https://doi.org/10.25130/tjfps.v3iprivate issue.240

TJFPS private issue

IRAQI Academic Scientific Journals

العراقية المجلات الاكاديمية العلمية

ISSN: 2663-9203 (Electronic)
ISSN: 2312-6639 (print)

Contents lists available at:
http://tjfps.tu.edu.iq/index.php/poiltic
Tikrit Journal For Political Science

Tikrit Journal For Political Science SINCE 2014

الأمن المجتمعي بين التحديات والتداعيات الأمنية السيبرانية والاستراتيجيات الإصلاحية المجتمعية

"Community Security between Cyber Security Challenges and Repercussions and Community Reform Strategies"

Ansam Faik Abdulrezzak Al_Obidi [a]
Baghdad University / College of sciences [a]

م . انسام فائق العبيدي [a]
جامعة بغداد / كلية العلوم /مديرة وحدة حقوق الانسان [a]

Article info.

Article history:
- Received.20. Apr.2023
- Accepted. 6. May.2023
- Available online.30. Sep. 2023

Key words:
- community security
- social reform
- Strategies
- Challenges
- cyber security

©2023. THIS IS AN OPEN ACCESS ARTICLE UNDER THE CC BY LICENSE
http://creativecommons.org/licenses/by/4.0/

Abstract: The end of the Cold War era between the poles of international powers and competitive displays of conventional arsenals of armaments، including weapons of mass destruction and nuclear weapons، does not mean the return of world peace، the restoration of international security and the cessation of the arms race. All the features of conflicts and wars still exist، but what is radically different is the nature of those wars and conflicts according to the requirements of cyber wars that are silent in their tools and destructive in their effects Stemming from the outputs of technological developments، where the fifth generation and artificial intelligence are two sides of the coin and one، where the comprehensive change in the dynamics of conflict and achievements until the measure of strength depends on the extent of control in the field of electronic spaces and professionalism capable of all its inputs in the midst of a huge amount of risks and cyber digital threats with momentary developments The latest complete coup at all levels، especially with regard to the specificity of societal security and the stability and sovereignty of states، the shift towards the digital world with all its features and developmental features of

human life has led to the emergence of challenges commensurate in their risks with the instantaneously developmental nature of the orientation، where cyberspace imposed new challenges and concepts of power، wars، threats and risks that threaten the safety of the individual and the security and sovereignty of the state، which in return necessitated the pursuit of countries to create rehabilitation strategies To achieve its security and national cyber stability In order to be a life path for society as a whole to ward off and deter future cyber risks and wars through cooperation and fruitful interaction between all members of society and supported by the exchange of international experiences and exceptional efforts to supplement cybersecurity by enacting deterrent international laws that determine the risks of future electronic wars.

معلومات البحث :

- الاستلام 20 نيسان/2023
- القبول : 6 حزيران/2023
-النشر المباشر: 3ايلول/2023

الكلمات المفتاحية :

- الامن المحتمعي
- تحديات الامن السيبراني
-التطور التكنولوجي
-الاستراتيجيات
-عسكرة الفضاءات الالكترونية

الخلاصة: يعد استقرار الامن الاقتصادي و الامن السياسي و الأمن الوطني الذين يصبون جميعهم في بوتقة واحدة الا وهي الأمن المجتمعي بمثابة الحجر الأساس للحفاظ على الهوية الوطنية و مقياسا لازدهار و استمرار استقرار وبناء الوطن. حيث يعد استتاب الأمن المجتمعي بمثابة الضامن لسلامة و امن الافراد و المجتمع و تحفيز الفرد الابداعي التطويري فضلا عن تشجيع الاستثمار المحلي و الاجنبي و بأعتماد اسس التنمية المستدامة لضمان بناء المستقبل الافضل للاجيال الحالية و المستقبلية.ان مقومات الامن المجتمعي وفق متطلبات العصر الحالي تقتضي اعتماد اسس بناء امن الفرد الذي يعد بمثابة الحافز لاستمرارالحفاظ على خصوصية الهوية الوطنية المجتمعية من خلال اعتماد الاستقرار السياسي المقرون بتوافر الاستقرار الاقتصادي و الثقافي وبالتزامن مع وجود اداء فاعل للقضاء العادل تحقيقا لسيادة الدولة في كافة مرافقها و على اختلاف مستوياتها لضمان القضاء على اشكال الفساد و البطالة حيث يكون احلال السلام و الامن المجتمعيين. لقد اصبح من ضرورارت ديمومة الاستقرار الامني للمجتمعات اعتماد تعاون كافة جهات الدولة على مستوى القطاعيين الخاص و العام و باعتماد كافة الوسائل العملية لرصد وتحديد و توحيد الاحصاءات و المعلومات لكافة التحديات و الاحتياجات الاصلاحية الاساسية منها و الفرعية التي تعتمد في خلق استراتيجيات استشرافية مستقبلية لتنظيم و تطوير كافة مرافق المجتمع و التركيز على الاهمية القصوى للجوانب الامنية منها خاصة في خضم عوامل التسابق التسلحي وفق عسكرة للفضاءات الالكترونية و استحداثات الامن السيبراني و المعلوماتي و تزايد المخاطر التي لا تعتبر العامل الاساسي في خلخلة الامن المجتمعي فحسب بل وخلق الارهاب المدمر للبناء المجتمعي و استقراره وسيادة امن الوطن.ان الاختراقات الامنية الحديثة تتناسب في كينونتها مع طبيعة التطور التكنولوجي اللحظي الذي يجتاح العالم برمته حتى ان تفاقم طبيعة وانواع الاختراقات الامنية الهادمة لاسس الاستقرار الفكري و المعتقداتي و امن الاوطان اصبح من اهم الظواهر و الاليات التي تسعى الحكومات الى مواجهة مخاطرها و الحد منها خاصة بأعتماد دولنا العربية لادمان العالم الافتراضي المتمركز في وسائل التواصل الاجتماعي و الالعاب الرقمية الالكترونية بصورة شاسعة و الذي اصبح يشكل كارثة مهددة لاستقرار امن المجتمعات وفقا للعلاقات التشابكية العنكبوتية التي اوجدها الفضاء الالكتروني في اجندات مدفوعة الثمن موجهة و مخاطر امنه السيبراني وقد ساهمت مظاهر العولمة في اثرائها وفق سيطرة سياسية ذات صبغة اقتصادية و احتكار للاسواق و ترويج المنتجات بجعل الدول العربية المستهلكة في الغالب في ظل انحسار الصناعات الوطنية و هيمنة المستورد منها وفقا لمخططات الاجندات السياسية و الجيوسياسية و الجيو افتصادية في قولبة المجتمعات العربية وثقافتها و استقرارها .

المقدمة :

ان توطيد الدعائم الامنية وترسيخها في اي مجتمع يعد منذ الازل الشغل الشاغل لاهتمام المجتمعات عبر التاريخ كونه الاساس الذي يستقيم من خلاله النظام السياسي لاي دولة ويكون العامل الحيوي للاستقرار الاقتصادي وتطور ونمو المجتمعات. لقد سلط الضوء على جانب الامن المجتمعي و السيبراني في الفترات الاخيرة بفعل التغيرات المتسارعة التي اوجدتها الثوة التكنولوجية و الظواهر العولمية التي رافقتها و التي اسهمت بصورة كبيرة في تغيير سمات المجتمعات الانسانية و طبيعة التهديدات الامنية التي اجتاحته سواء على مستوى الفرد او المجتمع حيث اصبح بمثابة الهاجس الذي لا تسعى الدول بكل امكانتها لتحقيق امنها السيبراني بل اصبح اساسا لامن الافراد على حد سواء وفقا لما تميزت به مظاهر التطورات التي غزت المجتمعات من تهديدات امنية و تقنية عالية الامكانات و التأثيرات .ان امن الانسان الدولي وفقا لما يمر به العالم من تطورات لحظية في عالم المواطنة الرقمية يقع فيها تحت مظلة مخاطر و تهديدات اختلفت عن طبيعة التهديدات الامنية المجتمعية في العهود السابقة ذات التوجه العسكري المباشر بين معارك و جيوش و مواجهات تسلح ثقيل و خسائر بشرية و بنى تحتية و تخطيطات دولية عسكرية الا ان التغيير الاني يرتكز في تأثيراته الامنية السياسية على الافراد اكثر من كونه على دول مع اختلاف اشكال و تنوع تلك المهددات فالتطورات و التداخلات التي صاحبت العولمة و الثورة التكنولوجية قد صاحبها التطور ذاته على صعيد طبيعة النزاعات المسلحة و امكاناتها الهائلة حيث طبيعة التسلح الالكتروني العالي التقنيات و الامكانات المستخدم في العمليات الارهابية والاغتيالات و النزاعات العرقية والطائفية و الدينية المسلحة حيث التركيز على الافراد اصبح هو الهدف الواجب حمايته و من جانب اخر لعبت الكوارث البيئية كمخاطر امنية مهددة لحياة الافراد كالاوبئة المميتة و التصحر و الزلازل و شحة المياه ونقص الغذاء حيث يتزايد في ظل تلك المسببات النتائج الكارثية المتمخضة عنها بين ارتفاع في نسب الامية و الجهل الى الفقر و الامراض والموت و هجرة العقول و الايدي العاملة و معاناة فقدان الهوية و التخلخل الديمغرافي السكاني تلك العوامل المعيقة لا لتنفيذ الخطط التنموية و التنمية المستدامة فحسب بل انها اصبحت عوامل مشجعه للفئات الشابة خاصة للتحول الى عوامل الكسب السريع المهدد لاستقرار الافراد و امنهم بالانظام لعصابات الاجرام الدولي المنظم بين اتجار بالبشر الى الاتجار بالمخدرات و السلاح حيث يكون امان و مستقبل الشباب في خطر لا على المستوى امن بناء مستقبلهم الشخصي فقط بل على مستوى مستقبل بناء الاوطان وتعميرها .

يعد التوظيف الالكتروني لتنظيم مفاصل حياة الفرد باكملها بمثابة السلاح ذو حدين بين فوائد و مخاطر لا حصر لها فأعتماد المجتمعات المتفاقم على التحول الرقمي على الرغم مما قدمه من تسهيلات و تنظيم للحياة الانسانية الا ان مايقابلها من تفاقم التهديدات الامنية السيبرانية على مستوى الفرد و المجتمع و الناتجه عن مجموعة من العوامل بين مجهولية من نتعامل معهم خلف الشاشة الالكترونية على تنوعها و التي تعد

الاهم بالنسبة لمجرمي الهجمات الالكتروني الى ضعف تأمين البنى التحتية الالكترونية من شبكات المعلومات و الاتصالات المحلية و الدولية الى ضعف القوانين صياغتاً و تنفيذا و بما يتوافق وطبيعة التحديات التي اوجدها مجرموا الامن السيبراني في فضاءات الكترونية لاحدود لها و في تطوير مستمر مما استوجب التعاون الدولي السيبراني الذي لا حدود له وبما يتناسب مع تلك التحديات التقنية و المجتمعية و القانونية و الانسانية و على كافة المستويات كون التوجه المجتمعي لدول العالم اصبح الكترونيا بحت في تحول رقمي لكافة تفاصيله فاصبح لزاما احتواء المخاطر الامنية السيبرانية للحفاظ على امن و سيادة الدول .

منهج البحث :اعتمدت الدراسة تحليل كافة الطروحات سعيا لايجاد حلول واقعية مثمرة وفق المنهج الوصفي التحليلي الانسب لواقع الامن المجتمعي وفق التحديات و الطروحات المناسبة لها وصولا لامن الإنسان ومجتمعه .

أهمية البحث: تكمن أهمية الدراسة من اهمية السيادة الامنية السيرانية للدول و إيضاح ماهية طبيعة الهجمات الإلكترونية و مخاطرها و اثارها على بناء و مستقبل المجتمعات و التي ترقى الى ان تكون العامل الحيوي الفاعل في تهديد الامن القومي المجتمعي لسيادة الدول ومن طبيعة تلك التهديدات الشاملة لامن الدولة ككل يكون استنباط سبل المعالجات و المواجهات و الحماية اي بالتخطيط الاستراتيجي الشامل و التنسيق التنفيذي الموحد حيث الحلول الجزئية المنفردة لا طائل منها وتتفاقم من خلالها المخاطر لذا فأن الضرورات الحتمية الآنية وفق لمؤشرات المتزايدة لمخاطر الامن السيبراني على سيادة امن الدولة تقتضي تأمين التحول الرقمي المجتمعي في تخطيط شامل استراتيجي تكنولوجي وفق اسس الامن المعلوماتي في بيئة و بنى تحتية معلوماتية قومية ضخمة في صيانة امن معلوماتها و جعلها مورد ساند مطور لاستراتيجية بناء و تنمية و امن الدولة.

