطناعي إلى إحداث تحولات عميقة في طبيعة الحروب التقليدية التي تعتمد على الأسلحة و الجيوش العسكرية ، كونه أضاف " تقنيات جديدة عززت من قدرات الدول في الإدراك البصري واستخدام الخوارزميات في صنع القرار لتنفيذ مجموعة من العمليات (الجوية والبرية

والبحرية). و كل هذا يسمح للدول بتنفيذ ضرباتها ضد العدو و اختراق الدفاعات الجوية المتطورة بصفة دقيقة .كما تسمح تلك الأسلحة المدعمة بتقنيات الذكاء الاصطناعي للدول بإبراز القوة العسكرية داخل المناطق المتنازع عليها وغير المسموح لها باختراقها"[1] (سارة عبد العزيز، 2019)

لكن لا يعني هذا أن الدول القوية محمية و بمعزل عن الحرب السيبرانية ، بدليل أن الولايات المتحدة الأمريكية تعرضت أنظمة معلوماتها لاختراقات عدة مرات ، مثلما حدث " عام 2018 ، حيث وجهت وزارة العدل الأميركية اتهامات جنائية وفرضت عقوبات على شركة إيرانية ، لاختراقهم أنظمة مئات الجامعات والشركات وضحايا آخرين، بهدف سرقة البحوث والبيانات الأكاديمية والملكية الفكرية. ووصفت وزارة العدل الأميركية القراصنة بأنّهم عصابة تسلّل إلكتروني[2]" (سارة عبد العزيز، 2019)

لهذا و بسبب طبيعة الفضاء السيبراني المفتوح كساحة عالمية عابرة للحدود، فإن قضية الأمن السيبراني تمتد من الدولة الواحدة لتشمل مخاطر وحروب تهدد كل الفاعلين في الساحة الدولية و هذا ما يجعل قضية الأمن الدولي مطروحة بشدة كرهان من رهانات الحروب السيبرانية في عصر الذكاء الاصطناعي.

[1]- سارة عبد العزيز سالم،(2019) ، قراءة في دراسة لجيمس جونسون، أتمتة الحروب ، تأثير الذكاء الاصطناعي في سباق التسلح العالمي، مجلة المستقبل للأبحاث و الدراسات المتقدمة ، متاح على الرابط: https://futureuae.com/en/Mainpage/Item/، تم الاطلاع عليه بتاريخ 2021/05/15 ، على الساعة 22:00.

[2]سالم عبد العزيز ، المرجع نفسه

بناءا على المعطيات التي ذكرناها، نحاول أن نعالج في هذه الدراسة ،موضوع الحروب السيبرانية الذي فرض نفسه كبديل للحروب التقليدية ، إذ طرحنا الإشكالية الآتية:

ما مدى تأثير الذكاء الاصطناعي على الحروب السيبرانية ؟ و ما هي رهانات ذلك على الأمن الدولي؟

تبدو أهمية هذه الدراسة في المخاطر و الرهانات التي تطرحها الحرب السيبرانية و مساهمة الذكاء الاصطناعي في تعزيز قوى الدول سيبرانيا لمواجهة أي مخاطر و اعتداءات محتملة، و كذا الرهانات و الإشكالات الجديدة التي يطرحها تطور الذكاء الاصطناعي على مختلف المجالات و خاصة منها المجال العسكري.

و حتى نتمكن من الإحاطة بهذا الموضوع ، ركزنا على الأدبيات الحالية التي تناولت كل من الحرب السيبرانية و الذكاء الاصطناعي في السنوات الأخيرة، و عالجناه على شكل محاور أو عناصر أساسية مهمة و ابتعدنا عن الطرق الكلاسيكية التي تتطلب الفصول و المباحث .

حيث تناولنا في البداية تعريف كل من مفهومي الحرب السيبرانية و الذكاء الاصطناعي ، ثم تعرضنا أهم الأسلحة المستعملة في الحروب السيبرانية ، مع إبراز دور الذكاء الاصطناعي في تعزيز القوى السيبرانية ،و بعدها تناولنا عسكرة الفضاء الرقمي و استحداث الجيوش السيبرانية ، و تعرضنا في الأخير إلى بعض الاتفاقات بين الدول لمواجهة الحرب السيبرانية.

1. مفهوم الحرب السيبرانية:

يرتكز مفهوم الحرب السيبرانية أساسا على اختراق مواقع الدول في العالم أو أنظمتها المعلوماتية خاصة تلك المتعلقة بالقطاعات الإستراتيجية كالدفاع و الطاقة و الاتصالات ، و ذلك إما بهدف التجسس عليها أو تعطيل خدماتها أو سرقة معلوماتها .

و يعود التنبؤ بالحرب السيبرانية إلى عام 1993 ، و ذلك من خلال مقال نشره كل من John Arquilla و David Ronfeldtt بعنوان " الحرب السيبرانية قادمةCyber – war Is Coming، وقد عرف الكاتبان الحرب السيبرانية بأنها "

تنفيذ،و الاستعداد لتنفيذ، العمليات العسكرية وفقًا للمبادئ المعلوماتية، من خلال تعطيل– إن لم يكن تدمير - نظم المعلومات و الاتصالات على أوسع نطاق " و كذلك " تدمير القاعدة العسكرية للعدو و منعه في الوقت نفسه من معرفة أي شيء عن الطرف الآخر، وتحويل ميزان المعرفة ليكون في صالح هذا الطرف"[3] (إيهاب خليفة، 2019، ص148)

