

اسم المقال: الخصوصية الانسانية في ظل عصر الابداع التكنولوجي

اسم الكاتب: انسام فائق العبيدي

رابط ثابت: <https://political-encyclopedia.org/library/9562>

تاريخ الاسترداد: 2026/04/10 14:07 +03

الموسوعة السياسية هي مبادرة أكاديمية غير هادفة للربح، تساعد الباحثين والطلاب على الوصول واستخدام وبناء مجموعات أوسع من المحتوى العلمي العربي في مجال علم السياسة واستخدامها في الأرشيف الرقمي الموثوق به لإغناء المحتوى العربي على الإنترنت. لمزيد من المعلومات حول الموسوعة السياسية - Encyclopedia Political، يرجى التواصل على info@political-encyclopedia.org

استخدامكم لأرشيف مكتبة الموسوعة السياسية - Encyclopedia Political يعني موافقتك على شروط وأحكام الاستخدام المتاحة على الموقع <https://political-encyclopedia.org/terms-of-use>

تم الحصول على هذا المقال من موقع مجلة قضايا سياسية الصادرة عن كلية العلوم السياسية في جامعة النهدين ورفده في مكتبة الموسوعة السياسية مستوفياً شروط حقوق الملكية الفكرية ومتطلبات رخصة المشاع الإبداعي التي ينضوي المقال تحتها.



الخصوصية الانسانية في ظل عصر الابداع التكنولوجي[∇]

Human privacy in the era of technological innovation

Ansam Faiq Al-Obidi

المدرس انسام فائق العبيدي*

المخلص:

لقد اصبحت سمة الاغتراب الانساني وفق اسس التوحد التكنولوجي من اهم سمات العصر الحالي. ان تلك التطورات التكنولوجية المستمرة بفضل العقل البشري هي ذاتها التي تسببت في تلك العزلة الانسانية سواءً على المستوى الاسري ام المجتمعي. و قد تداخلت تلك التقنيات في اثارها بين الايجابي التطويري و بين السلبي المتجسد بخلق مجتمعات جديدة بعيدة تماماً عن ادراك مخاطر و ابعاد فقدانها للخصوصية الانسانية نتاج التقلب وفق اسس التحول الالكتروني .

لقد هدفت الدراسة البحثية الى ايضاح ماهية و اهمية التحول الرقمي في المجتمع بكافة تقسيماته و طبيعة الاثار المترتبة عنها على خصوصية الفرد و امن الدولة. و بين الطروحات الايجابية للتحول الرقمي الى التحديات و الصعوبات تحتم جعلها اهدافاً. استوجب وضع استراتيجيات تطويرية تتزامن في فاعليتها مع مخرجات العصر الرقمي دائم التطوير. حيث خلقت تلك الثورة التكنولوجية تحديات على كافة المستويات خاصة فيما يتعلق بالقطاع المدني و القطاع العسكري وفق الحروب الالكترونية و شن الهجمات السيبرانية و الارهاب الالكتروني. ان تلك المسميات تجسد في جوهرها المخاطر و التحديات التي استوجب الحد منها وفق صيغ التعاون و التطوير على كافة الاصعدة المحلية و الدولية ضماناً لامن و سلامة و بناء الانسان.

أن المجتمعات لا تبنى بالاجهزة الالكترونية فحسب بل الاساس في الاستمرار الكوني نابع من تنمية و تطوير الثروة البشرية المحكوم بتوازن الوعي الانساني العقلاني وفق اسس تطويرية تكنولوجية. ان الخصوصية الانسانية جوهرها تأمين استمرارية الثروة البشرية و امنها. و قد تسبب ذلك في العديد من النزاعات و الحروب الاهلية منها و الدولية و النزاعات المسلحة ايضاً. لقد كانت الحروب السابقة للعصر التكنولوجي ذات سمات عديدة انحسر الكثير منها في ظل التطور التكنولوجي. الا ان القاسم المشترك للحروب ايا كان مسبباتها و كنهها والاطراف المتنازعة الخاسر منها و المنتصر لا يزال قائماً الا وهو الخسائر الجسيمة في الثروة البشرية سواءً بالقتل ام التشويه ام الامراض المزمنة و العقلية والنفسية. ان نتائج الحروب الالكترونية الانية وفق افرازات التطورات التكنولوجية قد انعكست بصورة

تاريخ النشر: 2025 /3/31

تاريخ القبول: 2025/2/13

∇ تاريخ التقديم : 2025/1/10

* جامعة بغداد / كلية العلوم / وحدة حقوق الانسان ansam.faik@sc.uobaghdadThis is an open access article under the CCBY license CC BY 4.0 Deed | Attribution 4.0 International
| Creative Common" : <https://creativecommons.org/licenses/by/4.0/>

جلية على الابعاد السياسية و الاقتصادية و الاجتماعية و الثقافية وحتى التوجهات الاخلاقية و التنموية المجتمعية. ان الحروب المعلوماتية التكنولوجية لا تتوقف في توجهاتها عند حدود غزو الفضاءات الالكترونية. حيث اصبح التوجه الاشد خطورة يكمن بأعتماد الانظمة الذكية لتغيير التوجهات الفكرية من عادات و تقاليد و قيم و اخلاقيات نتاج توظيف التقنيات الالكترونية. باعتماد استراتيجيات تحاكي بها العقول بل و تخاطب المشاعر و العواطف و تتسبب بخلق الارهاب الرقمي و اثاره وفق تغييرات مجتمعية شاملة على كافة المستويات السياسي و الاقتصادي والثقافي. و تشكل خطراً جسيماً على بناء و تغيير جوهره الامن الانساني الا و هو الفرد. وهو ما اعتمدته حروب الجيل الخامس و السادس كأساس في استراتيجياتها الممنهجة المستقبلية. لذا تعد الاكثر فتكاً في المجتمع بما تتسبب به من فجوة و خلل في العقول البشرية لخلق ازمات سياسية و اقتصادية و بالتالي تشكل اكبر تهديد للامن القومي. ان خلق استراتيجيات تطويريه تتناسب مع طبيعة تلك التطورات و توجهاتها اصبح ضرورة حتميه قصوى ضماناً لامن الانسان و بناء الدولة و امنها القومي .

الكلمات المفتاحية : الحروب المعلوماتية , التطورات التكنولوجية , الخصوصية الانسانية, التقنيات الالكترونية , التحول الرقمي . الامن المعلوماتي , الثروة البشرية , الارهاب الرقمي .

Abstract

This study aimed to identify the digital transformation and its challenges. Technology has no longer become as tools with techniques used to facilitate business performance and development. But, rather its impact has expanded to all aspects of our lives. Until it has become the tip of the spear that changes the global scene. Its huge influence which has spread all over the world on various aspects personal, societal, national and international and even the military aspects. Information warfare does not stop at simple forms of cyberattacks. The most dangerous approach lies in the adoption of smart systems to change intellectual orientations, customs, traditions, values, and ethics. This is achieved by adopting strategies that simulate minds and appeal to feelings and emotions, creating digital terrorism and its effects through comprehensive societal changes at all political, economic, and cultural levels. This poses a grave threat to the construction and transformation of the essence of human security: the human being.

Keywords: cyber warfare, technological developments, human privacy, electronic technologies, digital transformation, information security, human capital, digital terrorism.

This is an open access article under the CC BY license CC BY 4.0 Deed | Attribution 4.0 International | Creative Common" : <https://creativecommons.org/licenses/by/4.0/>

المقدمة

لقد استحدثت الثورة التكنولوجية نمط حياة جديد للبشرية جمعاء تعتمد التقنيات الالكترونية في تسيير كافة اموره الحياتيه. و قد تجسدت تلك التحولات الرقمية من خلال العديد من التقنيات الالكترونية كالحواسيب و الهواتف النقالة و الشبكات والتقنيات العسكرية الالكترونية المتنوعه حتى اصبحت السمات الالكترونية بكافة تقنياتها من اهم سمات عصرنا الحالي التي لا سبيل للاستغناء عنها. بل تستوجب التطوير الدائم لتكون الدولة عنصر فاعل في سباق التطور التكنولوجي الدولي العالمي. نتاج تلك التوجهات التقنية الشاملة فقد استحدث نمط جديد من الحروب السيبرانية غير المرئية على ارض الواقع الا في نتائجها الكارثية. حيث نزاعات الفضاءات الالكترونية ذات مسميات حربية جديدة بين الارهاب الالكتروني الى شن هجمات سيبرانية. لقد انتهى عهد الحروب النمطية التقليدية المباشرة. و الانتقال الانى لعهد اللامباشرة الالكترونية مخفية المصدر و جسمة الاثر المدمر للبنى التحتية الالكترونية للدول كالتجسس والفايروسات الالكترونية. حيث رهان سباق الحصول على المعلومات و استغلالها بات يعد من اسس الحروب الالكترونية المستقبلية و الذي يتسبب بخسائر فادحة عسكرياً اقتصادياً و سياسياً. ففي ظل التطور التكنولوجي العسكري و تقنياته المهولة تدار الحروب من خلال الشاشات الالكترونية. لذا فقد اصبح الاستثمار في الاتقان التكنولوجي العسكري من اهم ماتسعى الدول للتنافس على تطويره. لقد شمل هذا الميدان بتطوراته دخول العديد من الدول ميادين حروب الفضاءات الالكترونية سعياً للحفاظ على امنها القومي و خصوصيتها الانسانية . ان ماتشكله تلك التوجهات السيبرانية من مخاطر مستمرة متفاقمه قد اوجد تغييرات جذرية في طبيعة العلاقات الامنية و النزاعات و موازين العلاقات الدولية.

اهمية البحث : ان قولبت العالم في بوتقة العالم الالكتروني وفق صيغ ابداعية مبهرة طاغية في تأثيراتها على السمات الانسانية للحضارة البشرية. حيث توجهات العقل البشري الذي لا حدود لابداعته تتحد و تتحدد و تنحسر شي فشيء في تراجع في خصوصية سماتنا و امننا الانساني. حيث يطغى في الوقت ذاته التوجهات التخصصية في عالم الذكاء الاصطناعي و توظيفاته . و ينتشر هوس طغيان ذلك ليتجسد في مخاطر كارثية تتضح في طبيعة الحروب الالكترونية التي اجتاحت العالم. فضلا عن تفاقم اهمية القوة الالكترونية التي اثرت و غيرت بشكل مباشر و فاعل في طبيعة التفاعلات الدولية على المستوى الاقتصادي و السياسي والعسكري و الثقافي . مما استوجب التنوير على طبيعة تلك التحولات في المفاهيم الامنية و الصراعات الدولية في ظل تلك التطورات التكنولوجية و خاصة اهمية العلاقة بين الامن القومي و الامن الالكتروني و نتائجها على خصوصية الامن الانساني.

أهداف البحث : لقد هدف البحث الى توجيه الضوء على ماهية الغزو التكنولوجي و التحول و الحروب والارهاب الرقمي واثارها الشاملة لكافة نواحي حياتنا سواءاً على المستوى الاقتصادي ام السياسي او الاجتماعي او الثقافي. ان الطروحات البحثية شملت ايضا ماهية الامن الانساني و الحروب المعلوماتية

هدف ايضا الى التتوير على مايجب ان تكون عليه طبيعة العلاقة بين الانسان و التكنولوجيا في عصر ملئ بالتحديات و الابداعات التي سهلت علينا الحياة بتقنيات الذكاء الاصطناعي تلك. الا انها في الان ذاته خلقت مهددات كارثيه في اثارها تجاه امننا الانساني و خصوصيته. وحيث ان النئ عن العالم الرقمي اصبح من الفرضيات الخياليه. لذا استوجب الطروحات الافضل للتغلب على تلك التحديات بالذكاء البشري الذي اوجدها لحماية خصوصية هويته الانسانيه.

