أثر نشر المحتوى السلبي عبر الفضاء السيبراني على استقرار المجتمع السوداني

د. أنس علي بله علي

أستاذ تقانة المعلومات المساعد – كلية علوم الحاسوب وتقانة المعلومات
جامعة كسلا

المستخلص:

لقد فرض علينا الواقع أساليب جديدة للتواصل وتبادل المعلومات والأفكار التي يقدمها المجتمع في شكل فوائد معلوماتية متنوعة عبر المنصات الالكترونية المنتشرة في الفضاء السيبراني (الاتصال الرقمي والمعاملات الالكترونية). ولكن قد تأتي هذه الفوائد مقترنة بالعديد من المهددات التي يمكن لها أن تنشأ في لحظة لتخلف أضراراً هائلة بالمناطق الحيوية في الدولة، وهذا الضرر المحتمل يتزايد بصورة مضطردة عند ارتباطه بوسائل التواصل الحديثة. قدمت هذه الورقة دراسة شاملة عن ما يتم نشره من مهددات في المحتوى عبر الفضاء السيبراني في المنصات الالكترونية المختلفة، بدايةً تم الوقوف على ايجابيات المحتوى السيبراني والاستفادة منها، ثم التعرف على الآثار المترتبة على مهددات المحتوى بالفضاء السيبراني والعديد من التغيرات والمشاكل التي بدأت تظهر على المجتمع السوداني بصورة متزايدة عبر الفضاء السيبراني، حيث تناولت الورقة الحرب السيبرانية وأثرها على البنية التحتية للبلاد، وكذلك السمات الفريدة التى تتسم بها الحرب السيبرانية إضافةً إلى النزاع السيبراني واسبابه وكيفية الحد منه عن طريق ارساء ثقافة السلام السيبراني، وذلك بنشر الوعي التقني من أجل خلق بيئة تقنية معافاة من كافة المضار التقنية التي تفتك بالمجتمع ونشر ثقافة الفضيلة والقيم النبيلة من أجل التعايش السلمي بين المجتمعات المختلفة، كما تناولت الورقة أهمية الاستقرار الجيوسيبرانى الذي يمكن من خلاله أن نصل الى السلام السيبراني، كما تحدثت الدراسة عن أهمية السلام السيبرانى وتأثير فضاء السايبر على الحروب وخصوصاً ما يدور فى السودان.

الكلمات المفتاحية: الفضاء السيبراني، الصراع السيبراني، السلام السيبراني، الاستقرار الجيوسيبرانى.

The Impact of Publishing Negative Content via Cyberspace on the Stability of Sudanese Society

Dr. Anas Ali Balla Ali

Abstract:

Reality has imposed new methods of communication and information exchange, offering diverse informational benefits through e-platforms prevalent in cyberspace(digital communication and electronic transactions). However, these benefits may come with numerous threats that can arise instantly, causing immense damage to vital areas of the state. This potential harm increases steadily when linked to modern communication technologies. This paper presents

a comprehensive study of the threats posed by online content across various e-platforms. It begins by highlighting the positive aspects of online content and how to leverage them. The paper then examines the consequences of cyber threats and the numerous changes and problems that have increasingly emerged in Sudanese society through cyberspace. It addresses cyber warfare and its impact on the country's infrastructure, as well as the unique characteristics of cyber warfare. The paper also explores cyber conflict, its causes, and how to mitigate it by establishing a culture of cyberpeace. This involves raising technological awareness to create a safe technological environment free from the harmful effects of technology on society and promoting a culture of virtue and noble values for peaceful coexistence among different communities.Furthermore, paper discusses the importance of geocyber stability as means to achieve cyberpeace. Finally, the study examines the significance of cyberpeace and impact of cyberspace on warfare, particularly in the context of conflict in Sudan.
Keywords: Cyberspace, Cyber Confl i ct, Cyber Peace, Geocyber Stability

1. المقدمة:

تعتبر شبكة الإنترنت حالياً الجهاز العصبي المركزي الذي يحرك المجتمع عبر الوسائل المتاحة لتكنولوجيا المعلومات والاتصالات. وأصبحت تعتمد عليها كل القطاعات والمجتمع فى العالم والتي تخضع لأنظمة رقابة إشرافية في البلدان المختلفة من أجل التحكم في المعلومات المنتشرة وحيازتها وغيرها من عمليات الإدارة لوسائل التكنولوجيا الحديثة المعقدة. حيث تعتمد الحكومات على وسائل تكنولوجيا المعلومات والاتصالات لتقديم الخدمات لمجتمعاتها وإدارة العمليات المختلفة عبر مناطق جغرافية متنوعة من أجل الحفاظ على السلامة العامة للدولة وحمايتها، ولقد ارتبط الإنترنت عضوياً بكل أعمال الحياة اليومية للمجتمع. وتؤدي المنصات المنتشرة عبر الفضاء السيبراني دوراً مهماً في مجالات العمل والتعلم والتسلية، كما تقوم شبكة الإنترنت بنشر مجموعة من المعارف والمعلومات المتنوعة بشكل غير مسبوق في تاريخ العالم عبر صفحات الكترونية منتشرة في الفضاء السيبراني، مما يخلق قوة من التشابك الاجتماعي الذي يربط بين الناس ويؤثر عليهم بطرق منفصلة تماماً عن الحكومات بطريقة لا تتوقعها. فقد أتاح الفضاء السيبراني تمكين الأفراد والجماعات في التوسع الذاتي ونشر العديد من الأفكار الغير مألوفة عن طريق آليات لا تتأثر بالحدود ولا الاعتبارات الدبلوماسية أو السياسية، مما يصعب اقتفاء أثرها إلكترونياً. وأصبح اليوم باستطاعة أي فرد أن يؤثر بصورة سريعة على المفاهيم والقيم والأفكار والمعتقدات من خلال قدرته على إنشاء محتوى مؤثر وتوزيعه على صعيد عالمي عبر الفضاء السيبراني[11].

لقد أصبح التهديد بالحرب السيبرانية حالياً يتزايد بصورة أكبر، وذلك لتوفر كل عوامل هذه الحرب التي أساسها المعلومات المنتشرة والمتداولة بصورة واسعة في مختلف المنصات الالكترونية التي لا تحكمها الحدود الجغرافية. ويقاس التقدم التكنولوجي الآن بربط كل المجتمعات في مختلف الجهات من خلال أنظمة الكترونية في بنية رقمية معقدة ومتشابكة. مما يستدعي زيادة الطلب على خدمات الإنترنت والتواصل الرقمي بإستمرار اعتماداً على تكنولوجيا المعلومات والاتصالات واندماجها في كل متطلبات الواقع، مثل خدمات الأفراد والمؤسسات والآليات والبنى التحتية بالاضافة إلى أنظمة المراقبة المختلفة، علاوةً على إمدادات الكهرباء وأنظمة النقل والخدمات واللوجستيات العسكرية، فكل هذه الخدمات المعاصرة تقريباً تعتمد بصورة كبيرة على استخدام تكنولوجيا المعلومات والاتصالات واستقرار الفضاء السيبراني[1]. ويعتبر الفضاء السيبراني البيئة الحيوية والمادية للعالم والذي يحوى جميع الأنشطة والأنظمة الالكترونية، والتي قد تزيد من انتشار الحرب سيبرانياً بصورة واسعة وعريضة النطاق لأنها حرب تجري في الفضاء السيبراني باستخدام وسائل تكنولوجيا المعلومات والاتصالات. إعتماداً على المنصات والأنظمة المنتشرة على الإنترنت والتي تضع موارد البلدان ومراكز قرارها في متناول هؤلاء الذين يسعون إلى إحداث الفوضى في الحكومة وبين السكان المدنيين. لذلك فإن تعزيز الأمن السيبراني وحماية البنية التحتية الخاصة بالمعلومات الحساسة تمثل عناصر حيوية في أمن كل دولة وحمايتها. وقد أظهر الاستخدام السيء للفضاء السيبراني العديد من الصراعات والحروب التي دمرت الشعوب نتيجة لتداول المعلومات بصورة سلبية تحمل في طياتها كل أساليب التهديد عبر المحتوى السيبراني، والذي يعتبر الشرارة التي تقود المجتمعات للدخول في نزاعات كبيرة تقضي على جميع مظاهر الحياة بالدولة، وللحد من ذلك كان لابد من أن يطال السلام السيبراني المجتمعات وجميع المجالات العسكرية والاقتصادية والاجتماعية والسياسية والانسانية، من أجل بناء منظومة معلوماتية معافاة من كل المهدات السيبرانية والحفاظ على سلامة المعلومات المتداولة عبر الفضاء السيبراني.