كما عرف بعض المختصين ، الحرب السيبرانية بأنها تلك "الحرب التي تتم إدارتها في مجال الفضاء الرقمي، تمثل الدول فيها كفواعل رئيسية، حيث تستخدم الآليات والأسلحة الالكترونية في الهجوم الذي يكون موجه أساسا إلى أجهزة الحاسب الآلي أو الشبكات الالكترونية الخاصة بالعدو أو الأنظمة الإلكترونية وما تحتويه من معلومات والخاصة بالدول مما يحول دون استخدام هذه الأنظمة والأجهزة والشبكات أو تدميرها بالكامل"[4]. Klaus-Peter Saalbachm , (March2012, , p 4)

في حين اعتبرها البعض الآخر بأنها"حرب تخيلية أو افتراضية ذات طبيعة غير ملموسة تحاكي الواقع بشكل شبه تام ، وهي حرب قد تكون بلا دماء ، إذ

[3] إيهاب خليفة، (2018)، مجتمع ما بعد المعلومات ، تأثير الثورة الصناعية الرابعة على الأمن القومي ، سلسلة كتب المستقبل للأبحاث و الدراسات المتقدمة، العربي للنشر و التوزيع، القاهرة ، (مصر)، ص 148،

[4] Klaus-Peter Saalbach ,(March2012),Cyber War Methods and Practice, , LV.Internet Policy, Version 4.0 , p 4, www.dirk-koentopp.com/downloads/saalbach-cyberwar-methods-and practice.pdf, consulted on May 24, 2021, at 23 :00

تتلخص أدوات الصراع فيها بالمواجهات الالكترونية والبرمجيات التقنية وجنود من برامج التخريب المحوسب وطلقاتها لوحات المفاتيح ونقرات المبرمجين في بيئة اصطناعية تحاول ما أمكن الوصول إلى صورة حقيقية لملامح الحياة المادية والملموسة"[5] (كمال مساعد، 2006)

فهي حرب خفية بأسلحة إلكترونية وذكية، " يتم استخدامها للتهديد أو إحداث الضرر المادي أو الوظيفي للأجهزة أو النظم والهياكل الإلكترونية. وهي تختلف من حيث درجة خطورتها وتعقيدها، فمنها البسيطة وهي القادرة فقط على إحداث ضرر خارجي بالنظام الإلكتروني دون اختراقه، ومنها المعقّدة التي يمكن من خلالها اختراق النظام وإحداث أضرار بالغة به قد تصل إلى تدميره كليًّا أو توقفه عن العمل كلية".[6] (Thomas Rid, March 2012)

نستنتج من خلال التعاريف المقدمة، بأن الحرب السيبرانية(cybercrime) أو الحرب الإلكترونيّة (Cyber warfare) هي حرب تستخدم فيها مختلف التدابير أو الإجراءات السيبرانية في فضاء رقمي بهدف الدفاع أو الهجوم أو الاثنين معا مع امتلاك المعلومة الصحيحة و في وقتها، فهي حرب افتراضية ذات طبيعة غير ملموسة تحاكي الواقع بشكل شبه تام ، تستخدم مختلف المواجهات الالكترونية و برمجيات التسليح (Weaponized " wSoftare) وجنود من برامج التخريب المحوسب و لوحات المفاتيح ونقرات.

[5] كمال مساعد ، (2006) ، الحرب الافتراضية وسيناريوهات محاكاة الواقع ، مجلة الجيش اللبناني ، العدد(253) ، متاح على الرابط:
https://www.lebarmy.gov.lb/ar/content ، تم الاطلاع عليه بتاريخ 2021/06/07 ، على الساعة 10:00

[6] Thomas Rid,(March,2012) Cyber-weapons,Rusi Journal,Vol.157 No.1, https://www.tandfonline.com , accessed on june05, 2021 at 14:00.

المبرمجين في بيئة تحاول الوصول إلى صورة حقيقية لملامح الحياة المادية والملموسة.

بعدما تناولنا مفهوم الحرب السيبرانية ، نتطرق لمفهوم الذكاء الاصطناعي الذي أدمج في المجال العسكري و أعطى بذلك بعدا جديدا للحرب السيبرانية لا تتساوى فيها الجيوش التي تستخدم التكنولوجيا مع تلك التي لا تستخدمها ، والذي ساهم أيضا في توجيه القادة العسكريين في اتخاذ القرار.

2.مفهوم الذكاء الاصطناعي:

اختلف الباحثون في إيجاد تعريف دقيق لمفهوم الذكاء الاصطناعي ، نظرا لاختلاف ميولاتهم الفكرية و منطلقاتهم المعرفية و مجالاتهم البحثية ، حيث عرفه البعض بأنه " العلم الذي يهتم بتطوير أجهزة الحاسوب القادرة على الانخراط في عمليات التفكير الشبيهة بالإنسان مثل التعليم و الاستدلال و التصحيح الذاتي"[7] (Joost N. Kok, Egbert J.W. Boers, Walter A. Kosters, and Peter van der Putten, 2009)

و اعتبره بعض المختصين بأنه ذلك " الذكاء الذي تبديه الآلات والبرامج بما يحاكي القدرات الذهنية البشرية وأنماط عملها، مثل القدرة على التعلم والاستنتاج ورد الفعل على أوضاع لم تبرمج في الآلة، كما أنه اسم لحقل أكاديمي يعنى بكيفية صنع حواسيب وبرامج قادرة على اتخاذ سلوك ذكي" [8] (رماح الدلقموني ،2016)