مشكلة البحث : ان التغيير الشامل لطبيعة العلاقات والصراعات الدولية الذي فرضته التطورات التكنولوجية. اوجد واقعاً جديداً في مفاهيم الامن و النزاعات و الصراعات وفق الفضاءات الالكترونية و الاجيال العسكرية المستحدثة. ان مافرزته الثورة التكنولوجيا من تطورات شملت كافة جوانب الدول. وامتدت تلك التطورات لتشمل الجوانب السياسية و العسكرية و الامنية و المجتمعية و الثقافية. فهل خلقت تلك التوجهات الالكترونية علاقة تطويرية في المفاهيم و التوجهات الامنية ؟و الى اي مدى يقع الامن القومي و الانساني تحت طائلة تهديدات الحروب و الارهاب الالكتروني ؟ وفي طروحات البحث اجابة على العديد من الاسئلة من ضمنها :

- ما هية الحروب الالكترونية و الحروب السيبرانية ؟
- هل امننا الانساني يقع تحت طائلة مخاطر الارهاب الرقمي الدولي ؟
- هل غيرت الثورة التكنولوجيا مفاهيم القوة في العلاقات الدولية ؟

فرضية البحث : أن تزايد منافع التكنولوجيا بتطوراتها اللانهائية هو ذات التطور المتسبب بتزايد المخاطر على الامن و السلم الدوليين . اي كلما تقام اعتماد البشرية على التطورات الالكترونية كلما ارتفعت نسب المخاطر على امننا الانساني. فالتكنولوجيا الرقمية في المجال العسكري و الامني خاصة الغت الاستراتيجيات العسكرية التقليدية لتعتمد الفضاءات الالكترونية في ساحاتها القتالية المستقبلية. حيث تستقبل تلك الفضاءات فاعلين جدد ظاهرين و مستترين في الميادين السيبرانية. ليكون تزايد في نسب المخاطر التي ابتدعها الانسان. فتحديات الذكاء الاصطناعي تتمثل بفايروس قابل لهدم بنى تحتية الكترونية لدول باكملها. مما يستوجب الدخول في السباق الالكتروني حفاظ على امننا المستقبلي و حروبه الالكترونية القادمة.

منهجية البحث : اعتمدت الدراسة تحليل كافة الطروحات سعيا لايجاد حلول واقعية مثمرة وفق المنهج الوصفي التحليلي لماهية المفردات المطروحة و الاشكالات موضوعة البحث .

أولاً : الحروب المعلوماتية و اثارها على الامن الانساني

لقد تغيرت العديد من التوجهات و المفاهيم الامنية و السياسية و الاقتصادية نتاج ما ساهمت فيه التطورات التكنولوجية و الفضاءات الالكترونية و الحروب المعلوماتية من تغييرات اساسيه في طبيعة العلاقات الدولية .

"ساهم الطابع التكنولوجي في إيجاد طرق جديدة للصراع بديلة للحرب المباشرة بين الدول، حيث ساهمت الآليات التكنولوجية في مساعدة المنظمات والدول في التنسيق بين جهودها والتفاعلات فيما بينها الكترونياً بعيداً عن الاتصال المباشر، وأدت الثورة التكنولوجية الى تغيير شكل الحرب وأدواتها والفاعلين فيها مما ساعد على اختلاف درجة التهديد وآثاره وطبيعته ومصادره وظهور حرب الشبكات وحروب الفضاء الإلكتروني، وأصبح الارهاب جريمة عابرة للحدود القومية من حيث النشاط والخطط والتمويل والأعضاء، وتساعد نشاط الجماعات الارهابية عبر الفضاء الإلكتروني وتعزيز بعدها العالمي وتم استخدام المنجزات التكنولوجية في ممارسة الارهاب، والتي استطاع الارهابيون من خلالها تحقيق أضرار غير متوقعة وهائلة تتجاوز التهديدات التي تمثلها الدول لبعضها البعض، إذ استغلت الجماعات الارهابية بكافة أشكالها وأنماطها الفكرية المزايا الالكترونية كعنصر حيوي لدعم وتحقيق أهدافها، وتحولت بعد أن كانت مجموعات قلائل من الأفراد متوزعة جغرافياً الى مجتمع افتراضي غير محدد الأبعاد الكمية"⁽¹⁾

لقد تغيرت معالم الحياة بتوجهاتها الانسانية وفق الاجتياح الالكتروني بكافة قنواته الاعلاميه و وسائل التواصل الاجتماعي و سيطرت الهواتف النقالة وصولاً لغزو الفضاءات الالكترونية والاستراتيجيات الحربية السيبرانية. حيث اصبح تحقيق الاهداف وفق السباق الالكتروني يتوقف على كم القدرات المعرفية و التطويرية الالكترونية. ان الارهاب و الحروب الالكترونية العابرة للحدود القومية باتت تعتمد على ومدى سعة الامكانات التوظيفية التكنولوجية لكافة مرافق الدولة.و التي تحتاج تخصيصات ماليه سائده وفق اسس حماية دائمة التطوير. لم تعد الفضاءات الالكترونية محددة بكونها مجالات حديثة للتعاون و الصراعات الدولية. ان تكلفة الهجوم السيبراني الاقل تكلفه و اكثر دقه اوسع مدى في تحقيق الاهداف المخطط لها .اوجد مجالات تسويقية لهذه التوجهات و ترك للتقليدية منها. ففي ظل انحسار حدود السيادة الوطنية الجغرافية في الفضاءات الالكترونية و التي اصبحت تشكل عاملاً مشجعاً لدخول فاعلين جدد. ونظراً لمحدوده القدرات في الردع الالكتروني لصعوبه تحديد الجبهه الاجراميه وموقعها الجغرافي وضعف التوجه القانوني بهذا الخصوص قي الغالب. فقد انبثقت شركات دولية تخصصية في الهجمات السيبرانية. و اصبحت الدول ذات الامكانات المحدودة في التطورات التكنولوجيا تستثمر في تلك الشركات تحقيقاً لاهدافها في الدخول الى سباق التسلح الالكتروني. ان الكيانات الاستثمارية ذات التوجهات العسكريه

(1) ريهام عبد الرحمن رشاد، اثر الارهاب الالكتروني على تغيير مفهوم القوة في العلاقات الدولية دراسة حاله تنظيم الدولة الاسلاميه، المركز الديمقراطي العربي، 2016.

الالكترونية الناشطة في مجالات الامن السيبراتي و المتميزة بالهجمات السيبرانية قد اصبح لها دور فاعل حيوي في تغيير موازين التفاعلات الدولية.حتى ان العديد من الدول اعتمدتها باعتبارها منتج و مطوره لاجهزة مكافحة التجسس حفاظ على امنها القومي و اسناداً لاستمرار وجودها الانساني و خصوصيتها.

○ دراسات سابقة

"ووفقاً لدراسة أجرتها جامعة ستانفورد؛ فإن 64 في المئة من الأخبار المضللة التي تُنشر عبر الإنترنت تجري مشاركتها من دون تحقق. في حين وجدت دراسة لمعهد ماساتشوستس للتكنولوجيا أن الأخبار الخاطئة تنتشر أسرع من الأخبار الحقيقية؛ إذ يُعاد نشرها أكثر من الأخبار الصحيحة بنسبة 70 في المئة. وتبين هذه البيانات كيف أن الاستخدام الممنهج للتقنيات الرقمية يمكن أن يُحول المنصات المعلوماتية أسلحةً استراتيجيةً في الصراعات الحديثة، ولا سيما تلك التي تستهدف التأثير في الرأي العام، وتوجيه السلوك الجماعي" وفقاً لتقرير صادر عن شركة أبحاث الأمن السيبراني (Cybersecurity Ventures) ارتفعت الهجمات السيبرانية بنسبة 38 في المئة عام 2023، واستهدفت أساساً تعطيل البنى التحتية الرقمية الحكومية، مثل شبكات الطاقة والخدمات الصحية، وأنظمة النقل. وتشير إحصائيات في التقرير إلى أن هذه التهديدات السيبرانية تستهدف يومياً ملايين الأجهزة والأنظمة الحيوية في العالم، وأن الخسائر العالمية الناتجة منها تجاوزت 8.4 تريليون دولار في عام 2022، مقارنةً بـ5.99 تريليون في العام الذي سبقه وتبين تقارير البنك الدولي أن الاقتصادات الناشئة خسرت ما يقارب 12 في المئة من ناتجها المحلي الإجمالي بسبب الهجمات السيبرانية في الأعوام العشرة الأخيرة؛ ما يُظهر التأثير الهائل لهذه الحروب في استقرار الدول النامية، وإضعاف قدرة الأنظمة الوطنية على الاستجابة للأزمات. يُشير دانيال أبوت، الكاتب والباحث الأمريكي المتخصص بالشؤون السيبرانية، في كتابه "دليل حروب الجيل الخامس"، إلى أن هذا النوع من الحروب هو "حرب المعلومات والإدراك"؛ إذ يستهدف التأثير في عقلية المجتمع وسلوكه، وكذا الأفكار والتصورات العامة بدل التركيز على تدمير البنية التحتية المادية ويسهل عمل هذه الحروب الاعتماد المُكثف والمُفرط على التقنيات المتقدمة، مثل الذكاء الاصطناعي، وتحليل البيانات الضخمة، الذي سمح بفهم الأنماط السلوكية، وتوجيه القرارات الفردية والجماعية، وإنشاء واقع جديد من دون إدراك ووعي كاملين من الأفراد."⁽¹⁾

"هجمات سيبرانية واسعة على الشركات والمؤسسات التجارية الكبرى مثل: تسريب بيانات 250 مليون عميل من عملاء شركة ميكروسوفت العملاقة. اختراق مجموعة "ماريوت" الفندقية التي تضم 2.5 مليون

(1) علي محمد الخوري، المعارك الصامتة في حروب الجيل الخامس، أبوظبي، المصدر: مفكرو الإمارات، 2024

<https://arab-digital-economy.org/10756>

عمل. اختراق شركة "تويتر" عبر استهداف حسابات المشاهير على تويتر. اختراق شركة "زوم" وتسريب بيانات أكثر من 500 ألف مستخدم للتطبيق. اختراق شركة "إيزي جيت" البريطانية للطيران وتسريب بيانات أكثر من 9 ملايين عميل. تسريب بيانات 44 مليون عميل تابعين لشركة اتصال باكستانية. تسريب بيانات عملاء شركة "إنتل" العملاقة لتصنيع معالجات الكمبيوتر. اختراق شركة "فاير أي" واحدة من أهم شركات أمن المعلومات على المستوى العالمي-اختراق شركة "سولار ويندز" المنتجة للبرمجيات بشكل واسع عالمي⁽¹⁾

"تناولت الدراسة الفضاء الإلكتروني كمحور جديد للصراع الدولي، من شأنه أن يُسبب خسائر فادحة قد تكون اقتصادية أو عسكرية أو اجتماعية أو سياسية، وتُوضح أن أهم التهديدات التي تُدار في الفضاء الإلكتروني هي الإرهاب الإلكتروني والجريمة المنظمة مما جعلها تحديات للأمن العالمي كما تقترح الدراسة إطاراً نموذجياً لتعزيز الأمان في الفضاء الإلكتروني ويشمل كافة النواحي سواء الإستراتيجية أو التشريعية أو التنفيذية، وخلصت الدراسة لنتائج أهمها أن العصر الذي نعيشه هو عصر رقمي بامتياز وأن التدابير التقنية التي تُتخذ لمواجهة هذا النوع من الانتهاكات في الفضاء الإلكتروني غير قادرة على مكافحة هذا النوع ومن هنا تبرز أهمية وجود إطار تشريعي وطني في ظل تنسيق إقليمي يُستكمل بتعاون دولي"⁽²⁾

"وكانت لكورتل ويوب (2017) نظرة أخرى لمتطلبات التحول الرقمي حيث قسمها إلى متطلبات إدارية أهمها وضع الاستراتيجيات وخطط التأسيس وذلك بتشكيل إدارة أو هيئة للتخطيط والمتابعة والتنفيذ، والتحول إلى الهياكل المصفوفية والشبكات، ومتطلبات بشرية تركزت حول الاستثمار في العنصر البشري ورأس المال البشري عن طريق اكتشافهم وتطويرهم، ومتطلبات فنية عن طريق توفير البنية التحتية التي تشمل تحسين شبكة الاتصالات، والمتطلبات الأمنية لضمان أمن المعلومات وسريتها."⁽³⁾

تبين الدراسات السابقة أهمية توجيه الضوء على ماهية الهجمات السيبرانية و ماينتسبب به من اثار مدمرة واسعه على بناء و مستقبل الدول . لقد تغيرت مقاييس القوى العسكرية التي كانت محددة و لعقود مضت بمدى القدرات العسكرية من تجهيزات كالقنابل و الصواريخ و الاساطيل الحربية و حجم القوات العسكرية.فهجوم التطور التكنولوجي الذي اجتاح كافة توجهاتنا الحياتية و خاصة العسكرية منها اوجد مخاطر مهولة.و اصبح سباق الهيمنة التكنولوجية هي الاساس الذي سيشكل القوى العظمى الجديدة وفق

Frank Downs, Top Cyberattacks of 2020 and How to Build Cyberresiliency, November 2020, Available⁽¹⁾

⁽²⁾ حياة حسين، الفضاء الإلكتروني وتحديات الأمن العالمي، مجلة العلوم القانونية والسياسية، المجلد 12، العدد الأول، ابريل 2021.