أهداف البحث : ترتكز أهداف الدراسة في اكثر من توجه اولها يعتمد ايضاح اشكالية المفاهيم المطروحة خاصة فيما يتعلق بمفهوم الامن و الامن المعلوماتي و الامن السيبراني حيث تتنوع الطروحات وفقا للمنظورات و التوجهات المعرفية للباحثين في تخصصات الدراسات الامنية و السياسية فلم تعد امنية المجتمعات بتشعباتها و تنوع و تعدد تحدياتها و اثارها محصورة في الاطار الضيق كونها معضلة يسهل حلها او تجاوزها بل اخذت منحى اخر و اصبحت في غالبية طروحاتها قضية راي عام يؤثر و يتأثر قيه كافة اطراف المجتمع و بناء الانسان و استقراره الذي يعد اساس لتطور الدول . وقد هدفت الدراسة ايضا الى توجيه الضوء على طبيعة التهديدات الامنية الحديثة المعقدة الانماط في تحليل لمختلف انواع التحديات وفقا للتحديثات التي طالت مختلف نواحي الحياة وأصبحت عرضة لمختلف أشكال الهجوم و التدمير الالكتروني لحظي التطور و الذي استوجب العمل على استنباط استراتيجيات دفاعية امنية وفق لاطر تتناسب مع طبيعة تلك الهجومات و الحروب السيبرانية الالكترونية المهددة للامن الانساني و بقائه.

إشكالية البحث: ان مشكلة الدراسة لا تتوقف عند ايضاح اهمية مايتمخض عن تهديدات الامن السيبراني و الهجمات السيبرانية و الاستراتيجيات الملزمة للحد منها بل تناقش ماهية العلاقة بين الفضاءات السيبرانية و عسكرتها و ما تتسبب به من مشاكل جمة تتعلق بسيادة الدولة و امنها و استقرارها حيث السيادة السيبرانية وفق التحول الرقمي لكافة مجالات الحياة حل محل سيادة الدولة و امنها المتعارف عليه لعهود مضت .

هيكلية البحث : تنقسم هيكلية البحث الى ثلاثة مطالب كما يأتي :

المطلب الاول : الامن المحتمعي مفاهيم و مصطلحات الدراسة

المطلب الثاني : تداعيات الحروب السيبرانية على الامن المجتمعي

المطلب الثالث: الاستراتيجيات الاصلاحية الامنية السيبرانية المجتمعية

ان تداخل واقع الاسقاط للحدود الجغرافية و الثقافية والسياسة للدول الذي احدثته تكنولوجيا المعلومات الحديثة اوجد في الان ذاته تفاقماً سريعاً في تنوع و تعدد و شدة المخاطر الامنية وفقا للتكتيكات الامنية الالكترونية اللحظية التحديث حيث تشكل تحديات جسيمة على الامن القومي خاصة مع تغيير اليات ومفاهيم الحروب وفقا لتحديات الامن السيبراني والذي لم تتوقف مخاطره عند الجوانب الامنية العسكرية المنحى بل اتسعت وفقا لشمولية الامن السيبراني لخصوصية الامن المعلوماتي المتعلق بعمل الشبكات و الحاسوب و كافة الاجهزة الالكترونية التي اجتاحت كافة مرافق الدولة للتوثيق المعلوماتي و سرعة الانجاز وفق نظام الحوكمة الالكترونية المتبع في غالبية دول العالم حيث تتسع التحديات و التهديدات لتشمل الجوانب الاقتصادية و الاجتماعية وتقف بمثابة العائق لتطورات الاقتصاد المعرفي الرقمي و تصل مخاطر تلك الحروب السيبرانية لتهديد السيادة الوطنية للدول بما تتسبب به تلك الهجمات الالكترونية من اختراقات لكافة المؤسسات الحكومية و لمختلف درجات خصوصيتها مثل برامج التجسس و التلصص و التخريب و التعطيل و القرصنة الالكترونية والذي يستوجب العمل على استحداث استراتيجيات تعتمد احدث الاليات الدفاعية الامنية الالكترونية تنفذها الدولة حماية لامنها و اقتصادها و سيادتها الامنية و للارتقاء بالمستويات الامنية وفق ماتقتضيه تلك الحروب السبرانية و عسكرة الفضاءات الالكترونية على كافة الاصعدة سواء في الجوانب القانونية التشريعية او على مستوى التوعوي للمخاطر التكنولوجية لامن الانسان و الدولة من خلال توظيف وسائل الاعلام و التواصل الاجتماعي او حتى ادراجها كمادة علمية تتدرج في طروحاتها التقنية وفقا للمراحل الدراسية كافة كي تكون الاجيال القادمة على دراية و خبرات كاملة بحجم المخاطر و كيفية الوقاية و الحد منها حفاظ على الامن القومي و سيادة و استقرار الدولة.

ان امن الانسان الدولي وفقا لما يمر به العالم من تطورات لحظية وفقا للثورة التكنولوجية يقع فيها تحت مظلة مخاطر و تهديدات اختلفت عن طبيعة التهديدات الامنية المجتمعية في العهود السابقة ذات التوجه العسكري المباشر بين معارك و جيوش و مواجهات تسلح ثقيل و خسائر بشرية و بنى تحتية و تخطيطات

دولية عسكرية الا ان التغيير الاني يرتكز في تأثيراته الامنية السياسية على الافراد اكثر من كونه على دول مع اختلاف اشكال و تنوع تلك المهددات فالتطورات و التداخلات التي صاحبت العولمة و الثورة التكنولوجية قد صاحبها التطور ذاته على صعيد طبيعة النزاعات المسلحة و امكاناتها الهائلة حيث طبيعة التسلح الالكتروني العالي التقنيات و الامكانات المستخدم في العمليات الارهابية والاغتيالات و النزاعات العرقية والطائفية و الدينية المسلحة حيث التركيز على الافراد اصبح هو الهدف الواجب حمايته و من جانب اخر لعبت الكوارث البيئية كمخاطر امنية مهددة لحياة الافراد كالاوبئة المميتة و التصحر و الزلازل و شحة المياه ونقص الغذاء حيث يتزايد في ظل تلك المسببات النتائج الكارثية المتمخضة عنها بين ارتفاع في نسب الامية و الجهل الى الفقر و الامراض و الموت و هجرة العقول و الايدي العاملة و معاناة فقدان الهوية و التخلخل الديمغرافي السكاني تلك العوامل المعيقة لا لتنفيذ الخطط التنموية و التنمية المستدامة فحسب بل انها اصبحت عوامل مشجعه للفئات الشابة خاصة للتحول الى عوامل الكسب السريع المهدد لاستقرار الافراد و امنهم بالانظام لعصابات الاجرام الدولي المنظم بين اتجار بالبشر الى الاتجار بالمخدرات و السلاح حيث يكون امان و مستقبل الشباب في خطر لا على المستوى امن بناء مستقبلهم الشخصي فقط بل على مستوى مستقبل بناء الاوطان وتعميرها .

بعض الدراسات السابقة فيما يتعلق بخصوصية الاشكاليات الامنية المجتمعية :

تأسيسا على أفكار مدرسة ما بعد الاستعمار وتحت عنوان "الإشكالية الأمنية في العالم الثالث" يراجع محمد أيوب إسهامات عدد من الباحثين في سياق البحث عن مفاهيم أمنية تتجاوز التحيز في الخطاب الغربي، فمثلا كارولين توماس Caroline Thomas تعتبر أن مفهوم الأمن القومي في بلدان العالم الثالث لا يجب أن يقتصر على دراسة استخدام القوة العسكرية مثل غالب المحاورات الغربية حول المفهوم، ولكن يجب أن يشمل مجمل القضايا التي تمثل تهديدا وجوديا للاجتماع السياسي لتلك البلدان –والتي قد لا تمثل تهديدا في دول الغرب– مثل قضايا الهوية والانشطار الثقافي في مجتمعات ما بعد الاستعمار أو قضايا نقص الغذاء والتهديدات الصحية، أو ربما السعي لامتلاك أسلحة نووية من أجل التوازن الأمني في مقابل الدول الغربية"[1]

"هدفت الدراسة إلى تعرف الانعكاسات القانونية للعدالة البطيئة .فى ضوء المجتمع المعاصر .على الأمن الاجتماعى وذلك من خلال ممارسة القضاء لقضاياه التى تمس النواحى الحياتية لأفراد المجتمع. وتوصلت تلك الدراسة إلى أن تباطؤ القضاء في حسم الدعوى وفق الحق يولد شعور مقلقا وتتولد صراعات جديدة باتجاه العنف » الحل العشائرى « لطرفى الدعوى، ويصبح الاتجاه إلذي يرافقها اضطراب لعوائل المتنازعين

[1] Ayoob, M., & Wells, S. (1991). The Security Problematic of the Third World. World Politics, 43(2), 257–283. Retrieved January 16, 2021. p – 259

وتترسب أحقاد قد تنتهى بجرائم قتل.كما توصلت إلى أن النزاعات البسيطة، التى لم يتمكن القضاء من حسمها والنظام القبلى من تهدئتها، بالتالى لها تأثير على الأمن"[1]

وتوصلت تلك الدراسة إلى وجود ترابط بين الأمن الاجتماعى والأمن الاقتصادى فلا يوجد أمن اجتماعى بدون أمن اقتصادى وقد تأكد ذلك من خلال الآية الكريمة.(سورة قريش الآية ٥) **«الذى أطعمهم من جوع وآمنهم من خوف»** كما توصلت إلى وجود معوقات للأمن الاجتماعى والأمن الاقتصادى وهى متداخلة تشمل عدم استغلال الثروات والموارد الطبيعية وعدم العدالة فى توزيع العائدات على المجتمع مما يؤدى إلى إضعاف الوضع الاقتصادى للدولة ويشير إلى وجود حالة متدنية من القدرة الاستراتيجية والسياسية والاقتصادية للدولة. [2]

تعد هذه الدراسة أن ليس من السهل تناول مفهوم الأمن بشكل محدد، لكونه مفهوماً نسبياً ومتغيراً ومركّباً، وذا أبعاد ومستويات متنوعة، إضافة إلى أنه يتعرض لتحديات وتهديدات مختلفة، سواء كان يتعلق بأمن الفرد أو الدولة أو النظام الإقليمي أو الدولي، وبأشكاله السياسية والاجتماعية والاقتصادية ببعديه الوطني والإقليمي، مع ضرورة التفريق بين مفهومي التهديدات والتحديات، إذ إنّ التحديات تعني المشاكل والصعوبات أو المخاطر التي تواجه الدولة في تحقيق تقدمها، وتكون عثرة أمام تحقيق استقرارها، وتنتهي بانتهاء الأسباب، أما التهديدات فهي تدخل في نطاق الأثر المباشر والسريع؛ كاستخدام قوة عسكرية، أو التهديد بها.وتتعرض الدراسة المكونة من عشرين صفحة إلى أشكال التهديدات التي يواجهها الأمن، باعتبار أن العلاقة بين هذين العاملين هي علاقة ذات تأثير متبادل، بحيث يتم تحديد كل ما يهدد الأمن بتحديد الوسائل والإجراءات اللازمة لمواجهة المخاطر. وقد ركزت الدراسات الأمنية سابقاً على خطر الغزو العسكري، بينما تركز الدراسات الحديثة للأمن على مصادر أخرى لا تقل أهميتها عن البعد العسكري؛ تتمثل بالتهديدات السياسية والاقتصادية والاجتماعية ببعديها الداخلي والخارجي، وفق منظورات مختلفة، سواء كانت واقعية أو ليبرالية، لتحديد الأمن اللازم بمفهومه الإستراتيجي القائم على بلوغ المصالح والغايات القومية، والذي يتم تحديده بناء على فهم حقيقة التحولات الدولية والإقليمية، وانعكاسها على الأمن.[3]

ان تعدد الاشكاليات و التحديات السياسية و الامنية و الاقتصادية و المجتمعية التي تواجه استقرار الامن المجتمعي و تداخلاتها و تفاقمها استوجب استعراضها وفق الدراسة المطروحة من خلال التأكيد على طبيعة العلاقة الجدلية القائمة بين تلك التحديات و استقرار الامن المجتمعي وبنسب مختلفة و في الان

