الإرهاب السيبراني والأمن الدولي: التهديدات العالمية الجديدة وأساليب المواجهة.

Cybernetic Terrorism and International Security: The New Global Threats and the Ways of Overcoming

د. غريب حكيم¹

1أستاذ محاضر. المدرسة الوطنية العليا للعلوم السياسية

GHERIEBHAKIM@HOTMAIL.FR

تاريخ القبول: 2018/10/31

تاريخ الاستلام: 2018/06/02

الملخص:

تهدف هذه الدراسة إلى معالجة ظاهرة الإرهاب السيبراني التي استفادت بشكل كبير جدا وخطير أيضا من الثورة التكنولوجية في وسائل الإعلام والاتصال، بحيث أصبح للتطور التكنولوجي في عصرنا دور استراتيجي بالغ الأهمية وربما حيوي أيضا بالنسبة للمجتمع الدولي، ذلك على مختلف الأصعدة وفي شتى المجالات السياسية والاقتصادية والأمنية وغيرها. وفي المقابل نجد تفشي ظاهرة الاستخدام غير الشرعي للفضاء الرقمي في ظل معادلة تزوج ما بين تكنولوجيات الاتصال والمعلومات والإرهاب والأشكال الجديدة من الحروب. لقد أصبح الأمن الدولي في عصر العولمة مهددا من جميع الأصعدة، والإرهاب الإلكتروني واحد من التهديدات الأمنية الجديدة والخطيرة، إذ باتت التنظيمات الإرهابية تستغل الفضاء الرقمي كساحة للصراع والتأثير والاستقطاب، مما يتطلب البحث في طبيعة أو واقع التهديدات التي يشكلها ثم الأساليب المتاحة للتصدي له ومن ضمنها الأسلوب القانوني والأمني، بحيث أن التطور التكنولوجي ذاته لا يمكن أن يسير نحو الطريق السليم، طريق التنمية وخدمة الإنسانية، دون وجود أطر قانونية وإجراءات أمنية صارمة للحفاظ على أمن الفضاء السيبراني.

الكلمات المفتاحية: الفضاء السيبراني، الأمن الدولي، الإرهاب السيبراني، الثورة التكنولوجية، الأمن السيبراني.

Abstract :

The goal of this inquiry is finding the solutions for keeping the cyber area safe. Because the cyber-terrorism has been a true threat for the international security. Cyber terrorism is any deliberate, politically motivated attack against information, computer systems, computer programs, and data, which results in violence against non-combatant targets by sub-national groups or clandestine agents. Cyber-terrorism can be also defined as the intentional use of computers, networks, and public internet to cause destruction and harm for personal objectives. There are many different motives for cyber-attacks, especially perhaps the financial reasons. However, there is increasing evidence that hackers are becoming more politically motivated. Cyber-terrorists are aware that governments are reliant on the internet and have then badly exploited this. Therefore, States need strategies for keeping the cyber area safe, through conventions and major legal instruments that specifically deal with terrorist acts.

Key words: Cyberspace, international security, cyberterrorism, Technological revolution, Cyber Security.

مقدمة:

يشهد المجتمع الدولي في عصرنا الحالي جملة من التغييرات الناتجة عن معطيات الثورة التكنولوجية الهائلة، فهذه الثورة قد نقلت المجتمعات التقليدية إلى مصافّ المجتمعات الحديثة والذكية وهو ما نعيشه اليوم في ظل ظاهرة الفضاء السيبراني. ويتضمن هذا الفضاء كثيرا من الإيجابيات والسلبيات، ففي الأولى نجد بأنه قد أسهم بصورة كبيرة حقا في تسهيل الحياة اليومية على كافة الأصعدة، خاصة ما تعلق بالاتصالات ومعرفة الأخبار في العالم وغيرها، وفي الثانية -أي السلبيات- نجده قد أصبح مجالا للنزاع والصراع والتهديد، بحيث يتم استغلال التطور التكنولوجي في وسائل الاتصال في القيام بأعمال غير مشروعة كالاختراق والقرصنة، والأخطر من ذلك استغلال الفضاء السيبراني من قبل التنظيمات والجماعات الإرهابية.

لقد أصبح الفضاء السيبراني حاضنة لبروز ونمو أشكال جديدة من الإرهابيين، كمؤثر على الإرهاب غير التقليدي الذي يستهدف مهاجمة البنى التحتية الكونية للمعلومات، وليس هذا فحسب، بل حمل معه -أي الفضاء الرقمي- تحديات أمنية وقانونية وسياسية وتقنية، خاصة في ظل ضعف منظومات الحماية وعدم وجود أطر تشريعية واضحة لتنظيم هذا الفضاء. بالإضافة إلى عدم التوافق بين تدابير مكافحة والانتشار الهائل لتكنولوجيا الاتصال والمعلومات وزيادة الاعتماد الدولي عليها، فضلا عن محدودية أدوار المواجهة القانونية والأمنية والتقنية في مقابل التهديدات الحاصلة والتحديات والتداعيات على الأمن الدولي عامة. بالتالي ستعالج هذه الدراسة موضوع التهديدات التي يشكلها الفضاء الرقمي بالنسبة للأمن الدولي، بالتركيز على ظاهرة الإرهاب الإلكتروني والجهود الدولية للتصدي لها.

إشكالية الدراسة:

- ما هي مظاهر التهديدات التي يمثلها الإرهاب السيبراني بالنسبة للأمن الدولي؟ وما هي جهود مواجهته على الصعيد الدولي؟

أولاً: الفضاء السيبراني ساحة جديدة تُهدد الأمن الدولي.

تُعرِّج بدايةً على مفهومي الفضاء السيبراني والإرهاب الإلكتروني، بحيث لا توجد تعريفات دقيقة بشأنهما. ففي مفهوم الفضاء السيبراني نجد حوالي 28 تعريفاً، يتناول معظمها مكوناته من أجهزة الكمبيوتر والوسائط التكنولوجية وشبكة الإنترنت، في حين أنه يتضمن أيضاً العنصر البشري أو المعنوي.

تشير كلمة Cyber أو Cybernetics إلى "نظرية الاتصالات والتحكم المنظم في التغذية المرتدة التي تعتمد عليها دراسات الاتصالات والتحكم في الحياة وفي الآليات التي صنعها الإنسان، أي علم دراسة الاتصال والتحكم الآلي في النظم العصبية للكائنات الحية ومحاكاة الآلات لها". بالتالي فالمجال السيبري يتضمن "كل الاتصالات والشبكات وقواعد المعلومات والبيانات ومصادر المعلومات"¹.