⁽³⁾ فريد كورتل و آمال ويوب " القيادة الإدارية كأحد مقومات التحول الناجح للإدارة الإلكترونية". أبحاث المؤتمر الدولي المحكم : الإدارة الإلكترونية بين الواقع والحتمية .جامعة البليدة، الجزائر. 2017.

العالم الافتراضي ذا القوى القطبية التكنولوجية. لم تتحدد تأثيرات التقنيات الالكترونية بتسهيل امور حياتنا اليومية و تنظيمها فحسب. فقد اصبحت تلك التقنيات بمثابة الادمان الالكتروني الذي دخل مجتمعاتنا و استهلك اقتصادها. لكن التساؤلات التي تعد الاخطر انيا تتمثل في ماأنشاته تلك القوى الالكترونية الحربية العسكرية من عالم جديد يزداد خطورة بتزايد تطور تلك التقنيات. فهل خضعت بنية الانظمة الدولية لتغيير شامل وسط تلك الحروب و التفاعلات؟ وهل سيكون للفاعلين الجدد في مجالات الفضاءات الالكترونية و حروبها السيبرانية دورا فاعلا مستقبلا مغيرا لموازن القوى ؟ و هل اختفى العهد الذي فيه تكون ساحة القتال محددة و جهاتها الفاعله و مدتها من خلال استبدالها بالحروب السيبرانية التي تغلب عليها مجهولية المسبب و مهددة للسلم و الامن الدولي و لامن الانسان و تنميته. ان طروحات الدراسات السابقة تؤكد كل تلك المتغيرات و الاسوء يكمن في تغيير النهج الانساني و خصوصيته .

○ مفهوم الامن الانساني

"الامن الإنساني مصطلح جديد يستعمله أصحاب الاختصاص ليدل على كل أبعاد ومتطلبات الإنسان في كل مجالات الحياة، أى كل ما يحتاجه من أمن على نفسه وماله وأهله ووطنه،... ولذلك تناولت الدراسات المختلفة الأمن على الأرواح والأبدان والصحة، والأمن على الأموال والممتلكات والأعراض والكرامة، والأمن الغذائي والاقتصادي، الأمن البيئي والبحري، وأمن الشعوب والطوائف والأقليات، وغير ذلك من مشتقات الأمن ومفرداته التي تتطور وتتحدد بحسب التطور العلمي والاجتماعي والحضاري، وبحسب الاستخدامات والمفاهيم التي تتناولها المنظمات الدولية والدول"⁽¹⁾

"الامن الإنساني هو أسلوب للأمن الدولي والقومي يعطى أولوية للبشر وتفاعلاتهم الاقتصادية والاجتماعية المعقدة"⁽²⁾

"والامن الإنساني كذلك يعنى حماية الحريات الأساسية التي تعد جوهر الحياة وحماية البشر من التهديدات الشديدة وواسعة الانتشار؛ أى حماية جوهر الحياة لكل البشر بطرق تعزز حرياتهم وتلبى احتياجاتهم . ويعنى أيضا استخدام الآليات التي تبنى نقاط قوة وآمال البشر، وخلق أنساق اقتصادية وثقافية وعسكرية وسياسية واجتماعية وبيئية تعطى للبشر اللبنة الأساسية للبقاء على قيد الحياة واحترام الكرامة والحياة"⁽³⁾

(1) نور الدين مختار الخادمي، القواعد الفقهية المتعلقة بالأمن الشامل، المجلة العربية للدراسات الأمنية والتدريب، جامعة نايف العربية للعلوم الأمنية، العدد، 42، السنة، 2021، ص 21

(2) Gregoratti, catia , human security definition in : [www.britannica.com / topic/ human security](http://www.britannica.com/topic/human%20security), – 2016.

(3) Final report human security now in: – human security in theory and practice : an overview of human security concept and the United Nations Trust Fund for Human Security, new York , Human Security Unit, United Nations, 2009.p. 5.

"يرى الأمن المجتمعي أو الخاص بالدولة أنها الملاذ الأخير وأن الدولة المتحدثة الرسمي عن الفرد في حين يدعو الأمن الإنساني إلى التحرك تجاه كيانات أقل من الدولة أو أعلى لحماية البشر كما يتضمن ابعاد مختلفة أكثر من مجرد الحفاظ على الدولة أو الهوية التي تعتبر محورا اساسيا في الأمن المجتمعي".⁽¹⁾

"يتفق مفهوما الأمن الإنساني وحقوق الإنسان على أن كليهما ينص على توافر حد من الحقوق السياسية والاقتصادية والاجتماعية للأفراد بغض النظر عن النوع أو الدين أو العرق"⁽²⁾

يتوحد مفهوم الامن الانساني وفق التعاريف السابقة بتفاصيله مع مفهومي حقوق الانسان و حماية الحريات الاساسية للانسان. حيث يعد امن الفرد هو الاساس في امن الدولة. كون الثروة البشرية ذات الاولوية في بناء المجتمع. فأهمية امن الفرد من الخطوات الاستراتيجية الاساسية لبناء الدولة و مستقبلها. لقد اصبح امن الانسان و البشرية جمعاء تحت طائلة توجهات عديدة من المهددات لامنه و استمراره. الا ان هنالك توجهان يعدان من الاشد خطورة على الامن الانساني. التوجه الاول يتجسد بالكوارث البيئية المتفاقمه كالزلازل و الفيضانات و الاعاصير و الحرائق الجسيمة. و رغم كونها كوارث كونية. الا ان يد الانسان ايضا كان لها دوراً كبيراً في رفع نسب تلك الكوارث بتجاوزاته المدمرة لبقاء البيئة الخضراء و الحفاظ عليها .

"دأب الانسان على تدمير بيئته التي تعتبر الاطار الذي يعيش فيه ويحتاجها للحصول على مقومات حياته من ماء صالح للشرب و طعام واماكن ملائمة للسكن. الانسان هو أساس التغيرات البيئية وهو المسؤول عن استغلال جميع الموارد البيئية في الارض، والانسان هو صانع التنمية والقوة المتنفذة. إن احتياج الانسان لتأمين حياته وضمن العيش الآمن ادى الى استنزاف موارد الطبيعة مما نجم عنها الاخلال بالبيئة. يسر التقدم التكنولوجي للانسان مزيدا من فرص إحداث التغير في البيئة في ضوء ازدياد حاجته للغذاء والماء وتحقيق الرفاهية مما جعله يبحث عن وسائل توفر له ذلك حتى شن عملياته الواسعة بإزالة اشجار الغابات وحول ارضها لمجمعات سكنية ومعامل صناعية ومنشآت تجارية، كما افرت باستخدامه المبيدات الحشرية والاسمدة الكيماوية في الاراضي الزراعية واخيرا الرعي المكثف مما ساهم باخلال توازن النظام البيئي".⁽³⁾

(1) محمد العدوى، الأمن الإنساني ومنظومة حقوق الإنسان: دراسة في المفاهيم والعلاقات المتبادلة في

www.policemc.gov.hk2016

(2) خديجة عرفة، مفهوم الأمن الإنساني وتحديات الإصلاح في القرن الحادي والعشرون، شبكة إمارات نيوز في:

http://www.emase.com/, 2016

(3) عمر المنصوري، الانسان يدمر الارض الى غير رجعة، العراق 2017 /https://www.rudawarabia.net

اما التوجه الثاني فهو من صنع العقل البشري و تطويره. متمثلة بالثورة التكنولوجية بكافة وسائلها وتقنياتها بين الفضاءات الالكترونية و حروبها و بين ما تسببت به من تلوث فكري و خلق لعصر التفاهة. نتاج مايبث في وسائل التواصل الاجتماعي من تويتير و انستغرام و الالعاب الالكترونية بغرف الدردشة و الاباحية. لقد رافق تلك التوجهات الالكترونية اشكال الفساد و التحريض على العنف و الارهاب الالكتروني و التجاره المحرمة بمختلف اشكالها باعتماد توجيه العقول البشرية خاصة الفئات العمرية الفتية الشابة التي يسهل توجيهها لضمان تدمير العناصر الاساسية في بناء مستقبل الدول. فلم يتوقف حدود التغيير عند هذا التغيير الثقافي الجذري فقط بل اتسع ليكون عامل حيوي اساسي في بناء توجهاتهم المستقبليه بين الابتعاد عن التعليم الى اعتماد طرق يكون فيها الكسب السريع و تزييف الحقائق و المعلومات خاصة بمجال الاعلانات المزيفة الترويج . ان اجتياح الثورة التكنولوجيا للمجالات العسكرية و الامنية و السياسية تسبب في ايجاد نوع جديد من الحروب الالكترونية دائمة التحديث وفق طبيعه اجيال جديدة متطورة في ميادين الصراعات و النزاعات التكنية الذكية. مما اوجد تداخل للعديد من الدول في ميادين صراعات الفضاءات الالكترونية على عكس ماسبق العصر الالكتروني من تحديد لميزان القوى العظمى و ماهيتها و توجهاتها .

"إن الفرد هو جوهر المجتمع ونواته، ومن ثم فلا بد أن يكون الفرد هو جوهر ونواة الأمن الإنساني. والأمن الإنساني ليس فقط أمن الأرض، ولكنه أمن الشعوب، وليس محدودًا بالأمن من خلال السلاح، ولكنه الأمن من خلال التنمية، وهو ليس أمن الأمم فحسب، ولكنه أمن الأفراد في بيوتهم ووظائفهم، والتحرر من الخوف عن طريق حماية الأفراد من العنف والنزاع المسلح، والحروب الأهلية، والإرهاب الداخلي والخارجي الذي توجّه حروب الأجيال المتعاقبة التي أفرزتها تكنولوجيا الاتصال الحديثة، ومنها حروب الجيل الخامس بأبعادها السياسية والاقتصادية والاجتماعية والثقافية والأخلاقية، لتعمل على تزييف المعلومات والأفكار والعقول، فعن طريقها يمكن نقل معلومات مضلّة إلى أفراد مجتمع ما، بما يسهم في تدمير منظومة القيم التربوية والأخلاقية ذات الصلة بالمجتمع، وذلك من خلال ما تبثّه من مضامين إعلامية"⁽¹⁾

○ مفهوم الحروب المعلوماتية (السيبرانية) و تغييرها في طبيعة الصراعات الدولية

الأمن السيبراني أنه: "عبارة عن مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قرصنة الكمبيوتر وعواقبها، ويتضمن تنفيذ التدابير المضادة المطلوبة"⁽²⁾

(1) علياء عبدالفتاح رمضان، التربية الإعلامية في بيئة الإعلام الجديد، القاهرة: عالم الكتب، 2019، ص 11

(2) Lehto Martti , Neittaanmäk Pekka .Cyber Security: Analytics, Technology and Automation. Switzerland : Springer International Publishing, 2015.

ان التوظيف الإلكتروني لكافة معلومات الدولة رغم كونه اداة لتسهيل و سرعه العمل . الا انه اوجد تحديات و صعوبات كثيرة. فشبكة المعلومات تلك تحت طائلة المخاطر الإلكترونية مما استوجب الدراية التامة باساليب الحماية الدائمة سواء بالاجهزة او البرامجيات او الاشخاص المستخدمين لها وفق احدث التقنيات في مجال الثورة الرقمية.