[1] رياض هاني " العدالة البطيئة وانعكاسها على الأمن الاجتماعي"الحوار المتمدن ع 3722 ,2012

[2] سهيل حوامدة "الأمن الاجتماعى رهن الأمن الاقتصادى من منظور إسلامى " 2012م /5/ جريدة السبيل 24

[3] سليمان عبدالله الحربي "مفهوم الأمن: مستوياته وصيغه وتهديداته"، دراسة نظرية في المفاهيم والأطر، المجلة العربية للعلوم السياسية، مركز دراسات الوحدة العربية، ع: 19، بيروت. (2008)

ذاته السعي الى طروحات تتلائم مع تلك الاشكاليات بما يتناسب و طبيعتها و الامكانات المتاحة و التعاون الممكن المثمر.ان اختلال موازين التفاعلات السياسية و الاجتماعية و الاقتصادية يتسبب باختلال الامن المجتمعي و امن الانسان بما ينتج عنه من افرازات لظواهر هادمة لبناء الامن الانساني و تتسبب بالارباك القلق و المخاوف و اختلال موازين القيم المجتمعية بما ينتج عنها من انحرافات سلوكية ذات اضرار مادية ومعنوية و اخلاقية وتختلف مسميات و طرق تلك الظواهر و تجتمع في اثارها كالفساد والادمان والتهريب والتزوير و الابتزاز وعصابات الاتجار بالبشر والمخدرات و السلاح الا انها جميعا باتت تنخر في النسيج المجتمعي و تتسبب بذات الاثار التي تتركها الزلازل و الاعاصير بمكنونات و اسس التوازن المجتمعي ان فاعلية سيرورة ميكانزمات الامن المجتمعي قد تعرضت الى العديد من العوامل المستحدثة و المعرقلة لمسيرتها بالصورة السوية السليمة و الناتج من و اقعية انتشار اشكال الفساد واستفحال اثاره وفقا للسلوك غير السوي للافراد مع ضعف فاعلية القوانين وتنفيذها فضلا عن تغيير كبير في القيم المبادى الوطنية المجتمعية .

المطلب الأول : الأمن المجتمعي مفاهيم و مصطلحات الدراسة

الأمن بسكون الميم لغة : ضد الخوف ، وهو من باب أمن وفهم ، والأمن بكسر الميم : أى المستجير ليأمن على نفسه ، ومنه الآمن أى غير الخائف[1]

واصطلاحاً : لم يختلف المعنى الاصطلاحى عن المعنى اللغوى، لذا فقد عرفه الإمام الجرجانى بأنه : (عدم توقع مكروه فى الزمان الآتى)[2] لقد شكل عالم ما بعد الحرب الباردة أرضية خصبة لتنامي النقاشات النظرية بشكل كبير حول مفهوم الأمن ،بما ينسجم وطبيعة التوجهات الديناميكية المعاصرة،حيث تمكنت الطروحات الحديثة بما فيها النظرية النقدية للأمن من تقديم بدائل فيما يخص الموضوع المرجعي ،فلم تعد الدولة هي محور التركيز في الدراسات الأمنية بل أصبح الاتجاه نحو الفرد باعتباره وحدة التحليل الأساسية وما على الدولة سوى ضمان أمنه و رفاهيته .فمفهوم الأمن تطور وأصبح يتجه نحو الإنسان بشكل أساسي من خلال طرح مفهوم مستحدث وهو مفهوم الأمن الإنساني وترابطه بكل من الأمن المجتمعي والأمن العالمي بعدما كان تقليديا مقتصرا على المسائل العسكرية التي تمس أمن الدولة[3]

قدم "إحسان محمد الحسن" التصور السوسيولوجي للأمن الاجتماعي الذي يرى بأنه يشير إلى : سلامة الأفراد والجماعات من الأخطار الداخلية والخارجية التي قد تتحداهم وما يتعرض له الأفراد والجماعات من القتل والاختطاف والاعتداء على الممتلكات بالتخريب أو السرقة ، مسؤولية اجتماعية بوصفه ينبع من مسؤولية الفرد تجاه نفسه وأسرته.[4]

عرف "والتر ليبمان "Walter LIPPMAN الأمن على أنه: حفاظ الأمة على قيمها الأساسية وقدرتها على صيانة هذه القيم حتى وإن دخلت حربا لصيانتها.[5]

مفهوم الأمن الإنساني يعالج مسألة حماية الحريات المدنية الأساسية، وفي نفس الوقت يعنى بحماية الأفراد ضد التهديدات الخطيرة على مصيرهم ومستقبلهم. هذا يعني أيضا ضرورة إنشاء نظام يمنح للأفراد أساسيات

---

[1] القاموس المحيط للفيروزابادى ج4 ص 194 ، الهيئة المصرية العامة للكتاب عام 1400هـ- 1980م ، مختار الصحاح للرازى عنى بترتيبه : السيد محمود خاطر ، دار التراث العربى للطباعة والنشر بمصر. ص26.

[2] التعريفات للجرجانى ، تحقيق / إبراهيم الإبيارى ، دار الريان للتراث بمصر 1982. ص55

[3] جميلة علاق، خيرة ويفي ،"مفهوم الأمن بين الطرح التقليدي والطروحات النقدية الجديدة".في الملتقى الدولي: الجزائر والأمن في المتوسط:واقع وآفاق، جامعة قسنطينة ، 29-30 أفريل 2008 ، ص.316

[4] إحسان محمد الحسن، "علم اجتماع السياسي"، دار وائل، الأردن، 2009، ط3 ، ص 25

[5] John BAYLIS and Steve SMITH , Globalization of World Politics, second ed. Oxford university press, New York, 2001. p 255

العيش الكريم ويحقق لهم الرفاه في حده الأدنى، فأمن الإنسان يعنى أنواع من الحريات مثل تحرر الفرد من الحاجة ومن .وهناك تعريف آخر للأمن الخوف وحرية وصول الإنسان إلى جوهره"[1]

"الأمن من الحاجات الأساسيّة للنفس، وبمفهومه العام هو الاطمئنان الذي ينتج عن الثقة وأمن الإنسان من الفقر والحرمان والخوف والعنف، وعلى الرّغم من أهميّة مفهوم أمن الدولة إلّا أنه لا يكفي لتحقيق أمن الأفراد؛ لذلك فقد تطوّر مفهوم الأمن الإنساني نظراً لتطور المجتمعات وتزايد التهديدات الدّاخلية والخارجيّة، مما تطلّب تركيزاً واهتماماً بالإنسان كفرد فاعل ومؤثّر في المجتمع. يعتمد الأمن الإنساني على مجموعة من الخصائص وهنا نذكر عدداً منها: مفهوم شامل يشمل كلّ دول العالم بجميع إمكانيّاتها، نظراً للتهديدات الخارجية المشتركة التي تؤثر على الأفراد في كل مكان كالإرهاب والمخدّرات، لذلك فإنّ أيّ تجاوز يؤثّر على أمن الناس يستوجب تدخلاً من كل الدول لإيقافه ومنع تكراره. يهتم بأمن النّاس والظروف المتعلقة بكل شخص لتحقيق العدالة الاجتماعيّة، فهو يبتعد عن الحلول العسكريّة لحلّ المشكلات ويُركز على الاهتمام بالأفراد والتنمية البشريّة. أهم شعار للأمن الإنساني هو الوقاية خير من العلاج، لذلك يتمّ الحرص على تجنب حصول المشكلات وحلّها قبل تفاقمها بالتالي تجنّب حصول الصراعات بين الأفراد في المُجتمع الواحد[2]

بينما تميل الاتجاهات النقدية في الدراسات الأمنية –المستندة إلى ابستمولوجيا ما بعد وضعية– إلى طرح مفاهيم ذاتية للأمن، حيث يُعتبر الإنسان الوحدة المرجعية للأمن بدلا من الدولة، وشعور الإنسان بـ "الانعتاق" والتحرر هو القيمة المرجعية النهائية للأمن، بدلاً من التمركز حول مفهوم قوة الدولة. ويعد كين بوث –Ken Boothمن أهم المنظرين لهذا التيار، ويعرف بأنه مؤسس "مدرسة ويلز في الدراسات الأمنية"، التي تستند في تفسيراتها الأمنية علي أفكار النظرية النقدية التي طورها مفكرو مدرسة فرانكفورت، كما تستند على بعض أفكار جرامشي –Gramsciكمفاهيم تأسيسية، ويعرف كين بوث مفهوم الانعتاق بأنه "تحرير الناس من القيود والضغوط التي تمنعهم من ممارسة ما يريدونه بما يتوافق مع حرية الآخرين"[3]

وإذا كان المفهوم الغربي للأمن، في إطاره السائد، يتمركز حول الدولة باعتبارها الوحدة الرئيسية للأمن، فإن هذا التصور يبدو مبررا في سياق الاجتماع السياسي الغربي. بينما في دول ما بعد الاستعمار حيث تعاني الدولة من أزمة شرعية وتعاني المجتمعات من غياب الإجماع ومن الانشطار الثقافي، فثمة حاجة ماسة لتصورات للأمن أبعد من التمركز حول الدولة، بل أبعد كذلك من النظريات النقدية الغربية، فالدولة، فيما تم

---

[1] – Karim hussein, Donata Guisciet Et Julia Wanjiru. Sécurité et sécurité humaine. Présentation des concepts et des initiatives quelle conséquences pour l'Afrique de l'ouest ?. Rapport de club du sahel et de l'Afrique de l'ouest. 2004. P 16. www.oecd.org/fr/csao/publications/38826711.pdf 24 – ibid. p 16.

[2] الاء عيسى "مفهوم الأمن الإنساني"2018 (mawdoo3.com)

[3] Booth, K. (2007). Theory of world security (Vol. 105). Cambridge University Press–P: 112

توصيفه سابقاً العالم الثالث، تمثل بتعبير آنيا لومبا "استعمار ما بعد الاستعمار" قد تكون مصدر غياب الأمن ومصدر التهديد الرئيسي وليست الوحدة التحليلية للأمن كما عند الواقعيين الغربيين، إذ لا يمكن تجاهل الانتهاكات التي تقوم بها تلك الدول تجاه الحقوق الأساسية لمواطنيها[1]

نستنتج من المفاهيم الايضاحية السابقة، ان تعدد مكونات الامن المجتمعي بين السياسي الى الاجتماعي و الاقتصادي والثقافي جعل دائرة التحديات تتسع باتساع المكونات الا ان تحقيق الامن الشامل يبدا من تحقيق امن الانسان. ان التغيرات المستمرة على الساحة الدولية قد شملت في موجة التغيرات تلك وفق مااوجدته العولمة من تأثيرات فكرية ثقافية اثرت بصورة كبيرة في ابعاد مفهوم الامن المجتمعي فالتحول كان جليا من التركيز على امن الدولة فقط بصورة رئيسية الى تحويل ابعاد مفهوم الامن المجتمعي الشاملة للدولة ككل الى جعل اهم ابعادها تتمثل في تحقيق الامن الانساني من خلال خلق الاليات الضامنة لبناء مجتمع يكون اساسه احترام حدود الاخر و خصوصيته في توازن فاعل وفق اندماج قومي تعددي لايقف عند حدود الدين او العرق او الثقافة او اللهجة او اللغة حيث تحقيق الطمأنينة و الاستقرار و الامن المجتمعي في اطار من الحرية السياسية و العدالة المجتمعية . ان انحراف السلوك الانساني عن المسار السليم المتحدد بالقوانين و تنفيذها نابع من الاختلال الاكبر الا وهو الامن المجتمعي حيث يؤدي انتشار الظواهر المدمرة مجتمعيا كالاتجار بالبشر و المخدرات و الاسلحة تؤدي الى خلق الارباك و اختلال الموازين المجتمعية .ان طبيعة تلك التحديات التي بدات تجتاح العالم على مستوى العلاقات المحلية و الدولية خاصة بعد الحرب الباردة تبلورت شي فشيئا لتصبح بمثابة القوى العالمية النهج ذات تأثيرات و الادوار الدولية على خصوصية السياسات الاقتصادية و الاجتماعية و حتى السياسية منها وفقا لاتساع قوة و مدى تلك التهديدات المعاصرة حيث اصبحت الدول لاتقوى على مواجهة خطورة و مصاعب تلك التحولات بمفردها و التي حولت المفاهيم الامنية و خصوصيتها العسكرية السابقة الى انماط تهديدات امنية مهولة متنوعة و متعددة كالارهاب بشتى صوره و الحروب البايولوجية بصورها المختلفة كالاوبئة والحروب البيئية المفتعله وقد رافق كل ذلك مااثقلت به العولمة كاهل دول العالم الثالث من تبعات مستحدثة وفق مايسمى بألاستعمار الضمني المبطن مابعد انتهاء مظاهرالاستعمار العلني بجعلها دول مستهلكة لا منتجة و لا مصدرة بل تحدد دورها بين سوق تصريفي للمنتجات الخارجية فضلا عن مصدر للموارد الاولية للصناعات الخارجية وبفضل التطورات الالكترونية المهولة فقد اصبح التسلح سهل التداول و بتقنيات عالية حيث تصب كل تلك التحولات في بوتقة واحدة مهددة للامن المجتمعي و الذي يعد من اهم ابعاد الامن الانساني و تلك العوامل برمتها تعتبر ذات

[1] Acharya, A. The periphery as the core: The third world and security studies(1995).

