العناصر التقنية للتهديد الالكتروني

أ.م.د. بهاء عدنان السعبري
الباحث عماد عبد خضير الزرفي
كلية العلوم السياسية/ جامعة الكوفة

المقدمة:

لعبت الثورة التكنولوجية التي عرفها العالم في النصف الثاني من القرن العشرين، دورا كبيرا في تغيير العديد من المفاهيم التي كانت بمثابة مسلمات، وتم تعويضها بمفاهيم جديدة، ساهمت في تحليل ودراسة وحدات المجتمع الدولي، وحلّ الكثير من عقده. فدخل العالم مرحلة متقدمة ضمن آفاق عصر المعلومات، بغية الاستفادة من التقنيات المتوفرة في مجال المعلومات. والتي أصبحت معيارا يقاس به تقدُم المجتمعات وتطورها. إن العالم اليوم، غدا كقرية صغيرة، أوجبت تجاوز البعد الزماني والمكاني. فقامت الدول بتطوير الآليات التقنية والوسائل لمتابعة تنفيذ السياسات وتحقيق أعلى كفاءة ممكنة لأداء عملها الحكومي، وتهيئة المناخ لملائمة التطورات العالمية المتجددة. هذه التحديات فرضت على الحكومة الكلاسيكية، ضرورة مواكبة هذا التغير والتفكير في الانتقال إلى مرحلة الحكومة الإلكترونية. خاصة بعد انتقال كافة مكونات المجتمع المدني، الاقتصادي والإعلامي إلى الفضاء الإلكتروني. إن التكامل الإلكتروني يساعد على إدراك المصادر المهدَدة للأمن، وبالتالي سهولة تحديد الرئيسي منها والثانوي.

إن التطور التكنولوجي الهائل جعل المجتمع الدولي بمثابة قرية صغيرة تتشابك فيها العلاقات وتزداد حِدَةً يوما بعد يوم. هذا الترابط الشديد ازداد تعقيدا بسبب الشبكة الإلكترونية، فأصبحت التهديدات الأمنية ذات طابع جديد، استلزمت ضرورة توحيد الجهود لمواجهة هذه الأخطار. فعمِدت الدول إلى إنشاء أجهزة تشمل وسائل أكاديمية نظرية علمية، وأخرى عملية لحماية أمنها.

اشكالية البحث:

يعد الفضاء الالكتروني اليوم احد انماط التهديد التي تواجه النظام العالمي وقد ازداد استخدام هذا النوع من التهديدات بسبب التطورات التكنولوجية التي زادت من اعتماد الدول على ادارة شؤونها الاستراتيجية ومنها الامنية على التكنولوجيا، مما جعلها ساحة للصراع و الاختراق.

فرضية البحث:

تبرز فرضية البحث هنا من توظيف التكنولوجيا من قبل الدول في سياساتها ولذلك كلما زاد اعتماد الدول على التكنولوجيا وادارة شؤونها الامنية من خلال التكنولوجيا دون مستوى حماية ودفاع الكتروني متقدم كلما تعرض امن الدولة للتهديد ولأثبات صحة الفرضية يسعى البحث للإجابة على الاسئلة التالية:

١- كيف ارتبط الامن بالتكنولوجيا؟

٢- ما هو الامن الالكتروني؟

المبحث الاول: ارتباط الامن بالتكنولوجيا:

اصبح للتكنولوجيا الحديثة أثر في مفهوم القوة وتحولاتها، فظهر مفهوم القوة الإلكترونية Cyber Power ؛ حيث يعرفها جوزيف ناي بأنها (القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء الإلكتروني، أي أنها القدرة على استخدام الفضاء الالكتروني لخلق مزايا، والتأثير في الاحداث المتعلقة بالبيئات الواقعية الاخرى وذلك عبر أدوات إلكترونية) . ويعرفها دانيال كويل Daniel T. Kuehl بأنها (القدرة على استخدام الانترنت لخلق مزايا، والتأثير في الاحداث في البيئات التشغيلية كافة من خلال أدوات القوة) [١].

ويرى جوزيف ناي أن القوة الالكترونية مرتبطة بامتلاك المعرفة التكنولوجية، والقدرة على استخدامها، وهي تعني القدرة على استخدام الفضاء الإلكتروني فيخلق مميزات والتأثير في الاحداث التي تجري عبر البيئات

التشغيلية EnvironmentsOperational، وعبر أشكال وأدوات القوة المختلفة، سواء كانت عسكرية أو اقتصادية أو دبلوماسية أو معلوماتية [٢].

وقد حدد ناي ثلاثة أنواع من الفاعلين الذين يمتلكون القوة الإلكترونية يتمثل النوع الاول في الدولة، والنوع الثاني في الفاعلين من غير الدول، والنوع الثالث يتمثل في الافراد .وقد حدد ناي أنماطًا لاستخدام موارد القوة الافتراضية، وميز بين الاستخدام الناعم لها والاستخدام الصلب ويجادل جوزيف ناي بأن مفهوم القوة الإلكترونية يشير إلى (مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الالكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه الوسائل) [٣].

وتتعدد أدوات ممارسة القوة في العلاقات الدولية وفقًا لقدرات وإمكانيات ورغبات القوى المشاركة فيه، فقد تكون القوة العسكرية هي إحدى أهم هذه الأدوات. وقد تكون القوة الاقتصادية والحصار الاقتصادي والمالي هو العامل الرئيسي للسيطرة على الخصم وممارسة القوة عليه، وقد تكون الاداة المعلوماتية من خلال وسائل الاتصال والتكنولوجيا الحديث والانترنت هي العامل الرئيسي لحسم صراع بين دولتين. إلا أن ممارسة القوة والنفوذ قد تطورت بشكل هائل نتيجة للتطور الكبير في المعلومات؛ مما جعل هذهِ المعلومات هي الهدف الأساسي الذي تسعى الدول للحصول عليه .هذه المعلومة هي التي مكنت الدول من إنتاج السلاح النووي، وظل هذا التطور مستمرًا؛ حيث اعتمدت كل مرحلة من مراحل التطور الإنساني على سلطة أو قوة من طبيعة معينة تتناسب مع متطلبات هذه المرحلة.

ولقد أثرت هذه السلطة أو القوة بصورة مباشرة أو غير مباشرة في أدوات الصراع بين المجتمعات وآلياتها، وأفرزت مفردات ومكونات تكاملت معًا لتنتج نظامًا دوليًا سيطرت مفاهيمه بعض الوقت أو كل الوقت . وفي هذا الإطار تميز عصرنا الحالي بظاهرة الثورة العلمية والتكنولوجية .ولقد أزاحت وحيّدت التكنولوجيا كثيرًا من عناصر القوة عن مواقعها التي تربعت عليها فترة طويلة .مما عرّض المفهوم التقليدي للقوة إلى

انتقادات. وأفصح عن محتوى جديد للقوة فلم يعد ما في يد الدولة من قدرات عسكرية أو ما تمتلكه من أموال وثروات، كافية لبلورة دورها كقوة مؤثرة وفاعلة [٤].

وتصاعد الاهتمام الدولي بالعلاقة بين الامن والتكنولوجيا على اثر بعدين هامين الاول يتعلق بالتقدم التكنولوجي والانتشار السريع لتكنولوجيا الاتصال والمعلومات عالميا ودخولها في كافة مجالات الحياه وفي عمل المرافق الحيوية من خلال تطبيقاتها المتعددة، والثاني يتعلق بإمكانية استخدام ذلك التقدم وما اتاحة من ادوات واليات جديدة كوسيلة وكوسيط لتهديد عمل المرافق الحيوية والبنية التحتية الكونية للمعلومات وذلك من جراء تخطيها للحدود السيادية للدول وبما جعلها بيئة خصبة للاستخدام غير السلمي من جانب كافة الفاعليين على تنوعاتهم المختلفة والذين تراوحوا ما بين استخدام الدول الى الفاعليين من غير الدول، وظهر ذلك في استخدم الفضاء الالكتروني كساحة للحرب الباردة والحرب النفسية وحرب الافكار او من خلال استخدامه لشن الحروب والارهاب بين الدول او استخدام الافراد او الجماعات الارهابية او القراصنة او الجريمة المنظمة وبشكل يؤثر في الطبيعة المدنية او السلمية للفضاء الالكتروني. فمع انتهاء الحرب الباردة وانتشار الموجة التكنولوجية التي اجتاحت العالم اتجه معها الصراع الدولي بالأساس نحو المغالبة والتنافس في ساحة الإنجازات الاقتصادية والنجاحات التجارية من فوز بتعاقدات وزيادة صادرات وانتزاع الفرص وصراع حول الأفكار والإبداع والذي أصبح يترجم في شكل منتجات تكسب أسواقا وتدر أموالاً، وسعت الأمم الظافرة بكل السبل للسطو على الأسرار الاقتصادية والتقنية والعلمية والتجارية للدول الأخرى. وجاء الانتشار الواسع لتكنولوجيا الاتصال والمعلومات بمعدلات غير مسبوقة عالميا ودخولها في عمل العديد من المرافق الحيوية متزامنا مع القابلية للتعرض للعديد من الأخطار غير التقليدية التي ترتبط بها على نحو أصبح يهدد الامن القومي للدول في ظل بيئة امنية متغيرة غلب عليها سرعه انتقال الأفكار والأموال والافراد بين دول العالم. بفعل الثورة التكنولوجية والتغير

في المجال الاقتصادي والاعتماد المتبادل بين دول العالم وضعف دور الدولة وبروز الفاعلين الدوليين من غير الدول[٥]. وساهمت تلك المتغيرات في بروز وعي كوني عالمي ممتد بما يحدث ودرجة عالية من التأثير والتأثر في ارجاء العالم المختلفة. وكان لذلك دور في إعادة التفكير في حركية وديناميكية الصراع والامن على نحو عكس المرحلة التاريخية التي يمر بها المجتمع العالمي.

