

هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين

م.م. علي عبد الرحيم العبودي^(*)

الملخص

عرف التاريخ البشري صراعات وحروب عدة بين الدول وكان ميدانها الرئيس ارض الواقع، ولها حدود معينة ضمن رقعة جغرافية محددة، وتدار بأدوات معروفة تتناسب مع هذا الصراع أو ذاك (بري، بحري، جوي)، ولكل طرف من هذا الصراع سواء اكان اقليمياً أو دولياً أدواته الخاصة التقليدية في الردع والهجوم والدفاع، بمعنى أكثر وضوحاً، أن كل الاطراف الداخلة في الصراع بإمكانها تحديد العدو والصديق مسبقاً، وما لها وما عليها والأهداف التي ترغب في تحقيقها عند دخولها في صراع ما . إلا أنه ومع نهاية القرن الثاني ودخول القرن الثالث وبفضل الثورة المعلوماتية المتمثلة في الكم الهائل من المعرفة والمعلومات والثورة التكنولوجية المتمثلة في الاقمار الصناعية والاتصال المباشر بها عبر الحواسيب الذكية وشبكات الانترنت (الشبكة العنكبوتية)، أصبح هناك مسرح آخر وفضاء آخر تدار عليه الصراعات بكل انواعها وصنوفها، وهذا المسرح يختلف تماماً عن المسارح القديمة للصراعات (البري، البحري، الجوي)، فهو مسرح آتى متلائماً مع هذا العصر، فقد أدى التطور التكنولوجي، كانتشار الإنترنت والحواسيب، والأجهزة النقلة، وتوافر الحزمة العريضة للإنترنت عبر الأجهزة النقلة وتدني كلفتها، إلى ارتفاع أعداد مستخدمي الإنترنت وتزايد اعتماد الدول على هذه التكنولوجيات في التنمية الاقتصادية والاجتماعية . إلا أن الانفتاح الذي يميّز شبكة الإنترنت، والفضاء السيبراني عموماً، جعلها عرضة للتعديات والأنشطة الغير سلمية،

^(*) جامعة بغداد - كلية العلوم السياسية.

فصار مستخدمو الفضاء السيبراني من الدول وغير الدول عرضة للانتهاكات والتهديد لمنظومتها الإلكترونية، إذ لا يمكن لأي حكومة، أو إدارة، سواء أكانت من العالم الثالث، أم في الدول الأكثر تقدماً، أن تنأى بنفسها عن الهم الذي يمثل اختراق الشبكات، وتهديد أمنها ومصالحها.

Abstract

Human history has known many conflicts and wars among nations and its field has been the ground, and are run by well-known instruments suited to this or that conflict (land, sea, air). Each party, regional or international, has its own traditional tools In deterrence, attack and defense, in a more obvious sense, that all parties involved in the conflict can determine the enemy and the friend in advance, what they have and what they have and the goals they want to achieve when entering into a conflict. However, by the end of the second century and the entry of the third century and thanks to the information revolution, which is the vast amount of knowledge and information and the technological revolution of satellite and direct communication through smart computers and the Internet, there is another theater and space is managed by all kinds of conflicts and their names , This theater is quite different from the old theaters of conflicts (land, sea, air), it is a theater that came in line with this era, Technological development, such as Internet access, computers, mobile devices, broadband Internet availability and low cost mobile devices, has led to an increase in the number of Internet users and increased adoption by States of these technologies for economic and social development. However, the openness that characterizes the Internet and cyberspace in general has made it vulnerable to transgressions and non-peaceful activities. Cyberspace users from both countries and non-states are vulnerable to violations and threats to their electronic systems. No government, no management, no third world, The more advanced countries, to distance themselves from the concern that represents the penetration of networks, and threaten its security and interests.

مقدمة

على مدى التاريخ البشري والصراعات بين الدول تجري على ارض الواقع، ولها حدود معينة ضمن رقعة جغرافية محددة، وتدار بأدوات معروفة تتناسب مع هذا الصراع أو ذاك (بري، بحري، جوي)، ولكل طرف من هذا الصراع سواء اكان اقليمياً أو دولياً أدواته الخاصة التقليدية في الردع والهجوم والدفاع، بمعنى أكثر وضوحاً، أن كل الاطراف الداخلة في الصراع بإمكانها تحديد العدو والصديق مسبقاً، وما لها وما عليها والأهداف التي ترغب في تحقيقها عند دخولها في صراع ما . إلا أنه ومع نهاية القرن الثاني ودخول القرن الثالث وبفضل الثورة المعلوماتية المتمثلة في الكم الهائل من المعرفة والمعلومات والثورة التكنولوجية المتمثلة في الاقمار الصناعية والاتصال المباشر بها عبر الحواسيب الذكية وشبكات الإنترنت (الشبكة العنكبوتية)، أصبح هناك مسرح اخر وفضاء اخر تدار عليه الصراعات بكل انواعها وصنوفها، وهذا المسرح يختلف تماماً عن المسارح القديمة للصراعات (البري، البحري، الجوي)، فهو مسرح آتى متلائماً مع هذا العصر.

ووفقاً للدراسات أن أي ظاهرة أو حدث لا ينمو ويزدهر إلا في ظل بيئة حاضنة، وظروف مواتية تحفز على اتجاه داعم لها من التشجيع والمساندة المجتمعية، وهذا ما وجدته الشبكات الرقمية (الإنترنت) فعلاً من قبول واسع النطاق في كل انحاء المعمورة، فمنذ نهايات القرن العشرين وتحديداً عام 1981 عندما استخدم الإنترنت بشكل فعلي بدأ العالم يشهد طفرات نوعية سريعة لم يشهدها قبل هذا التاريخ، خاصة في مجال المعلومات والتكنولوجيا والاتصالات، هذا التطور الكبير والمزاوجة بين المعلومات وتكنولوجيا الاتصالات خاصة في بداية القرن الحادي والعشرين، افرز لنا مجتمع وساحة افتراضية متكاملة ينشيط في ظلها ليس الانسان فحسب بل الدول، ويؤثرون ويتأثرون بها .

وتبعاً لذلك اخذت الدول والمنظمات والشركات الكبرى تولي أهمية كبيرة بالفضاء السيبراني (الالكتروني)، وذلك لتحقيق اهدافهم ومصالحهم ، لذلك اصبحت المواقع الإلكترونية والبرامج عبر الإنترنت خاصة تلك البرامج المرتبطة بالبنى التحتية للدول

وسيلة وأداة وهدف تسعى إلى امتلاكها واستغلالها هذه الدولة أو تلك لمصلحتها الخاصة .

وعلى وفق ذلك ولحدثة الموضوع وغموضه سيتمحور هذا البحث حول جملة من التساؤلات التي تكون اشكاليته وهي : ما هو الصراع السيبراني وكيف نشأ ومدى اختلافه عن الصراع التقليدي؟ من هم الفاعلين في هذا الفضاء السيبراني وطبيعة الصراعات داخله؟ وما خصائص هذا الفضاء والحروب داخله؟ ومدى تأثير مثل هكذا صراعات على الأمن والسلم الدوليين؟ .

وينطلق البحث من فرضية مفادها : أن الصراعات بين الفاعلين الدوليين والسباق بينهما للاستحواذ والسيطرة على الفضاء السيبراني (الإلكتروني) سوف يكون له الأثر الواسع في تحول هذه الصراعات من مجرد مناورات إلى حروب واقعية يكون ميدانها الرئيس الفضاء الرقمي .

وتبعاً لذلك وللتأكد من صحة هذه الفرضية أو عدمها تم تقسيم هذا البحث وفق الآتي:

اولاً - الصراع التقليدي السيبراني مدخل في المفهوم ومراحل التحول

ثم علاقة ارتباطية بين طبيعة الصراعات وأشكالها ، فهي تعتمد على ما تشهده المجتمعات والدول من تطورات مادية وغير مادية ، ولكل شكل من اشكال الصراع قواعده وحواضنه ومسبباته وأطرافه الفاعلين (أفراد، جماعات، دول) . وعلى وفق ذلك يتعين علينا فهم ماهية الصراع السيبراني ودرجة اختلافه عن الصراعات التقليدية .

1- السيبرانية النشأة والتطور والمفاهيم المقارنة

كلمة السيبراني مشتقة من كلمة (ساير cyber) والتي تعني (إلكتروني) وبإضافة اي كلمة لها تعطىها الصفة الإلكترونية، على سبيل المثال لا الحصر (cyber security) تعني الأمن الإلكتروني⁽¹⁾. وارتبط الصراع السيبراني (الإلكتروني) ارتباطاً وثيقاً بظهور شبكة الإنترنت ، إذ تأسست شبكة الانترنت في الأصل بالولايات المتحدة الأمريكية في أواخر الستينيات كمشروع تشرف عليه وكالة مشاريع البحوث

المتقدمة التابعة لوزارة الدفاع الأمريكية ، وقد كانت يطلق على هذه الشبكة في بداية أمرها (ارنت)، ويشير احد المتخصصين في شبكة الإنترنت في أمريكا إلى تاريخ هذه الشبكة يرجع إلى عام 1969، وجرى أول عرض لها خلال المؤتمر العلمي حول اتصالات الحاسوب بواشنطن عام 1972، أما شكل الرسائل الإلكترونية فقد حددت في عام 1977⁽²⁾.

ومسمى الإنترنت (Internet)) مشتق من مسمى شبكة المعلومات الدولية التي ينطق عليها باللغة الانجليزية (International Net Work))، كما يطلق على الإنترنت تسميات عدة منها (The Net)، والشبكة العالمية (World Net)، والشبكة العنكبوتية (The Web)، والطريق الإلكتروني السريع للمعلومات⁽³⁾ (Electronic Super High Way).

