الفضاء الجيوسبراني وتأثيره في الجغرافيا السياسية للدول دراسة تطبيقية على ليبيا

د. جمال سالم النعاس
استاذ مشارك بقسم العلوم السياسية/ كلية الاقتصاد/ جامعة عمر المختار
Jamal.alnaas@omu.edu.ly

الملخص:

شهد المجال السيبراني في المنطقة العربية دوراً كبيراً في إحداث عدد من المتغيرات ذات الطبيعة السياسية والأمنية وبخاصة بعد عام 2011، وهو ما كان له تأثيرات كبرى على المجتمع وعلى علاقته بالدولة، بل بالتأثير المباشر على "الدولة العربية " بإفشالها وانهيار مؤسساتها خاصة في تلك الدول التي تشهد تراجع في الحداثة والتنمية، مثل: حالة اليمن وليبيا، التي لعبت دوراً سياسياً في دول أخرى، مثل: حالة مصر وتونس، والتي تتميز بتطور مرتكزات الدولة والطبيعة المدنية لشعوبها، وبينما جمعت استخدامات "المجال السيبراني " بين الدور السياسي والعسكري في الحالة السورية، وتعرضت المنطقة عبر المجال السيبراني إلى حروب نفسية استهدفت التأثير على الكتلة الحرجة من الشباب عبر الشبكات الاجتماعية سواء من قبل فرقاء على أساس الاختلاف السياسي أو الديني أو المذهبي، ومن جهة أخرى مارست قوى خارجية التدخل " سيبرانياً " للتأثير على الأمن والاستقرار، وتغذية النزاعات الطائفية، لذلك اهتم هذا البحث بدراسة الأمن السيبراني وعلاقته بالجغرافية السياسية، وما موقع ليبيا في الأمن السيبراني؟ وما المخاطر التي تعرضت لها ليبيا؟ وما المخاطر المستقبلية في حال عدم حماية مجالها الجيوسبراني؟ .

الكلمات المفتاحية: الأمن السيبراني، الفضاء الجيوسبراني، الجغرافيا السياسية، الإرهاب السيبراني، الأخطار السيبرانية.

Geospatial dangers to countries A study of cyber security and its impact on the geo-cyber situation in Libya

Dr. Jamal Salem Al Naas
Department of Political Science Faculty of Economics,
Omar Al-Mukhtar University
Jamal.alnaas@omu.edu.ly

Abstracts :

The cyber domain in the Arab region, with its failure and the collapse of government institutions in those countries, is witnessing a state of decline in modernity, while it pretends to play politically in other countries, such as the case of Egypt and Tunisia, as simple as the development of foundations, the civil nature of its people, and a science that collected the uses of the "cyber domain" Between the political and military role in the Syrian case, and the region was exposed through the cyber domain to psychological wars aimed at influencing the critical mass of young people through social networks, whether by parties on the basis of political, religious or sectarian differences, and on the other hand, external forces practiced “cyber” intervention to influence On security and stability, whether by feeding sectarian conflicts, so this study focused on studying cybersecurity and its relationship to geopolitics, what is the position of Libya in cybersecurity, what are the risks to which Libya was exposed, and what are the future risks in the event of not protecting its geo cyber sphere**.**

Keywords*:* (cyber security - geospatial space - political geography - cyber terrorism - cyber threats)

مقدمة:

تدرس الجغرافيا السياسية تنافس القوة والتأثير على الإقليم، وعلى مستويات مختلفة من التحليل، حيث أنها مهتمة بديناميات أي نزاع على الأرض، والمتناقضات واستراتيجيات الجهات الفاعلة من أجل سيطرتها، وتخصيصها والدفاع عن مصالحها داخل الحيز الجغرافي، فهناك الجغرافيا السياسية في الفضاء الإلكتروني ، وهناك نهج دبلوماسي لإدارة الفضاء الإلكتروني، ويتكون الفضاء الإلكتروني من أربع طبقات ، وهناك طبقات مادية وهي شبكه عالمية من الكابلات ومحطة التبديل ومركز تخزين البيانات ، وهناك أيضاً طبقات منطقية وبيانات اجتماعية، وجميع الطبقات الأربع هي سياسية وجيوسياسية (Carlos Exk, 2017, p339).

كانت بداية القرن الحادي والعشرين انتقاله جديدة في الجغرافيا، التي تطورت عبر مراحل زمنية ليست بالقليلة في موجات ثلاث زراعية، وصناعية، وأخيراً تكنولوجية، وفي هذه الموجة الأخيرة تعالى الجدل حول أفول الجغرافيا ونهايتها بعد أن خلق الفضاء الإلكتروني حدوداً كونية ألغت حدود الدول الرسمية، وأصبح الانتقال بين الدول في مجال الاتصالات، والتجارة، والتعاملات المصرفية، وحتى النقود أمراً غير ملموس يجري عبر الفضاء الإلكتروني باستخدام تقنية الأنترنت مما قلص الزمن ووسع المكان، وأن تلك التغييرات التي طرأت على العالم في نهاية القرن العشرين، والتي مثلت حقبة من الصراع اتخذت أشكالاً متعددة انتهت بظهور صراع مفتوح أُلغيت فيه حدود الدولة القومية، وظهر على إثرها نظام دولي جديد (المزروعي، ب ت).

من الواضح أن التقدم العلمي والتكنولوجي قد قصر المسافات وقلص أبعاد العالم ويسر التفوق عليه، فأظهر الجغرافيا بأشكال متجددة، ومن المعروف أن المكان في الجغرافيا يعد منظماً ومتميزاً بآن واحد، وحدوده السياسية وتقسيماته إلى دول ومجموعات بنظام واحد هو الإطار الذي تُمارس فيه السياسة لغرض الحصول على التغييرات المطلوبة، إلا أن الفضاء الإلكتروني ألغى هذا النظام وبات الانتقال الاقتصادي والاجتماعي عابر للحدود القومية (المزروعي، ب ت).

أهمية البحث :

1. التعرف على التطورات الحديثة في مجال دراسات الجغرافيا السياسية .
2. أهمية دراسة الأمن السيبراني لما له من دور في حماية الدولة .
3. مدى استخدام الدول للفضاء السيبراني للتهديد والحرب .
4. الوضع الجيوسبراني لليبيا وخصوصا بعد أحداث 17 فبراير 2011 .

أهداف البحث :

1. توضيح العلاقة بين الجغرافيا السياسية والأمن السيبراني .
2. تحديد المجالات الحديثة للدراسة في الجغرافيا السياسية .
3. توضيح أهمية موقع ليبيا وأهمية تأمين ودعم أمنها السيبراني؛ لحماية فضائها الجيوسبراني .

مشكلة البحث :

بانتشار وتوسع استخدام الأنترنت وتوسع شبكات الأنترنت عالمياً والتوسع الهائل في مواقع التواصل الاجتماعي، وفي ظل ضعف الدول وضعف رقابتها على أمنها السيبراني ، فإن ذلك يؤدي إلى ضعف حماية فضائها الجيوسبراني، وبالتالي يؤدي إلى حدوث العديد من المخاطر على العديد من المستويات الاقتصادية والسياسية والجغرافية والتي تؤدي في النهاية إلى خسارتها للحروب، أو حدوث تفكك داخلي في حال تعددت الأقليات العرقية بها .

منهجية البحث :

سيعتمد هذا البحث على الدراسات التي أنصبت على موضوع الأمن السيبراني، والأمن الجيوسبراني، وسيقسم البحث إلى عدد من المباحث تتناول تعريف السيبرانية، والأمن السيبراني والجغرافيا السياسية ، والوضع الجيوبولتيكي الليبي في العالم في نظريات الجيوبولتيكية العالمية، ثم مبحث حول الفضاء السيبراني الليبي، وأخيراً مبحث يتعلق بدراسة الوضع الجيوسبراني في ليبيا .

الدراسات السابقة :

– دراسة خريسان، (2021)، بعنوان الأمن السيبراني في العراق قراءة في مؤشر الأمن السيبراني العالمي، حيث أهتمت الدراسة بتحديد موقع العراق من حيث أمنها السيبراني،

وموقعها في الترتيب العالمي، وأوضحت أن ترتيب العراق قد حل متأخراً على مستوى العالم حيث كان ترتيبها 129 عالمياً من أصل 184 دولة.

– **دراسة طاله، (2020)**، بعنوان التهديدات والجرائم السيبرانية، تأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها، وأوضحت الدراسة أن الأمن السيبراني سلاحاً استراتيجياً بين الحكومات والأفراد، ولا سيما أن الحرب السيبرانية أصبحت جزاءً لا يتجزأ من التكتيكات الحديثة للحروب، والهجمات بين الدول، ويشمل الأمن السيبراني أمن المعلومات على أجهزة وشبكات الحاسب الآلي .

– **دراسة رفيق، (2018)**، الجيوبولتيكس السيبرانية والاستقرار في الشرق، وقد تناولت الدراسة التطور والصراع الجيوسياسي السبراني بين دول الشرق الأوسط وخصوصاً بين إيران وإسرائيل، الأمر الذي أدى إلى زيادة الاهتمام بالأمن السيبراني لدى دول الخليج العربي بعد تعرضها للعديد من الهجمات الإلكترونية ، وخصوصاً في قطر والأمارات والسعودية .

– **دراسة فرج، (2021)**، بعنوان: دور مواقع التواصل الاجتماعي في نشر وتداول الشائعات لمتعلقة بجائحة كورونا وقد كانت دراسة ميدانية لعينة من مستخدمي مواقع التواصل الاجتماعي بمدينة سرت بليبيا وقد أوضحت الدراسة أن وسائل التواصل الاجتماعي بيئة خصبة لانتشار الشائعات وتداولها بشكل فائق السرعة بفعل خصائص والبث الفوري والتداول الجماعي التي تتمتع بها، فضلاً عن توافر أدوات تزييف الصور وفبركة الفيديوهات، والتي تضفي بدورها حبكة محكمة على محتوى الشائعات تساعد في انتشارها، ولعل أحدث مثال على كيفية توظيف مواقع التواصل الاجتماعي في نشر الشائعات، هو أزمة فيروس كورونا (كوفيد–19)، حيث تم إجراء دراسة ميدانية حول الشائعات المنشورة حول مرض كوفيد –19 لعينة بلغت 186 مبحوث ، وضحت أن نسبة 83.87 % يرون أن مواقع التواصل الاجتماعي تنشر الشائعات المتعلقة بجائحة كورونا وتداولها بين مستخدميها.

المبحث الأول

تعريف السيبرانية ومفهومها

1– تعريف السيبرانية: يستخدم مصطلح (Cyber سايبر أو إلكتروني) لوصف أي شيء تقريباً يستخدم في الشبكات وأجهزة الكمبيوتر لا سيما في مجال أمن الدولة، فضلاً عن

إنشاء ميدان للدراسة والبحث في الصراعات والتهديدات التي ارتبطت بمفهوم الفضاء الإلكتروني، والتي استخدمت فيها الحواسيب ومواقع التواصل الاجتماعي والشبكات الخاصة غير المرتبطة بشبكات الانترنت ، فظهرت مصطلحات حديثة كالحرب الإلكترونية "الإرهاب الإلكتروني" – الهاكر – الجريمة الإلكترونية... الخ، وتتميز هذه الفترة بعدم وجود توافق في أراء الدول حول ماهية الفضاء الإلكتروني وكيفية السيطرة عليه مع غياب قانون يضبط حرية التحرك فيه والاستخدام كبقية المجالات الجغرافية الأخرى .

جاء مصطلح السيبرانية **Cybernetic** مشتقاً من المصطلح الإغريقي **Kyber-netes** ويعني الطيار أو قائد الدفة أو الحاكم، ويفيد الاشتقاق الحديث بأن كلمة سيبرانية تتضمن آليات تعقيب تتيح وظائف القيادة والتحكم في الأنظمة المعلقة (بيتر بي سيل، 2017، ص22)، والسيبرانية مأخوذة من كلمة سيبر وتعني صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات، أو الواقع الافتراضي (بن عبدالرحمن، 2017، ص6) .

بينما يذهب المختصون بالرجوع إلى اللغة العربية فثمة تحدياً يواجهونه في اختيار مصطلح مقارب للسيبرانية، وذلك لعدم شيوع استخدام لكلمة السيبرانية في الأدبيات العربية، إذ تم اعتماد مصطلح القوة الإلكترونية للدلالة على القوة السيبرانية، وتجدر الإشارة إلى أن هذا خطاء شائع غير دقيق علمياً، وذلك لكون الترجمة الحرفية للقوة الإلكترونية هو Electronic Cyber (خليفة، ب.ت، ص 3).

يُعَدُّ **وليام جيبسون William Gibson** أول من استخدم كلمة **Cyber** مقترنة بكلمة **Space** لتظهر في مصطلح الفضاء السيبراني **Cyber Space** في كتابة الكلاسيكي عام 1984 (عبدالصادق، 2009، ص3)، وقد جاء استخدام الفضاء السيبراني كنمط من استخدام القوة عن طريق التأثير على عمل مصادر المعلومات وأنظمة الاتصالات عن طريق الهجوم السيبراني بما يؤدي ذلك إلى إرباك عمل البنية التحتية الحيوية (شلوش، 2018، ص200)، ولقد عرفته الوكالة الفرنسية لأمن أنظمة الأعلام **ANSSI** على أنه فضاء التواصل المشكل من خلال الربط البيئي لمعدات المعالجة الآبية للمعطيات الرقمية (إسماعيل،2007، ص4).

وهناك من يرى فيه واحداً من سبع مجالات إلى جانب الجو والفضاء الخارجي والبحر والبر والفضاء الإلكترومغناطيسي والإنسان وأنه "ساحة الحرب الخامسة"، بعد البر والبحر والجو (محمود، 2013، ص5).

وممَّا سبق تبيَّن – وعلى الرغم من عدم وجود تعريف متفق عليه للفضاء السيبراني–، إلا أن معظم ما تم استعراضه يؤكد أن مفهومه واسع ويشتمل على أنظمة عديدة متصلة شكلياً تمتد من شبكات إدارية شاسعة "الشبكات المنزلية" – شبكات Lan خاصة بالمكاتب، مروراً بالاتصالات بعيدة المسافات التي ترتكز على الفضاء، ووصولاً إلى أنظمة التحكم المعقدة الخاصة بالبنى التحتية، كما أنه يحوي تقنيات مثل "أنظمة تشغيل – بروتكولات اتصال– تطبيقات برامج وغيرها"، وأن هذه التقنيات تستخدم في شبكات وظيفية متعددة مثل الخدمة المصرفية، أو التصنيع وغيرها، إذ نلاحظ أن مفهوم الفضاء السيبراني أتخذ ثلاث اتجاهات هي (مادية، وغير مادية، وحلقة وصل بين المادية وغير المادية، وهي الشبكات المترابطة، ومن هنا فإن الاختلاف في مفهوم الفضاء الإلكتروني في بعض دول العالم في اعتماده على الاتجاهات الثلاث أعلاه يبين (المزروعي، ب ت، ص5) :

1- إنَّ الفضاء السيبراني يعتمد الإنسان بالدرجة الأولى كمكتشف، ومُصنع، ومُدير، ومُستخدم لهذا المجال الحيوي الجديد.

2- كل التعريفات لمفهوم الفضاء السيبراني اتفقت على أنه يشتمل بصورة رئيسة على المعلومات، وعمليات التخزين للمعلومات، والبيانات، تتم عبر أجهزة تعمل على نقل ذلك المحتوى .

3- إنَّ الفضاء السيبراني يشتمل الملموسات كالأجهزة والأسلاك، كما وأنه ظاهري.

4- لم تتم الإشارة إلى الفضاء السيبراني من جانب واحد يشتمل تكنولوجيا المعلومات بصورة رئيسة إلا من جهات قليله جداً.

2– سمات الفضاء السيبراني.

ولعل أهم سمات الفضاء السيبراني هي الآتي (عبدالرحمن، 2017، ص7):

1- مجال عملياتي حيث يعد الميدان الخامس للحروب المدنية.

2- تُعَدُّ البنى التحتية لأنظمة الاتصالات وتقنية المعلومات جزء أساسي من الفضاء السيبراني.