وعلى قدر ما ساعدت العولمة في توليد الكثير من فرص التعاون والتقدم في مختلف أرجاء العالم فإنها عملت ايضا على خلق حالة من الانكشاف الأمني، وانتشار عوامل الخطر والاضطراب، مع زيادة حساسية الدول إزاء صدمات الأزمات العالمية. وأصبحت شبكة الإنترنت أحد معالم ذلك المجتمع وإحدى مؤسسات العولمة الهامة. مع القوة الاتصالية العالية والتي جعلت العالم كقرية صغيرة مع سرعة تدفق السلع ورؤوس الأموال والأفكار والبشر من مكان إلى آخر.

وبرز مجتمع المعلومات العالمي، والذي تميز بوجود اقتصاديات قائمة على إنتاج المعلومات وتوزيعها و مورد استراتيجي جديد في النمو الاقتصادي بدلا من الموارد الطبيعية، وتحول اقتصاد الدول إلى جزء من اقتصاد عالمي متكامل ومتشابك يغلب عليه طابع التخصص والتكتل. ورافق ذلك ظهور المخاطر البيئية والأزمات الاقتصادية الدولية والشبكات الإرهابية والجريمة المنظمة والهجرة غير الشرعية والفقر وغيرها من التهديدات متعدية الحدود ،واتسع نطاق العلاقات الدولية والاعتماد الدولي المتبادل، وتميزت البيئة الاستراتيجية التي يعمل بها النظام الدولي بوجود عدد من مسببات الصراع مثل دور الجماعات الإرهابية والتنظيمات المسلحة التي تقف ضد الدول وترفض النظام الدولي القائم، بالإضافة لوجود الدول التي يحكمها قيادات راديكالية وتسعى للحصول على الأسلحة غير التقليدية، وهناك دول لا تستطيع السيطرة على وضعها الداخلي وتملك مقدرات استراتيجية واخرى دول فاشلة تمثل بيئة خصبة لبروز تنظيمات مسلحة تسعي لتحقيق أهدافها بالقوة المسلحة، وهناك عنصر القوة المتزايدة لعدد من الدول، ويمكن أن

تتفاعل كل تلك المكونات السابقة نحو زيادة عوامل عدم اليقين المولد لحالة الصراع. وخاصة مع حالة من التفاوت داخل الدول وبين الدول وبعضها البعض، وتواجه العديد من الدول تحديات تتعلق بشرعيتها مع انحسار دورها في المجال الاقتصادي، وصعود قوة الأسواق المالية والشركات متعددة الجنسية بالتزامن مع زيادة طابعها الدولي بما ساعد على الحد من قوة الحكومات الوطنية لصالح الجماعات تحت القومية، والتي تتفاعل مع بعضها دولياً دون العبور على الدولة الرسمية بالضرورة، وأصبح هناك حد من قوة الدولة وسيطرتها على تدفق رؤوس الأموال أو فرض العقوبات أو تنظيم عمليات الإنتاج [٦]. وذلك بعد ما وفرت التكنولوجيا آليات وأدوات لتحسين الاتصالات وتسهيل عملية انتقال الأفراد والأموال والأسلحة والأفكار، وكان لكل تلك المتغيرات تداعيات على الأمن القومي للدول فرادي وعلى الامن الدولي ككل، وذلك من منطلق ان مفهوم الأمن القومي لم يعد متعلقاً فقط بذلك الكيان المادي الذي تعلق بحماية الموارد والسكان والحدود والحفاظ على عناصر قوة الدولة والمقدرات القومية لها، وارتبطت القوة العسكرية بالتحكم في أربعه مجالات تتشكل من القدرة على السيطرة على البر والبحر والجو والفضاء الخارجي، وكان الفكر الأمني مرتبطاً بمسالة الدفاع والهجوم عن طريق الجيوش التقليدية أو دعم الحلفاء وكان يتحقق ذلك الأمن عن طريق عده عناصر سياسية واقتصادية ودبلوماسية وتكنولوجية وعسكرية، وكانت تلك العناصر ذات علاقة ترابطية فيما بينهما حيث يدعم كل منهما الأخر، حيث يؤدي الضعف في أحدها الى ضعف العناصر الأخرى والعكس، وكانت الدول في السابق أكثر انعزالاً عن بعضها البعض، وكانت مسالة الدفاع عن حدودها القومية جزءا هاما من حماية عناصر قوتها القومية. وجاء الفضاء الالكتروني بخصائص وعناصر مميزة، وليكون له تأثير على الأمن والاقتصاد الدوليين [٧].

بل وأصبح المفهوم الجديد للأمن القومي يدور في فلك الحفاظ على سلامة الدولة في ظل تلك التطورات التكنولوجية ومن ثم اختلفت آليات التعامل معها. وأصبح الامن انعكاساً للمرحلة التاريخية التي يمر بها

وطبيعة الصراع الدولي في ظل الموجة المعلوماتية التي يشهدها العالم، وانعكس ذلك في تغير طبيعة الصراع والقوة وممارستها وفي إحداث تغييرات داخل البيئة الأمنية للنظام الدولي.

وأصبح الصراع الجديد يعنى بكل ما من شأنه التنافس والترابط التكنولوجي وارتباط شكله وانماطه في عصر المعلومات بمعرفة.. من يعرف؟ وأين؟ ولماذا؟ وكيف؟. وأخذت ظاهرة استخدام القوة في العلاقات الدولية تأخذ شكلاً جديداً في طبيعتها ووسائلها وأدواتها واتجه الصراع الدولي بالأساس نحو التنافس في ساحة الإنجازات الاقتصادية والنجاحات التجارية من فوز بتعاقدات وزيادة صادرات وانتزاع الفرص وصراع حول الأفكار والإبداع والذي أصبح يترجم في شكل منتجات تكسب أسواقا وتدر أموالاً، وسعت الأمم الظافرة بكل السبل للسطو على الأسرار الاقتصادية والتقنية والعلمية والتجارية للدول الأخرى حيث اصبح للاقتصاد الرقمي الجديد دور في خلق وظائف جديدة ورفع انتاجية العامل وتوزيع جديد للدخول بين الافراد وتحفيز النمو الاقتصادي والاستثمار في المنتجات التكنولوجية والتجارة الالكترونية والتحويلات المالية وعمل البنوك واداء الحكومات الالكترونية وسهولة عملية انتقال رؤوس الاموال ، فقد استأثر اقتصاد المعرفة على ٧% من الناتج القومي الاجمالي عالميا وتنمو بمعدل ١٠% سنويا ويبلغ نصيبة من حجم النمو الانتاجي للاتحاد الاوربي ٥٠% ، وتلعب عملية انتاج واستخدام تكنولوجيا الاتصال والمعلومات والابتكار والموارد البشرية دورا هاما في هذا الاقتصاد واصبح موضع تنافس بين الدول والشركات حيث غلبة الصراع التقني والتجاري والاقتصادي على الصراع العسكري [٨].

وأضاف الطابع التكنولوجي للصراع طرقاً بديلة عن الحرب المباشرة بين الدول أو بين الخصوم. وأصبحت تلك الصراعات تحتاج لتحالفات من الحكومة والمنظمات الدولية والقطاع الخاص، وذلك في ظل نشأة أشكال جديدة من التنظيم الاجتماعي وأنماط جديدة من الصراعات الاجتماعية – السياسية والتعبير عن الصراعات الأثنية والعرقية [٩].