وانتشرت شبكة الإنترنت في دول العالم مع بداية الثمانينيات، وكان لها الدور الكبير في ربط الشبكات بين دول العالم، مما أدى إلى سهولة نقل البيانات والمعلومات⁽⁴⁾. وتتمتع شبكة الإنترنت بخصائص فريدة من نوعها يمكن إجمالها بالاتي⁽⁵⁾:

- 1- إلغاء فكرة الحدود بين الدول .
- 2- المرونة في الحصول على المعلومات .
- 3- تكلفة اقل مقارنة مع الاهداف المنشودة منها .
- 4- امكانية استخدامها والوصول عبرها إلى جميع انحاء العالم (افراد، جماعات، دول) .

وعند تتبع التأريخ نجد أن النواة الأولى لنشأت الفضاء الإلكتروني (CyberSpace) تعود لمرحلة اندلاع الحرب الاهلية في الولايات المتحدة الامريكية عام 1861، إذ استخدمت لأول مرة البرقية لإدارة الحرب، حينها اصبحت برقية التلغراف جزء مهم من منظومة الحرب⁽⁶⁾. وفي عام 1888 ، أثبت عالم الماني أن الطاقة الكهربائية تخلق ترددات في الفضاء تكون بمثابة اشارات يمكن اعتمادها ورصدها، وقد قاد هذا الاكتشاف إلى الاهتمام بما عرف فيما بعد بـ(الذبذبات الهرتزية)

التي استخدمت في تطوير نظام الراديو في انكلترا، وكان التطبيق العملي الأول لهذه التقنية أثناء الحرب الروسية-اليابانية عام 1904 ، حينما قصفت السفينتان اليابانيتان الحريتان (كاسوجا ونيشين) القاعدة البحرية الروسية في ميناء (آرثر)، وكانت معهما سفينة صغيرة تصحح النيران باستخدام الراديو (اللاسلكي)، وسمع أحد عمال الروس الإشارة بالمصادفة ، وتضمنت تعليمات تصحيح النيران فاستخدم جهاز الارسال اللاسلكي في إعاقة الاتصال الياباني بالضغط على مفتاح الارسال على تردد الشبكة اليابانية نفسها ، مما عطل بلاغات تصحيح النيران من أن تُبلغ لمدفعية السفينتين؛ وهكذا، لم ينتج عن هذا القصف البحري سوى إصابات طفيفة، بفضل هذا الاكتشاف⁽⁷⁾.

كانت الحربان العالميتان الثان شهدهما العالم في النصف الأول من القرن العشرين نقطة الانطلاق للتفكير في دور التقنية في إدارة الصراع وتحقيق النصر ، لذلك سعت الدول المتحاربة على تطوير امكانياتها التقنية المتمثلة في الاتصال اللاسلكي (الرادار) وقتذاك⁽⁸⁾. وفي ثلاثينيات القرن الماضي طورت كل من الولايات المتحدة وبريطانيا وألمانيا اجهزة الارسال بشكل ملحوظ وأنتجت اجهزة استقبال ذات حساسية عالية وهوائيات دقيقة التوجيه ، فأصبح جهاز الرادار قادراً على اكتشاف الطائرات على مسافة نحو (50) ميلاً⁽⁹⁾.

وفي النصف الثاني من القرن العشرين ، ونظراً للتنافس بين القطبين العالميين الاتحاد السوفيتي الاسبق والولايات المتحدة الامريكية ، جرى سباق في تطوير الأدوات الإلكترونية ، فكانت النتيجة تطوير منظومات التسليح واستخدام التقنيات الحديثة في انظمة الاتصال والسيطرة والتحكم عن بعد⁽¹⁰⁾. وعلى صعيد الشرق الاوسط والصراع العربي - الاسرائيلي ، فقد استخدم كثيرا الخداع الإلكتروني من قبل الطرفين في إدارة هذا الصراع، وذلك عبر التشويش التكتيكي لمنظومة الاتصال والاستطلاع للطرفين⁽¹¹⁾.

ومع نهاية القرن العشرين وبداية القرن الحادي والعشرين، وبالتوظيف المكثف للشورة المعلوماتية والثورة التقنية المتمثلة بالإنترنت اتسع الاعتماد على الوسائل الإلكترونية

(الفضاء الرقمي)، حتى تبدل الهدف النهائي للحرب من التدمير للإنساني للخصم إلى التحكم المفرط في تشكيل سلوكه؛ سبيلا لتحقيق الغايات النهائية من فن إدارة الصراع، لذلك شهدت القواميس والموسوعات المعرفية ولادة مصطلحات جديدة مثل (حرب المعلومات، الحرب الإلكترونية، والحرب الرقمية، وحرب الشبكات)⁽¹²⁾ . حيث انتقلت مثل هذه المفاهيم من المستوى النظري المجرد، إلى المستوى الواقعي الملموس، بفضل حدوث ثلاث متغيرات متزامنة ؛ أولهما- اتساع تطبيق نظام الحكومة الالكترونية (E-government)، والثاني- زيادة اعتماد مختلف الهيئات الحكومية على نظام التخزين (DATA)، وأخيراً- زيادة حجم التكلفة المادية والبشرية لنمط الصراعات التقليدية⁽¹³⁾ .

2-التحول من الصراع التقليدي إلى الصراع السيبراني .

كانت الصراعات المحلية والإقليمية والدولية تدار على ارض الواقع ، أي على المجال المادي المنظور، فيعكس هذا المجال القضايا والأحداث بين الفاعلين فيه ، إذ جرت صراعات وحروب عدة على مدى العصور، وكان الفضاء العام التقليدي (براً ، بحراً ، جواً)، هو الميدان الرئيس الذي يعبر فيه الفاعلون الدوليون عن مصالحهم وقضاياهم ، على سبيل المثال لا الحصر ؛ فقد شهد العالم الحديث ومنذ ظهور الدول القومية حربين عالميتين مدويتين ، حيث تم إدارة هذا الصراع العالمي بين الدول بأدوات تقليدية (قذائف ، طائرات، صواريخ ، مدافع...الخ)، وذلك لتحقيق اهدافهم ومصالحهم⁽¹⁴⁾ .

بعد افول هاتين الحربين وانتصار احد اطرافها على الاخر وفرضه محددات وقيود على الطرف المغلوب، فضلا عن تأسيس منظمة الأمم المتحدة للحيلولة دون وقوع صراعات عالمية اخرى وفض النزاعات بين الدول والمنظمات بالطرق السلمية عن طريق فروعها ، انخفض التوتر الدولي ، خاصة مع وجود قاعدة الردع النووي وتوازن القوى الذي فرضه النصف الثاني من القرن العشرين⁽¹⁵⁾ .

ومع الثورة التكنولوجية التي شهدتها العالم برز الفضاء الإلكتروني أو السيبراني (CyberSpace) كساحة للصراع العالمي، ومع ظهور هذا الفضاء واجهت المفاهيم التقليدية، مثل الصراع، وأمن الدولة، والقوة الكمية، والسيادة، تحديات واضحة، خاصة من جهة ملاءمتها، أو حتى تكيفها مع طبيعة التفاعلات في هذا الفضاء الافتراضي. ولكن ما هي حروب الفضاء الإلكتروني؟.

كانت حرب الفضاء غير واضحة المعالم في تسعينيات القرن الماضي، لأنها كانت مختلطة مع الحروب النفسية والدعائية، وكانت مقصورة على عمليات التشويش على أنظمة الرادار وأجهزة الإنذار كما ذكر انفاً، في حين أن اتساع شبكة الإنترنت فتح آفاق كبيرة للأجهزة المخبرية لاستغلال هذه الشبكة في حروبها الدولية، والتغلغل في أي شبكة من شبكات الإنترنت والسيطرة على هذه الشبكة وتعطيلها أو تغيير البيانات عليها أو إتلافها أو التحكم فيها من خلال الضغط على بضعة أزرار⁽¹⁶⁾.

ويعرف مصطلح حروب (الفضاء الإلكتروني) السيبرانية على أنه الإجراءات التي تتخذها أي دولة أو منظمة أو مجموعة لاختراق أجهزة الحاسوب أو الشبكات الخاصة بدولة أخرى لغرض السيطرة عليها أو التحكم بها أو إتلافها أو تعطيلها عن العمل، من خلال إرسال رسائل مكتوبة باللغة الرقمية الثنائية المكونة من رقمي (0-1)⁽¹⁷⁾.

ودفع التطور في مجال الفضاء الإلكتروني خاصة في نهاية القرن العشرين وبداية القرن الحادي والعشرين، الدول على تعزيز دفاعاتها ضد خطر التعرض للهجمات الإلكترونية، ولكنها اتجهت إلى التحول من اتخاذ إجراءات وقائية ذات طابع دفاعي إلى الاتجاه إلى تبني سياسات هجومية، ويحمل ذلك في طياته مخاطر عسكرية الفضاء الإلكتروني، خاصة وأن القدرة على السيطرة على مثل هذا النوع من الأسلحة ضئيلة بالمقارنة مع الأسلحة التقليدية، وهناك مسألة صعوبة تحديد الأسلحة التي يمتلكها الآخرون ومن ثم يتعذر على المجتمع الدولي القدرة على التدخل لاحتواء التقدم في مثل هكذا أسلحة⁽¹⁸⁾.

ورغم الجدل الحاصل حول نشأت مثل هكذا حروب، إلا أنه يكون ممكناً للاعتبارات الآتية⁽¹⁹⁾:

- 1- وجود ثغرة في تصميم الإنترنت .
- 2- وجود ثغرات في المعدات والبرمجيات .
- 3- الاتجاه في ربط المزيد من الاجهزة والقطاعات على شبكات الفضاء الإلكتروني .