[7] Joost N. Kok, Egbert J.W. Boers, Walter A. Kosters, and Peter van der Putten, Artificial Intelligence : Definition , Trends ,Techniques and Cases , p02, Faculty of Computer Science, University of Twente, the Netherlands, available in: https://www.eolss.net/Sample-Chapters/C15/E6-44.pdf , consulted on june11 , 2021 at 16:30

[8] رماح الدلقموني، (2016)، الذكاء الاصطناعي ماهو؟ و ما أبرز مظاهره؟، متاح على الرابط : https://www.aljazeera.net/news/scienceandtechnology/2016/5/4
تم الاطلاع عليه بتاريخ 2021/06/08 على الساعة 22:00

في حين اعتبر أهل اختصاص بأن التعريف الشامل لمفهوم الذكاء الاصطناعي هو التعريف الذي اقترحه شابيرو عام 1992 و الذي ذهب إلى أن هذا المفهوم " مجال مثل مجال العلوم و الهندسة الذي تناول الفهم بمساعدة الحاسوب و السلوك الذكي و كذا إنشاء أنظمة اصطناعية التي تعيد إنتاج هذا السلوك " [9]

Yvon Haradji Moustafa Zouinar, Catherine Delgoulet et Alexandre Morais,2020)

لكن رغم الاختلافات القائمة بشأن تعريف المفهوم ، إلا أنه انتشر على نطاق واسع في مختلف المجالات كالصناعة و البحث العلمي و علم الحاسوب والخدمات الذكية و الحكومات و المنظمات و غيرها.

3. الهجمات السيبرانية هي أسلحة سيبرانية لتعزيز الحرب السيبرانية:

تتميز الحرب السيبرانية عن الحرب التقليدية في اعتمادها على أسلحة الكترونية تلائم طبيعة الصراع القائم بين مختلف الأطراف في الفضاء الرقمي، حيث تستخدم عدة أسلحة تتمثل أساسا في مختلف البرامج الضارة التي تحملها الحواسب كالفيروسات(Viruses)

و الديدان (Worms) و البرامج الخبيثة (Malware) و القنابل المنطقية (Logic Bombs) ، و هي برامج تستهدف أساسا أنظمة المعلومات بهدف إلحاق الضرر بها و تخريبها ، أو اختراق الأنظمة العسكرية ، و التجسس على الأفراد و المعلومات الخاصة بحياتهم الشخصية و استهداف الشخصيات الرسمية و البارزة ، مما يؤدي إلى تدمير البنى التحتية للدول بأسرها.

[9] Yvon Haradji, Moustafa Zouinar, Catherine Delgoulet et Alexandre Morais,(2020), robotique, automatisation : quelles évolutions pour l'activité humaine ? , activités, Vol 17, N1 ? ,disponible sur site : https://journals.openedition.org/activites/4941, consulté le 03 /05/2021 à 10 :00

بالإضافة إلى هذه الأسلحة المذكورة ، نجد بعض الأسلحة المعروفة لدى المختصين في الأمن السيبراني و المتمثلة في الجوسسة ، الدعاية ، الحرمان من خدمة الإنترنت ، تعديل البيانات والتلاعب بها، وتعطيل البنى التحتية الحيوية .

و تعتبر الحرمان من الخدمة، أو "هجوم حجب الخدمة" Denial of service attack، من أبرز أنواع الأسلحة الإلكترونية وأكثرها استخداما على الساحة الدولية، و هي عبارة عن " هجمات تتم عن طريق إغراق المواقع بسيل من البيانات غير المهمة، يتم إرسالها على المواقع المستهدفة بشكل كثيف مما يسبب بطء الخدمات أو زحاماً مرورياً بهذه المواقع، ينتج عنه صعوبة وصول المستخدمين لها بسبب هذا " الاكتظاظ المعلوماتي"[10] (عبدالغفار عفيفي الدويك ، 2019)

و لعل ما تعرضت له ، استونيا عام 2007، نموذج حي في مجال الحروب السيبرانية من طرف روسيا و ذلك عن طريق " إغراق المواقع الالكترونية بسيل من البيانات غير اللازمة ، حيث وجهت ما يقارب من مليون حاسبة من عدة نقاط في العالم، و استهدفت المواقع الحكومية و الصحف و الجامعات و المستشفيات و المصارف و خدمات الإطفاء و الإسعاف و ذلك بهدف إسقاط و شل الحكومة الإستونية " [11](يحي ياسين سعود، 2018، ص89)

[10]عبدالغفار عفيفي الدويك،(2018) ، الأزمات والحروب السيبرانية... تهديدات تتجاوز الفضاء الإليكتروني، مركز الأهرامات والدراسات الإستراتيجية متاح على الرابط:
https://acpss.ahram.org.eg/News/16843.aspx، تم الاطلاع عليه بتاريخ : 2121/05/01 ، على الساعة09:00

[11]يحي ياسين سعود، (2018)، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلة القانونية ، جامعة القاهرة - كلية الحقوق - فرع الخرطوم، المجلد رقم 04، ص 89، متاح على الرابط :
https://jlaw.journals.ekb.eg/article_45192_52d735c1a23cca2bf7dbbe56c4eb6846.pdf