2. مشكلة الورقة:

عند النظر لواقع الحال الآن، يقدم المجتمع فوائد معلوماتية متعددة عبر المنصات الالكترونية المنتشرة في الفضاء السيبراني، ولكن هذه الفوائد قد تأتي مقترنة بتهديدات سيبرانية يمكن لها أن تنشأ في أي زمان وأي مكان لتسبب ضرراً هائلاً بالأماكن الحيوية في لحظتها. وهذا الضرر من المحتمل أن يتزايد بصورة مضطردة عند ارتباطه بوسائل التكنولوجيا الحديثة والاتصالات سريعة الانتشار، عليه تتمثل مشكلة هذه الورقة فى دراسة تزايد مهددات المحتوى السلبي بالفضاء السيبراني وكيفية الحد منها من خلال نشر وترويج ثقافة السلام السيبراني.

3. أهداف الورقة:

التعرف على الآثار الايجابية والسلبية لاستخدام وسائل تكنولوجيا المعلومات الحديثة على المجتمع الآن.

دراسة آثار المحتوى السلبي بالفضاء السيبراني والتعرف على اتجاهاتها في ظل الحرب بالسودان.

تحديد الآثار الناتجة من صراع المحتوى المنتشر بالفضاء السيبراني عبر المنصات الالكترونية المختلفة.

التعريف بمفهوم السلام السيبراني ونشر ثقافته، وتثبيت مبدأ السلوك السلمي للمحتوى بالفضاء السيبراني.

وضع خارطة طريق مستقبلية لنشر وترويج ثقافة السلام السيبراني للحد من النشر السلبي عن الواقع.

4. أهمية الورقة:

الحد من الاستخدام السلبي للتقنيات الحديثة للمعلومات والمنصات الالكترونية المنتشرة عبر الفضاء السيبراني لتقيل اضرارها على المجتمع.

التغلب على أسباب نشر المحتوى السلبي بالفضاء السيبراني واتجاهاتها والتغلب عليها.

معرفة مسببات صراع المحتوى بالفضاء السيبراني المنتشر عبر المنصات الالكترونية المختلفة والحد منها

نشر ثقافة السلام السيبراني من خلال الترويج للقيم النبيلة والمحتوى الايجابي عبر الفضاء السيبراني.

5. منهجية الورقة:

تقوم هذه الورقة على دراسة وتحليل ما يتم نشره من محتوى عبر الفضاء السيبراني سوى كان سلبياً أو ايجابياً في المنصات الالكترونية المختلفة، وذلك بغرض الوقوف على ايجابيات هذا المحتوى بالفضاء السيبراني والاستفادة منها اضافة إلى دراسة وتحليل مهددات نشر المحتوى السلبي بالفضاء السيبراني والتعرف على اسبابها وكيفية الحد منها عن طريق ارساء ثقافة السلام السيبراني وذلك بنشر الوعي التقني والاستخدام الايجابي لوسائل التكنولوجيا الحديثة من أجل خلق بيئة تقنية معافاة من كافة المضار التقنية التي تفتك بالمجتمع ونشر ثقافة الفضيلة والقيم النبيلة من أجل التعايش السلمي بين المجتمعات المختلفة.

6. الفضاء السيبراني: Cyberspace:

هو المجال الافتراضي الذي اكتشفه الانسان عند استخدامه للحاسبات عبر شبكة الانترنت التي يتم فيها تبادل الكم الهائل من البيانات والمعلومات، ويعتبر الفضاء السيبراني البيئة الخصبة لصراع الجيوش الحديثة[2]، كما عرفته وكالة أمن أنظمة الاعلام(ANSSI) على أنه: «فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للبيانات الرقمية»[12]، وعرفه الاتحاد الدولي للاتصالات بأنه: «المجال المادي وغير المادي الذي يتكون وينتج عن عناصر أجهزة الحاسوب، الشبكات، البرمجيات، حوسبة المعلومات، المحتوى، بيانات النقل والتحكم، ومستخدموا كل هذه العناصر»[13].

ووفقاً للتعريفات السابقة نخلص إلى أن الفضاء السيبراني هو مجال تفاعل افتراضي حديث يعتمد على مجموعة من الأجهزة الرقمية والبرمجيات والشبكات وانظمة الاتصالات ومستخدموا هذه الأجهزة وخلق بيئة تفاعلية افتراضية يتم فيها التواصل وتبادل البيانات والمعلومات. وتقوم البيئة الإفتراضية التي تتفاعل فيها العناصر المادية والبرمجية بخلق تواصل بين كل أجزاء العالم عن

طريق الشبكات الالكترونية المترابطة وذلك بغرض تبادل المعلومات المتنوعة. ويتميز هذا الفضاء بالتنوع والتجانس والمرونة ولايتقيد بالحدود الجغرافية حيث يسمح للكل بالدخول فيه دون قيود وفي أي لحظة. [3] ويعتبر الفضاء السيبراني العنصر الرئيسي في تسيير دولاب العمل في الدول المتقدمة، ويمثل العنصر الفاعل الذي لايمكن الاستغناء عنه لما له من مزايا عديدة، بالإضافة لأهميته في المجال العسكري الاستراتيجي، وذلك لتطور أدوات القتال في الحروب في هذا العصر، حيث يمكن الفضاء السيبراني من إدارة العمليات العسكرية بواسطة الأنظمة المعلوماتية المترابطة مع بعضها البعض، وإدارة العمليات القيادية التي تجمع بين الهجمات الالكترونية والعادية للجهة المعادية وتعطيلها. [4]

7. محتوى الفضاء السيبراني:Cyberspace Content:

محتوى الفضاء السيبراني هو مجموعة من عناصر المعلومات المستخدمة عبر أجهزة الفضاء الرقمية والتي يتم انشاؤها في شكل(نصوص، أصوات، صور، فيديوهات، أشكال متحركة) ليتم تبادلها ونقلها عبر الشبكات، ويتضمن المحتوى المنشور عبر الفضاء السيبراني مجموعة من البيانات والانظمة التشغيلية التي تكون في شكل ملفات معلوماتية متنوعة يتم تشغيلها داخل الأجهزة الرقمية بغرض تبادلها عبر الشبكات لتحقيق اغراض محددة.