وعلى الرغم من ذلك كله، فإن الحروب في الفضاء الإلكتروني، لا تلغي الحروب التقليدية، بل على العكس من ذلك ، إذ أن الصراع بين الفاعلين على السيطرة على الفضاء الإلكتروني ما هو إلا انعكاس للمصالح المادية الواقعية بين الدول والمنظمات والجماعات . وعليه يُمكننا القول بأن : (الفضاء السيبراني هو مجال مركّب مادي وغير مادي يشمل مجموعة من العناصر هي : أجهزة الكمبيوتر، أنظمة الشبكات والبرمجيات، حوسبة المعلومات، نقل وتخزين البيانات، ومستخدمو كل هذه العناصر)⁽²⁰⁾ .

ثانياً- خصائص الفضاء السيبراني وحروب الفضاء

على الرغم من وجود بعض التشابه بين الفضاء التقليدي والفضاء السيبراني، إلا ان هناك مجموعة من الخصائص يتميز بها الفضاء السيبراني بصورة عامة، والحروب السيبرانية (الإلكترونية) بصورة خاصة، عن الفضاء العام التقليدي .

1- خصائص الفضاء السيبراني

في مضمونه الشامل، كما طرحه يورجين هابرماس⁽²¹⁾ . فإن المجال العام هو الساحة التي يعبر فيها الأفراد او الجماعات ، أيًا كانت انتماءاتهم، عن آرائهم بحرية دون قيود أو تأثيرات من جهات رسمية او غير رسمية، ومن ثم فهو أكثر اتساعاً، من حيث القضايا والفاعلون أو الديناميات من المجالات الأخرى كالسياسي الذي ينحصر في التنافس على السلطة⁽²²⁾ .

لكن مع بروز الفضاء الإلكتروني أو السيبراني جعل ذلك المفهوم للمجال العام أكثر اتساعاً ، وذلك يعزى للإقبال المتزايد عليه من قبل الأفراد والجماعات والدول للتعبير عن موقفهم بحرية، لاسيما مع ما وفرته أدوات التكنولوجيا الحديثة، مثل الإنترنت

وتقنيات الاتصال المتطورة، كالحاسوب، والهواتف الذكية، وغيرها من حراك، وانتشار وديناميكية⁽²³⁾.

هنا يمكن النظر إلى المجال العام السيبراني (الفضاء الإلكتروني) على أنه امتداد للمجال العام التقليدي في الفضاء الإلكتروني، وعاكس في الوقت عينه لفاعلية، وقضاياه، وتفاعلاته. ووفقاً لذلك يمكن تلخيص سمات عدة أساسية للمجال العام السيبراني، وهي كالآتي⁽²⁴⁾:

- الحرية النسبية، وضعف السيطرة الحكومية: إذ إن طبيعة المجال العام السيبراني، التي تحفل بملايين النقاشات اليومية، تصعب من سيطرة الحكومات عليه، ولذا، يستطيع الأفراد والجماعات التعبير عن مواقفها وآرائهم في أي وقت، ومن أي مكان، بما يشكل دافع أكبر لهم للمشاركة في النقاش والتفاعل حول القضايا العامة.

- القدرة على التشبيك، وبناء روابط افتراضية: حيث تتيح الأدوات السيبرانية للأفراد، والجماعات قدرة أكبر على التواصل والتشبيك وبناء مجتمعات افتراضية بأشكال مختلفة للتأثير في القضايا عبر وسائل التواصل الاجتماعي والمنتديات الإلكترونية وغيرها... ذلك الأمر قد لا يتوافر في المجال العام التقليدي، لاسيما مع القيود التي تفرضها الانظمة السلطوية على عملية التنظيم التي قد يُقدم عليها الأفراد والجماعات.

- الطبيعة الطوعية وليس الجبرية: وهي خاصية ممتدة من المجال العام التقليدي إلى السيبراني، وإن اتسع مع هذا الأخير، بل إنها تفسر الإقبال الشديد عليه، بحسبانه، خالاً من الاجبار الذي يعانيه المواطن في العديد من مجالات حياته اليومية، خاصة في علاقته بالدولة والقوانين.

- القدرة على تداول الأفكار بشكل سريع ومؤثر: فمع معرفة الافراد أو الجماعات أن هناك ملايين البشر يستخدمون الإنترنت، والمواقع الإلكترونية يومياً، فإن فكرة مشاركتهم في المجال العام تكون أكثر إغراء لان آرائهم ومواقفهم ستصل عندئذ إلى جمهور أوسع، فبالمقارنة، مثلاً، بالصحف الورقية،

التي تنشر على نطاق جغرافي معين، وترتبط بدفع مبالغ نقدية، إلى جانب الرقابة على محتواها، يعد المجال العام السيبراني أكثر تنوعاً وتحراً من تلك القيود، مما ينعكس على المحتوى الذي يتعرض له المشاركون في هذا المجال .

▪ الفضاء الإلكتروني لا حدود له، حيث يتشارك كل الفاعلين بما فيهم الدول من الاستخدام الشخصي إلى البرامج الاقتصادية إلى التطبيقات العسكرية، كلها تعتمد على الفضاء الإلكتروني . وعلى العكس من التهديدات التقليدية الملموسة والممكن التنبؤ بها، فإن تهديدات الفضاء الإلكتروني يمكن أن تأخذ شكل و مصدر إفتراضي و تفرض أخطاراً لا يمكن التنبؤ بها (25) .

2- خصائص الحروب السيبرانية

تحتوي الحروب السيبرانية على مجموعة من الخصائص والتي تميزها عن الحروب التقليدية، ويمكن اجمالها بالآتي (26):

1- الحرب الرقمية هي حرب تقنية متطورة ، جسدت قمة التطور الذي بلغته ثورة المعلومات وبوابتها الحاسبة الإلكترونية التي شكلت بدورها الأداة المحورية لهذا النوع من الحروب والميدان الرئيس لها فكانت نتيجة لذلك عرضة للتطور المستمر والتنوع والابتكار في تقنياتها ووسائلها لارتباطها الرأسي بقمي الهرم التقني للحضارة الإنسانية ، والمصالح الحيوية للدول .

2- حرب لا تناظرية (Asymmetric) : بحساب التكلفة المتدنية نسبياً للأدوات اللازمة لشنها ، فلا تحتاج الدول في سياق ذلك إلى تخصيص ميزانيات ضخمة لإنتاج أسلحتها أسوة بالأسلحة المستخدمة في النزاعات العنيفة التقليدية ذات الكلفة العالية جداً كحاملات الطائرات والمقاتلات المتطورة ؛ لتفرض تهديداً خطيراً وحقيقياً على الدول الكبرى مثل الولايات المتحدة الأمريكية وروسيا الاتحادية على سبيل المثال .

5- تمتّع المهاجم بأفضلية واضحة في حروب الإنترنت على المدافع، فهذه الحروب تتميز بالسرعة والمرونة والمراوغة وفي بيئة مماثلة يتمتّع بها المهاجم بأفضلية، من الصعب جداً على عقلية التحصّن لوحدها أن تنجح؛ فالتحصين بهذا

المعنى سيجعل من هذا الطرف عرضة لمزيد من محاولات الاختراق ، وبالتالي المزيد من الضغط .

8- حرب هلامية الشكل والملح ، فهي متعددة بميادينها ، متنوعة ومتطورة بوسائلها المرتبطة بأكثر المجالات التقنية تطورا وتبدلا في الحياة المعاصرة للدول ، وهي ، فضل عن ذلك ، غير محددة الأهداف والتأثيرات ، إذ قد تعدى مخاطرها ميادين القتال التقليدية لتطال بدمارها حتى أكثر المواقع السيادية والحساسة تحصينا وبعدا عن دائرة القتال .

26- فشل نماذج "الردع" المعروفة : يعد مفهوم الردع الذي تمّ تطبيقه بشكل أساس في الحرب الباردة غير ذي جدوى في حروب الفضاء الإلكتروني ؛ فالردع بالانتقام ، أو العقاب ، لا ينطبق على مثل هكذا حروب . فعلى عكس الحروب التقليدية عندما ينطلق الصاروخ من أماكن يتم رصدها والرد عليها فإنه من الصعوبة بمكان ، بل ومن المستحيل في كثير من الأحيان تحديد مكان وشخصية القائم بالهجمات الإلكترونية ذات الزخم العالي؛ لكونها لا تترك أثرا ، او دليل ، على حصولها ، إذ إن معظم الهجمات الإلكترونية يتم اكتشافها بالصدفة ، وبعد وقت طويل ، وبلاستعانة بخبرة فنية عالية المستوى في كشف مصدر الهجوم ، وهذا أمر قد يتطلب وقت ليس بالقصير ، ما يعني إلغاء مفعول الردع بالانتقام ، والأكثر من هذا ، فحتى إذا تم اكتشاف مصدر الهجوم الإلكتروني ، وتبين أنها تعود لفاعلين غير حكوميين ، فإنه في هذه الحالة لن يكون لديهم أصول ، أو قواعد ، حتى يتم الرد عليها .

27- كذلك تتميز الحرب السيبرانية (Cyber War) بأن بها تدمير لا تصاحبه دماء وأشلاء بالضرورة ، إذ يتضمن التجسس والتسلل ثم النسف لكن لا دخان ولا أنقاض ولا غبار ، ويتميز أطرافه بعدم الوضوح وتكون تداعياته خطيرة سواء عن طريق تدمير المواقع على الإنترنت ونسفها وقصفها بوابل من الفيروسات أو العمل على استخدام أسلحة الفضاء الإلكتروني المتعددة ، للنيل من سلامة تلك المواقع ، وهي أسلحة يسهل الحصول عليها من خلال مواقع الإنترنت أيضا وتعلم كيفية

استخدامها، كما إن انتشار الفضاء الإلكتروني وسهولة الدخول إليه يمكن أن يوسع دائرة استهداف المواقع بالإضافة إلى زيادة عدد المهاجمين، ولتدور تلك الهجمات المتبادلة على نحو من الكر والفر ليعبر عن حالة صراع ممتد يرتبط بطبيعة الفضاء الإلكتروني المختلفة⁽²⁷⁾.