3- الفضاء السيبراني لا يقتصر على شبكة الانترنت فقط؛ وإنما شبكات عالمية وخاصة **GPS /ACARS / SWIFT / PSTN** .

ولما أصبح الفضاء السيبراني ميداناً للحروب الحديثة فإن تركيبة الفواعل فيه تتكون من مستويين وكما يأتي (إسماعيل،2007، ص5) :

1- **الفواعل الدولية:** إذ تعد الدولة فاعل محوري في تسيير الفضاء السيبراني انطلاقاً من إمكانياتها المادية والبنيوية والبشرية والقانونية.

2- **الفواعل من غير الدول:** وهنا يأتي دور الأفراد والجامعات والمنظمات غير الحكومية والشركات الذين أصبح بإمكانهم التحكم في توجهات الدول وفق سياسات معينة.

وتتمثل عملية التأثير والتأثر من وإلى الفضاء السيبراني عبر مسارات القوة واتجاهات سيطرت على المجال العام الدولي حيث أصبح (شلوش، 2018، ص200-201):

- **المسار الأول:** يتعلق بعملية الانتقال للأحداث من أرض الواقع إلى الفضاء السيبراني.

- **المسار الثاني:** يتعلق بانتقال وتحديد الفضاء السيبراني لعناصر تهديد إلى أرض الواقع عن طريق الاستجابة.

- **المسار الثالث:** يتعلق بدور الفضاء السيبراني كوسيلة إعلام يتم استخدامها كنشاط مواز للحوادث على الأرض.

- **المسار الرابع:** يتعلق بما يتم نشره عبر الفضاء السيبراني مثل إطلاق الفيروسات أو القرصنة أو سرقة المعلومات أو التجسس.

مفاهيم الأمن السيبراني.

تعددت مفاهيم الأمن السيبراني وسيتم عرض أهم المفاهيم المرتبطة بالأمن السيبراني:

– الأمن السيبراني: هو مفهوم ظهر بعد الحرب الباردة استجابة للمزيد من الابتكارات التكنولوجية والظروف الجيوسياسية المتغيرة، ثم استخدم لأول مره من قبل علماء الكمبيوتر في أوائل التسعينيات من القرن الماضي للتأكيد على سلسلة من حالات عدم الأمان المرتبطة بأجهزة الكمبيوتر لكنه تجاوز مفهومة التقني لأمن الكمبيوتر عندما حث المؤيدين على أن التهديدات الناشئة عن التقنيات الرقمية يمكن أن يكون لها أثار اجتماعية مدمرة (Lean Hansen, 2009, p1155-1175).

ويعرف الأمن السيبراني بأنه: هو العملية أو قدرة الدولة الناتجة بموجبها حماية أنظمة الاتصالات والمعلومات الواردة إليها، والدفاع عنها ضد الضرر أو الاستخدام غير المصرح به أو التعديل أو الاستغلال، ويُعّرف أيضاً بأنه أمن الشبكات والأنظمة المعلوماتية والبيانات والمعلومات والأجهزة المتصلة بالأنترنت، وعليه فهو المجال الذي يتعلق بإجراءات مقاييس ومعايير الحماية المفروض أتخاذها والالتزام بها لمواجهة التهديدات ومنع التعديات أو للحد من أثارها في أحسن وأسواء الأحوال (علي، 2016).

كما يعرف الأمن السيبراني انطلاقاً من أهدافة بأنه النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار التي تترتب في حالة تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن بحيث لا تتوقف عجلة الإنتاج ولا تتحول الأضرار إلى خسائر دائمة (جبور، 2012، ص3) .

– **الفضاء السيبراني:** هو مجال علمي في بيئة المعلومات الذي يتميز من خلال استخدام الإلكترونيات والطيف الكهرومغناطيسي لإنشاء وتخزين وتعديل وتبادل واستغلال المعلومات عبر شبكات مترابطة باستخدام تقنيات الاتصالات المعلوماتية (عبدالصادق، 2013).

والفضاء السيبراني كبيئة افتراضية عالمية لأنظمة المعلومات العامة والخاصة المترابطة فيما بينها الذي تتم فيه إنشاء أنواع مختلفة من المعلومات وتخزينها ونقلها داخل الفضاء السيبراني، بما في ذلك أنواع معينة من المعلومات التي تهيمن على متطلبات أمن المعلومات بشكل عام، وكذلك القوانين واللوائح الوطنية والدولية المختلفة (Aleksander Klaic, 2015, p86).

– **الفضاء الجيوسبراني:** وهو العلاقة بين الانترنت والجغرافيا والديموغرافيا والاقتصاد والسياسة للدولة وسياستها الخارجية (المشهدي، 2019، ص41) .

– **الاستقرار الجيوسبراني** : قدرة جميع البلدان على الاستفادة من الإنترنت لتحقيق فوائد اقتصادية وسياسية وديموغرافية مع الامتناع عن أنشطة يمكن أن تسبب معاناة ودمار لها (المشهدي، 2019، ص41) .

– **القوة السيبرانية:** وهي القدرة على استخدام الفضاء السيبراني لخلق مزايا والتأثير على الاحداث في البيئات التشغيلية الأخرى، وعبر أدوات القوة وهي مجموعة من الوسائل، والطاقات، والإمكانيات المادية وغير المادية، المنظورة وغير المنظورة التي بحوزة الدولة، وتتمثل

الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الإلكترونية، والبنية التحتية والمعلوماتية، والمهارات البشرية المدربة للتفاعل مع هذه الوسائل، ويستخدمها صانع القرار في فعل مؤثر يحقق مصالح الدولة، وتؤثر في سلوك الوحدات السياسية الأخرى (خليفة، 2017، ص24).

– **الإرهاب السيبراني:** هو الهجوم ذو الدوافع السياسية أو التهديد بالهجوم على أجهزة الكمبيوتر أو الشبكات أو أنظمة المعلومات من أجل تدمير البنية التحتية وترهيب الحكومة أو المواطنين، وإجبارهم على تحقيق أهداف سياسية واجتماعية بعيدة المدى، بمعنى أوسع فإن الإرهاب السيبراني يعني استخدام الإنترنت للتواصل والدعاية والتضليل من قبل المنظمات الإرهابية (المشهدي، 2019، ص242).

– **الاستراتيجية السيبرانية:** تعني تطوير وتوظيف قدرات متكاملة ومتناسقة مع المجالات التشغيلية الأخرى للعمل في الفضاء السيبراني، لدعم تحقيق الأهداف عبر عناصر السلطة الوطنية ويتناول القضايا الرئيسية المرتبطة بالاستراتيجية السيبرانية التحدي المتمثل في ابتكار "ردع مخصص" للتأثير على سلوك الكيانات الرئيسية التي تدعمها التطورات في الفضاء السيبراني (المشهدي، 2019، ص41) .

المبحث الثاني

الأمن السيبراني والجغرافية السياسية

الجغرافيا السياسية هي العلم الذي يصف ويحلل ويعالج العلاقات المكانية التي تتصل بالوحدات السياسية، وإذا كانت الجيوبولتيكيا تعالج الموضوع ذاته في إطار مصلحة الدولة القومية في إطار السياسة الدولية، وإذا كان كلاهما يهتم بالمكان سواء أكان براً أو بحراً أو جواً أو فضاء خارجي، فإن الفضاء السيبراني هو ذلك البعد الخامس إلى سيتناوله الجغرافيون السياسيون والجيوبولتيكيون، والذي سيعتمد كأداة دفاع وهجوم في كل من الأبعاد المادية والغير مادية وحلقة الوصل بينها، وأيضاً هو البعد الذي سيعتمد المكان كهدف أساسي له .

إنَّ المكان مرتبط بالتوجهات السياسية الاستراتيجية بالرغم من اختلاف طبيعة الصراع، فمن أجل الفضاء السيبراني والتكنولوجيا الحديثة تدخل الولايات المتحدة عسكرياً في (البوسنة، وكوسوفو، ويوغسلافيا، والعراق، وأفغانستان، والخليج العربي، والصومال، وتايوان،

وكولومبيا، وبنما)، واستطاعت من خلال تلك الجولات أن تضع لها قواعد عسكرية توظفها بصور أساسية كقواعد مهيمنة تستخدم شبكات الفضاء السيبراني فيها، وبصورة جبرية إذا تم ملاحظة أن تلك الدول في قسم منها تعد دولاً مغلقة قبل احتلالها ، لا تملك تلك الشبكات المعتمدة في الفضاء السيبراني، إلا ما يخص مركز السلطة، ولا يمكن اختراقها أو استهداف السلطة فيها، أو الوصول إلى الرأي العام فيها، إلا من خلال التدخل عسكرياً وفرض السياسة الجديدة وبما يناسب مصالح الدول الكبرى، ومما سمح بهذا التدخل والتغيير هو غطاء الاستقرار الأمني للولايات المتحدة من عدو محتمل خفي (المزروعي، ب ت، ص 6-8).

أصبحت مساحة المعلومات مجالاً جديداً للجغرافيا السياسية وغيرت توازن القوى بين الجغرافيا السياسية للدول وقد أوجد الأنترنت فضاءً عاماً جديداً بالكامل، إذ يتجاوز فضاء المعلومات المساحة الجغرافية المكانية التقليدية ويغير العلاقة المكانية للجغرافيا السياسية، ويؤثر بعمق في الفضاء الجغرافي المكاني التقليدي (WANG Limao, 2016, p3-13).

ولا يشكل فضاء المعلومات نوعاً جديداً من الفضاء الجغرافي السياسي فقط، بل يغير أيضاً توازن القوى بين الهيئات الجيوسياسية الأصلية، مما يجعل القوى المختلفة المشاركة في السياسة الدولية من خلال الشبكة تتمتع بالمساواة النسبية في الوضع، فلم تعد السياسة الدولية منطقة حصرية للحكومة وإنما تشارك الحكومة التقليدية المنظمات غير الحكومية والشركات متعددة الجنسيات باعتبارها الموضوعات السياسية الدولية الرائدة إلى جانب تقدم تكنولوجيا شبكة المعلومات وصعود موجة التحول الديمقراطي سيصبح الأفراد بعد الحكومة والمنظمات غير الحكومية والشركات متعددة الجنسية، وقد أظهرت الشبكة تأثيرات سياسية وعسكرية وثقافية قوية إذ بدأت الحرب الإلكترونية السيبرانية مثل حرب حرية الرأي العام والحرب الثقافية والأيدولوجية وحرب المعلومات والاستخبارات التي حدثت على الأنترنت في عالم المعلومات الجغرافية الجديد مراراً وتكراراً (Michael Sentonas, 2018, p15-16).

مع دخول الرقمية إلى الصناعات المختلفة ، أصبحت الجغرافيا السياسية – وهي استخدام المهارة السياسية والأصول للحصول على نفوذ في الشئون الدولية – بعيدة بشكل كبير عن الإطار الجغرافي الأصلي لها، ويستضيف الفضاء الإلكتروني (السيبراني) – وهو الشبكة العالمية لتكنولوجيا المعلومات المترابطة بما في ذلك الأجهزة والبرمجيات والمعلومات – بعض أهم الأسلحة ونقاط الضعف الجيوسياسية للدول على حد سواء، وبما أنه لا يمكن

التفريق بين التهديدات الإلكترونية والتهديدات الجسدية، فمن المرجح أن تكون الجيوسياسية الإلكترونية في طليعة المنافسة الجيوسياسية في المستقبل، وتشمل الأدوات السيبرانية المستخدمة من أجل تحقيق الأهداف الجيوسياسية مجموعة كبيرة من الأدوات، مثل تلك المتعلقة بالمراقبة والتجسس، والتضليل، أو الهجمات المدمرة، ويمكن تقسيم الهجمات السيبرانية إلى نوعين (رفيق، 2018، ص2):

1. الاختراقات التي تستهدف جمع المعلومات (التجسس الرقمي).
2. الهجمات على الأنظمة الأجنبية لإيقاف شبكات الأعداء أو إتلافها مثل الهيئات الحكومية والأهداف الرمزية والبنية التحتية الحيوية.

إن دراسة مخاطر الحرب الإلكترونية تستلزم أولاً إجراء مقارنة بين الحرب التقليدية والحرب الإلكترونية بناءً على مجموعة من المؤشرات، الجدول (1) .

الجدول (1) مقارنة بين الأسلحة الرقمية والأسلحة التقليدية

البيان	السلاح الرقمي	السلاح التقليدي
خسارة الأرواح	محدودة	علية جداً
المدى بالكيلو متر	يطول أي نقطة وصل إليها الأنترنت حتى الفضاء	محدود، ويعتمد على نوعية السلاح
التأثير في الراي العام	عالٍ	منخفض
الحرب التقنية	عالية	عالية
تكلفة الاقتناء والصيانة	منخفضة	عالية
الاستخدام للتجسس	عالٍ	منخفض
عدد مرات الاستخدام	مرات عديدة مادام السلاح الرقمي تحت سيطرة القيادة	مرة واحدة (إطلاق تفجير)
المهارات البشرية المطلوبة	مهارات ناعمة	مهارات خشنة

المصدر : عباس بدران، الحرب الإلكترونية .. الاشتباك في عالم المعلومات، بيروت، 2010، ص 45.

وانطلاقًا من جملة المؤشرات التي يوضحها الجدول السابق يتجلى اتساع مدى تأثير الحرب الإلكترونية في الرأي العام وانخفاض تكلفتها، وقدرتها على التجسس مقارنة بالحرب التقليدية، مما يجعلها حروباً أكثر خطورة من الحروب التقليدية ومن بين أهم هذه المخاطر :

1. اختراق المخططات العسكرية .
2. إمكانية توقف الأنترنت كليـاً في بلـد معين، وتوقف كافة الأعمال والمعامـلات البنكية

والحكومية.

3. تلاعب أجهزة المخابرات بالأمكنة الجغرافية على خرائط جوجل الإلكترونية للتمويه أو لإيهام العدو بوجود مراكز معينة متخصصه بأعمال عسكرية بينما هي مدنية .
4. اختراق المواقع الحكومية ، مثال نشر إعلان حالة الطواري في وزارة الدفاع مما يثير حالة من الهلع الحرب (الحرب النفسية). (هادي، 2017، ص137) .

ومن أجل ذلك تصاعد إنفاق الدول على الأمن السيبراني من 86 مليار دولارًا عام 2017 إلى 90 ملياراً في 2018، و161 ملياراً في 2019، وينتظر أن يقفز إلى 363 مليار دولارًا بحلول سنة 2025 (أبوالحسن، 2021) .

تعددت وجهات النظر الجغرافية والجيوبولوتيكية، التي تصف الفضاء السيبراني وعلاقته بالجغرافية، ويمكن ملاحظة الرؤى المختلفة لمعظم الباحثين في مجال الجغرافيا والفضاء السيبراني في توضيح مفهوم الفضاء السيبراني .

– يصفه مولر بأنه "مجال جديد مصمم بشكل مميز يختلف عن المجال البري والجوي والبحري والفضاء، وهو من صنع الإنسان ويحدد بالنشاط البشري، كما ويعتمد المعلومات كمجال بشكل جوهري ، ويستخدم لإنشاء وتنظيم ونقل وإعادة استيعاب ونشر البيانات (Martin Dodge,1999, p4) .

– يرى رون ديبيرت من خلال علاقة الفضاء الإلكتروني بالجيوبولتيك "أن الفضاء الإلكتروني هو مجال منفرد مساوي لكل من المجالات الأخرى (البري – البحري – الجوي، والفضاء الخارجي ومرتبط بها) (Eischen, E. T. &. K, 2003, p3).

– إنَّ جغرافيا الفضاء الإلكتروني أكثر تفاعلاً من بيئة البر أو البحر من الجبال والمحيطات، فتاك يصعب نقلها وهي ثابتة، إلا أن الفضاء الإلكتروني يمكن التحكم بأجزائه، وتشغيله، وإيقافه، ونقله بمجرد الضغط على أحد الأزرار، وله حدود لا متناهية، ويخضع لقوانين فيزيائية ويعتمد على قدرات ومعرفة لمنظمات وأشخاص .(John O Loughlin, p7-8)، (الجدول 2) .

