تمظهرات الأمن السيبراني والممارسة الأعلامية وعلاقتهما بصناعة الحرب النفسية الأفتراضية (رؤية نقدية علائقية)

أ.م.د.سهام حسن علي الشمري
كلية الاعلام/ جامعة بغداد
Shwww64@yahoo.com

الملخص
يتحدد موضوع تمظهرات الأمن السيبراني والممارسة الإعلامية وعلاقتهما بصناعة الحرب النفسية الافتراضية من التركيز على رؤى نقدية علائقية، وفق تحولات المشهد الاتصالي الجديد، الذي يتخذ بعدا موازيا للتطور التقني الفعال، والتحديات التي يواجهها الأمن السيبراني، ويستهدف البحث التعرف على الاسس التي يتبناها الأمن السيبراني والإعلام التي يتم بموجبها استخدام الفضاء السيبراني، لذا تحدد الهدف الرئيس للبحث في ضرورة التعامل الجاد من أجل حماية الأمن السيبراني للعراق، إذ تمثل هذه القضية إشكالية خطيرة من ناحية نظرية وعلمية تتطلب البحث والمناقشة، الأمر الذي يعطى أهمية كبرى للتركيز على الخروقات الامنية والمجتمعية كأساليب ردعية للحرب النفسية الافتراضية الموجهة للعراق، عن طريق وضع الحلول ورصد وتحليل مضمون ما يتعلق بكل المنظومة السيبرانية، والاستدلال على الأبعاد المختلفة للظاهرة الاتصالية، إذ أن الفضاءات السيبرانية فتحت بفضل خواصها وديناميتها التواصلية آفاقا غير مسبوقة للاهتمام بالأمن، كما خلقت أنماط اتصالية وتشبيكية ما كان من الممكن وجودها في مرحلة ما قبل الإنترنت، فأهمية الأمن السيبراني في المجتمع، عكسها عصر التكنولوجيا الذي أصبح لأمن المعلومات الدور الأكبر لصد ومنع أي هجوم إلكتروني قد تتعرض له أنظمة الدولة المختلفة.

Manifestations of cyber security media practice and its relationship to the virtual psychological warfare industry. (Relational Critical lnsights)

Sihaam Hassan Ali Al-Shujairi
Assistant Professor
Baghdad University/College of Mass Communication

Abstract:
The topic of cybersecurity manifestations and media practice and their relationship to the virtual psychological warfare industry is determined

by focusing on relational critical insights, according to the transformations of the new communication landscape, which takes a parallel dimension to the effective technical development, and the challenges facing cybersecurity, and the research aims to identify the foundations adopted by cybersecurity and the media. Under which cyberspace is used, so the main goal of research is determined in the necessity of serious dealing in order to protect the cyber security of Iraq, as this issue represents a serious theoretical and scientific problem that requires research and discussion, which gives great importance to focusing on security and societal breaches as deterrent methods of psychological warfare. Virtualization directed at Iraq, by developing solutions, monitoring and analyzing the content of what is related to the whole cyber system, and inferring the different dimensions of the communication phenomenon, as the cyber spaces, thanks to their communicative properties and dynamics, opened unprecedented horizons for attention to security, as well as creating communication and networking patterns that could not exist in Before the Internet, the importance of cybersecurity in society is reflected in the era Technology, which has become information security, has the largest role to prevent and prevent any cyber attack that may be exposed to various state systems

أولا- المدخل:

ان موضوع تمظهرات الأمن السيبراني والإعلام وعلاقتهما بصناعة الحرب النفسية الافتراضية وفق تحولات المشهد الاتصالي الجديد، يتخذ بعدا موازيا للتطور التقني الفعال، ذلك ان الإعلام المفتوح والتدفق المعلوماتي الكبير جعل الحرب النفسية تتصدر الاولويات في الرصد والتحليل، إذ أحدثت الحروب المعلوماتية في ظل التطور التقاني وتفاعل الفضاء السيبراني تأثيرات كبيرة في كل دول العالم، محققة أهدافا استراتيجية لهذا النوع من الحروب اوسع مما خطط لها، فأصبحت المواجهات الإعلامية على المواقع الالكترونية وخاصة مواقع التواصل الاجتماعي، الفيسبوك واليوتيوب والتويتر، والفضائيات، تتعامل مع جميع المفردات المعلوماتية التي يتلقاها الانسان بوصفه مجموعة أو أفرادا أو كيانا اجتماعيا بهدف إحداث التأثير من خلال زرع الرعب والخوف والتخويف والتهليل والتضليل المعلوماتي الذي يصور الخيال أقرب الى الواقع، فنشطت هذه الانواع من الحروب وفق الفضاء السيبراني، مهددة الأمن المجتمعي

والدولي، وارتبطت بالحرب النفسية، واصبحت بحاجة الى تأمل ودراسة لمعرفة انواعها وطرقها ونتائجها، وقد بدأ ظهور هذا العالم عند ظهور التكنولوجيا الحديثة والمتطورة في عالم الكمبيوتر، فضلا من أن ظهورا قويا للإرهاب، وارتباطه بمفهوم الإرهاب السيبراني كتهديد أمني جديد عابر للحدود، للدول والمجتمعات، إذ يقوم على استخدام التقنيات الحديثة لشن هجومات إرهابية بهدف نشر الخوف والرعب، وهنا فأن الإرهاب والإنترنت مرتبطان بطريقتين هما: ممارسة الأعمال التخريبية عبر شبكات الحاسوب والإنترنت، وبأن الإنترنت أصبح منبرا للجماعات والأفراد لنشر رسائل الكراهية والعنف والتحريض، وللاتصال ببعضهم البعض وبمؤيديهم والمتعاطفين معهم، وهو ما نتطرق اليه ونفسره في هذا البحث من خلال معطيات تلك التمظهرات والتحولات في المشهد الاتصالي الجديد، وعلاقته بالحرب النفسية الافتراضية، وتطور أجيالها.

ثانيا-أهمية البحث والحاجة إليه:

تنبع أهمية البحث من عدة عوامل مترابطة، وذلك على النحو الآتي:

١-يعد البحث محاولة بحثية للتعرف على القضايا المطروحة المتعلقة بتمظهرات الأمن السيبراني والإعلام وعلاقتهما بصناعة الحرب النفسية الافتراضية وفق رؤى نقدية علائقية.

٢-إرتباطه بالتطورات السريعة في مجال تكنولوجيا المعلومات الذي أفضى إلى متغيرات بعيدة المدى في جميع مجالات الحياة تقريباً، ولا سيما في المجالين العسكري والأمني.

٣-تتأكد أهمية البحث من واقع أهمية الوقوف على الأساليب والوسائل النفسية وتأثيرهما، وهو ما يمنحنا فرصة لفهم الآليات التي أستند إليها الفضاء السيبراني من أجل الوصول إلى فهم أكبر الحرب النفسية.

٤- المستجدات التي طرأت على أنماط التفكير الاستراتيجي، وعلى بلورة عقيدة قتالية تتلاءم مع الواقع المتغير وفق ثورة التقانة وتكنولوجيا المعلومات.

ثالثا-إشكالية البحث:

تحددت إشكالية البحث وفقا للمعايير العلمية بالتساؤلات الآتية:

١-كيفية رصد وتحليل تمظهرات الأمن السيبراني والإعلام وعلاقتهما بصناعة الحرب النفسية الافتراضية؟

٢-هل الأمن السيبراني يشكل جزءاً أساسياً من أية سياسة أمنية وطنية؟

٣-ما أهمية الأمن السيبراني وارتباطه بالإعلام وبصناعة الحرب النفسية الافتراضية؟

٤-ما فواعل الأمن السيبراني، في الإعلام؟

٥-ما التحديات التي يواجهها الأمن السيبراني بالترافق مع اجيال الحرب النفسية الافتراضية؟

رابعا- هدف البحث:

يستهدف البحث التعرف على الاسس التي تتبناها تمظهرات الأمن السيبراني والإعلام وعلاقتهما بصناعة الحرب النفسية الافتراضية وفق رؤى نقدية علائقية، ووفق اجيال الحروب النفسية التي يتم بموجبها استخدام الفضاء السيبراني، إذ تتعرض أغلب دول العالم اليوم إلى هجمات مستمرة من قبل ما يسمى بالهاكرز، لذا تحدد الهدف الرئيس للبحث في ضرورة التعامل الجاد من أجل حماية الأمن السيبراني للعراق، إذ تمثل هذه القضية إشكالية خطيرة من ناحية نظرية وعلمية تتطلب البحث والمناقشة، الأمر الذي يعطى أهمية كبرى للتركيز على الخروقات الامنية والمجتمعية كأساليب ردعية للحرب النفسية الافتراضية الموجهة للعراق، عن طريق وضع الحلول ورصد وتحليل مضمون ما يتعلق بكل المنظومة السيبرانية لذلك تحدد هدف البحث في الإجابة عن التساؤلات التي طرحتها الاشكالية وكالاتي:

١-رصد وتحليل تمظهرات الأمن السيبراني والإعلام وعلاقتهما بصناعة الحرب النفسية الافتراضية.

٢-الكشف على أن الأمن السيبراني يشكل جزءاً أساسياً من أية سياسة أمنية وطنية.

٣-الاطلاع على أهمية الأمن السيبراني وارتباطه بالإعلام وبصناعة الحرب النفسية الافتراضية.

٤-رصد فواعل الأمن السيبراني، في الإعلام.

٥-معرفة طبيعة التحديات التي يواجهها الأمن السيبراني بالترافق مع اجيال الحرب النفسية الافتراضية.