ثالثاً- ملامح الفاعلين وطبيعة الصراع داخل الفضاء السيبراني

1- ملامح الفاعلين داخل الفضاء السيبراني

قبل بروز الإنترنت عدت الدول الفاعلين الاساسيين في الفضاء العام التقليدي ، هذا لا يعني عدم وجود فاعلين اخرين ، بل بعدها المتسيدة على بقية الفاعلين من غير الدول الذين لهم دور شبة هامشي داخل الفضاء التقليدي ، وذلك بحكم الإمكانيات والقدرات التي تمتلكها الدول ، أما بعد التطور السريع في تكنولوجيا الاتصالات والمعلومات وظهور الفضاء الإلكتروني (السيبراني) كفضاء أكثر اتساعاً من الفضاء التقليدي ، برز معه فاعلين دوليين من غير الدول ، إذ سنح لهم هذا الفضاء الجديد بلعب دوراً كبيراً ومؤثراً على الساحة الدولية يكاد يكون متساوياً مع الدور الذي تلعبه الدول الكبرى، ويعزى ذلك لتغيير مفهوم القوة الذي فرضه الفضاء الإلكتروني، ومن ثم، تلاشي الفارق في القوة التقليدي بين الدول والفاعلين من غير الدول.

يمكن اجمال الفاعلين الرئيسيين داخل الفضاء السيبراني على النحو الآتي:

1. الدول والحكومات : مع نهاية القرن العشرين أدركت الدول، وخاصة الكبرى ، بضرورة تغيير استراتيجياتها أو اضافة استراتيجية إلى استراتيجياتها بما يتلائم مع بيئة القرن الحادي والعشرين ، وما طرأ عليه من تطورات وترتيب في سلم الأولويات . لذا شهد العقدان الأخيران سباقاً محموماً بين بعض القوى الإقليمية في مناطق العالم المختلفة لتعظيم الاستفادة من الفضاء السيبراني (Cyberspace)، إذ عدت هذه الدول والحكومات القدرات السيبرانية (Cyber Capabilities) وسيلة لبسط النفوذ اقليمياً ، وتحقيق مكاسب

استراتيجية، وسياسية، ومالية، واقتصادية، لم تكن لتحقيقها عبر الوسائل العسكرية والدبلوماسية التقليدية⁽²⁸⁾.

ونظراً لما أحدثته المجال العام في الفضاء الإلكتروني أو السيبراني من انتشار وفعالية، فقد تم توظيفه في الصراعات السياسية والتنافس الاقتصادي بين الدول، وتجلى ذلك بشكل واضح ابان الثورات العربية (الربيع العربي) التي انطلقت في عام 2010، حيث استخدمت المعارضة الشعبية المدعومة من الخارج مواقع التواصل الاجتماعي، والهواتف المحمولة والحواسيب من أجل التعبئة للاحتجاجات وخلع السلطة في كثير من الدول العربية⁽²⁹⁾.

وبحسب التقسيم الذي قدمه عالم السياسة الأمريكي (جوزيف ناي) لأنماط القوة، القوة الصلبة والقوة الناعمة، حيث عرف القدرات السيبرانية على انها جزء من القوة الناعمة، وهي بذلك تُعد مظهر من مظاهر القوة في التفاعلات الإقليمية والدولية، ومن ثم، تنطوي قوة دولة ما سيبرانياً على ما تملكه من قدرات وإمكانيات في الفضاء الإلكتروني⁽³⁰⁾. لذلك سعت الدول على تطوير قدراتها السيبرانية، حتى اتسعت في الوقت الحالي قائمة الدول ذات القدرات السيبرانية المتطورة، فلم تعد القائمة تقتصر على الدول العظمى والكبرى كالولايات المتحدة، والصين، وبريطانيا، وروسيا، بل ظهرت في اقاليم مختلفة قوة سيبرانية يعتد بها، كاستراليا، والهند، وإندونيسيا، وكوريا الجنوبية، والمكسيك، والأرجنتين، وإيران، وتركيا⁽³¹⁾.

2. الشركات متعددة الجنسية: تعد الشركات المتعددة الجنسيات من أكثر الأنماط تعبيراً عن عولمة الاقتصاد، لما تملكه من إمكانيات مادية وبشرية هائلة تمتد إلى مختلف دول العالم، وتنوع نشاطاتها لتشمل قطاعات الإنتاج والتجارة والخدمات والمال والمصارف الدولية، بغية توزيع المخاطر وتنويع مصادر الربح، وسعيها لتحويل العالم إلى ساحة اقتصادية واحدة بغية بسط نفوذها، وإحكام سيطرتها على قطاعات الأعمال في العالم، مستفيدة من منجزات التقدم العلمي والتقني⁽³²⁾. لذا كونت هذه الشركات رؤوس أموال ضخمة وأنشأت فروع في دول

عدة مما اتاح لها السيطرة على التعليمات البرمجية الخاصة، الأمر الذي جعلها من الفاعلين الرئيسيين داخل الفضاء السيبراني⁽³³⁾.

3. الجماعات المسلحة أو الارهابية : مع تزايد اعتماد العالم على الفضاء الرقمي (الإنترنت) اتجهت الجماعات المسلحة بالاتجاه نفسه في اتخاذ الفضاء الإلكتروني كساحة للعبئة ، وتبعاً لذلك ، قد تمكنت معظم التنظيمات الإرهابية شبه المنظمة من امتلاك أدوات المعرفة والتقنية اللازمة لاختراق العالم الافتراضي بدرجة كبيرة ، وتكفي الإشارة هنا إلى زيادة عدد المواقع المحسوبة لجماعات مسلحة عالمية ، فوفقاً لكتاب (الإرهاب العالمي والإعلام الجديد) لمؤلفيه فليب سيب ودانا جانبك - الخبيرين في الدراسات الإعلامية - فإن عدد المواقع المحسوبة لجماعات الإرهاب العالمي ارتفع من نحو (12) موقعاً إلكترونياً عام 1997، إلى (4,350) موقعاً في أوائل عام 2005، ثم (4,800) موقع عام 2006، وتجاوز أكثر من (6) آلاف موقع إلكتروني في نهاية عام 2008، ومن الملحوظ أن تنظيم القاعدة كان له السبق في الاعتماد على المواقع الإلكترونية لتحقيق الأهداف الاستراتيجية، وتسهيل القيام بالعمليات التكتيكية⁽³⁴⁾. وذلك عبر استقطاب وتوجيه جنود جدد من خلال المواقع الإلكترونية التابعة لهم مثل موقع النداء الإلكتروني، ومجلتهم الإلكترونية المسمى (البتا)..الخ⁽³⁵⁾. أما التنظيم الإرهابي (داعش)، الذي يُعد مثلاً حياً للفاعلين المسلحين من غير الدول، فله أزيد من (53) ألف موقع إلكتروني، (90) ألف صفحة باللغة العربية و (13) ألف بلغات أخرى ، وهذا ما ساهم في تجنيده حوالي (3400) شاب شهرياً عبر مواقعهم الإلكترونية ، بحسب تقرير الخبير الأمني في قضايا الإرهاب الرقمي جيف باردين⁽³⁶⁾ (bardin jeff).

4. الأنونيموس وويكيليكس : فالأنونيموس أو المجهولون هم جماعات احتجاجية منتشرة حول العالم داخل الفضاء الإلكتروني ، لهم اهداف سياسية ، من ابرز وظائفهم هو توزيع المعلومات السرية، وتشويه المواقع، وتوليد احتجاجات حول القضايا السياسية، وهم نمط جديد من الفاعلين السياسيين الذين يعتمدون

على اخفاء الهوية ، والقيادة بلا جسد وانخراط الافراد بلا عضوية دائمة ، وعلى هجمات افتراضية ضد اهداف مادية وحيوية من اجل تشجيع التغيير السياسي . أما "ويكيليكس" فهو موقع تم تأسيسه في عام 2007 ، ويستهدف فضح الانظمة السياسية عبر تسريب الوثائق والأسرار حول الحكومات والشخصيات العامة، وشكل كل من الانونيموس وويكيليكس نماذج لما قد يسببه الفاعلون من غير الدول من تأثيرات صراعية محلية وإقليمية ودولية عبر الفضاء الإلكتروني⁽³⁷⁾. وخير دليل على ذلك ما قام به موقع ويكيليكس من نشر فيديو لمروحية أمريكية وهي تقصف مدنيين عراقيين بينهم صحفي، ليتبع ذلك العديد من المنشورات التي أظهرت السلوك السياسي الخارجي لبعض دول العالم التي تدعي الديمقراطية والحرية، مما سبب لها أزمات تعلقة بأمنها الاجتماعي والسياسي، ونظرتها للحريات، وحقوق الإنسان تجاه العالم الآخر⁽³⁸⁾.

5. الفرد (Individuel): على الرغم من قلة درجة تأثيره بالنسبة للصراع داخل الفضاء السيبراني ، إلا إنه أضحي فاعلاً مهماً في الفضاء السيبراني ، حتى أنه له القدرة على إحداث الثورة الرقمية، وتصبح تلك الثورة مجال استخدام للدولة نفسها ، ومثال ذلك ما قام به مارك زوكرباغ (Mark Zoukerberg) عام 2004 ، حين أسس شبكة (فيسبوك) لتستقطب أكثر من نحو مليار مستخدم عبر العالم⁽³⁹⁾.