الجدول (2) ميزات الفضاء السيبراني مع نطاقات البر والبحر والجو والفضاء

الصفة	البحر	البر	الجو	الفضاء	الفضاء السيبراني
الوسيلة	السفن	المركبات	الطائرات	سفن الفضاء	بروتكولات الأنترنت
الوسط الحركي	الجو والسطح	السطح	الهواء	الفضاء	الموجات الكهرومغناطيسية (البر – البحر – الجو) والأسلاك الفيزيائية
الأسلحة	الصواريخ والقنابل	الصواريخ والقنابل	الصواريخ والقنابل	طاقة مباشرة	الحلول الحسابية " الخوارزميات "
التأثير المرغوب	تدمير– تلوث– منع–تشويش	تدمير– تلوث–منع– تشويش	تدمير– تلوث–منع– تشويش	تدمير – تشويش	تدمير– تلوث–منع–تشويش– خداع وتضليل
السيطرة	ملاح (في قارب أو على أجهزة السيطرة عن بعد)	سائق	طيار (في طائرة أو على أجهزة سيطرة عن بعد)	محطات المهمات الأرضية	ارتباطات شبكة الإنترنت التي تراقب تحركات العدو في الجو – الأرض – الفضاء – وكذلك تحرك المركبات بأنواعها / لوحة الخوارزميات
أقل الاحتمالات للاعتراض	تسلل طبيعي	تسلل طبيعي	تسلل طبيعي	تسلل طبيعي	تسلل برمجيات
لأقل احتمالات الكشف	تسلل (المحيط الواسع)	مناطق تغطية	مناطق تغطية	تسلل طبيعي	شبكات تغطية سرية
القاعدة الأساسية	حاملة الطائرات	مختلف المركبات والمنشآت	الحقل الجوي (المطار)	مدار كبلر	أي بوابة من بوابات الفضاء السيبراني
الخدمات اللوجستية	بطيئة – مستمرة – واضحة – غير متكررة	بطيئة – مستمرة – واضحة – غير متكررة	بطيئة – مستمرة	بطيئة – مستمرة	بطيئة – مستمرة – واضحة – غير متكررة

المصدر:

Paul W. Phister Jr, Cyberspace: The Ultimate, Complex Adaptive System, The International C2 Journal | Vol 4, No 2, Focus & Convergence for Complex Endeavors ,2010-2011,p.3

ومن خلال الجدول (2) يتبيَّن ميزة عمل الفضاء السيبراني مقارنة بالمجالات الجغرافية الأخرى، إذ يلاحظ من الجدول أن الفضاء الإلكتروني بميزاته الفريدة يتداخل في المجالات الجغرافية الأربعة، وانه يعمل على خلق ميزات جديدة للمجالات الأربعة، ومن الملاحظة للجدول يمكن أن يستنتج أن الفضاء السيبراني يتحرك في مجال جغرافي واسع ليخلق مجالات أخرى سيبرانية (اقتصادية – سياسية – اجتماعية .... الخ)، إن سيطرة النطاقات الجغرافية الأربعة تعتمد على شبكات المجال الخامس في التحكم والانتشار وتوزيع المعلومات التي تعد الركيزة الأساسية في الفضاء السيبراني، كما أن احتمالات الخسائر في الفضاء السيبراني تكاد

تكون شبه معدومة مقارنة لاحتمالات الخسائر في المجالات الجغرافية الأربعة الأخرى، لكونها لا يمكن تتبع مصدر التهديد أو موقعة أو التنبؤ بساعة الهجوم (المزروعي، ب ت، ص 9) .

عند مقارنة ميزات الفضاء السيبراني مع نطاقات البحر والجو والفضاء فأنه نجد أن الفضاء السيبراني هو المجال الأخطر من ناحية التقدم التكنولوجي، إذ أنه يعتمد المعرفة والمعلومات، وهي ليست حصراً بدول العالم المتقدم، مما يجعلها تشكل تهديداً مستمراً في إمكانية امتلاكها واستخدامها كسلاح لأي دولة كانت، كما أن الفضاء السيبراني ولارتباطه بالمعرفة فإنه يكون اسرع تطوراً وتجدداً من باقي المجالات الأخرى .

كذلك فإن الفضاء السيبراني مرتبط بجميع مجالات الجغرافية الأخرى، ويستخدم فيها كتكنولوجيا تسهم في جميع مجالات الحياة على اليابس والتسيير والتحكم بجميع القواعد البحرية سواء العسكرية، أو العلمية البحثية، أو التجارية التي تعتمد الأساطيل البحرية من سفن، وغواصات، وحتى مراكب الصيد الصغيرة، أو السياحية، كذا الحال في ارتباطه بجميع الأساطيل الجوية سواء كانت عسكرية، أو مدنية فضلاً عن ارتباطه بتكنولوجيا الفضاء الخارجي من خلال استخدام الشبكات الأرضية أو الأقمار الصناعية أو المركبات الفضائية .

كذلك فأنه يتميز عن باقي المجالات في أنه كوني، فهو لا يتحدد بمكان معين، أنه مرتبط باليابس والبحر والجو والفضاء، أنه مجال عام لا حدود له كامل السيطرة والتحكم بالمجالات الأخرى تكنولوجيا، كذلك يرتبط الفضاء السيبراني مع المجال الجوي والفضاء الخارجي في أنه يعتمد الكادر البشري المتخصص في تحريكه وإدارته وتطبيقه، كذلك فأن الفضاء السيبراني بيئة متاحة للكل والدخول إليه مكفول بتوفر تقانات حديثة لكي يكون للراغب بالدخول ووجود فيها (المزروعي، ب ت، ص 8-11).(الجدول 3)

يرى أخرون أن ارتباط الفضاء السيبراني بالجغرافيا من خلال الحاجة إلى: (تيلور، و فلنت، 2002، ص81) :

1. أرض رخيصة تكون قاعدة لمد الكابلات والأسلاك الخاصة بجميع شبكات الفضاء السيبراني بديلة عن الكابلات التي تعبر المحيط والمكلفة. (الشكل 1)
2. توفر الموارد الطبيعية في موقع يكون وسط لقارات العالم ليوفر بيئة خصبة باعتباره مركز للبيانات الدولية .

3. إنَّ شركات الأنترنت الكبرى مثل (مايكروسوفت – قوقل – ياهو) يتركز نشاط معظمها في أمريكا الشمالية وأوروبا، وبالإمكان استثمار البنى الأساسية لشبكة الأنترنت في البلدان الأفريقية، مثلاً عن طريق توفير وسائل اتصال أفضل مقابل السماح بإنشاء مراكز للبيانات في مجالات النشاط الاقتصادي، كما أنه بالمقابل ستوفر فرص عمل وتدريب مما سيخلق نمو اقتصادي للمعلومات في المنطقة، وهذا يمكن أن يحدث من خلال شركات مستعمرة .

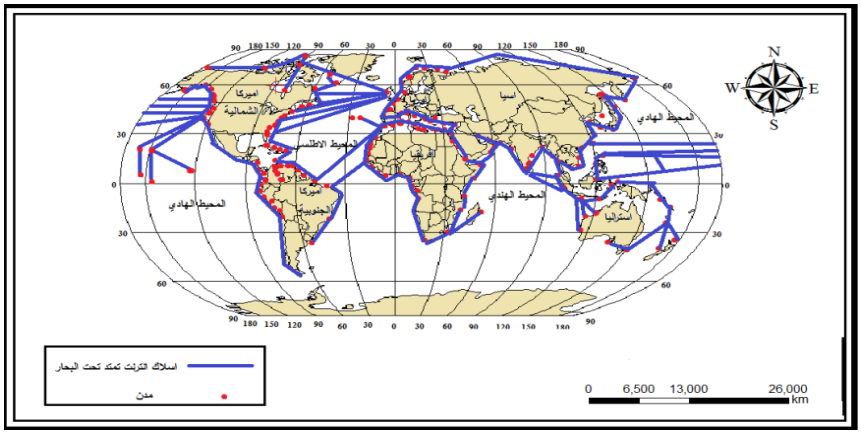
الجدول (3) مقارنة استراتيجية للفضاء السيبراني مع البيئات الجغرافية الأخرى

	اليابس	البحار	الجو	الفضاء	الفضاء السيبراني
التقدم التكنولوجي	السكك الحديدية والاتصالات تتطلب التركيز على منطقة القلب	قوة البخار والحديد أظهرت قوة عالمية جديدة	سحق مراكز الخطورة مباشرة	خلق بيئة أرضية جديدة	استراتيجية جديدة تمكن من لعب دور اللادولة
سرعة ونطاق العمليات	التركيز على خطوط الاتصال والنقل	مكنت من توجيه ضربات نحو حافة منطقة القلب	تنهي الصراع بشكل أسرع	الاستمرار بالعمليات والمشاريع العالمية	سرعة فائقة في العمليات العالمية بقيادة وسيطرة آلية
مميزات سيطرة المجال	ميزة القلب ، سرعة التعبئة الحيوية	مكنت من إزالة الحواجز الجغرافية في مناطق التماس	الضربة الأولى تكون موجهه نحو القواعد الجوية	ضمان الوصول من خلال السيطرة والتحكم بمنطقة المدار	بيئة يتحكم بها الإنسان تؤدي إلى تغييرات سريعة
التعبئة الوطنية	موقع المصادر الحيوية أو الموارد	حماية التجارة كعنصر رئيسي من عناصر القوة الوطنية	ضمان كادر من الفنيين المتخصصين وربطهم بالمركز	ضمان كادر من الفنيين المتخصصين وربطهم بالمركز	ضمان كادر من الفنيين المتخصصين وربطهم بالمركز

المصدر:

Gregory J. Rattray, An Environmental Approach to Understanding Cyberpower.USA,p.16

الشكل (1) أسلاك الإنترنت وتوزيعها تحت البحار في نهاية القرن العشرين



المصدر: مثنى مشعان المزروعي، جدلية العلاقة بين الجغرافية السياسية والفضاء الإلكتروني، ب.ت، ص 17

من يمتلك الأدوات السيبرانية ؟.

أفضل من أشار إلى الفاعلين في عالم الفضاء والأمن السيبراني هو البروفيسور الأمريكي **جوزيف أس.ناي** صاحب رؤية القوة الناعمة، وعنده أن هناك عدة قوى حول العالم تمثل العناصر المحركة الرئيسة في هذا المجال (أمين، 2020):

أولاً: الدول بمختلف أحجامها كبرى أم صغرى، فقد باتت مسألة الشراكة في الفضاء السيبراني ميسرة لأصحاب العقول، غير أن الهجومات السيبرانية ربما هي التي تحتاج إلى دول كبرى فاعلة تمتلك بنى تحتية سيبرانية لإحداث خسائر في أعدائها على المستوى الدولي .

ثانياً: قوى غير دولية أصغر في مقدراتها وقد تكون أقرب إلى الكيانات الأممية، وعادة ما يكون لهؤلاء أهدافاً تخريبية، إلا أن قدرتهم على القيام بعمليات واسعة النطاق تعوزها مساعدة أجهزة استخبارات دولية، وإن كان من اليسير عليها اختراق الموقع الإلكترونية واستهداف الأنظمة الفاعلة .

ثالثاً: وسائط التواصل الاجتماعي العالمية الكبرى مثل فيسبوك وجوجل وتويتر وغيرها، وهذه تمتلك قدر من المعلومات يسر لها قدرات تفوق في واقع الحال قدرات بعض الدول، ومن خلال تلك المعلومات تستطيع اختراق الأسواق السيبرانية بل توجه المجتمعات وتشكل الرأي العام .

رابعاً: الجماعات الإرهابية، وهنا تتضح المخاطر الحقيقية للعالم السيبراني، إذ تستخدم العصابات الإجرامية هذا الفضاء لسرقة وتسهيل كل ما هو مشروع من عينة تجارة الأسلحة وتجارة البشر، عطفاً على ما يسمى السوق السوداء أو المظلمة على الشبكة العنكبوتية .

خامساً: الأشخاص الاعتياديين، وهنا فإننا نرى أن فرداً حقيقياً يمكنه أن يغير ويبدل من حال العالم، والمثال على ذلك هو ويكليكس حيث أستطاع مخترق للأمن المعلوماتي الأمريكي أن يهدد أكبر دولة في العالم ويكشف أوراقها وتحالفاتها على الكرة الأرضية .

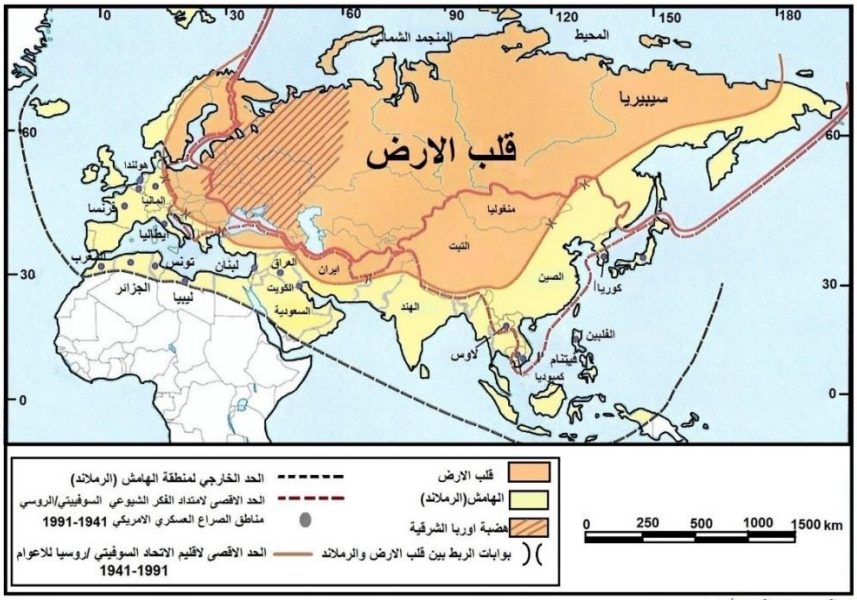
المبحث الثالث

الأمن السيبراني في ليبيا

1- الوضع الجيوبولتيكي الليبي في العالم في نظريات الجيوبولتيكه العالمية .

إنَّ ماكندر أعطى مفهوماً فضفاضاً للتاريخ العالمي عندما جعل من آسيا الوسطى منطقة محورية لمجريات الأحداث التاريخية، وفي تعديله الثاني أعاد ماكندر تعريف آسيا الوسطى على أنها منطقة المركز والتي أصبحت أكثر أتساعاً من المنطقة المحورية الأصلية، وقد بنى هذا التعديل على إعادة تقييم لإمكانات الاختراق للقوى البحرية (تايلور، و فنلنت، 2002، ص102)، حيث جعل منطقة شبه الجزيرة العربية ضمن الهلال الحيوي لمنطقة القلب، في إشارة إلى حيوية المنطقة وأبعاد إحتوائها مستقبلاً للسيطرة على منطقة القلب، وإن احتواء المنطقة سيعتمد على سكانها من خلال إيصال تقنية الفضاء الإلكتروني لتكون في متناولهم بما يسمح أن يجعلهم تحت التهديد وفي الوقت ذاته هم في مأمن من الهجوم المعاكس من خلال احتكار المعرفة في هذا الصراع. (الشكل رقم 2)

الشكل (2) خريطة حدود قلب العالم 1991.



الخريطة من عمل الباحثة اعتماداً على: The Human Mosaic , Political Geography ; A Divided World , Eleventh Edition ,W.H.Freeman and company 2010,p.27

وحسب نظرية ماكندر فإن ليبيا تقع ضمن منطقة الوصل بين قلبي العالم الشمالي والجنوبي الذي يضم أجزاء الوطن العربي الإفريقي والمتوسطي، ولأهمية موقع ليبيا في وسط شمال إفريقيا وجنوب حوض المتوسط يجعلها أكثر من غيرها حلقة وصل بين أوربا وإفريقيا جنوب الصحراء يساعدها في ذلك امتداد ساحلها ودخوله نحو الجنوب عند خليج سرت حيث تتوزع الموانئ على طول الساحل، هذه الأهمية جعلت ليبيا عرضة لتنافس القوى البحرية والبرية، في الوقت نفسه استطاعت ليبيا امتلاك القوتين معاً وسيطرت على سواحلها وحوض البحر المتوسط إبان عهد الأسرة القرمانلية سيطرة تامة، حتى إنها أرغمت السفن الأمريكية على دفع الإتاوة مقابل تأمين حركتها في حوض المتوسط .