وساعدت الثورة التكنولوجية في تغيير شكل الحرب وأدواتها وعمل اجهزة الجيش وأثرت على الفاعلين بها، وساهمت في إعادة التفكير في حركية وديناميكية الصراع وأدى ذلك لاختلاف درجات التهديد ومصادرة وطبيعته وأثاره على المجتمع الدولي. وظهر شكلين من الصراع في عصر المعلومات هما حرب الشبكات وحرب الفضاء الإلكتروني Cyber war & Net war، والتي جاءت مواكبة أو معبرة عن استخدام الآليات التقليدية للصراع ولكن بوجه تكنولوجي يتواكب مع العصر. وانعكس ذلك في لعب دور اساسي في إحداث ثوره في الشئون العسكرية، وتعلقها بجميع مجالات وخدمات الحياة المدنية والبنية التحتية الكونية للمعلومات، وتزايدت بذلك العلاقة ما بين التكنولوجيا والأمن لارتباط الدول بها في عمليات الاتصالات والإنتاج والخدمات، والتي قد تكون هدفا سهلا للهجمات مع عملية الانتشار والتنوع في المصالح على المستوى الدولي. وتطبيق تكنولوجيا الاتصال والمعلومات في عمل أسلحة الدمار الشامل كالبرامج البيولوجية والكيماوية والنووية، بما قد يحمل في مضمونه امكانية تعرضها لخطر الاستخدام الخاطئ أو التعرض لدرجات الأمان مع انتشار المعرفة التقنية والتعليمية الخاصة بالفيزياء أو الكيمياء أو البيولوجيا مع إتاحة المعلومات في ظل ظهور مجتمع المعرفة (١٠).

وظهرت الحروب الجديدة في سياق دولي يغلب علية الطابع التكنولوجي، وذلك بخلاف الحروب القديمة بين الدول، والتي كان هدفها تحقيق اكبر درجة من الضرر للخصم والاستخدام المنظم للقوة في مواجهه قوة أخرى، ولكن نهاية الشكل القديم للحرب بين الدول لم يعن– بأي حال – انتهاء العنف، فشهد المجتمع الدولي بروز أنواع جديدة من العنف يمكن أن يطلق عليها "حروب جديدة "، وهذه الحروب يمكن أن تتم داخل الشبكات متعدية الحدود والتي قد تشمل دولاً وأطرافاً من غير الدول، ويكون هدفها ليس مجرد النصر العسكري بل قد يشمل التعبئة السياسية فقط بدلا من الإخضاع والسيطرة على إرادة الخصم، ويتم تعبئة المواطنين للمشاركة في المجهود الحربي سواء بالانضمام للجيش أو إنتاج أسلحة، وعلى عكس

الحروب القديمة قد لا يتم توجيه العنف مباشرة للعدو، وذلك مع سهولة مد شبكات التطرف والعنف واختراق امن الدول الداخلي، واصبح هناك عدم اعتماد كامل على المعارك العسكرية التقليدية بل اخذت صورا للتنافس والصراع على المعطيات التكنولوجية. هذا بالإضافة الى ظهور الارهاب الجديد الممتزج بتكنولوجيا الاتصال والمعلومات كشكل جديد للتهديدات الأمنية الجديدة للمجتمع الدولي وأصبح أكثر إلحاحا من أنواع الإرهاب التقليدي [١١].

وذلك ينبع من خصائصه وآثاره وطبيعة أطرافه وإمكانية استخدامه في كافة الأنشطة الحساسة والأكثر تهديدا للأمن الدولي كالإرهاب النووي والبيولوجي والكيماوي والالكتروني .

يعد الفضاء الإلكتروني عبارة عن فيض رقمي من المعلومات لا يعتمد كليا على البيئة المحسوبة التي توفرها شبكات المعلومات بل تتعامل أيضا بكثافة مع مفرداته مثل سرعة تناقل البيانات وصلاحية الدخول إلى الشبكة بالإضافة إلى المعالجات التي تتناول البيانات المتدفقة ضمن البيئة الالكترونية " [١٢].

ويتميز الفضاء الالكتروني باستخدام الالكترونيات والمجال الكهرومغناطيسي لتخزين وتعديل أو تغيير البيانات عن طريق النظم المتصلة والمرتبطة بالبنية التحتية الطبيعية ويتكون من المكون الأول الطبيعي أو المادي والذي يتمثل في الأسلاك والمحولات والبنية التحتية المعلوماتية كالكابلات HARDWARE، والمكون الثاني يتمثل في المحتوى والذي يعكس شكل المعلومات في الفضاء الإلكتروني SOFTWARE، أما المكون الثالث فيتمثل في عملية التوصيل بين المعلومات والبشر وحركة التفاعل ما بين البرمجيات والمعدات، وارتباط ذلك بتصورات وقيم وسلوك المستخدمين من البشر، وأصبحت المعلومات المتوافرة لها قيمة اقتصادية وقيمة ميدانية بالنسبة إلى الجهات العسكرية وكلما زادت الفاعلية في إدارة تلك المعلومات كلما زادت الفائدة التي يمكن الحصول عليها وأصبح تفوق المعلومات إحدى القيم الأساسية للقوة العسكرية وأصبحت المعلومات مجالا للسيطرة والتحكم. ويتعلق ذلك بعمليات

المعلومات التي تشير للبيئة التي يمكن من خلالها شن عمليات الهجوم والدفاع والتي تكون متصلة ومستخدمة عبر الشبكات [١٣].

وليصبح التدفق الهائل للمعلومات داخل الفضاء الإلكتروني لا يقل عن قيمة هذه المعلومات. وترسم طرق الحصول على هذه المعلومات شكل السلطة والقوة والتي تنقسم لمعلومات مجانية متوافرة لمن يريدها واخرى تجارية متوفرة لمن يرغب بالدفع ،وهناك المعلومات الاستراتيجية المتوفرة لمن يسمح له بمعرفتها فقط، ونظرا للطبيعة غير المادية للمعلومات فان وضعها في الفضاء الإلكتروني يجعلها متوافرة ومتاحة للجميع عالميا من خلال شبكة من التواصل والعلاقات بين من يستخدمونه ويتفاعلون معه مع انتقال كافة مجالات الحياة من إعلام وصحة وتعليم وحكومة والمواطنة والاقتصاد والسياسية إلى الفضاء الإلكتروني فيما يشبه بالحياة الأخرى.

ومن ناحية اخرى اصبح يستخدم الفضاء الإلكتروني كوسيط وكوسيلة لشن الهجوم وتنفيذ الإعمال العدائية بين الخصوم كغيرة من مجالات الجو أو الفضاء أو البحر، فبينما تسيطر قلة من الدول على القدرات التكنولوجية لغزو الفضاء الخارجي واستخدامه نجد أن الفضاء الإلكتروني على العكس حيث يمكن لأي دولة او فرد او جماعه أن تؤثر فيه وتتفاعل من خلاله مع تميزه بالطابع الفردي في الاستخدام ، وبما قد يؤثر على طبيعة الصراع و القوة التي تمارس من خلاله، ويعبر ذلك عن نوع جديد من ممارسة القوة عبر شكل جديد من أساليب الحرب الالكترونية عبر الفضاء الإلكتروني.

ويأتي هذا مع خطر انتقال ساحة المواجهة في الحرب من الفضاء الواقعي للفضاء الإلكتروني ليصبح هناك عالم آخر بديلا لما يدور على ارض الواقع، حيث يوجد مواقع انترنت ومتصلة بالأهداف الاستراتيجية والمرافق الحيوية يمكن ضربها، لتظهر حرب جديدة بدون إراقة للدماء ولا تميز بين ما هو مدني وما هو عسكري. وليمثل ذلك سلاحاً جديداً وفاعلين جدداً، فيما يشبه بحرب العصابات حيث تبادل

هجمات الكر والفر حيث ينقلنا ذلك لنوع أخر من الحرب اقرب إلى مفهوم الإرهاب حيث الاعتماد على الضربات الاستباقية وبث الرعب والخوف وعدم وضوح مصدر الهجوم وعدم توقع نتائجه، وتمثل الإعمال العدائية التي تدور في الفضاء الإلكتروني وعمليات الدفاع والهجوم مشابها لمفاهيم القتال التقليدية إلا أنها تأتي في إطار الحرب الحديثة، كما إن الطابع الفردي لعمليات القتال تجعل هناك مجموعه متنوعة من الأعداء كما أن تحديد العدو وعملية السيطرة على الدخول تمثل تحديات لعمليات الفضاء الإلكتروني للقوات الجوية والتي يكون من مهامها التغلب والسيطرة عليها [١٤].

وتعزيزا للدور العسكري للفضاء الالكتروني أقرت هيئة الأركان الأمريكية تعريفا عسكريا له بانه "مجال يتميز باستخدام الالكترونيات والكهرومغناطيسية لتخزين تأثيرات متحركة أو ساكنة ضد الإشارات (الرادار – وأجهزة الاتصال) ونقاط ربط وشبكات النظام الدفاعي، حيث يتم الوصول إلى الهدف بسرعة الصوت أو بسرعة الضوء عند استعمال قدرتها الفضائية الالكترونية، بل وأعلنت القوات الجوية الأمريكية في ٧ ديسمبر ٢٠٠٥ تعريفا جديداً لمهامها القتالية " بان حددت مهمة القوات الجوبة في تسلم المهام للدفاع عن الولايات المتحدة ومصالحها العالمية بقدرتها على الطيران والقتال في الجو والفضاء الخارجي وفي الفضاء الإلكتروني، "وأصبح من مهام القوات الجوية منع هجوم الفضاء الإلكتروني للتعرض للبنية التحتية، والاستجابة السريعة للهجمات وإعادة الإصلاح للشبكات، والوعي الكافي بأهمية الفضاء الإلكتروني كساحة للصراع، والعمل على إلحاق الهزيمة بالخصوم والأعداء في ومن خلال الفضاء الإلكتروني بالإضافة إلى ضمان حرية الحركة للقوات داخل الفضاء الإلكتروني [١٥].