2- طبيعة الصراع داخل الفضاء السيبراني

اختصر الفضاء السيبراني حاجر الزمان والمكان ، وخلق مساحات للتفاعلات الإقليمية والدولية، ومن ثم، برزت فضاءات جديدة للصراع ، وبأدوات جديدة ايضاً تختلف عن تلك التي كان يستخدمها الفاعلين في إدارة صراعاتهم . وتعود اسباب اهتمام الفاعلين، سواء أكانوا من الدول أو غير الدول بهذا الفضاء الجديد للاعتبارات الآتية⁽⁴⁰⁾:

- ساحة صراع افتراضية : فيما أنه ليس مساحة جغرافية ، لذلك يتخطى الفضاء السيبراني العديد من الثنائيات التي تظهر في الصراعات التقليدية ، حيث يشارك

في الصراع داخل هذا الفضاء المدنيون والعسكريون، وترتبط صراعاتهم بالتطورات المادية، والسياسية، والاقتصادية، والعسكرية، على الفضاء المادي التقليدي، فضلاً عن انها اقل تكلفة وأكثر تحديداً للأهداف مقارنة بنظيرتها التقليدية .

- زيادة الاعتماد الإلكتروني : إذ باتت الكثير من الدول يربط بيتها التحتية بالفضاء الإلكتروني، خاصة شبكات المياه، والكهرباء، والبنوك، والبورصة، والاتصالات، وغيرها، فضلاً عن انظمة السيطرة والتحكم، لذلك أضحت استهداف وحماية تلك البنى التحتية إلكترونياً احد عوامل الصراع والقوة للدولة.
- اضمحلال حدود الدداخل والخارج : أي اصحب هناك حالة من التأثير الشبكي المتزايد بين الدولة وخارجها، حيث اتسع استخدام الأفراد، والجماعات، والدول للتكنولوجيا الحديثة المرتبطة بالفضاء السيبراني، سواء أكانت مواقع تواصل اجتماعي (انترنت)، أم هواتف ذكية، بما يجعل الخدمات والمعلومات متاحة للجميع .

- صعوبة الردع الإلكتروني وغياب الشفافية : إذ يصعب على الدول وضع حدود لسيادتها داخل الفضاء السيبراني، كما يصعب على الجهة المستهدفة تحديد الطرف المهاجم .

كل هذه المزايا وأكثر دفعت الدول والفاعلين من غير الدول إلى تعظيم نشاطهم داخل هذا الفضاء السيبراني من أجل السيطرة عليه والتحكم به . وللصراع السيبراني (**Cyber conflict**) تعاريف عدة ، إذ يعرف في احدهن : (إن الفاعلين سواء أكانوا دول أم غير الدول، تستخدم قدرات الفضاء الإلكتروني من أجل تحقيق أهدافها المتعارضة، سواء داخل أو عبر البنية السيبرانية). إلا إن هذا المعنى يتضمن تعقيدات كبيرة بسبب أننا أمام ظاهرة صراعية هجين أو مختلطة، تتداخل بها الحسابات الإنسانية والتكنولوجية على حدٍ سواء ، وتشابك فيها طبيعة، واهداف، وهويات الفاعلين⁽⁴¹⁾.

وتبعاً لذلك ، يصعب فهم طبيعة الصراع داخل الفضاء السيبراني دون إيلاء أهمية لمستويين اساسيين في تفاعلاته؛ أولهما-ينصرف على أنه نزاع تجري وقائعه بالأساس

داخل البيئة الرقمية، ومن خلال أدواتها، حيث تسعى الاطراف المتنازعة لفرض هيمنتها المعلوماتية، وذلك عبر الإقدام على اختراق، أو تدمير، أو تعديل، أو تجسس على المعلومات المخزنة في أحد أجهزة الحاسوب أو الاتصال المرتبطة بالفضاء الإلكتروني، فيما يسمى (الهجمات الإلكترونية) . وثانيهما- يتعلق بأنه نزاع إلكتروني مرتبط أساساً بتفاعلات الواقع، خاصة أن الفضاء السيبراني يظل في النهاية منتجاً من مصنع الإنسان، ومن ثم، قد يستخدم هذا الفضاء لكي تحقق الاطراف اهدافها على الأرض⁽⁴²⁾.

وعلى الرغم من اختلاف الصراع السيبراني عن الصراع التقليدي، بالأخص العسكري، التي تُعد حكرًا على الدول والجماعات المسلحة، وهي صراعات تدور في بيئة جغرافية معينة، وتستمر لمدة زمنية معينة، إلا أن هذه الصراعات التقليدية قد دخلت فيها أدوات تكنولوجية سيبرانية، فمجرد نشوب صراع تقليدي بين الدول، تصبح قطاعات الاتصالات، والمعلومات، والبنى التحتية، والمعلوماتية ضمن اهداف الدول، ومن ثم، باتت هناك اسلحة ذات طابع إلكتروني ضمن الحروب، مثل وسائل التواصل الاجتماعي، والاقمار الصناعية، واسلحة تكنولوجيا النانو، والطائرات دون طيار، والاسلحة الروبوتية⁽⁴³⁾.

ويوفر الفضاء السيبراني للفاعلين ليس من الدول فحسب، بل كذلك الفاعلين من غير الدول ، هامشاً كبيراً من المناورة ، وتحقيق الاهداف ، دون اللجوء إلى الاعمال العسكرية، لذلك يُعد بعض العلماء السياسيين والاستراتيجيين، إن الصراع داخل الفضاء السيبراني هو نموذج للحرب غير المتكافئة، باعتبارها توفر القدرة لصغار الفاعلين على ممارسة القوتين الصلبة والناعمة أكثر من أي فضاء آخر⁽⁴⁴⁾.

ونستخلص من ذلك، إن الصراع داخل الفضاء السيبراني (الإلكتروني) بين الفاعلين، يستمد دوافعه من المصالح والأهداف الواقعية، أي الموجودة أصلاً على الفضاء العام التقليدي، ليس هذا فحسب، بل أن الصراعات بين الدول والجماعات المسلحة داخل الفضاء التقليدي تتطلب استخدام الوسائل والأدوات الإلكترونية ذاتها في إدارة

صراعاتها وتنافسهم، خاصة بعدما اصبحت ميزة القرن الحادي والعشرين هو عصر الإنترنت .

رابعاً- تداعيات الحروب السيبراني على الأمن والسلم الدوليين

أدى التطور التكنولوجي، كانتشار الإنترنت والحواسيب، والأجهزة النقالة، وتوافر الحزمة العريضة للإنترنت عبر الأجهزة النقالة وتدني كلفتها، إلى ارتفاع أعداد مستخدمي الإنترنت وتزايد اعتماد الدول على هذه التكنولوجيات في التنمية الاقتصادية والاجتماعية . إلا أن الانفتاح الذي يميز شبكة الإنترنت، والفضاء السيبراني عموماً، جعلها عرضة للتعديات والأنشطة الغير سلمية، فصار مستخدمو الفضاء السيبراني من الدول وغير الدول عرضة للانتهاكات والتهديد لمنظومتها الإلكترونية، إذ لا يمكن لأي حكومة ، أو إدارة، سواء أكانت من العالم الثالث، أم في الدول الاكثر تقدماً، أن تنأى بنفسها عن الهم الذي يمثل اختراق الشبكات، وتهديد أمنها ومصالحتها.

ولعب الفضاء السيبراني (الإلكتروني)، ومنذ ظهوره، دوراً أساسياً في تعظيم القوة أو الاستحواذ على عناصرها الاساسية في العلاقات الدولية، حيث أصبح التفوق في ذلك المجال عنصراً حيوياً في تنفيذ عمليات ذات فاعلية على الأرض، والبحر، والجو، والفضاء، واعتماد القدرة والتفوق في الفضاء الإلكتروني على نظم التحكم والسيطرة التكنولوجية . أدى ذلك إلى تغيير ليس في مفهوم الأمن القومي للدولة فحسب، بل لمفهوم القوة الوطنية للدولة ايضاً، إذ بات بالإمكان تعريفها على أنها (مجموعة الوسائل، والطاقات، والإمكانات، المادية وغير المادية، المنظورة وغير المنظورة التي تمتلكها الدولة، ويستخدمها صانع القرار في فعل مؤثر يحقق مصالح الدولة، وتؤثر في سلوك الوحدات السياسية الأخرى)⁽⁴⁵⁾.

ينظر ذوي الاختصاص إلى الحرب الإلكترونية على أنها حرب العصر الحقيقية، مسارها الرئيس الشبكات الرقمية والإلكترونية، كذلك الوسائل التكنولوجية الأخرى، والأدوات الإعلامية، وكل ما يتعلق بعالم المعلوماتية والحدثات، والغاية الرئيسية لهذه الحرب هي

الأضرار النفسية والمعنوية بالدرجة الأولى، ثم تتبعها الأضرار المادية، وهي حرب ناعمة، صامتة، مظلمة، بعيدة عن الوسائل الحربية الخشنة، لكنها لا تمانع في امتطاء الترسانات المسلحة والعسكرية الضخمة⁽⁴⁶⁾. باعتبار أن الغاية الرئيسة والنواة الأولى من ابتكار الأقمار الصناعية، والفضاء الإلكتروني كانت عسكرية بامتياز كما تم ذكره آنفاً.

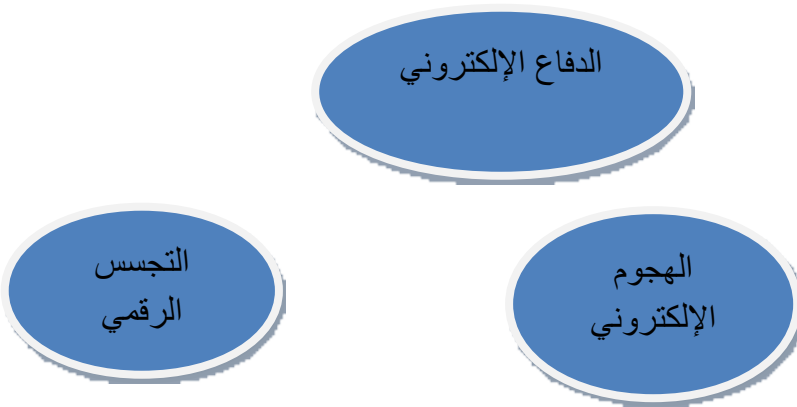
ويعتبر آخرون أن الحرب الإلكترونية هي امتداداً للحروب التقليدية والمادية، بحيث يتألف جندها من المدنيين والعسكريين في آنٍ واحدٍ . كما أنها حرب أدمغة بالدرجة الأولى، كونها تستهدف في المقام الأول تدمير البنية العلمية والمعلوماتية للهدف، وتأخذ أشكالاً عدة؛ كشكل الاتصالات بين الجيوش وقياداتها، وإضعاف شبكات النقل والإمدادات اللوجستية، وضرب المعلومات الاقتصادية، وإحراج الساسة، والعبث بالمحتوى التقني والرقمي وغيرها⁽⁴⁷⁾.