واستمر التنافس على موقع ليبيا لاستراتيجي بين القوتين البحرية والبرية لكونها تمثل البوابة الشمالية لقلب العالم الجنوبي، وضمن المجال الحيوي لمنظومة الأمن الأوربي المتوسطي؛ لأن أمن جنوب أوروبا مرتبط بمستوى علاقاتها بدول الساحل الجنوبي لحوض المتوسط " شمال أفريقيا "، ولا سيما أن ليبيا تمتلك أطول الشواطئ الجنوبية على حوض المتوسط 1900 كم، مما جعلها أهم قاعدة بحرية في حوض المتوسط لسهولة اتصالها جنوباً ،وشمالاً، وشرقاً، وغرباً، وكواحدة من أهم ساحات الحرب العالمية الثانية لإدارة العمليات العسكرية بين الحلفاء والمحور، وزادت أهميتها بعد بداية الحرب الباردة بين المعسكرين الشيوعي والشمالي، حيث أقامت دول الحلفاء المنتصرة في الحرب (بريطانيا، أمريكا، فرنسا)، قواعد في الأراضي الليبية للسيطرة على أهم شرايين المواصلات في البحر المتوسط، كان لموقع ليبيا الجغرافي وحسب نظرية ماكندر أكسبها خصائص جيواستراتيجية تفاعلت مكوناتها مع منظور القوة البحرية، وشكلت ملامح للعلاقات الليبية الخارجية قديماً وحديثاً استطاعت من خلال استغلال قوة مواردها النفطية لبناء كيانها، وقوتها الذاتية حتى أصبحت لها مكانتها الاستراتيجية في حوض المتوسط وفي منطقة الشرق الأوسط وإفريقيا .

بعد انتصار الغرب في الحرب الباردة قامت نظرية العولمة ونظرية نهاية العالم والعالم الواحد التي تؤكد في القضاء على كافة التعددية الجيوبولتيكية بشكل نهائي، وتحل حقبة الحضارات المشتركة القائمة على مبادئ الديمقراطية الليبرالية، وهذا مشروع فرنسيس فوكاياما صاحب نظرية نهاية التاريخ، فيما يرى صموئيل هنتجتون في نظريته صدام الحضارات والتي ظهرت تلخيصاً لمشروع جيوبولتيكي كبير بعنوان التحولات في الأمن الكوني والمصالح القومية

الأمريكية، إذ يرى هنتجتون أن على الأطلسيين أن يدعموا بكل السبل المواقع الاستراتيجية لحضارتهم الخاصة بهم، وأن يستعدوا للمواجهة وأن ينسقوا قواهم الاستراتيجية وأن يبطلوا الميول المناوئة للأطلسيين في التشكيلات الجيوبولتيكية الأخرى، إذ يرى أن توحيد هذه التشكيلات في حلف قاري يشكل خطراً على الغرب، وأن هذه التشكيلات المناوئة للغرب أخطرها هي: (المزروعي، ب ت، ص26) :

1. الكونفوشيوسية (الصين).
2. الدول الإسلامية.

وعلى هذا الأساس يقدم هنتجتون النصائح لدول الغرب، وهي الحد من التطور العسكري للدول الإسلامية والصينية، واستغلال المصاعب والنزاعات في العلاقات المتبادلة بين الدول الإسلامية والصينية، واستغلال المصاعب والنزاعات بين الدول الإسلامية نفسها، وذلك لأن هذه الدول الإسلامية هم الأعداء الأكثر احتمالاً للغرب.

ومن هنا جاء اهتمام الولايات المتحدة بالمنطقة الممتدة من باكستان إلى المغرب العربي على أنها تأتي على رأس المناطق التي تمثل مصالح الولايات المتحدة لكونها قلب منابع النفط والاحتياطي الأكبر في العالم، كما أنها سوق استهلاكية للبضائع الأمريكية والعالم الغربي.

ومن خلال العرض السريع للنظريات السابقة نجد أن موقع ليبيا جيوبولتيكياً يقع ضمن مناطق الاهتمام في كافة النظريات الأمر الذي يضعها دائماً في موقع يسعى الكثير إلى السيطرة عليه سواء لموقعه الجغرافي أو لما يمتلكه من موارد سواء نفطية أو ثروات، هذا الأمر يضعها دائماً في الاستعداد لمواجهة أي أخطار خارجية سواء من الدول الغربية أو الدول العربية والإسلامية، حيث ان نظرية قلب العالم تدعو أغلب الدول للاستفادة من مواقعها لفرض السيطرة، فما هي الاستعدادات التي قامت بها ليبيا بخصوص مواجهة أي مخاطر سيبرانية، ولا سيما وأننا الأن في عصر التكنولوجيا، وانتشار هذه الحروب حالياً على الساحة العالمية، كان أخرها هو أتهام أوكرانيا للاتحاد السوفيتي بقيامة لأكثر من 70 عملية اختراق سيبراني لكافة المواقع الحكومية وتعطيلها وأخرجاها عن العمل (أوكرانيا تكرّر اتهام روسيا بالهجوم الالكتروني وتؤكّد أن لديها "أدلة"، https://www.france24.com/ar).

2- الفضاء السيبراني في ليبيا.

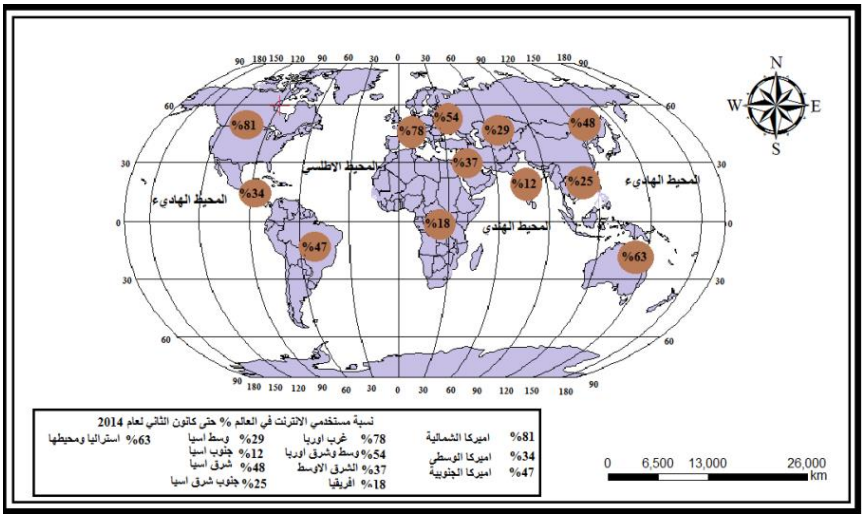
بدأ استخدام الإنترنت في ليبيا من قبل الجمهور في أواخر تسعينيات القرن العشرين، وبعدد سكان وصل في يوليو 2010 إلى 6,461,454 نسمة فقد وصل عدد مستخدمي الإنترنت في 2009 (سواء المنتظمين أو غير المنتظمين) إلى 353,900 نسمة (https://web.archive.org/web/20180626163329)، وأرتفع في العام 2012 إلى 1,115,025 نسمة، وبلغ ترتيبها عالمياً 119 فيما تم تقدير نسبة المستخدمين من السكان للإنترنت بحوالي 19.9 % (Calculated using penetration,2013)، وقد بلغ عدد المستخدمين من الذكور الـ 65 % ومن الإناث الـ 35.% بينما كانت الفئة العمرية من 18-24 هي الأكثر استخدامًا للفيس بنسبة 34 % ثم تليها الفئة العمرية من 25-34 بنسبة 32% والفئة العمرية من 35-44 بنسبة 14% (https://www.eanlibya.com).

وصل عدد مستخدمي الفيسبوك في ليبيا إلى حوالي 5 ملايين مستخدم فيسبوك نشط شهرياً، ووصلت نسبة عدد مستخدمي التطبيق إلى أكثر من 74% من عدد السكان العام في البلاد، في وقت بلغت فيه نسبه الليبيين المستخدمين للأنترنت حوالي 85 % من السكان خلال يناير 2020، في الوقت الذي لم يتجاوزا 850 ألف نسمة خلال العام 2003 (الهيئة العامة للاتصالات والمعلوماتية، تقرير المؤشرات المحلية)، وقد بلغ عدد الليبيين الذين لديهم ثقة في الإنترنت كبديل عن القنوات المرئية وذلك خلال فترة الانقسام السياسي حوالي 52 % من إجمالي السكان (الهيئة العامة للاتصالات والمعلوماتية، تقرير المؤشرات المحلية).

في شهر 6 من عام 2021 بلغ عدد مستخدمي فيسبوك حوالي 4 مليارات مستخدم على مستوى العالم، منهم 188 مليونًا في العالم العربي، يستخدمون الموقع بشكل مستمر، بلغ منهم 40 مليونًا في مصر ، 28 مليونا في الجزائر، 25 مليونًا في العراق، 19 مليونا في السعودية، 17 مليونًا في المغرب، 10 ملايين في السودان، 8.8 مليون في الإمارات، 8 ملايين في تونس، 7.5 مليون في سوريا، 6 ملايين في الأردن، 3 ملايين في الكويت، 2.5 مليون في لبنان، 2.4 مليونًا في ليبيا، 2.1 مليون في قطر، مليونان في اليمن، 1.8 مليون في سلطنة عمان، 1.2 مليون في البحرين، 1.1 مليون في موريتانيا، مليون مستخدم في فلسطين، 900 ألفًا في جيبوتي، 400 ألف في الصومال و300 ألفًا

في جزر القمر(مُحَمَّد البحيري ، 274 مليون عربيًا يستخدمون وسائل التواصل الاجتماعي). (الشكل 3)

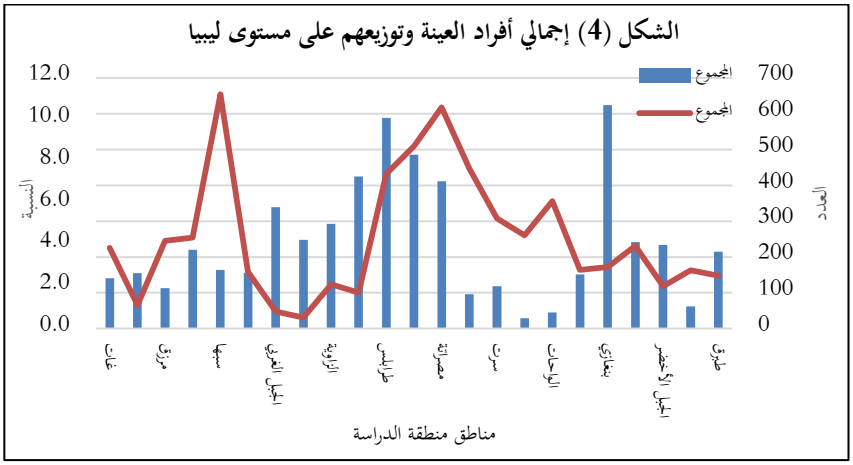
الشكل (3) نسبة مستخدمي الأنترنت 2014.



المصدر: مثنى مشعان المزروعي، جدلية العلاقة بين الجغرافية السياسية والفضاء الإلكتروني، ب.ت، ب.ن، ص 29.

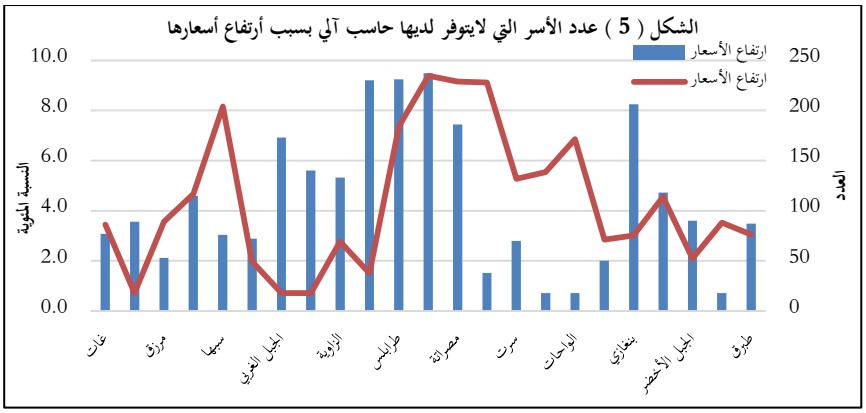
من خلال دراسة مستخدمي أجهزة الكمبيوتر في ليبيا، فقد أفادت دراسة قامت بها الهيئة العامة للاتصالات والمعلوماتية لعدد 5557 أسرة على مستوى ليبيا، كانت أعلاها في مدينة طرابلس وبعدد 589 أسره وأقلها بمدينة الكفرة لعدد 29 أسرة. (الشكل 4)

الشكل (4) إجمالي أفراد العينة وتوزيعهم على مستوى ليبيا



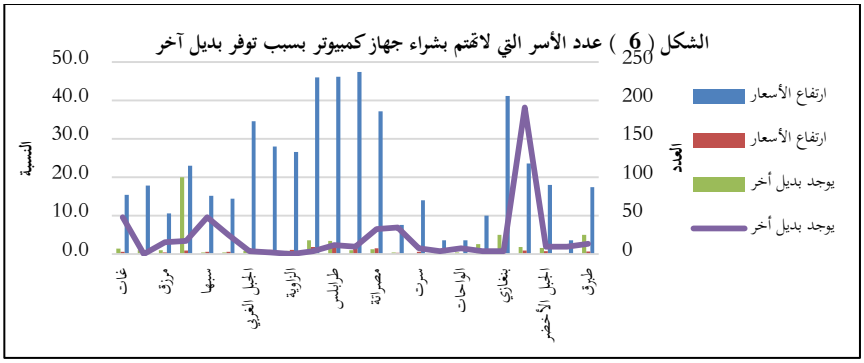
المصدر: الهيئة العامة للاتصالات والمعلوماتية، تقرير المؤشرات المحلية، مؤشرات الأسرة والفرد ،ملخص لمشروع مشترك مع مصلحة الإحصاء، نتائج مسح تقنية المعلومات والاتصالات https://www.cim.gov.ly/local-indicators .

وعند دراسة التوزيع النسبي للأسر التي لا يتوفر لديها كمبيوتر، وذلك حسب أسباب عدم التوفر فقد أفادت 2525 أسرة من أسر مجتمع الدراسة أن السبب الرئيس لعدم امتلاك جهاز كمبيوتر يرجع بسبب ارتفاع أسعارها ، وقد بلغت أعلى نسبه من عينة الدراسة في كل من مديني المرقب وطرابلس وبنسبة بلغت 9.4 % و 9.1 % على التوالي، فيما كانت أقل نسبه بمدينة درنة والواحات والكفرة حيث بلغ فيها جميعها 0.7 % .(الشكل 5)



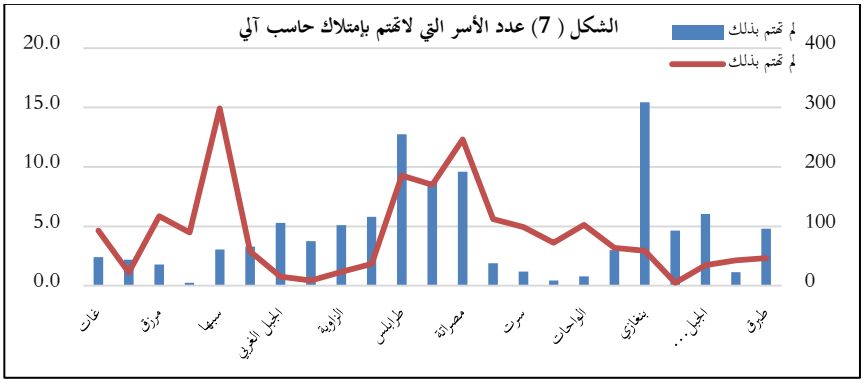
المصدر: الهيئة العامة للاتصالات والمعلوماتية، تقرير المؤشرات المحلية، مؤشرات الأسرة والفرد ،ملخص لمشروع مشترك مع مصلحة الإحصاء، نتائج مسح تقنية المعلومات والاتصالات https://www.cim.gov.ly/local-indicators.