1.7 المحتوى السلبي بالفضاء السيبراني:

يتضمن المحتوى السلبي بالفضاء السيبراني بعض الأنشطة السلبية الضارة كنشر المهددات والهجمات والبرامج الخبيثة، ويقوم الأمن السيبراني بحماية بيئة هذا المحتوى من كافة التهديدات ومواجهتها عبر تقنيات أمنية متخصصة. ومن أمثلة مهددات نشر المحتوى السلبي بالفضاء السيبراني نذكر:

نشر فيروسات البرامج الضارة Malware :

التصيد والاحتيال Phishing بخداع المستخدمين للحصول على معلوماتهم الحساسة عبر تطبيقات الاحتيال العاطفي والمادي.

التهديد والابتزاز بنشر صور خاصة مقابل مبلغ من المال.

مخططات الاحتيال الوهمية، لاختراق الحسابات، وسرقة البيانات.

2.7 تداول معلومات المحتوى السلبي وتأثيرها على الحرب في السودان:

منذ اندلاع الحرب في أبريل2023، أصبحت المجالات السياسية واالاقتصادية والصحية والاجتماعية في السودان غارقة في التضليل الإعلامي وخطاب الكراهية وغيرهما من أشكال المعلومات الضارة. هذه التحركات ليست منفصلة عن العنف على الأرض بل تتشابك معه بشكل عميق، وغالباً ما تصاحب أو تتبع الهجمات على البنية التحتية المدنية التي تشنها القوات المسلحة السودانية(الجيش السوداني) وقوات الدعم السريع. وكثيراً ما تعكس موجات نشر الروايات الضارة على وسائل التواصل االجتماعي هذه الأعمال العنيفة أو تعمل على تضخيمها، مما يؤدي إلى إثارة الإرتباك والخوف وانعدام الثقة بين المجتمعات.

قدمت Canada Grand Challenges في عام 2024 مجموعة أبحاث حول آثار المعلومات الضارة في سياقات أخرى كالأوبئة والانتخابات وأزمات المناخ، مما يترك فجوة حرجة في فهم دورها

والاستجابة لها في البيئات المتضررة من النزاعات وألأزمات الإنسانية، وفي عام2025 حددت اللجنة الدولية للصليب الأحمر أن العلاقة بين المعلومات الضارة والنتائج الإنسانية لا تزال غير مستكشفة بما يكفي، خاصة في البيئات الأكثر ضعفاً.

منذ بدء الحرب، واجهت وسائل الإعلام السودانية تحديات هائلة، بما في ذلك تدمير ونهب الموارد كما ذكرت جهات إعلامية مثل معهد الجزيرة للإعلام. ويواجه الصحفيون الاضطهاد والهجمات وحملات ممنهجة من الدعاية المضللة والكاذبة. وحسب تقرير مراسلون بلا حدود في العام 2025 فقد فر أكثر من 400 صحفي إلى الدول المجاورة مثل أوغندا وكينيا، وخاصة مصر، ومع ذلك فقد تم تأسيس أو مواصلة عمل ما لا يقل عن عشرة منافذ إعلامية سودانية في المنفى منذ اندلاع هذه الحرب قبل أكثر من عامين.

هناك معركة شرسة على النفوذ عبر الإنترنت، تحاكي تكتيكات مثل «التأييد الزائف» وهو الترويج لدعم طرف من أطراف الحرب من خلال شبكات من الحسابات المزيفة. ورغم أن هذه المعركة الرقمية على الاهتمام والتأثير قد تبدو مجردة إلا أن لها عواقب ملموسة في العالم الواقعي. فالهجمات المتعمدة عبر الإنترنت تستهدف بشكل متزايد مقدمي المساعدات الإنسانية، بما في ذلك مجموعات العون المتبادل، مما يجعل عملهم أكثر صعوبة وأقل أماناً. وردًا على ذلك، يتبنى العديد من الأشخاص استراتيجيات تواصل قائمة على تجنب المخاطر، فيختارون عدم الإعلان عن الخدمات علناً على حساب التأثير المحتمل بدلاً من المخاطرة بتعطيل العمليات وتعريض الأرواح للخطر. وتُظهر المشاورات المجتمعية التي أجرتها منظمة(Ground Truth Solutions غراوند تروث سوليشونز2025) في جنوب دارفور والقضارف، كيف تؤدي هذه التحركات إلى تفاقم التحديات الإنسانية؟. وفي حين يظل نقص المساعدات هو الشاغل الرئيسي للناس، فإن هذا الأمر يزداد سوءًا بسبب المعلومات المضللة ونقص المعلومات الموثوقة. وكما شهد أحد المشاركين في القضارف، «إن بعض النازحين لا يعرفون تاريخ التوزيع، وعندما يصلون إلى نقطة التوزيع، يجدون أن المساعدات قد نفدت».

3.7 الصراع السيبراني:

أوجد الفضاء السيبراني مساحات للتفاعل مع الواقع بطريقة افتراضية مختصراً حاجز الزمان والمكان، ثم ظهرت فضاءات جديدة للصراع عبر أدوات ووسائل تقنية متنوعة خلقت أنماط جيدة للصراع تختلف عن الصراعات التقليدية، ولعل ابرز ما يعزز انتشار الصراع في الفضاء السيبراني[5] :

اعتماد الناس بصورة متزايدة على استخدام المنصات الالكترونية المنتشرة عبر الفضاء السيبراني مع زيادة خطر تعرض البنية التحتية للمعلومات للهجوم السيبراني.

استخدام الهواة لهذا الفضاء السيبراني للتحدي وتحقيق اهدافهم يؤثر ذلك سلباً على سيادة الدولة. انسحاب الدولة من قطاعات استراتيجية كالاتصالات لصالح القطاع الخاص.

صعوبة تعامل الدولة مع العديد من مؤسسات نشر المحتوى السيبراني ذات القدرات العالية مثل(التيك توك، اليوتيوب، الفيسبوك، منصة اكس)، التي اصبحت فاعلة دولياً بصورة مبالغ فيها.

عليه فقد أصبح الفضاء السيبراني ساحة جديدة للصراع بصورة سيبرانية تعكس المشاكل التي تقع داخل الدول وخارجها والتي يخوض فيها مجموعة من الفاعلين ذوي الايدولوجيات المتعددة، وينتشر الصراع السيبراني من خلال شبكات الاتصالات والمعلومات التي أصبحت قادرة على تجاوز الحدود الجغرافية وسيادة الدولة.

الصراع السيبراني عادة ما يتم تحريكه بدوافع سياسية تأخذ طابعاً عسكرياً يتم فيه استخدام المحتوى بطريقة هجومية أو دفاعية عبر الفضاء السيبراني، كما يتحول الصراع السيبراني إلى طابع تنافسي عن طريق التأثير في المشاعر والأفكار بغرض الحصول على المعلومات الاجتماعية والاقتصادية والعلمية الخاصة والتحكم فيها، ثم العمل على اختراق الأمن القومي للدول والتأثير على الاقتصاد وتدمير البنية التحتية بنفس العمل الذي يحدث بالطريقة التقليدية. ويمكن استخدام الفضاء السيبراني كوسيلة للصراع داخل الدولة وبين مكوناتها على أساس قبلي أو طائفي أو ديني.

إن هذا التحول في نمط الصراع أوجد مهددات جديدة غيرت من طبيعة الصراع التقليدي وقواعد الاشتباك إلى صراع واشتباك سيبراني فرض على الواقع تحولات جذرية على العديد من المفاهيم المستخدمة في تنظيم قواعد الحرب ووسائلها وآلياتها مما فرض على الدول ايجاد أساليب جديدة تحد من انتشار هذا النوع من الصراع.