وتعرف كليات الحرب الأمريكية الإرهاب السيبراني، أو كما تسميه "هجمات الشبكات الكمبيوترية"، انطلاقاً من تصنيفه تحت بند "العمليات الإلكترونية"²، وهو يندرج في إطار الحرب الرقمية التي تُعرف من خلال "الإجراءات التي يتم اتخاذها للتأثير بشكل سلبي على المعلومات ونظم المعلومات، وفي الوقت نفسه الدفاع عن هذه المعلومات والنظم التي تحتويها"³. والإرهاب الرقمي يستهدف أمن العمليات، العمليات النفسية، الخداع العسكري، الهجمات الفيزيائية، ومهاجمة شبكات الكمبيوتر. ولا يوجد إجماع حول تعريف الإرهاب السيبراني، لكنه يشير عموماً إلى شكل جديد من أشكال الإرهاب يندرج في إطار الجرائم الإلكترونية، وقد أخذ تسميته من استخدام وسائل ووسائط التكنولوجيا المعلوماتية والاتصالية في تنفيذ أعمال إرهابية تتجاوز تداعياتها الأبعاد المحلية والوطنية لتؤثر بشكل كبير على الأمن الدولي. ويتضمن الإرهاب الإلكتروني أو الرقمي بهذا المعنى أعمال اختراق المواقع وأنظمة المعلومات، القرصنة، نشر الرعب وأشكال التهديد الموجهة نحو الأفراد أو الدول، استقطاب الأفراد للانخراط في التنظيمات الإرهابية.

لقد أفرزت العولمة مجموعة من التطورات وتحديداً على الصعيد التكنولوجي والمعرفي، فحدث الدمج بين الفضاء السيبراني والأساليب والتكتيكات المستخدمة في الصراعات الدولية، وأصبحت حرب المعلومات عمليات عسكرية⁴ تدور في ميدان تكنولوجي رفيع المستوى، بحيث تستخدم أطراف الصراع

وسائل تكنولوجيا المعلومات للحصول على الموقع الأفضل استراتيجيا، ذلك بالتوظيف الفعال لجميع الأسلحة المعلوماتية، ليصبح الإرهاب السيبراني بهذا المعنى تعبيراً عن صراع رقمي بين القيادات الصديقة والقيادات المعادية، بهدف التأثير على قدرات الخصم واختراق كيانه السيبراني، ومهاجمة جهاز المعلومات المعادي وإفشاله في إطار حرب المعلومات⁵.

والحروب بهذا المعنى تختلف كثيرا عن الحروب التقليدية، بحيث أن الصراع في الفضاء السيبراني يظل محاطا بعلامات استفهام بخصوص النتائج المرتقبة أو المتوقعة، مثلا في ظل محاولة السيطرة الكاملة على المؤسسات والهياكل الاستراتيجية للدول عن طريق استعمال أسلحة تكنولوجيا المعلومات والاتصالات، أو مهاجمة المعلومات من خلال الوسائط الإلكترونية، وهو ما يؤدي في نهاية المطاف إلى شلل هذه الأنظمة⁶ والتهديد المباشر للأمن الوطني من خلال الهجوم على أنظمة صنع القرار والأنظمة الدفاعية للدولة والسعي إلى السيطرة على قواعد المعلومات، ومن ثم إمكانية حدوث رد فعل انطلاقا من الحق الشرعي في الدفاع عن النفس، كما أنّ استهداف الاتصالات وأنظمة المواصلات والخدمات العامة للمواطن والدولة يمكن أن يؤدي إلى الإضرار بالحياة والممتلكات⁷.

تُعتبر هجمات الفضاء السيبراني أحد أنواع النزاع أو الصراع المسلح الأكثر ديناميكية، فهي تختلف عن أشكال النزاعات التقليدية، ويمكنها الحدوث بشكل غير مرئي وغير مشهود، مثل أن تقوم المخابرات الخاصة لأية دولة بشن هجمات باستخدام الأسلحة السيبرانية من أجل تخريب البنية التحتية المعلوماتية الخاصة بدولة أخرى. وتأتي هذه الملامح لتُظهر نواحي الاستخدامات غير القانونية وغير المشروعة لهذا الفضاء، فضلا عما يمثله ذلك من تهديد للأمن الدولي في المجال السيبراني والبنية التحتية الكونية لثورة المعلومات من جانب جميع الفاعلين في مجتمع المعلومات العالمي، خاصة التنظيمات الإرهابية والدول، والجماعات الإجرامية المنظمة، مما يطرح هواجس ويشكل تداعيات كبيرة على الأمن الدولي بصورة عامة.

ثانيا: مظاهر تهديد الإرهاب السيبراني للأمن الدولي.

يمثل الفضاء السيبراني عنصر جذب مهما للتنظيمات الإرهابية على تعدد أنواعها واختلاف أيديولوجياتها، نظرا لما يتيح من وسيلة إعلام دولية وسلاح في ذات الوقت، إذ يمكن استخدامه من قبل الأطراف المتعددة. ويعد تنظيم "داعش" الإرهابي أكثر التنظيمات التي مثلت تهديدا حقيقيا لسلامة شبكة الإنترنت العالمية باستخدامها في الدعاية والتجنيد والتمويل وجمع المعلومات، وتنسيق الهجمات الإرهابية، ووسيلة لحشد المتعاطفين معه، وهم المنتشرون في كثير من دول العالم. ويستخدم تنظيم "داعش" الإرهابي

مواقع التواصل الاجتماعي بغرض للتجنيد ونشر فكره في أوساط الشباب، وكان بإمكان حملته عبر الإنترنت في بعض الأحيان أن تكون كافية لإثارة أعمال العنف والخوف والرعب لدى الدول والمجتمعات.

في هذا الإطار، يحدد "أبو بكر ناجي" في كتابه "إدارة التوحش" أساليب توظيف الإعلام الجهادي ضمن استراتيجية التنظيمات الإرهابية. وهي بالنسبة لتنظيم "داعش" تستهدف وتركز على فئتين:

✓ فئة الشعوب: بحيث يتم العمل على دمج أكبر عدد منهم للانضمام إلى صفوف الجهاد ودعمها، من جهة أخرى، التعاطي السلبي مع من لا يلتحق بالتنظيم.

✓ جنود العدو: خاصة أصحاب الرواتب الدنيا، للدفع بهم نحو الانضمام إلى صفوف المجاهدين أو على الأقل الفرار من خدمة العدو.