"تختلف الحرب السيبرانية في جوهرها عن الحرب الإلكترونية. إذ تركز على الهجمات التي تستهدف الشبكات الحاسوبية والأنظمة الرقمية. هذه الهجمات يمكن أن تتراوح بين سرقة البيانات الحساسة وتعطيل البنية التحتية الرقمية، مثل محطات الطاقة أو شبكات الاتصالات. أما أنواعها فهي تشمل عدة أشكال من الهجمات، منها -الاختراقات: (Hacking) حيث يقوم القراصنة (هاكرز) باختراق الأنظمة الرقمية بهدف سرقة المعلومات أو تعطيلها -الهجمات بالبرامج الخبيثة: (Malware Attacks) مثل الفيروسات أو البرامجيات التي تصيب الأنظمة الحاسوبية وتتسبب في تعطيلها أو السيطرة عليها - الهجمات الموزعة لقطع الخدمة: (Distributed Denial of Service - DDoS) وتعتمد هذه الهجمات على إغراق الشبكات الرقمية بطلبات زائفة، ما يؤدي إلى توقف النظام عن العمل بشكل صحيح -التجسس السيبراني: (Cyber Espionage) حيث تستخدم الدول أو الجماعات أدوات سيبرانية لجمع المعلومات الاستخبارية أو التجسس على مؤسسات أو أفراد. وعلى الرغم من أن الحربين تتشابهان من حيث اعتمادهما على التكنولوجيا الحديثة، فإن هناك فروقاً جوهرية بينهما. فمن حيث المجال العملي، فإن الحرب الإلكترونية تعمل ضمن الطيف الكهرومغناطيسي، مثل موجات الراديو والترددات اللاسلكية. وتهدف إلى التشويش أو تعطيل الاتصالات المادية التي تتم عبر هذه الموجات، بينما الحرب السيبرانية تركز على الفضاء الرقمي، حيث تستهدف الشبكات الحاسوبية، قواعد البيانات، وبرمجيات الحماية. الأدوات هنا تكون فيروسات، برامج خبيثة، وهجمات على الأنظمة الرقمية. أن الحرب السيبرانية تُستخدم بشكل واسع للتجسس على الدول الأخرى وسرقة معلومات حساسة قد تؤثر في الأمن القومي. بالإضافة إلى التأثير في الرأي العام من خلال هجمات على وسائل الإعلام أو مواقع التواصل الاجتماعي، إذ يمكن للحرب السيبرانية التأثير في تشكيل الرأي العام وتوجيهه في اتجاهات معينة.."⁽¹⁾

عرفتها الباحثة في معهد أكسفورد للإنترنت بأنها " حرب تُركز على استخدامات معينة لتكنولوجيا المعلومات والاتصالات ضمن استراتيجية عسكرية هجومية أو دفاعية أقرتها الدولة، وتهدف إلى تعطيل الفوري أو السيطرة على موارد العدو والتي تُشن داخل بيئة المعلومات مع أهداف تتراوح بين الصعيد المادي والمجالات غير المادية والتي قد يختلف مستوى الدمار فيها على حسب طبيعة وحجم الهجوم"⁽²⁾

(1) فيولا مخزوم ،ما الفرق بين الحرب الإلكترونية والحرب السيبرانية ، لبنان 2024

<https://www.almayadeen.net/arts-culture>

(2) Global Cyber Security Index. Available at: <https://cutt.us/g9nUk2024>

تعد وسائل الحروب الالكترونية حديثة ذات تقنيات عالية سهلة الحمل و الانتقال حجما لكنها اكبر اثراً. ان تلك الحروب لا تستوجب نقل الاسلحة و الدبابات و الطائرات الحربية فقد تم الاستغناء عن كل تلك التكلفة المادية و حتى عن الجنود و الجيوش و تدريباتها و تخصيصاتها المالية . و الاستعاضة عن ذلك بهجوم فايروسي او هكر متخصص في اقتحام المواقع الالكترونية . حتى ان الدول اصبحت تستعين بشركات متخصصة في مجال الحروب الالكترونية لاداء الاختراقات و تنفيذ الحروب الالكترونية . واصبحت الحروب النفسية و المعلوماتية الالكترونية هي الاكثر فاعلية و الاقل تكلفة . فالتأثير بالعقول و تغيير التوجهات الفكرية اصبح الاساس في التغييرات السياسية و الامنية و زعزعة استقرار الدول و امنها القومي . "وتبنت العديد من الدول استراتيجيات حرب المعلومات باعتبارها حرباً للمستقبل، والتي يتم خوضها بهدف التشتيت وإثارة الاضطرابات في عملية صناعة القرارات عبر: الدخول إلى أنظمة الطرف الآخر، استخدام ونقل معلوماته بعد الأهمية المتزايدة للفضاء الإلكتروني. وترى الدول الكبرى أن من يحدد مصير المعركة ليس من يملك القوة، وإنما القادر على شلّ القوة والتشويش على المعلومة." (1)

لقد اصبح للحروب الالكترونية اسواقاً تنافسية. فرغم خصوصية الفضاءات الالكترونية. الا ان التنافس التكنولوجي لا يقتصر على دولة او جهة معينة كما في الحروب التقليدية. فالشركات القائمة على تطوير و بيع برامج الحماية من جانب و تنفيذ حروب الكترونية من جانب اخر . اصبحت في تنافس قائم على ارتفاع نسب الطلب عليها و نسب الاجور المدفوعه . حيث خلقت تلك الحروب الالكترونية اسواقا اقتصادية الكترونية حديثة تتسم بالسرية في الاداء و الاجور العاليه وفقا لطبيعته المهام التدميري و اثارها. تعد من اهم عناصر الحروب المستقبلية الالكترونية اعتماد تشويش المعلومة و تغييرها لتشتيت و شل القوى الساندة للقوى السياسية و زرع الفتن وهو ما يسمى بالارهاب الصامت والقوى الناعمة تتخذه بعض الجهات و الدول وسيلة لضرب الاقتصاد و السياسات الخاصة بالدولة و استنزاف قوتها و استقرارها . "ويمكن تعريف الحروب الإلكترونية من النظرة القانونية بأنها نظام قائم على الرعب المنتشر في الشبكة العنكبوتية تهدف إلى تنفيذ العديد من الأعمال لترويع أمن الأفراد والجماعات والمؤسسات والدول وإرهابهم إقتصادياً وإدخالهم في أزمات نفسية واجتماعية ناتجة عما يعرف بالإرهاب الصامت، وينطلق هذا المفهوم من الواقع الغربي، وهي حرب ناعمة صامتة تأخذ أشكالاً عدة كشكل الاتصالات بين الجيوش وقاداتها وإضعاف شبكات النقل والإمدادات اللوجستية وضرب المعلومات الاقتصادية وإحراج الساسة والعبث بالمحتوى الفني والتقني" (2)

(1) E.Nakashima. "U.S. Accelerating Cyberweapon Research", The Washington Post, online e-article, https://www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/2012/03/13/gIqAMRGVLS_story.html

(2) صلاح حيدر عبد الواحد، حروب الفضاء الإلكتروني: دراسة في مفهومها وخصائصها وسبل مواجهتها، جامعة الشرق الأوسط،

ثانياً : الانسان يقود التكنولوجيا ام العكس في عصر الثورة التكنولوجية

○ المخاطر التكنولوجية و البيئية على الانسان

"باتت العلاقة بين الأمن والتكنولوجيا علاقة متزايدة مع إمكانية تعرض المصالح الاستراتيجية - ذات الطبيعة الإلكترونية - إلى أخطار إلكترونية، وتهدد بتحول الفضاء الإلكتروني لوسيط ومصدرًا لأدوات جديدة للصراع الدولي المتعدد الأطراف ودورها في تغذية التوترات الدولية. ومن جهة أخرى فرضت تلك التطورات إعادة التفكير في مفهوم الأمن القومي الذي يُعنى بحماية قيم المجتمع الأساسية وإبعاد مصادر التهديد عنها، غياب الخوف من خطر تعرُّض هذه القيم للهجوم" (1)

أن الباري عز و جل و اصطفى الانسان عن سائر المخلوقات بنعمة العقل و ميزه بها. ان كل التطورات التكنولوجية التي تميز عصرنا الانى و استمرارها بفضل العقل البشري و تطلعاته و ابتكاراته و ابداعاته. الا ان الاستخدام لاي من نتاجات العقل البشري تلك يشابه لتعامل الانسان مع الطبيعة . اما يستخدمها بالطرق الايجابية المثمرة بما يكون فيه الفائدة و الحفاظ على الجنس البشري و ذلك ما يسمى بالتعامل الايجابي . او على العكس كما يتعامل البشر حالياً في قطع الغابات و الاسراف بالمياه و و تجريف الاراضي الزراعية . فضلاً عن الحروب و اثارها المدمره للمجتمع سواءً على مستوى الثروه البشرية او التلوث البيئي او حتى تغيير السمات الديمغرافية للدول التي تتعرض للحروب و تتسبب التكتلات البشرية تحت مسميات النازحين او المهاجرين غير الشرعيين او الهجرة من الارياف الى المدينة بدواعي التغيير للافضل. و التي تتطلب الكثير من الخدمات التي ترتكز في اماكن دون اخرى وهجران الزراعة والارياف. وترتفع بذلك كلف الاستيراد و تعم ظاهرة البطالة للمزارعين المهاجرين داخلها. ترافق كل تلك المتغيرات انخفاض في التوجهات التنموية الاقتصادية و تراجع في قدرات الدول على توفير الخدمات الصحية و التعليمية و الثقافية و الاقتصادية بشكل عام. "مع تزايد معاناة المجتمعات الانسانية من الاثار الضارة وغير المرغوبة للتطور التكنولوجي فقد باتت الحاجة ماسة إلي ضبط مسيرة التطور التكنولوجي بضوابط قانونية تضمن تحقيق المصالح العامة للمجتمعات الانسانية وتدرأ أو تقلل من المفاصد والاثار السلبية للثورة التكنولوجية على مختلف مجالات الحياة، وإذا تبين ذلك، فإن الامر يتطلب الكلام عن هذه الضوابط، والتي يمكن أن تستمد من القيم العليا للمجتمعات الانسانية، والمبادئ العامة للشرائع السماوية عامة، والشريعة الاسلامية خاصة، والمناهج والدراسات العلمية التي عنيت بهذا الامر." (2)

(1) مصطفى علوي، مفهوم الأمن في مرحلة ما بعد الحرب الباردة، أبحاث المؤتمر الذي عقده مركز الدراسات الآسيوية 4-5 تحرير

هدى ميتكيس، والسيد صدقي عابدين. القاهرة: كلية الاقتصاد والعلوم السياسية، 2004.

(2) محمد عيد الغريب، التجارب الطبية والعلمية وحرمة الكيان الجسدي للانسان، دراسة مقارنة، ط1، القاهرة، مطبعة أبناء وهبة حسان، 1989، ص 5.

○ تكنولوجيا الذكاء الاصطناعي والإنسانية

"يتحقق الأمن الإنساني عبر آليتين رئيسيتين هما الحماية "Protection"، والتمكين "Empowerment". الحماية : مفهوم الأمن الإنساني ذو طابع وقائي ويعمل بشكل مسبق لمواجهة التهديدات التي تحيط بالأفراد، كالأزمات المالية العالمية والصراعات العنيفة والأعمال الإرهابية والأمراض وانحدر مستويات مؤسسات الخدمات الأساسية، وهو ما يتطلب وضع معايير على الصعيدين الوطني والدولي للتصدي لأوجه انعدام الأمن بطريقة شاملة ووقائية لا تقتصر على ردود الأفعال تجاه التهديدات، بل تعمل بشكل وقائي وتكشف ثغرات البنية الأساسية للحماية .التمكين: أي إكساب الأفراد القدرة على التصرف والتخطيط سواء لصالحهم أم لصالح بقية أفراد المجتمع، وجعلهم يمتلكون قدرة المطالبة بالحلول باحترام حقوقهم وحررياتهم والتصدي للكثير من المشكلات ويجاد لها، الأمر الذي يتطلب النهوض بكل ما من شأنه تعزيز هذه القدرات ومن الملاحظ أن كلتا الآليتين مترابطتان؛ فالحماية تفسح المجال لإعمال التمكين والأفراد الممكنون قادرون على تجنب المخاطر والمطالبة بتحسين آليات الحماية"⁽¹⁾

ان اعتماد الانسان على الذكاء الاصطناعي في كافة المجالات لا يعني الغاء العقل البشري و مسؤولياته في اتخاذ القرارات و تحمل المسؤوليات و تنشيط المهارات الذهنية و الابداعات الانسانية . أن الذكاء الاصطناعي وفر العديد من المزايا التي لا يمكن الاستغناء عنها في جميع جوانب الحياة .ان الجوانب الانسانية التي ساهمت بها التكنولوجيا تطويراً سواءً فيما يتعلق بتطوير العملية التعليمية او تحسين الخدمات الصحية او تطوير في الجانب الانتاجي الصناعي وابتداع التجارة الالكترونية و اثارها التنموية الاقتصادية و تطوير جانب النقل وفق البرامج الخاصة بايضاح الطرق وخرائط التنقل و غيرها من الخدمات التي رقد بها الذكاء الاصطناعي و اسس وفقها حياة ذات طابع اسرع اكثر سلاسة في الانجاز . الا ان تلك التكنولوجيا الرقمية تسببت بكوارث انسانية في الان ذاته . فالتكلفة العالية للبرامج و الاجهزة و الحماية لكافة التوجهات التعليمية ام الصحية ام النقل او التجارة الالكترونية ام الصناعات تسببت بخلق فوارق طبقية و تمييز في القدرات الانتاجية و ضعف في قدرات تقديم الخدمات الصحية سواء على مستوى احتياجات الفرد او الحكومة. فضلا عن احلال الروبوتات محل الانسان و خلق البطالة وتبعاتها التدميرية للاسرة و انعكاساتها في المجتمع .ان تلك التوجهات و ما يصاحب الادمان الالكتروني من انحرافات و افساد للاخلاق العامة خاصة من خلال الالعاب الالكترونية .تسبب بخلق فجوة انسانية واسعة بين الانسان و بيئته و اسرته . حيث طغى الجانب الالكتروني على الجانب الانساني و دمر خصوصيته في تحولات غيرت من الثقافات و الاخلاقيات العربية الاصلية لاحتواء مبهم مدمر الكتروني

(1) خولة يوسف، أمل يازجي، مفهوم الأمن الإنساني وأبعاده في القانون الدولي العام، مجلة جامعة دمشق للعلوم الاقتصادية والقانون ، سوريا ،المجلد : ٢٨ ع:2، ٢٠١٢، ص ٥٢٩ .