إذا ، يستطيع أحد أطراف الصراع أن يوقع خسائر فادحة بالطرف الآخر و يتسبب في شل منظومة المعلومات الخاصة به من خلال" قطع أنظمة الاتصال بين الوحدات العسكرية وبعضها البعض أو تضليل معلوماتها أو سرقة معلومات سرية عنها، أو من خلال التلاعب بالبيانات الاقتصادية والمالية وتزييفها أو مسحها من أجهزة الحواسيب، باستعمال أسلحة بسيطة ، تتمثل في فيروسات إلكترونية تخترق شبكة الحاسب الآلي وتنتشر بسرعة بين الأجهزة، وتبدأ عملها في سرية تامة وبكفاءة عالية، وهي في ذلك لا تفرق بين المقاتل والمدني، وبين العام والخاص، وبين السري والمعلوم [12](محمد الحمامصي، 2014)

و لهذا فإن مختلف الاعتداءات و الهجمات التي تتعرض لها شبكات الحاسب الآلي تمس مختلف الأماكن التي تتواجد فيها و لا نستطيع أن نعرف مصدرها و لا الجهة التي تنتمي إليها و لا التي تتحكم فيها ، رغم أن المسألة في سياقها السياسي و الدولي العام مفصول فيها ، لأن الجميع يعرف من يقف وراء هذه الاعتداءات .

و كل هذا يستدعي تسطير إستراتيجية أو مخطط للتفاعل السيبراني، يعتمد أساسا على أنظمة معلومات دفاعية و برامج قادرة على أداء مهامها و تنفيذ مختلف عملياتها و يعتمد أيضا على خبراء مسلحين ببرامج تكون قادرة على تحقيق الدفاع النشط سيبرانيا و بصفة دائمة و مستمرة و فعالة و تكون قادرة أيضا على التأقلم مع الهجومات السيبرانية غير المتوقعة ، حتى تستطيع أن تتحول من

تم الاطلاع عليه بتاريخ 06/03 /2021 على الساعة 20:30

[12]محمد الحمامصي، (2014) ، القوة الإلكترونية عنصر أساسي مؤثر في النظام العالمي، موقع العرب، متاح على الرابط: https://alarab.co.uk/ ، تم الاطلاع عليه بتاريخ 2021/06/15 ، على الساعة 13:00

حالة الدفاع إلى حالة الهجوم السيبراني المضاد و تشكل بذلك قوة دفاعية متينة للبلد.

4.دور الذكاء الاصطناعي في تعزيز القوى الدفاعية للدول :

انتشرت الحروب السيبرانية بشكل واسع مع ظهور ما يسمى بالذكاء الاصطناعي و الاستثمار فيه و كذا ظهور التقنيات التكنولوجية المرتبطة به كالحوسبة السحابية و أنترنت الأشياء و الأنظمة الذاتية ، حيث أدت إلى خلق تكتلات عديدة و أحلاف جديدة ، تشارك سواء في الهجوم أو في الدفاع ، حسب المصالح المشتركة لكل من هذه التكتلات ، و هذا من شأنه أن يحدث تحولا في مستقبل التوازنات العسكرية على المستوى العالمي.

فقد تحول الفضاء الإلكتروني إلى ساحة للتفاعلات الدولية تستخدم فيه الدول تقنيات الذكاء الاصطناعي في أنظمة الأسلحة والتي تقوم بتنفيذ مهامها بالكامل دون تدخل بشري بناءً على معايير الاستهداف المرمجة مسبقًا، فقد طرأت على أنماط التفكير الاستراتيجي عقيدة قتالية تتلائم مع الواقع الالكتروني ، الذي يعتمد على البيانات الضخمة(Big data) لها قدرات فائقة على الإدراك واتخاذ القرار.

و أدى هذا التحول بالدول المتقدمة تكنولوجيا و القوية معلوماتيا إلى وضع الذكاء الاصطناعي ضمن اهتماماتها الأساسية ، كما هو الشأن " بالنسبة للولايات المتحدة الأمريكية التي حدثت فيها الكثير من ابتكارات الذكاء الاصطناعي و انتشرت بسرعة لا سيما مع الضغوط الأكاديمية والتجارية القوية لجعل الذكاء الاصطناعي في متناول الجميع.

إلاّ أنّ تزايد مبتكري الذكاء الاصطناعي وخبراتهم في دول أخرى مثل الصين يشكل إشارة أكثر دلالة إلى فقدان الولايات المتحدة ميزة المتحرّك الأول في مجال الذكاء الاصطناعي وقد زاد تخلي الولايات المتحدة عن الهيمنة في الحوسبة عالية

الأداء من تعقيد الساحة " [13] (أوسوندي أ .أوسوبا، ويليام ويلسر الرابع،2017)

و هذا يؤكد بأن الابتكارات التكنولوجية أصبحت متوفرة عالميا ، و لم تعد حكرا على الولايات المتحدة الأمريكية ، بل نجد الصين أيضا إلى جانب كل من روسيا و كوريا الشمالية و هي الدول ذاتها التي تتبادل الأدوار في الساحة الافتراضية.

و لعل انتشار " انترنت الأشياء " كإفراز من إفرازات الذكاء الاصطناعي وتطبيقاته ، أدى إلى تفاقم المخاطر المهددة للأفراد و الدول وحتى للمنظمات وخاصة الأجهزة التي باتت موجودة في مختلف القطاعات الحساسة ، و هذا من شأنه أن يعطي أبعاد أخرى للحرب السيبرانية .

فهذه الأجهزة المرتبطة بالأنترنت يمكن أن تستخدم لشن هجمات على نطاقات واسعة في المجتمعات ، كما يمكن لها أن تتعرض للهجمات التي تتطور بتطور التكنولوجيا التي أفرزتها خاصة و أن طرق الهجوم تتجدد باستمرار وبسرعة في ظل وجود الأدوات المفتوحة المصدر و المتاحة بدون رقابة على شبكة الأنترنت .