وقد عمل تنظيم "داعش" الإرهابي على تجنيد جيش إعلامي متخصص في الإعلام الإلكتروني، يعمل تحت تسميات مختلفة، مثل المراكز والمؤسسات والكتائب الإعلامية، وهي على شكل شبكات بحيث تتواجد كل شبكة ضمن منتدى من منتديات "الجهادية" أو موقع من مواقع التواصل الاجتماعي، لدعم هدف من الأهداف التي يُقرّها الإعلام المركزي الخاص بتنظيم "داعش" الإرهابي (مركز الفجر للإعلام، مؤسسة الفرقان الإعلامية). كما وظّف تنظيم "داعش" الصور والفيديوهات من خلال مواقع التواصل الاجتماعي، بحيث يظهر فيها إرهابيو التنظيم وهم يقطعون الرؤوس، فاحتوت مضامين الفيديوهات والصور على مشاهد عنف غير مسبوق، الغرض منها بثّ قدر كبير من الرعب والترجيع في نفوس الأفراد والمجتمعات والدول.

لقد استغلت الجماعات والتنظيمات الإرهابية، على شتى أشكالها وأنماطها الفكرية، تسهيلات عصر المعلوماتية والرقمية بوصفها عنصرا حيويا لدعم وتحقيق أهدافها، ومنفذا لوجيستيكا داعما وحاضنا للنشاط الإعلامي لها في مناطق مختلفة عبر العالم، بالتالي تشكيل مجتمع افتراضي خاص بها، يساعدها على الالتحام والتواصل الدائم، الذي يوهم البعض بأن هذا المجتمع غير محدد الأبعاد الكميّة، وهو ما كان له دور كبير في تضخيم الصورة الذهنية لقوة وحجم تلك المجموعات.

قد يُنظر إلى الإرهاب بأنه سلاح الضعيف الذي لا يقدر على تنظيم حرب ضد الدولة، فعن طريق الإرهاب يُمكن إلحاق الأذى ومحاولة هزيمة القوى العظمى، وهذا ما يتضح في الجماعات الإثنية والمليشيات العنصرية والأصوليات الدينية، وبعض الأقليات التي لا تمتلك القوة. ويكون الإرهاب وسيلة لتأكيد الهوية وجذب الانتباه والاهتمام، فهو بالتأكيد وسيلة من وسائل الصراع.

يتعلق الإرهاب بالسموات المفتوحة والفضاءات التكنولوجية، ويكون وسيلة لتحقيق أهداف مستقبلية عبر تحطيم الحاضر للوصول إليها، بحيث يكون التحطيم بداية لظهور شيء معين من تحت رُكامه، ويكون مدفوعاً بقيم أخلاقية أو ثقافية⁸.

وينشأ الإرهاب إما بدافع الثأر وتوقيع العقوبة على أخطاء الماضي، أو القدرة على الإلهام والتبشير بعهد جديد. ففي الأول، يكون العنف استراتيجياً بشكل كبير، والأهداف محددة وواضحة، بينما الثاني يُعبر عن كيفية تغيير العالم عن طريق الإرهاب، وبالرغم من تلك الاختلافات فإنها لا تعني بالضرورة وجود تمايزات. في كل الأحوال هنالك عنف، وتأتي هذه الأسباب لتندعم في عصر الثورة المعلوماتية. إن الإرهاب بطبيعته ليس ظاهرة ثابتة، بل هو تهديد دائم التغير والتحول، بحيث يغير مرتكبه ملامحهم ووسائلهم ليتكيفوا مع زمانهم ومواقفهم، ولضمان تحقيق ما يهدفون إليها.

كما استفاد الإرهابيون من التطور التكنولوجي والثورة الرقمية بحيث أصبح بمقدورهم شراء المنتجات التكنولوجية التجارية والاستفادة مما تم إنفاقه في البحث والتطوير، فتمكنوا من الحصول على أجهزة كونية المدى وفائقة السرعة، متنوعة، معقدة ومشفرة، وبدون أية تكاليف باهظة. وهو أمر منطقي إذ أتاحت شبكة الإنترنت الفرصة للحصول لاكتساب المعلومات، إصدار الأوامر والسيطرة على العمليات المخطط لها⁹.

وتتملك الجماعات المتطرفة، بجميع أشكالها ومختلف توجهاتها السياسية، مواقع على شبكة الإنترنت وبشكل خاص شبكات التواصل الاجتماعي، ومنها ما يمتلك أكثر من موقع، يقدم خدماته بأكثر من لغة، كما هو شأن تنظيم "داعش"، من أجل التعريف بالتنظيم وتاريخه ومؤسسيه وأبطاله وأنشطته، وخلفياته السياسية والاجتماعية، وأهدافه السياسية والأيدولوجية، وأحدث الأخبار ومضامين الانتصارات المحققة. كما أن رسائل المواقع تكون لها صور متعددة، مثل الدعم الفكري لهذه التنظيمات وتبجيل أفرادها، أو مهاجمة المفكرين والشيوخ المعتدلين، أو مهاجمة الحكومات والأجهزة الأمنية، وجميعها يؤثر على الأمن الدولي بكافة مستوياته وعلى جميع الأصعدة.

قد تسعى تلك المواقع للتغطية على موقفها الداعم للإرهاب بالسماح بنقد يسير، والاستناد في ترويج فكرها إلى بعض الكتابات الأيدولوجية والدينية، وإلحاقها بتفسير معينة وقصص تاريخية وُضعت ضمن تأويل متعسف لكي تُفنع المنلقي بمشروعية عملها، بحيث يتم استغلال الدين باعتباره مظلة أيدولوجية توهم لاستقطاب عناصر جديدة، كما يتم نشر تلك الأفكار وإدارتها من قبل أشخاص ذوي أفكار أحادية لا تسمح بوجود أحد يناقشها أو يعرض رأياً يخالفها¹⁰.

○ أنماط الجمهور التي تستهدفها رسائل المواقع الجهادية:

- ✓ **النمط الأول:** هو جمهور المؤيدين الحاليين والمحتملين، وذلك عبر تقديم معلومات مفصلة حول أنشطة المنظمة الإرهابية وسياساتها الداخلية، وحلفائها ومناقسيها، وعادة ما يكون هذا الجمهور جمهوراً محلياً.
- ✓ **النمط الثاني من الجمهور:** هو الرأي العام العالمي، وهو الجمهور غير المتورط مباشرة في الصراع، ولكن لديه بعض المصالح في القضايا المطروحة¹¹. ويضم هذا الجمهور المستهدف الصحفيين ووسائل الإعلام التي تستخدم مواقع هذه التنظيمات للحصول على وجهات نظرها. يساعدها في ذلك طرح خدمات المواقع بلغات عدّة.
- ✓ **النمط الثالث:** يتمثل في الأعداء، وتسعى مواقع هذه التنظيمات إلى إضعاف معنوياتهم من خلال توجيه التهديدات وتعزيز الشعور بالذنب لديهم إزاء الأفعال والدوافع¹².