تهديد فاعل لامن الانسان و استمرار وجوده و تحقيق خصوصيته الابداعية و التي بها يكون تحقيق التنمية المجتمعية وفق اليات يكون من خلالها العمل على خلق مجتمع تعددي الخصوصية الثقافية و الدينية و العرقية وفق تعايش سلمي امني يتقبل الاخر و يندمج معه بأعتماد اسس سياسية اجتماعية اقتصادية يكون فيها احقاق الامن المجتمعي .

لقد استحدث عصر المعلوماتية الحالي نمط جديد من الحروب الاستراتيجية االالكترونية و بالرغم من تعدد معرفي مفهوم الحرب السيبرانية و الامن السيبراني الا ان الاتفاق في كون حجم النتائج المترتبة عنها مشابه في اثارها للحروب النووية للقرون الماضية حتى ان التنافسية الدولية في مجالات الابتكار و الابداع و التسلح في الفضاءات الالكترونية اصبحت شاملة مجالات الحياة الاقتصادية و السياسية و الاجتماعية و التنموية لشمولية التوضيف الالكترونية لمجالات حياتنا الحالية و المستقبلية في تسابق تسلحي الكتروني شاملا مختلف انماط العسكرة للفضاءات السيبرانية مثير للقلق و الرعب المجتمعي المجلي و الدولي خاصة فيما يتعلق بمستقبل الاستقرار و السيادة الامنية لشعوب العالم باجمعه .

ويُقصد بالإرهاب الإلكتروني العبث بالنظم الإلكترونية لمجرد إثارة الذعر أو الخوف. ويعتمد الإرهاب الإلكتروني على استخدام الإمكانيات العلمية والتقنية، واستغلال وسائل الاتصالات والشبكات المعلوماتية من أجل تخويف الآخرين وترويعهم، وإلحاق الضرر بهم، أو تهديدهم. وغالبًا ما تهاجم الجماعات الإرهابية التي ترغب في بث الخوف والدمار والخسائر في الأرواح البنية التحتية الحيوية. ومن الأمثلة على هذه البنى التحتية المعرَّضة للخطر في الغالب التحكم في الحركة الجوية والشبكات الكهربائية ومحطات الطاقة النووية[1]

المطلب الثاني : تداعيات الحروب السيبرانية على الامن المجتمعي

يتعلق مضمون الحرب الإلكترونية بالتطبيقات العسكرية للفضاء السيبراني، حيث تعني –في أحد تعريفاتها– قيام دولة أو فواعل من غير الدول بشن هجوم إلكتروني في إطار متبادل، أو من قبل طرف واحد. وبرغم ذيوع مسمي "الحرب الإلكترونية" إعلاميا، فإنه يعد مصطلحا قديما كان بالأساس مقصورا على رصد حالات التشويش على أنظمة الاتصال، والرادار، وأجهزة الإنذار، بينما يكشف الواقع الراهن في الفضاء الإلكتروني عن دخول شبكات الاتصال والمعلومات إلى بنية ومجال الاستخدامات الحربية [2]

---

[1] 2021ICS Cybersecurity Year in Review. Dragos ,https://bit.ly/3W8reVn

See: Al-Bayati, Raji Youssef. "Cyber terrorism (models of international efforts to reduce it)." Tikrit Journal For Political Science 2.28 (2022): 91-121.

[2] عادل عبدالصادق،" حروب المستقبل الهجوم الإلكتروني على برنامج إيران النووي"، مجلة السياسة الدولية، مؤسسة الأهرام، أبريل 2011.

ان الحروب ايا كان تصنيفها تعد صورة من صور الارهاب لجميع المشتركين فيها لما تتسبب به من الاثارالمترتبة عنها خاصة فيما يتعلق بخسائر الثروة البشرية التي هي اساس بناء المجتمعات و تطويرها خاصة مع مايشهده العالم من تطورات الثورة التكنولوجية و ابداعاتها وفوائدها وفي الان ذاته تداعياتها والحروب السيبرانية المتسببة بها و التي تعد بمثابة شاهد اثبات ان العقول البشرية لا حدود لمداها . تتشابه الحروب السيبراني في اثارها مع الحروب التقليدية في مجالات عديدة رغم كونها لا تلتقي في اساليبها و تطبيقاتها مع تلك الحروب الا ان كلا الصنفين من الحروب يكون المتضررين بالدرجة الاولى هم المدنيين حيث الحروب التقليدية يكون الاستهداف المباشر للافراد و للبنى التحتية وتدميرها كالمؤسسات الصحية و التعليمية والعسكرية من خلال مايشاهد من قوات عسكرية و دبابات و طائرات عسكرية مدمرة وتسبقها تخطيطات و ميزانيات مالية ضخمة تخصصها الدول للتطويروالاعداد العكسري. اما فيما يتعلق بخصوصية الحروب و الهجمات السيبرانية فتعد الثروة البشرية المتضررالمشترك الا ان طغيان العالم الاكتروني في تحول رقمي شامل لدول العالم بأكمله اوجد مظاهر حرب سيبرانية فائقة التقنيات مخفية المسبب كارثية النتائج محدودة التكاليف و المحاسبة القانونية دائمة التحديث في كافة توجهاتها حيث لا تتعدى ضغطة زر الكتروني متسببة بهجوم سيبراني مهول في اثاره التخريبية لامن المعلوماتي لاي دولة في العالم حيث لا حدود تقف عائقا بوجه تلك الحروب السيبرانية المدمرة كون الفضاءات السيبرانية المتاحة ملعبها و ساحتها القتالية ، و في ظل التوضيف الالكتروني لكافة مرافق الدول في اعتمادها التحول للعوالم الرقمية حيث لا تتحدد الاثار المدمرة عند واقع العالم الالكتروني فحسب بل يشمل في تدميره لكافة البنى التحتية المعلوماتية الالكترونية لمؤسسات الدولة العامة و الخاصة و و المصرفية و الامنية منها بالذات في مخاطر كارثية تتصاعد اثارها و تتفاقم مع تفاقم التطورات وفق سباقات التسلح التكنولوجية التي باتت تهدد بحروب كارثية تجتاح العالم برمته و هو ماتختلف معه الحروب التقليدية محددة المكان و الزمن و الاثار .

ظهر مصطلح الفضاء السيبراني، أو الفضاء الإلكتروني، لأول مرة، عام 1982، في رواية خيال علمي، للكاتبWilliam Gibson ، باسم Neuromancer ، ولا يوجد تعريف، واحد، متفق عليه، دولياً، لمصطلح الفضاء السيبراني، إنما بعض التعريفات، المقبولة، على مستويات مختلفة، مثل الأمن القومي، وأمن المعلومات. وبعيداً عن روايةWilliam Gibson ، فالفضاء السيبراني لم يعد خيالاً علمياً، بل أصبح واقعاً علمياً، ذو تأثيرات اجتماعية وسياسية واقتصادية. فلغوياً يشتق لفظ"Cyber" ، من الكلمة اللاتينية "Kubernētēs"، بمعنى قائد الدفة، في إشارة إلى القيادة والإدارة، إلا أن اللفظ التصق، لاحقاً، بكل ما يخص الفضاء"Space" ، واستخدم في كل ما يتعلق بالإنترنت، بعد ظهوره، وانتشار استخدامه بشكل كبير. فصار من المعلوم أن الفضاء السيبراني، أو الفضاء الإلكتروني، هو الوسط الذي تتواجد به، وتعمل فيه

شبكات الحواسيب الإلكترونية، في العالم كله، بما في ذلك أجهزة الكمبيوتر، وأنظمة الشبكات، والبرمجيات، وحوسبة المعلومات، ونقلها، وتخزينها، ومستخدميها من البشر والهيئات والمؤسسات.[1]

ان أهداف الحرب السيبرانية لا نطاق او حدود لها كونها لا تتحدد بزمان او مكان او تكوين معين سواء في طريقة التنفيذ او المسببات فبين هجمات الكترونية يكون نتاجها سرقة ادق المعلومات الامنية الى تحويلات مصرفية تفلس بها كبرى المصارف الدولية فضلا عن تحويل المسارات للصواريخ و لمختلف الرحلات البحرية و الجوية و توقيف الانظمة الالكترونية للعالم اجمع لوقت و هدف تدميري يظهر لنا بصورة جلية الخطورة العالمية للحرب السيبرانية المستقبلية على العالم اجمع.

حيث يتزامن التطوير مع الاستهداف من قبل مجرمي الهجمات الالكترونية خاصة مع اجهزة الجيل الخامس و انتشار المدن الذكية و الحوسبة السحابية و انترنت الاشياء .ان تعدد الاشكاليات و التحديات التي تواجه استقرار الامن المجتمعي و الانساني و الالكتروني و تداخلاتها و تفاقمها استوجب التأكيد على العلاقة الجدلية القائمة بين طبيعة تلك التحديات وسرعة تفاقمها وتطويرها و اثارها و المتناسبة مع طبيعة الثورة التكنولوجية العولمية وانماط الاجتياحات الالكترونية المتنوعة التي تقع تحتى مسمى الحروب السيبرانية وفق سباق عسكرة الفضاءات الالكترونية الذي لا حدود له.

إن الهجمات التي تُشن ببرمجيات الفدية، بكافة أنواعها سواء أكانت برامج الفدية الشائعة أو نظيراتها المستهدفة أو برامج فدية الثغرات المجهولة، سوف تبقى من بين أكبر التهديدات التي تواجه الدول والمؤسسات العامة والخاصة. ومن المتوقع أن يشهد عام 2023 نموًا في الهجمات الإلكترونية ذات الدوافع المالية والمعروفة ببرامج الفدية، خاصةً أن المجرمين يستهدفون بدرجة متزايدة أجهزة الجيل الخامس والحوسبة السحابية وإنترنت الأشياء، مما يتسبب في مزيد من الاضطرابات وزيادة متطلبات الأمن السيبراني الجديدة. بمعنى آخر، من المرجح حدوث ارتفاع في تهديدات برامج الفدية وأن تواصل اتجاهها التصاعدي، حيث سيستمر الفاعلون المهددون المنخرطون في ابتزاز متعدد الأوجه في إيجاد المزيد من السبُل لابتزاز ضحاياهم. وطبقًا لبعض التقديرات، فإن تكلفة برامج الفدية 265 مليار دولار سنويًا[2]

لقد اصبحت مفردة تكنولوجيا من اكثر الكلمات تداولاً في عصرنا الحالي بين الناس لدخولها الفعلي في جوانب حياتنا اليومية و توظيفها و تنظيمها للمجالات الاقتصادية و الصناعية و التعليمية و الاجتماعية بمختلف الاشكال و صولا الى الجانب العسكري وتغيير الشامل للطبيعة العسكرية لعصور خلت في توجه تسابق ملحوظ نحو التسلح وعسكرة الفضاءات الالكترونية و استحداثات الامن السيبراني و خصوصية

[1] سمير فرج " الفضاء السيبراني" 2020 مصر https://samir-farag.com/

[2] Anupama A , Amritha Saravanan, , 7 cybersecurity trends to watch for in 2023, Manage Engine , 31Oct 2022, https://bit.ly/3WJyeJk

القوانين المستحدثة في مجالات الحماية الالكترونية سواءاً على المستوى الشخصي للفرد او على مستوى المجتمع المحلي و الدولي لاتساع دائرة الاستحداثات الالكترونية و فوائدها و مخاطرها في الان ذاته حيث اصبح معيار تطور الدول اقتصاديا واجتماعيا و علميا يعتمد وفقا لما تم تحقيقه وتميزت به تلك الدول تكنولوجياً وفقا لمحور عجلة التقدم في عالمنا الحالي في تحديات كبيرة مستمرة في السوق العالمي الاقتصادي في تنافسية تكنولوجية تصاعدية في كافة مجالات الحياة المدنية و العسكرية منها.