من خلال شاشة الكترونية لا يدرك من ورائها. ان طغيان الذكاء الاصطناعي على الذكاء الانساني قد يكلف الدول خسائر لا حصر لها فسلوك الاجهزة يبرمج من قبل الانسان و مراقبة التنفيذ يجب ان تتم من خلاله. اي ان صاحب القرار و التوجيه و التطوير يكون من خلال الذكاء البشري لكونه يتمتع بالحس الانساني . فلا تزال الانسانية و الرحمة و التمييز و الادراك من ارقى و اهم ماميزنا به الخالق عز و جل . "مقاله جوزيف وايزنباوم، رائد الذكاء الاصطناعي، بأنه يجب ألا ندع أجهزة الكمبيوتر تتخذ قرارات مهمة نيابة عنا لأن الذكاء الاصطناعي كآلة لن يمتلك أبدًا صفات إنسانية مثل الرحمة والحكمة للتمييز والحكم الأخلاقي" (1)

ثالثاً : المخاطر الامنية في ظل التحولات الرقمية

○ مفهوم التحول الرقمي

"عملية تهدف إلى تحسين الكيانات والمؤسسات من خلال إطلاق تغييرات كبيرة على خصائصها باستخدام مجموعات من تقنيات المعلومات والحوسبة والاتصالات" (2)

"عملية انتقال وتحول للمنشآت للعمل وفقاً لنماذج الأعمال التي تعتمد على التكنولوجيا الرقمية، والبنية التحتية المعلوماتية المبنية على المعرفة والابتكار والابداع في تقديم المنتجات والخدمات بكفاءة وفعالية وبأسلوب آمن من خلال وسائل تكنولوجية رقمية" (3)

○ التحول الرقمي في المجال التعليمي

"أن التحوّل الرقمي في التعليم يُعبر عن تحويل العمليات الإدارية والممارسات التعليمية إلى عمليات تعتمد على التقنية أجهزة وبرامج بشكل تام أو جزئي، وتركز على جانبي تقليل التكاليف ورفع جودة العمل، تهدف لتطوير العمليات التعليمية" (4)

(1) Joseph W. Computer Power and Human Reason from Judgement to Calculation. San Francisco: W H Freeman Publishing; 1976.

(2) Johannes Huebner, Denis Vuckovac. (2019). "Ilic fintechs and the new wave offinancial intermediaries completed", Research paper, 23rd Pacific Asia Conference on Information Systems , China, P:P1-14.

(3) Steiber, A.; Aleange, S. and Ghosh, S. (2020). "Digital transformation of industrial firms: an innovation diffusion perspective", European Journal of Innovation Management , Emerald Publishing Limited, pp. 1-22.- Tomte, C.; Fosslund,

(4) محمد إبراهيم الحجيلان، " التحوّل الرقمي في التعليم: رؤية ملقّي تقنيات التعليم HP I. وفق مفهوم تحسين الأداء البشري في ضوء رؤية المملكة 2030 "الرياض: جامعة الملك سعود. ص:4 (2020).

ان تحويل المنظومة التعليمية التقليدية الى الكترونية اصبح من ضرورات تطوير العملية التعليمية و اساسياتها. فالمنظومة التعليمية الالكترونية نك موثقة لكافة المعلومات و لمختلف التخصصات و المراحل الدراسية و متاحة اغلبها دون اجور بصورة دائمه و بشكل تسجيلي ثلاثي الابعاد لكافة التجارب العلمية. ان ذلك الاسناد التعليمي الغى الفروقات الاستيعابية و جعل لذوي الاحتياجات الخاصة و لتاركي التعليم لظروف صحية او اقتصادية ضعيفه فرص التعليم بصورة افضل بتكلفه بسيطة . كما تتيح التخصص باكثر من اختصاص و تفتح مجالات العمل الحر بالدورات المتاحة كالتخصصات الحرفية وتعد فرص اعاده للحياة .

"ان المنظومة التعليمية بمختلف التخصصات العلمي و المهني في تحويلها الى منظومة رقمية تعليمية تسببت في معالجة العديد من التحديات حيث يعد توفير المادة العلمية في اي وقت و زمان و بصورة تجسيدية ثلاثية الابعاد وشرح تفصيلي و تنفيذي قد ساعد في الغاء فروقات الاستيعاب عند الطلبة نتاج زخم القاعات الدراسية و قلة الادوات التوضيحية فضلا عن معاناة ذوي الاحتياجات الخاصة في سبيل مواصلة التعليم و اتاحت فرص تعليم لتاركيه نظرا لظروف صحية و مادية اي ان التحول الرقمي كان بمثابة الاسناد و التطوير و التحفيز للابداع و الابتكار, لقد سد الإنترنت فجوة الإعاقة من خلال التقنيات الرقمية، فأصبح أمام ذوي الإعاقة فرصة للتواصل والتعبير عن الذات وتطوير المهارات، كذلك تصف ما تحقق في حياتها بفضل الإنترنت طفلة معاقة فتقول: "تغيرت حياتي بعد الاتصال بالإنترنت"⁽¹⁾

○ التحول الرقمي في المجال الاقتصادي

"ويعتبر النمو الاقتصادي من الأهداف الأساسية التي تسعى إلي تحقيقها الدول، ولقد أصبحت مسألة النمو الاقتصادي حالياً مرتبطة ارتباطاً كلياً بمدى جاهزية الدولة للتحول الرقمي والإعتماد علي الوسائل الجديدة بدلاً من عناصر الإنتاج القديمة مما يتطلب وجود البنية التحتية لقطاع الإتصالات وتكنولوجيا المعلومات والإطار القانوني والتشريعي اللازم للأعمال الإلكترونية."⁽²⁾

ان الاثار الايجابية للذكاء الاصطناعي في المجالات الاقتصادية تجعل اي تطور اقتصادي غير قابل للتنفيذ دون اعتمادها. حيث الاجتياح الرقمي للمجالات الصناعية رفع من نسب الانتاج و جودته و دقته فضلا عن التنظيمات التسويقيه التجارية الرقمية التي اثمرت في سرعة الانجازات للمشاريع حيث الكلف البسيطة في مجال المراسلات الالكترونية التجارية. فضلا عن اتاحة الفرص الابداعية للشباب في الترويج لمشاريعهم الصغيره بسبل ترويجيه مبهره و السعي لاتقان و ابداع اكبر في عالم تنافسي الكتروني واسع لا حدود له.

⁽¹⁾يرجع إلى "أطفال في عالم رقمي"، تقرير اليونسيف عن حالة أطفال العالم سنة 2017

⁽²⁾ أمل صبري محمد جميل، "محددات نجاح التحول إلى الاقتصاد الرقمي في الدول النامية -دراسة حالة مصر-"، رسالة ماجستير غير منشورة، معهد البحوث والدراسات العربية، جامعة الدول العربية، القاهرة (2020).

" الفوائد المترتبة على استخدام التكنولوجيا في مجال الأعمال وأهميتها : توفر التكنولوجيا العديد من الآليات التي تسهم في رفع كفاءة العمل والإنتاجية المنوطة بها، إلى جانب تسريع عملية العمل وتسهيلها. تتوفر العديد من البرامج الحاسوبية التي تساعد على تحقيق الدقة في المعاملات المالية وما يتعلق بها من رواتب موظفين، أو دفع فواتير أو غير ذلك، وتجعل من تنفيذ هذه المهام أكثر سهولة. تحقق التكنولوجيا درجة عالية من التنافس بين الشركات أو المؤسسات، وتقدم العديد من الآليات المساعدة على ذلك والتي من ضمنها التسويق والبيع عبر الانترنت، بالإضافة للتواصل مع العملاء الملائمين في المكان والوقت المناسب. تسهل عملية التواصل ما بين زملاء العمل أو حتى مع العملاء والمستهلكين"⁽¹⁾

○ التحول الرقمي في المجال الثقافي

"إن تقريب المعلومة من الناس وفتح باب التواصل والتعارف على مصراعيه سهل الولوج إلى عالم الثقافة والمعرفة والاستفادة منه واستثماره بتكلفة أقل، مما فتح الباب أمام الإنتاج والإبداع الإنساني في كل المجالات بلا حدود وبلا قيود، فأصبحنا أمام وفرة إبداعية محفزة على الإبداع، واتسع مجال تقاسم المعلومة، وبات الفضاء الرقمي فرصة كبيرة لثقافة تعاونية وتطويرية لقدرات الإنسان"⁽²⁾

يعد التحول الرقمي الثقافي من المجالات المهمة لتلاحق الأفكار و الثقافات . فالقدرات الابتكارية الإبداعية المحلية الوطنية ستكون متاحة وفق التوثيق المميز من قبل شباب المستقبل .و حتى تراثيات الماضي التي تعد أرث وطني يستوجب التذكير و النشر حفاظ على تاريخ البلد ومعالمه .حيث التوثيق الإبداعي لا على مستوى النتاجات الفكرية كالشعر و القصة و غيرها .بل اصبح وسيلة ثقافية تخصصيه في تنشيط السياحة بأيضاح تصويري توثيقي لاماكن السياحة الدينية و الترفيهية و الاثرية و سرد لكافة المعلومات التثقيفية التوضيحية لاهميتها و ماهيتها حيث تزخر دولنا العربية بكم لا حصر له من الارث التاريخي و كنوز المعرفة التي تستوجب التوثيق و النشر في خطوات ايجابية للتعايش السلمي و الامن المجتمعي .

" الأثر الإيجابي للتكنولوجيا على المجتمع :تطوير ثقافة الأفراد وتوسيع مداركهم، وإبقائهم متابعين لأحداث العالم جميعها دون أي أعمارٍ تحُول بينهم وبين المجتمعات الأخرى. تطوير قدرات الأفراد عبر إتاحة وسائل التّعلّم كافة؛ كتعلّم اللغات، وتعلّم برامج التصميم مثلاً. تقريب الآراء ووجهات النّظر؛ من خلال إتاحة التّكنولوجيا للتواصل المُجمعي؛ الأمر الذي ساهم بشكلٍ كبير في التّعرف على آراء ونظريّات الطرف الآخر، وأسلوب تفكيرهم والتّعامل معهم، فتزيد خبرتهم وعلمهم وطريقة تعاطيهم مع المشكلات تطوير جوانب الاقتصاد والطبّ والتّعليم؛ ممّا يؤثّر على المُجتمع وبنيتّه إيجاباً."⁽³⁾

(1) Linda Emma, "Importance of Technology in the Workplace", www.chron.com, Retrieved 2018.

(2) ريمي ريفل، " الثورة الرقمية "، ترجمة سعيد بلمبخوت، الكويت: سلسلة عالم المعرفة، العدد 462، 2018، ص 97.

(3) أحمد الشايب "التقدم التكنولوجي في العصر الحديث"، الألوكة، مصر 30-4-2017.