○ أشكال الخطابات الدعائية التي تستخدمها الجماعات المتطرفة:

- ✓ **الخطاب الأول:** يتمثل في الادعاء بأنه ليس أمامها خيار سوى التحوّل إلى العنف الذي يقمّ بوصفه ضرورة أجبر عليها الضعيف للرد على العدو الظالم. ويتم تأكيد أعمال القوة التي تستخدمها الحكومات والأنظمة ضدها وضد تنفيذ مطالبها، كما يتم استخدام مصطلحات كالذبح والقتل والإبادة، وتصف التنظيمات المتطرفة نفسها بالمضطهدة والمطاردة من قبل القوى الكبرى أو دولة قوية، وهو ما يعطي انطبعا لدى جمهور المتعاطفين بأن التنظيم المتطرف والإرهابي ضحية.
- ✓ **الخطاب الثاني:** يرتبط بشرعية استخدام العنف، فأعضاء الحركة أو التنظيم يعتبرون أنفسهم مقاتلين من أجل الحرية، ومجبرين -بما يتنافى وإرادتهم- على استخدام العنف، نظراً لأن العدو يسحق كرامة الشعوب وحقوق التنظيم ذاته، وأن عدو الحركة أو الجماعة هو الإرهابي الحقيقي.
- ✓ **الخطاب الثالث:** هو الاستخدام الواسع لمبدأ اللاعنف في محاولة لدرء الصورة العنيفة عن التنظيم المتطرف والإرهابي، بمعنى التمويه والتلاعب بالمشاعر، فعلى الرغم من كون تلك الجماعات جماعات عنيفة، فإن المواقع المرتبطة بها تدّعي سعيها للحلول السلمية، وأن هدفها النهائي هو التسوية الدبلوماسية التي تتحقق عبر المفاوضات والضغط الدولي على النظم الجائرة¹³.

وقد برزت العلاقة ما بين الفضاء الإلكتروني والإرهاب من خلال عدد من المظاهر، لعل أهمّها كونه -أي هذا الفضاء- يتّسم بخصائص تنافسية بشكل يجعله مسرح جذب للإرهابيين والقيام بإدارة الفكرة المدركة أو التحكم بالصورة المنطبعة (أي تصوير أنفسهم وأعمالهم بالضبط في الضوء والسّيّاق الذي يريدونه)، دون أن يعرقل ذلك تفحص وسائل الإعلام الرسمية لذلك التصوير أو غربلته أو تحويره¹⁴. وقد

بدأ الإرهابيون بالفعل في استخدام الفضاء الإلكتروني في التأثير على الرأي العام، وتجنيد أعضاء جدد، وجمع الأموال.

وقد استخدم الإرهابُ الفضاءَ الإلكتروني كوسيط إعلامي يتكون من أربعة عناصر: جهاز الإرسال (الإرهابي)، المتلقي المقصود (الهدف)، الرسالة (التفجير، الكمين)، التغذية الاسترجاعية، وردّ فعل الجمهور المستهدف. ويمارس الإرهابيون في ذلك أشكالاً مكررة من استخدام اللغة المؤثرة، الهادفة إلى الإقناع شفويا وكتابيا وتصويريا، مما يرغم وسائل الإعلام على توفير الوصول إليها والذي بدوره لا يستطيع الإرهابُ تحقيق أهدافه. وتتألف كل وحدة إرهابية من أربعة أعضاء على الأقل: المرتكب، المصور، فني الصوت والمخرج¹⁵.

لقد أصبح الفضاء الإلكتروني منبراً للجماعات الإرهابية عبر نشر رسائل الكراهية والعنف، والاتصال ببعضها البعض وبمؤيديها والمتعاطفين، وليست المواقع الإلكترونية سوى واحدة من خدمات الانترنت التي سطا عليها الإرهابيون، فهناك تسهيلات عديدة أخرى كالبريد الإلكتروني، غرف المحادثة والمجموعات الإلكترونية.

يستخدم الكثير من التنظيمات الإرهابية هذه المواقع الإلكترونية لشن الحرب النفسية ضد الدول المعادية وقواتها المسلحة، من خلال عرض أفلام مرعبة للرهائن والأسرى أثناء إعدامهم، واغتيال العسكريين في الميدان على أيدي القناصين، أو إسقاط طائراتهم بالقذائف المحمولة على الأكتاف، أو نسف عرباتهم باستخدام القنابل المخفية على جانب الطرق أو على يد مفجرين انتحاريين. وتسعى الرسائل الشفهية والمصورة تثبيط عزيمة العدو وتخويفه أو خلق شعور بالذنب والشك والانشقاق الداخلي، في الوقت الذي تبلغ فيه رسالة تهديد إلى الحكومات المختلفة ومواطنيها. ويحرز الإرهابيون قوتهم من رد الفعل على ما قد يثيرونه من خوف لدى العدو¹⁶.

انطلاقاً من كل ما سبق ذكره، نقول بأن الإرهاب السيبراني قد شكل قاعدة للتغيير والتعبير عن الرؤى المتطرفة التي تتبنى العنف أسلوباً ووسيلة، مستفيداً في ذلك مما آل إليه الإنترنت من تقسيم الجمهور إلى فئات ومجموعات صغيرة، وأخذ هذا التنوع في تنمية ظاهرة التشنت الثقافي، بوصفه إعلاماً فنوياً يُستخدم لإذكاء نيران الصراعات العنصرية وتنمية اتجاهات الكراهية لدى الكثير من الفئات المناهضة للفئات الأخرى. وفي مقابل تلك النظرة التقنيتية للمجتمعات، جاء ذلك الإعلام للترويج لرؤى عالمية. ففي حين تستغله الولايات المتحدة للترويج للرأسمالية والهيمنة، تستغله تنظيمات إرهابية للترويج للخلافة الإسلامية والجهاد العالمي.

لقد قوّض الإرهاب السيبراني من سلطة الدولة بنقل الحوادث الإرهابية إلى الرأي العام، بما يشكل خطرًا نفسيًا وضغطًا على الحكومات بإجبارها على المثول للمطالب السياسية التي تتبناها الجماعات الإرهابية، وتهديدًا لشرعية النظم السياسية الحاكمة، وعمل ذلك على الحدّ من استخدام القوة في صنع القرار من جانب الدولة التي فرض انسحابها من قطاعات استراتيجيّة لصالح القطاع الخاص تحديات أمنية متزايدة. وتطرح مسألة المواجهة الأمنية قضية حرية الرأي والتعبير عبر الإنترنت وارتباطها بالقيم الديمقراطية، وكذلك مسألة الاستغلال السياسي للنظم الحاكمة لمواجهة معارضيتها بشكل لا يعكس الفصل بين أمن النظام وأمن المجتمع، وفي مقابل تلك الجهود لإغلاق مواقع الإنترنت، تزداد قدرة الإرهابيين على استخدام الفضاء الرقمي بشكل أكثر عمقًا¹⁷.