وقد شهدت الأسلحة الإلكترونية تطورا أكبر في قدرتها على التأثير في الخصوم، مثل أسلحة الميكروويف عالية القدرة، والهجمات الإلكترونية عبر الفيروسات، مثل شن إسرائيل هجمات فيروس ستاكسنت ضد المنشآت النووية الإيرانية بالتعاون مع الولايات المتحدة في عام 2010(20)، وكان قد تم تطوير هذا الفيروس وتجربته في إسرائيل خلال عام 2007[1]

لم تعد التكنولوجيا عبارة عن ادوات ذات تقنيات توظف لتسهيل اداء الاعمال و تطويره بل اتسع تأثيرها لكافة نواحي حياتنا حتى اصبحت بمثابة راس الحربة المغيرة للمشهد العالمي على مختلف المستويات الشخصية و المجتمعية و الاقتصادية و العسكرية سواء على المستوى المحلي ام الدولي بكافة مكوناتها و توجهاتها حتى انتشر تأثير التكنولوجيا و اصبح ذلك الطغيان بمثابة سلاح ذا حدين بين ضرورة مواكبة التطورات التكنولوجية المتسارعة في ظل عصر التحولات الرقمية الى المخاطر الالكترونية التصاعدية الموازية في حجم اثارها لسرعة التطور في اثاره و تداعياته فبين الابهار التكنولوجي المستمر و لهاثنا لاقتناء الاحدث نغفل عن ما تتضمنه تلك التطورات من التاثيرات التي لا تنحسر في حدود الايجابية الابداعية منها بل تمتد تأثيراتها السلبية لتغيير خصوصيات مجتمعاتنا و عقولنا و تكويننا الانساني الذي بات يتضائل دون ادراكنا ليطغى ادمان التفرد مع اجهزتنا الالكترونية و انماط حياتنا التي توحدت معه .

الاستعداد لحروب المستقبل، حيث تبني العديد من الدول استراتيجية حرب المعلومات بحسبانها حربا للمستقبل، والتي يتم خوضها بهدف التشتيت، وإثارة الاضطرابات في عملية صناعة القرار لدي الخصوم، عبر اختراق أنظمتهم، واستخدام ونقل معلوماتهم وهنا، تري الدول الكبري أن من يحدد مصير تلك المعركة المستقبلية ليس من يملك القوة فقط، وإنما القادر على شل القوة، والتشويش على المعلومة[2]

[1] William. J. Broad, John Markoff and David E. Sanger, “Israeli Test on Worm Called Crucial in Iran Nuclear Delay”, The New York Times (15 Jan 2011), online e-article, http://www.nytimes.com/16/01/2011/

[2] -E. Nakashima. “U.S. Accelerating Cyber weapon Research”, The Washington Post, online e-article, https://www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/13/03/2012/gIQAMRGVLS_story.html

ان طبيعة الموازين الدولية فيما يتعلق بماهية الدول التي تشكل القوى العظمى قد اختلفت مع تفاقم و اتساع و تنوع المخاطر الامنية السيبرانية فلم تعد المخاطر الامنية محدده بالدول العظمى فقط بل اتسعت المخاطر لتشمل العديد من الفاعلون بين الشركات التخصصية في الامن و الجرائم و القرصنة الالكترونية حتى انها شملت محترفوا القرصنة وشبكاتهم الاجرامية ايضا حيث يعد تجنيدهم لاداء الهجمات الالكترونية دون اثر دال عليهم و بأجور لا تكاد توازي مايخصص من ميزانيات الحروب التقليدية فضلا عن عدم تحمل الدول المستأجرة لاعباء التقنيات المستعملة في الحروب السيبرانية اصبح الاسهل و الافضل كونها لا تعد شريك واضح المعالم في ما تتسبب به تلك الجروب السيبرانية من دمار و اثار تخريبية .و من جانب اخر فقد عززت تلك الجرائم و الحروب السيبرانية من اهمية و تنافسية الشركات التخصصية بكل ما يتعلق بالامن الالكتروني مما ادى الى رفع نسب تخصيصات ميزانيات الدول بكل ما من شئنه تأمين البنى التحتية السيبرانية فضلا عن اتساع و تفاقم التسلح و عسكرة الفضاءات الالكترونية الدولية لتطوير القدرات الهجومية و الحماية في الان ذاته درءاً لمخاطر الحروب السيبرانية المستقبلية .

عمل الفضاء الإلكتروني على إعادة تشكيل قدرة الأطراف المؤثرة، مثل الولايات المتحدة. فبعدما كانت الأخيرة تملك ما يشبه الاحتكار لمصادر القوة، بعد انتهاء الحرب الباردة، برزت عملية انتشار القوة بين أطراف متعددة، سواء أكانت دولا، أم من غير الدول[1]

ان كارثية سلبيات الفضاء السيبراني تتفاقم بشدة و سرعة كبرى لا رادع دولي موحد جاد لارتفاع نسب الجرائم الالكترونية كما تظهر في الاحصاءات التالية فضلا عن تذبذب قواعد اللعبة الدولية فيما يتعلق بنسب العسكرة للفضاء الرقمي السيبراني والتي هي نتاج تداخلات المصالح السياسية و الاقتصادية و الامنية حيث تتصاعد المشاركات الخفية للعديد من الدول في الحروب السيبرانية التي لم تعد تتحدد بالدول العظمى فقط مثل امريكا و روسيا و الصين حيث شجعت الطبيعة الخفية للمتسببين بتلك الحروب السيبرانية و كوارثها لدخول العديد من الدول في ساحة النزاعات السيبرانية و فضاءاتها و عسكرتها مثل تركيا و فرنسا و العديد من الدول التي عمدت الى الدخول في سباقات التطور الالكتروني و بالتالي في الحروب السيبرانية .

18سبتمبر 2020 :قام قراصنة صينيين بسرقة بيانات من مختبرات إسبانية تسعى لتطوير لقاح ضد كوفيد-19 1.سبتمبر 2020 : نشرقراصنة فيروس يدعى "ريتادوب" وتم تثبيته على "خادم" (سيرفر) فرنسي، وقاموا بمحاولة اختراق(850) ألف جهاز حاسوب حول العالم 29.يوليو 2020 :نفذ قراصنة صينيين عدة هجمات إلكترونية على شبكات الكمبيوتر بالفاتيكان 17.يوليو 2020: شنت مجموعة" APT29" هجمات إلكترونية على مؤسسات تشارك في تطوير لقاح مضاد لكوفيد19 في كندا والولايات المتحدة والمملكة المتحدة،.وأكد

[1] Joseph S. Nye. The Future of Power (New York: Public Affairs, 2011).

مركز الأمن الإلكتروني الوطني البريطاني أن هذا لصالح جهاز المخابرات الروسي. وفقاً لـ 3."BBC" مايو 2020:تعرضت مجموعة من المستشفيات الأميركية ومختبرات البحث ومزودي الخدمات الطبية وشركات الأدوية لهجمات إلكترونية ومحاولات اختراق من قبل قراصنة إلكترونيين ويعتقد أن الصين وراء ذلك 21. فبراير 2020 :اتهمت جورجيا روسيا بقيامها بهجمات سيبرانية " بهدف "زرع الانقسام وزعزعة الأمن وتقويض المؤسسات الديمقراطية". وفقاً لـ "سكاي نيوز 21"فبراير 2020 :تعرضت أستراليا لهجوم إلكتروني اخترق الأحزاب الرئيسية والبرلمان، من قبل أن قراصنة يقيمون في إيران ويعملون في جهة تتعاون مع الحرس الثوري 5.يناير 2020 : تعرضت وزارة الخارجية النمساوية لهجوم إلكتروني يُشتبه تنفيذه من بلد آخر 4.يناير 2020 : تعرض المئات من السياسيين الألمان، لعملية تسريب واسعة لمعلومات خاصة، ويعتقد أن مجموعة "تورلا"أو"أوروبوروس"، المرتبطة بالاستخبارات الروسية متورطة بذلك. وفقاً لـ "العرب اللندنية 17" أكتوبر 2019 : شنت واشنطن هجوما إلكترونيا ضد طهران استهدفت قواعد بيانات إيرانية ومراكز تحكم،[1]

المطلب الثالث :الاستراتيجيات الإصلاحية الأمنية السيبرانية المجتمعية

تعددت المخاطر العسكرية وغير العسكرية التي تهدد الامن القومي وتمثل تحدياً كبيراً وعلى رأسه الحروب والهجمات السيبرانية التي تؤثر على تفاعلات السياسة الدولية [2]

ان الثورة التكنولوجية المستمرة في تطوير و تسهيل كافة جوانب حياتنا اليومية هي ذاتها التي تعمل على تعزيز التطورات الانية في الفضاءات السيبرانية وفق تطور لحظي ادى الى مظاهر مهولة لسباق التسلح السيبراني الدولي حيث ولى عهد الاستثمار في تطوير الجيوش الواقعية وفق تحول جذري الكتروني حيث اصبحت تنافسية الهجمات السيبرانية المعلوماتية بمثابة الحافز الاهم للدول الكبرى في تحدي متواصل لا لتبني استراتيجيات تطويرية في حرب المعلومات السيبرانية فحسب بل بالعمل على تشكيل مؤسسات دولية تخصصية احترافية في التدريبات الامنية السيبرانية و المعلوماتية تضطلع بمهام سباق عسكرة الفضاء السيبراني كونه من اهم مايميز الحروب الالكترونية المستقبلية.

عكف بعض الحكومات أيضا على إقامة مجموعة من القراصنة المدنيين من القطاع الخاص الذين يمكن اللجوء إليهم عند الحاجة، ويمكن أن تكون هذه الجهات الناشطة في مجال القرصنة، أفرادا متخصصين في

---

[1] بسمة فايد "الحروب السيبرانية .. ترسانات رقمية وتهديدات دولية" المركز الأوروبي لدراسات مكافحة الإرهاب والإستخبارات , 2020. المانيا https://www.europarabct.com/

[2] منى الاشقر جبور"الامن السيبراني : التحديات مستلزمات المواجهة(اللقاء السنوي الاول للمختصين في أمن وسلامة الفضاء السيبراني "، بيروت 27-28 أغسطس 2012 صـ 8 . الرابط

https://carjj.org/sites/default/files/wrq_ml_lmrkz_-_d._mn_lshqr.docx

مجال التكنولوجيا أو حتى قراصنة سابقين غير شرعيين تم تعيينهم وتدريبهم لاستخدام مهاراتهم لأغراض الأمن الوطني، وقد تلجأ بعض الدول إلى الاستعانة بوكلاء وقراصنة ومتخصصين من دول أخرى يعملون بالنيابة عنها، وتبين هذه التغيرات كلها التحول عن استراتيجيات رد الفعل إزاء التهديدات السيبرانية وإعادة توجيه نحو تطوير نهج استباقية لحرب المعلومات للعمل بفعالية في ظروف التكنولوجيا العالية[1]

حيث عمدت العديد من الدول في خضم تلك الصراعات و الهجمات السيبرانية الدولية الى توجيه هجماتها السيبرانية من خلال اداء هجومي سيبراني موجه و مدفوع الثمن لتلك الشركات التخصصية الامنية السيبرانية الدولية الاحترافية و المعتمدة في ادائها التنفيذي الهجومي السيبراني الماجور على العديد من الامور الساندة لها في استمرارها مثل محدودية فاعلية القوانين الدولية تجاه الجرائم الالكترونية من جانب فضلا عن العجز عن تحديد المسببات وفق النتائج الكارثية المهولة لتلك الحروب السيبرانية لضعف الاثباتات الاجرامية الملموسة حول تحديد الجهات الفاعلة ومحاسبتها او الحذر منها في خطوات استباقية لذا فهي الحروب الاخطر التي ترتكز الخبرات الاحترافية في الفضاء السيبراني و عسكرته لا على مستوى الدول فحسب بل على مستوى الشركات بل و الافراد ذوي الخبرات الاحترافية السيبرانية المتجددة و المؤثرة في قطاعات الحياة بمجملها و مستقبلها.