إذن، الحرب السيبرانية هي حرب تتخذ من الفضاء الإلكتروني ساحة وميدان لتفاعلاتها وقضاياها ومصالحها، وتستمد هذه القضايا والمصالح من الفضاء العام التقليدي . وعلى وفق ذلك، ومنذ اجتياح الإنترنت العالم، وما تبعه من مخلفات واسعة، أصبح هاجساً للدول الكبرى، وهذا يعزى لارتباطه بمستقبل الاستقرار العالمي، إذ صار له رده فعل خطيرة على النظام العالمي، لذلك يشهد العالم الآن تسابق في فهم التحركات الأساسية للنظام الإلكتروني والآثار المترتبة منه⁽⁴⁸⁾. وعليه، بدأت الولايات المتحدة، وروسيا، والصين، وإيران، وغيرها من الدول المتطورة بتشكيل خلايا غير معلنة ضمن تشكيلاتها العسكرية والأمنية مهمتها القيام بهجوم أو صد هجوم إلكتروني على بنيتها التحتية، وموازة أي حرب حقيقية قد تقع عبر توظيف المعلومات والاتصالات في تدمير البنية الاقتصادية للدولة أو سرقة معلومات مخبرية⁽⁴⁹⁾.

وعند التمهيد في ما يشهده النظام العالمي بشكل عام، والأمن والسلم الدوليين بشكل خاص، لتوضح وبشكل جلي، أن العالم منقسم إلى كتلتين كبيرتين في إطار التحالفات الاستراتيجية؛ الأول - بقيادة الولايات المتحدة وبريطانيا واسرائيل، والثاني - بقيادة روسيا والصين وإيران، هذا الوضع هو أشبه بالوضع الذي سبق الحرب العالمية

الأولى والثانية، والتي كان الفضاء العام التقليدي ميدانها الرئيس، لكن هذه المرة ويفعل العصرية سيكون الميدان الرئيس هو الفضاء السيبراني (الإلكتروني) . ويمكن تقسيم الحرب الإلكترونية إلى ثلاث مجالات؛ أولهما-الدفاع الإلكتروني، الذي يعني بالدفاع عن أنظمة وأجهزة ومعلومات الدولة والجيش والمجتمع، وثانيهما-الهجوم الإلكتروني، وهو المجال المختص بالعمليات الإلكترونية، والتي تهدف للتشويش على مصادر المعلومات وتدميرها وحرمان العدو من استخدامها لمصلحتهم، وأخيراً- التجسس الرقمي على امكانيات وقدرات الفاعلين الآخرين⁽⁵⁰⁾.

مجالات الحرب الإلكترونية



وعليه، فقد أصبح الفضاء الإلكتروني ساحة جديدة للصراع بشكله التقليدي ولكنه ذو طابع إلكتروني يعكس النزاعات التي تخوضها الدول أو الفاعلين من غير الدول على خلفيات دينية أو عرقية أو إيديولوجية أو اقتصادية أو سياسية، ويتمدد الصراع الإلكتروني بداخل شبكات الاتصال والمعلومات متجاوزا الحدود التقليدية وسيادة الدول، ويؤثر ذلك في امتداد مجاله وتداعياته أو آثاره، ويخلق حالة من عدم الثقة بين الدول⁽⁵¹⁾.

ونظراً لارتباط الشبكات المحلية للدول بالشبكات العالمية للإنترنت⁽⁵²⁾. وبما أن هناك ضعف وثغرة في انظمة التشغيل الإلكترونية، يصبح احتمال انتقال الصراعات إلى حروب سيبرانية بين الدول قائماً⁽⁵³⁾. وخير دليل على ذلك، هي الاختراقات الإلكترونية المتبادلة بين الدول والفاعلين الدوليين في الآونة الأخيرة. ينظر الجدول⁽⁵⁴⁾

جدول: أمثلة على الصراعات السيبرانية

السنة	اسم الهجوم السيبراني
منذ عام 2003م	نشوء جماعات دولية للقرصنة مثل «ويكيليكس وأنونيموس» (تمثل مواقف سياسية، وحقوقية)
1999م	هجمات حلف الناتو الإلكترونية على يوغوسلافيا واستهدفت تعطيل شبكات الاتصالات
2006م	الحرب الإلكترونية بين حزب الله وإسرائيل
2007م	الأزمات الدولية، مثل التوتر بين استونيا وروسيا
2008م	الأزمة الإلكترونية بين روسيا وجورجيا
2010م	هجمات إسرائيل (فيروس ستاكسنت) بالتعاون مع أمريكا، ضد المنشآت النووية الإيرانية
2008م - 2012م	المواجهات الإلكترونية بين حماس وإسرائيل
2012م - 2017م	هجمات فايروس «شمعون» على المملكة (مهاجمة أجهزة كمبيوتر شركة أرامكو وبعض الجهات الحكومية ومنشآت حيوية)
2014م - 2015م	هجمات فيروس «دوكو» على شبكة فنادق استضافت محادثات تتعلق بالملف النووي الإيراني
2016م	اتهام روسيا بالقرصنة الإلكترونية في الانتخابات الأمريكية الأخيرة لدعم المرشح الجمهوري دونالد ترامب
منذ عام 2007 الى يومنا هذا	الاختراقات المتبادلة بين الصين والولايات المتحدة وروسيا، أو ما بين طهران وواشنطن في عام 2010م
2016م	اتهام روسيا بشن هجمات إلكترونية على النرويج، والتشيك، وبريطانيا
2017م	هجوم فيروس «WannaCrypt أوWannacrypt 2.0» (تضرر 230 ألف جهاز إلكتروني في 99)

فضلاً عن ذلك، الاختراق الذي اصاب شركة (SONY) الامريكية عام 2014، وكان الهدف من ذلك منع إطلاق فيلم "The Interview" من إنتاج الشركة، وهو فيلم كوميدي يدور حول مؤامرة لاغتيال الزعيم الكوري الشمالي (كيم جونج أون)، إذ اتهمت بذلك كوريا الشمالية⁽⁵⁵⁾. كذلك الاتهام الموجه إلى الصين، الذي مفاده هجوم صيني الإلكتروني على مؤسسات الدول الاقتصادية، وبخاصة الامريكية، وسرقة الاسرار التجارية وتوظيفها لصالح صناعاتها الخاصة، مما احدث نوع من الحساسية الدولية⁽⁵⁶⁾. ايضاً ما حصل لقطر من هجوم سيبراني، حيث شنت الدول الرباعية (السعودية والإمارات والبحرين ومصر) في بداية حصارها لقطر هجوماً سيبرانياً لفقت به خطاباً مفبركاً لأمير البلاد، الشيخ (تميم بن حمد آل ثاني)، استعملته تبريراً لإجراءاتها العدائية⁽⁵⁷⁾.

ونظراً، للإضرار الخطيرة التي قد تسببها الحرب الإلكترونية على كل من الامن القومي، والعسكري، والاقتصادي، والاجتماعي، ويهدد البيئة التحتية والحرية للدول، وأسواق المال والقطاعات المصرفية، والسلم الدولي، والمنشآت النووية، والمؤسسات الصحية، وقطاعات النقل بكل انواعه (البري والبحري والجوي)، ورفاه الشعوب⁽⁵⁸⁾. وغياب الاطارين التشريعي والتنظيمي الحاكم للفضاء السيبراني⁽⁵⁹⁾. اتجهت معظم الدول المتقدمة، الى اقرار سياسات وقائية ودفاعية، ضد الهجمات السيبرانية، وخصصت الدول الكبرى، مثل الولايات المتحدة الاميركية، واستراليا، والمملكة المتحدة، واسرائيل مبالغ طائلة، لإنشاء هيئات وأقسام تهتم بذلك، ومعالجة مسائل الامن السيبراني، واستقرار الفضاء السيبراني⁽⁶⁰⁾،⁽⁶¹⁾. وليست هذه الحقيقة، سوى مؤشر، الى

مدى الاهتمام الذي توليه هذه الدول، لارساء الثقة والاستقرار، كما السلامة والأمن في هذا الفضاء . فاقصاد العالم، كما حياتنا اليومية، متصلان اتصالاً وثيقاً بالفضاء السيبراني، والخدمات الحيوية، كما الامن، والدفاع، والعلاقات الدولية، مهددة في كل لحظة، نتيجة الاختراقات، والاعتداءات على الشبكة العالمية للمعلومات، وعلى الانظمة المعلوماتية، وقواعد المعلومات، ولم تتأخر الادارة الاميركية، عن استحداث قيادة عسكرية جديدة، مختصة بأمن الفضاء السيبراني⁽⁶²⁾. وتتولى مروحة من النشاطات العسكرية، تشمل الى الحماية، والقيام بمناورات سيبرانية، سواء لتحديد مدى فاعلية الحماية، أو مدى القدرة على الرد، أو للتعرف الى مكان الضعف، والتدريب على آليات الرد، ويتم ذلك، في اطار استراتيجية اعدتها وزارة الدفاع في العام 2011 حول كيفية العمل في الفضاء السيبراني⁽⁶³⁾.