لقد مثّلت عملية التزاوج بين الإعلام والإرهاب سلاحًا ذا حدّين في مجال استخدام الإعلام الجماهيري، أحدهما سلبي، بحيث إنها قد تكون سببًا لنشر الرعب والخوف على الملأ من خلال تغطيتها غير الواعية للعمليات الإرهابية وآثارها. محققة بذلك للإرهابيين هدفين مهمين كما تضمنت هذه الدراسة: الأول هو إثارة الرأي العام ولفت انتباهه إلى وجود ظاهرة الإرهاب، وإلى أن الإرهابي صاحب قضية يجب الاعتراف والاهتمام بها ومعالجتها. والثاني هو الحصول على الشرعية الدولية لما يطالب به الإرهابيون. ويحرص الإرهابيون على تنفيذ عمليات مثيرة من حيث الأسلوب، أو حجم الخسائر، أو مكان وزمان وقوعها ليكون ذلك مدعاة لجذب الإعلاميين الباحثين دائمًا -وفقا لطبيعة عملهم- عن الأخبار المثيرة والمهمة بالنسبة لأكبر عدد ممكن من الجماهير. أما الجانب الإيجابي لسلاح الإعلام فيتمثل في التغطية الواعية لقضايا الإرهابيين وعملياتهم، وفق أسلوب توعية يُفَرّ الرأي العام من تلك الأعمال الإجرامية، ويُبرز بشاعة مرتكبيها وعداءهم للمجتمع، وسعيهم إلى التدمير والتخريب ونشر القلق في أوساط الأفراد والمجتمعات.

○ الإرهاب الإلكتروني كعنصر من عناصر القوة العسكرية والهجوم المسلح:

كما هو الحال في أي حرب، فإن الجيوش المتصارعة تستهدف دومًا ثلاثة أمور أساسية من أجل كسب المعركة، هي العناصر العسكرية، الاقتصادية والسياسية، أو بعبارة أخرى "إرادة الخصم". وفي عالم حروب المعلومات نجد ذاتَ العناصر بالتسميات الآتية: مراكز القيادة والتحكم العسكرية، البنوك والمؤسسات المالية، مؤسسات المنافع كمؤسسات المياه والكهرباء، وذلك لإخضاع إرادة الشعوب. وإذا دمّرت دولة شبكة الإنترنت بشكل متعمد، فإن دولة أخرى قد تعتبر هذا الأمر عملاً عدائيًا.

وقد لا يكون الهدف هو تدمير الشبكة كليًا أو تعطيلها، بحيث إنها تساعد حتى الطرف المعتدي في مراقبة المحادثات بين الأعداء أو نشر معلومات خاطئة. الأمر الذي يُعتبر فرصة استخباراتية مُذهلة. كما

أن استخدام الإنترنت في السيطرة على المعلومات يمكن أن يعود بفائدة تفوق الفائدة المطلوبة من تعطيل الشبكة نفسها أو تعريضها للهجوم، خاصة عندما يخص الأمر الاستراتيجية العسكرية، العمل على إضعاف إرادة الجيوش، شنّ حرب نفسية والتحكم وفي المعلومات¹⁸.

تُعدّ هجمات شبكات الكمبيوتر أو الحروب السيبرانية جزءاً من عمليات المعلومات التي يمكن أن يتم استخدامها في مستويات ومراحل الصراع المختلفة، سواءً على الجانب التكتيكي، الاستراتيجي أو العملي، ويتم استخدام الهجمات في أيّ وقت، سواءً في وقت السلم أو الحرب أو الأزمات. وتوجد طرق عديدة يمكن من خلالها تنفيذ الهجمات عبر الفضاء الإلكتروني، منها الهجمات المباشرة من خلال التدمير الفيزيائي لأجهزة الخصم، أو نقاط الاتصالات المهمة ضمن شبكاته، وذلك باستخدام القوة العسكرية المباشرة. وهناك أيضاً سرقة المعلومات من أجهزة الخصم، ومن ثم اتخاذ قرارات أفضل في المعركة. إضافة إلى تخريب قواعد بيانات الخصم والتلاعب بها، لجعل الخصم يخطئ في اتخاذ القرارات، وبالطبع هناك استخدام الفيروسات والأساليب الإلكترونية، مثل هجمات الحرمان من الخدمات للتأثير على مواقع الخصم، مما يؤدي إلى التقليل من قدرة العدو على الاتصال وإبطاء قدرته على اتخاذ القرار.

تتضمن هجمات الكمبيوتر حدوث هجوم على خطوط الاتصالات، وتأتي تلك الهجمات من مسافة بعيدة عن مصدر الهجوم، من خلال الشبكات الدولية للمعلومات العابرة للحدود، موجات الراديو أو الشبكات الدولية للاتصالات، بدون تدخل مادي أو طبيعي في الأراضي الخاصة بدولة أخرى أو القيام بغزوة تقليدية. وعلى الرغم من الاستخدامات الحديثة لهجمات الفضاء الإلكتروني في الصراعات الحديثة، فإنه لم يتم إدماجها بشكل كامل في العقيدة العسكرية للجيوش الحديثة، وإن كان الواقع تمهيداً لبداية لأخذها بعين الاعتبار في سبيل الاستحواذ على القوة وامتلاكها من خلال تطوير أسلحة الفضاء الإلكتروني ليتم استخدامها في حروب المستقبل، بما ينطوي عليه تغيير المبادئ الخاصة بشن الحرب، ميدان الحرب، الطرق والوسائل الحربية المتاحة¹⁹.

لقد ظهر الفضاء السيبراني كأحد مجالات الحرب، مثله في ذلك مثل الجو والفضاء الخارجي والأرض والبحر، وأصبح يُستخدم كمجال عسكري وغير سلمي. وقد لا تؤدي الحرب في الفضاء الرقمي إلى مأساة إلكترونية بالضرورة، وإنما إلى فرض نوع من السيطرة على مجرى الأحداث في العالم وفق مصلحة من يشنها على جبهة واسعة النطاق من السهل الاحتماء بها، كما أن آثار الهجوم قد لا تتساوى مع تكاليفه، فضلاً عن صعوبة تحديد هوية مصدر الهجوم الذي يصدر من جانب واحد، الأمر الذي يجبر ضحايا الهجوم على اتخاذ وضع الدفاع، مع عدم قدرتهم على شن هجوم مضاد، وفي حالة حدوثه يكون تأثيره محدوداً، لعدم معرفة مصدر الهجوم²⁰.