8. الحرب السيبرانية:

لقد شهد هذا العصر العديد من التطورات التقنية التي دمجت في الفضاء السيبراني واستخدمت في الصراعات الدولية، فظهرت حرب المعلومات والتي تعتبر من أهم العمليات العسكرية التي تدور في ميدان التكنولوجيا الحديثة لتشكل حرب ذات طابع سيبراني بين الدول، وجعلتها تواجه الآن نوعاً جديداً من الحروب التي تستخدم فيها طرق جديدة للقتال خارج أرض المعركة العادية وهي ما تسمى بالحروب السيبرانية، والتي برزت بظهور انتشار استخدام وسائل التكنولوجيا الحديثة والأنظمة المعلوماتية عبر الشبكات، وأصبحت تحتل مكانة بالغة الأهمية في واقع الدول، وتشكل دور أساسي في حفظ أمنها واستقرارها. [6] وتعني الحرب السيبرانية بالأفعال التي تقوم بها بعض الدول بإختراق نظم وشبكات المعلومات للدول الأخرى بغرض احداث الضرر والتخريب والتفكيك وتعطيل العمل. كما تعرف بأنها كل مخطط فردي أو جماعي يهدف للمساس بإلحاق الضرر على سلامة النظم المعلوماتية للمؤسسات والمنظمات أو الدول مما يؤدي إلى حدوث أضرار نفس الأضرار الناجمة عن استخدام القوة العسكرية المسلحة، وقد صنفت هذه الحرب السيبرانية إلى حرب سيبرانية هجومية ودفاعية واستخباراتية. [3]

تختلف الحرب السيبرانية عن الحرب العادية من حيث طريقة الصراع الذي يدار داخل الفضاء السيبراني، فهي تعتبر حروب تهدد وتستهدف المجالات الرقمية للدول بصفة مباشرة عن طريق شل وتعطيل النظم المعلوماتية المرتبطة بالمجالات الحيوية للدول المستهدفة بصورة غير ملموسة. [6]

1.8 سمات الحرب السيبرانية وأثرها:

رغم أن الحرب السيبرانية يمكن أن تُشبه في أبعادها الحرب التقليدية من عدة جوانب، لكن السمات الفريدة للفضاء السيبراني يمكن أن تُنشئ إلى جانب ذلك أبعاداً جديدة وغير متوقعة.

ونظراً لأن الأنظمة في الفضاء السيبراني ترتبط بالحواسيب وشبكات الاتصال فإن الاضطراب الذي ينشأ عن أي هجوم محتمل يعمل على تعطيل النظام الخدمي بالبلد قد يتجاوز ذلك حدود هذا البلد في كثير من الأحيان، مما يؤثر ذلك على عمليات كثيرة تعتمد على نقل البيانات في أكثر من بلد واحد. وتعتمد الكثير من البلدان في خدمات الإنترنت على خدمات تأتي من خارج نطاق هذه الدول، بل إن الأعطال في هذه الخدمات يمكن أن يسبب أضراراً مالية ضخمة في شركات الأعمال التي تقوم على أساس التجارة الإلكترونية بالاعتماد على شبكات الاتصالات بالبلد. ولا تعتبر شبكات الاتصالات المدنية هي النظم الوحيدة المعرضة للهجوم والمتضررة منه، لذا فإن الاعتماد عليها بشكل أساسي يمثل عنصر مخاطرة كبير جداً لنظم الاتصالات العسكرية. وبعكس ما يفعله المقاتلين التقليديين، لا يحتاج المهاجمون السيبرانيون إلى التواجد في المكان الذي يحدث فيه أثر الهجوم أو حتى المكان الذي يحتمل أن ينشأ فيه الهجوم. حيث يستطيع المهاجمون أثناء القيام بالهجوم استخدام تكنولوجيا اتصال مجهول الهوية وتشفيرها لإخفاء هويتهم[7].

إن الهجمات القائمة على أساس تكنولوجيا المعلومات والاتصالات هي عموماً أرخص من العمليات العسكرية العادية بل ويمكن أن تقوم بها الدول الصغيرة. وقد أصبح الآن بمقدور دولة تملك تاريخياً قدرات عسكرية أقل أن توجه ضربة قاصمة إلى البنية التحتية الحساسة لأعظم دولة من خلال الهجمات السيبرانية. وهذا الاختلال المحتمل في التوازن يجعل الحرب السيبرانية طريقة استراتيجية جاذبة لتحقيق درجة من المساواة في الفرص في فرض واقع سيكون خلاف عن سيناريو قوة غالبة ضد قوة ضعيفة. والخوف من الحرب السيبرانية الذي يُعززه وقوع هجمات سيبرانية فعلية (حتى وإن كانت محدودة) يقوض ثقة الجمهور في تكنولوجيا المعلومات والاتصالات. وهكذا فإن التذبذبات النفسية المحتملة للنزاع السيبراني يُمكن أن تنضوي على آثار واسعة الانتشار لتعطيل الاستخدام الفعلي للتقنيات الجديدة وعرقلة التقدم في قطاعات كثيرة.

مهددات النزاع السيبرانى:

إن مهددات الحروب المعلوماتية قديمة قدم النزاع البشري، وظلت الدوافع الكامنة وراء هذه الحروب على حالها. وتشمل هذه الدوافع السعي لتقويض ثقة الخصم، وتعطيل خطوط اتصالاته وإرباكها، وخلق الأوهام في نفسه بشأن طبيعة النزاع ومسرحه[14]. ولم تزل مثل هذه الدوافع قائمة في عالم اليوم. أما ما استجد في القرن الحادي والعشرين الذي تشيد فيه البنى التحتية المعلوماتية الإلكترونية بصلاتها الرقمية ذات النطاق العريض السريع والمتوسعة أكثر فأكثر فيتمثل في:

شراسة الهجمات المعلوماتية التي يمكن أن تمزق النسيج الاجتماعي في البلاد وتكررها.

القدرة البالغة على إلحاق أضرار مادية واسعة.

الطاقات والقدرات الوبائية للهجمات المعلوماتية المتواصلة والمتاحة للجهات الفاعلة غير الحكومية بل والخاصة القادرة الآن على المشاركة في الحروب غير المتناظرة.

نشوء حالة كامنة متفشية من النزاع الدائم منخفض المستوى، وهو ما يمكن أن يُطلق عليه اسم الحرب السيبرانية الباردة.

كـما أدى الاسـتخدام المكثـف لوسـائل تكنولوجيـا المعلومـات الحديثـة إلى تعزيـز القـدرات القتاليـة للأسـلحة التقليديـة والتقنيـات العسـكرية الأخـرى. ولهـذا السـبب فـإن العسـكريين ينظـرون إلى تكنولوجيـا المعلومـات والاتصـالات عـلى أنهـا سـلاح وهـدف في آن معـاً كما يعتـبرون الفضـاء السـيبراني ميدانـاً لخـوض الحـروب مثلـه مثـل الجـو، والفضـاء، والبر، والبحـر. وخـلال العقديـن الماضيـين قامـت البلـدان الصناعيـة بنـشر شـبكات واسـعة مـن الأصـول الاقتصاديـة، والماديـة، والاجتماعيـة الهامـة المربوطة عـبر تكنولوجيـا المعلومـات والاتصـالات للنهـوض بمسـتوياتها المعيشـية، ورخائهـا الاقتصـادي، وتأثيرهـا، وقوتهـا عـلى المسـتوى الـدولي. وبالمثـل فـإن البلـدان الناميـة تنظـر إلى تكنولوجيـا المعلومـات عـلى أنهـا مسـار اقتصـادي سريـع نحـو المشـاركة الكاملـة في الاقتصـاد العالمـي. وثمـة اعتمادهـا عـلى كـم هائـل مـن الأجهـزة الذكيـة الصناعيـة المحتويـة عـلى الحساسـات، وكذلـك الأجهـزة الاسـتهلاكية ذات المعالجـات الدقيقـة والقـدرات اللاسـلكية مثـل الهواتـف الخلويـة، والمسـاعِدات الرقميـة الشـخصية، والمفكـرات الإلكترونيـة. وتتيـح شـبكات الاتصـالات الواسـعة الاسـتخدام المكثـف لمـوارد المعلومـات لتيسـير التجـارة، وتوفـير الخدمـات، ورصـد البيئـة، ومعالجـة المشـكلات الاجتماعيـة الشـائكة. وتشـهد كل هـذه الأجهـزة تطـوراً سريعـاً مـع قدرتهـا عـلى الاتصـال بالأجهـزة الأخـرى في أي مـكان في العـالم[8].