خامسا-منهج البحث:

ينتمي البحث إلى البحوث الوصفية النظرية التي تسعى إلى تجاوز وصف المحتوى الظاهر للرسالة الاتصالية إلى الكشف عن المعاني الكامنة، والاستدلال على الأبعاد المختلفة للظاهرة الاتصالية، للوصول إلى نتائج دقيقة ومفيدة في مجال إثراء الدراسات البحثية الوصفية النظرية من خلال وصفها، وفق مضمونها النظري، وهذا المنهج يمثل جهداً علمياً منظماً يساعد في الحصول على المعلومات عن الظاهرة موضوع البحث كونها تأصيل لتمظهرات الأمن السيبراني والإعلام وعلاقتهما بصناعة الحرب النفسية الافتراضية وفق رؤى نقدية علائقية، ويعد هذا البحث أيضاً من البحوث الاستطلاعية التي تنتمي إلى الدراسات الوصفية التفسيرية التي تهتم بدراسة الحقائق الراهنة المتعلقة بموضوع البحث.

سادسا-تحديد المفاهيم والمصطلحات:

١-الأمن السيبراني: عبارة عن مجموع الوسائل التقنية والتنظيمية والادارية التي يتم استخدامها لمنع الاستخدام غير المصرح به وسوء الاستغلال واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني.
٢-الحرب النفسية: استخدام أية وسيلة بهدف التأثير على الروح المعنوية وعلى سلوك أية جماعة.
٣-الافتراضية: أو الواقع الافتراضيّ: محاكاة يولِّدها الحاسوب لمناظر ثلاثيّة الأبعاد لمحيط الأحداث تمكِّن النَّاظر ليستخدم جهازًا إلكترونيًّا خاصًّا من أن يراها على شاشة عرض ويتفاعل معها بطريقة تبدو فعليّة.

سابعا: رصد وتحليل تمظهرات الأمن السيبراني والإعلام وعلاقتهما بصناعة الحرب النفسية الافتراضية:

لم تعد الطائرة والدبابة تحتكر دور البطولة في معارك هذا العصر.. يقول محمد عبدالسلام في كتابه "الحرب في زمن التغريدات" ويضيف: أرض المعركة نفسها تغيرت كثيرا، تمر ايام واسابيع بل وشهور لا يلتقي الجنود وجها لوجه، ورغم ذلك يتساقط العشرات والمئات من القتلى والمصابين والابرياء، خدعونا ستون عاما بأبحاثهم عن "الأكوان المتوازية" لوضع حد للحروب بين البشر بحثا عن أرض جديدة، ولكنهم فاجئونا بـ"عوالم متوازنة" لإشعال حربا كونية ثالثة داخل هذا العالم الافتراضي، لم يكن عالم الحاسوب الامريكي "إيفان سنرلاند" مجنونا كما أوهمونا عندما قال: أنه بالعالم الافتراضي سننشأ حياة ثانية"، ولم تتصف "إيرين غرانت" بالبلاهة حينما أشارت إلى إنه: "بالحياة الثانية سننشئ مجتمعا جديدا نسيطر به على العالم"، طيلة قرن من الزمان عاش العالم ٩٠ صداما مسلحا، أودي بحياة ما يقرب من ٢٠٠ مليون إنسان، ٥٦% منهم قتلوا في حربين عالميتين، ومع نهاية القرن الماضي وتحديدا قبل الغزو الامريكي للعراق في ٢٠٠٣، بدأت فلسفة الحروب تنحى منحى جديدا: "الإنترنت.. مواقع التواصل الاجتماعي.. مواقع الارهاب.. اليوتيوب" كانت الحلبة الافتراضية لمعارك العصر الحديث ورغم انها معارك افتراضية تلعب دائما على "العمليات النفسية"، إلا أنها اثبتت ما يمكن ان تلحقه من دمار.([1])

١-مفهوم الفضاء السيبراني:

يعد الفضاء السيبراني مجالا افتراضيا من صنع الإنسان يعتمد على نظم الكمبيوتر وشبكات الأنترنت وكم هائل من البيانات والمعلومات والأجهزة، وهناك من عرف الفضاء السيبراني بوصفه الذراع الرابعة للجيوش الحديثة، وهناك من يرى أنه البعد الخامس للحرب، وهذا التعريف يحصر الفضاء السيبراني في المجال العسكري فقط دون التطرق للمجالات الأخرى، وعرفته الوكالة الفرنسية لأمن أنظمة الإعلام (ANSSI) وهي وكالة حكومية مكلفة بالدفاع السيبراني الفرنسي على أنه: "فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات

الرقمية" وهذا التعريف يركز على الجانب التقني، ويغفل العامل البشري، والذي يعد جزءا أساسيا في فهم الفضاء السيبراني، كما جاء تعريف الاتحاد الدولي للاتصالات للفضاء السيبراني بأنه: "المجال المادي وغير المادي الذي يتكون وينتج عن عناصر هي: أجهزة الكمبيوتر، الشبكات، البرمجيات، حوسبة المعلومات، المحتوى، معطيات النقل والتحكم، ومستخدمو كل هذه العناصر" ويمكن القول بأن: "الفضاء السيبراني هو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، مكون من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو مستعملين"، وتجدر الإشارة إلى أن مسألة تحديد مفهوم "الفضاء السيبراني"، هي مسألة نسبية تتوقف على طبيعة إدراك وفهم كل من الدول والهيئات كل حسب رؤيته واستراتيجيته وقدرته على استغلال المزايا المتاحة ومواجهة المخاطر الكامنة في هذا الفضاء.([٢])

ويُعرّف "الأمن السيبراني" بأنه "الإجراءات المتخذة لحماية الأنظمة والشبكات المعلوماتية والبنى التحتية الحرجة من حوادث الأمن السيبراني، ومقاومة الحرب النفسية الافتراضية التي تمارس على الافراد والشعوب، والقدرة على استعادة عملها واستمراريتها سواء كان الوصول إليها بدون تصريح أو سوء استخدام، أو نتيجة الإخفاق في اتباع الإجراءات الأمنية أو التعرض للخداع الذي يؤدي إلى ذلك"، ويُقصد بالبنية التحتية الحرجة "مجموعة الأنظمة والشبكات الإلكترونية والأصول المادية وغير المادية أو الأصول السيبرانية والأنظمة، التي يعدّ تشغيلها المستمر ضرورة لضمان أمن الدولة واقتصادها وسلامة المجتمع"، ويُتداول مصطلح "الفضاء السيبراني" على أكثر من صعيد، ذلك كونه أساسا فضاءا اجتماعيا للتواصل والتبادل، إلَا أنَه أضحى مجالا حيويا وجيواستراتيجيا تُخاض فيه العديد من الحروب والهجمات الرقمية، كما أن عملية تعزيز الجانب الدلالي لهذا الفضاء تستدعي تحليل البنية التركيبية له، إذ يُمكن اعتبارها بنية ذي ثلاث طبقات هي:([٣])

أ-الطبقة المادية: تشمل معدات الحواسيب، والبرمجيات، والمعدات الضرورية لعملية الربط البيني.

ب-الطبقة المنطقية: تشمل مجموع البرامج المترجمة للمعلومة على شكل معطيات رقمية، حيث يتم الانتقال من لغة الإنسان إلى لغة الآلة في شكل خوارزمية، ومنها إلى برامج مطوَرة بلغة البرمجة.

ح-الطبقة الإعلامية: وتتمثل هذه الطبقة في البُعد الاجتماعي الذي يُضاف إلى الطبقتين السابقتين، حيث أنه في الفضاء الرقمي يُمكن أن يكون لكل إنسان عدة هويات رقمية (عنوان بريده الالكتروني، رقم هاتفه النقال، صور رمزية على مواقع التواصل الاجتماعي...الخ).

ويُعد الأمن السيبراني من المجالات المتعددة التخصصات، ويتناول المسائل المتعلقة بحماية المعلومات التي تتم على جميع مستويات أنظمة الحوسبة والشبكات الإلكترونية وضمان موثوقيتها، وقد صُمِّم برنامج ماجستير العلوم في الأمن السيبراني لتدريب الخريجين والمحترفين ورجال الأعمال والقادة والباحثين، وتزويدهم بالمعرفة والمهارات اللازمة ليستوعبوا بشكل تام التقنيات المتطورة في مجال الأمن السيبراني، وسياسات وأخلاقيات تكنولوجيا المعلومات وطريقة تطبيقها بشكل فعَّال، وعليه فأن الفضاء السيبراني: عبارة عن بيئة افتراضية، تتصل عن طريق شبكات الكمبيوتر وتعمل بها المعلومات الإلكترونية، ويعرف بأنه المجال الكهرومغناطيسي لتخزين وتعديل أو تغيير البيانات المتصلة والمرتبطة بشبكة البنية التحية الطبيعة، ويتضمن عملية الاندماج ما بين الانترنت والمحمول وأجهزة الاتصالات والأقمار الصناعية، والفضاء الإلكتروني أكبر من الانترنت، لما يحتويه من قدرات توجيهية للطاقة التي توجد في جزء من الموجات الكهرومغناطيسية.([٤])

٢- وظائف الامن السيبراني الذي يشكل جزءاً أساسياً من أية سياسة أمنية وطنية:

يوفر خبراء الأمن السيبراني الحماية للشبكات والخوادم والشبكات الداخلية وأنظمة الكمبيوتر، كما أنه يضمن أن الأشخاص المصرح لهم فقط يمكنهم الوصول إلى تلك المعلومات. في أحد الإعدادات المكتبية، قد يذهب أحد الأفراد إلى كمبيوتر شخص آخر، ويقوم بتثبيت محرك أقراص محمول ونسخ معلومات سرية، هذا يندرج أكثر تحت فئة أمن المعلومات، إذا تمكن شخص ما في منتصف الطريق عبر العالم من اختراق شبكة شركة أخرى وخرق نظامه، فستحتاج هذه الشركة إلى أمان إنترنت أفضل، إذ أن الأمن السيبراني هو "جزء متزايد الأهمية في حياتنا اليوم، ودرجة الترابط بين الشبكات يعني أن أي شيء وكل شيء يمكن أن يتعرض للهجمات السيبرانية"، وتسهل مواقع الشبكات الاجتماعية عبر صفحات الويب التفاعل النشط بين الاعضاء المشتركين فيها، وتهدف الى توفير مختلف وسائل التفاعل مثل المراسلة التزامنية وغير التزامنية، الفيديو، الدردشة، تبادل الملفات، مجموعات النقاش، البريد الالكتروني، المدونات، وتقوم الفكرة الرئيسية للشبكات الاجتماعية، على جمع بيانات الاعضاء المشتركين في الشبكة، ويتم نشر هذه البيانات علنا على الشبكة حتى يتجمع الاعضاء ذو المصالح المشتركة، كما تعمل على تسهيل الحياة الاجتماعية بين مجموعة من المعارف والاصدقاء، كما تمكن الاصدقاء القدامى من الاتصال بعضهم البعض، وتمكنهم ايضا من التواصل المرئي، والصوتي وتبادل المعارف.([٥])