ان الطروحات الثقافية المعززة من ترسيخ القوى الوطنية للمجتمع و تمكنه من نشر و تعميم الافكار و العادات و التقاليد و القيم الحضارية المجتمعية بتوثيقها بطروحات الكترونية حفاظ على تاريخ و اصالة الدولة . تعد من اساسيات الحفاظ على استمرارية ثقافة المجتمع في مواجهة التحديات الخارجية الفكرية التي تعمد على هدم اسس الحضارة و فق افكار عولمية هادمة للبناء الاسري و المجتمعي . بل انها تعد وسيلة لتحسين الفنون و الاداب و العلوم من الطروحات المشوه لتاريخ و حضارة الامه و امنها القومي .

أشار أندرو مارشال إلى أنّ الثورة الرقمية والمعلوماتية في الشؤون العسكرية تحتوي على ثلاثة مكونات: الابتكار التكنولوجي في مجالات الحوسبة، والاتصالات، المفهوم العملياتي أو المذهب، والتكيف التنظيمي" (1)

ان طروحات ماسبق فيما يتعلق بمفاهيم التحول الرقمي في جوانب الحياة كاهه يصل بنا الى ان عالمية التكنولوجيا الرقمية و توجهاتها اصبحت عاملا اساسيا حيويا في تغيير مسار المؤسسات الحكومية بمجملها و حتى الشركات و القطاع الخاص على السواء . وقد فرض ذلك تطوير في طبيعة و توجهات الاستراتيجية التنموية الاقتصادية و السياسية للدول . حيث خضعت لاسس التحول الرقمي و متطلباته وصولا الى متطلبات الامن السيبراني كوقاية من مخاطر التحول الرقمي . ان التكنولوجيا الرقمية التي استحوذت على شعوب العالم اوجدت تحكم اقتصادي تكنولوجي عولمي و ريادة جديدة بعالم الذكاء الاصطناعي . وقد حجم بالمقابل العديد من الدول بحدود الاستهلاك و سوق للتصريف الالكتروني الداعم لاقتصادهم .

"يكاد المتأمل لحال العالم بعد جائحة كورونا يجزم أن إرادة خفية تسعى لجعل هذا الحدث فرصة للزج بالإنسانية بوتيرة أسرع في عالم الرقمنة، تشير الإحصائيات أن الجائحة صاحبها تزايد في استخدام الهواتف المحمولة بنسبة 50%، وزيادة استخدام البيانات بنحو 40%، وكانت إيطاليا أول دولة تشهد ارتفاعاً في حركة تدفق البيانات عبر الإنترنت من قبل القطاع المنزلي التي زادت بنحو 75% لكونها أول دولة تدخل مرحلة الإغلاق الكامل في العالم" (2)

ان اعتماد التحول الرقمي لم يعد خياراً قابلاً للمناقشة خاصة بعد عام 2020 لكافة دول العالم ولو بنسب متفاوتة وفق الامكانيات المتاحة مادياً و تقنياً . فقد وجه الضوء على الاهمية الالكترونية في ظل الانتشار الوبائي لادامة التواصل و اتعليم و الصحة خاصة . و اصبح من الاسس التي تستوجب

(1) F. G. Hoffman, Will War's Nature Change in the Seventh Military Revolution? , US Army War College: Parameters, VOL. 47 NO. 4, winter 2017-18, Pp19-31

(2) سفيان قعلول والوليد طلحة، "دراسة الاقتصاد الرقمي في الدول العربية"، صندوق النقد العربي، أكتوبر 2020، ص 22، نقلًا عن

تخصيصات مالية معززة في ميزانيات الدول . وبين ايجابيات الكترونية وفرها التحول الرقمي و اصبحت من اهم الوسائل الداعمة لتسهيل و سرعة الاداء في كافة امور حياتنا اليومية لكافة مرافق الدولة. اصبح ذلك التحول عبئاً أثقل كاهل ميزانيات الدول خاصة فيما يتعلق بجوانب بناء بنى تحتيه الكترونيه وتدريب كوادر تقنيه و توفير مستلزمات الامن السيبراني التي استوجبها التحول الرقمي . و رغم كون غالبية دولنا العربية تعتبر استهلاكيه فيما يتعلق بالنتاجات الالكترونية لا انتاجية. الا ان توفير متطلبات البيئه الالكترونية اصبح ملزماً لتكون بمصاف الدول الاخرى اقتصاديا و تنموياً و عسكرياً و امنياً. أن التواجد في عالم الذكاء الاصطناعي بشكل فاعل مثمر للفرد و الدولة استوجب البنى التحتية الوقائية الالكترونية لاستدامة الحماية الانسانية و خصوصيتها.

" القضية الرئيسية في التحول الرقمي هو تغيير الفكر ونموذج العمل وليس استخدام تكنولوجيا المعلومات من عدمه، وليس الميكنة . أما إذا ظلت الحكومة تحت قيود الميكنة وتعمل في جزر (قلاع) منعزلة ولا تتكامل مع بعضها البعض، فإن التحول الرقمي لن يحدث. إن كل الدول الناشئة مجبرة على التغيير، فإن لم تتغير ستصادفها متاعب ومصاعب جمة، وسيهرب المستثمرون إلى أماكن أخرى، حيث أن المستثمر يرغب في وجود بيئة مواتية للعمل والاستثمار، فإن لم يجدها سيبحث عن مكان تواجدها ويذهب إليه، وبذلك يقل الاستثمار المباشر ولن تتحمل الدول التي لم تقم بعملية التغيير مثل هذا الموقف، فنحن نعيش في حالة تنافس شديد، فإذا تركنا في الخلف سنؤكل".⁽¹⁾

○ التحول الرقمي في المجال العسكري و السياسي

"أسهم الفضاء الإلكتروني أيضًا في إلغاء حواجز المكان والزمان بشكل واسع، وأضحى مجالًا جديدًا لتحقيق الهيمنة والنفوذ اعتمادًا على كونه ساحة صراع افتراضية بتكلفة أقل ودقة أكبر، كما يرتبط بالفضاء المدني والعسكري وبالبنى السياسية والاقتصادية والعسكرية أيضًا، بجانب زيادة اعتماد الدول على البنى التكنولوجية لربط الشبكات الحيوية في الدول بأنظمة تحكم تكنولوجية يمكن استهدافها عن بُعد، يضاف لذلك صعوبة الردع الإلكتروني في ظل عدم وجود خطوط سيادية جغرافية واضحة على الفضاء الإلكتروني، وبخاصة مع إمكانية إخفاء الهوية وغياب الشفافية الدولية والقوانين الدولية الحاكمة للفضاء الإلكتروني خاصة مع تزايد الجهات المستخدمة"⁽²⁾

ان تبني التحول الرقمي بكافة اهدافه الحيوية التطويرية تقتضي التخطيط الاستراتيجي من كافة الجهات الفاعلة في ادارة الدولة. فالسعي لانجاح تنفيذ الاهداف الرقمية و متطلباتها تستوجب الرصد

(1) أحمد محمود درويش و أحمد السبكي " التحول الرقمي الفرص و التحديات " ورقة بحثيه , مصر , 19/3/2024 -

(2) سماح عبدالصبور، الصراع السيبراني: طبيعة المفهوم وملامح الفاعلين، مجلة السياسة الدولية: ملحق اتجاهات نظرية، ع: 53،

أبريل 2017

المسبق لتحديد حجم و متطلبات التنفيذ لا على صعيد التخصيصات المالية فحسب بل على مستوى تهيئة الكوادر التنفيذية. ان الكفاءات الالكترونية تستوجب التأهيل سواءً على مستوى الموظفين او المعلمين او الاكاديمين لانجاح البيئة الرقمية. ان الجانب الاساس في التنفيذ الاسلم لتطبيقات الذكاء الاصطناعي يجب ان يعتمد من خلال المؤسسات الامنية و التعليمية كونها الضامن الفعلي للتطبيق الصحيح والامن . فضلا عن كونهم وسيلة لنشر الكيقيه التي تعتمد للحيلولة دون التعرض للهجمات السيبرانية و اجتياح كافة المعلومات الخاصة بالدولة و تهديد استقرارها و امنها .

"وجود خطة استراتيجية تدعم رؤية الدولة لتعظيم قوتها الإلكترونية: الدولة التي تسعى لامتلاك قوة إلكترونية لأبد وأن تمتلك خطة استراتيجية تحدد فيها أهدافها، وآليات التنفيذ، وتحدد وظائف كل جهة، حتى لا يحدث إهدار للموارد، وتخبط في الاختصاصات" (1)

ان ما اثمرت عنه الثورة المعلوماتية من مميزات صاحبها قوى جديده وهي القوى الالكترونية . ان التحول الرقمي قد حول كل مايخص الدولة الى ميدان معلوماتي الكتروني. حيث اصبح هذا المصدر المعلوماتي متاحاً للأفراد و للمؤسسات و القطاع الخاص. ان تلك الفضاءات الالكترونية افرزت محدودية الدولة في السيطرة الداخلية . واتاح بذلك فرص للاعبين جدد في تحديد اجندة الدولة و سياساتها وفق توجهات القوى الناعمة التي لا تستوجب الامكانيات المالية العالية .

"عانى الكثير من المستخدمين حول العالم من هجوم فيروس ransomware ضار يدعي فايروس Wanacry، حيث إستهدفت هذه البرمجية الخبيثة أكثر من 100 الف جهاز حاسوب حول العالم في اليومين الماضيين، البرمجية الضارة قامت بإصابة العديد من المصالح الحكومية حول العالم مثل دائرة الصحة الوطنية في المملكة المتحدة وشركة الاتصالات الاسبانية تليفونيكا و FedEx في الولايات المتحدة الأمريكية من بين عشرات الالاف من الضحايا. الفيروس يدعى "أريد البكاء Want to Cry" او اتريد فك التشفير Want Decryptor و قد اشار ادوارد سنودن عميل وكالة ال CIAالهارب بأن الفيروس هو من صناعة وكالة الأمن القومي الأمريكي و انه تمت سرقة من قبل الهاكرز و اوضح انه حذرهم من تطوير برامج اختراق مماثله لأنها تمثل خطوره عليهم بالمقام الاول و ها هو السحر ينقلب علي الساحر حيث قام الهاكرز بمهاجمة دولة المنشأ بنفس ما صنعوا السؤال المهم الان كيف نحمل انفسنا من فايروس Wanacry حيث انه يهاجم حتى الاشخاص العاديين و يعطيهم فترة اسبوع لدفع الفدية او ان يفقدوا جميع البيانات على جهازهم للأبد!"(2)

(1) إيهاب خليفة، استخدام القوة في إدارة التفاعلات الدولية: الولايات المتحدة نموذجا ، 2012 ، مصر ، ص 55، 56.

(2) خالد ميمون، فايروس Wanacry الضار يصيب أكثر من 100 الف جهاز حاسوب حول العالم في يوم واحد، 2025 ، الجزائر ،

موقع <https://now.eljazeera.com>

مع امكانات تأثير متزايدة من خلال استغلال الفضاءات الالكترونية قليلة التكاليف. فالجرائم الالكترونية تبدأ من الاقل الى الاعلى اي لا يمكن لن تتوحد بنموذج شن هجوم الكتروني يعطل كافة دوائر الدولة الكترونية او بحجم التعطيل الدولي لكافة الحواسيب من خلال فايروس واحد. فمن الممكن ان تبدأ تلك الهجمات الالكترونية لتهدد موقع خاص بمؤسسه اقتصادية فيكون سبب معطل لخطط التنمويه الاقتصادية فبين قوى صلبة بمكوناتها الهجومية الى قوى ناعمة وفق محدودية اثارها التدميرية تبقى كافة تحولات مؤسساتنا الرقمية تحت مخاطر الاعمال التخريبية الالكترونية و تطوراتها .