ونتيجة الهجمات السيبرانية ظهرت شركات متخصصة في الأمن السيبراني؛ لا تقتصر مهمتها على تأمين الشركات والمؤسسات العامة من أي هجومٍ محتملٍ فحسب، وإنما أيضًا القيام بالهجمات السيبرانية لصالح أفراد ودول ضد دولٍ أخرى. بعض هذه الشركات يقوم بإنشاء وبيع أسلحة إلكترونية، يمكن لأي شخصٍ استخدامها وإحداث ضررٍ إلكتروني. ومن هنا تأتي خطورة الاستحواذ العشوائي لمثل هذه الأسلحة الإلكترونية من قبل أشخاص خطيرين وغير كفؤ، كما هو الحال تمامًا مع الأسلحة التي عهدناها على مدى قرون.[2]

ان طبيعة متطلبات العصر الحالي تستوجب التحول الالكتروني لكافة جوانب الحياة لذا يستوجب التنويه ولو بصورة مبسطة عن طبيعة منافع الحوكمة الالكترونية التي تسعى لتحقيقها الدول العربية لا الخوض في مجال مخاطرها فحسب رغم اتساع ثقل هذا الجانهب في مايترتب من اثاره الا ان الحوكمة الالكترونية في تطبيقاتها للبنى العلوماتية لكافة دوائر و مؤسسات الدولة العامة منها و الخاصة تكون قد حققت العديد من الانجازات و المنافع لا تتوقف عند السرعة في اداء المهام و الانجاز المنظم و التقليل في حجم الانفاق و

[1] حمدون توريه وآخرون "البحث عن السلام السيبراني"، (جنيف: الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء للطبع، جانفي 2011 ص. 80 .81

[2] "كل ما تحتاج معرفته عن الهجمات السيبرانية "2021 (computer-wd.com)

التكاليف و الوقت و الجهد بل يتعداها الى بناء اسس الحوكمة الرشيدة اي بناء و تعزيز جسور الثقة بين المواطنيين والحكومة وفق خطوات ضامنة لتحسين اداء في شفافية تعامل متاحة المعلومات للجميع الكترونيا وتعد بمثابة الضمان الحقيقي للحد من انتشار الفساد و السعي للقضاء عليه بكافة اشكاله وفق ثورة معلوماتيه جذرية اساسها رفع كفاءة الاداء و الابتكار و التطوير المجتمعي .

وما يمكن التركيز عليه في هذا المجال هو أن التهديدات الأمنية تبقى محتملة الظهور نتيجة التقدم الهام الذي أحدثته تكنولوجيا المعلومات، والتي تبين هشاشة الأمن الوطني على المدى الطويل خاصة بالنسبة للدول التي تستورد التكنولوجيا وذلك لاحتمال وقوعها في تبعية أمنية للدول التي تستورد منها، لتتحول بهذه التكنولوجيا المتطورة من وسائط تستخدمها الدول لزيادة التحكم في أمنها إلى وسيلة تقحم الدول في تبعية أمنية من جراء التسابق في اقتناء مضادات الفيروسات الإلكترونية وأنظمة منع التشويش، وهو ما يبرر استمرار قطاع الدفاع في الاستثمار ودعم البحوث العلمية وهذا للاستفادة من كل جهد يتم التوصل إليه دون الاعتماد على جبهة مصدرة، وبذلك يسمح البحث والتطوير في المجال العسكري بالتغلب على المفاهيم التقليدية في حماية الشبكات المعلوماتية والإلكترونية[1]

ان التحول للعالم المعلوماتي الرقمي و تأسيس بنية معلوماتية قومية اصبح ضرورة لكافة انحاء العالم فلا مناص من هذا التحول و السير في ركب التطور التكنولوجي الدولي الا ان تحويل البنية المعلوماتية لمؤسسات الدولة باكملها على اتساعها و شموليتها الى بنية الكترونية وفق ماتقتضيه الحوكمة الالكترونية يستوجب استراتيجية استباقية محكمة منظمة لمواجهة تحديات و مخاطر الامن المعلوماتي اساسها الشراكة التعاونية التوعوية المثمرة في مجال الامن المعلوماتي و فوائده و مخاطره بين كافة دوائر و مؤسسات الدولة و بضمنها القطاع الخاص و منظمات المجتمع المدني لضمان كفاءة الانتقال الالكتروني الايجابي و خصوصية الاهمية المعلوماتية وفقا لمخاطر العصر المعلوماتي التي نشهدها بصورة يومية.

إن تعقيد الأمن السيبراني الحديث يتطلب سرعة التعاون بين مختلف الجهات المعنية، في سبيل مكافحة التهديدات الإلكترونية التي تتعرض لها القطاعات والأفراد وحتى الدول بأكملها. إن العمل الجماعي الدولي هو السبيل الوحيد للوصول إلى النتائج المنشودة لمواجهة مخاطر وتهديدات الأمن السيبراني. وبتعبير آخر، يجب بناء تحالف أمني سيبراني قوي تشارك فيه جميع الدول والمنظمات المتعددة الأطراف. حيث لايزال

[1] رقية العاقل، "دور الثورة المعلوماتية في تطوير الاستراتيجية العسكرية للدول"، المجلة الجزائرية للدراسات السياسية، ع. 8 ، ديسمبر 2017 ، ص. 269.

العنصر البشري يعتبر الحلقة الأضعف في هذا المجال، إذ كشفت الأبحاث أن 88% من الانتهاكات الأمنية تحدث نتيجة الأخطاء البشرية[1]

ان مفهوم السيادة الوطنية و امن الدولة قد ارتبط لعهود طويلة بالصيغ التقليدية سواء على المستوى المكاني و الحدود الجغرافية والزماني بكافة مداخلاته و حدوده والتمكن من خلال ذلك من السيطرة المطلقة للدولة امنيا و معلوماتيا و عسكريا .الا ان هيمنة الثورة التكنولوجية وعصر المعلوماتية اضعف و غير معايير السيادة و مفاهيمها من خلال خلق الفضاءات الالكترونية السيبرانية في ظل التحول نحو الحوكمة الالكترونية و الاندماج بالشبكات العالمية المعلوماتية وبين ظاهر تطويري للمجتمعات الى باطن خفي يمتاز بأضعاف السيادة الوطنية و استبدالها بالسيادة السيبرانية يكون الامن السيبراني ضرورة حتمية يجب ان تتقنه كافة مرافق الدولة و تسعى لاستحقاق سيادتها السيبرانيه خاصة فيما يتعلق بدولنا العربية حيث التطوير لا يتوقف عند حدود الاجهزة و مستخدميها بل الابتكار و الابداع و اعتماد خصوصية فضاءات عربية سيبرانيه يكون فيه ضمان لامن و مستقبل المجتمعات .

وفي ظل هذا السباق السيبراني الدولي المفتوح، وفي إطار التحول الرقمي المتزايد في دولة الإمارات، وما واكبه من تنامي التهديدات الإلكترونية، بصورها وأشكالها العديدة والمتنوعة، على الدولة والمجتمع وبنيتهما التحتية الحيوية، اتخذت الحكومة الإماراتية العديد من الإجراءات والتدابير والمبادرات لتعزيز أمنها السيبراني وتأمين فضائها الإلكتروني. ومن أهم هذه الجهود تنفيذ شبكة إلكترونية اتحادية (FedNet) تسمح بالتوصيل البيني، وتبادل البيانات بين جميع الجهات المحلية والاتحادية في الدولة، وتعزز قنوات التواصل فيما بينها باستخدام بنية تكنولوجية موحدة وآمنة. كما أسست مركز الاستجابة الوطني لطوارئ الحاسب الآلي (aeCERT)، الذي يهدف إلى تحسين معايير أمن المعلومات وممارساته، وحماية البنى التحتية لقطاع الاتصالات وتقنية المعلومات من مخاطر شبكة الإنترنت واختراقاتها. واتخذت مبادرات عدة في السلامة الإلكترونية، مثل مبادرة سالم التوعوية، وسفراء الإمارات للأمن الإلكتروني، ومبادرة الابتزاز الإلكتروني، ومبادرة سايبر سي 3 (Cyber C3)، وشهادة المواطنة الرقمية، ومبادرة "النبض السيبراني" Cyber Pulse. وتأتي المبادرة الأخيرة لمراكمة الجهود التي باشرتها دولة الإمارات في مجال السلامة السيبرانية، وتهدف إلى ضمان تحولٍ رقمي آمن، يمكن جميع الأفراد والقطاعات من استخدام منجزات التكنولوجيا الرقمية في بيئةٍ أقل تهديدًا، ورفع مستوى الوعي بالممارسات الجيدة للأمن السيبراني وتحفيز الاهتمام العام بالتعرف

[1] ألويسيوس تشيانغ، "الإمارات تركز على الأمن السيبراني للوفاء بمتطلبات العصر الرقمي"، جريدة البيان، 19 أكتوبر 2022، https://bit.ly/3Qjn9MI

على الأمان والأمن السيبراني عبر مختلف الفئات العمرية في دولة الإمارات. وقد قام مجلس الأمن السيبراني بسلسلة متواصلة من البرامج التدريبية لقطاعات الدولة المختلفة ولشرائح المجتمع المتباينة لتعزيز ثقافة المسؤولية المجتمعية من خلال تأمين الفضاء الإلكتروني للدولة؛ لكي ينمو ويترسخ مفهوم الولاء الوطني السيبراني[1]

تعد التجربة الاماراتية و السعودية ايضا من التجارب الرائدة في غمار العالم السيبراني بمثابة المثال الذي يحتذى به فيما يتعلق باطار التحول الرقمي الذي تنتهجه الدول العربية في جوانب الحياة المختلفة فلم تتوقف عند حدود التحول الرقمي التام في حوكمة الكترونية نموذجية بل كان السعي وفق استراتيجيات اساسها اعتماد رقمنة الحياة العلمة بكافة مدخلاتها من خلال تعزيز الكفاءات التقنية لمختلف قطاعات الدولة العامة و الخاصة في ظل بيئة ذكية تعتمد تحول رقمي امن حيث الخطوات الستراتيجية البناءة في فهم التكنولوجيا و الشبكات المستقبلية لا للمتخصصين فحسب بل باعتمادها كثقافة حياة و مجتمع و تعزيز التعاون العالمي لاسناد ديمومتها و تطويرها الدائم وفق معايير قانونية داعمة للحد و مكافحة الجرائم السيبرانية و ضمان البيئة الالكترونية الامنة المتاحة للجميع.ان استعانت المجتمعات العربية في تعاون مثمر لتكرار نجاحات التحول الرقمي لبناء بيئة الكترونية عربية موحدة و اثرائها بقوى اسناد قانونية موحدة داعمة لحماية الامن السيبراني و استمرار التطوير التكنولوجي بعناصر شبابنا العربي المبدع يعتبر من اهم الخطوات لرفد مجتمعاتنا بالهوية الرقمية العربية الموحدة و تطويرها وفق الاسس العالمية لضمان الامن الانساني و السيبراني .