تعتمد القدرة القتالية في الفضاء السيبراني على نظام التحكم والسيطرة، وقد أوجدت ملايين أجهزة الكمبيوتر المنتشرة في كل مكان عالما افتراضيا نشأ نتيجة عملية الاتصال، ومثل ذلك وسيطا جديدا للقوة، بحيث يمكن للقراصنة دخول المجال الرقمي ومحاولة السيطرة على الأجهزة، وسرقة المعلومات وإفسادها أو تعطيلها، وذلك بعدما أصبحت المجتمعات والجيوش الحديثة تعتمد اعتمادا كبيرا على أجهزة الكمبيوتر، الأمر الذي يعرضها للخطر، فصار الإنترنت بهذا المضمون مرادفا لاستخدام "الذكاء الاصطناعي"²¹.

لقد ظهرت أسلحة سيبرانية جديدة ومتعددة كالفيروسات، الهجمات الإلكترونية، الاختراقات، القرصنة، سرقة المعلومات، التشويش. وتلعب القنابل الإلكترونية دورا كبيرا جدا في تنفيذ عدد من المهام الاستراتيجية، مثل تعطيل الاتصالات والتشويش عليها، التتصت على المكالمات، بث معلومات مضللة عبر شبكات الحاسوب الآلي والهاتف، تقليد الأصوات، وخاصة أصوات القادة العسكريين، وعن طريق ذلك يمكن إصدار أوامر خطيرة، استهداف شبكات الحاسب بالتخريب عن طريق نشر الفيروسات، مسح الذاكرة الخاصة بالأجهزة المعادية، منع تدفق الأموال وتغيير مسار الودائع، إيقاف محطات الكهرباء عن العمل، وقد صممت لذلك الهدف قنبلة إلكترونية خاصة أطلق عليها اسم **94cbu** تنطلق منها عدة قنابل في الجو تستهدف محطات الكهرباء وتؤدي إلى احتراقها وتدميرها الكامل.

وبناءً على ما سبق ذكره، يمكن تصنيف الفضاء السيبراني من حيث تعرّضه لأنماط الحرب والصراع إلى صراع مرتفع الشدة وآخر منخفض الشدة. وقد جاءت الحرب المنخفضة الشدة بصورة مستمرة ودائمة، وهي تُعبّر عن صراعات أعمق وأطول أمدا، وترتبط بالصراعات ذات الطبيعة المعقدة والمتداخلة. وأصبح الفضاء الإلكتروني ساحة لنقل الصراعات وتصفية الخلافات بجميع أنواعها بين الفرقاء. ولا يمكن إحصاء الحالات التي تحتوي على هجمات إرهابية وإجرامية، ولكن معظمها يركز على مراكز الطاقة، البنى التحتية لنظم الاتصالات، شركات الإنترنت، نظام مراقبة الملاحة الجوية، المصارف، مهام الجيش، وغيرها.

ولا يزال الصراع بكل أنماطه عبر الفضاء الإلكتروني في بدايته، بيد أنه مرشح حتماً لأن يشهد في غضون السنوات القليلة المقبلة تنوعاً غير مسبوق في أساليب الصراع والرقابة والدفاع وطبيعة الأطراف، من باب أنّ ميدان المعركة والحرب هو الفضاء الإلكتروني. ويرتبط هذا النوع من الصراع بميادين الحرب الإلكترونية وبأسلحة إلكترونية جديدة توازت مع مثلتها التقليدية في نتائجها التدميرية، إن لم تكن قد تفوقت عليها، وفرضت نفسها بقوة على واقع الصراعات المسلحة وغير المسلحة. فالصراعات في عصر المعلوماتية تتميز بأنها لا تنتهي حتى بانتهاء مظاهر الصراع المسلح، وتمثل بيئة وسياقا إما للتطور نحو الحرب بشكل ساخن عبر تحريك الآلة العسكرية، أو للتعبير عن نمط طبيعي وخلافات تدخل في سياق التنافس الذي يعد سمة أساسية من سمات المجتمع البشري أو جزءا من عمل أجهزة

الاستخبارات الدولية، أو التنافس بين الشركات العاملة في تكنولوجيا الاتصال والمعلومات، وكان أبرز مثال على ذلك النوع من الصراعات: الخلاف الروسي - الإستوني (نسبة إلى إستونيا) في شهر ماي من عام 2008.

ثالثا: الجهود الدولية في مجال مكافحة الإرهاب السيبراني.

للفضاء السيبراني في عصر العولمة دورٌ مهمّ في جميع ميادين الحياة، فقد جعل من العالم قرية صغيرة، وبسببه نمت مخاطر وتهديدات باتت تهدد دوره وأهميته الاستراتيجية بعد التحول الرئيسي الذي ظهر في سياسات الأمن والدفاع مع انتهاء فترة الحرب الباردة، بحيث كان للأمن خلال تلك الفترة مضامين معينة، ثم جاءت ثورة المعلومات والتكنولوجيا لتضيف إليها ملامح وأبعاد أخرى جديدة.

مع بداية سنوات التسعينيات من القرن الماضي، بدأت موجة الانتشار الدولي لتكنولوجيا الاتصال والإعلام والمعلومات، لتتدخل في مختلف ميادين الحياة السياسية والاجتماعية والأمنية والاقتصادية وغيرها. وفي الوقت نفسه، تعرضت الوسائل التكنولوجية الجديدة للاستعمال الخطير من قبل التنظيمات الإرهابية التي استفادت بشكل كبير من التسهيلات التي أتى بها المجال السيبراني باعتباره أحد المحددات الجديدة للقوة، وبالنظر إلى الأبعاد الجديدة التي تتطوي عليها القوة الإلكترونية من حيث طبيعتها وأنماط استعمالها، بل وأيضا طبيعة الفاعلين، وهو ما شكّل تأثيرات كبيرة وعميقة على قدرات الدول وعلاقاتها الخارجية، مجموعة وسائلها وطاقاتها وإمكانياتها المادية وغير المادية، المنظورة وغير المنظورة، والتي يستخدمها صانع القرار في تحقيق مصالح الدولة والتأثير في سلوك الوحدات السياسية الأخرى²².