ومثل ذلك بداية إدخال المجال الإلكتروني ضمن القوات الجوية والتأكيد على دوره في القدرة العسكرية اللازمة للدفاع عن الدول ومصالحها، وتحول المجال الإلكتروني إلى مجال للعمليات العسكرية ومجالا لاستخدام القوة والسيطرة بما يهدد البنية التحتية الكونية للمعلومات [١٦].

ودفعت عملية إدخال المجال الإلكتروني كمجال حربي لضرورة معرفة من هم الأعداء وكيفية محاولتهم للتدخل في هذا المجال وإفساد أو تعطيل عمل الخدمات المدنية أو العسكرية، وكذلك كيف يتم الاستخدام العسكري للموجات الكهرومغناطيسية التي تعتمد عليها القوات العسكرية اعتمادا كبيرا في عمليات القيادة والسيطرة، وهذا الاستخدام يتراوح من التعرض لهجمات منع وإنكار الخدمة أو التدخل في عمل الأسلحة الالكترونية وخاصة مع حرية الفضاء الإلكتروني التي تمكن الدول والفاعلين من غير الدول للاستخدام غير السلمي لهذا المجال، وخاصة مع انخفاض التكلفة والحاجة فقط إلى المعرفة والإمكانيات الفنية التي يمكن من خلالها دخول القوات الجوية إلى هذا المجال، والذي أصبح مجالا أسهل من غيره من المجالات الأخرى حيث يتم شن الهجمات من أي مكان وفي أي وقت مقارنة بالحرب التقليدية وهذا ما يجعل هناك صعوبة أمام المقاتلين في الفضاء الإلكتروني لاكتشاف وتحديد مصدر الهجوم [١٧].

وأصبح المجال الإلكتروني لا يختلف عن المجالات الأخرى كالجو والبر والبحر فيما يتعلق بمبادئ الحرب وخصائص القوة حيث تسري في الفضاء الإلكتروني العقيدة العسكرية ذاتها والتي تركز على لامركزية التنفيذ ومركزية السيطرة، كما إن ذلك النوع الجديد من الحرب يأتي مشابها في أدواتها مع أدوات الحرب التقليدية من القذائف والصواريخ والدبابات والمتفجرات والحرب النفسية والتي تستخدم في ميدان المعركة إلا أن يتم استخدام أدوات أخرى شبيهه بها. والتي تتميز عن غيرها من الأدوات التقليدية بانخفاض تكلفتها حيث قد يتم شن حرب الكترونية عبر الفضاء الالكتروني بتكلفة دبابة فقط كما تنتشر مصادر الهجوم والدفاع الى الحد الذي يمكن ان توصف بانها اسلحة الانتشار الشامل والتي تتميز بالطابع الالكتروني لها وينعكس ذلك على قدرتها وتأثيرها المختلف واللامحدود، مع تجاوز الفضاء الإلكتروني للحدود الدولية، ويمكن للعمل العسكري أو العدائي ان ينتقل بسهولة من طابعه المحلي الى ان

يحدث تأثير عالمي ومنتشر عبر تمدد شبكات المعلومات والاتصال في زمن قياسي لا يتعدى الملي من الثانية [١٨].

وفرضت تلك التحديات اعادة التفكير في الاجندة الامنية الدولية وخاصة مع اتساع مفهوم الامن والذي يتعلق بتلك الدرجة التي تمكن الدولة من أن تصبح في مأمن من خطر التعرض للهجوم العسكري أو الإرهابي، وتعني كلمة الأمن في مجال الفضاء الإلكتروني إجراءات الحماية ضد التعرض للأعمال العدائية والاستخدام السيئ لتكنولوجيا الاتصال والمعلومات، ومن جهة أخرى فان الأمن القومي يعني بحماية وغياب التهديد لقيم المجتمع الأساسية وغياب الخوف من خطر تعرض هذه القيم للهجوم، وتشير كلمة الأمن إلى طيف واسع من المجالات ضمن وخارج حقل تقنية المعلومات. واخذت تلك القضية بالتصاعد في الاهتمام الدولي خاصة بعد بروز عدد من المتغيرات أبرزها نجاح تنظيم القاعدة في استخدامه بعد أحداث ١١ سبتمبر عام ٢٠٠١، ودخوله في عمل أجهزة الاستخبارات الدولية ، وحدوث طفرة هائلة في انتشار تكنولوجيا الاتصال والمعلومات عالميا ويأتي ذلك ايضا مع تصاعد حالات القرصنة والجريمة الالكترونية وتأثيرها على الاقتصاد الدولي ، وذلك في مقابل تزايد اخطار وتهديدات شبكة الانترنت وضعف الحماية امامها ، وأصبحت تتحول بذلك القضية من بعدها التكنولوجي الي الأمني ثم الي اعتبارها قضية اقتصادية الى اعتبارها قضية تتعلق بالأمن القومي للدول ثم تكتمل الصورة في التأثير الشامل لها علي المجتمع الدولي [١٩]. لذلك تزايدت العلاقة بين الأمن والتكنولوجيا، خاصة مع إمكانية تعرض المصالح الاستراتيجية للدول إلى أخطار وتهديدات، الأمر الذي حول الفضاء الإلكتروني لوسيط ومصدر لأدوات جديدة للصراع الدولي. وفرضت تلك التطورات إعادة التفكير في مفهوم "الأمن القومي للدولة"، والذي يعني بحماية قيم المجتمع الأساسية، وإبعاد مصادر التهديد عنها، وغياب الخوف من خطر تعرض هذه القيم للهجوم[٢٠].

وبات توافر أمن الكتروني يتحقق حال وجود إجراءات الحماية ضد التعرض للأعمال العدائية، والاستخدام السيئ لتكنولوجيا الاتصال والمعلومات[٢١]. وعني ذلك الأمن الإلكتروني بعملية وضع المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين بها عبر الاتصالات، ولضمان أصالة وصحة هذه الاتصالات. بيد أن طبيعة ذلك الفضاء، كساحة عالمية عابرة لحدود الدول، جعل الأمن الالكتروني يمتد من داخل الدولة إلى النظام الدولي ليشكل نوعا من الأمن الجماعي العالمي، خاصة مع وجود مخاطر تهدد جميع الفاعلين في مجتمع المعلومات العالمي. لذلك، أصبحت هناك مصلحة قطرية، وكذلك دولية، في الحفاظ على أمن الفضاء الإلكتروني، على أساس أن الأخير صار جزءا من الأمن العالمي. ودعم ذلك الطبيعة المتغيرة للتفاعلات الإلكترونية، خاصة مع تطور القدرات البشرية على إنتاج تقنيات جديدة، فضلا عن تصاعد مخاطر التهديدات الإلكترونية على البنية التحتية الكونية للمعلومات. ولم يقتصر الاهتمام بالأمن الإلكتروني على البعد التقني فحسب، بل تجاوزه إلى أبعاد أخرى ذات طبيعة ثقافية، واجتماعية، واقتصادية، وعسكرية، وغيرها، خاصة أن الاستخدام غير السلمي للفضاء الإلكتروني يؤثر في الرخاء الاقتصادي، والاستقرار الاجتماعي لجميع الدول التي أصبحت تعتمد بنيتها التحتية على الفضاء الإلكتروني [٢٢].

كما أن تراجع سيادة الدولة مع تصاعد دور الفاعلين من غير الدول في العلاقات الدولية (مثل الشركات التكنولوجية العابرة للحدود، وشبكات الجريمة، والقرصنة الإلكترونية، والجماعات الإرهابية وغيرها) فرض تحديات عديدة في الحفاظ على الأمن الالكتروني العالمي. ودفع ذلك إلى بروز اتجاهات تعددية لتحقيق ذلك الأمن عبر التنسيق بين أصحاب المصلحة من الحكومات، والمجتمع المدني، والشركات التكنولوجية، ووسائل الإعلام، وغيرها.