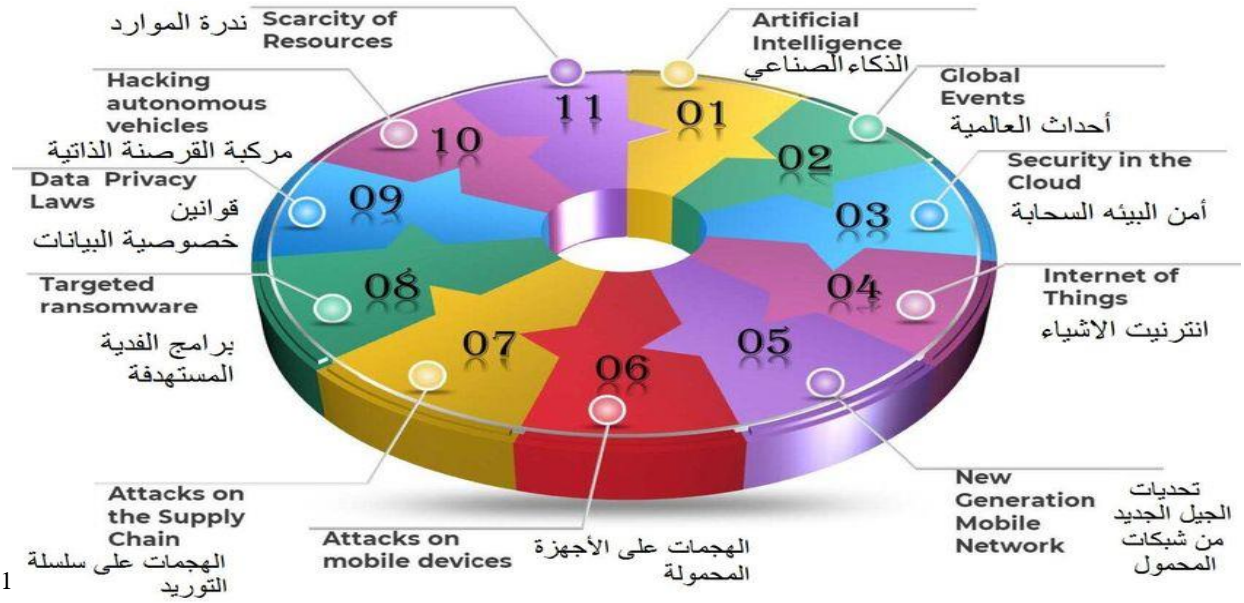
يهدف الردع إلى خلق مجموعة من المحفزات المانعة لقيام أحد أطراف الصراع من القيام باعتداء أو هجوم مستقبلا، وإذا كان ذلك هو هدف الردع في التفاعلات الدولية على أرض الواقع، فإنه مختلف جزئيا عن حالة الردع الإلكتروني، لأن أحد الفواعل غير قادر على إزالة تدمير الطرف الآخر كليا كما في حالة الردع النووي مثلا، كما أنه ليس من السهل تحقيق الردع الإلكتروني بسبب خاصية التخفي، والتي تمنع مستخدم القوة الإلكترونية من التعرف على خصمه أو التوقع من أين سوف تأتيه الضربة، وفي ظل نظام دولي يتميز بتعدد القطبية ما يزيد من حالات الصراع، فضلا عن تعدد الفاعلين من الدول وغير الدول الذين

[1] محمد الكويتي، الاتجاهات المتباينة للأمن السيبراني: مبادرة النبض السيبراني.. دراسة حالة، أوراق محاضرات (3)، أبوظبي: مركز ترينداز للبحوث والاستشارات، سبتمبر 2022؛ محمد مسعود الأحبابي، "نبض الأمن السيبراني"، جريدة الوطن، 5 سبتمبر 2022؛ عماد العلي وأحمد النعيمي، "مجلس الأمن السيبراني يستعرض أحدث الابتكارات والمشاريع الرقمية خلال جيتكس 2022،" وكالة أنباء وام، 9 أكتوبر 2022، https://bit.ly/3jZZCo1

يستخدمون فضاء القوة السيبرانية في التفاعلات الدولية، بالإضافة إلى خاصية التخفي فإن احتمالات الصراع الدولي تزداد مع التقدم التقني[1]

ان العمل على تأمين البنى التحتية الالكترونية لم يعد مبتغى الدول الكبرى فقد اتسعت استراتيجيات الامن القومي الدولي لتشمل ثلاث توجهات اساسية تبدا بالحفاظ على تمكنها من القوة السيبرانية واسنادها بالتطوير الدائم لتنتهي بخطوات دفاعية رادعه استباقية لاشكال الهجوم السيبراني بعد تفاقم مخاطر التهديدات الناتجه عنه والتي شملت اعداد خطط لمواجهة الطوارئ التي تعتمد من الوحدات المستحدثة المتخصصة في تطوير قدرات الامن السيبراني و تحصين امن البنى التحتية قانونيا و من خلال التعاون وفقا للجهود الدولية المتواصلة لسن القوانين المشتركة الرادعه للمتسببين بالهجمات الالكترونية يكون تأسيس رادع للحد من الصراعات و النزاعات و حروب الفضاءات السيبرانية واحتواء بلورتها لحروب شاملة العالم برمته وفق اتفاقات تعتمد نظام اداء استراتيجيات متماثلة في الفضاءات السيبرانية . وفقا لرأي الأساتذة المختصين بموضوع الأمن السيبراني فأن اهم مواضيع وتحديات الامن السبراني خلال العام 2023 ستكون كما موضح في الشكل ادناه حيث تشعبت و تعددت التحديات و بالتالي تعددت الجهات التي يجب ان تعمل على الحد من تأثيرات الحروب السيبرانية القادمة و بين جهود دولية الى محلية فردية منها و حكومية يجب ان يكون واجبا حتميا على الجميع ادراك كنه المخاطر السيبرانية المقبلة و تحدياتها و تداركها قانونيا و معرفيا و خبرات و بنى تحتية الكترونية متينة داعمة لتنفيذ كل ذلك .

[1] إيهاب خليفة،" القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الأنترنت، القاهرة العربي للنشر والتوزيع 2017، ص. 100



[1]

الاستنتاجات و الخاتمة

ان اعتماد الهجمات السيبرانية في ادارة الحروب المستقبلية ناتج عن ثلاثة عوامل اساسية فبين تنوع الاثار المدمرة و مداها العابر للحدود الى صعوبة شديدة او قد تصل الى انعدام معرفة الجهه الممولة و المتسببة بهذه الهجمات الشاملة لنزاعات دولية منظمة الاهداف فضلا عن رخص التكلفة التنفيذية لتلك الهجمات في الغالب و المحدودية القانونية الدولية لمحاسبة وردع المتسببين

ان التحول الرقمي اصبح ضرورة لبناء مجتمعات متطورة و لعل من اهم التحديات التي تواجه ذلك التحول تتمثل في ضعف البنى التحتية الالكترونية و قلة الخبرات خاصة فيما يتعلق بلامن السيبراني لحماية المعلومات وضعف الوعي المجتمعي.

تعد من اهم التحديات التي تواجه سعي الحكومات للحد من تهديدات الحروب الالكترونية صعوبة فرض الرقابة على وسائل التواصل الاجتماعي و تحديد توجهات الافراد الالكترونية فبين الحرية المطلقة و التحديدات الملزمة يكون حفاظ الحكومات على امنها و امن مواطنيها من المهمات التي تزداد صعوبة خاصة مع سباق التطور السيبراني.

ان من الضروري التنوير على ايجابيات التحديثات الرقمية التي تسهم في تطوير الجانب الاقتصادي المسؤولة عن تحسين الكفاءات الانتاجية للقطاع العام و الخاص ورفع ايرادات الدولة و جودة خدماتها

[1] https://www.facebook.com/photo.php?fbid=623452483132456&set=pb.100064031290172.-2207520000.&type=3&locale=de_DE

المنظمة و المسهلة لحياة المواطنين سواء على مستوى الصحة او التعليم او الخدمات الالكترونية بمختلف اشكالها و تطبيقاتها.

ان التغيير الجذري لمفهوم الحروب لم يتوقف عند طبيعة الاستراتيجيات والتخصيصات المالية و التسلح والحدود المكانية بل استبدل بانماط حروب جديدة اقليميا و دوليا

ان تغيير القوى اللاعبة دوليا وفق ماتاحته الفضاءات الالكترونية ويسرته بتوحيد الجهات المهمشة سياسيا في هياكل تنظيمية وفق انتماءات عرقية و دينية لخلق الشبكات المعارضة او المؤيدة لا على مستوى الصراعات الداخلية فحسب بل خلق بيئات ذات تأثيرات دولية و اسعة لتسهيل فاعلية التجنيد و التمويل .

لقد اضحت طبيعة الصراعات السيبرانية متنوعة و مختلفة وفق الاهداف المعدة لها فالدوافع السياسية المحركة للهجمات السيبرانية تأخذ في تطبيقاتها النهج العسكري في توجهات تدميرية للبنى و الشبكات التحتية المعلوماتية للعمل على تحجيم فاعلية النظام السياسي و الاخلال بسيادة الدولة حيث الفاعلين اما محليين او خارجيين بتوجيه و تمويل سياسي الاهداف .

ان تكلفة الحروب السيبرانية النفسية الاعلامية اقل مادية حيث تسخير وسائل الاعلام و التواصل الاجتماعي ويكون العامل النفسي الدعائي هو المرتكز المضعف لسيطرة سيادة الدولة و انظمتها و الموجه للمواطنين وفق التوجهات المدفوعة الثمن حيث الصراع السيبراني ذا الطبيعة الناعمة الطروحات و الادوات لكنها مماثلة لدس السم في العسل في اثارها و ما تتسبب به من صراعات لا حدودو لها

ان التقدم التكنولوجي و عسكرة الفضاءات الالكترونية اضحى ذا طبيعة تنافسية تصاعدية النهج في سباق سيبراني يعتمد السرقات المعلوماتية و التجسس و اختراق الامن القومي وفق الاساليب التقنية الاخذة بالتطور حيث ميزان القوى الدولي تخلخل نتاج الشركات الالكترونية العملاقة المتخصصة في التجسس و السرقات و التدمير الالكتروني في احترافية مأجورة دون الاحتياج الى وسائل التدمير و التفجير التقليدية التي الغيت من مفردات قواميس الحروب حيث تزايد عدد الدول الفاعلة الخفية في تلك الحروب بالتكلفة المالية لانجاز الهجمات السيبرانية المدمرة.

ان الصعوبات التي تحد من امكانات رجال القانون و صانعي السياسات في سعيهم لطرح المعالجات الفاعلة المثمرة للجرائم الالكترونية و الصراعات الامنية السيبرانية مستمرة تصاعديا كونها نابعة من الطبيعة المعقدة للمكونات التقنية الالكترونية و المتسمة بسرعة و استمرارية التطور اللحظي حيث لا حدود لتطوير العقل البشري.

ان بيئة الفضاءات الالكترونية لا تسمح بالتمييز بين طبيعة الاستخدام السياسي او العسكري او الاجرامي او الاستخباراتي فهي بيئة ذات طبيعة متاحة للجميع وفقا للقدرات الاحترافية و الامنية للدول و الشركات و الجماعات و حتى الافراد لرخص تكلفة الاتصال و التوظيف وفقا للاهداف سياسية او عسكرية او اقتصادية

او اجتماعية حيث يعد تحجيم عاملي الرقابة و التعرف على المتسبب ذا قوة جاذبة لصعوبتهما ومناعتهما وفق لخبرات المستخدمين و قراصنة الانترنت المحترفون .

ان اداء الاجهزة الامنية بشفافية بمعزل عن التداخلات السياسية اصبح ضرورة كي تتحقق تلك المصداقية في تنفيذ مهني قانوني ولمنع فشل اداء الاجهزة الامنية

ان الضرورات الاصلاحية تستوجب الاصلاح للنظام السياسي كي يتم اصلاح القطاع الامني و ضرورة توحيده للحد من التنافسية التعددية للاجهزة الامنية فضلا عن وضع اليات تنفيذية فعالة لتامين فاعلية الرقابة على القطاعات التشريعية و المدنية و القضائية.

ان التعاون في مجال تبادل الخبرات و المعلومات التكاملية في مجال الفضاء الالكتروني للحد من الاثار الارهابية الالكترونية المدمرة لاستقرار المجتمعات اصبح ضرورة حتمية لدعم مسارات و مساعي الدول للحفاظ على امنها و استقرارها في ظل عصر الحوكمة الالكترونية .

العمل على تنظيم حملات مكثفة بمختلف الوسائل خاصة وسائل التواصل الاجتماعي تستهدف التثقيف و التوعية و الوقاية بكل مايتعلق بمخاطر الامن السيبراني بشكل دوري تنسيقي يستهدف كافة طلبقات المجتمع تكون داعم في تعزيز و نشر ثقافة الامن السيبراني الانساني المنحى خاصة فيما يتعلق بالتحول نحو نظام المواطنة الرقمية التي تجتاح دولنا العربية

العمل على بناء مجتمع امن سيبرانياً اي اعتماد الاستفادة من التوظيف والتطوير التكنولوجي لمختلف مجالات الحياة من خلال بناء شراكات ذات مسؤولية مجتمعية تنظيمية بين مؤسسات الدولة بأكملها في تعاون مثمر مع المؤسسات الامنية التخصصية في مجال الامن السيبراني لتأمين استفادتهم التطويرية وفق اسس الدفاع و الردع الاستباقي لمخاطر الامن المعلوماتي .