٣-عناصر الأمن السيبراني: ([٦])

حتى يتحقق الهدف من الأمن السيبراني، لا بد من توفر مجموعة من العناصر مع بعضها البعض لتكمل الدور في ذلك، ومن أهم أبعاد وعناصر الأمن السيبراني:

أ-التقنية (technology): تشكل التكنولوجيا والتقنية دورًا في غاية الأهمية في حياة الأفراد والمنظمات، حيث توفر الحماية الفائقة لهم أمام الهجمات السيبرانية، وتشتمل حماية الأجهزة بمختلف أشكالها الذكية والحاسوبية والشبكات بالاعتماد على جدران الحماية واستخدام البرامج الضارة ومكافحة الفيروسات وغيرها.

ب-الأشخاص(People) : يستوجب الأمر لزومًا على الأشخاص من مستخدمي البيانات والأنظمة في منشأة ما استخدام مبادئ حماية البيانات الرئيسية كتحديد كلمة مرور قوية، وتفادي فتح الروابط الخارجية والمرفقات عبر البريد الإلكتروني، إلى جانبِ القيام بعمل نسخ احتياطية للبيانات.

ج-الأنشطة والعمليات (Process): يتم توظيف الأشخاص والتقنيات للقيام بالعديد من العمليات والأنشطة وتسييرها بما يتماشى مع تطبيق أسس الأمن السيبراني والتصدي لهجماته بكل كفاءة.

ان الشبكات الاجتماعية، تمثل اليوم أهم ثورة الكترونية عرفتها البشرية في مجال التواصل الاجتماعي، والتفاعل الدائم بين أعضاء البنى الاجتماعية، ليكونوا بناءا إلكترونيا تفاعليا يحقق لهم اسرع الطرق للتواصل وأبسطها لتلبية حاجاتهم ورغباتهم، والتي تتراوح بين الحاجة إلى المعرفة والوصول الى المعلومة الجديدة، أو الاتصال، أو الانتماء، أو الترفيه...الخ، ويبدو أن من أشهر الشبكات الاجتماعية وأكثرها جماهيرية، هناك الفيسبوك والتويتر، حتى وصل الأمر لاستخدامها كوسيلة سياسية تسهم في الحراك السياسي والاجتماعي لدول العالم، فقد ساهمت الشبكات الاجتماعية منذ ظهورها في كسر الحواجز التقليدية للفضاء العمومي والتي تشكلها وسائل الاعلام التقليدية، ومع توسع استعمال الإعلام الإلكتروني بدأت نواة الفضاء العمومي الافتراضي، تتشكل تدريجيا لتبلغ ذروة التبلور مع توسع استخدام الفيسبوك واليوتيوب بشكل اساسي، مستغلا حالة الكبت الإعلامي الذي يعيشه الفرد العربي نتيجة الرقابة المفروضة على وسائل الإعلام التقليدية.([٧])

٤- فواعل الأمن السيبراني، في الإعلام: تتكون تركيبة الفواعل في الفضاء السيبراني من مستويين، الأول على المستوى الدولاتي، أمَا الثاني فهو على المستوى اللادولاتي:([٨])

أ-الفواعل الدولاتية: وهنا نُشير أساسا إلى الاحتكار القانوني والمُنظم للدولة للفضاء الافتراضي، من خلال مختلف أجهزتها(وزارات، وحدات الأمن...الخ)، حيث تعد الدولة فاعل محوري في تسيير الفضاء الافتراضي انطلاقا من إمكاناتها المادية والبنيوية والبشرية والقانونية، ولذلك لابد للدولة من التحكم في مجال الفضاء السيبراني، وهو

الفضاء الذي يزاحمها فيه العديد من الفواعل الأخرى، التي قد تصل حد تهديد مصالح الدولة نفسها، بل وممارسة كل أنواع الحروب النفسية الافتراضية على مواطنيها.

ب-الفواعل اللادولاتية: هنا يأتي دور الأفراد والجماعات والمنظمات غير الحكومية والشركات اللذين أصبحوا بإمكانهم التحكم في توجهات الدول وإدارتها وفق سياسات معينة من خلال الفضاء السيبراني، ومن أهم هذه الفواعل كالتالي:

أ-الفرد: أضحى الفرد فاعلا مهما في الفضاء السيبراني، حتى أنَه له القدرة على إحداث الثورة الرقمية، وتُصبح تلك الثورة مجال استخدام للدولة نفسها، ومثال ذلك ما قام به "مارك زوكربيرغ" عام ٢٠٠٤، حين أسَس شبكة فيسبوك لتستقطب أكثر من مليار مستخدم عبر العالم.

ب-المنظمات غير الحكومية: تعتمد هذه المنظمات بشكل كبير على شبكة الانترنت ووسائل التكنولوجيا الحديثة في تعبئة الرأي العام، والضغط على الحكومات من خلال ترتيب الحملات الاجتماعية وتعبئة المجتمع المدني من أجل الضغط على الحكومات للتغيير في سياسات معينة، مثل ما تقوم به اليوم معظم منظمات البيئة العالمية على اثر قرار الرئيس الأمريكي (دونالد ترامب) التخلي عن اتفاقيات التغير المناخي.

ج-المجموعات الافتراضية: هنا يأتي دور القراصنة (Hackers) وغالبا ما يسعون لتحقيق أهداف مختلفة (ربحية، سياسية، إيديولوجية...)، ومثال ذلك نجد المجموعة الافتراضية المشهورة (Anonymous)، والتي تسعى لتسويق خطابات ومطالب سياسية في العالم.

٥-أنواع الهجمات السيبرانية وعلاقتها بأجيال الحرب النفسية التقليدية والافتراضية:
هنالك أنواع عديدة للهجمات السيبرانية اوسعها هي:([٩])

- **سرقة كلمات المرور للمستخدمين للتسلل في النظام:** مثل التخمين والخداع والبرمجيات الخبيثة والنفاذ إلى ملف تخزين كلمة المرور والسطو على كلمات المرور السرية والتجسس على المستخدمين.
- **هجمات رفض أداء الخدمة "إنكار الخدمة"** (هجمات دوس DDOS) والتي تستخدم لزيادة التحميل على الانترنت والبنية التحتية للشبكات والخدمات وهو يزعج الشركات والمنظمات، على العكس من التقنيات التي يستخدمها مجرمو الانترنت، فهي تمنع المستخدمين الشرعيين من الوصول إلى المنتجات والخدمات ويمكن أن يرتكبها فرد أو جماعة، باعتمادها على العديد من الروبوتات.

- **الهجمات الطمسية:** عن طريق استبدال الصفحات بغيرها بهدف الشك والتقلب.
- **هجمات البنية التحتية:** تستهدف شبكات الكهرباء والاتصالات والأغذية والصرافة والمالية والمهام الحكومية...الخ.
- **قراصنة المعلومات:** يتمثل ذلك في الهاكرز والأنونميوس والكراكرز، فالهاكرز: هما المبرمجين القادرين على التعامل مع الكمبيوتر ومشاكله بدراية احتراف ويقدمون حلولاً لمشاكل البرمجة بشكل تطوعي وهما نوعان:

-المحترفون: والذين يستخدمون برامج او تقنيات في محاولات للاختراق الانظمة والاجهزة للحصول على معلومات سرية او للتخريب.

-المبتدؤون: يتسللون عبر الشبكات الهاتفية اعتمادا على تقنية غير قانونية وهما من أخطر أنواع الهاكرز، وأحد أخطر ممارسي الحروب النفسية الافتراضية في العالم.

6-الأسلحة الإلكترونية واستراتيجيات الدول لحماية أمنها في عصر الفضاء السيبراني:

ظهرت أساليب جديدة للتسلح والدفاع، وبعد ظهور فيروس ستاكس نت عام ٢٠١٠، كانت نقطة تحول هامة في مجال الأسلحة الإلكترونية لأنه تحول من مجرد اتلاف أو سرقة المعلومات أو تعطيل الأنظمة إلى مرحلة متطورة وهى إصابة المكون المادي والذى تمثل في تطوير المنشآت والمفاعل النووي.(١٠)

وفى المستقبل سيكون الصراع على المعرفة والتي تلعب الدور الحاسم في الصراع على السلطة على الصعيد الدولي والمؤسسات، الهجوم الإلكتروني يعد بديلاً عن السلاح النووي، ولا يحتاج إلى حدود جغرافية معينة ولا يوجد في نظام الانترنت نظام رادار كما في الحروب العسكرية التقليدية لاكتشاف مصدر الهجوم والبيانات على شبكة الانترنت، وهى ليست محمية بدرجة عالية من الكفاءة، ولذلك يسهل اختراقها والتلاعب بالبيانات والمعلومات المتواجدة عليها، والبيئة السيبرانية، هي من صنع الإنسان، ولذلك فهي متقلبة وتتفاوت هذه القوة بين الفاعلين من دون الدول، ومن ضمن أسلحة الفضاء السيبرانى هي الفيروسات والبرمجيات الخبيثة وبرامج التجسس والتي تستخدمها بعض الشركات أحياناً.(١١)

وكانت ثورة المعلومات وظهور الأنترنت إيذانا ببزوغ العصر السيبري، وخلق بيئة جديدة هي الفضاء (السيبراني – space Cyber) إضافة إلى الأرض والبحر والجو

والفضاء الذي أصبح يؤثر في النظام الدولي، خاصة مع بروز شكل جديد من القوة هو القوة السيبرانية (Cyber power) التي توزعت وانتشرت ببن عدد أكبر من الفاعلين على المستوى الدولي والمحلي، ما جعل الفضاء السيبراني مجالا جديدا للصراع ببن الدول.([١٢]) متسلحا بدعم الحرب النفسية الافتراضية وأجيالها في مختلف الازمان.