هذا ما يؤكد بأن الذكاء الاصطناعي سيُعزز من قدرة الأنظمة العسكرية سواء من حيث الدفاع أو الهجوم. فمن حيث الهجوم، سيساهم الذكاء الاصطناعي في صعوبة تحديد منفذي الهجمات السيبرانية، أو التنبؤ بها، وكذلك دقة تحديد الأهداف المراد الهجوم عليها، أما من حيث الدفاع السيبراني، فقد

[13] أوسوندي أ .أوسوبا، ويليام ويلسر الرابع،(2017) ، مخاطر الذكاء الاصطناعي على الأمن و مستقبل العمل ، منظور تحليلي ، مؤسسة RAND، ص 16، متاح على الرابط:
https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE237/RAND_PE237z1.arabic.pdf.

تم الاطلاع عليه بتاريخ 2021/06/06 على الساعة 10:00

يعزز الذكاء الاصطناعي من تقليل مخاطر الهجمات السيبرانية من خلال تحسين عمليات مراقبة الشبكات، وتحديد التهديدات بسرعة، والدفاع عنها تلقائيًا.

بناءا على ما ذكرنا ، نجد ثلاث قوى مسيطرة في العالم هي الولايات المتحدة الأمريكية و روسيا و الصين.

5.عسكرة الفضاء الرقمي و استحداث الجيوش السيبرانية :

تعدّ المجالات العسكرية من أكثر المجالات التصاقاً بالحروب الالكترونية ، وتعرف الحروب السيبرانية تبعا لترابطها بالقوة العسكرية بأنها تلك " الحروب التي تتسم بالتعاون مع الحرب العسكرية إذ أنها تصوب نيرانها نحو الأهداف الالكترونية والرقمية والمعلوماتية كالتجسس على المعلومات والإشارات الصادرة من الأجهزة الالكترونية التابعة إلى الأهداف المستهدفة ، وكذلك تتبع الموجات المطلقة من الاتصالات اللاسلكية وغيرها ، إذ تستهدف هذه النيران الالكترونية المصالح القومية والسياسية والعسكرية والأمنية للدول المستهدفة متخذة شكل الهجمات الإلكترونية أو الاختراقات الكترونية الهادفة لتعطيل البنية المعلوماتية للدولة المستهدفة [14] (عباس بدران، 2010، ص30)

فمع انتشار الذكاء الاصطناعي تعززت القدرات العسكرية للدول سوء على المستوى التشغيلي أو المستوى التكتيكي.فعلى" المستوى التشغيلي، يعزز الذكاء الاصطناعي من القدرات العسكرية من خلال إمكانات (الاستشعار عن بعد، والإدراك اللحظي للمتغيرات، والمناورة، واتخاذ القرار تحت ضغط) ، أما على المستوى الاستراتيجي التكتيكي في صنع القرار العسكري، فستتمكن أنظمة القيادة المعززة بتكنولوجيا الذكاء الاصطناعي من تجنب العديد من أوجه القصور الملازمة

[14] عباس بدران ، (2010) ، الحرب الالكترونية : الاشتباك في عالم المعلومات ، مركز دراسات الحكومة الالكترونية للنشر والتوزيع ، بيروت (لبنان)، ص30.

لعملية اتخاذ القرارات الإستراتيجية التقليدية، حيث ستكتسب القدرة على اتخاذ القرار السريع -بل والتلقائي- بناءً على المعلومات المعززة، وهو الأمر الذي يُجنّبها الأخطاء البشرية، ويُكسبها ميزةً تنافسيةً مقارنةً بأنظمة اتخاذ القرار التقليدية."[15](سارة عبد العزيز سالم، 2019)

و هكذا ازدادت المخاوف لدى كل دول العالم من أن يصبح الفضاء الرقمي ذا طابع عسكري فعلي تسوده تجاوزات لا يمكن السيطرة عليها أمام الدخول في سباق نحو التسلح الرقمي منذ سنوات ، و هذا ما دفع بأكثر من " 100 دولة ببناء قدراتها الهجومية الرقمية في إطار لعبة حرة ومتزايدة الخطورة على أساس المعاملة بالمثل من الناحية الإستراتيجية إذ أن الاستخدام الضار لتكنولوجيا المعلومات والاتصالات معلن بوضوح في المذاهب ذات الصلة كوسيلة لتحقيق الأهداف العسكرية والسياسية وهذه المخاوف لا تستبعد الحاجة المشروعة للدفاع عن النفس" [16](حمدون إ. توريه، 2016، ص5)

كما أصبحت الحروب السيبرانية أحد أوجه الصراع الدولي، إذ يستطيع أحد أطراف الصراع أن يوقع خسائر فادحة بالطرف الآخر، وأن يتسبب في شل البنية المعلوماتية و الإتصالاتية الخاصة به، وهو ما يسبب خسائر عسكرية واقتصادية فادحة، من خلال" قطع أنظمة الاتصال بين الوحدات العسكرية وبعضها البعض أو تضليل معلوماتها أو سرقة معلومات سرية عنها، أو من خلال التلاعب بالبيانات الاقتصادية والمالية وتزييفها أو مسحها من أجهزة الحواسيب، وبالرغم من فداحة الخسائر، إلا أن الأسلحة بسيطة لا تتعدى الكيلو بايتس،

[15]سارة عبد العزيز سالم،(2019)، قراءة في دراسة لجيمس جونسون، أتمتة الحروب ، تأثير الذكاء الاصطناعي في سباق التسلح العالمي، مرجع سبق ذكره.