"انماط استخدامات القوة الإلكترونية في التفاعلات الدولية: يتم استخدام القوة عبر الفضاء الإلكتروني في التفاعلات الدولية، من خلال نمطين. النمط الأول: ممارسة نمط القوة الصلبة عبر الفضاء الإلكتروني. حيث يتم استخدامه في أعمال تدميرية وتخريبية من خلال قطع كابلات الاتصال، والأقمار الصناعية بين الوحدات العسكرية، أو استخدام الأسلحة الإلكترونية المتقدمة في سرقة المعلومات وتدمير الأنظمة المعلوماتية الشبكات لمناطق حيوية بما يهدد أمن الدولة والأفراد، مثال تعرض أستونيا لهجمات إلكترونية عام 2007، وفي الحرب بين جورجيا وروسيا في 2008. النمط الثاني: استخدام نمط القوة الناعمة عبر الفضاء الإلكتروني من خلال دعم دوره في التأثير على الرأي العام، وفي العمليات النفسية، وتكوين التحالفات الدولية، وفي عمل أجهزة الاستخبارات الدولية من خلال توفيره للمعلومات، والتي لا تقتصر على وجهة النظر الرسمية في الدولة، إنما أيضا يمتد لدور الأفراد في إنتاج المعلومات، مع قدرته على التأثير على أفكار الأفراد، من خلال نشر المعلومات والأفكار، ودعم عمليات التغيير الثقافي، من خلال سهولة بث المنتجات الثقافية، كالأفلام والتقارير المصورة، وأيضا نشر برامج التعاطف والولاء عبر برامج تعليم اللغات الأجنبية"⁽¹⁾

○ المخاطر الامنية الالكترونية و توجهاتها

"أصبح للفضاء الإلكتروني دور فيما يطلق عليه "القوة المؤسسية" في السياسة الدولية والتي تعني أن يكون لها دور في قوة الفاعلين وتحقيق أهدافهم وقيمهم في ظل التنافس مع الآخرين، والمساهمة في تشكل الفعل الاجتماعي في ظل المعرفة والمحددات المتاحة والتي تؤثر في نظريات العلاقات الدولية وتشكيل السياسة العالمية."⁽²⁾

يعد التساؤل المطروح بصورة مستمرة لماذا المخاوف المتزايدة من الاعتماد على الشبكات الرقمية رغم الفوائد الموهولة التي تقدمها للبناء المجتمعي ومستقبله ؟ ان اعتماد الدول و بشكل تام على الانظمة الرقمية شكل مخاطر توازي في حجمها الخدمات التي توفرها تلك الانظمة . يعد العامل الاساس في

(1) عادل عبدالصادق، أثر الفضاء الإلكتروني في تغير طبيعة العلاقات الدولية، 2018، ص 205: 208

(2) David Held et al., Global Transformations: Politics, Economics, and Culture (California: Stanford University Press, 1999)

الجرائم الالكترونية هو توظيف الاليات و الاسلحة الالكترونية لتنفيذ عمليات اجرامية الكترونيا. ان اعتماد التنفيذ الالكتروني لمختلف الجرائم تحت العديد من المسميات التي تفرض حجم الاثار المترتبة عنها في الغالب مثل الهجمات السيبرانية و الاختراقات والارهاب و الابتزاز الالكتروني التجارة الوهمية و الاحتيال و سرقة بطاقات الائتمان و البطاقات المصرفية و غيرها عديدة.

"وتتعدد أشكال جرائم الاحتيال عبر الإنترنت ومن أهمها القيام ببيع سلع وهمية rogue traders أو سرقة معلومات البطاقات الائتمانية واستخدامها credit card fraud ، أو توجيه المستخدم إلى موقع خاطئ الغرض منه التحايل pharming ، أو الاصطياد الاحتيالي phishing والذي يتعرض فيه الأفراد للخداع عن طريق توجيههم إلى مواقع يتم فيها الحصول على أكبر قدر من المعلومات الخاصة بهم، ثم استخدامها من قبل القائم بالجريمة لتحقيق مكاسب مالية"⁽¹⁾

أن الاختلاف على ماهية الجريمة الالكترونية و تحديد كنهها لكي يتم المحاسبة القانونية على اثرها لا يزال محل خلاف كبير دولياً. فضلا عن صعوبة تحديد المتسبب بذلك الجرم كونه ضمن الفضاءات الافتراضية و من السهولة اخفاء و تدمير الاجهزة الالكترونية التي تسببت بالجرم كالحاسوب و الانترنت. ان ضعف الاجراءات القانونية لردع تلك الجرائم الالكترونية تسبب في اعتمادها بدل الجرائم التقليدية كونها تحقق الغرض الاجرامي دون عقاب. ورغم توفر اليات الكترونية لحماية الاجهزة الالكترونية و ارتفاع اثمانها بما يتناسب و التحديثات الاجرامية الالكترونية الا ان التطور السريع الذي يجتاح العالم الالكتروني لا يدع مجال لتلك الحميات الالكترونية لتكون فاعله بشكل كبير و مؤثر بالإضافة الى قلة الكوادر المتمرسه بالخبرات التقنية الالكترونية المنفذة لتلك البرامج بصورة مستمرة .

ان الهجمات السيبرانية تكمن خطورتها في كونها تشكل مخاطر على الامن القومي للدولة. حيث استهداف شبكات المعلومات الاساسية المتعلقة بالمصارف و الجهات العسكرية و الامنية و التنمية الاقتصادية و الاستثمار اي استهداف ايا من البنى التحتية الالكترونية للدولة والتي توثق كافة متعلقاتها. ان جاهزية حماية تلك الجهات يستوجب ان تبقى في حماية الدولة التي تكون مسؤوليتها استمرار التطوير التكنولوجي للاجهزة و البرامجيات و للكوادر البشرية المسؤولة عنها .

○ مخاطر الإرهاب الرقمي

"عقب أحداث الحادي عشر من سبتمبر عام 2001، شهد الإرهاب تحول جذري كبير في أدواته وآلياته، حيث باتت التكنولوجيا من الوسائل الدائمة للعمل الإرهابي والمُساهمة في زيادة ديناميكية وسهولة إنتشاره

(1) Abdullah M. Alnajim. (2009). Fighting Internet Fraud: Anti-phishing Effectiveness for Phishing Websites Detection, *Durham Thesis*. Durham University. pp:10,11. Available at Durham E-Thesis Online: <http://etheses.dur.ac.uk/2149/>.

وتعاطف أثره، على اعتبار أن التكنولوجيا هي مجموعة المعارف والأساليب المتاحة اللازمة للتتمية في كل عصر من العصور، أما تكنولوجيا الإرهاب فتشتمل على جانب (مادي) يتمثل بالمواد، والأدوات، والتجهيزات، والوسائل التي يستخدمها الإرهابي، وجانب آخر (عقلي) يتمثل بالخبرة، والمعرفة ، وإسلوب التعامل في البيئة المحيطة⁽¹⁾

ان التوجهات الفكرية الدافعه لايجاد و تنشيط الارهاب الالكتروني تختلف من شخص لآخر وفق مسببات عديدة تكون في الغالب مشتركة مع مسببات الارهاب ذا الاسلحة التقليدية. فالاسباب المرضيه النفسيه التي تعد نتاج للاوضاع الاقتصادية و الاجتماعية بين الفقر و البطالة و مخلفاتها من التسبب الاسري. تلك التوجهات تخلق من الفرد انسان هش قابل للتوجيه الفكري الارهابي خاصة مع الاحتياجات المالية و الاجتماعية و النفسية. اما الادمان الالكتروني لمختلف وسائل التواصل الاجتماعي و وسائل الاعلام و الادمان للالعاب الالكترونية . كل تلك التوجهات خطيره مجتمعه تعتبر من افضل السبل للاحتواء الفكري في غسيل للادمغة للفئات الشبابية خاصة في توجهات مظلة مدمرة لهم و للدولة. فبين البث الفاسد الاباحي خلال الالعاب الالكترونية و الاحاد من جانب .و البث المتواصل لافكار دينية مشوه لمبادئ الدين السليمة و مشجعه لجعل المتابع متطرفاً غاضباً رافضاً لتقبل الاخر . غالباً مايرتبط هذا التوجيه الفكري المظلل بالتمويل و استغلال فقر و جهل الفئات العمرية الصغيره و توجيهها لما فيه التشجيع على كسب اخزين في نفس التوجهات المدمره الارهابية. ان نتاج كل ماسبق ينشأ الفكر الارهابي يعد الاخطر كونه لا يكون مرئياً الا من خلال التنفيذ الاجرامي . فالعمل على بث ثقافة ذات توجه جديد يتسم بالعنصرية و الطائفية و الزعزعه الفكرية يكون ذا دوافع مادية و فقدان للهوية الوطنية . ويتم تجنيد هؤلاء الشباب في توجه عسكري مضاد لسياسة و امن الدوله. بل و السعي لجعلهم عامل جذب لآخرين بمختلف السبل الفكرية و المالية و العنف والتهديد .حيث اصبح امن الانسان و تفكيره و توجهاته وعمله و استدامة الثروة البشرية و امنها هو الاكثر عرضة للمخاطر و الاكثر صعوبة في توفير حماية للخصوصية الانسانية و استمرار بنائها و امنها. ان العمل على وضع تطبيقات التحولات الرقمية و توجهاتها في يد الدولة حصراً اصبح ضرورة وفق المخاطر التي تواجه امن الانسان و مستقبله في مجال الذكاء الاصطناعي و تعدد مصادر مخاطر تطبيقات الثورة التكنولوجيا .

"مما لا يمكن نكرانه هو الآثار الناجمة عن النزاعات و الحرب السيبرانية ومن عواقب وخيمة على المدنيين فهناك ضرورة لتطبيق القانون الدولي على العمليات السيبرانية في النزاعات المسلحة والحروب، لوجود ضرر على المؤسسات والافراد وانتهاك للامن وسيادة الدول"⁽²⁾

(1) Ruwantissa Abeyratne, " cyber terrorism and aviation-national and international responses journal of transportation security, vol.4, issue.4, December 2011 p.337.

(2) رزق أحمدسمودي، ديسمبر 2018، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية ، 2018، ص 338 .

ان الهجوم الارهابي الالكتروني اصبح اشد خطر من الارهاب التقليدي مع ما وفرتة تلك التقنيات الحديثة من وسائل متاحة للجميع و بتكلفه اقل. ان تلك الهجمات الارهابية الالكترونية المتزايدة جعلت امكانية الحماية الالكترونية في نفس مدى المخاطر ورغم ما ينتج عنها من اثار مضره و مدمره . الا ان تزايد الاعتماد على تلك التقنيات في كافة دقائق الحياة . جعل تحقيق الارهاب الالكتروني اسهل بكثير من التكلفة و التنفيذ الارهابي المعتاد رغم كون النتائج تصب بذات المنحى الا وهو احداث الاضرار النفسية و الجسدية و الاقتصادية و السياسية و الاجتماعية على مستوى الفرد و الدولة و امنها القومي و الانساني.

" تكمن اهمية القوانين السيبرانية في إنها؛ تفرض إجراءات للاستخدام و تقيس وردود الفعل العام في الفضاء السيبراني، وترتفع نسبة الامان والحماية للمعاملات التي تجرى عبر الإنترنت، وتخضع جميع الأنشطة عبر الإنترنت للمراقبة من قبل مسؤولي القانون السيبراني، وتوفير الحماية لجميع البيانات والممتلكات الخاصة بالأفراد والمنظمات والحكومة، ويساعد في الحد من الأنشطة السيبرانية غير القانونية عن طريق بذل الرقابة والعناية الواجبة من قبل مؤسسات الدولة المختصة، وردود الفعل التي يتم قياسها على أي فضاء إلكتروني لها زاوية قانونية مرتبطة بها تختلف باختلاف توجهها، سواء كان يتعلق بالتجارة أو بالخدمات أم الامن بمختلف انواعه، ووجود قوانين سيبرانية يعني وجود اتفاقيات دولية في هذا المجال مما يتيح تتبع جميع السجلات الإلكترونية عن طريق تحقيق التعاون الدولي لتتبع الجرائم المنظمة، ويساعد على إنشاء الحوكمة الإلكترونية والتي بدورها ترفع جودة حياة المستخدمين من خدمات الحكومة الإلكترونية"⁽¹⁾

الخاتمة:

ان العمل على تحقيق الامن السيبراني الدولي لايمكن ان يتم من خلال جهود دولة و احدة و ان كانت الاكثر تقدماً في ذلك المجال. فلا يزال السباق الدولي في مجال الذكاء الاصطناعي واحتلال الفضاءات الالكترونية و الحروب السيبرانية المستقبلية مشرعة الابواب للجميع. لذا فقد اصبح الاتفاق على وضع معايير و قوانين و اسس وفق استراتيجيات و بروتوكولات دولية من اهم السبل التي يكون فيها حماية للسياسات الدولية و للامن القومي للدول .فالقوانين دون تنفيذ كالحبر على الورق لا طائل منها .و دون توعية و تثقيف مجتمعي من قبل الدولة من جانب و مراقبه فعليته دولية للجرائم و الارهاب الالكتروني من جانب اخر ذا الطابع الدولي سيكون الطغيان الالكتروني على خصوصيتنا الانسانية. ان بناء الثروة البشرية يعد الاهم لان العقل الانساني المسؤول عن بناء الثورة التكنولوجية هو ذاته المسؤول عن استمرار امنه الانساني بتغليب الانسانية على التكنولوجيا الرقمية.