7- أهمية الأمن السيبراني وارتباطه بالإعلام والحرب النفسية الافتراضية، وأنماط التهديدات السيبرانية:

تقسم التهديدات السيبرانية التي تواجهها الدول والأفراد إلى أربعة أنماط رئيسية هي:([١٣])

أ-هجمات الحرمان من الخدمة: إذ يتم إطلاق حزمة كبيرة من الطلبات والمهمات على خوادم الضحية بصورة تفوق قدرة الخادم أو الجهاز على معالجتها والاستجابة لها، مما يؤدي إلى توقفه بصورة جزئية أو كلية أو إبطاء عمله، وهذا ما يسبب ضرر للمستخدم النهائي، وهي تستعمل كثيرا ضد مواقع الأنترنت أو البنوك أو المؤسسات من أجل التأثير عليها أو لدفع فدية مالية، مثل تهكير برنامج (البشير شو) كل جمعة.

ب-إتلاف المعلومات أو تعديلها: ويقصد به الوصول إلى معلومات الضحية عبر شبكة الأنترنت أو الشبكات الخاصة، والقيام بعملية تعديل البيانات الهامة دون أن يكتشف الضحية ذلك، فالبيانات تبقى موجودة لكنها مضللة قد تؤدي إلى نتائج كارثية خاصة إذا كانت خطط عسكرية أو مواعيد آو خرائط سرية.

ح-التجسس على الشبكات: ويقصد به الدخول غير المصرح والتجسس على شبكات الخصم، دون تدمير آو تغيير في البيانات، والهدف منه الحصول معلومات قد تكون خطط عسكرية أو أسرار حربية، اقتصادية، أو مالية، أو سياسية، مما يؤثر سلبا على مهام الخصم.

د-تدمير المعلومات: وبتم في هذه الحالة مسح وتدمير كامل للأصول والمعلومات والبيانات الموجودة على الشبكة، يصطلح عليه **"تهديد لسلامة المحتوى"** ويعني بها إحداث تغيير في البيانات سواء بالحذف أو التدمير من قبل أشخاص غير مخولين.

وهناك من يميز بين عدة أنواع لمخاطر التهديدات السيبرانية نذكر منها:([١٤])

أ-التعرض لسرية الاتصالات التي تطال البريد الالكتروني، والدخول إلى الأنظمة والملفات دون إذن، وهذا يعد اعتداءا على الحريات والحقوق الشخصية.

ب-التلاعب بالمعلومات الموجودة في نظام معين، وتشويهها او إتلافها، عبر الاختراق أو نشر الفيروسات.

ح-الجرائم العادية تستخدم الأنترنت، كالسرقة والغش وسرقة الهويات، والاعتداء على الملكية الفكرية وغيرها.

د-الجرائم التي تندرج في إطار الجريمة المنظمة، والتي تهدد امن الأفراد والدول، كتبييض الأموال والإرهاب.

8- العلاقة بين الإعلام والأمن السيبراني:

ان العلاقة المباشرة بين الإعلام والأمن السيبراني تشكل تمظهرا واضحا في افق التصدي للظواهر الخطرة والتداعيات المرتبطة بها، لمعالجة تلك التداعيات المتعلقة بالفضاءات السيبرانية وارتباطها بالإعلام، وأمن المعلومات، إذ أن الاهتمام بالأمن السيبراني يأتي من الحرب السيبرانية التي أصبحت جزءاً لا يتجزأ من الحرب النفسية الافتراضية، ويلتحق ايضا بالتكتيكات الحديثة للحروب والهجمات بين الدول، وفي هذا الاطار يشير دوغلاس كيلنر (Douglass Kellner) الى أن الانترنت يوفر مدى عريض من المعلومات، والرؤى، ووجهات النظر الصادرة عن العديد من المصادر ذات التوجهات المختلفة، كما يعد الانترنت الطريق الاسرع للحصول على المعلومات مقارنة بالوسائل المعلوماتية الأخرى، ونظرا لأن آليات هذا الإعلام الجديد، تقوم على دعم الحوار، والنقاش الجماهيري، من ثم فإن تلك المسوغات مجتمعة ترجح الرأي القائل بأن الأنترنت يمثل رافدا مهما لتفعيل وتنشيط العملية الديمقراطية، وإعادة الحيوية إليها.([١٥])

٩ــ معرفة طبيعة التحديات التي يواجهها الامن السيبراني بالترافق مع اجيال الحرب النفسية الافتراضية:

يقول الفين توفلر: أن أساليب التسلح الجديدة تعتمد على المعرفة وتكنولوجيا ووسائل جمع المعلومات ومعدات الكترونية شديدة التطور([١٦]) ومن هنا فأن تمظهرات الأمن السيبراني والإعلام وعلاقتهما بصناعة الحرب النفسية الافتراضية وفق تحولات المشهد الاتصالي الجديد، يتخذ بعدا موازيا للتطور التقني الفعال، ذلك ان الإعلام المفتوح والتدفق المعلوماتي الكبير جعل الحرب النفسية تتصدر الاولويات في الرصد والتحليل، وأحدثت الحروب المعلوماتية في ظل التطور التقاني تأثيرات كبيرة في كل دول العالم، محققة أهدافا استراتيجية لهذا النوع من الحروب اوسع مما خطط لها.

أ-الحرب النفسية الافتراضية: مفهوم الحرب النفسية الافتراضية: استخدام أية وسيلة بهدف التأثير على الروح المعنوية وعلى سلوك اية جماعة، واول من استخدم اصطلاح الحرب النفسية بصورة صريحة وواضحة في عام ١٩٥٤، المفكر العسكري الامريكي

(لينار برجر) ومن يومها تلقفه العالم واصبح من المصطلحات المهمة التي استحدثت على نطاق واسع، وعرفها بأنها: استخدام الدعاية ضد العدو مع اتخاذ اجراءات عملية اخرى ذات طبيعة عسكرية او اقتصادية او سياسية، ويرتكز على نقطتين رئيسيتين هما:

- اقتصار العمل النفسي على الروح المعنوية، وهي جزء من العمل النفسي الشامل للتأثير على افكار واتجاهات وسلوكيات الفرد عن قناعة لرفع الروح المعنوية لوقت محدد دون ان تكون هناك قناعة بالدوافع والمؤثرات.
- ترتبط بغرض عسكري محدد، اي لا يبين استخدامها الا وقت الصراع المسلح وضد غدر العدو.

ب-خصائص الحرب النفسية: تعد احد الاسلحة الفعالة التي تسير جنبا الى جنب مع الحرب الميكانيكية الميدانية او قبلها او العناصر المهمة في الحرب الشاملة وتسهم الى حد كبير في تحقيق بعدها؛ فهي احد اهدافها، ولا تقتصر العمليات النفسية على اوقات الحرب، وانما تستخدم ايضا في اوقات السلم، وذلك كما كان سائدا ابان الحرب الباردة بين المعسكر الشيوعي والرأسمالي، كما انها لا تلتزم بقوانين او اعراف دولية او دينية او مبادئ الرقابة المتفق عليها دوليا، كما هو الحال في الحروب العسكرية التقليدية.

ت-اهداف الحرب النفسية: للحرب النفسية عدة أهداف أبرزها:

- **اهداف سياسية:** ترتبط العمليات النفسية ارتباطا وثيقا بسياسات الدولة التخصصية والاهداف تهدف الى تحقيق اهداف (خلق الانفعالات- الاتجاهات- السلوك) سياسية والغايات القومية مختلفة، سواء من حيث التخصص (سياسية- اقتصادية- عسكرية...الخ) او من حيث البعد الزمني (اهداف سياسية بعيدة- منظورة- قريبة) اقناع الرأي العام العالمي/ الاقليمي، بحدث معين، وكذلك عزل العدو عن اصدقائه/حلفائه وكسب التأييد من جانب الحلفاء والاصدقاء.
- **اهداف داخلية:** توجه اساسا الى الجهة الداخلية للعدو وتهدف الى:

-اثارة الفتن والنعرات القبلية والعرفية والنازعات الطائفية بالمجتمع الداخلي للدولة الهدف.

-العمل على زعزعة ثقة الافراد والجماعات في نظام الحكم واثارة الفرقة وافتعال الازمات.

-محاولة النيل من ثقة الشعب في قواته المسلحة.

-العمل على افقاد الشعب الثقة في نظامه الاقتصادي والاجتماعي والايديولوجي.

- **اهداف عسكرية:** زيادة الاستعداد النفسي لكل من افراد الشعب والقوات المسلحة، حيث تبدأ قبل وخلال وبعد مرحلة الصراع المسلح لزيادة الثقة وغرس الروح العسكرية لدى افراد الشعب، من خلال المحافظة على الروح المعنوية لكل افراد القوات المسلحة اثناء فترة الصراع المسلح، ومن الجانب الأخر، زرع الرعب والخوف في نفوس العدو.