المبحث الثاني: الامن الالكتروني:

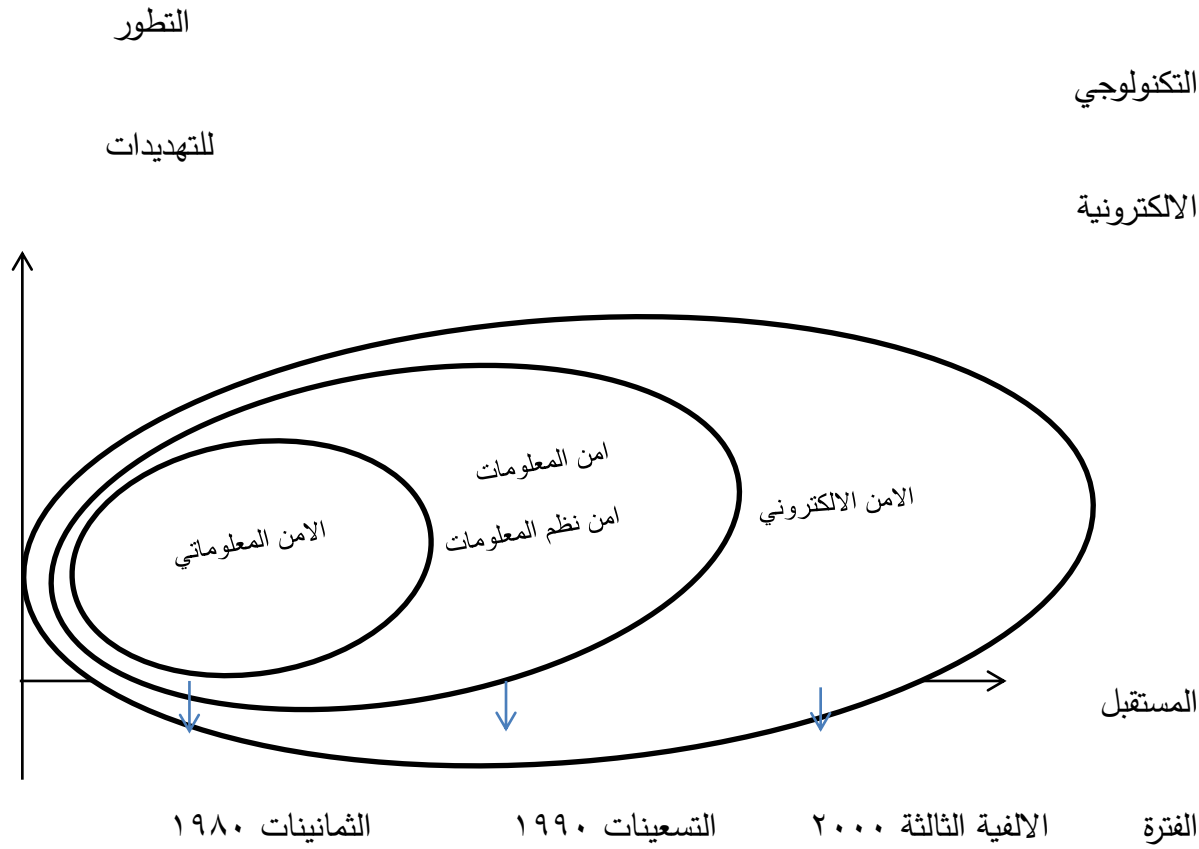
يعرف الأمن الالكتروني بأنه امن الشبكات والأنظمة المعلوماتية، والبيانات، والمعلومات، والأجهزة المتصلة بالأنترنت، وعليه فهو المجال الذي يتعلق بإجراءات، ومقاييس، ومعايير الحماية المفروض اتخاذها، أو الالتزام بها، لمواجهة التهديدات، ومنع التعديات، او على الأقل الحد من آثارها [٢٣].

ويعرف ريتشارد كمرر Richard A.Kemmerer الامن الالكتروني بأنه (عبارة عن وسائل دفاعية من شأنها كشف واحباط المحاولات التي يقوم بها القراصنة) [٢٤].

بينما عرفه ادورد امورسو AmorsoEdward على انه (وسائل من شأنها الحد من خطر الهجوم على البرمجيات او اجهزة الحاسوب او الشبكات وتشمل تلك الوسائل الادوات المستخدمة في مواجهة القرصنة وكشف الفيروسات و وقفها [٢٥]. أو بعبارة أخرى هو :مجموعة الاستراتيجيات، السياسات، الإجراءات، الخطط، والتدابير التنظيمية، او لقانونية والبشرية ومجموعة الوسائل التقنية التي تستخدم لحفظ وحماية تداول المعلومات المخزنة في الوسائط الرقمية والإجراءات المجردة ماديا والأنظمة المعلوماتية وما تحويه من أجهزة وشبكات وهذا من المخاطر الإلكترونية التي قد تهددها وضمان استرجاع هذه المعلومات والتخفيف من الضرر الذي ينجم عن إفسادها في حال وقوع هذه المخاطر الإلكترونية [٢٦].

وعند البحث في موضوع الأمن الإلكتروني هناك عدّة مصطلحات مشابهة له كأمن المعلومات وأمن المعلومات ونظم المعلومات [٢٧]. ومن خلال البحث تبين لنا أن هذه المصطلحات تعبر عن مراحل زمنية مختلفة مرّ بها الأمن الإلكتروني، أي أنه عرف عدّة مراحل متلاحقة مرتبطة بفترات تاريخية . ويوضح الشكل التالي التطور التاريخي للأمن الإلكتروني وفق زيادة مستوى التعقيد التكنولوجي وخطر التهديدات الإلكترونية عبر الزمن.

الشكل (١) : التطور التاريخي لمفهوم الامن الالكتروني



المصدر: اعداد الباحث .

بدأ تطبيق الأمن الإلكتروني بالتركيز على الحماية المادية والفيزيائية للأجهزة الإلكترونية أو البنية التحتية للمؤسسة من حواسيب ولواحقها من الأخطار البيئية أو الطبيعية. ويشير هذا إلى المفهوم التقليدي للأمن الذي كان يسمى بالأمن المعلوماتي .ثم برز في بداية سنوات الثمانينات الاهتمام بالمعلومة كمصدر

للتفوق التنافسي، فجاء تطبيق الأمن لحماية كل ما يتعلق بجمع وتخزين ومعالجة وايصال المعلومات داخل المؤسسة من محاولات المنافسين للحصول عليها بطرق غير مسموح بها إلى جانب الحماية المادية وأطلق عليه مصطلح أمن المعلومة أو أمن نظم المعلومات .ومع الانتشار الواسع لاستخدام تكنولوجيا المعلومات والاتصال أتسع مفهوم الأمن الإلكتروني ليشمل حماية الأعمال الإلكترونية في المؤسسة والإدارة الإلكترونية في الإدارة العامة في إشارة إلى مفهوم أشمل يتضمن حماية التعاملات الإلكترونية بين الأطراف الداخلية للمؤسسة والإدارة وبينها وبين العالم الخارجي.

عليه، وبناءً على ما يمثله الشكل (٢) لم تلغ المفاهيم السابقة للأمن الإلكتروني وانما توسعت إلى مفهوم شامل يتكيف مع التطورات التكنولوجية والتهديدات الإلكترونية والرهانات المختلفة على الصعيد الاستراتيجي كالحرب الإلكترونية والدفاع الرقمي، وعلى الصعيد القانوني كالمراقبة الإلكترونية وحماية الحياة الخاصة والتراث اللاملموس، ومع الرهانات على الصعيد الاقتصادي كالتنافسية والحاجة إلى الإبداع [٢٨].

أمّا فيما يخص مفهوم الأمن الالكتروني فيمكن ادراجه كالتالي:

لذلك تخشى دول العالم أجمع على أمنها القومي، في عصرٍ باتت تحكمه آلة التكنولوجيا، وتسير أعماله مليارات من نقرات (Clicks) مستخدمي الحواسيب والإنترنيت، وتسافر أمواله عبر قنوات الاقتصاد الرقمي والمعرفي، وتسوده لغة الّتقننة والحوسبة الإلكترونية والمعلوماتية، وتتضخم احتياجاته الأمنية بتضخم منظومته الثقافية الإلكترونية. ضمن هذا الواقع المحوسب؛ بادرت حكومات دول العالم إلى تحصين معلوماتها الإلكترونية القومية من أساليب التحايل الإلكتروني، ووسائل القرصنة المعلوماتية المنتشرة في الفضاء الإلكتروني، خاصة مما يعرف ب (أساليب الهندسة الاجتماعية) Social Engineering Methods والتي تعني استخدام حيلٍ نفسيةٍ وتكنولوجيةٍ لسحب المعلومات ، الحساسة

من مستخدمي الحواسيب والإنترنيت، والوصول إلى عمق مخزونهم المعلوماتي، سواء كان فكريًا أو محوسبًا ، خاصة تلك المعلومات المتعلقة بواقعهم القومي والاجتماعي، ومن ثم إعادة صياغتها بشكلٍ سياسي واقتصادي واجتماعي وأمني يضر بالأمن القومي للدولة المستهدفة. [٢٩]

يتلخص مبدأ عمل الهندسة الاجتماعية تقنياً، من خلال تلك المواقع الإلكترونية الموجودة على الإنترنيت، والتي تطلب من روادها إدخال معلوماتٍ عن واقعهم الاجتماعي والاقتصادي والثقافي، كمواقع طلبات التوظيف الوهمية، وبعض المواقع الإحصائية، بحيث يقدم رواد هذه المواقع معلوما تٍ مجانيةٍ عن واقعهم المعيشي لجهاتٍ مجهولةٍ قد تضر بأمنهم القومي .وبالتالي، تصبح مثل هذه المعلومات القومية سلاحًا فعالا بيد جهاتٍ مجهولة، ساهم في تقديمها أشخاصًا ينقصهم الحس الأمني، والإلمام الواعي بما يشمله البوح بمثل هذه المعلومات من تهديداتٍ أمنيةٍ قد تمس واقعهم الأمني، وإحداث العديد من الأزمات والمشاكل لأمن بلادهم القومي [٣٠].