وعليه، فقد انتقل الاهتمام الذي كان مخصصاً للتجهيزات والتطويرات العسكرية التقليدية للدول، الى الاهتمام لإيجاد الوسائل الملائمة لطبيعة الخطر السيبراني، والكفيلة بتداركه وردعه⁽⁶⁴⁾. هذا الامر ينذر بسباق للتسلح، وعسكرة الفضاء السيبراني، مما سيكون له الأثر في زعزعة الأمن والسلم الدوليين في المستقبل المنظور⁽⁶⁵⁾.

الخاتمة

عند الرجوع إلى قواعد العلاقات الدولية، نجد مبدأ (الامتناع عن استخدام القوة)، خاصة في ظل امتلاك الدول العظمى ترسانات نووية، وانطلاقاً من قاعدة الرد والرد المضاد، والتشريعات والأحكام الدولية التي نص عليها ميثاق الأمم المتحدة، حفظ السلم والأمن الدوليين، على مدى أكثر من نصف قرن . لكن ومع التطورات السريعة التي شهدتها العالم، وبروز الفضاء الإلكتروني كساحة للتفاعلات الدولية، سرعان ما كشف استخدامه عن حالة التعارض الحقيقي أو المتخيل للاحتياجات والقيم والمصالح بين العديد من الفرقاء الدوليين، وبما ساعد على بلورة أساليب للصراع الدولي ذات الطابع التقني والتجاري والاقتصادي والعسكري، إلى جانب ظهور طرق

بديلة عن الحرب المباشرة بين الدول أو بين الخصوم عبر شبكات الاتصال والمعلومات، إذ أصبحت عملية التجسس والمراقبة السيبرانية من قبل الدول، إلى ممارسات يومية تقوم بها اغلب الدول على الشبكة العالمية للمعلومات، وذلك نتيجة فشل التعاون بين البلدان المختلفة، لذلك يبقى احتمال اندلاع حروب كنتيجة لها قائماً . ومما تقدم يمكن أن نخلص بعض الاستنتاجات، وهي كالآتي :

1. تعني الحروب السيبرانية بأنها: (الحروب التي تتم بالتعاون مع الحرب العسكرية، إذ أنها تصوب نيرانها نحو الأهداف الإلكترونية والرقمية والمعلوماتية، كالتجسس على الإشارات الصادرة من الأجهزة الحاسوبية التابعة للفتات المستهدفة، وتتبع الموجات المنطلقة من الهواتف النقالة وغيرها). وبالتالي، تستهدف هذه النيران الإلكترونية المصالح القومية والسياسية والعسكرية والأمنية للفئة المستهدفة، متخذةً لأجل ذلك شكل الهجمات الإلكترونية، أو الاختراقات الإلكترونية الهادفة لتعطيل البنية المعلوماتية لها .
2. تكمن أهمية هذا النوع من الحروب، في أن المواطن الحديث أصبح أكثر اعتماداً على البرامج الإلكترونية، وبدلاً من أن تتحكم الدولة بآراء مواطنيها أصبح العكس من ذلك، فقد أصبح المواطن العادي بكل بساطة يمتلك مجموعة كبيرة ومتنوعة من الخيارات الإعلامية، فهو قادر على سماع وجهات النظر الأخرى بكل سهولة من مصادر مختلفة وعبر قنوات تكنولوجية متنوعة. لذلك تسابقت الدول نحو السيطرة على الإعلام الرقمي، ورصدت ميزانيات ضخمة لتصدير افكارها عبر الفضاء الرقمي .
3. ان تكنولوجيا المعلومات والاتصالات، تتيح امكانات هائلة، وغير مسبوقة، لإنتاجية افضل في جميع القطاعات، وللتواصل عبر القارات. إلا إن البنية التحتية لهذه التقنيات، تمثل ارتباطاً بين مصالح متعددة، وخدمات مختلفة، وبلدان عديدة، الامر الذي جعل من الاخطار في الفضاء السيبراني، اخطاراً عالمية .

4. نظراً لارتباط العالم المتزايد بالفضاء الإلكتروني، وعدم وجود تشريعات قانونية تنظم وتحكم الفضاء السيبراني، فضلاً عن وجود سباق بين الدول للسيطرة والتحكم بالنظام العالمي، يصبح احتمال الحرب السيبرانية وارد بقوة.

توصيات

وأخيراً يمكن تقديم بعض التوصيات التي من شأنها الحد من المخاطر والتهديدات التي تكتنف الفضاء السيبراني، والتي ستعزز في حفظ حالة الأمن والسلم الدوليين . وهي كالآتي :

- إعادة النظر في مفهوم الأمن القومي، إذ ينبغي أن يأخذ بنظر الاعتبار التطورات السريعة التي يشهدها العالم، خاصة في مجال الاتصالات والمعلومات .
- ينبغي على الأمم المتحدة تشريع قوانين حاکمة للفضاء السيبراني، وإيجاد طريقة مناسبة لتطبيقها، عن طريق الاستعانة بخبراء في هذا التخصص .
- على الدول، خاصة العظمى والكبرى ، ان تستغل التطور التكنولوجي في مجال الاتصالات، والثورة المعلوماتية، بما يخدم رفاه الدول بصورة عامة، والإنسان بصورة خاصة، بدل من تسخيرها في الصراعات والحروب .
- إذا تعذر على المجتمع الدولي تطبيق التوصيات السابقة، فقد يكون الحل في وضع البلقنة الإلكترونية؛ أي بناء حدود سيادية داخل الفضاء السيبراني، عبر انشاء شبكات صغيرة وليس شبكة دولية واحدة للمعلومات (الإنترنت) كما هو الآن، تتبع هذه الشبكات الفاعلين المختلفين، مثلها كمثل وضع الشبكات الهاتفية، وفي وضع كهذا تصبح عملية الاختراقات الإلكترونية اصعب، ومن ثم اضمحلال الصراعات والحروب السيبرانية .

الهوامش

(1) عبدالله صادق دحلان، الأمن السيبراني علم ينبغي أن يدرس، تقرير عبر قناة العربية، 2018 . متوفر على الرابط :

<https://www.alarabiya.net/ar/sauditoday/views/2018/08/05/%D8%A7%D9%84%D8%A3%D9%85%D9%86%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A%D8%B9%D9%84%D9%85-%D9%8A>

%D9%86%D8%A8%D8%BA%D9%8A-%D8%A3%D9%86-%D9%8A%D8%AF
%D8%B1%D9%91%D8%B3.html.

(2) حمزة غشوة ومعمّر حمزة، دور المواقع الإلكترونية في الترويج السياحي، رسالة ماجستير (غير منشورة)،

(جمهورية الجزائر، جامعة قاصدي مرباح-ورقلة، كلية العلوم الانسانية والعلوم الاجتماعية، 2015)، ص 17 .

(3) ماهر عودة الشمايلة وآخرون، الإعلام الرقمي الجديد، ط 1، (الأردن : دار الاعصار العالمي للنشر والتوزيع،

2015)، ص 39 .

(4) محمد سيد ريان، الإعلام الجديد، ط 1، (القاهرة : مركز الاهرام للنشر والترجمة والتوزيع ، 2012)، ص 7 .

(5) ماهر عودة الشمايلة وآخرون، المصدر السابق، ص 46 - 47 .

(6) Rex Hughes, Towards a Global Regime for Cyber Warfare, (Cyber Security Project, Chatham House, London, 2009),p.3 .

(7) للمزيد ينظر : مختار علي حيدر ، نشأة الحرب الإلكترونية وتطورها ، (مقال منشور على موقع منتدى

التكنولوجيا العسكرية والفضاء، تاريخ الوصول ١٩/٢/٢٠١٩). على الرابط :

<https://army-tech.net/forum/index.php?threads>

(8) Alfred Price, The History of US Electronic Warfare. 1st ed.(Arlington, VA: Association of Old Crows, 1984),p.6.

(9) Ali Can Kucukozyigit, leestronic warfare (EW) historilcil perspectives and its relationship to information operations (IO)—considerations for turkey, thesis Introduced to: naval posgraduate school , calivornia , September 2006,p . 47.

(10) H.Banks, R. Mc Quillan, Electronic Warfare Test and Evaluation, Flight Test Techniques Series, researh and tachtology organization- north atlntic treaty organization,Canada,2000,p.2

(11) مصطفى طلس وآخرون ، الإستراتيجية السياسية العسكرية ، ط 2، (دار طلس للدراسات - والترجمة والنشر ،

دمشق : 2119)، ص 289 - 282 .

(12) للمزيد ينظر : بيتر سينجر ، الحرب عن بعد : دور التكنولوجيا في الحرب ، (مركز الإمارات للدراسات والبحوث

الإستراتيجية ، ابو

ظبي : 2010)، ص 555 وما بعدها .

(13) قادي إسماعيل، إدارة الحروب النفسية في الفضاء الإلكتروني: الإستراتيجية الأمريكية الجديدة في الشرق الأوسط،

(ندوة دولية بعنوان : عولمة الإعلام السياسي وتحديات الأمن القومي للدول النامية، الجزائر: 2017)، ص 1. متوفر

على الرابط : <https://manifest.univ-ouargla>

(14) للمزيد ينظر : علي عبد الرحيم العبودي، الانسحاب البريطاني من الاتحاد الأوروبي : الابعاد السياسية والاقتصادية،

(دار الدكتور للعلوم الادارية والاقتصادية، بغداد : 2019)، ص 54 .63

(15) المصدر السابق نفسه، ص 54 .63

(16) ريتشارد كلارك وروبرت نيك، حرب الفضاء الإلكتروني : التهديد التالي للأمن القومي وكيفية التعامل معه، ط ١، (مركز

الإمارات للبحوث والدراسات الإستراتيجية، الإمارات العربية المتحدة: 2012)، ص 53 .