ث-أنواع الحروب النفسية الافتراضية: ومنها:

- **الحروب المعلوماتية:** في عصر المعلومات تحولت الحروب الى حروب معلوماتية، فلم تعد القدرة العسكرية هي الاساس، بل اصبحت للبيانات والمعلومات وأدواتها هجمات معلوماتية تحقق الاهداف بأقل عدد من الخسائر البشرية، وفق الفضاء السيبراني، كذلك مازال الانسان يحاول البحث عن طرق لجعل الاسلحة أكثر ذكاء بهدف التقليل من الخسائر وما زال يبحث عن الطرق البديلة للاستخدام البشري في ساحات القتال ومازال يبحث عن اراض جديدة لتكون ساحات للقتال فوجد ان الساحات الافتراضية والمنصات الدعائية وخطوط الشبكة العنكبوتية مجالا خصبا لتحقيق هذه المواقف، حيث يضع العسكريون الحروب المعلوماتية في قائمة الحروب غير المتساوقة في عملياتها طرقا غير تقليدية تمارسها مجاميع محدودة من المهاجمين تمنح المعلومات لأفراد فرصة أحداث خلل كبير في منظومة المعلومات المحلية التي تديرها، وفيها ثلاثة مستويات هي:
- **حرب الشبكات:** وهي المعلومات ذات الصلة بالصراع مع المستوى الكبير بين الامم والمجتمعات وتشمل تعطيل وارباك وتدمير البنية التحتية لدى الخصم.
- **الحرب السيبرانية:** تتعلق بالعمليات العسكرية التي تتم وفق المبادئ المتصلة بالمعلومات.
- **الارهاب السيبراني:** وهو استخدام الارهاب للمعلومات ومهاجمة البناء التحتي المعلوماتي اي عمليات مخططة تصاحبها معلومات ومؤثرات منتقاة موجهة للتأثير على مشاعرهم ودوافعهم وتبريراتهم بأقصى درجة لسلوكيات الاخرين.
- **الحروب المدمجة:** اندماج تقنيات اتصالية هي الاقمار الصناعية والكمبيوتر والنظام الرقمي يؤدي الى تغيير سريع في الثقافات وانهيار ثقافات أخرى.
- **حروب التقنيات الدعائية الكثيفة:** استخدمت في عدة حروب إذ تلجا الاطراف المتحاربة كنوع من الاسلحة المكملة هدفها التأثير في العدو وبث البلبلة في

صفوفه واختراقه نفسيا، باستخدام التقنيات الدعائية كاستخدام المجاميع الارهابية داعش وغيرها.

- **الحروب السيكولوجية الالكترونية:** الحرب النفسية الالكترونية اثبتت فعالية الانترنت كسلاح دعائي في الحرب النفسية وأعطت للصراع بعدا أخر، فالعمل الدعائي على الانترنت يتطلب استراتيجية ذكية تكمن في وضع قائمة بأسماء الشخصيات الفاعلة واغراق صناديقها الالكترونية بالرسائل الدعائية من كل نوع، ومن ابرز الاسلحة المستخدمة في الحرب النفسية الالكترونية هي:

-حروب التضخم المعلوماتي وإغراق الخصم بالمعلومات: حتى يصعب عليه التمييز بين الخطأ والصواب، كما حصل في القضية السورية وكما حدث سابقا قبل احتلال العراق وبعده، وكان أكثر بروزا في القضية الفلسطينية.

-حروب التجهيل والتضليل: من خلال بث بعض المعلومات بأساليب معينة تؤدي الى دفع الجمهور لاتخاذ ردود افعال ومواقف طبقا لما تريده تلك القوى المسيطرة على عملية تدفق الاخبار وتؤدي الى زيادة الخوف لدى الجمهور والخضوع لسياسة الخصم وهذا ما اتبعته الولايات المتحدة عقب أحداث ١١ ايلول ٢٠٠١، ومن ثم احتلال افغانستان والعراق.

-حروب الارهاب المعلوماتي: نوع من انواع العنف للتأثير في الرأي العام أو إثارة الرعب والخوف والهلع في المجتمع المستهدف، عبر بث فيض من المعلومات وتدفقها تجاه الجمهور المستهدف.

-حروب الارهاب السيبراني: الذي يسعى الى بث المتبنيات السياسية لخلق القلق المستمر في المتلقين ويتضح سياسيا أكثر من اي غرض أخر وخاصة في البرامج السياسية.

ح-**حروب الاستعمار الإعلامي:** تتعرض فيها ملكية وسائل الإعلام وتركيبها ومضمونها في دولة ما لضغوط خارجية من المصالح الإعلامية لدول أخرى، مما يستدعي الضغوط الكبيرة عليها ومن ثم الحاق الاذى والملاحقة نفسيا ودعائيا وهو ما يسميه البعض بالاستعمار الإعلامي الجديد وفق معطيات البيئة التقنية الحديثة وأدواتها.

ج-**حروب استعراض القوة:** يتم ذلك عن طريق نظم الإعلام الالكتروني والسعي لتوجيه خطابات عن حجم تلك القوة لخلق الرعب والخوف تجاه الاخر المختلف.

خ-**حروب القوة الناعمة:** باستخدام القوى اللينة وطبيعتها الرمزية لجذب وترغيب الاخر لأجل انتزاع الارادة الجماعية: وتتجه وفق خمسة أنواع: حروب عسكرية/ حروب

سياسية/ حروب اقتصادية/ حروب الاستعمال الاتصالي/ الحروب الثقافية/ حروب الاجهزة الالكترونية.

د-**حروب القوة والتحكم بقدرات الأخر:** هذه الحروب تعتمد على السيطرة على كل الاتجاهات من خلال الاتصال على النحو الاتي:

- التهديد بالسيطرة النووية عبر الترويج في مختلف وسائل الإعلام الالكتروني.
- التهديد بالسيطرة السياسية من خلال الخطاب الإعلامي في مواقع التواصل الاجتماعي.
- التهديد بالسيطرة الاقتصادية من خلال الخطاب الإعلامي في المواقع الالكترونية.
- التهديد بالسيطرة الثقافية عن طريق ادخال قيم وتقاليد عبر الإعلام الالكتروني المفتوح.

ذ-**حروب الشبكة العنكبوتية:** ويتضح ذلك من خلال:([١٧])

- تفعيل موضوعة الحصار الافتراضي من خلال ضخ معلومات عبر المواقع الالكترونية تتسبب بتشويش المتلقي.
- تزاحم الفيضان المعلوماتي الذي يؤدي الى فقدان القدرة على الاحاطة بكل تفاصيل الموضوعات.
- استخدام الهاكرز لكل المواقع، وقضية سرقة البيانات التي اتهم بها مارك زوكربيرغ دليل على حرب نفسية من خلال استخدام بيانات الاشخاص والدول ضدهم.
- توظيف الفايروسات في مختلف مواقع شبكات المعلومات الوطنية بقصد إحداث خلل يجعل المستخدم في حالة من الهلع والخوف مما يؤثر على الحالة النفسية للمتلقي.
- محاولة الاغراق بالمعلومات من خلال ضخها بطريقة مشوهة ومزيفة.
- حجب المعلومات عن الكثير من المشكلات الكثيرة التي تحدث في مختلف البلدان.
- تجهيل المعلومات وتزييفها وعدم أمداد المتلقي بالمعلومات اللازمة.

- ارتباط حروب المعلومات كثيرا بعمليات الاتصال.
- السعي الى قولبة الصراع مع الخصم ليتخذ اسلوب مهاجمة العقول وتشكيل نمط إدراكي جديد يساهم في تغيير الرأي العام أتجاه القضية التي تطرحها وسائل الإعلام الالكترونية.

ر-**حروب التسريبات:** وهي حروب نفسية اعتمدت على تسريب المعلومات التي تتعلق بأشخاص حكوميون ومسؤولون محليون ودوليون، كشفت عن الكثير من السلوك السياسي المتعلق باستحواذ على حقوق الاخر أو سرقات، أو كومشنات، أو قضايا مختلفة تمس الأمن المدني للمواطنين أو الأمن الاقتصادي أو الاجتماعي، مثل تسريبات ويكيليكس ووثائق بنما التي زرعت الخوف والرعب النفسي في نفوس الاشخاص المتهمين بها.

ز- **حروب مواقع التواصل الاجتماعي:** وهي حروب نفسية علنية تتعلق بكشف فضائح وافعال غير سوية للأخر سواء اكان مواطنا عاديا أم من ذوي المناصب وغيرها والتي تحاول جهة ان تنتقم او تنتقص أو تسقط هذا الشخص او ذاك لأسباب سياسية او اجتماعية او مصلحية عموما، وقد تبنت مواقع التواصل الاجتماعي تلك الحملات المكثفة عن مختلف الموضوعات، وفق الفضاءات السيبرانية، وبثت فيديوهات تشهر بأسماء مشهورة ومعروفة ومحاولة زرع الرعب والخوف فيها، أو كتابة التغريدات على التويتر لأغراض سياسية واضحة غرضها التخويف والابتزاز كما يفعل الرئيس الامريكي ترامب في تغريداته السياسية وتوعده للعالم المختلف معه، كما تتضح حروب مواقع التواصل الاجتماعي عند حدوث مشكلات سياسية في مختلف دول العالم، ومنها المنطقة العربية، يصحبها التلاسن والتلاعن والتشاتم، وأبلسة الخصم وشيطنته في منصات الفيسبوك كلما حدثت مشكلة او تفاعلت قضية، ومثله كل أنواع مواقع التواصل الاجتماعي، مما يركز على إثارة انفعال المتلقي المقصود ومن ثم زرع الرعب والخوف في نفوس المتلقين، ويعد تهديدا للأمن السيبراني.

س-**حروب الالعاب الالكترونية الخطرة:** وابرزها العاب الذكاء الاصطناعي، او العاب قاتلة للمستخدم كما في لعبة (مريم) و(الحوت الازرق) ولعبة (البو بجي) إذ تعد آلية العمليات النفسية التي تستعملها الدول حاليا في ادارة الحروب الحديثة، ذات ذكاء اصطناعي فاعل، كالألعاب الذكية الخطرة التي تؤدي بمستخدمها الى الانتحار، لذا تعتمد الحرب النفسية الافتراضية على مجموعة من الخبراء والمحللين والمعلومات النفسية، فضلاً عن وجود اقتصاديين وعسكريين واجتماعيين بهدف وضع استراتيجية وخطة متكاملة على المديين الطويل والقصير من اجل اعداد البيانات والمعلومات التي تحد من هذه الخطورة.