أمَّا من حيث أنه يكون هناك بديل في مكان آخر لاستعمالها، فقد بلغت عدد الأسر 262 أسرة، وقد كانت أعلى نسبة من هذا السؤال في منطقة وادي الشاطئي حيث بلغت نسبتهم 38.2 %، فيما كانت أقلها في مدينة درنة وسرت حيث كانت النسبة بهما 0%. (الشكل 6)



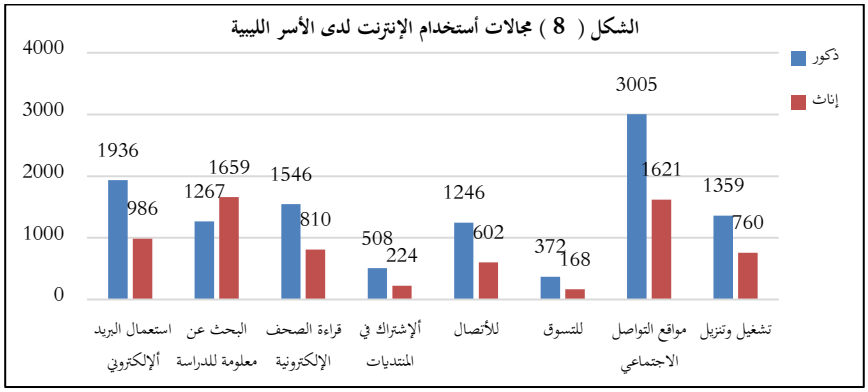
المصدر: الهيئة العامة للاتصالات والمعلوماتية، تقرير المؤشرات المحلية ، مؤشرات الأسرة والفرد، ملخص لمشروع مشترك مع مصلحة الإحصاء، نتائج مسح تقنية المعلومات والاتصالات https://www.cim.gov.ly/local-indicators.

أمَّا من حيث عدد الأسر التي لا تهتم بامتلاك جهاز كمبيوتر فقد بلغ عددها 2071 أسرة، وبلغ أكبر عدد بها في مدينة طرابلس وبعدد 255 أسرة، أمَّا أقلها فقد كانت في منطقة وادي الشاطئ وبنسبة لم تتجاوز 5 % .(الشكل 7).



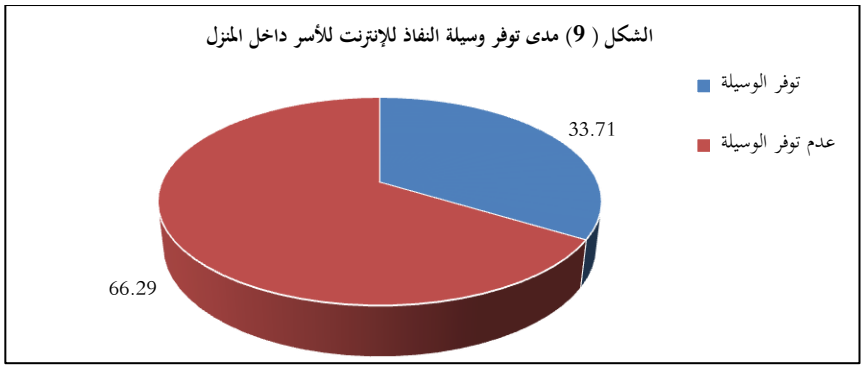
المصدر: الهيئة العامة للاتصالات والمعلوماتية، تقرير المؤشرات المحلية، مؤشرات الأسرة والفرد ،ملخص لمشروع مشترك مع مصلحة الإحصاء، نتائج مسح تقنية المعلومات والاتصالات https://www.cim.gov.ly/local-indicators .

أمَّا من حيث استخدام أفراد الدراسة للأنترنت حسب النشاط فقد تم تقسيمها إلى 8 أنشطة رئيسة حسب استخدام الإنترنت بلغ أعلاها لمستخدمي مواقع الاتصال الاجتماعي حيث أفاد عدد 4626 أسرة أنها تستخدمه بمواقع التواصل الاجتماعي، تليها نشاط البحث عن معلومات دراسية، وقد بلغ عدد أعلى عدد للذكور حسب النشاط في نشاط مواقع التواصل الاجتماعي فيما بلغت أعلى أعداد للإناث في مجال البحث عن معلومات للدراسة.(الشكل 8)



المصدر: الهيئة العامة للاتصالات والمعلوماتية، تقرير المؤشرات المحلية، مؤشرات الأسرة والفرد ،ملخص لمشروع مشترك مع مصلحة الإحصاء، نتائج مسح تقنية المعلومات والاتصالات https://www.cim.gov.ly/local-indicators.

أما من حيث توفر وسلة النفاذ للإنترنت من داخل المنزل، فقد بلغ مجموع الأسر التي شاركت في هذا السؤال 8583 أسرة، بلغت نسبة إمكانية النفاذ من داخل المنزل حوالي 33.71 % وبعدد 2893، فيما بلغت عدد من لا يستطيعون النفاذية حوالي 5690 أسرة، وهذا مؤشر خطير حيث أن أغلب مجتمع العينة يعمل على الإنترنت من خارج المنزل وهنا تغيب الرقابة الأسرية على محتوى الإنترنت. (الشكل 9)

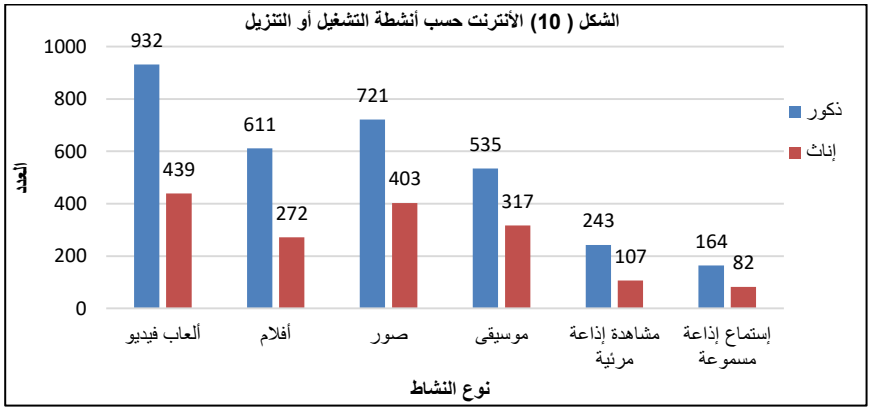


المصدر: الهيئة العامة للاتصالات والمعلوماتية، تقرير المؤشرات المحلية، مؤشرات الأسرة والفرد ،ملخص لمشروع مشترك مع مصلحة الإحصاء، نتائج مسح تقنية المعلومات والاتصالات https://www.cim.gov.ly/local-indicators .

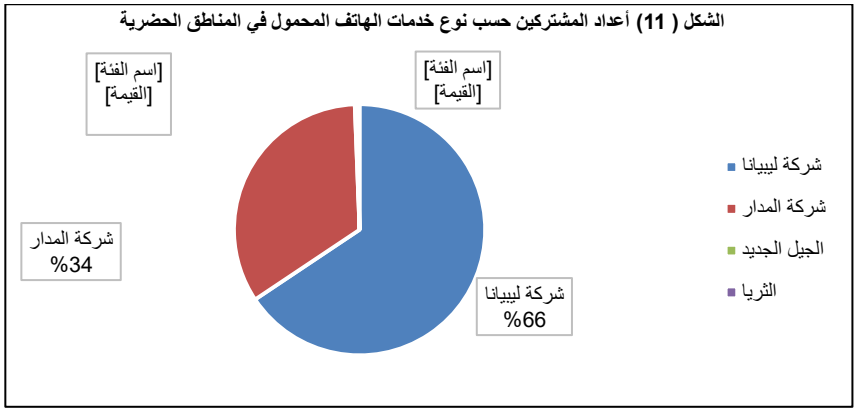
ومن خلال الشكل السابق يتبيَّن أن أغلب وسائل توفر الإنترنت تكون عبر الهاتف، حيث أشارت ما نسبته 66.29 % أنه لا يوجد جهاز إنترنت في المنزل.

أما من حيث المحتوى الذي يتم متابعته عبر الأنترنت فقد تم حصر عدد 6 أنشطة يتم من خلالها التشغيل أو التنزيل لمحتوياتها، وهي ألعاب الفيديو، أفلام، صور، موسيقى، مشاهدة إذاعة مرئية، استماع إلى إذاعة مسموعة، وقد بلغ عددهم 4826 مستخدمًا بلغ عدد الذكور منهم 3206 والإناث 1620 مستخدمًا (الشكل 10)، بلغ أكثر نشاط من بينها هو ألعاب الفيديو وأقلها الاستماع إلى إذاعة مسموعة.

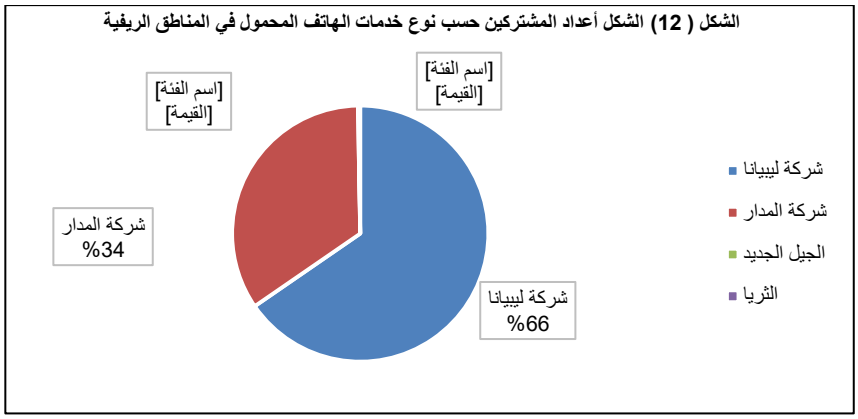
ومن خلال البيانات يتضح أن نوع الخدمة توفر عبر عدد أربع شركات هاتف في ليبيا وهي شركة ليبيانا، وشركة المدار الجديد، وهواتف الثريا، والجيل الجديد، وقد اشتملت دراسة على عدد 31257 شخصًا، توزعوا بين الحضر والريف حيث بلغت نسبه الحضر منهم 90 % والريف حوالي 10 %، وقد كانت شركة ليبيانا هي الأكثر اشتراكاً في الخدمة حيث بلغ مستخدميها حوالي 65 % سواء في الحضر أو الريف (الشكل (11) والشكل (12)).



المصدر :الهيئة العامة للاتصالات والمعلوماتية ، تقرير المؤشرات المحلية ، مؤشرات الأسرة والفرد ،ملخص لمشروع مشترك مع مصلحة الإحصاء ،نتائج مسح تقنية المعلومات والاتصالاتhttps://www.cim.gov.ly/local-indicators .



المصدر: نفس مصدر الشكل 10.



المصدر: نفس مصدر الشكل 10.

ومن خلال البيانات للدراسات السابقة، يتبين أن المجتمع الليبي مجتمع متصفح ومشغل للإنترنت، ويسعى للحصول عليها سواء عن طريق أجهزة الكمبيوتر، وأجهزة الهاتف، أو مزودات الخدمة، وقد كانت أعلى نسبه منهم تستخدم الأنترنت لمتابعة مواقع التواصل الاجتماعي والتي بلغ عددهم 4626 .

إنَّ وسائل التواصل الاجتماعي أصبحت بديلاً لليبيين للتعبير عن آرائهم ومصدراً لوسائل الإعلام التقليدية سواء الصحف أو الإذاعات أو المحطات التلفازية، حيث أصبحت الأجندة الإعلامية ترتب بناءً على أهم الأحداث التي تحدث في العالم الرقمي.

ولما لمواقع التواصل الاجتماعي من دور في الوصول إلى كل مواطن، وقد تعرضنا في بداية دراستنا على خطورة المواقع الاجتماعية من حيث المحتوى، ومدى خطورتها على الدول، ولا سيما الدول التي بها مشاكل سياسية أو عسكرية، كما هو الحال الذي تعيشه ليبيا منذ عشر سنوات، فما هي الحماية السيبرانية التي تتخذها الدولة الليبية في سبيل حماية فضائها السيبراني، ومدى قوتها، وما التشريعات والقوانين التي تسعى لحماية فضائها السيبراني.

المبحث الرابع

التحديات والمخاطر الجيوسبرانية في ليبيا

أصبح الاعتماد على شبكة الإنترنت ووسائل الاتصالات الحديثة في مختلف مجالات الحياة كبيراً جدًا بشكل أبرز أهمية قصوى للتركيز على المخاطر التي قد تنتج. وعلى الرغم من أنه ليست هناك ضمانات كاملة للحماية من المخاطر إلا أن هناك خطوات وقائية توفر الحماية والسلامة، مما أستدعي قيام وزارة الاتصالات والمعلوماتية بالتحرك سريعًا لإنشاء اللبنة الاساسية عن طريق إدارة أمن وسلامة المعلومات بالوزارة. ولحرص الوزارة و الحكومة علي أهمية الدور المنوط بهذه الإدارة تم اقتراح أنشاء هيئة وطنية لأمن وسلامة المعلومات، وقد صدر القرار رقم (28) رسمياً من مجلس الوزراء بتاريخ 22 يناير 2013.(الحكومة المؤقتة، قرار 23 لسنة 2013)، وقد كان الهدف من وراء إنشائها الآتي :

1. القيام بالتنسيق بين جميع مؤسسات الدولة لإدارة مركز العمليات الأمنية لتوفير بيئة آمنة لتبادل المعلومات والاتصالات.

2. تجهيز البيئة التشريعية والقانونية ووضع السياسات الأمنية المعلوماتية للدولة وفقًا للمعايير الدولية.
3. وضع المواصفات والمعايير للتجهيزات والبرامج لحماية المؤسسات التابعة للدولة.
4. وضع سياسات التعامل مع المشاكل الأمنية المعلوماتية لحلها في أقصر وقت عند حدوثها والحد من تأثيراتها.
5. نشر الوعي وثقافة أمن المعلومات لجميع الاطياف والقطاعات.
6. إجراء اختبارات ضمان الجودة لحماية الشبكة والأنظمة.
7. البحث المتواصل عما يستجد في مجال الاختصاص لترشيح التقنيات التي يمكن اقتناؤها لتحسين بيئة العمل والإنتاج.
8. اعتماد نظم التشفير التي توفر مستوى عال من الأمن للمعلومات والبيانات مع المحافظة على المرونة في تدفقها وتداولها.
9. توفير الوسائل اللازمة لضمان بيئة آمنة للتعاملات الإلكترونية بين المؤسسات الحكومية وبين المواطنين ومختلف الأطراف.
10. العمل على ضمان مكانة متميزة لليبيا في مجال أمن وسلامة المعلومات إقليميًا وقاريًا ودوليًا.
11. ضمان السلامة المعلوماتية والأنظمة، بحيث يمكن التأكد من عدم تعرضها لأي نوع من التغيير غير المصرح به.

في العام 2016 بلغ ترتيب ليبيا في الحماية السيبرانية الترتيب 104 عالمياً وبنسبة بلغت 0.224 من برنامج الأمن السيبراني العالمي (GCA)، والتي وضعت كإطار للتعاون الدولي بين أصحاب المصلحة المتعددين نحو مجتمع المعلومات أكثر سلامةً وأمناً، والذي يركز على مجالات العمل الخمسة التالية وهي التدابير القانونية، والتدابير التقنية، والتدابير التنظيمية، وبناء القدرات، والتعاون.