1.9 انماط المهددات السيبرانية:

- اتـلاف المعلومـات أو تعديلهـا: يقصـد بـه الوصـول لمعلومـات الضحيـة عـبر الانترنـت أو الشـبكات الخاصـة بغـرض القيـام بعمليـة تعديـل للمعلومـات المهمـة مـما يـؤدي إلى نتائـج كارثيـة.
- التجسـس عـلى الشـبكات: يقصـد بـه الدخـول غـير المـصرح بـه عـلى شـبكة الخصـم بغـرض الحصـول عـلى معلومـات حساسـة.
- تدمـير المعلومـات: تعنـي مسـح شـامل لأصـول المعلومـات الموجـودة بالشـبكة مـن قبـل أشـخاص غـير مخولـين.

2.9 مخاطر المهددات السيبرانية:

- الاعتـداء عـلى الحريـات والحقـوق الشـخصية بالتعـرض لسريـة الاتصـالات والبريـد الالكتروني والدخـول للأنظمـة والملفـات دون اذن.
- التلاعب بالمعلومات المخزنة على نظام معين واتلافها عبر الاختراق الفيروسي.
- ارتكاب جرائم عبر الانترنت كالسرقة والغش والاعتداء على الملكية الفكرية وغيرها.
- الجرائـم المنظمـة والتـي تهـدد أمـن الأفـراد والـدول كغسـيل الأمـوال والإرهـاب والتهديـدات الخاصـة بالفدية.

10. الحرب السيبرانية وتأثيرها على السودان:

اضافـةً لمـا سـبق مـن مفاهيـم عـن الحـرب السـيبرانية وجـد أنـه لا تسـتهدف الحـرب السـيبرانية القـدرات والأنظمـة العسـكرية فحسـب، بـل تسـتهدف أيضـاً القضايـا الحيويـة للمجتمع عـن طريـق توظيـف شـبكات ذكيـة وأدوات مراقبـة إشرافيـة لحيـازة البيانـات والمعلومـات والتـي تسـتخدم للدفـاع عـن وضـع المجتمعـات. وعنـد التعامـل مـع الفضـاء السـيبراني باسـتخدام وسـائل تكنولوجيـا المعلومـات والاتصـالات الحديثـة يسـتطيع الأعـداء نـشر أسـلحتهم الافتراضيـة والدخـول في نـزاع هجومـي ودفاعـي

أشبه بالحرب العادية[15]. وتركز تكتيكات الحرب السيبرانية نمطياً على جمع البيانات التي تساعد في التسلل لأنظمة المعلومات الحساسة بواسطة الأدوات السيبرانية المناسبة لإحداث الضرر فيها. وعند تزايد الهجمات على الشبكات الخاصة بالدولة يزيد من تعرض المرافق الخدمية بالبلد للكثير من الأعطال. وتعتبر هذه الشبكات الذكية أنظمة الكترونية مرقمنة تربط إمدادات المرافق الخدمية بشبكات رصد مركزية تُسمى بشبكة سكادا(SCADA). وهي الشبكة التي تجمع معلومات عن استخدام خدمات الطاقة وإمداداتها كما تتيح أيضاً انسياب المعلومات بين المستهلك والمورد عبر قناة رقمية. وتُستخدم هذه التقنيات الآن في مجموعة واسعة من عمليات أنظمة المعلومات الخدمية مثل: أنظمة إدارة المياه، خطوط أنابيب الغاز، نقل وتوزيع الكهرباء، أنظمة البث الهوائية، أنظمة الاتصالات، الصناعة التحويلية والإنتاج، أنظمة النقل العام، أنظمة المراقبة البيئية ومراقبة الحركة الجوية وإشارات المرور. وتتزايد خدمات هذه الأنظمة يوماً بعد يوم عبر الربط الشبكي بالإنترنت لإتاحة النفاذ إليها للحصول على الخدمات عن بُعد وزيادة الاستفادة منها. وتُمثل الهجمات السيبرانية أكبر خطر على الشبكات الوطنية لتوليد الطاقة، فمن السهل جداً اختراق أي مقسم(موزع) ذكي(مقسم كهربائي موصول بالشبكة) وتلويثه بسهولة كبيرة إلى حد ما، وبعد ذلك يمكن استخدامه لنشر فايروس(دودة) إلى المقسمات الأخرى مما يرفع من شدة التيار في شبكة الطاقة أو إغلاقها. ويُمكن بسهولة توجيه هجوم عن بُعد لاستهداف البنية التحتية المادية مثل مولدات ومحولات الكهرباء بحيث تجعلها تُدمر نفسها من الناحية العملية. ومن المرجح أن أي هجوم من هذا النوع سيؤدي إلى عواقب بعيدة المدى نظراً لأن شركات الكهرباء في السودان لا تقوم في العادة بتخزين قطع الغيار الباهظة التكلفة، وقد يستغرق هذا الأمر فترة طويلة لاستجلابها أو تصنيعها. وأي هجوم على هذه الشبكة لن يحرم العملاء من الطاقة فحسب بل يؤدي أيضاً إلى تكاليف مالية كبيرة تصل إلى ملايين الدولارات والتي قد تفوق التكاليف المالية المرصودة لها. إضافة إلى إمكانية حدوث تدمير مادي واسع وخسارة مالية فورية. لذا فإن التهديد بالهجمات السيبرانية قد يُقوض في المستقبل الثقة في التكنولوجيات القائمة والجديدة والشبكات الذكية، فضياع هذه الثقة وحده يمكن أن يُسبب اضطرابات مجتمعية واقتصادية هائلة.

إضافة إلى الهجمات التقليدية والاستراتيجيات الدفاعية، يمكن أن تتبع الحرب السيبرانية أيضاً أسلوب الهجوم على كيان النظام الداخلي للبلد من أجل التشتيت أو العرقلة مؤقتاً بصورة غير مباشرة. وقد تختار أحد البلدان هذا النوع من الهجوم السيبراني إذا كانت تُريد أن تشل الدعم المتحالف للعدو المستهدف لفترة تكفي لتحقيق هدف محدد.

1.10 تأثير الحرب السيبرانية على قطاع الإتصالات:

وضعت الحرب الدائرة في السودان في بداياتها قطاع الاتصالات بالبلاد على حافة الانهيار الكامل، وتقلصت نسبة تغطية بعض الشركات إلى أقل من 20 %، وسط مخاوف من تأثيرات اقتصادية كارثية. وتراجع مستوى خدمات الاتصالات والانترنت في كافة أنحاء البلاد وسط تباين في نسب التدهور من منطقة لأخرى، وتعد العاصمة الخرطوم واقليمي دارفور وكردفان الأكثر تأثراً إذ تنقطع الخدمة بشكل كامل في كثير من المناطق، الأمر الذي دفع المواطنين للعودة إلى وسائل بدائية للتواصل الرسائل البريدية، بينما أغلقت البنوك أبوابها في وجه العملاء وتعثرت التطبيقات

المصرفية مثل «بنكك، وفوري، أوكاش، وغيرها».