لقد اتسعت البيئة التكنولوجية مع انتشار تكنولوجيا الاتصال والمعلومات وارتباطها بأعمال المال والاقتصاد والمجتمع الدولي، حتى أصبح الأمن السيبراني تحديا يندرج ضمن أجندات الأمن الوطني للدول، خاصة مع علاقته بالإرهاب وحماية البنية التحتية. وفي ذات الأثناء، ظهرت قطاعات حديثة في الاقتصاد تعتمد على التكنولوجيا المعلوماتية اعتمادًا كبيرًا، وأصبح الأمن السيبراني يمثل عنصراً مهماً من عناصر الأمن الوطني واستراتيجياته، بالنظر إلى أهمية الفضاء السيبراني في تطور الاقتصاديات الحديثة²³.

إنّ الخطورة لا تكمن فقط في تعرّض أنظمة المعلومات للفشل، بل أيضا في أنها أصبحت أهدافا محتملة للتعرّض للهجمات التي تؤثر بدورها على عمل البنية التحتية الكونية للمعلومات والخدمات التي تقدمها، وما لذلك من آثار اقتصادية وسياسية واجتماعية وأمنية كبيرة. وما يزيد حجم المعضلة أن تلك الهجمات قد تكون صغيرة ورخيصة، ولكنها تُحدث آثارا ضخمة من خلال شبكات المعلومات والاتصال،

لذا أصبحت التهديدات الجديدة تستحوذ على اهتمام متزايد من العديد من الدول، خاصة تلك التي ترتبط بالتكنولوجيا والمتقدمة صناعيا، إذ يهتم بها صانعو القرار، وتقع ضمن أولويات الأجندة الأمنية والسياسية. تعود أولى الجهود الدولية لمواجهة الجريمة السيبرانية والإرهاب الرقمي إلى ثلاثة عقود مضت، حين ناقش الأنترربول الدولي في عام 1981 إمكانية إيجاد تشريع قانوني خاص بالجريمة الالكترونية. وقد كان التقدم بطيئا، لكنه أخذ في التسارع المطرد بعد انتهاء الحرب الباردة، ولعل إنشاء معهد قانون الفضاء السيبراني في جامعة جورج تاون الأمريكية عام 1995م يدل على نمط المشكلة، بحيث تواجد فيه ثلاثون متخصصا من الذين يعملون على كيفية التعامل مع مشكلات الفضاء السيبراني²⁴.

وأمام التحديات المطروحة، وُجدت ثلاث استراتيجيات لحماية البنية التحتية للمعلومات في الولايات المتحدة الأمريكية، تتضمن: الفعل العسكري- «التدخل»، الحلول الفنية لتأمين الأنظمة-«الاستعداد»، وبناء الوعي-«المعلومات». في حين جاءت السياسات الحكومية الخاصة بمكافحة هجمات الفضاء السيبراني وتعزيز الأمن السيبراني متنوعة في مراحل تنفيذها، بعضها كان قويا، بينما كانت الأخرى مجرد اقتراحات، وجاءت بأشكال وصور متنوعة من بينها اتباع سياسة تنظيمية خاصة بالبنية التحتية للمعلومات لتضمين الإجراءات الخاصة بالأمن السيبراني في الجهود العامة لمكافحة الإرهاب.

لقد أخذ الاهتمام بالأمن السيبراني في الانتشار على المستوى الدولي، وخاصة داخل الدول المتقدمة، وظهر ذلك في تبني سياسات أمنية متعددة، وسعت العديد من الدول العالم خلال سنوات قليلة إلى زيادة الاهتمام بهذه الظاهرة، رغبة في تأمين نظم المعلومات التي أصبحت تهدد النمو الاقتصادي والأمن الوطني والدولي.

وقد اتجهت الدول إلى تبني العديد من المبادرات على المستوى الوطني والثنائي والإقليمي والدولي، من أجل العمل على حماية البنية التحتية الكونية للمعلومات من خطر التعرض للتهديدات السيبرانية، وعملت على إيجاد أطر تشريعية جديدة تتعامل مع تلك الظاهرة المستحدثة في إطار صياغة مفهوم جديد للأمن الوطني، ثم الاتجاه إلى التعاون الدولي. وقد فرض ذلك الحاجة إلى تحديد ما يمكن أن يمثل بنية تحتية حرجة، في ظل تبني إجراءات قانونية وأمنية صارمة بإمكانها الوقاية والتصدي للتهديدات ذات الخصائص غير التقليدية كحال الإرهاب الإلكتروني²⁵.

وقد عكست الجهود الدولية في مجال الأمن السيبراني اهتماما واضحا ومتزايدا من جانب القطاعين الخاص والعام أو بالتعاون فيما بينهما، كما سعى العديد من البلدان المتقدمة إلى تبني استراتيجية دولية في مجال تأمين الفضاء السيبراني، من خلال جملة من القوانين وأهمها مبادرة الشراكة الدولية المتعددة الأطراف لمكافحة الإرهاب السيبراني IMPACT، التي تهدف إلى حشد الجهود الدولية

من جانب القطاعات الحكومية والقطاع الخاص والمجتمع المدني لمواجهة التهديدات المتزايدة التي يمثلها الإرهاب السيبراني. كما سعت المبادرة إلى جمع الرؤى والأفكار حول التدريب وتبادل الخبرات، وتم إنشاء العديد من مواقع الإنترنت لمكافحة الإرهاب الرقمي وحماية الأمن السيبراني، وكانت تلك المواقع نقطة التقاء بالنسبة لخبراء أمن المعلومات والسياسيين من أجل التباحث حول ماهية خطر الإرهاب السيبراني وكيفية مواجهته، مثل مجموعة "SITE" للاستخبارات، التي تعد جهاز استخبارات متخصصا في رصد الإرهاب عبر الإنترنت ودراسة المصادر الأولية للإرهابيين والمرجعيات الفكرية لهم، وترجمة أحاديثهم، ومراقبة دعاية الإرهابيين.