وتشكل المجالات الخمسة السابقة الذكر أساس مؤشرات الرقم القياسي العالمي للأمن السيبراني (GCI) (الجدول 4)، وهذه المؤشرات الخمسة بالغة الأهمية لقياس القدرات الوطنية في مجال الأمن السيبراني؛ لأنها تشكل اللبنات المتأصلة في ثقافة وطنية، ويمتلك الأمن السيبراني مجال تطبيق يتقاطع مع جميع الصناعات وجميع القطاعات، عمودياً وأفقياً، وبالتالي

فإن تمكين القدرات الوطنية وتطويرها يتطلب الاستثمار من جانب القوى السياسية، والاقتصادية، والاجتماعية، ويمكن القيام بذلك من جانب دوائر لإنفاذ القانون، والعدل، والمؤسسات التعليمية، والوزارات، وشركات القطاع الخاص، ومطوري التكنولوجيا، وبالشراكات بين القطاع العام والخاص، والتعاون ضمن الدولة نفسها .

جدول (4) الدول العشر الأكثر قدرة على مواجهة التهديدات السيبرانية

الدولة	التدابير القانونية	التدابير الفنية	التدابير التنظيمية	بناء القدرات	التعاون	عوامل النجاح الرئيسية
سنغافورة	0.95	0.96	0.88	0.97	87.	0.92
أمريكيا	1	0.96	0.92	1	0.73	0.91
ماليزيا	0.87	0.96	0.77	1	0.87	0.89
سلطنة عمان	0.98	0.82	0.85	0.95	0.75	0.87
استونيا	0.99	0.82	0.85	0.94	0.64	0.84
موريشيوس	0.85	0.96	0.74	0.91	0.70	0.82
استراليا	0.94	0.96	0.86	0.94	0.44	0.82
جورجيا	0.91	0.77	0.82	0.90	0.70	0.81
فرنسا	0.94	0.96	0.60	1	0.61	0.81
كندا	0.94	0.93	0.71	0.82	0.70	0.81

المصدر: الاتحاد الدولي للاتصالات، مؤشر الأمن السيبراني العالمي، 2017، ص 17 .

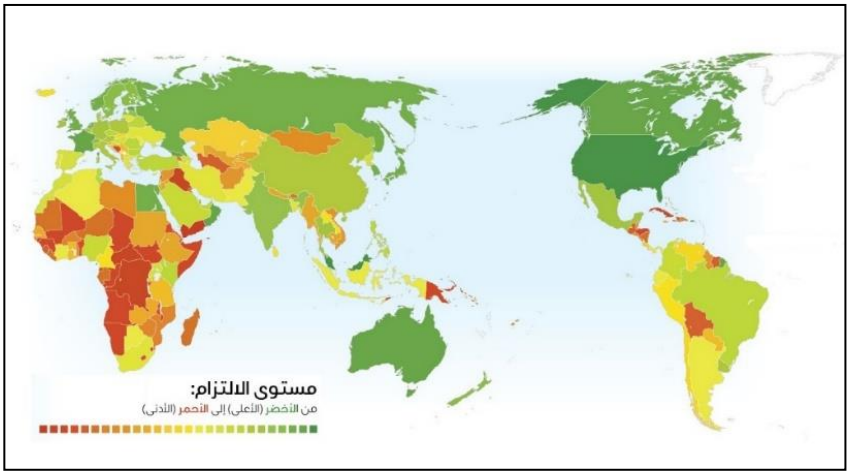
وبالرغم من هذه الخطوات إلا أنه في العام 2018 تراجعت ليصبح ترتيبها 117 عالمياً وبنقاط بلغت 0.206، أما إقليميًا فكان ترتيبها على مستوى الدول العربية هو الترتيب 16.

في العام 2021 تقدم ترتيبها بعض النقاط حيث أصبحت تحل في الترتيب 113 عالمياً، وبنقاط بلغت 28.78، ولتصبح في الترتيب 14 عربياً، فيما حلت المملكة العربية السعودية في الترتيب الأول وبنقاط 99.54 من نقاط الإجراءات السيبرانية الخمسة.

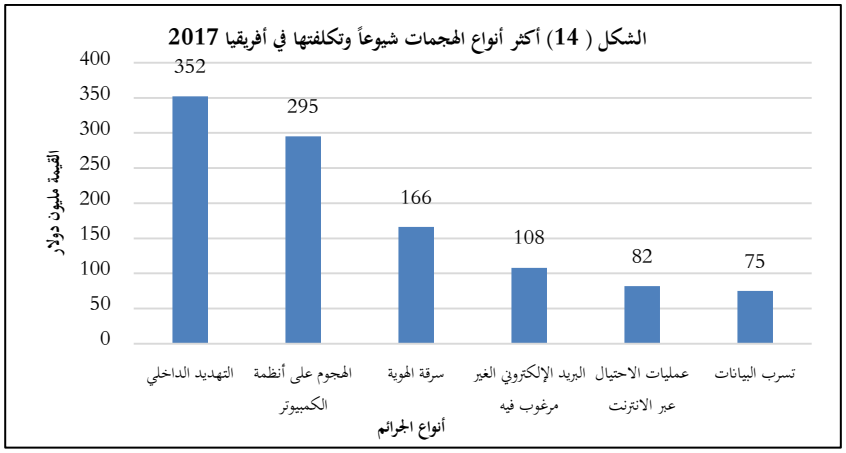
وبالرغم من تقدم المؤشرات المتعلقة بعمليات الأمن السيبراني إلا أن موقع ليبيا عالمياً لا يزال ضعيفاً حيث وصل إلى 113 من بين 182 دولة مشتركة في البرامج الأمنية لحماية الفضاء السيبراني الخاص بها.(الشكل 13)، شأنها في ذلك شأن أغلب الدول في قارة أفريقيا والتي لاتزال تعاني من ضعف الأمن السيبراني لديها ،حيث خسرت أوغنداء في العام 2017 حوالي 67 مليون دولارًا، ونيجيريا 649 مليون دولارًا، وتنزانيا 99 مليون دولارًا، وغانا 54

مليون دولارًا، وكينيا 210 مليون دولاراً، في الوقت الذي اشارت فيه المغرب أنها تعرضت لهجوم سيبراني أدى إلى إيقاف العمل في مصنع السيارات، كما أفاد أكثر من ثلثي مستخدمي الأنترنت في جنوب أفريقيا إلى تعرضهم لهجمات سيبرانية (الشكل 14).

الشكل (13) الإلتزامات الوطنية في أفريقيا المتعلقة بالأمن السيبراني



المصدر: تقرير مؤشر الأمن السيبراني العالمي 2017 .



المصدر: تقرير مؤشر الأمن السيبراني العالمي 2017 .

بتاريخ 1 ديسمبر 2021 أصدرت شركة ميتا (Adversarial Threat Report, 2021, p14) في تقريرها أن شركة فيس بوك حذفت شبكة حسابات مزيفة تدار من

تركيا وتستهدف ليبيا قالت شركة ميتا إن منصتيها فيسبوك وإنستغرام، حذفتا شبكة حسابات مزيفة تتخذ من تركيا مقرًا، وتستهدف ليبيا بشكل أساسي، كما وجدت رابطًا بين نشاط هذه الحسابات وحزب العدالة والبناء، وجاء ذلك في تقرير مفصل عبر موقعها الإلكتروني، كجزء من تلخيص تنفيذي للسلوك المزيف المنسق لعام 2021 . وقالت الشركة إنها أزالت 41 حسابًا على فيسبوك و133 صفحة وثلاث مجموعات و14 حسابًا على إنستغرام، وجدت أنها تنتهك سياسة الشركة ضد السلوك المنسق غير الأصيل، لافتة إلى أن هذه الشبكة نشأت في المقام الأول في تركيا واستهدفت ليبيا بشكل أساسي، وهذه العملية ضمن 52 شبكة أزالتها الشركة، خلال العام 2021، عندما وجدت أنها شاركت في جهود منسقة للتلاعب أو إفساد النقاش العام من أجل هدف استراتيجي، مع الاعتماد بشكل مركزي على الحسابات المزيفة لتضليل الناس، وقالت الشركة إن الشبكات المزيفة التي رصدتها على مدار العام أُنشئت في 34 دولة، بما في ذلك أميركا اللاتينية ومنطقة آسيا والمحيط الهادئ وأوروبا والشرق الأوسط وأفريقي، وفيما يخص شبكة الحسابات التي تستهدف ليبيا، أفادت الشركة بأن الأشخاص الذين يقفون وراء الحسابات المزيفة (السلوك المنسق غير الأصيل)، تم اكتشاف بعضها وتعطيله، كانوا يستهدفون نشر المجموعات والصفحات وإدارتها، بما في ذلك تلك التي يُزعم أنها تنتمي إلى شخصيات ومؤسسات عامة في ليبيا، بما في ذلك المطارات والهيئات الحكومية، رئيس وزراء سابق وسياسيون وصحفيون ونشطاء، لافتة إلى أنها قامت بتعطيل بعض صفحات هذه الشبكة بسبب انتحال الهوية وانتهاكات أخرى، وأوضحت أن الأشخاص الذين يقفون وراء هذا النشاط نشروا أخبارًا وأحداثًا باللغة العربية جارية في المنطقة، بما في ذلك تأخر الانتخابات وانتقاد صعود المرأة في السياسة والمجتمع والإعلام، ولفتت إلى أن هذه الشبكة أنشأت صفحات تزعم أنها تدار من قبل شخصيات عامة نسائية للإدلاء ببيانات تحريضية نيابة عنهن، ثم يستخدمون صفحاتهم الأخرى للإشارة إلى هذه التعليقات الوهمية لانتقادهم، على الأرجح لتشجيع المضايقات . وعلى الرغم من أن الأشخاص الذين يقفون وراءها حاولوا إخفاء هوياتهم وتنسيقهم، تقول ميتا إنها وجدت روابط مع حزب العدالة والبناء التابع لجماعة الإخوان المسلمين، وقالت الشركة إنها وجدت هذه الشبكة كجزء من تحقيق داخلي في السلوك غير الصحيح المنسق المشتبه به في ليبيا المرتبط بتقارير سابقة عن انتحال الهوية ،وبشأن البيانات التفصيلية،

وأفادت الشركة إن حوالي 1.7 مليون حساب تابع واحدًا أو أكثر من هذه الصفحات، وانضم حوالي 600 شخصًا إلى واحدة أو أكثر من المجموعات، وتابع حوالي 4000 حسابًا واحدًا أو أكثر من حسابات إنستغرام، وأوضحت الشركة، أن حوالي 59 ألف دولارًا أمريكي جرى إنفاقها على الإعلانات على فيسبوك وإنستغرام تُدفع بالدولار الأميركي والفرنك السويسري في المقام الأول(Adversarial Threat Report,2021,p14-15) .

تعاظم دور وسائل التواصل الاجتماعي في الآونة الأخيرة، والذي لم يأت من فراغ، وإنما كان نتيجة مجموعة من العوامل والاعتبارات، **لعل أهمها**:

1. التزايد المستمر في أعداد مستخدمي وسائل التواصل الاجتماعي.
2. القدرة على التأثير في الرأي العام.
3. تشكل وسائل التواصل الاجتماعي نقلة نوعية في عالم الإعلام الرقمي.
4. التفاعل المكثف.
5. باتت وسائل التواصل الاجتماعي أحد أهم الفاعلين الدوليين.

تلعب وسائل التواصل الاجتماعي دوراً فاعلاً في صناعة الرأي العام وتشكيله، حيث تسهم في ترويج الأفكار التي تعتنقها النخبة في المجتمع، لتصبح ذات قيمة اجتماعية معترف بها، وتحظى بالانتشار بين الأشخاص العاديين، ومن ثم التأثير على سلوكهم وفي تشكيل توجهاتهم إزاء قضايا بعينها؛ وهذا الدور وفقاً لنظرية التسويق الاجتماعي يتشابه إلى حد كبير مع حملات التسويق التي تستهدف الترويج لسلعة معينة وإقناع المستهلكين بها (معتوق، 2017)، وعلى أية حال، فإن وسائل التواصل الاجتماعي باتت شريك رئيس في صناعة الرأي العام **من خلال العديد من الأدوار**:

1. التأثير في الوعي.
2. تنامي دور الفرد في التأثير على الرأي العام.
3. عامل مساعد في حركة التغيير.

في الوقت الذي تلعب فيه وسائل التواصل الاجتماعي العديد من الأدوار الإيجابية، سواء في ما يتعلق بتنمية الوعي والتأثير في الرأي العام والدفاع عن قضايا الحريات العامة، إلا أنها في المقابل يساء توظيفها بصورة تهدد الأمن والسلم في الدول، خاصة أنها لا تخضع لأطر أو قوانين تضبط المحتوى الذي يتم نشره عليها، بل أنها تحولت في الآونة الأخيرة إلى أداة

تساعد التنظيمات المتطرفة في نشر الأفكار الهدامة والتحريض على العنف والكراهية، وفي نشر الشائعات وإثارة الفوضى والاضطراب، وهذا ما يمكن أن يطلق عليه الأدوار الشائكة والخطيرة لوسائل التواصل الاجتماعي، والتي يمكن الإشارة إليها على النحو الآتي:

1.**تضليل الرأي العام:** مع أن وسائل التواصل الاجتماعي تسهم بدور رئيسي في صناعة الرأي العام وتشكيله، إلا أنها قد تتحول في بعض الأحيان إلى منصات للتضليل الإعلامي، وتوجيه الرأي العام في بعض الدول بشكل معين يخدم مصالح دول أو جماعات بعينها، بعيداً عن الحقيقة.

التضليل الإعلامي لا يتوقف عند هذا الحد بل يكون أيضًا من خلال حسابات وهمية خارجية، لكنها تتبنى مواقف بعينها للتأثير في الرأي العام داخل دولة محددة، كما أن وسائل التواصل الاجتماعي، حسب دراسة صدرت عن جامعة أوكسفورد في يونيو عام 2017 تحولت إلى أدوات في أيدي بعض الحكومات للتأثير في مضامين الرأي العام في الداخل؛ ومن أمثلة التضليل الإعلامي ما يحدث أثناء الانتخابات حين يتم توظيف وسائل التواصل الاجتماعي في إطلاق شائعات وأخبار تحاول إما صرف الانتباه عن الاستحقاق الانتخابي برمته، أو التأثير على صورة أحد الأطراف لتحقيق مصالح أطراف أخرى.

2.**توظيف وسائل التواصل الاجتماعي في نشر التطرف والترويج لخطاب الكراهية** فغالباً ما تلجأ الجماعات الإرهابية إلى منصات ومواقع التواصل الاجتماعي لنشر أفكارها المتطرفة، لأنها تجد فيها وسيلة رخيصة نسبياً وملائمة وآمنة لإيصال رسائلها، فضلاً عمّا تتيحه من وسائط متعددة مثل الصور والفيديوهات والمقاطع المسجل، ولعل ما يساعد التنظيمات المتطرفة والإرهابية أيضاً في استغلال وسائل التواصل الاجتماعي، ما يطلق عليه "البشر المتنكرون" الذين يستخدمون مواقع التواصل الاجتماعي بأسماء وهمية، لكنهم في الأصل تابعون لتنظيمات متطرفة ويروجون لأفكارها الهدامة والتخريبية، وهؤلاء البشر المتنكرون أو "أصحاب الحسابات الوهمية" على مواقع التواصل الاجتماعي باتوا يشكلون خطراً متفاقماً، خاصة أنهم يوظفون وسائل التواصل الاجتماعي بشكل يضر بالأمن الوطني للدول والمجتمعات من خلال بث الأخبار الكاذبة والإشاعات المغرضة التي تضر بمصالح هذه الدول، وإثارة الفوضى فيها، وقد استخدمت الجماعات الإرهابية من مقاتلي داعش هذه المواقع في خلق نوع من الإرهاب في ليبيا خلال السنوات 2015-2018 .

3.**نشر الشائعات الهدامة** تمثل واحدة من المخاطر الناجمة عن سوء توظيف وسائل التواصل الاجتماعي، والتي أصبحت تمثل المصدر الرئيسي للعديد من الشائعات، خاصة مع تنامي ظاهرة الحسابات الوهمية في وسائل التواصل الاجتماعي، والتي لا يمكن السيطرة عليها بسهولة، فضلاً عما تتميز به وسائل التواصل الاجتماعي من سهولة وسرعة في نشر وتداول المعلومات والأخبار عليه، وذلك لعدم وجود رقيب أو قواعد وأسس للنشر على تلك المواقع.