وجاءت نتيجة تقلص نسبة تغطية بعض شركات الاتصالات في السودان نسبة لتحول مقر مزودات الخدمة الرئيسية المتمركزة في العاصمة الخرطوم إلى ثكنات عسكرية وتدمير العديد من محطات الربط الشبكي (أبراج الاتصالات) جراء المعارك الحربية، حيث تعمل في السودان 4 شركات اتصالات للهاتف السيار، هي زين، سوداني، أم تي أن، إضافة إلى شركة كنار للهاتف الثابت، وجميعها تزود الجمهور بخدمة المكالمات الصوتية والانترنت.

وتشير إحصاءات إلى أنه من بين سكان السودان المقدر عددهم بحوالي 43.33 مليون نسمة، يستخدم منهم 13.38 مليون نسمة الانترنت، فيما يستخدم الموبايل»الهاتف المحمول» 32.83 مليون شخص بما يعادل 76 % من مجموع السكان، في حين تبلغ نسبة التغطية بخدمة الاتصالات في البلاد 60 %. وكانت خدمات الاتصالات والانترنت رديئة حتى قبل اندلاع حرب 15 أبريل نتيجة لعدم استجابة الشركات للكم الهائل من المشتركين بتوسعة البنية التحتية من محطات ربط شبكي وغيرها، وقد وصل وضعها لمراحل متأخرة عقب اندلاع القتال، فقد انقطعت الخدمة بشكل كامل عن مناطق واسعة بإقليم دارفور وكردفان وجزء من العاصمة الخرطوم، وصارت ولاية الجزيرة ونهر النيل المتاخمة لمناطق القتال مهددة بالمصير نفسه.

وتقول منظمة "نت بلوكس" التي تُعنى برصد الوصول الى شبكة الانترنت في العالم ومقرها العاصمة البريطانية لندن خلال تقرير صدر في 23 أبريل الماضي، إن «بيانات الشبكة تظهر انهيار شبه كامل للاتصال بالإنترنت في السودان، حيث تبلغ نسبة الاتصال الوطني حاليا 2 % مقارنة بالمستويات العادية».

2.10 تأثير الحرب السيبرانية على القطاع الإقتصادى (المصارف):

وإلى جانب تأثير الحرب السيبرانية الواسعة على عملية الاتصال والتواصل الاجتماعي، تسبب ضعف الاتصالات في مصاعب اقتصادية كبيرة على السكان الذين أصبحوا يعتمدون بشكل أساسي على التطبيقات المصرفية عبر الهاتف المحمول في عمليات سحب وإيداع وإرسال الأموال وذلك بعد أن تسببت المعارك العسكرية في اغلاق البنوك في الخرطوم وكل مناطق النزاع.

11. النزاع المعلوماتي وطبيعة أسلحته:

يؤدي الاستخدام المكثف لتكنولوجيا المعلومات الحديثة إلى تعزيز القدرات العسكرية من حيث المعلومات، وإدخال تغييرات نوعية في الميادين العسكرية، الاستطلاع، والاتصالات. كما تزيد من سرعة اتخاذ القرارات الحربية المعقدة، وتمكّن من التحول السريع في التحكم بالقوات والأسلحة على مختلف المستويات الاستراتيجية. ويزيد استخدام تكنولوجيا المعلومات من القدرات القتالية في ميادين الحرب الإلكترونية، وتخلق نوعاً جديداً من الأسلحة المعلوماتية المصممة لإتلاف البنية التحتية المعلوماتية العسكرية والمدنية للخصم عبر اختراق أنظمته شبكاته [5].

وفقاً لما جاء عن خبراء أمريكيين فإن تسليط الأسلحة المعلوماتية على البينة التحتية للأنظمة العسكرية والمدنية الحيوية يمكن أن ينهي النزاع قبل بدء العمليات القتالية الحركية للأطراف من خلال تصعيد الهجوم المعلوماتي. ويتيح امتلاك أسلحة المعلومات ميزة ساحقة للبلدان التي تفتقر إليها. وبالمستطاع استخدام هذه الأسلحة كعامل ضغط سياسي رادع. ومما لاشك فيه

فإن الأسلحة المعلوماتية أصبحت اليوم عنصراً بارزاً في القدرات العسكرية للبلدان، وأن الكثير من هذه البلدان تستعد الآن بنشاط وإصرار لشن حروب معلوماتية[4].

النزاع المعلوماتي هو أحد مشكلات الحرب السيبرانية الدائرة الآن وهو أكبر مهدد للأمن المعلوماتي. وذلك من خلال السمات المميزة للأسلحة المعلوماتية المستخدمة فيه، والذي ينبغي أن يُعامل على أنه نزاع مسلح. لما له من قدرة على الإضرار بالبنية التحتية المعلوماتية العسكرية والمدنية. وهناك نهج يمكن بمقتضاه اعتبار السلاح المعلوماتي على أنه أحد وسائل التدمير التي تستخدم تكنولوجيا المعلومات والاتصالات. وبما أن تكنولوجيا المعلومات والاتصالات تشكل جزءاً كبيراً من البنية التحتية للمجتمع الحديث فإنها تندرج ضمن مجموعة الأدوات المتاحة لبلد ما في حربه ضد أعدائه[9]. وتتخذ العديد من البلدان إجراءات لمجابهة التهديدات الموجهة إلى الأمن المعلوماتي؛ وفي مثل هذه الظروف فليس بمقدور أي بلد أن يتمتع بالسلامة إذا ما حاول التصدي بمفرده للتهديدات المعلوماتية. ولا يمكن الحد من انتشار الأسلحة المعلوماتية وتقليل خطر نشوب حروب معلوماتية، وعمليات إرهابية معلوماتية، وجرائم سيبرانية، إلا بإرساء نظام دولي للأمن المعلوماتي. وفي الحد الأدنى فإن بالإمكان اعتبار البرمجيات المصممة خصيصاً لتدمير البنية التحتية المعلوماتية كالفيروسات المختلفة ، وما إلى ذلك. على أنها بدون أدنى شك أسلحة معلوماتية. غير أن الغالبية العظمى من الوسائل المتطورة للصراع المسلح التي تستخدم تكنولوجيا المعلومات والاتصالات هي ذات استخدامات متعددة، أي أنها ليست مصممة فحسب لتدمير البنى التحتية المعلوماتية بل لمهام قتالية أخرى أيضا. وتتمتع البلدان التي تمتلك أنظمة أسلحة متطورة، ووسائل استطلاع، واتصال، وملاحة، وتحكم مستندة إلى الاستخدام الواسع لتكنولوجيا المعلومات والاتصالات بتفوق عسكري حاسم؛ ومن ثم فإن من المشكوك فيه أن تنضم هذه الدول إلى اتفاقيات تحد من مزاياها الاستراتيجية.