ش-**حروب الروبوت(الذكاء الاصطناعي):**اسهمت ثورة المعلومات والاتصال في احداث تحول على المشهد الاعلامي في العقد الاخير من القرن العشرين، وشهد العصر الذي نعيشه تطورات هائلة، واضحى يطلق عليه الاعلام الجديد، وعصر المعلومات والاعلام الاجتماعي واعلام الوسائط المتعددة، وقد ادت هذه التطورات في وسائل الاعلام الى تغييرات في قدرات الدولة، وهددت أمنها، اذ باتت المعلومات عناصر مهمة ومؤثرة في تامين استقرار الدولة، ودعم نفوذها الاقليمي، وهناك العديد من التقارير الصادرة إما عن جهات مهتمة في بيع الحلول الأمنية في تكنولوجيا المعلومات والاتصالات مثل شركات ماكافي (MacAfee) وسيمانتيك (Symantec) وكاسبيرسكي (Kaspersky)أو عن جهات أخرى تناقش القضايا الأمنية الأعم أو تهتم في أمن ما يخصها من أنظمة ومنتجات تكنولوجيا المعلومات، أما فئات أساليب الجريمة السيبرانية التي يغلب تناولها في هذه التقارير فهي كما يلي:([١٨])

-الشفرة الخبيثة أو البرمجيات الضارة: برمجيات قائمة على النية المبيتة لمبرمجها وليس على أي سمات خاصة، وتشمل البرمجيات الضارة فيروسات الحاسوب والديدان وأحصنة طروادة وبرمجيات التجسس والبرمجيات الدعائية المخادعة والبرمجيات الإجرامية ومعظم الجذور الخفية وغيرها من البرامج الخبيثة وغير المرغوب فيها . وقد رصدت شركة سيمانتيك زيادة التهديدات الخبيثة الجديدة من ٦٢٤٠٠٠ إلى٦٥٦٠٠٠ تهديدا ما بين العامين ٢٠٠٧ و٢٠٠٨.

-الرسائل الاقتحامية: إساءة استخدام أنظمة الرسائل الإلكترونية (بما في ذلك معظم وسائط البث، وأنظمة التسليم الرقمي) لإرسال الرسائل غير المرغوب فيها بالجملة من دون تمييز، وأكثر أشكال الرسائل الاقتحامية شيوعاً البريد الإلكتروني الاقتحامي أو رسائل البريد الإلكتروني غير المرغوب فيها ذات المضمون التجاري والمرسلة بكميات كبيرة، بيد أن الرسائل الاقتحامية تُرسَل على نحو متزايد بنية إجرامية فتحوي برمجيات ضارة أو تسعى للإيقاع بالناس لحملهم على أداء دفعات مالية أو الإفشاء بمعلومات وما إلى ذلك، ولإخفاء عنوان المرسل وتمكين حجم عال من الإرسال، كثيراً ما يستخدم المجرمون حواسيب مأمورة (zombies) أو (مسيّرة) (bots) حواسيب الآخرين التي تنقاد عن بعد في إطار تحكم خارجي دون علم المالك أو (شبكات من الحواسيب المأمورة) وتدعى أيضاً شبكات الحواسيب المسيّرة (botnets) وتشير التقديرات إلى أنه في عام ٢٠٠٨، أُرسل ما مجموعه ٣٥٠ مليار رسالة اقتحامية، ٩٠ في المائة منها عن طريق شبكات الحواسيب المسيّرة. ويشكل ذلك قرابة ٨٥ في المائة من مجموع الرسائل في جميع أنحاء العالم.

-التصيد الاحتياطي: تقوم مواقع الويب والاستضافة للتصيد الاحتيالي بتقليد أو انتحال صفة موقع الويب أو عناوين البريد الإلكتروني لكيانات جديرة بالثقة (مصارف على سبيل المثال) مع القصد الجنائي الرامي للحصول على معلومات حساسة مثل كلمات المرور، أو أسماء أو تفاصيل بطاقة ائتمان، إذ يمكن تثبيت برمجيات ضارة على الحاسوب الذي سيوجه المستخدم إلى موقع ويب للتصيد الاحتيالي بدلاً من الموقع المقصود الموثوق به، أو يمكن إرسال رسائل اقتحامية بعناوين منتَحلة تدعو المستخدم للنقر على وصلة إلى موقع تصيد احتيالي، وقد اكتشفت التقارير زهاء ٥٥٠٠٠ موقع يستضيف التصيد الاحتيالي في عام ٢٠٠٨، بزيادة قدرها ٦٦ في المائة مقارنة بعام ٢٠٠٧.

ص- حروب التغريدات: أو ما يسمى **بـ"**سلاح التويتات" وهي عبارة هزلية لكنها تلخص ما جاء في دراسة مركز "بروكينجز" الأمريكي والتي أعدها خصيصا عن تنظيم "داعش الإرهابي" وكشفت مدى استفادة التنظيم من الأساليب المتطورة عن طريق شبكة الإنترنت لاستقطاب أعداد كبيرة من المجندين في صفوفه حيث يعتمد على أكثر من ٤٥ ألف حساب على تويتر الإلكتروني من أجل الترويج ونشر لحملاته الدعائية عبر مواقع التواصل الاجتماعي، إذ أن نحو ٤٥ ألف شخص من مستخدمي موقع تويتر ممن تمكن تنظيم "داعش" الإرهابي من تجنيدهم لصالحه يعملون على نشر دعايات التنظيم الإرهابي ورسائله، ولديهم آلاف الحسابات الإلكترونية التابعة لهم الأمر الذى أسهم بتطورهم بشكل متواصل على الرغم من محاولات تعليق أعمالهم وحساباتهم على الإنترنت، في محاولات اعتبرت ناجحة لوقف أعمال هؤلاء الأشخاص ووقف انتشارهم، أما عن الكيفية التي استخدم بها التنظيم الإرهابي شبكة الانترنت ومواقع التواصل الاجتماعي فلم تكن غامضة، فقد كان من الضروري استهداف مستخدميه الأكثر نشاطاً، خاصة تلك الحسابات التي تعمل بطريقة منسقة لتوسيع رسائل التنظيم، كما ان موقع تويتر الإلكتروني بدأ باستهداف حسابات التنظيم قبل فترة قصيرة من نشر شريط الفيديو الذى يظهر إعدام "جيمس فولي" ([١٩])

ض-حروب الفيديوهات المسربة: وهي الحرب الالكترونية التي تدور بين الشعوب وحكامها، والتي تستخدم فيديوهات ترصد فيها الخروقات بالتعامل مع الجمهور المنتفض أو المتظاهر، إذ تدور حرب إلكترونية بين المؤيدين للأنظمة والمعارضين لها، حرب قوامها التسجيلات التي تنشر على الشبكة العنكبوتية، فعدا الفيديوهات التي تُظهر المظاهرات المؤيدة للأنظمة وتلك المعارضة لها، هناك فئة ثالثة من التسجيلات يستعملها كلا الطرفين لكنّ كلا منهما يرفقها بمعلومات تناقض الآخر، وهكذا يحصل التسجيل ذاته على عنوان مختلف وتعريف مختلف، مما يهدد الفضاء السيبراني لكلا الطرفين، خاصة وأن حرب الفيديوهات يستخدمها البعض حتى للتهديد لأفراد المجتمع،

وهو ما يسمى بالابتزاز الالكتروني، الذي يهدد العائلات من خلال فيديوهات وصور لغرض ابتزازي.

ط-حروب الطائرات المسيّرة في الشرق الأوسط: تشكل اتساع استخدام الطائرات المسيرة بدون طيار، إذ أصبحت الطائرات بلا طيّار عنصرًا رئيسًا في أهم جيوش العالم وأكثرها تقدمًا، وفي طليعتها الولايات المتحدة الأميركية التي عدّتها سبيلاً إلى (الحرب الشاملة على الإرهاب) واليوم تصنف الطائرة بلا طيّار كطائرة مُتعدِّدة المهام في العمليات العسكرية الحاليّة والمستقبليّة، وتتميَّز الطائرات بلا طيّار العسكريّة بعدّة خصائص، منها:([٢٠])

١-وضع تقارير متواصلة عن الأحوال الجويّة فوق مسرح العمليّات العسكريّة.

٢- تخفيف التشويش المعادي لأجهزة استقبال بيانات نُظم تحديد الموقع الجغرافيّ (GPS).

٣-التشويش على منصّات إطلاق الصواريخ (نشر رقائق معدنيّة، مثلاً) وبطاريات الدفاع الجوّي.

٤-التحكم الجوي الأمامي الذي يُمكِّن الطائرة بلا طيّار من القيام بثلاث مهمّات أساسيّة (العزل الجوي، والدعم الجوي القريب، والبحث والإنقاذ خلال القتال).

٥- تعقُّب الأهداف وتعليمها أو إضاءتها ليلاً لمُعاونة الطائرات الهجوميّة التي تستخدم منظار الرؤية الليلية، وكشف الأهداف المُعادية.

٦-تقوية محطات الإرسال.

٧- التحوُّل إلى صاروخ مُوجَّه عند فشل المهمة أو وجود هدف حيوي يجب تدميره.

٨- اكتشاف الأهداف الجوية، على مختلف الارتفاعات، وإنذار القوات العسكريّة بشكل مُسبق للتعامل معها.

٩-قيادة عمليات المقاتلات الاعتراضيّة وتوجيهها.

١٠-توفير المعلومات اللازمة لتوجيه الصواريخ أرض/جو،

١١- مُتابعة القاذفات والطائرات الصديقة أو الحليفة وتوجيهها.