وتُعَدُّ وسائل التواصل الاجتماعي بيئة خصبة لانتشار الشائعات وتداولها بشكل فائق السرعة بفعل خصائص والبث الفوري والتداول الجماعي التي تتمتع بها، فضلاً عن توافر أدوات تزييف الصور وفبركة الفيديوهات، والتي تضفي بدورها حبكة محكمة على محتوى الشائعات تساعد في انتشارها (عبدالفتاح، 2017)، ولعل أحدث مثال على كيفية توظيف مواقع التواصل الاجتماعي في نشر الشائعات، هو أزمة فيروس كورونا (كوفيد-19)، وفي دراسة ميدانية في ليبيا حول الشائعات المنشورة حول مرض كوفيد -19 لعينة بلغت 186 مبحوث، أوضحت أن نسبة 83.87 % يرون أن مواقع التواصل الاجتماعي تنشر الشائعات المتعلقة بجائحة كورونا وتداولها بين مستخدميها، وقد أوضحت الدراسة أيضاً أن أعلى نسبة لمصدر الشائعات كانت عالمية أم محلية أم إقليمية فقد أفادت النتائج أن النسب كانت الأعلى عالمية حيث بلغت نسبتها 77.42 % يليها المحلي، وقد كانت أعلى نسبة من الشائعات تنتشر على موقع الفيسبوك حيث بلغت النسبة المئوية له 61.29 % من مجتمع الدراسة، يليه اليوتيوب، ثم التويتر، والإنستغرام، وجوجل بلس، وبنسب 24.20%، 8.06 %، 4.84 %، 1.61 %، على التوالي (فرج، 2021، ص275-277) .

4.**التحريض على الفوضى وإثارة الاضطرابات:** مع التوسع في استخدام وسائل التواصل الاجتماعي فقد أصبحت ضمن أهم الأدوات التي يتم توظيفها في التحريض على الفوضى وزعزعة الأمن والاستقرار في العديد من الدول العربية. وتشير إحدى الدراسات الغربية إلى أنه لولا وسائل التواصل الاجتماعي لما كان ما يعرف بـ"أحداث الربيع العربي" التي شهدتها بعض الدول منذ نهاية العام 2010، أن تنطلق وتمتد من دولة إلى أخرى، وقد كان من أشهرها في ليبيا صفحة أطلق عليها "لنجعله يوم الغضب 17 فبراير" وقد كان لهذه الصفحة دور هام في تعزيز ثورة 17 فبراير .

إنَّ وسائل التواصل الاجتماعي باتت تمثل أهم الأدوات التي يتم توظيفها في إدارة الصراعات والأزمات الدولية، سواء من خلال بث الإشاعات الاقتصادية والسياسية والعسكرية التي يمكن أن تزلزل اقتصادات دول كبيرة، كالإشاعات التي تروج حول شركات عابرة للقارات فتؤدي تلك الإشاعات لتدهور أسهمها في البورصة، أو من خلال نقل أخبار بعينها عبر مواقع تجسس، أو مواقع ناقلة لمعلومات سرية مثل "**ويكليكس**" لإثارة الخلافات بين الدول، أو تكريس الانقسامات داخل الدول ومؤسسات الحكم فيها. ولهذا فإن من يمتلك آليات توظيف وسائل التواصل الاجتماعي يكون أكثر قدرة على تحقيق أهدافه والتأثير في سلوك الفاعلين الآخرين (خليفة، 2014، ص7).

على مدى أربعة عقود، كان نظام القذافي هو المصدر الوحيد للمعلومات في ليبيا. كانت المعلومات شحيحة، واعتاد الناس على تلقي ما يحتاجون لمعرفته من مصدر واحد. عندما انفتحت الأمور بين عامي 2011، 2013 لم تكن هناك مؤسسات أو منشآت للحقائق الموثوقة، كان لدى بعض الوكالات الحكومية صفحتان أو ثلاث صفحات على فيسبوك، وكان من المستحيل معرفة أيٍ منها هو الشرعي. تعرض العديد من المواطنين لفيض من المعلومات التي كان من الصعب فرزها. توقفت بعد فترة وجيزة عملية تطوير وسائل إعلام رقمية محلية موضوعية بسبب صعود الجماعات المسلحة، التي أرهبت الأصوات المستقلة لمنع المعلومات واحتكارها بالطريقة التي اعتاد عليها الليبيون في عهد القذافي. في ظل هذه البيئة، ازدادت حدة المعلومات المضللة والمسببة للتنافر على وسائل التواصل الاجتماعي بشكل خاص. غالبًا ما كانت تتم برمجة خوارزميات الوسائط الاجتماعية لإيصال المستخدمين إلى محتوىً يشبه ما يحبونه أو يتابعونه بالفعل. وهذا يعني أنه في المساحات الرقمية التي تطغى عليها مصادر المعلومات المنحازة أو المزيفة، يمكن أن تؤول تجارب المستخدمين عبر الإنترنت بسهولة إلى غرف صدى رقمية دون الكثير من التنوع أو المعلومات الموثوقة.

كيف تؤثر المعلومات المضللة على المجتمع الليبي؟

لقد أدى تأثير هذا الوضع – حيث ينتهي الأمر بالعديد من مستخدمي الإنترنت الليبيين إلى نفق مظلم من المعلومات المضللة وغرف صدى حيث تتزاحم الأصوات المحلية مع حسابات مزيفة – إلى تأجيج التنافر في المجتمع الليبي، فتجربة وسائل التواصل الاجتماعي لشخص يعيش في جنوب ليبيا مختلفة تمامًا عن تجربة شخص يعيش في الغرب أو الشرق،

فكل منهم يرى العالم بشكل مختلف تمامًا عن الآخر من خلال تجربته الرقمية، وبعض الأشخاص يعرف كيفية الالتفاف حول هذا الأمر والعثور على أصوات أخرى، لكن الكثير من الناس سئموا من الافتقار إلى المعلومات الموثوقة وأصيبوا بجنون الريبة وفقدوا الثقة في جميع المعلومات خارج الحي الذي يقطنون فيه أو مجموعات وسائل التواصل الاجتماعي المحلية، والتي غالبًا ما تكون الطريقة الوحيدة للحصول على معلومات حول ما يجري حاليًا، حيث برز بعض الأشخاص كمصادر موثوقة في أحد الأحياء أو البلدات، أطلق عليهم اسم "حلقات الوصل"، فهم المسؤولون عن نشر المعلومات لمجتمعهم.

ولكن ماذا سيحدث بعدئذٍ إذا كان هذا الشخص أو هذه الهيئة منحازة فبمجرد أن يكتسب هؤلاء الأشخاص متابعين لهم على منصاتهم، يمكن في كثير من الأحيان أن يتم اختيارهم للنشر نيابة عن جماعة مسلحة أو حملة سياسية مقابل أجرة. لذلك يصبح كل شيء بعدها مشوهًا ونرجع إلى نموذج القذافي ولكن على نطاق محلي للغاية، كما يتوافر على بعض مواقع التواصل الاجتماعي وجود محتوى يحرض على البغضاء الحقيقية تجاه الأشخاص في مختلف مناطق البلاد ويعزز العمى العاطفي، حيث لا يرغب الناس حتى في الاستماع إلى الجانب الآخر لأن كل ما يقولونه هو خطأ، كل ما يقولونه شر. تعتبر قوة روايات التنافر هذه هي الأبرز نظرًا للغة والدين المشتركين بين الجماعات الليبية المختلفة. إن شيطنة المعارضين السياسيين ستصبح عقبة كبيرة أمام أي نوع من الحوار السياسي أو الجدل في المستقبل.

في 26 أكتوبر 2021، صدّق مجلس النواب الليبي على قانون مكافحة الجرائم الإلكترونية، في وقت استثنائي في ليبيا؛ إذ من المتوقع إجراء انتخابات رئاسية يوم 24 ديسمبر، وسيكون من الضروري ضمان حرية الرأي والتعبير والصحافة، بما في ذلك في الفضاء الإلكتروني، حتى يتسنى لهذه الانتخابات أن تكون حرة ونزيهة وشفافة.

تمت مواجهة هذا القانون بالرفض من العديد المنظمات، والتي بلغ عددها حوالي 31 منظمة، وعند مراجعة لتلك المنظمات ، وجد الباحث أن هناك العديد منها ليس ليبي المنشأ، ولا توجد مواقع إدارتها داخل ليبيا بل أن منها ما هو في الولايات المتحدة الأمريكية، وسويسرا، وبرلين، ومصر، ولندن، هذا الأمر يعتبر غير صائب لأن المستفيد من هذا القانون هو ليبيا، وإن تدخل هذه المنظمات في الاعتراض على القانون لا يعطيها الحق، فهذا القانون وضع وذلك للحد من الأثار السلبية لاستغلال مواقع التواصل الاجتماعي والفضاء

الإلكتروني، والتي تنصب في الأخير على حماية السيادة الليبية، وعدم وجود مشاكل سياسية و إقليمية، واجتماعية، وفيما يلي أسماء تلك المنظمات ومواقع إداراتها (الجدول 5):

الجدول (5) المنظمات الغير ليبية والتي تعارض قانون مكافحة الجرائم الإلكترونية الصادر عن البرلمان الليبي

ت	أسم المنظمة	الرابط الإلكتروني	موقع المنظمة
1	أكساس ناو	https://www.accessnow.org/	واشنطن ، نيويورك ، برلين
2	مراسلون بلا حدود	https://rsf.org/	باريس
3	منا لحقوق الإنسان	https://www.menarights.org/	جنيف
4	منظمة التخوم الإلكترونية	https://www.eff.org/	غير محددة المكان
5	مؤسسة البيرو الإلكترونية	https://elbiro.net/	تأسست بعد صدور قانون الجرائم في البرلمان الليبي حيث تأسست في شهر يناير 2022
6	سمكس	https://smex.org/	غير محدوده الموقع
7	إمباكت الدولية لحقوق الإنسان	https://impactpolicies.org/	لندن
8	المرصد الأور متوسطي لحقوق الإنسان	https://euromedmonitor.org/	جنيف
9	مركز القاهرة لدراسات وحقوق الإنسان	https://cihrs.org/	القاهرة
10	منظمة رصد الجرائم الليبية	https://libyancrimeswatch.org/	لندن

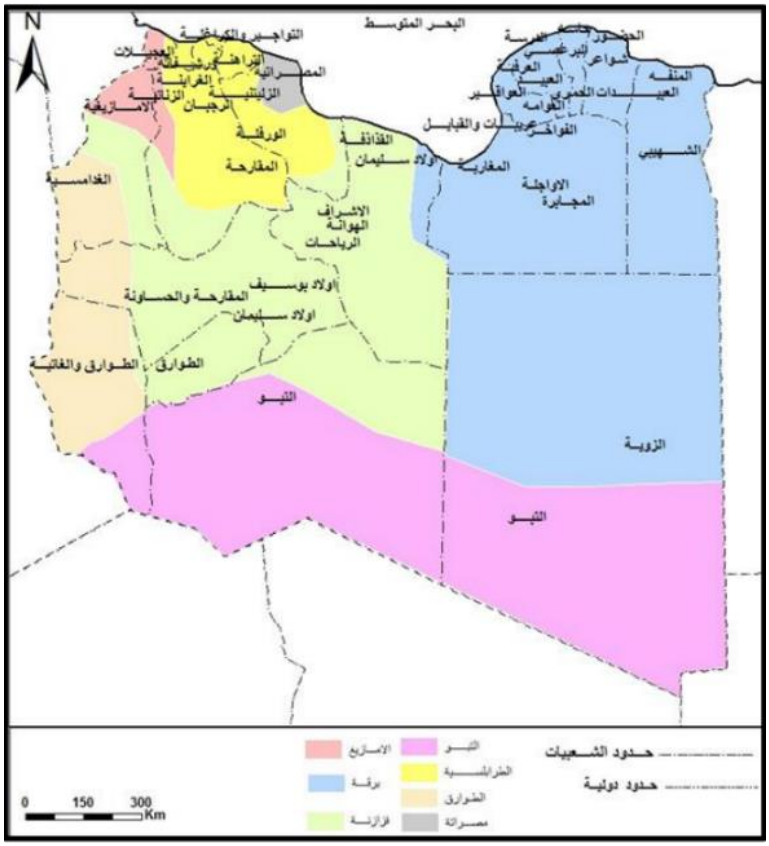
المصدر : ليبيا قانون مكافحة الجرائم الإلكترونية يهدد بتقييد حرية التعبير على الرابط:
https://ifex.org/ar/libya-cybercrime-law-threatens-to-restrict-free-expression/

شهد تاريخ ليبيا السياسي عبر العقود الماضية العديد من التعقيدات، فهي دولة تم تكوينها عبر اتحاد ثلاث أقاليم جغرافية وهي برقة وطرابلس وفزان، كما أنها دولة يوجد من بين سكانها العديد من الأقليات سواء الأمازيغية أم التبو أم الطوارق، وإن كان المذهب الإسلامي فيها واحد ولا يوجد دين غير الدين الإسلامي هو السائد في الدولة، إلا أن الأحداث خلال السنوات الماشية والحروب التي حدثت بين الشرق والغرب، عدا عن أنها دولة تسود فيها القبائل وتنتشر في أغلب أرجاء ليبيا .(الشكل 15)

كذلك فإن ليبيا لديها العديد من المشاكل الجيوبولتيكية التي تنعكس على الحجم السياسي للدولة، فهي تحمل مشاكل إقليمية عديدة ومعقدة، وتحتاج دائماً أن توضع في حساب التخطيط السياسي الناجح، وهي هامشية المعمور والتشتت الطبيعي والثنائية الإقليمية، والتي في وجود فضاء سيبراني غير آمن ستكون عرضه للعديد من الهجمات السيبرانية، والتي كان أشدها خلال أحداث عام 2018-2019 ما بين الحكومة المؤقتة في الشرق، وحكومة الوفاق في الغرب، حيث تم اعتبار هذه الحرب هي حرب إقليمية بين شرق

البلاد وغربها، حيث تم استخدام مواقع التواصل الاجتماعي في تأجيج الأعمال والدعوة للانفصال بين شطري البلاد .

الشكل (15) التوزيع الجغرافي للقبائل الليبية.



المصدر : فرج عبدالعزيز نجم ، القبيله والإسلام والدولة ، مكتبة الدعوة بالأزهر ، القاهرة ، 2005 ، ص 263.
السنوسي مُحَمَّد الغزالي ، برقة قديماً وحديثاً ، دار الكتاب الليبي ، بنغازي ، 1973 ، ص 180.

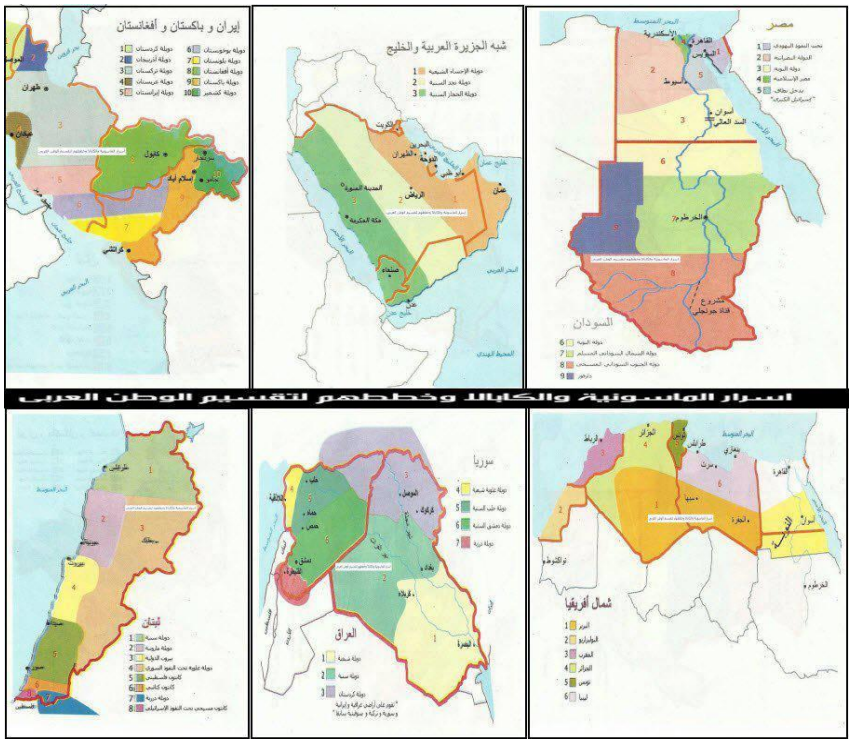
كذلك يجب أو يوضع في الحسبان، الدعوات والدراسات والخطط الاستراتيجية التي تم وضعها من قبل العديد من الباحثين الأوربيين والأمريكان والإسرائيليين والداعية إلى تقسيم دول الوطن العربي إلى دويلات قزمية، حيث تم دراسة تقسيم ليبيا إلى عدة دويلات، والتي يعود بداية التقسيم منذ مشروع بيفن /سفورزا، وأكثرها دعوة للتقسيم هي دراسة برنارد لويس والذي قام فيه بوضع تقسيم لليبيا إلى عدد من المناطق وهي (الجوجري، ب.ت، ص6-7):

1- دولة البربر: على امتداد دويلة النوبة بمصر والسودان.