[16]حمدون إ. توريه، (نوفمر 2014) ، فريق الرصد الدائم لأمن المعلومات (الاتحاد العالمي للعلماء)، البحث عن الثقة السيبرانية، الاتحاد الدولي للاتصالات، سويسرا، ص 5.

تتمثل في فيروسات إلكترونية تخترق شبكة الحاسب الآلي وتنتشر بسرعة بين الأجهزة، وتبدأ عملها في سرية تامة وبكفاءة عالية، وهي في ذلك لا تفرق بين المقاتل والمدني، وبين العام والخاص، وبين السري والمعلوم [17] (محمد الحمامصي، 2014)

أمام هذا الوضع دفع بالدول إلى حشد جيوشها من الخبراء المعلوماتيين لضمان أمن وسلامة أنظمتها المعلوماتية من جهة و من جهة أخرى ، ومواجهة مختلف الاختراقات التي قد تحدث حيث تعمل على تنفيذ عمليات التجسس وإدارة الهجمات الإلكترونية بالإضافة إلى شن حروب المعلوماتية في وسائل الإعلام ومواقع التواصل المختلفة .

و " يمكن تصنيف المهام التي يمكن أن تقوم بها الجيوش السيبرانية في ثلاثة أنواع رئيسية و هي[18]: (إيهاب خليفة، 2019 ، ص .ص 150.151)

أولا: مهاجمة الشبكات :

تشمل اختراق الشبكات بكمٍّ هائل من البيانات أو وضع بيانات ومعلومات محرفة لإرباك مستخدمي الحاسبات، ونشر الفيروسات و البرامج الصغيرة المؤذية مثل الديدان، وتلغيمها بالقنابل المنطقية التي يتم تنشيطها في الوقت المناسب للمهاجم لكي تتلف ما تحتويه الحاسبات من بيانات وبرمجيات، أو القيام بهجمات سيبرانية أو مادية لقطع خدمات الإنترنت عن الخصم، وتدمير قواعد البيانات التي يمتلكها، وتعطيل قدرته على النشر السريع لقدراته وإمكانياته وقواته، أو قطع أنظمة الاتصال بين الوحدات العسكرية وبعضها وتعطيل شبكات

[17] محمد الحمامصي ، القوة الإلكترونية عنصر أساسي مؤثر في النظام العالمي، موقع العرب ، متاح على الرابط : https://alarab.co.uk/، تم الاطلاع عليه بتاريخ 2021/006/15، على الساعة 22:00

[18] إيهاب خليفة، مجتمع ما بعد المعلومات ، تأثير الثورة الصناعية الرابعة على الأمن القومي، ص. ص 151.150

الكمبيوتر، أو شل أنظمة الدفاع الجوي أو التوجيه الإلكتروني للخصم، أو السيطرة على وحدات القيادة والتوجيه، أو فقدان العدو قدرته على التحكم أو الاتصال بالأقمار الصِّناعيَّة.

ثانيا: الدفاع عن الشبكات:

تشمل هذه العملية حماية الشبكات وأجهزة الكمبيوتر من أي عملية اختراق خارجي ، ويجب أن يكون التأمين على مستوى البرمجيات(Software) ،و المكون المادي للشبكات (Hardware)، بحيث يتم تأمين الشبكة من أي اختراق ، وكذلك تأمين المكون المادي للشبكات مثل الخوادم أو الشَّرائح الإلكترونية، والتي قد تكون مبرمجة من قبل المصمم لكي تعمل في ظروف غير عادية لصالحه.

ثالثا :استطلاع الشبكات :

تعني القدرة على الدخول غير المشروع والتجسس على شبكات الخصم، دون أن يصاحب ذلك تدمير أو تخريب للبيانات والمعلومات ، والتي قد تشمل خطط دفاع وهجوم عسكري، أو أسرارًا عسكرية وحربية، أو معلومات سياسية و استخباراتية، ولا تتوقف وظيفتها على ذلك فحسب، بل يمكن من خلالها عمل خرائط لشبكات الحاسب الآلي واستخدامها مستقبلا في عمليات الهجوم الإلكتروني، كما يمكن أيضًا استخدامها في التأثير على أفكار وسلوكيات الخصم من خال شن حرب نفسية، وذلك بنشر مثل هذه الخطط العسكرية والبيانات أو إرسالها إليه مرَّة أخرى لكي يدرك إلى أي مدى هو مُخترق ولن يستطيع المواجهة.

و يمكن للذكاء الاصطناعي حسب المنظور الصيني محاكاة المناورات العسكرية عبر خلق خصوم اصطناعيين أذكياء، وهي بمثابة انتصار كبير لعدة دول سواء تلك التي تفتقر للخبرة القتالية مثلما هو الصين أو بالنسبة للولايات المتحدة

الأمريكية التي تريد دائما الاحتفاظ بالزعامة في المجال التكنولوجية و لا تقبل أي دولة تتفوق عليها أو بالنسبة لروسيا أو لكوريا الشمالية .

نظرا للأهمية الذكاء الاصطناعي و مساهمته في تغيير موازين القوى افتراضيا، أولت الدول المذكورة أهمية قصوى بتنمية قدراتها السيبرانية ، وخصصت مبالغ مالية هامة ، كما سطرت استراتيجيات تهدف كلها إلى الحفاظ على أمنها السيبراني و التصدي لمختلف الهجومات المحتملة مستقبلا .