١٢-عمليات الإنقاذ والاستطلاع البحري.

١٣-توفير المعلومات اللازمة لمراكز العمليات العسكريّة والقوات البريّة.

١٤- تنظيم حركة الملاحة الجويّة.

١٥- رصد أفراد الحركات أو التنظيمات المُعادية وعناصرها وتعقُّبهم ومن ثمّ اغتيالهم.

وهناك أهم تقنيات الكشف والاعتراض للطائرات المسيرة، وابرزها:

١-الكشف والتتبع، على الرادار.
٢-رصد الترددات اللاسلكية، والكاميرات الكهربائية البصرية.
٣-أجهزة الاستشعار العاملة بالأشعة تحت الحمراء.
٤-أجهزة الاستشعار الصوتية التي تكشف الصوت المميز الذي يصدره النوع الشائع من الطائرات دون طيار.

وهناك أهم طرق التصدي للطائرات المسيرة:

١- تشويش الصلات اللاسلكية.
٢-تشويش أنظمة تحديد المواقع العالمية.
٣- الانتحال: تقنية للسيطرة على طائرة بدون طيار من خلال الاستحواذ على رابطة الاتصالات الخاصة بها
٤-أجهزة الليزر، والموجات الكهرومغناطيسية، وأنظمة الشِّباك أو التشابك الأخرى.
٥-المقذوفات الحركية، وثانية على الجمع بين هذه الأساليب.
٦-طريقة الشباك للالتقاط/ الصيد للطائرة.
٧-استخدام الصقور لاعتراض الطائرة او التقاطها.

ج- أجيال الحروب النفسية:

- **حرب الجيل الأول:** هي الحرب التقليدية بين دولتين وجيشين نظاميين ويعرفها الخبراء العسكريون: بأنها حروب الحقبة من ١٦٤٨ حتى ١٨٦٠ حيث عرفت بالحروب بين جيوش نظامية وأرض معارك محددة بين جيشين يمثلون دول في حرب ومواجهة مباشرة. وخلال حروب الجيل الأول يتم تنفيذ عدد محدود من العمليات العسكرية وتشمل عمليات المناورة والالتفاف لتطويق الخصم وضربه في أجنحته للقضاء عليه وتدميره وبدأت هذه النوعية من الحروب مبكرًا من تاريخ البشرية واستمرت حتى منتصف القرن العشرين.
- **حرب الجيل الثاني:** يعرفها البعض بحرب العصابات والتي كانت تدور في دول أمريكا اللاتينية ويعرفها الخبير الأمريكي ويليام ليند بالحرب الشبيهة بالجيل الأول من الحروب التقليدية ولكن تم استخدام النيران والدبابات والطائرات بين العصابات والأطراف المتنازعة، وتتميز حرب الجيل الثاني بخصوصية أكثر دقة من ناحية القدرة على إحداث أكبر قدر ممكن من الخسائر في طرفي النزاع وهى حرب لها استراتيجيتها وفكرها الخاص فهي تنشأ من الصراع المستمر والطويل مما يحتم عليها اتخاذ تدابير معينة ومحددة تتبع فيها أسلوب المفاجأة والمباغتة في القتال ضد التنظيمات العسكرية التقليدية مدعمة

بتسليح أقل عدداً ونوعاً من تسليح الجيوش بحيث تقاتل في ظروف غير ملائمة للجيش النظامي بما يحقق ضربات موجعة للعدو في معارك ومواجهات صغيرة ومتعددة تحقق لهم الهدف الأساسي وهو إضعاف قدرة الخصم وجعله يتراجع عن أهدافه تحت ضغط الضربات المتلاحقة من خصم يظهر ويختفى ويقاتل وفق استراتيجية يفرض فيها نفسه وشروطه يحدد فيها مكانها وزمانها بما يضمن له النجاح فيها وتعتمد حرب العصابات على مساندة الإعلام بشكل رئيسي وذلك في تصوير ونشر العمليات العسكرية قبل عملية عسكرية أو كما يتطلب الموقف، كما أن التركيز في استخدام الحرب النفسية والدعاية مهم بالنسبة لعناصر حرب العصابات وذلك لكسب المزيد من الأنصار والتبرعات بالأموال.

- **حرب الجيل الثالث:** يعرفه البعض بالحروب الوقائية أو الاستباقية، كالحرب على العراق مثلا، ويعرفها الخبير الأمريكي ويليام ليند ويصفها بأنها طوُرَت من قبل الألمان في الحرب العالمية الثانية وسميت بحرب المناورات وتميزت بالمرونة والسرعة في الحركة واستخدم فيها عنصر المفاجأة وأيضاً الحرب وراء خطوط العدو، وتتميز العمليات الخاصة بحروب الجيل الثالث باستخدام سلاح الطيران والقاذفات الاستراتيجية، والصواريخ الموجهة على وجه الخصوص ولعل ما شاهده وسمع العالم عنه في حرب العراق الثانية يلقى كثيرًا من الضوء على نوعية هذه الحروب وتصاحبها في العادة حملات إعلامية مركزة.
- **حرب الجيل الرابع:** اتفق الخبراء العسكريون بأن حرب الجيل الرابع هي حرب أمريكية صرفة، طورت من قبل الجيش الأمريكي وعرفوها بـ(الحرب اللامتماثلة)، حيث وجد الجيش الأمريكي نفسه يحارب لا دولة بعد أحداث ١١ سبتمبر ٢٠٠١، بمعنى آخر محاربة تنظيمات منتشرة حول العالم وهذه التنظيمات محترفة وتملك إمكانيات ممتازة ولها خلايا خفية تنشط لضرب مصالح الدول الاخرى، كالمرافق الاقتصادية وخطوط المواصلات لمحاولة إضعافها امام الرأي العام الداخلي بحجة إرغامها على الانسحاب من التدخل في مناطق نفوذها ومثال على هذه التنظيمات: القاعدة، داعش... الخ، كما يطلق البعض عليها مسمى الحرب الهجينة لأنها عبارة عن نوع متميز من القتال يعجز فيه الجيش النظامي على الاطاحة بالخصم الذي يعتقد انه غير محترف، وهو عادة ما يكون كذلك لكنه يخوض حرباً غير نظامية بأفكار مبتكرة تعد خليطاً من مفهوم الحرب الشعبية والحرب الثورية، وأسلوب حرب العصابات، ومن مظاهر الجيل الرابع للحروب سعى الأفراد والمجموعات غير الحكومية للوصول إلى المعرفة المتطورة والتكنولوجيا الحديثة واستخدامها كوسائل

هجومية في معارك غير متماثلة لتحقيق المصالح الفردية والجماعية وذلك من خلال القدرة على تنفيذ الأعمال التخريبية من خلال الانترنت والوسائط الالكترونية المختلفة فيما بات يعرف بالحرب السيبرانية أو الحرب الرقمية، ومن ابرز سمات هذا الجيل من الحروب انها ليست نمطية كحروب الاجيال السابقة وتعتمد على التقدم التكنولوجي ولا تستخدم فيها الأسلحة التقليدية بل الذهنية (القوة الذكية) وتعمل على تحويل الدول المستهدفة من حالة الدولة الثابتة إلى الدولة الهشة وتستهدف الدولة بالكامل(بمن فيها المدنيون) وتتسم بعدم وضوح الخطوط الفاصلة بين الحرب والسياسة، والعسكريين، والمدنيين، وهذا ما يفسر الضبابية الشديدة وعلامات الاستفهام المحيرة لهذا النوع من الصراع، وتعد حروب الجيل الرابع المثلى هي التي تبدأ ولا يشعر بها احد، وتستخدم القوة الذكية (Smart Power)

- **حرب الجيل الخامس:** ميدانها الفضاء الإلكتروني و«النت»، وفيما يخص حرب الفضاء الإلكتروني يتطرق "جون باسيت" إلى الهجمات الإلكترونية التي يجرى تنفيذها بالتسلل عبر سلاسل الإمداد، واستغلال السلوك البشرى لإنتاج أسلحة إلكترونية واستخدامها عبر إطلاق "البرمجيات الخبيثة"، لذلك يرى أن الوتيرة المتسارعة لتطور هذه الأسلحة ونشرها تهدد بأن يتقدم هذا التطور كثيراً على الجهود الدولية الرامية إلى تأمين الفضاء الإلكتروني ليصبح مجالاً للجميع، ومع بدء عهد التواصل الاجتماعي تغيرت طبيعة وشكل التنظيم الإرهابي، فقد تمكنت التنظيمات الإرهابية كـ "داعش" وأخواتها، أنها من خلال تلك التقنية الحديثة يمكنها أن تدخل كل بيت في قارات العالم الست، وأن تلك التقنية ستحقق لها عدة أهداف، أولها وأهمها الانتشار وبث الرعب في قلوب محاربيها والأكثر اهمية تجنيد عملاء جدد يرغبون في الانتماء اليها.([٢١]) ويتحدث الكاتب الأمريكي جون روب في مؤلفه عن حرب الجيل الخامس بأن جنودها عبارة عن أفراد لا يرتدون الزي العسكري، وأنها حرب أفكار، وأنها تطلق دوامة من العنف، وتدار بأسلوب التدمير الفجائي لقوى الخصم معنوياً ونفسياً، بإطلاق عملية من شأنها إشاعة الإحباط لدى الخصم، وأن ميدانها الفضاء الالكتروني، وشبكات التواصل الاجتماعي، لنشر مشاعر الخوف، وفقدان الثقة بالنفس لدى المجتمع، وأيضا تجاه قادته السياسيين، كما إن حرب الجيل الخامس عبارة عن تطور يركز على نشر أفكار مقصودة، من خلال طاقة إعلامية مثلت ظاهرة أو لغز، ويركز على أربع وسائل رئيسية هي:

أ-استغلال شبكات التواصل عبر الإنترنت، بإطلاق معلومات مجهزة والترويج لها.