من سوء الطالع أن أغلب التقنيات الحديثة للمعلومات والاتصالات التي تُستخدم لأغراض عسكرية، وإرهابية، وإجرامية هي من إنتاج الصناعات المدنية؛ ومن ثم فإن التحكم بتطويرها وانتشارها سيكون عسيراً جداً. والتهديد الذي تطرحه أدوات النزاع السيبراني والحرب المعلوماتية هو تهديد حقيقي بالنسبة للجميع. ولا يمكن التخفيف من حدة التهديد المؤذي لتكنولوجيا المعلومات إلا من خلال جهود المجتمع الدولي من أجل حماية البنى التحتية المعلوماتية الوطنية الهامة. وسيتيح توافق الآراء إلى توفير ردع فعال وإجراءات وقائية كفوءة، بما في ذلك الحق في لجوء البلدان إلى إجراءات ثأرية في حال تنفيذ عمليات معلوماتية ضدها مع توخي الحذر الشديد. فمن غير المبرر الشروع في حرب حركية نتيجة عمل ما مهما كان نوعه من الأعمال المعلوماتية العدوانية؛ ومن السيء جداً منح الحكومات الحجج اللازمة لكي تبت في الأمر بنفسها[9].

12. الحد من النزاع السيبراني:

يؤدي عدم التناظر المحتمل بين التقنيات المعلوماتية الهجومية والدفاعية إلى وضع يستطيع فيه المستخدمون الفعليون شن «حروب سيبرانية» شخصية ضد البنية التحتية المعلوماتية المهمة للمجتمع وذلك بنفس القوة التي يمكن أن تستخدمها الدول القومية تقريباً. وبالتالي فإن النظام القانوني والسياسي لردع النزاع السيبراني والحد منه بين الدول سيرتبط بحكم الواقع بالأطر القانونية والإجرائية المتعلقة بردع الإرهاب السيبراني والجريمة السيبرانية والتعامل معهما. ويمكن

إنشاء إطار قانوني عابر للدول يرسي القواعد والعقوبات المتعلقة بالنزاع السيبراني في مجموعة من الاتفاقيات الملزمة المنظمة والناتجة عن مفاوضات دولية. ومن الواجب أن تحدد مثل هذه القواعد التزامات البلدان الموقعة فيما يتعلق بضبط المنظمات أو الشبكات غير الحكومية التي تعمل فعلياً ضمن حدودها.

كما ينبغي أن يعمل الاطار القانوني الفعال على وضع التدابير التي يمكن اتخاذها ضد المهاجمين من غير الدول إذا كان بالمستطاع فعلاً تحديدهم. وفي حال ظهور أي عمل إرهابي نابع من البلد المتعرض للهجوم، فإنه بالإمكان اتخاذ التدابير بحق المهاجم في سياق القانون الجزائي للبلد. أما بالنسبة للهجمات المنطلقة من دول محايدة أو متعاونة فإن هناك خيارات متعددة هي:

تسليم الفاعل إلى الدولة التي تعرضت للهجوم.

المحاكمة المحلية في البلد المحايد الذي انطلق منه الهجوم.

تسليم الفاعل إلى طرف ثالث يدَّعي ولاية قضائية عالمية ويلتزم عموماً بالحدود المناسبة للإجراءات. وفي حال انطلاق الهجمات السيبرانية من دول مارقة أو غير متعاونة فإن ذلك يؤدي إلى استبعاد توافر القنوات العادية للتعاون في التحقيقات المتعلقة بالهجمات. وبالتالي فإن مثل هذه الحالات تتحول بالطبع إلى مسائل للتدخل بالقوة أو عبر العقوبات الدولية. ومن الخيارات المفتوحة أمام البلد الذي تعرض للهجوم هي:

- رد ثأري ضد البلد المعني.
- دخول بدون تفويض واعتقال المذنبين المشتبه بهم.
- الاحترام اللائق للسيادة من خلال إشراك دولة طرف ثالث كوسيط.[16]

13. الاستقرار الجيوسيبراني:

الجيوسيبرانية تعرف على أنها العلاقة بين شبكة الإنترنت والجغرافيا، والديموغرافيا، والاقتصاد، والسياسة لبلد ما وسياسته الخارجية. أما «الاستقرار الجيوسيبراني» فهو قدرة كل البلدان على استخدام الإنترنت لاستخلاص منافع اقتصادية، وسياسية، وديموغرافية مع الإحجام عن القيام بأنشطة قد تؤدي إلى أنماط من المعاناة والتدمير لا داعي لها. فمن الصعب جداً تحمل وتيرة تصاعد الجريمة السيبرانية. فالجهات الفاعلة المارقة التي تستخدم الشبكات المستعبَدة الاختراقية بصورة معتادة لاستخلاص المعلومات السرية والخاضعة لحقوق الملكية وشن هجمات توزيعية تعطِّل الخدمات التي توفرها نظم الحكومات والشركات. وتدرك البلدان أن نظمها التابعة للحكومة وقطاع الأعمال قيِّمة وأن أمنها القومي والاقتصادي معرض للخطر فقد شرعت في تطوير استراتيجيات للحرب السيبرانية وإرساء مراكز قيادة سيبرانية ذات قدرات هجومية ودفاعية. في حين أن مثل هذه التدابير مناسبة ومنتظرة، فإن هناك خواء ملحوظاً فيما يتصل بالحوار المتعلق بالسلام السيبراني للحفاظ على مستوى مقبول من الاستقرار الجيوسيبراني.[17]

ولتحقيق الاستقرار الجيوسيبرانى يجب:

حماية قدر معين من البنية التحتية الحيوية لمنع أوجه التدمير، والأذى، والمعاناة غير الضرورية وضمان الحد الأدنى من الإتصالات الأساسية.

حظر استخدام شبكات الاختراق الخاصة VPN والقوات السيبرانية الأخرى غير النظامية.

على البلدان احترام حياد البلدان الأخرى ومساعدة بعضها في التحقيقات المتعلقة بالجريمة السيبرانية.

14. السلام السيبرانى:

يعتبر السلام هو حالة من الهدوء النافع، وغياب للفوضى والصراعات والعنف. ويعني سيادة المبادئ القانونية والأخلاقية العامة وفق إمكانيات وإجراءات تسوية النزاعات والاستدامة والاستقرار[10].

ويمكن أن تصبح التقنيات الحديثة للمعلومات وسيلة خير وأداة للسلام ومن ثم فهي أيضاً أداة للنزاع. ويتطلب استغلال فوائد هذه التقنيات على أن تكون شبكات المعلومات وأنظمتها سهلة الاستخدام وآمنة وموثوقة ويمكن الاعتماد عليها. ويتطلب السلام السيبراني أمن واستقرار الفضاء السيبراني وتضافر الجهود الدولية بصورة عامة.

1.14 مبادئ السلام السيبرانى:

تضمن مبادئ السلام السيبرانى الأمن والاستقرار في الفضاء السيبراني، وقد قام الاتحاد العالمي للإتصالات بترجمة المبادئ العامة التي أقرتها الأمم المتحدة والتي يمكن تطبيقها في البيئة السيبرانية بمزيد من التفصيل، في «إعلان إيريس بشأن مبادئ الاستقرار السيبراني والسلام السيبراني» في أغسطس 2009. ويبين هذا الإعلان أن تحقيق الاستقرار والسلام السيبراني أمران متداخلان معاً. ويتسم الإعلان بالإيجاز ويركز على العناصر التشغيلية الأساسية للسلام السيبراني[1]. وهي كالتالي:

1. على جميع الحكومات الاعتراف بأن القانون الدولي يضمن التدفق الحر للمعلومات والأفكار للأفراد عبر الفضاء السيبراني؛ مع عدم فرض قيود إلا عند الاقتضاء، بعد الخضوع لعملية مراجعة قانونية.
2. على جميع البلدان العمل معاً لوضع مدونة مشتركة للسلوك السيبراني في إطار قانوني عالمي منسق، يكفل احترام الخصوصية وحقوق الإنسان. وينبغي لجميع الحكومات وموفري الخدمات والمستخدمين دعم الجهود المبذولة في سبيل إنفاذ القانون الدولي ضد مرتكبي الجرائم السيبرانية.
3. على جميع المستخدمين وموفري الخدمات والحكومات العمل معاً لضمان ألا يستخدم الفضاء السيبراني لاستغلال المستخدمين، لا سيما الشباب والمستضعفين منهم، من خلال العنف أو الإذلال.
4. على الحكومات والمنظمات والقطاع الخاص والأفراد، تنفيذ برامج شاملة للأمن وتحديثها بناءً على أفضل الممارسات والمعايير المقبولة دولياً واستخدام تقنيات حماية الخصوصية والأمن.
5. على مطوري البرمجيات والأجهزة السعي إلى تطوير تقنيات آمنة تعزز القدرة على التصدي وتقاوم نقاط الضعف.
6. على الحكومات أن تشارك بفعالية في جهود الأمم المتحدة الرامية إلى النهوض بالأمن السيبراني والسلام السيبراني في العالم وأن تتفادى استخدام الفضاء السيبراني من أجل النزاعات.