أعادت الوسائل التقنية والإلكترونية الحديثة شريعة الغاب التي عاش بها الإنسان في عصوره الأولى، ولكن بمشهدٍ تكنولوجي ومعلوماتي تخلو منه الأخلاق والمبادئ، وتعلو فيه صيحة المصلحة، حتى وإن كلف ذلك في سياق حديثنا عن الواقع الرقمي *الاعتداء على المعلومات الإلكترونية للآخرين، وإلحاق الخسائر بهم، في ترجمة حقيقية لمقولة المهاتما *غاندي (Mahatma Gandhi) الشهيرة " :سياسة بلا مبادئ، وتجارة بلا أخلاق، وثروة بلا عمل، وتعليم بلا تربية، وعلم بلا ضمير، وعبادة بلا تضحية" [٣١].

وما يدعو حقا للقلق في التطور الّتقني هذا، هو تجمع خيوط صناعة وتنظيم تكنولوجيا المعلومات بيد أعدادٍ قليلةٍ في العالم، تتحكم بصناعتها وتشغيلها، واختزانها وتوزيعها، وتملك قنوات تمريرها، ومعرفة أسرار بيئتها وعملها، في مشهدٍ قد ين عكس سلبًا على الأمن القومي لبعض دول العالم فحتى ولو تناولنا البعد الداخلي لأية دولةٍ صناعيةٍ ومعلوماتيةٍ في العالم؛ نلاحظ أن من يقبض سيطرته على الحكم هم

الأشخاص الذين يمتلكون نواصي المعرفة الرقمية والإلكترونية، ووسائل نقل المعلومات بمختلف أشكالها، ومنابع التمويل الاقتصادي والمالي.

بمعنى آخر امتلاك أدوات توزيع الثروة المعلوماتية والرقمية الحديثة [٣٢]. والتي أصبحت إحدى الأدوات الهامة في حماية أمن المعلومات الإلكترونية لأية دولةٍ في العالم.

ارتباطًا بما سبق، يمكن سرد أهم النُقاط والتجارب التي تدعو دول العالم لحماية أمن معلوماتها الإلكترونية القومية، والتي تحقق لها الأهمية والأفضلية الاستراتيجية المتلخصة بحماية أمنها القومي ككل، إلى ما يأتي:

١- تحصين رأس الهرم والنواة المعلوماتية الأساسية للأمن القومي لأي دولة في العالم، والمتلخصة بالمحتوى الحربي والعسكري والتكتيكي، والتي تشكل رأس الهرم الأمني [٣٣].

٢- تدعيم معلومات القطاع الاقتصادي والمالي، وتوفير بيئةٍ آمنةٍ لتنظيم أعماله، خاصة وأنه يحوي جانبًا كبيرًا من العمليات القومية الاقتصادية لأي دولةٍ في العالم، كالبورصات، وبطاقات الائتمان، وقطاع البترولیات، وسوق الأموال والتداول، وبيانات الموازنة العامة، وصناديق الاستثمار، وقطاعات العمل المصرفي والمالي التابعة للقطاعات الخاصة [٣٤].

٣- تنظيم مصالح قطاعات العمل السياسي والحزبي والحكومي داخل الدولة، بحيث تضفي على المجتمع تنوعًا صحيًا اجتماعيًا وثقافيًا، يقاوم تيارات العبث الق ائمة على ضرب الأمن القومي بواسطة أساليب الهندسة الاجتماعي ة .فتوفير مثل هذه الحريات للشعوب؛ يساهم في تعزيز الإدراك بأن ضرورة حماية أمن المعلومات القومية الإلكترونية هي منظومة ثقافية تقع على كاهل الجميع، وذلك من خلال إحداث التغيير البنيوي والاجتماعي السياسي الرامي لتكريس التنمية المستدامة [٣٥].

٤- وضع سياسات الانتقال الجماعي نحو التحول شبه المتكامل إلى المجتمع المعلوماتي، وذلك ببناء بنية متقدمة للاتصالات وتكنولوجيا المعلومات، تسهم بحماية الداخل القومي لأي دولةٍ في العالم، ومن ثم الانتقال إلى الإبحار في الفضاء الدولي الإلكتروني، والذي سيقوي موقعها الاقتصادي والسياسي على المسرح العالم ي .مع محاولة التخفيف من الآثار الجانبية التي قد تظهر أثناء عملية التحول الرقمي، والتي تقلل من الجريمة الإلكترونية، خاصة الجوانب الإنسانية منها [٣٦].

٥- توفير بيئة عمل بحثية مناسبة لقطاعات البحث العلمي في الدولة، كالجامعات ومراكز الأبحاث العلمية والقومية، والتي تلقي بثمرها الرقمي على المجتمع ككل.

كما ان هناك الكثير من الدول لديها تجارب في كيفية تحقيق امنها الالكتروني ومن هذه الدول:

اولا: تجربة الولايات المتحدة الأمريكية : -

تعتبر التجربة المعلوماتية القومية الأمريكية واحدة من أكثر التجارب ثراء ونجاحًا في العالم، كونها تتمتع بمخزونٍ ثرواتي تكنولوجي ضخم . فهي رائدة الابتكار الاتصال السحري في عصرنا الحالي (الإنترنيت)، علاوًة على امتلاكها قاعدة بياناتٍ واتصالاتٍ تحوي العديد من أنظمة التشغيل، وبرتوكولات التواصل، واسترجاع المعلومات، والأرشيف المعلوماتي المشفر.

التفتت الولايات المتحدة الأمريكية إلى أهمية حماية معلوماتها الإلكترونية القومية منذ وقتٍ مبكر، والاستفادة من توفير منظومةٍ أمنيةٍ لمعلوماتها الرقمية، لتشرع بتطبيق سلسلةٍ من الإجراءات القانونية والّتقنية والرقابية التي تتناسب وحجم محتواها المعلوماتي، واتساع رقعتها الجغرافية، وتوجهاتها السياسية والاقتصادية والاجتماعية والثقافة الداخلية والخارجية نحو جعلها أكثر البلاد أمنًا في العالم، وأضخمها احتضانًا للمعلومات الإلكترونية [٣٧].

تقوم التجربة الأمنية المعلوماتية الأمريكية على ثلاثةِ منظوماتٍ سياسيةٍ وبنائيةٍ متشابكةٍ بشكلٍ متسلسلٍ، ومتداخلةٍ بطريقةٍ متينة، فما أن ينتهي إعداد وتطبيق المنظومة الأولى، حتى تدخل في إعداد وتطبيق المنظومة الثانية، لتصل إلى الثالثة بشكلٍ متكاملٍ وسريع يتوافق مع سرعة تطور النظم المعلوماتية في العالم .والمنظومات الثلاثة هي [٣٨] .

١- المنظومة الأولى القانونية : تضم سلسلة من القوانين الفيدرالية التي تنظم التعامل مع المعلومات الإلكترونية من منظورٍ أمني وقومي، كمنظومة القوانين الفيدرالية المسؤولة عن أمن وإدارة المعلومات، والتي تهتم بقضايا الأمن المعلوماتي داخل الولايات المتحدة الأمريكية، وقانون الخصوصية القاضي بعدم الوصول إلى معلومات الأفراد إلا من خلال الأشخاص المخولين من إدارة الدولة، وقانون إصلاح وإدارة قطاع تكنولوجيا المعلومات والإصلاح الاستحواذي، والذي يهدف إلى تقييم وتوفير الإرشادات الخاصة بممارسة الوكالات والشركات الرأسمالية الكبرى للمعلومات الرقمية القومية، وقانون الحرية الالكترونية، وغيرها من القوانين الأخرى.

٢- المنظومة الثانية الفنية : وهي التي تقوم بوضع المعايير الفنية والّتقنية الموحدة للتعامل مع أمن المعلومات بشكلٍ آمنٍ .تتشكل هذه المنظومة من عدة جهات مختصةٍ بأمن المعلومات القومية داخل الولايات المتحدة الأمريكية، كالمعهد القومي للتكنولوجيا والمعايير، والذي يقوم على تطوير الاختبارات والمنهجيات المرجعية الهادفة لتحليل البنية المعلوماتية .ولجنة السياسة القومية لتشفير المعلومات، والهادفة إلى تشفير وترميز) تكويد (Coding) المعلومات والبيانات المتداولة إلكترونيًا عبر المجتمع الأمريكي ككل، وحفظها من الاندثار أو التداول اللاسلمي.