2- دويلة البوليساريو .

3- الباقي دويلات ليبيا والمغرب والجزائر. (الشكل 16)

الشكل (16) تقسيم دول الوطن العربي حسب تقسيم برنارد لويس.



المصدر: عادل الجوجري، برنارد لويس سياف الشرق الأوسط ومهندس سايكس بيكو 2، دار الكتاب العربي، القاهرة، (ب.ت)، ص 233-237.

منذ أحداث 17 فبراير عام 2011، والتي لعبت فيها العديد من صفحات التواصل الاجتماعي – ومن أهمها فيس بوك – دوراً رئيساً في القضاء على النظام السابق، ولكن بعد ذلك أصبحت ليبيا مقسمه إلى العديد من الأقاليم، والتي نادت كل منها بإعادة أمجاد تاريخها السابق، ورفعت أعلام خاصة بأقلياتها ولا سيما في غرب البلاد وهم قبائل الأمازيغ، أو رفعت علمها التاريخي مثال برقة في شرق ليبيا، كذلك تعرض جنوب ليبيا إلى العديد من عمليات التهجير من سكان دولة تشاد في جنوب ليبيا، ومنها تهجير سكان مدينة مرزق منذ الهجوم من قبل داعش ومرتزقة تشاديين بتاريخ 23 أغسطس 2019،

والتي تزامنت مع هجوم جيش الحكومة المؤقتة على مدينة طرابلس ضد حكومة الوفاق الوطني، والتي أدت إلى تهجير ما يقارب 5000 أسرة ليبية من منطقة مرزق (الحوني، في ذكرى التهجير)، وبهذه القرائن السياسية المتعلقة الجيوبولتيكيا الليبية نجد أنه قد بدأت تتحقق معطيات ورغبة تقسيم ليبيا من قبل الدول التي قامت بوضع مخططات لتقسيم البلاد، وقد تزامنت تلك الأحداث للدعوات للتقسيم عبر الفضاء السيبراني بظهور العديد من الصفحات والتي تنادي كل منها للانفصال سواء على حسب الهوية أو على حسب الإقليم الجغرافي أو على حسب الانتماء العرقي.

عدا عن استخدام هذه الصفحات للجوانب السياسية، إلا أنه قد تم استخدامها أيضًا من المجموعات الإرهابية وذلك لبث الرعب في نفوس الليبيين، وذلك من خلال ما تقوم به من عرض لبعض أفلامها المرئية والتي تصور عمليات الإعدامات والقتل من قبل الجمعات الإرهابية، حيث قامت بعرض لعمليات إعدامات في كل من مدينة درنة ومدينة سرت، وغيرها من الأماكن المتفرقة في ليبيا، وذلك لمحاولة منها لتخويف المواطنين وارهابهم لغرض إخضاعهم ورضوخهم لهم بدون أي مقاومة.

النتائج :

1. ليبيا معرضة للعديد من المخاطر وخصوصاً وأنها ضمن خريطة التقسيمات السياسية والتي تم وضعها في العديد من النظريات العالمية لتفتيت المنطقة العربية، ويعتبر فضاؤها الجيوسبراني في خطر بسبب الحروب السائدة بها وضعف القيادة السياسية وتعددها .
2. إنَّ الجغرافيا السياسية للدولة لها أهمية خاصة في مواجهة التهديدات المتعلقة بالأمن السيبراني.
3. تعتبر الحروب السيبرانية ساحة الحرب الخامسة، وتتميز باستخدام أسلحة غير مرئية لها قدرات عالية ومنخفضة التكلفة بالنسبة للحروب التقليدية.
4. تعتبر الدول النامية والدول العربية من أكثر الدول تعرضاً لخطر الحروب الإلكترونية وذلك بسبب عدم امتلاكها لصناعة الالكترونات وعدم السيطرة لديها على الأنترنت في العالم.
5. نتيجة للتطور السيبراني في العالم تعرضت العديد من الدول إلى خسائر مالية وعسكرية، وخصوصاً في الدول التي ليس لديها أي حماية أمنيه سيبرانية.

6. نتيجة للتطور في المجال السيبراني أصبحت الحروب أكثر تطوراً وأقل خسائر.
7. نتيجة لتطور شبكات الإنترنت أصبحت الدول الضعيفة في دفاعها السيبراني وعدم وجود أي حماية لفضائها الجيوسبراني من أكثر الدول المستهدفة، وخصوصاً الدول التي تمر بأزمات سياسية وعسكرية.
8. يعتبر الشباب من أكثر من يتم استهدافهم في مواقع التواصل الاجتماعي لبث الأفكار السياسية والمعادية.
9. تعتبر ليبيا من الدول المستهدفة؛ وذلك بسبب النظام القبلي بها، وتعدد العرقيات، وضعف الأمن والدفاع السيبراني لديها، وتوفر العديد من المقومات الاقتصادية.
10. بالرغم من صدور العديد من القرارات والخاصة بالحماية السيبرانية في ليبيا، إلا أن ترتيبها عربياً وأفريقياً لايزال متأخرًا.

التوصيات :

1. ينبغي على الدول التعاون فيما بينها من أجل الحصول على فضاء آمن.
2. يجب على ليبيا أن تعزز دفاعها وتدابيرها الوقائية، وذلك لضمان استقرارها مستقبلاً وابتعادها عن أي عمليات سيبرانية تهدد مستقبل جغرافيتها وتماسكها.
3. يجب وضع العديد من البرامج لحماية فضائها السيبراني، وذلك عن طريق بناء القدرات البشرية الماهرة في الدفاع والحماية السيبرانية، وذلك لخطورتها وسهولة تغلغلها في ليبيا.
4. على الدول العربية عقد اتفاقيات وتفعيلها لحماية فضائها العربي؛ وذلك بسبب عدم قدرتها على امتلاك تقنية الإنترنت في العالم.
5. العمل على حماية وأمن وسرية البيانات والمعلومات والشبكات الخاصة، وخصوصاً البنكية.
6. لا يوجد أي جهات في ليبيا فاعلة حتى يمكن تتبع عدد الجرائم الإلكترونية التي حدثت، حيث أن دولة الإمارات وبالرغم من تقدمها، إلا أنها لم تستطيع السيطرة على فضائها السيبراني.
7. ضرورة العمل على تحقيق أمن جماعي عالمي، وذلك من أجل حماية الدول من الحروب الإلكترونية والإرهاب الإلكتروني، وعدم استخدام الفضاء السيبراني كساحة حرب جديدة.

المصادر والمراجع:

- أبو الحسن، مُحَمَّد حسين، (2022)، معركة "النفط الجديد" في "أرض الظلام"... الحروب السيبرانية ترعب العالم! النهار العربي على الرابط:
https://www.annaharar.com/arabic/makalat/opinions/22062021072926144 بتاريخ 2022/01/16 الساعة 11:45
- اسماعيل، قادير، (2007)، إدارة الحروب التقنية في الفضاء الإلكتروني، الاستراتيجية الأمريكية الجديدة في الشرق الأوسط، الندوة الدولية: عولمة الإعلام السياسي وتحديات الأمن القومي للدول النامة، قسم العلوم السياسية كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ن الجزائر (7 مارس 2007).
- أمين، أميل، (2020)، الأمن السيبراني العالمي ... حروب خلفية ومساحات إرهابية، موجود على الرابط: https://www.independentarabia.com / node/93586/ الأربعاء 12 فبراير 2020.
- أوكرانيا تكرّر اتهام روسيا بالهجوم الالكتروني وتؤكّد أن لديها "أدلة، الرابط:
https://www.france24.com/ar، نشرت في 16:06 – 16/01/2022
- بدران، عباس، (2010)، الحرب الإلكترونية .. الاشتباك في عالم المعلومات، بيروت.
- بن عبدالرحمن، صالح بن علي، (2017)، الأمن الرقمي وحماية المستخدم من مخاطر الأنترنت، رؤية 2030، هيئة الاتصالات وتقنية المعلومات، السعودية.
- بيتر بي سيل، ترجمة: ضياء داوود، (2017)، الكون الرقمي: الثورة العالمية في الاتصالات، مؤسسة هنداوي سي أي سي، المملكة المتحدة.
- تيلور، بيتر، فلنت، كولن، (2002)، الجغرافيا السياسية لعالمنا لمعاصر، سلسلة عالم المعرفة، العدد 282، مطابع السياسة، الكويت.
- جبور، منى الأشقر، (2012)، الأمن السيبراني :التحديات ومستلزمات المواجهة، المركز العربي للبحوث القانونية والقضائية.
- الجوجري، عادل، (ب ت)، برنارد لويس سياف الشرق الأوسط ومهندس سايكس بيكو 2، دار الكتاب العربي، القاهرة.
- خريسان، باسم على، (2021)، الأمن السيبراني في العراق: قراءة في مؤشر الأمن السيبراني العالمي 2020، العراق، بغداد ، مركز البيان للدراسات والتخطيط.
- خليفة، أيهاب، (2014)، القوة ألإلكترونية : كيف يمكن أنتدير الدولة شئونها في عصر الأنترنت " الولايات المتحدة نموذجاً "، العربي للنشر والتوزيع، القاهرة.
- خليفة، أيهاب، (2017)، القوة الإلكترونية وابعاد التحول في خصائص القوة، الإسكندرية، مطبعة الإسكندرية.

- رفيق، عادل، (2018)، الجيوبولتيكس السيبرانية – الاستقرار في الشرق الأوسط، المعهد المصري للدراسات، ترجمات، 1 يناير 2018 .

- شلوش، نورة، (2018)، القرصنة الإلكترونية في الفضاء السيبراني " التهديد المتصاعد من الدول"، مجلة مركز بابل للدراسات الإنسانية، مجلد 8 ، العدد 2 ، جامعة بابل.

- طاله، لامية، (2020)، التهديدات والجرائم السيبرانية: تأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها، مجلة معالم للدراسات القانونية والسياسية، المجلد 4 ، العدد 2 .

- عبدالصادق، عادل، (2009)، الإرهاب الإلكتروني: القوة في العلاقات الدولية " نمط جديد وتحديات مختلفة"، مركز الدراسات السياسية والاستراتيجية بالأهرام، القاهرة.

- عبدالصادق، عادل، (2013)، الفضاء الإلكتروني والرأي العام : تغير المجتمع والأدوات والتأثير، المركز العربي لأبحاث الفضاء الإلكتروني، قضايا استراتيجية، العدد 2459.

- عبدالفتاح، فاطمة الزهراء، (2017)، التشارك الإلكتروني: آليات مكافحة الشائعات في الفضاء السيبراني. https://futureuae.com/ar-/Mainpage/Item/2841

- علي، نسرين الشحات الصباحي، (2016)، الأبعاد العسكرية للقوة السيبرانية على الأمن القومي للدول، دراسة حالة إسرائيل منذ عام 2016، المركز الديمقراطي العربي، 29 أبريل 2016 .

- الغزال، السنوسي مُحَمَّد، (1973)، برقة قديماً وحديثاً، دار الكتاب الليبي، بنغازي.

- فرج، فاطمة منصور، (2021)، دور مواقع التواصل الاجتماعي في نشر وتداول الشائعات المتعلقة بجائحة كورونا " دراسة ميدانية على عينة من مستخدمي مواقع التواصل الاجتماعي بمدينة سرت/ ليبيا)، مجلة جامعة سرت، العدد الثاني، ديسمبر 2021 .

- محمود، خالد وليد، (2013)، الهجمات عبر الانترنت، ساحة الصراع الإلكتروني الجديدة، سلسلة دراسات، دراسات سياسية، المركز العربي للأبحاث، قطر.

- المزروعي، مثنى مشعان، (ب ت)، جدلية العلاقة بين الجغرافية السياسية والفضاء الإلكتروني "رؤية جغرافية سياسية"، بحث مستل عن أطروحة الدكتوراه الموسومة (الصراع الجيوستراتيجي الأمريكي – الروسي في الفضاء الإلكتروني للطالبة ابتسام عبد الزهرة العقابي، جامعة بغداد ، كلية التربية للبنات، قسم الجغرافية. موجود على الرابط:
https://www.researchgate.net/publication/332209274_jdlyt_allaqt_byn_aljghrafyt_alsyasyt_walfda_alalktrwny

- المشهدي، تغريد معين حسن، (2019)، اثر العسكري للأمن السيبراني في الجغرافيا السياسية للدولة، مجلة البحوث الجغرافية، العدد 30 ، المجلد الأول.

- نجم، فرج عبدالعزيز، (2005)، القبيله والإسلام والدولة، مكتبة الدعوة بالأزهر، القاهرة.

- هادي، سهيلة، (2017)، الحرب الإلكترونية في ظل عصر المعلومات، رؤى إستراتيجية ، يونيو.

– الهيئة العامة للاتصالات والمعلوماتية، تقرير المؤشرات المحلية، مؤشرات الأسرة والفرد، ملخص لمشروع مشترك مع مصلحة الإحصاء، نتائج مسح تقنية المعلومات والاتصالات، من الرابط:
. https://www.cim.gov.ly/local-indicators
– الحكومة المؤقتة، قرار 23 لسنة 2013.
– الاتحاد الدولي للاتصالات، مؤشر الأمن السيبراني العالمي، 2017.
– ليبيا قانون مكافحة الجرائم الإلكترونية يهدد بتقييد حرية التعبير على الرابط:
https://ifex.org/ar/libya-cybercrime-law-threatens-to-restrict-free-expression/

- Carlos Exk, 2017, The World Evolves, Copenhagen, translation, Raffi Adorard, 2018.
- Martin Dodge, The Geography of Cyberspace, paper 8, Centre for Advanced Spatial Analysis, University College London, London,1999.
- Eischen, E. T. &. K. , The Geography of Cyberspace. M/C: A Journal of Media and Culture,2003.
- John O Loughlin, Geography as space and geography as place: The divide between political science and political geography continues, Institute of Behavioral Science and Department of Geography , University of Colorado.
- Paul W. Phister Jr, Cyberspace: The Ultimate, Complex Adaptive System, The International C2 Journal | Vol 4, No 2, Focus & Convergence for Complex Endeavors ,2010-2011.
- WANG Limao, M. Changes in driving forces of geopolitical evolution and the new trends in geopolitics studies[J]. Geographical Research, 2016 , 35 (1).
- Michael Sentonas, Cybercrime, the new tool in geopolitics VP Technology Strategy at Crowd Strike, Michael Sentonas (CSO Online) on 01 February, 2018.
- Aleksander Klaic ,A Method for the Development of cyber Security Strategies Information & Security : An International Journal , I&S Volume 34 (2015).
- Lean Hansen –Helen Nissenbaum ,Digital Disaster ,Cyber Security and the Copenhagen School ,International Studies Quarterly (2009),53,1155-1175.
- Gregory J. Rattray, An Environmental Approach to Understanding Cyber power .USA.
- Adversarial Threat Report,2021 .