2.14 أبعاد السلام السيبراني

يطال السلام السيبراني جميع المجالات العسكرية والاقتصادية والاجتماعية والسياسية والانسانية، ليحقق منظومة معلوماتية معافاة من كل المهدات السيبرانية والحفاظ على سلامة المعلومات المتداولة عبر الفضاء السيبراني، ومن أبعاده نذكر:

البعد الاجتماعي: يكمن في الحفاظ على قيم وأخلاقيات المجتمع مما يسمح بتبادل المعلومات وتدفقها بسلام. ويفوق مستخدمي مواقع التواصل الاجتماعي بالعالم أكثر من 3 مليار شخص مما يجعلها أكبر تجمع للتفاعل البشري وتبادل الأفكار ويعرض ذلك هويات الأشخاص لعمليات الاختراق الخارجي الذي يتسبب في تهديد السلم الاجتماعي للدولة، فالبد من العمل على توعية المستخدمين بهذه المخاطر لتحقيق السلام السيبراني في بعده الاجتماعي.

البعد السياسي: الحد من الاستغلال السيء لاستخدام منصات التواصل الالكترونية المختلفة وتوظيف معلوماتها لتحقيق اغراض خاصة تخدم جهات سياسية تريد ان تزيد من حجم ثغلها السياسي وفقاً للسجلات والحسابات التي تمتلكها هذه المنصات.

البعد القانوني: ان التطورات التقنية المتسارعة تفرض علينا مواكبة التشريعات القانونية لها عن طريق وضع أطر وتشريعات قانونية خاصة بالفضاء السيبراني، لأن الجريمة السيبرانية الآن تفتقد لوجود أطر قانونية تتيح كيفية التعامل معها، بالاضافة لتفعيل قانون التعاون الدولي المشترك لمكافحتها.

الخاتمة:

لقد توفرت الآن للمجتمع العديد من الفرص المفيدة للتواصل وتبادل المعلومات والأفكار عبر المنصات الالكترونية المنتشرة في الفضاء السيبراني، وهذه الفرص والفوائد جاءت مقترنة بالعديد من المهددات التي خلفت أضراراً كثيرة للدولة. نتيجة للاستخدام السيء لوسائل التواصل الحديثة.

تم في هذه الورقة تقديم دراسة شاملة عن ما ينشر من محتوى عبر الفضاء السيبراني في المنصات الالكترونية المختلفة، ثم تم الوقوف على ايجابيات هذا المحتوى المنشور عبر الفضاء السيبراني والاستفادة منها اضافة إلى التعرف على الآثار المترتبة على سلبيات المحتوى السيبراني والعديد من التغيرات والمشاكل التي ظهرت على المجتمع السوداني من الاستخدام السيء لبيئة الفضاء السيبراني، وتناولت الورقة أثر الحرب السيبرانية على البنية التحتية للبلاد، بالاضافة للسمات الفريدة للحرب السيبرانية ثم الوقوف على النزاع السيبرانى واسبابه وكيفية الحد منه عبر ارساء ثقافة السلام السيبراني وبنشر ثقافة الفضيلة والقيم النبيلة من أجل خلق بيئة تقنية معافاة من كافة المضار التقنية التي تفتك بالمجتمع من أجل التعايش السلمي بين المجتمعات، كما تحدثت الورقة عن أهمية الإستقرار الجيوسيبرانى الذي يقود الى السلام السيبرانى وأهميته، وتأثير فضاء السايبر على الحروب الدائرة فى السودان.

المصادر والمراجع:

(1) إ. توريه، حمدون، البحث عن السلام السيبرانى ، وثيقة الاتحاد الدولي للاتصالات، يناير 2011م.

(2) عباس بدران، الحروب الالكترونية: الاشتباك في عالم متغير، مركز دراسات الحكومة الالكترونية، بيروت 2010،

(3) عادل محمد عسكر محمد.(2021)وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم دراسة على ضوء دليل تالين بشان القانون الدولي المطبق على العمليات -السيبرانية . مجلة البحوث القانونية والإقتصادية.المجلد 33 .العدد 01 .

(4) بوبرطخ نسيم(2020) ، الفضاء السيبراني مسرح الصراعات الجيوسياسية المعاصرة، مجلة الجيش، العدد 685 .

(5) عادل عبد الصادق أسلحة الفضاء الالكتروني في ضوء القانون الدولي، سلسلة أوراق، العدد23، مكتبة الاسكندرية، مصر،2016 ، ص17 – 18

(6) غريب حكيم. (2018) الإرهاب السيبراني والأمن الدولي التهديدات العالمية الجديدة وأساليب المواجهة. المجلة الجزائرية للدراسات السياسية، المجلد 05 العدد 02.

(7) هشام الحلبى2023م، تأثير التكنولوجيا على التطور فى أشكال الحروب.

(8) ايهاب خليفة القوة الالكترونية وأبعاد النحول في خصائص القوة، مكتبة الاسكندرية، مصر، 2014، ص 33 – 42

(9) منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، بيروت 2017، ص 25

(10) صلاح حيدر عبد الواحد2021، حروب الفضاء الإلكتروني؛ دراسة مفهومها وخصائصها وسبل مواجهتها، رسالة إستكمالاً لمتطلبات الحصول على درجة الماجستير في العلوم السياسية، جامعة الشرق الأوسط، كلية الآداب والعلوم

(11) Richard A. Clarke , Robert Knake, Cyber War: Hardcover – April 20, 2010.

(12) . Olivier KEMPF, Introduction à la Cyberstratégie, Paris, Economica, 2012, P 9.

(13) 13. The International Télécommunication Union, ITU Toolkit for CybercrimeLégislation,Geneva,2010,P 12

(14) Stephen Elliot, "Analysis on Defense and Cyberwarfare," *Infosec Island*, 8 July 2010, https:// infosecisland.com/blogview/5160-Analysis-on-Defense-and-Cyber-Warfare.html (hereinafter "Elliot")

(15) Allin Mesmer,"Cyberattack Seen as Top Threat to Zap U.S. Power Grid," *NetworkWorld*, 2 June 2010, www.networkworld.com/news/2010060210-/nerc-cyberattack-power-grid.html

(16) Elliot Van Boscert،"Denial-of-Service Attack Knocks Twitter Offline (Updated)," Wired.com،، 7 Aug. 2007،www.wired.com/epicenter/200908//twitter-apparently-down/

(17) Thomas Klaborn، "Under Cyberattack, Georgia Finds 'Bullet-Proof' Hosting With Google And Elsewhere," *InformationWeek*, 12 Aug. 2008