و نعرض نماذج من الدول تعد قوى تكنولوجية في العالم أعدت جيوشا سيبرانية ، جعلتها في مرحلة تأهب قصور لمواجهة أي خطر محتمل ،و هي [19](عبد الغفار عفيفي الدويك،2019)

1.الصين :

خصص الجيش الصيني الكثير من الاهتمام لحرب المعلومات على مدى العقد الماضي ، و اهتم بتوسيع قدراته السيبرانية و اتخذ كعقيدة أساسية له " وثيقة "الشبكة الإلكترونية المتكاملة للحرب" Integrated Network‘ Electronic Warfare’. حيث انتقل تفكير الصيني إلى دمج كل من الجوانب الإلكترونية وغير الإلكترونية لحرب المعلومات داخل سلطة قيادة واحدة." 19و" منذ عام 2008، كانت العمليات العسكرية الرئيسية لهذا الجيش تشتمل على مكونات "الإنترنت" وعمليات المعلومات التي كانت ذات طبيعة هجومية ودفاعية في الوقت نفسه. كما أُعيد تنظيم الجيش عام 2015، من خلال إنشاء ثلاثة

[19]عبد الغفار عفيفي الدويك، (2019) ، إعادة تقسيم العالم على أسس سيبرانية: قراءة في تقرير التوازن العسكري 2018، مركز الأهرام للدراسات السياسية و الإستراتيجية ، متاح على الرابط: https://acpss.ahra.org.eg/News/16814.aspx
تم الاطلاع بتاريخ 2021/06/10، على الساعة 22:00

فروع دعم جديدة، بما في ذلك قوة الدعم الاستراتيجي (SSF) ، الأول للتعامل مع الاستخبارات والعمليات العسكرية في الفضاء السيبراني (دفاعية وهجومية)، والثاني للعمليات الفضائية العسكرية (المراقبة والأقمار الصناعية)، والثالث المسئول عن القدرات الدفاعية والهجومية والذكاء الإلكتروني.

2. المتحدة الأمريكية :

تتمتع الولايات المتحدة الأمريكية بقدرات إلكترونية متطورة و حددت إستراتيجية للدفاع عن النفس عام 2015 عن طريق "وزارة الدفاع ، حيث اعتبرت الفضاء (الأنترنت) كتهديد استراتيجي رئيسي للولايات المتحدة الأمريكية ، ووضعته في مرتبة تسبق الإرهاب للمرة الأولى منذ عام 2001. وتخطط القوات الجوية الأمريكية لدمج العمليات الإلكترونية الهجومية والدفاعية في نطاق قدرات "أنترنت" واسعة النطاق تسمى سرب العمليات الإلكترونية Cyber Operations Squadron بحلول عام 2026" وكان " الجيش الأمريكي قد أصدر دليلاً ميدانياً للحرب الإلكترونية في أبريل 2017، ثم أعلن الاتجاه إلى تطوير إستراتيجية في هذا المجال، تشمل الجهات الفاعلة على نطاق أوسع، وتتضمن سيناريوهات لتأمين البنية التحتية الحيوية الوطنية.

3. روسيا الاتحادية:

صدر أول بيان رسمي حول دور الجيش الروسي في الفضاء السيبراني "الآراء المفاهيمية حول نشاط القوات المسلحة للاتحاد الروسي" Russian Armed Federation في نهاية عام 2011. وحدد التقرير مهام القوة السيبرانية، مركزاً على دورها الدفاعي، والوقاية من حرب المعلومات.

كما أُعلن فى يناير 2012 عن ثلاث مهام رئيسية هى: تعطيل أنظمة المعلومات العدوانية، والدفاع عن أنظمة الاتصالات والقيادة، والعمل على الرأي

العام المحلي والأجنبي باستخدام وسائل الإعلام والإنترنت، واعتبار الحرب السيبرانية جزء لا يتجزأ من حرب المعلومات

4.كوريا الشمالية:

دخل الجيش الكوري الشمالي مجال الحرب المعلوماتية (IW) information-warfare تحت مفهوم "حرب الاستخبارات الإلكترونية" .(EIW) 'electronic intelligence warfare ، عن طريق " منظمتين هما مكتب الاستطلاع العام Reconnaissance General Bureau ,(RGB)، الذي يقوم بعمليات سرية في وقت السلم، وإدارة الأركان العامة General Staff Department (GSD)، وهي المسئولة عن العمليات السيبرانية لدعم الجهود العسكرية التقليدية.

6. الاتفاق الدولي لمواجهة الحرب السيبرانية

نظرا لخطورة الوضع أبدت بعض الدول استعدادها لخوض مثل هذه الحروب ، و أنشأت جيوشا سيبرانية ، في حين عقدت دولا أخرى اتفاقيات سياسية و عسكرية ، حيث توصلت الولايات المتحدة الأمريكية والصين في عام 2015 لاتفاق خاص بالحروب السيبرانية، يقضي بعدم شن أي هجمة سيبرانية بين الدولتين على البنية التحتية وشركات القطاع الخاص في حالة السلم[20]") Scott W. Harold, 2016)

[20] Scott W. Harold, The U.S.,(2016), China Cyber Agreement: A Good First Step, RAND, available in
https://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.htmll, consulted on june 13 , 2021 at 16:30