ضرورة العمل على ادراج مفردات الامن السسيبراني في المناهج الدراسية منذ المراحل الدراسية الاولى و تطوير طروحاتها التعليمية بصورة تدريجية وفق المراحل الدراسية وبما يتناسب و مستوى الادراك و الاتقان و التدرب لكل مايتعلق بخصوصية الامن السيبراني و مخاطره و الاستغلال الارهابي التكنولوجي الذي يعمل عليه المجرمين الالكترونيين وايضاح مدى خطورة ونتائج تلك التوجهات الارهابية على امن الفرد و المجتمع كي يكونوا بمثابة الناقل الامين لكافة تلك التوجهات الامنية لافراد اسرهم و توعيتهم اي يجعلون من انفسهم الشعلة المنيرة لامان اسرهم.

ان شيوع الاستخدام الالكتروني في مجتمعاتنا العربية لمختلف الفئات المجتمعية اصبح واقعا لا مناص منه خاصة فيما يتعلق بأدمان الالعاب الالكترونية و مواقع التواصل الاجتماعي و الذان يعتبران ثغره مدمرة لبناء المجتمع الانساني و امنه مما استوجب استغلال تلك المواقع لبث كل ما من شئنه توعية افراد المجتمع من

خلال التوجيه الاعلامي التثقيفي لتأهيل الافراد و توجيههم بمخاطره و الاستغلال و التدمير الذي ممكن ان يكون واقعهم المستقبلي.

ان الحلول الفردية في مجال الامن المعلوماتي ذات اثار محددة الفاعلية لذا فان عقد اتفاقات وفق بروتوكولات موثقة دولية مع الجهات الامنية المتخصصة و الدول ذات التجارب الرائدة الناجحة في هذا المجال اصبح ضرورة حتمية خاصة بالنسبة لدولنا العربية حيث كسب الخبرات التخصصية في مجال الامن المعلوماتي من خلال الدورات التدريبية التي توفرها تلك الاتفاقات لنقل الخبرات و تطويرها وتوفير كوادر ذات مهارات سيبرانية مؤهلة قادرة على التعامل مع الهجمات السيبرانية و الحد من مخاطرها .

العمل على اعداد برامج و انشطة و تطبيقات و منصات الكترونية ذات خدمات مجانية مدروسة تتسم بالدقة و السلاسه و الترغيب في طروحاتها فضلا عن دورات تدريبية تخصصية تطويرية جاذبة لتطوير اكبر عدد ممكن من افراد المجتمع في خطوات استراتيجية مراقبة لانتقاء الكوادر المتميزة الابداعية الابتكارية في مجال الامن السيبراني كي تكون نواة تأسيس و بناء مشروع توعوي متكامل تخصصي في مجال الامن السيبراني و استحداث لمراكز تخصصية تأهيلية تعمل على الحفاظ على امن الدولة و استقرار سيادتها.

ان اثار الهجمات السيبرانية و تفاقم التسابق التسلحي في عسكرة الفضاءات الالكترونية استوجب بالمقابل التكاتف الدولي في خطوات فاعله للحفاظ على الامن و الاقتصاد الدولي و امن المواطن و سلامة مستقبله من خلال السعي لاستحداث جهات دولية محوكمة ذات خبرات احترافية في مجلات الامن السيبراني و حقوق الانسان تعمل على وضع اسس قانونية منظمة وفق قواعد عالمية المنحى شاملة رادعه يكون الالتزام الدولي موجب لتجريم و ردع كافة الجهات الفاعلة و المتسببة بالهجمات السيبرانية و السعي للحد من مخاطرها .

العمل على توفير الحماية المطلوبة للبنية التحتية الالكترونية خاصة فيما يتعلق بمنظومة المعلومات الامنية و المالية الحكومية من خلال تطوير الاستراتيجيات الامنية الالكترونية الوطنية و الكادر التقني المسؤول عن ادامتها و متانة البنى التحتية المعلوماتية و شبكاتها وفق برامج حماية دائمة التطوير وصيانة و ادامة و مراقبة مستمرة لضمان سلامة و امن التحول الرقمي لمجتمعاتنا العربية .

ان انتهاء زمن الحرب الباردة بين اقطاب القوى الدولية واستعراضات تنافسية ترسانات التسلح التقليدية منها و اسلحة الدمار الشامل و النووي لايعني عودة السلام العالمي واستتاب الامن الدولي وتوقف السباق التسلحي فكل ملامح الصراعات و الحروب لاتزال قائمة لكن مااختلف جذريا هو طبيعة تلك الحروب والصراعات وفق مقتضيات الحروب السيبرانية الصامته في ادواتها و المدمرة في اثارها النابعة من مخرجات التطورات التكنولوجية حيث الجيل الخامس و الذكاء الاصطناعي وجهان لعملة و احدة حيث التغيير الشامل في ديناميكة الصراع و الانجازات حتى اضحى مقياس القوة يعتمد على مدى السيطرة في مجال الفضاءات الالكترونية و الاحترافية المتمكنة من كافة مدخلاتها في خضم كم هائل من المخاطر و التهديدات الرقمية

السيبرانية ذات التطورات اللحظية .ان غزو الثورة التكنولوجية بكافة تقنياتها الالكترونية لكافة منافذ الحياة الانسانية احدث انقلاب تام على كافة الاصعدة و خاصة فيما يتعلق بخصوصية الامن المجتمعي واستقرار و سيادة الدول فقد ادى التحول نحو العالم الرقمي بكافة مميزاته و سماته التطويرية للحياة البشرية الى ظهور تحديات تتناسب في مخاطرها مع الطبيعة التطويرية اللحظية المنحى حيث فرض الفضاء السيبراني تحديات و مفاهيم جديدة للقوة و للحروب و للتهديدات و المخاطر التي تهدد سلامة الفرد و امن و سيادة الدولة و الذي استوجب في المقابل سعي الدول لخلق استراتيجيات تأهيلية لتحقيق امنها و استقرارها الوطني السيبراني للحد من المخاطر و التهديدات الحالية وفق تفاقم مخاطر الهجمات السيبرانية فضلا عن العمل على نشر و تحديث ثقافات الامن السيبراني كي تكون مسار حياة للمجتمع ككل لدرء و ردع المخاطر و الحروب السيبرانية المستقبلية من خلال التعاون و التفاعل المثمر بين جميع افراد المجتمع و المسند بتبادل الخبرات الدولية و الجهود الاستثنائية لرفد الامن السيبراني بسن القوانين الدولية الرادعه و المحدده لمخاطر الحروب الالكترونية المستقبلية.

Conclusion:

This study concerned with the importance of the cyber security and the challenges of espionage and electronic penetration of countries through cyberspace. It aims to focus on clarifying the various cyber challenges and risks that have become one of the most important dilemmas facing the security stability of countries، which requires giving the same importance to adopting electronic deterrent defense means to achieve national cyber security in light of international cyber challenges. Countries must seek to create rehabilitation strategies to achieve their security and national cyber stability to reduce the current risks and threats according to the exacerbation of the risks of cyber attacks، as well as the dissemination and modernization of cybersecurity cultures in order to be a life path for society as a whole to ward off and deter future cyber risks and wars through cooperation and fruitful interaction between all members of society and supported by the exchange of international experiences to supplement cybersecurity by enacting international laws that deter and determine the risks of future cyber wars.

In the conclusion، this study demonstrating the country who possesses a cyber-power depending advanced technology will be eligible to constitute an influential force in cyberspace and achieve cybersecurity that supports national sovereignty and state security.

قائمة المصادر :

البحوث

1. إحسان محمد الحسن، علم اجتماع السياسي، دار وائل، الأردن، 2009، ط3 ، ط25
2. إيهاب خليفة، القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الأنترنت، القاهرة العربي للنشر والتوزيع 2017، ص. 100
3. القاموس المحيط للفيروزابادى ج4 ص 194 ، الهيئة المصرية العامة للكتاب عام 1400هـ-، مختار الصحاح للرازى ص26 ،عنى بترتيبه : السيد محمود خاطر ، دار التراث العربى للطباعة والنشر بمصر1980.
4. التعريفات للجرجانى ص55 ، تحقيق / إبراهيم الإبيارى ، دار الريان للتراث بمصر 1982.
5. ألويسيوس تشيانغ، الإمارات تركز على الأمن السيبراني للوفاء بمتطلبات العصر الرقمي، جريدة البيان، 19 أكتوبر 2022، https://bit.ly/3Qjn9MI
6.حمدون توريه وآخرون البحث عن السلام السيبراني، (جنيف: الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء للطبع، جانفي 2011 ص. 80 .81
7.جميلة علاق،خيرة ويفي ،مفهوم الأمن بين الطرح التقليدي والطروحات النقدية الجديدة.في الملتقى الدولي: الجزائر والأمن في المتوسط:واقع وآفاق، جامعة قسنطينة ، 29-30 أفريل 2008 ، ص.316
8.رياض هاني العدالة البطيئة وانعكاسها على الأمن الاجتماعي"الحوار المتمدن ع 3722 ،2012
9. رقية العاقل، "دور الثورة المعلوماتية في تطوير الاستراتيجية العسكرية للدول"، المجلة الجزائرية للدراسات السياسية، ع. 8 ،ديسمبر 2017 ، ص. 269.
10. سهيل حوامدة "الأمن الاجتماعى رهن الأمن الاقتصادى من منظور إسلامى " ٢٠١٢ م /٥/ جريدة السبيل ،ع ٢٤
11. سليمان عبدالله الحربي "مفهوم الأمن: مستوياته وصيغه وتهديداته"، دراسة نظرية في المفاهيم والأطر، المجلة العربية للعلوم السياسية، مركز دراسات الوحدة العربية، ع: 19، بيروت. (2008)
.15
12. عادل عبدالصادق،" حروب المستقبل الهجوم الإلكتروني على برنامج إيران النووي"، مجلة السياسة الدولية، مؤسسة الأهرام، أبريل 2011.
13. منى الاشقر جبور"الامن السيبراني : التحديات مستلزمات المواجهة(اللقاء السنوي الاول للمختصين في أمن وسلامة الفضاء السيبراني"، بيروت 27-28 أغسطس 2012 صـ 8 /https://carjj.org/sites/default

شبكة المعلومات الدولية :

1. الاء عيسى "مفهوم الأمن الإنساني"2018 (mawdoo3.com)
2. بسمة فايد "الحروب السيبرانية .. ترسانات رقمية وتهديدات دولية" المركز الأوروبي لدراسات مكافحة الإرهاب والإستخبارات ، 2020. المانيا https://www.europarabct.com /
3. "كل ما تحتاج معرفته عن الهجمات السيبرانية "2021 (computer-wd.com)
4. سمير فرج " الفضاء السيبراني" 2020 مصر https://samir-farag.com/

References

1.Acharya، A. (1995). The periphery as the core: The third world and security studies

2. Ayoob، M.، & Wells، S. (1991). The Security Problematic of the Third World. World Politics، 43(2)، 257-283 Retrieved January 16، 2021.

3.Anupama A، Amritha Saravanan، 7 cybersecurity trends to watch for in 2023، Manage Engine ، 31Oct 2022، https://bit.ly/3WJyeJk

4.Booth،K Theory of world security (Vol. 105). Cambridge University Press، (2007)

5. E.Nakashima."U.S. Accelerating Cyber weapon Research"، The Washington Post، online e-article،https://www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/13/03/2012/gIQAMRGVLS_story.html

6.https://www.facebook.com/photo.php?fbid=623452483132456&set=pb.100064031290172.-2207520000.&type=3&locale=de_DE

7. ICS Cybersecurity Year in Review.2021 Dr.agos ،https://bit.ly/3W8reVn

8. John BAYLIS and Steve SMITH ، Globalization of World Politics، second ed. Oxford university press، New York، 2001. p 255

9. Joseph S. Nye. The Future of Power (New York: Public Affairs، 2011).

10. Karim hussein، Donata Guisciet Et Julia Wanjiru. Sécurité et sécurité humaine. Présentation des concepts et des initiatives quelle conséquences pour l'Afrique de l'ouest ?. Rapport de club du sahel et de l'Afrique de l'ouest. 2004. P 16. www.oecd.org/fr/csao/publications/38826711.pdf 24 - ibid. p 16.

11. William. J. Broad، John Markoff and David E. Sanger، "Israeli Test on Worm Called Crucial in Iran Nuclear Delay"، The New York Times، 2011 online e-article، www.nytimes.com/16/01/2011/world/middleeast/16stuxnet

Al-Bayati, Raji Youssef. "Cyber terrorism (models of international efforts to reduce it)." Tikrit Journal For Political Science 2.28 (2022).