الخاتمة:

حاولت هذه الدراسة تسليط الضوء على الفضاء الرقمي وتأثيراته على الأمن الدولي، من خلال التركيز على الإرهاب الإلكتروني وأساليب التصدي له. لقد طرح موضوع الفضاء السيبراني في العلاقات الدولية الكثير من علامات الاستفهام، باعتباره ظاهرة جديدة تزامنت مع عصر العولمة الرقمية، فكان التفكير كُله مرتكزا على أساليب التعامل مع هذه الظاهرة والسعي إلى إحاطتها بالإطار القانوني الأنسب من أجل تقليص سلبياتها قدر الإمكان وفي مقدمة السلبيات نجد الإرهاب الإلكتروني وما يتضمنه من بثّ للكراهية والأحقاد الطائفية والنزعات العنصرية. بالتالي بات التصدي لهذا النوع الجديد من التهديدات الأمنية ضرورة ملحة، في سبيل حفظ الأمن الدولي والإنساني ومبدأ التعايش المشترك. يُضاف إلى ذلك أن التعامل من مُنطلق السيادة لم يعد واردا، فالسيادة في عصرنا الحالي نسبية، والفضاء السيبراني خير دليل على ذلك بالنظر إلى التهديدات التي تحيط به وتؤثر على الأمن القومي للدول مجتمعة وحتى أمن الفرد والمجتمع بشكل خاص، بالتالي نقول بأن التصدي لظاهرة بحجم الإرهاب الإلكتروني يتطلب تعاوننا دوليا مشتركا، بدءا بالأطر القانونية والأمنية كما تناولنا في هذه الدراسة، لكن الظاهرة تظل أوسع وأعمق مما يتصوره البعض، لأنها مرتبطة بمجال مطاطي وغير مرئي، وطبيعة هذا المجال هي التي شجعت تكاثر الجرائم الإلكترونية ومن ضمنها الإرهاب الرقمي.

الهوامش:

- ¹ إيهاب خليفة، القوة الإلكترونية وأبعاد التحول في خصائص القوة. مصر: مكتبة الإلكندرية، 2014، ص. 21.
- ²Jennie M. Williamson, Information Operations: Computer Network Attack in the 21s Century. Carlisle Barracks, PA, U.S. Army War College. 2002. Pp: 22–25. Also available online at: (<http://handle.dtic.mil/100.2/ADA402018>).
- ³Michael Wynne, "Flying and Fighting in Cyberspace", Space Power Journal &Air, fall 2007, pp: 1–11, (<http://www.airpower.au.af.mil/apjinternational/apj-a/2007/fal07/wynne.pdf>)
- ⁴Myriam A. Dunn. "The Internet and the Changing Face of International Relations and Security". Volume number: 7, Issue number: 1, ProCon Ltd., Sofia, Bulgaria, 2001.
- ⁵Wang Baocun and Li Fei. "Information Warfare" Liberation Army Daily, June 13 and June 20, 1995.
- ⁶Mark R. Shulman. "Discrimination in the Laws of Information Warfare", School of Law Faculty Publications, Pace University, Columbia Journal of transnational Law, 1999, pp 937-998. (<http://digitalcommons.pace.edu/lawfaculty/224>).
- ⁷Martin C.Libicki, "Conquest in Cyberspace: National Security and Information Warfare", New York, Cambridge University Press, 2007. Pp.13- 323.
- ⁸Dorothy Denning, "Information Warfare and Cyber-terrorism", Women in International Security (WIIS) Seminar, Washington, D.C. D.C. (15 December 1999).
- ⁹The National Strategy to Secure Cyberspaces, Washington, whitehouse, February 2003. p61. Also available online at: (http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf)
- ¹⁰G8 Justice and Home Affairs Communiqué, Washington DC, May 11, 2004, p.10.
- ¹¹United States. General Accounting Office. Critical Infrastructure Protection: Significant Homeland Security Challenges Need to Be Addressed. Washington, GAO, 2002. P:44. Also available online at: (<http://www.gao.gov/new.items/d02918t.pdf>)
- ¹²United States. General Accounting Office. Critical Infrastructure Protection: Significant Homeland Security Challenges Need to Be Addressed. Washington, GAO, 2002. P:44. Also available online at: (<http://www.gao.gov/new.items/d02918t.pdf>)
- ¹³Seymour E.Goodman and Herbert S.Lin (eds), "Toward a Safer and More Secure Cyberspace, Washington, National Academies Press, 2007. P: 307.
- ¹⁴New Global Partnership to Fight Cyber Terrorism Seeks the Business, Zeichner Risk Assessment Newsletters, Vol. 1. No. 30, May 30, 2008.
- ¹⁵عادل عبد الصادق، "هل يمثل الإرهاب الإلكتروني شكلاً جديداً من أشكال الصراع الدولي؟" ملف الأهرام الاستراتيجي، مركز الدراسات السياسية والاستراتيجية بالأهرام، العدد 156 ديسمبر 2007.
- ¹⁶مصطفى علوي، "مفهوم الأمن في مرحلة ما بعد الحرب الباردة"، فيدهنيميكيس، السيد صدقي عابدين (محررين)، قضايا الأمن في آسيا، (القاهرة: مركز الدراسات الأسيوية، كلية الاقتصاد والعلوم السياسية 2004) ص 14.

¹⁷Athina Karatzogianni,(ed), "Cyber–Conflict and Global Politics", Routledge and Taylor & Francis Group. 11th September 2008, pp. 240– 272.

¹⁸Rebecca Grant, "Victory in Cyberspace", The Eaker Institute, the policy and research arm, TheAir Force Association of US, October 9, 2007.

(www.afa.org/media/reports/victorycyberspace.pdf–)

¹⁹عادل عبد الصادق، " أمريكا وتشكيل قيادة عسكرية في الفضاء الإلكتروني. هل بدأ الاستعداد لحروب المستقبل؟،مجلة

تعليقات مصرية، مركز الدراسات السياسية والاستراتيجية بالأهرام، العدد 130، 12 جوان 2009م

(<http://acpss.ahram.org.eg/Ahram/2009/7/12/COMMO.HTM>)

²⁰Kevin G.Coleman, A Cyber War has begun, Cyber Warfare, The Technolytics Institute, September 2007, (http://www.technolytics.com/Technolytics_Cyber War.pdf)

²¹Martin C.Libicki, "Conquest in Cyberspace National Security and Information Warfare". Cambridge University Press, RAND Cooperation, California, 2007, pp: 100,124,166,215,230,285,306.

²²Arsenio T.Gumahad, Cyber Troops and Net War: The Profession of Arms in the Information Age. Maxwell AFB, AL: Air University, Air War College, April 1996. pp.57–156.

²³Tim Jordan, "Cyber power: The Culture and Politics of Cyberspace and the Internet". Rout ledge, 2000, pp: 160–254.

²⁴Adam Peake, Internet governance and the World Summit on the Information Society WSIS)– Prepared for the Association for Progressive Communications (APC), June 2004, P: 3.

²⁵وليد عبد الحي، "إشكالية الفضاء الإلكتروني في حقوق الملكية الفكرية"،المؤتمر العالمي العلمي الأول حول الملكية

الفكرية، جامعة اليرموك، المملكة الأردنية الهاشمية، 2000/07/10.