٣- المنظومة الثالثة التنفيذية والتطبيقية والرقابية : وهي عبارة عن مجموعة من الهيئات والوكالات الفيدرالية المسؤولة عن تطبيق وتنفيذ سياسات أمن المعلومات في الولايات المتحدة الأمريكية، والتي لها

ارتباطاتٍ عديدةٍ مع باقي المؤسسات والوزارات القومية في الداخل الأمريكي، حيث تقدم لها الاستشارات والتطبيقات المعلوماتية والأمنية الإلكترونية .تقوم هذه المنظومة بالتنسيق مع العشرات من الوكالات الأمريكية، على رأسها وكالة المخابرات الأمريكية، ووكالة الأمن القومي، ووزارة الدفاع، ومكاتب الاستطلاع الداخلية والخارجية، والمكاتب المعنية بالشؤون الاقتصادية والاجتماعية، وغيرها من الجهات والوزارات القومية الأمريكية، بهدف إبقاء الوضع المعلومات متزن مع جميع الجهات، والحصول على قدرٍ كافٍ من المعلومات المتعلقة بالأمن القومي الأمريكي [٣٩].

ثانيا: تجربة الاتحاد الاوروبي :-

تعد تجربة الاتحاد الأوروبي من أكثر التجارب فاعلية، كونها تحوي العديد من القوميات المتحدة في بوتقةٍ تكنولوجيةٍ واقتصاديةٍ واحدة .استثمر الاتحاد الأوروبي هيئات البريد والبرق والهاتف (يورونت) (Euro Net) التي كانت تعمل في أوروبا، ليزيد من قدرتها المعلوماتية بشكلٍ كبير، ويحولها إلى ما يعرف بالشبكة الأوروبية للوصول المباشر للمعلومات (European Network for Direct Access to the Information) انطلقت أوروبا بعد هذه الخطوات التّقنية نحو التحول الكامل إلى المجتمعات المعلوماتية، لما لها من أهميةٍ في تعزيز الوحدة الأوروبية، وإزالة كافة المعيقات القانونية والإدارية والإلكترونية التي تقف أمام العمل الوحدوي [٤٠].

نادى الاتحاد الأوروبي بضرورة اعتبار (الصناعة الإلكترونية) صناعة استراتيجية، وهي الفكرة التي تشير إلى تجربة الاتحاد الأوروبي في مجال أمنية المعلومات القومية، بحيث اشتمل تطبيق هذه التجربة أو المبادرة على القطاعين العام والخاص في أوروبا، والتي نافست وبشكلٍ قوي تجربة الولايات المتحدة الأمريكية، ومن بعدها اليابان. تنافس أوروبا (خاصّة ألمانيا وفرنسا وبريطانيا) الآن الولايات المتحدة

الأمريكية في المجالات المعلوماتية والصناعة الرقمية، خصوصًا بعد تنفيذ إجراءات سوق المعلومات التي أقرتها وزارات الاتحاد الأوروبي.

ثالثا: التجربة الاسرائيلية :-

بادرت إسرائيل منذ عام ١٩٥٩ إلى تكثيف جهودها الإلكترونية والّتقنية والمعلوماتية الداعية لتدعيم أمنها القومي، في قلب منطقة تعج بالصراعات الرافضة لمثل هذا الوجود الإسرائيلي .اعتمدت إسرائيل على الكادر البشري الموجود لديها في هذا المجال، وبالتعاون مع الولايات المتحدة الأمريكية والدول الكبرى من خلفها، لنقل غالبية ما تمتلكه هذه الدول من تقنياتٍ حديثةٍ ومتطورةٍ إلى داخل العمق الإسرائيلي. ركزت إسرائيل في أولى خطواتها الّتقنية على تعزيز تكنولوجيات الفضاء الخارجي لديها، والتي رأت بأن سيطرتها على الفضاء الخارجي سيعزز من وجودها الأمني، لتنتشر مراكز التصنيع التكنولوجي في قلب (تل ابيب) (Tel Aviv) (تل الربيع) والتي عملت على تصميم جميع متطلبات العمل الذاتي والتكنولوجي للقلب القومي الإسرائيلي [٤١].

أنشأت إسرائيل في عام ١٩٥٩ لجنة قومية تعنى بشؤون الفضاء وأمنية المعلومات .وفي عام ١٩٦٤ ، اتفقت مع أمريكا على تشييد محطة للأقمار الاصطناعية والتحسسية المعلوماتية لكي لا تترك فضاءها الخارجي مكشوفًا، حيث أخرجت للنور في عام ١٩٦٧ م أول ابتكارها الصناعية الفضائية، كتجربةٍ أمنيةٍ ومعلوماتيةٍ أولية .لتتوالى بعد ذلك الابتكارات الإسرائيلية، والتي قادها نخبة من القيادات الإسرائيلية، لتصل إلى مستوى عالٍ من التطور الأمني الّتقني. وفي عام ١٩٨٣ تأسست وكالة سالا (Sala) الفضائية الإسرائيلية على يد وزير البحث العلمي الاسرائيلي انذاك يوفال نئمان، (Yufal Neeman) والذي قام بالعديد من الخطوات الّتقنية لخلق جيلٍ إسرائيلي معلوماتي قادرًا على ربط أمن إسرائيل بالكوكبة الرقمية [٤٢].

عملت إسرائيل على ربط نواة معلوماتها القومية بعضها ببعض، كربط وكالة سالا بجامعة تل أبيب، وربط كافة المراكز البحثية بشبكةٍ واحدة، كمعهد التخنيون (Technion) المتخصص بالتكنولوجيات المعلوماتية، والذي تم ربطه بالجامعة العبرية بالقدس، وجامعة النقب، ومعهد وايزمان (Wiseman) المختص بالعلوم الطبيعية، والذي تم ربطه بكبريات دول العالم، كفرنسا وروسيا واليابان . مكنت هذه الخطوات إسرائيل من بناء قاعدةٍ معلوماتيةٍ قوميةٍ قويةٍ، معتمدةٍ على مجموعةٍ من الأقمار الصناعية المختصة بالتجسس، كالأقمار (أفق ١، أفق٢، أفق٣)، و القمر (Amos)عاموس وغيرها، والتي أحدثت تطوراتٍ في الاتصالات الإسرائيلية الداخلية والخارجية [٤٣].

التجربة العربية :-

يسيطر على عالمنا اليوم معادلة مفادها أنه من يمتلك الوسائل المعرفية من تكنولوجيات، وشبكات اتصالية، ووسائل رقمية؛ يمتلك أسباب القوة، ويستطيع أن يفرض سيطرته على مقدرات الأمم الأخرى، خاصة وأن مثل هذه الوسائل تعد قوة ناعمة (Soft Powers) بيد الدولة، تختلف عن قوتها التقليدية في العديد من الأمور، والتي تؤهلها لأن تبقى في صدارة الحدث. لا تنطبق هذه المعادلة على معظم الدول العربية، والتي تعاني من فجوةٍ رقميةٍ داخليةٍ وأخرى خارجية، نتيجة تبعيتها للتكنولوجيا الغربية والمستوردة، والتي تدل على ضعف البلدان العربية في انتاج التكنولوجيا، الامر الذي جعل هذه البلدان تعاني من ضعف واضح جدا في الاعتماد على هذه التكنولوجيا في ادارة شؤونها الامنية والخدمية، على الرغم من وجود مؤشر بسيط في بعض دول العربية ولاسيما دول الخليج العربي، التي حاولت الاعتماد التكنولوجيا في ادارة شؤونها [٤٤].

إن التأخر العربي الفادح لا يقتصر فقط على التعامل مع وسائل القوة الناعمة، بل يتعدى ذلك ليصل التأثير التكنولوجي في البنى التحتية الاقتصادية والسياسية والاجتماعية والامنية والخدمية والتعليمية والاتصالية، مما جعل الساحة العربية مرتعًا لعمليات القرصنة الخارجية [٤٥].