(17) Andrew Lohn, Cyber Warfare, (Objective analysis. Effective solutions (RAND), 1 Nov 2018) . look at : <https://www.rand.org/topics/cyber-warfare.html>

(18) عادل عبد الصادق، القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، (السياسة الدولية ، مركز

الاهرام للدراسات السياسية والاستراتيجية، العدد 188، مصر : 2012)، ص 33 .

(19) ريتشارد كلارك وروبرت نيك، مصدر سبق ذكره، ص 98 .

- (20) قاديرو إسماعيل، مصدر سابق، ص 4 .
- (21) يورجين هابرماس : فيلسوف وعالم اجتماع ألماني معاصر يعتبر من أهم علماء الاجتماع والسياسة في عالمنا المعاصر. ولد في دوسلدورف، ألمانيا وما زال يعيش بألمانيا. يعد من أهم منظري مدرسة فرانكفورت النقدية له ازيد من خمسين مؤلفا يتحدث عن مواضيع عديدة في الفلسفة وعلم الاجتماع وهو صاحب نظرية الفعل التواصلي.
- (22) look : Jurgen Habermas, Between Facts and Norms, (Contributions to a Discourse Theory of Law and Democracy, The MIT Press, Cambridge, Massachusetts , Second printing, 1996) . Available on : <http://blogs.unpad.ac.id/.../J%25C3%25BCrgen-Habermas-Between-Facts-and-Norms.pdf>
- (23) ابتسام علي حسين، فرص وقيود الاطراف المتنازعة على المجال العام السيبراني، (مجلة السياسة الدولية، ملحق اتجاهات نظرية، العدد 208، مصر: 2017)، ص 11 .
- (24) ينظر : ابتسام علي حسين، المصدر السابق، ص 11-12 . كذلك علي محمد رحومة، علم الاجتماع الآلي: مقارنة في علم الاجتماع العربي الاتصال عبر الحاسوب، (سلسلة عالم المعرفة، العدد 347، لسنة 2008) .
- (25) Michael Chertoff, The Cyber Domain And The Evolution of Smart Power, (Symposium Three, :Employing Smart Power, Co-Sponsored by U.S Naval Institute, March 24,2009),p.25 . look at : https://www.asymmetrichreat.net/pdf/symposium3_report.pdf
- (26) اشرف السعيد احمد ، القرصنة الإلكترونية ، (دار النهضة العربية ، القاهرة ، 2013) ، ص 45-47 .
- (27) نورة شلوش، القرصنة الالكترونية في الفضاء السيبراني "التهديد المتصاعد لأمن الدول، (مجلة مركز بابل للدراسات الانسانية، المجلد 8، العدد 2، 2018)، ص 195 .
- (28) احمد زكي عثمان، تأثيرات القدرات السيبرانية في الصراعات الإقليمية، (مجلة السياسة الدولية، ملحق اتجاهات نظرية، العدد 208، المجلد 52، مصر : 2017)، ص 17 .
- (29) ابتسام علي حسين، مصدر سابق، ص 11 .
- (30) احمد زكي عثمان، مصدر سابق، ص 19 .
- (31) المصدر نفسه، ص 17 .
- (32) احمد عبد العزيز واخرون، الشركات متعددة الجنسية واثرها على الدول النامية، (مجلة الادارة والاقتصاد، العدد 85، لسنة 2010)، ص 113 .
- (33) سماح عبد الصبور، الصراع السيبراني... طبيعة المفهوم وملامح الفاعلين، (مجلة السياسة الدولية، ملحق اتجاهات نظرية، العدد 208، مصر : 2017)، ص 8 .
- (34) Philip Seib and Dana M. Janbek, Global Terrorism and New Media: The Post-Al Qaeda Generation, (New York: Routledge, 2011), p. 44 .
- (35) بن مرزوق عنتر وحرشاي محي الدين، الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية، (بحث متوفر على شبكة المعلومات الدولية، الجزائر: 2016)، ص 68 . متوفر على الرابط : <https://manifest.univ-ouargla>
- (36) المصدر نفسه، ص 68 .
- (37) سماح عبد الصبور، مصدر سابق، ص 8 .
- (38) لجنة الجيوسي، سلطة التكنولوجيا وتكنولوجيا السلطة، المركز العربي للأبحاث ودراسة السياسات (معهد الدوحة)، حزينان/ يونيو 2011. ينظر الرابط : <http://www.dohainstitute.org/release/7e261629-2aab-46cd-83bd-046c9ca1a7e4>

(39) قادير إسماعيل ، إدارة الحروب النفسية في الفضاء الإلكتروني: الإستراتيجية الأمريكية الجديدة في الشرق الأوسط، (ندوة بعنوان : عولمة الاعلام السياسي وتحديات الأمن القومي للدول النامية، الجزائر، 2017)، ص 5-6 . متوفر على

الرابط : <https://manifest.univ-ouargla>

(40) سماح عبد الصبور، مصدر سابق، ص 5-6 .

(41) خالد حنفي علي، إشكاليات تداخل الصراع السيبراني والتقليدي، (مجلة السياسة الدولية، ملحق اتجاهات نظرية، العدد 208، مصر: 2017)، ص 3.

(42) المصدر نفسه، ص 3-4 .

(43) سماح عبد الصبور، مصدر سابق، ص 6 .

(44) أحمد زكي عثمان، مصدر سابق، ص 19 .

(45) عادل عبد الصادق، أنماط الحرب السيبرانية وتداعياتها على الأمن العالمي، (مجلة السياسة الدولية، ملحق اتجاهات نظرية، العدد 208، مصر: 2017)، ص 33 .

(46) يحيى اليحياوي، حرب المعلومات ، بحث منشور على شبكة المعلومات الدولية، (موقع الكاتب يحيى اليحياوي،

تاريخ النشر 13/12/2010). وعلى الرابط : http://www.elyahyaoui.org/medias_war.htm

(47) عبد الجليل المرهون، عصر الردع الإلكتروني، تقرير منشور في موقع (قناة الجزيرة)، بتاريخ 26/10/2012. وعلى

الرابط : <https://www.aljazeera.net>

(48) بيتر وارن سينغر و آلن أ. فريدمان، الأمن الإلكتروني والحرب الإلكترونية، ترجمة : مجاهد فخرالدين قاسم أحمد،

(بحث تكميلي لبليل درجة الماجستير في الترجمة، جامعة السودان للعلوم والتكنولوجيا، كلية الدراسات العليا، ٢٠١٤)،

ص 9 .

(49) عباس بدران، الحرب الإلكترونية : الاشتباك في عالم المعلومات، (مركز دراسات الحكومة الإلكترونية، بيروت -

لبنان، 2010)، ص 4 .

(50) عباس بدران، المصدر السابق، ص 30 .

(51) نورة شلوش، مصدر سابق، ص 193 .

(52) جنان الخوري، مؤتمر الأمن السيبراني والدفاع السيبراني: تحديات وآفاق، (الجامعة اللبنانية والوكالة الجامعية

للفرنكوفونية - AUF، لبنان، ٢٠١٧)، ص 18 . للمزيد ينظر الرابط :

https://ul.edu.lb/files/news_20171023.pdf

(53) عباس بدران، مصدر سابق، ص 12-13 .

(54) عبد الله محمد العصيمي، «السيبرانية».. وأشكال الحروب في المستقبل، (جريدة الجزيرة - السعودية، العدد

١٦٥١٩، لسنة ٢٠١٧)، ص ٢ .

(55) إيهاب شوقي، الحرب السيبرانية... حرب المستقبل المفزعة، مقال على موقع (شبكة الاخبار العربية)، تاريخ النشر

19 فبراير، 2015 . متوفر على الرابط : <http://www.annetv.tv/new/showsubject.aspx?id=101954>

(56) سامانثا رافيش، الحرب السيبرانية وأميركا، (موقع اتجاهات البيان، تاريخ النشر ٢٤ أبريل ٢٠١٨) . للمزيد ينظر

الرابط : <https://www.albayan.ae/opinions/articles/2018-04-24-1.3246237>

(57) محمد الدوراني، قتال غير مرئي: الحرب السيبرانية في الأزمة الخليجية، (تقرير: مركز الجزيرة للدراسات، تاريخ النشر

13 مايو، 2018) . للمزيد ينظر الرابط :

<http://studies.aljazeera.net/ar/reports/2018/05/180513101447007.html>

(58) منى الأشقر جبور، الأمن السيبراني: التحديات ومستلزمات المواجهة، (اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، بيروت 27 - 28 أغسطس /آب 2012)، ص ٤ . للمزيد ينظر الرابط :

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

(59) منى الأشقر جبور، السيبرانية هاجس العصر، (المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، 2016)، ص 34 .

(60) Barry Jaber, Cyber Security M&A: Decoding deals in the global, (November 2011), p, 5 . look at : <https://www.pwc.com/gx/en/aerospace-defence/pdf/cyber-security-mergers-acquisitions.pdf>

(61) جيل برعام، تأثير تطور تكنولوجيا الحرب السيبرانية على بناء القوة في إسرائيل، (مؤسسة الدراسات الفلسطينية، فلسطين : ٢٠١٤)، ص 2 . للمزيد ينظر الرابط :

<https://www.palestine-studies.org/sites/default/files/uploads/files/cyberwarfare.pdf>

(62) منى الأشقر جبور، الأمن السيبراني: التحديات ومستلزمات المواجهة، مصدر سابق .

(63) See more: Strategy for Operating in Cyberspace, (US Department of Defense, July 2011). look at : <http://www.defense.gov/news/d20110714cyber.pdf>

(64) منى الأشقر جبور، السيبرانية هاجس العصر، مصدر سابق، ص 58 .

(65) عادل عبد الصديق، أنماط الحرب السيبرانية وتداعياتها على الأمن العالمي، مصدر سابق، ص 35 .