كما أعلن الاتحاد الأوروبي في أكتوبر عام 2017 أن شن هجمة سيبرانية من دولة عدائية على دول الاتحاد الأوروبي يعتبر" تصرف حرب "يستوجب الدفاع عن النفس. [21](Phil Muncaster,2017)

و بناءا على هذه المعطيات ، نؤكد بأن الدول التي تسبب تكون سببا في الحرب السيبرانية أو ضحية هذه الحرب، لابد أن تعيد النظر في مختلف المفاهيم التي فرضتها هذه الحرب السيبرانية خاصة في هذا العصر الذي يسيطر عليه الذكاء الاصطناعي،و التعامل بحذر أمام المخاطر و الهجومات غير المرتقبة ، أمام بروز مفهوم " الديبلوماسية السيبرانية، الذي يتطلب وضع معايير دولية ضد مختلف التهديدات مع فرض العقوبات في إطار دولي، في ظل غياب اتفاقيات دولية تنظّم انتشار واستخدام هذه الأسلحة الرقمية، فالقانون السائد حاليا في هذا المجال يسير وفق قاعدة "البقاء للأقوى". [22] (حمد الحمامصي، 2015)

كما تسعى بعض الدول للتفاوض فيما بينها وهذا في إطار الديبلوماسية السيبرانية عن طريق تبادل المعلومات حول الجرائم المعلوماتية وتحدياتها المختلفة من أجل بناء الثقة ، فقد "اتفقت كل من الولايات المتحدة الأمريكية وروسيا بعد مفاوضات على تحديد طرق التعاون في الأزمات السيبرانية وذلك عبر خط ساخن ومراكز الرد على الطواريء التي تحدث بسبب الأنترنت أو "طوارئ

[21] Phil Muncaster, (2017) EU to Declare Cyber-Attacks "Act of War", Infosecuritymagazine,
https://www.infosecurity-magazine.com/news/eu-to-declare-cyber-attacks-act-of/ consulted on may 28 , 2021 at 16:30

[22] حمد الحمامصي، الأنترنت شريك صناعة الإرهاب في العالم، مرجع سيق ذكره، متاح على الرابط : https://alarab.co.uk ، تم الإطلاع عليه بتاريخ 2021/05/25 على الساعة (10:00)

الأنترنت" وكذا الاتصال بين المراكز النووية لمواجهة مخاطر الجريمة المعلوماتية" [23] (United Nations Institute for Disarmament Reaserch, 2013)

فتفاوض الولايات المتحدة الأمريكية في المجال السيبراني و احتراسها على شن أي حرب سيبرانية يعود أساسا إلى اقتناعها " بامكانية تعرض بنيتها التحتية الرئيسية و اقتصادها لضرر كبير، حتى و ان كان ضررا مؤقتا، فهي توافق على الفكرة القائلة بأن حربا إلكترونية شاملة لن يربح فيها أحد " [24] David C.Gompert، 2016)

و هذا ما يؤكد استعداد الدول للتفاوض من أجل تحقيق الأمن الدولي الذي تهدده عدة مخاطر و اعتداءات من مختلف الجبهات في الفضاء السيبراني .

[23] United Nations Institute for Disarmament Reaserch, (2013)The Cyber Index International Security Trends and Realities, (United Nations Publications.

New York, available: www.unidir.org/files/publications/pdf , consulted on may 23, 2021 at 20:30.

24-ديفيد س. غومبرت ، هانس بيننديك ،(2016)، القدرة على الإرغام مواجهة الأعداء دون حرب، Approyou Center RAND، كاليفورنيا، (الولايات المتحدة الأمريكية) ، ص29 ، متاح على الرابط: file:///C:/Users/hp/Desktop/RAND_RR1000z1.arabic.pdf

تم الاطلاع بتاريخ 2021/06/07، على الساعة 21:00

7. خاتمة:

أصبح الفضاء السيبراني جزءاً لا يتجزأ من التفاعلات الدولية التى تبذل الأمم المتحدة والمجتمع الدولي الجهود لضبط الأمن فيه، خاصة و أن التهديدات في تزايد سريع و مستمر و فرص الحرب السيبرانية تتوسع باستمرار بشكل كبير ، و الأطراف المشاركة فيها تزداد يوما بعد يوم خاصة مع انتشار الذكاء الاصطناعي و أتمتة الأجهزة و أنترنت الأشياء ، مما يؤدي إلى ظهور كتل و تحالفات جديدة ، تتوحد بفضل المعلومة و التكنولوجيا و القوة السيبرانية و هي بوادر الخريطة الجديدة للعالم الافتراضي الذي بدت ملامحه تبرز منذ ظهور الصراعات القائمة بين المعسكر التكنولوجي الذي يقوده الولايات المتحدة الأمريكية و بين المعسكر التكنولوجي الثاني الذي يقوده الصين في انتظار انضمام الدول إلى التحالفين وفقا لمبدأ المصلحة المشتركة المبنية أساسا على القوة السيبرانية والقدرة على صناعتها وإدارتها و هذا كله من شأنه أن يؤثر على الأمن الدولي في ظل غياب أطر قانونية دولية رادعة للحروب السيبرانية و منظمة لتطبيقات الذكاء الاصطناعي التي تجاوزت كل التشريعات في العالم.

و لهذا و حتى تتمكن الدول من الحد من هذه الحروب و التخفيف من حجم الصراعات الموجودة لابد من تحقيق الأمن السيبراني الذي لن يتأتى إلا بمشاركة كل الفواعل في المجتمع من حكومات و أفراد ومنظمات و مجتمع مدني و شركات تكنولوجية و هيئات بحثية .