(1) Herbert Lin, Cyber conflict and international humanitarian law International review of the red cross, 2012, Vol. 94, N886, p.515

النتائج والتوصيات

○ توصلت الدراسة للعديد من النتائج أهمها:

- ان البعد الاستراتيجي لطبيعة الصراعات الدولية قد تغيرت تماما بفعل ما فرضته الفضاءات الالكترونية .
- ان التطور التكنولوجي المتزايد يعد عنصرا فاعلا في تزايد المخاطر الامنية على الوجود الانساني و خصوصيته و هو ما اثبتته الدراسة وفق مؤشرات عديدة تم استعراضها.
- ان شكل الحروب المستقبلية سيكون بمنى عن التقليدية منها. سواءاً على مستوى التخطيط العسكري ام التنفيذ تبعاً لمعطيات الذكاء الاصطناعي وفق السباق التكنولوجي و فضاءاته الالكترونية.
- لم تعد البنى التحتية الامنية التقليدية و تقنياتها في المجالات الحربية و النزاعات كافية للحد من المخاطر التي تواجه الوجود الانساني و امنه.
- ان العصر الانساني وفق تطبيقات الذكاء الاصطناعي على كافة المستويات قد اوجد تحديات و مخاطر امنية تتفاقم لحظياً مع مستوى التطورات التقنية المستمرة.
- ان اطمئنان الفرد يعد الغاية الاساسية لتحقيق الابداع و التغيير وفق تخطيط استراتيجي اقتصادي تنموي.
- فأنتهاء عصر الحروب السابقة لا يعني وجود الامان و الاستقرار حيث التطورات التكنولوجية التي ازدهرت بها الحياة خاصة الصناعية و التجارية. الا انها شكلت مخاطر على الامن القومي و استقرار الدول التكنولوجية.
- ان استخدام الادوات التكنولوجية في اعمال الارهاب الرقمي و الجرائم الالكترونية زعزع من أمن و استقرار المجتمعات الانسانية و اوجد مخاوف لا حصر لها نظراً للادمان الحاصل في مجتمعاتنا العربية كمشاهدين لا منتجين الكترونياً.
- ان التحول الرقمي اثبت فاعليته في مجال التعليم من خلال تحسين العملية التعليمية و فرص التعليم للتاركن و لذوي الاحتياجات الخاصة.
- اثبت الذكاء الاصطناعي في المجال الصناعي قدرات تحسين العملية الانتاجية برمتها سواء على مستوى الجودة و الدقة و السرعة .
- وفي مجال الصحة فقد كان للتحول الرقمي مدى واسع في التشخيص و العلاج و خدمات الرعاية الصحية المتوقعة و السريعة.
- أن استحداث التجارة الالكترونية يعد سابقه اسهمت في ايجاد فرص لعمل الفئات الشبابية و تنشيط الاقتصاد بسرعة و دقة في انجاز العمليات التجارية الكترونياً .
- ان التغييرات التي فرضها الذكاء الاصطناعي اوجدت ضرورات امنية اولها التغيير في المفاهيم الامنية و ابعادها لتحديد كنه الجرم الحاصل و ما يستتبعه من عقوبات و الذي اوجد تحديات قانونية دولية.
- ان الامن الانساني يقع تحت مخاطر كبيرة بين البيئي الى الارهابي الرقمي فضلا عن الوبئة و الكوارث الطبيعية خاصة فيما يتعلق بشحة الماء و الغذاء مما يوجد انعدام استقرار امني و نفسي دائم للفرد و للمجتمع .

○ التوصيات

- ان التحديث في المفاهيم الامنية وفق مقتضيات توجهات الذكاء الاصطناعي يعد حجر الاساس في استيعاب ماهية المخاطر و التحديات التي تواجه الوجود الانساني و استمراره .

- ان المخاطر و التحديات التي اوجدها الذكاء الاصطناعي تهدد الامن الانساني.لذا فأن الانسان هو العنصر الاساس الفاعل في تخطي تلك التحديات من خلال اعتماد نشر التوعية و التثقيف و التدريبات المتعلقة بتلك الحروب الالكترونية و مخاطرها ليكون العنصر الفاعل الرادع و الضمان لامنه و امن الدوله .
- ان طبيعة المخاطر الامنية الحديثة تستوجب بالمقابل استراتيجيات تتناسب في تخطيطاتها مع تلك المخاطر على كافة المستويات القانونية و السياسية و الاقتصادية و حتى الاجتماعية و الثقافية فلم تعد الحروب الالكترونية المستقبلية محددة بتوجهات معينة بل هي شاملة بتوجهاتها و اثارها المدمرة .
- ان الصراعات الالكترونية المستقبلية لن تتحدد في الحدود العسكرية او زمان او مكان معين. بل سيكون الصراع المستقبلي شاملا للمجتمع بصورة كاملة و دون حدود جغرافيه او زمنية مما يستوجب تشارك اساليب الحماية و الدفاع مجتمعي و دوليا اي لم تعد مقتصره على الجهات الامنية و العسكرية فقط.
- ان دوافع الارهاب الرقمي المؤدي الى ادخال الدوله في صراعات ينعدم فيها الاستقرار السياسي و الامن القومي بنشر نغرات طائفية و متطرفه تستوجب الحلول السريعه و الاحتواء من الدوله بتوفير فرص عمل و قروض صغيره دون فوائد.
- ان استثمار الدول في المجالات الالكترونية اصبح ضرورة اي رفع في حجم التخصيصات المالية لتوجهات الذكاء الاصطناعي و الحماية التكنولوجيا سواء على المستوى المدني ام العسكري لضمان امن الانسان و خصوصيته .
- ان تطوير السياسات و الاستراتيجيات المتعلقة بالذكاء الاصطناعي لا يتوقف عند حدود فاعلية التنفيذ و الحماية بل يتسع ليشمل التوجهات القانونية الضامنة لحماية الدولة و الفرد.
- ضرورة خلق تعاون دولي في شراكات تعتمد الاستخدام الاسلم لتقنيات الذكاء الاصطناعي في التطوير المجتمعي .
- ان التطورات التكنولوجية اوجدت تحديات و متغيرات على الساحة الامنية استوجبت خلق اجيال جديدة تعمل على تفعيل توازن استخدامات التقنيات الالكترونية و بين الوجود الانساني و خصوصيته.
- ان الثروة البشرية تعد الجانب الفاعل في الحفاظ على امن و مستقبل الانسان فكما ابدع الذكاء البشري في خلق تلك التطورات التكنولوجية فهو ايضا قادراً على حماية امنه و مستقبل بلده التكنولوجي
- ان القوانين التنظيمية للجوانب العسكرية الامنية التكنولوجية تستوجب التحديث الدائم وفق مقتضيات التطور الحاصل في بكافة خصائصها.
- تعد من متطلبات التحول الرقمي و اعتماد التطوير ضرورة تعزيز المهارات التقنية لكافة منتسبي دوائر الدولة بصورة دورية بالدورات الالكترونية التطويرية المحلية و الدولية.
- يعد من اهم الخطوات الفاعلة للمحافظة على الخصوصية الانسانية و الوطنية بوضع سياسات و تشريعات تكون رادعه للاستخدامات غير الاخلاقية ضمانا لامن و سلامة المواطن.
- ان التطوير في المجالات الالكترونية سواء على مستوى الاستخدام ام الحماية يستوجب اتاحة الخدمات الالكترونية للجميع دون تمييز لضمان امنهم و تحديد من نشر الافكار السلبية المدمره.
- ضرورة ايجاد صيغ تعاون مثمر مع الجهات الدولية التخصصية في مكافحة الهجمات السيبرانية و هيمنة الفضاءات الالكترونية و مخاطرها وفق صيغ قانونية يتفق عليها في بروتوكولات تتناسب مع طبيعة المتغيرات التي فرضها الذكاء الاصطناعي و تطويراته.
- ان الارهاب الرقمي المتفام كما هو الارهاب التقليدي في مسباته و كارثيته. ويستوجب التخصيصات الامنية و المالية و الكوادر البشرية التي تعمل على مكافحته قبل استفحال اثاره المدمره.

- يعد الاستقرار الامني و السياسي من خلال العمل على معالجة الفساد و توفير فرص عمل و جعل حرية الرأي و المناقشات الفكرية اساس للفئات الشبابية لكي يتم اعتماد احترام الرأي الاخر في تعايش سلمي امني مجتمعي يعد كأفضل ضمان للحد من الارهاب و منعه.
- ان تحقيق رفاهية المجتمع الانساني هو ماوجدت لاجله تلك التحولات الرقمية وفق توجهات الثورة التكنولوجيا لا العكس.

References:

1. Reham Abdel Rahman Rashad, "The Impact of Cyber Terrorism on Changing the Concept of Power in International Relations: A Case Study of the Islamic State Organization," Arab Democratic Center, 2016.
2. 4- Nour El-Din Mokhtar El-Khademi, "Jurisprudential Rules Related to Comprehensive Security," Arab Journal of Security Studies and Training, Naif Arab University for Security Sciences, Issue 42, 2021, p. 21.
3. 5- Hayat Hussein, "Cyberspace and the Challenges of Global Security," Journal of Legal and Political Sciences, Volume 12, Issue 1, 2021.
4. 6- Farid Kurtal and Amal Weyoub, "Administrative Leadership as a Component of Successful E-Government Transformation." Proceedings of the International Refereed Conference: E-Government Between Reality and Inevitability. University of Blida, Algeria, 2017
5. 11- Alia Abdel Fattah Ramadan, Media Education in the New Media Environment, Cairo: Alam Al-Kutub, 2019, p. 11
6. 17- Salah Haidar Abdel Wahid, Cyber Wars: A Study of Their Concept, Characteristics, and Ways to Confront Them, Middle East University, 2021
7. 18- Mustafa Alawi, The Concept of Security in the Post-Cold War Era, Research Papers of the Conference Held by the Center for Asian Studies, 4-5, edited by Hoda Metkes and Sayed Sedki Abdeen. Cairo: Faculty of Economics and Political Science, 2004
8. 19- Muhammad Eid Al-Gharib, Medical and Scientific Experiments and the Sanctity of the Human Bodily Entity: A Comparative Study, 1st ed., Cairo, Abnaa Wahba Hassan Press, 1989, p. 5
9. 20- Khawla Youssef and Amal Yazigi, The Concept of Human Security and Its Dimensions in Public International Law, Damascus University Journal for Economics and Law, Syria, Vol. 28 Issue 2, 2012, p. 529.
10. 24_ Muhammad Ibrahim Al-Hujailan, "Digital Transformation in Education: The Vision of the HP Education Technology Forum. According to the Concept of Improving Human Performance in Light of Saudi Vision 2030," Riyadh: King Saud University, p. 4 (2020).
11. 25_ UNICEF Report, "Children in a Digital World," on the State of the World's Children 2017.
12. 26_ Amal Sabry Muhammad Jamil, "Determinants of the Successful Transition to the Digital Economy in Developing Countries - A Case Study of Egypt," unpublished master's thesis, Institute of Arab Research and Studies, League of Arab States, Cairo (2020).

13. 28_ Rémi Rivel, "The Digital Revolution," translated by Saeed Belmabkhout, Kuwait: World of Knowledge Series, Issue 462, 2018, p. 97.
14. 29_ Ahmad Al-Shaib, "Technological Progress in the Modern Era," Al-Aloka, Egypt, April 30, 2017.
15. 32- Ahmed Mahmoud Darwish and Ahmed El-Sobky, "Digital Transformation: Opportunities and Challenges," Research Paper, Egypt, March 19, 2024.
16. 33- Samah Abdel-Sabour, "Cyber Conflict: The Nature of the Concept and Characteristics of Actors," International Politics Journal: Theoretical Trends Supplement, No. 53, April 2017.
17. 34- Ihab Khalifa, "The Use of Force in Managing International Interactions: The United States as a Model," 2012, Egypt, pp. 55-56.
18. 36- Adel Abdel-Sadek, "The Impact of Cyberspace on Changing the Nature of International Relations," Egypt, 2018, pp. 205-208.
19. 40- Rizk Ahmed Samoudi, "The Right to Self-Defense in the Face of Cyber Attacks," 2018, p. 338.