ب-العمل على خلق مجال تواصل افتراضي يسمح لمستخدمي هذه الشبكات، بإضافة معلومات من جانبهم حتى يكتمل التأثير العام .

ت-إيجاد شبكة متقاربة مع بعضها من المتابعين لهذه العملية .

ث-التصدي لكل من يظهر كمعارض لهذه العملية، والسيطرة على أي تدفق معلومات مضادة .

ويرمي برنامج الأمن السيبراني العالمي للسيطرة على الحرب النفسية الافتراضية إلى تحقيق سبعة أهداف استراتيجية رئيسية هي:([٢٢])

أ-وضع استراتيجيات لاستحداث تشريع نموذجي لمكافحة الجريمة السيبرانية يمكن تطبيقه عالمياً وقابل للاستخدام مع التدابير التشريعية القائمة على الصعيدين الوطني والإقليمي.

ب-وضع استراتيجيات عالمية لإيجاد الهياكل التنظيمية والسياسات العامة الملائمة على الصعيدين الوطني والإقليمي بشأن الجريمة السيبرانية.

ت-وضع استراتيجية لصوغ معايير أمنية دنيا وخطط اعتماد للأجهزة الحاسوبية ولتطبيقات البرمجيات والأنظمة تكون مقبولة عالمياً.

ث-وضع استراتيجيات لإيجاد إطار عالمي للرصد والإنذار والاستجابة للحوادث لضمان التنسيق عبر الحدود بين المبادرات الجديدة والقائمة.

ح-وضع استراتيجيات عالمية لإنشاء وإقرار نظام هوية رقمي عام عالمي، والهياكل التنظيمية اللازمة لضمان الاعتراف بوثائق التفويض الرقمية عبر الحدود الجغرافية.

ج-وضع استراتيجية عالمية لتيسير بناء القدرات البشرية والمؤسسية من أجل تعزيز المعارف والمهارات عبر القطاعات وفي المجالات الآنفة الذكر.

خ-وضع مقترحات بشأن إطار لاستراتيجية عالمية لأصحاب المصلحة المتعددين لتحقيق التعاون والحوار والتنسيق على الصعيد الدولي في جميع المجالات الآنفة الذكر.

١٠-أستنتاجات البحث:

أ-يشمل مفهوم الحرب السيبرانية استهداف لا للقدرات والأنظمة العسكرية فحسب بل أيضاً استهداف البنية التحتية الحيوية للمجتمع بما في ذلك الشبكات الذكية وشبكات المراقبة الإشرافية وحيازة البيانات (SCADA) التي تسمح لها بالعمل والدفاع عن نفسها.

ب-أن الفضاءات السيبرانية فتحت بفضل خواصها وديناميكياتها التواصلية آفاقا غير مسبوقة للاهتمام بالأمن، وخلقت أنماط اتصالية وتشبيكية ما كان من الممكن وجودها في

مرحلة ما قبل الإنترنت، فأهمية الأمن السيبراني في المجتمع، عكسها عصر التكنولوجيا الذي أصبح لأمن المعلومات الدور الأكبر لصد ومنع أي هجوم إلكتروني قد تتعرض له أنظمة الدولة المختلفة.

ج-أن الأمن السيبراني يشكل جزءاً أساسياً من أية سياسة أمنية وطنية، وتهدف إلى حماية الفضاء السيبراني الوطني من ما تفعله المواقع الالكترونية وخلق الحروب النفسية للمتلقي، مع التركيز على ضمان توافر أنظمة المعلومات، وتمتين الخصوصية، وحماية سرية المعلومات الشخصية، واتخاذ جميع الإجراءات الضرورية لحماية المواطنين والمستهلكين من مخاطر الفضاء السيبراني.

ح-بروز الارهاب السيبراني وهو استخدام الارهاب للمعلومات ومهاجمة البناء التحتي المعلوماتي اي عمليات مخططة تصاحبها معلومات ومؤثرات منتقاة موجهة للتأثير على مشاعرهم ودوافعهم وتبريراتهم بأقصى درجة.

خ- أصبح الإنترنت هو الجهاز العصبي المركزي في المجتمع، والإنترنت الآن يتصل اتصالاً عضوياً بكل وظائف الحياة اليومية وبحياة الأفراد، مما تؤثر تأثيرا كبيرا على الأمن السيبراني للبلد.

د- تفاعل النزاع السيبراني إذ أنه ربما يشمل سيناريوهات يمكن وصفها تحت عنوان "الحرب السيبرانية"، مما يعرض ألأمن السيبراني للمخاطر والهجمات المحتملة في حالة التغاضي عنه، أو إهمال متابعته، لأن الفضاء السيبراني ميدان حروب المستقبل والحاضر.

ذ- تفاعل الحروب المختلفة لأغراض سياسية واضحة للسيطرة على الشعوب، فيما تحفزت أجيال الحرب النفسية، للتركيز على الخروقات الامنية والمجتمعية كأساليب ردعية لتلك الحرب الموجهة للعراق.

الهوامش

[1]- **محمد عبدالسلام، الحرب في زمن التغريدات.. تكنولوجيا المعارك الافتراضية، دار أكتب للنشر والتوزيع، القاهرة، ٢٠١٩، ص٥**

[2]- **سليم دحماني، أثر التهديدات "السيبرانية" على الأمن القومي- الولايات المتحدة الأمريكية – انموذجا – (٢٠١٧-٢٠٠١) رسالة ماجستير/ جامعة محمد بوضياف – المسيلة، ٢٠١٧-٢٠١٨، ص٢٢-٢٣**

[3]- **د. قادير إسماعيل، إدارة الحروب النفسية في الفضاء الالكتروني: الاستراتيجية الأمريكية الجديدة في الشرق الأوسط، متاح على الموقع الالكتروني:**
)http://www.grenc.com/show_article_main.cfm?id=29509(

[4]- **للمزيد أنظر: عادل عبد الصادق، "الفضاء الإلكتروني والرأي العام: تغير المجتمع والأدوات والتأثير"، المركز العربي لأبحاث الفضاء الإلكتروني: مجلة قضايا استراتيجية، العدد ٢٠١٣،٢٤٥٩.**

[5]- **اشرف جلال حسن، أثر شبكات العلاقات الاجتماعية التفاعلية بالأنترنت ورسائل الفضائيات على العلاقات الاجتماعية والاتصالية للأسرة المصرية والقطرية، دراسة مقارنة على الشباب وأولياء الأمور في ضوء مدخل الإعلام البديل، المؤتمر العلمي الأول، بعنوان (الاسرة وتحديات العصر من ١٥-١٧ فبراير، جامعة القاهرة، كلية الإعلام، ٢٠١٩، ص٤٧٩**

[٦]-عناصر الأمن السيبراني: متاح على الموقع الالكتروني: http://bit.ly/2XFeYRP
[٧]- رضوان قطبي، شبكات التواصل الاجتماعي والفضاء العمومي الافتراضي بالمغرب، مجلة الدراسات الإعلامية، العدد الرابع، اغسطس/آب ٢٠١٨، المركز الديمقراطي الغربي، برلين-ألمانيا، ص٢٥٢
[٨]- د. قادير إسماعيل، إدارة الحروب النفسية في الفضاء الالكتروني، م، س، ذ.
[٩]- خالد وليد محمود، الهجمات عبر الانترنت ساحة الصراع الإلكتروني الجديدة، المركز العربي للأبحاث ودراسة السياسات، ٢٠١٣، ص١١
[١٠]- عادل عبد الصادق، أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، مجلة السياسة الدولية، ٢٠١٢ ، العدد ١٨٨، ص٢-٣.
[١١]- الفين توفلر، تحول السلطة: المعرفة والثورة والعنف على أعتاب القرن الحادي والعشرين، الجزء الثاني: ترجمة: لبنى الريدى، القاهرة: الهيئة المصرية العامة للكتاب، ١٩٩٦، ص ٧٧، ٧٩، ٨٠.
[١٢]- سليم دحماني، أثر التهديدات "السيبرانية" على الأمن القومي- الولايات المتحدة الأمريكية – أنموذجا، م. س، ذ، ص٢٢.
[١٣]- محمد مختار، "هل يمكن للدول أن تتجنب مخاطر الهجمات الإلكترونية؟"، مفاهيم المستقبل، العدد ٦، مركز المستقبل للأبحاث والتطوير، ٢٠١٥، ص ٥-٦
[١٤]- محمد مختار، "هل يمكن للدول أن تتجنب مخاطر الهجمات الإلكترونية؟"، م، س، ذ، ص٣٢-٣٣
[١٥]- رضوان قطبي، شبكات التواصل الاجتماعي والفضاء العمومي الافتراضي بالمغرب، م، س، ذ، ص٢٥٨-٢٥٩
[١٦]- ألفين توفلر، تحول السلطة: المعرفة والثورة والعنف على أعتاب القرن الحادي والعشرين، م، س، ذ.
[١٧]-متاح على الرابط: https://www.diplomaticourier.com/book-review-the-perfect-weapon
[١٨]- حمدون إ. توريه، تقرير الاتحاد الدولي للاتصالات، البحث عن السلام السيبراني، يناير، ٢٠١١، ص٣٥-٣٦
[١٩]- محمد عبدالسلام، الحرب في زمن التغريدات، تكنولوجيا المعارك الافتراضية، القاهرة، دار أكتب للنشر والتوزيع، ٢٠١٩، ص٤٣
[٢٠]- عماد علو، حروب الطائرات المسيّرة في الشرق الأوسط، المركز الاوربي لدراسات مكافحة الارهاب، منشور في جريدة الزمان، ٢٠١٩/٩/٢٤
[٢١]- محمد عبدالسلام، الحرب في زمن التغريدات، تكنولوجيا المعارك الافتراضية، م، س، ذ، ص٤٣
[٢٢]- حمدون إ. توريه، تقرير الاتحاد الدولي للاتصالات، البحث عن السلام السيبراني، ص٩٧، م، س، ذ.