ومن جانب اخر، تعاني غالبية دول العالم الثالث من مشاكل متعددةٍ ذات تأثيرٍ كبيرٍ على أمنها القومي والوطني والسيادي .فقد ظهرت العديد من أشكال التبعية التي أغرقت هذه الدول في وحلٍ من الأزمات الاقتصادية والسياسية والاجتماعية والّتقنية والأمنية، وحولتها إلى أسواقٍ استهلاكيةٍ وحقول تجارب لكل ما تنتجه الدول المتقدمة اقتصاديًا وعسكريًا وتكنولوجيا .وخير مثالٍ على هذه الدول المدرجة تحت تصنيفات العالم الثالث أو النامي، هي الدول العربية. سارت دول العالم بعد الثورة الّتقنية نحو إدراج الابتكارات الإلكترونية ضمن سياساتها الأمنية لحماية أمنها القومي، وهو أمر لم توفره غالبية دول العالم العربي في خططها الاستراتيجية والمستقبلية، مما أدخلها في مستنقع التبعية التكنولوجية. حيث اعتمدت معظم الدول العربية وبشكلٍ جزئي أو كلي على الابتكارات التكنولوجية الغربية والأجنبية في تدعيم مرافقها العامة، ومنافذ توزيع معلوماتها الاتصالية، وشبكاتها السلكية واللاسلكية، ومحطاتها التلفازية، ونشاطاتها الفضائية المتعلقة بنشر الأقمار الصناعية، والتي استباحت أمنها القومي والسيادي بشكلٍ مخيف. وهذا ما يؤشر الى ان معظم انظمة التشغيل والحماية التي تعتمد عليها الدول العربية هي انظمة خارجية وليس وطنية. إن المجتمع العربي ليس مجتمعًا منتجاً معلوماتياً على صعيد البرمجيات ولا على صعيد التجهيزات الإلكترونية الصلبة. وما زال يعاني من ضعف البيئة القانونية وقلة خبرة أهل المهن القانونية، ونقص التعليم الجامعي لهذه المادة، وهو يشهد واقعاً صعباً وغير متجانِس مع المعايير والمتطلبات الدولية والذي يعرض الكيانات العربية للأخطار والهجمات الالكترونية من قبل أفراد، مجموعات منظمة، مؤسسات

خاصة، منظمات ارهابية (داعش)، دول متضررة او معادية (اسرائيل)، للنهوض من هذا الواقع الجامد ومواكبة التحديات[٤٦].

تزداد الحاجة القومية والعربية هنا، وفي ظل هذه السطوة التكنولوجية التي تمارسها أنظمة المعلومات الإلكترونية على الساحة العربية، إلى امتلاك استراتيجية قوميةٍ ووطنيةٍ تستجيب إلى متطلبات العملية التنموية الشاملة الجارية في العالم، وُتواكب التطورات الحاصلة في حقل المعلومات الإلكترونية، وكيفية حمايتها من الأخطار الخارجية، وتوظيفها بشكلٍ إيجابي يؤثر على صنع القرار العربي الفردي والجماعي [٤٧]، إضافة إلى محاولة التحرر من الاعتماد الكلي أو الجزئي على التكنولوجيات الغربية والأجنبية، أو صقلها بالطابع العربي الداعم للأمن القومي العرب ي .فلو نظرنا مثلا في نشأة الانترنيت، لوجدنا أن تاريخه الإنشائي يعود إلى وزارة الدفاع الأمريكية، أي أنه ابن للمؤسسة العسكرية الأمريكية، مما يعني مزيدًا من الاستباحة للأمن القومي العربي.

وفي النهاية، يعاني الأمن القومي العربي من ضعف الاهتمام بوسائل حمايته بشكلٍ تقليدي وإلكتروني، علاوًة على ضعف الاهتمام بطرق جمع المعلومات المتعلقة بمكافحة السطوة الرقمية التي أوجدتها الثقافة الاستهلاكية العربية .ولكن، ورغم هذه الفجوة التكنولوجية التي تلازم المشهد الأمني المعلوماتي العربي؛ ألا أن هناك فريقٌ من الشباب العربي والإسلامي قد استطاع كسر هذا القالب الّتقني الاستهلاكي، وتوظيف تكنولوجيا المعلومات بشكلٍ تنموي وتوعوي مفيد.

الخاتمة:

خلقت التطورات الّتقنية والتكنولوجية الحديثة العديد من التهديدات الأمنية والمعلوماتية، خاصًة على مستوى الأمن القومي، والذي أصبح أكثر عرضة وخطرًا نظرًا لسهولة الانكشاف المعلوماتي الذي وفرته وسائل الاتصال والتواصل الحديثة، وانتشار مختلف أنواع المعلومات بزخمٍ كبيرٍ على شبكات الانترنيت،

ترافقها العديد من أساليب الاقتناص الأمني والمعلوماتي الرامية للاستحواذ على المعلومات المنتشرة عبر الفضاء الإلكتروني بكافة الطرق والأساليب.

ومع تصاعد وتيرة التحول العالمي نحو بناء مجتمعات المعلومات في العالم، وتكثيف الاعتماد علي أدوات تكنولوجيا المعلومات والاتصالات في مختلف مناحي الحياة أدركت البشرية أن عليها تأمين هذه المعلومات بشدة، لأن تداولها وإدارتها إلكترونيا وعبر شبكات المعلومات والاتصالات التي ترابطت محليا وإقليميا وعالميا جعلها معرضَة لخطر الاختراقات المعلوماتية، الأمر الذي يخلف العديد من الآثار على الأمن القومي لتلك الدول المتعمدة على شبكات المعلومات وأدوات الاتصال الحديثة.

دفعت هذه المخاطر دول العالم لاتخاذ العديد من سبل حماية أمنها القومي من مخاطر الانفتاح الّتقني والمعلوماتي، وذلك عبر ربط أمن معلوماتها الرقمية باستراتيجياتٍ شاملةٍ تندرج تحت منظومة أمنها القومي، وذلك بغية الحفاظ على معلوماتها القومية والوطنية والعسكرية والسياسية والاجتماعية والاقتصادية من الانكشاف الأمني، والذي قد يجبرها على دفع ضريبة التكنولوجيا، وربما انهيار منظومتها الأمنية في ظل احتدام الحروب الإلكترونية عبر الفضاء الرقمي والمعلوماتي، في مشهدٍ غير كثيرًا من أساليب الصراع والتصادم حول العالم.

لذلك أصبحت التهديدات الالكترونية أحد التحديات الرئيسية التي يتحتم على الدول مواجهتها خلال الفترة الحالية، ومع تزايد الاعتماد على (التكنولوجيا)، خاصة في المجالات التي تتعلق بالأمن القومي، مثل الشبكات العسكرية والبيانات المالية والمصرفية، تزايد الحديث عن أهمية مواجهة هذه التهديدات.

الهوامش:

١) Joseph S. Nye, Cyber Power, Belfer Center for Science and International Affairs, Cambridge: Harvard Kennedy School, Cambridge, MA , 2010,p 4

٢) Kuehl, “From Cyber Space to Cyber Power: Defining the Problems”. Op. Cit. p.48

٣) Joseph S. Nye, Cyber Power. Op. Cit. p 3.

٤ عادل عبد الصادق، الارهاب الالكتروني القوة في العلاقات الدولية.. نمط جديد وتحديات مختلفة"، مركز الدراسات السياسية والاستراتيجية بالأهرام، ط١، القاهرة، ٢٠٠٩، ص٥٠

٥ صدقي عابدين، قضايا الأمن في آسيا، مركز الدراسات الأسيوية ،كلية الاقتصاد والعلوم السياسية، القاهرة،٢٠٠٤، ص ١٤

٦) Todd A. Megill, The Dark Fruit of Globalization: Hostile Use of the Internet, U.S. Army War College,Pennsylvania, 2005,p.16

٧) James R. Hosek, “The Soldier of the 21st Century,” in New Challenges, New Tools for Defense Decision making, ed. Stuart E. Johnson, Martin C. Libicki, and Gregory F. Treverton, Rand, Santa Monica, ٢٠٠٣,p. ١٩٦.

٨) Steven Metz," Armed Conflict In The 21st century: The Information Revolution And Post-Modern Warfare", Strategic Studies Institute, U.S. Army War, Pennsylvania, 2000 ,pp 5 -73

٩) Jerome C. Glenn and Theodore J. Gordon," 2004 State of the Future", Chapter 5,Technology, The Millennium Project American Council for the UNU, Millennium Project Publications, Washington, D.C, 2004 ,pp 1-401

١٠عادل عبد الصادق، الارهاب الالكتروني، مصدر سبق ذكره، ص٣٠

١١عادل عبد الصادق، الارهاب الالكتروني، مصدر سبق ذكره، ص٣٥

١٢) Acicognani,"on the linguistic nature of cyber space and virtual communities", virtual reality ,vol.(3), Springer-Verlag , London,1998 ,pp16-24

١٣١٣١٣١٣) James M. Liepman, Jr.," Cyberspace: The Third Domain", Zel Technologies, LLC and Global Cyberspace Integration Center, New York, 2007.

http://www.au.af.mil/au/aunews/archive/0223/Articles/Cyberspace%20Third%20Domain%20-%20Liepman.

١٤) Vincent Moscow, The Digital Sublime : Myth, Power, and Cyberspace, MIT press, Cambridge, Massachusetts, 2004.p 218

١٥عادل عبد الصادق، الارهاب الالكتروني، مصدر سبق ذكره، ص٤٢

١٦) Patrick D Allen, Information Operations Planning, Artech House, Norwood, MA, 2007. p323

١٧) James M. Liepman, Jr, Op.Cit. pp 12-15

١٨عادل عبد الصادق، الارهاب الالكتروني، مصدر سبق ذكره، ص٤٣

١٩عادل عبد الصادق ، "هجمات الفضاء الإلكتروني و استراتيجيات الأمن القومي "، جريدة الاهرام ،العدد (٤٤٨١٦)، القاهرة،١٩ اب ٢٠٠٩.ص٧

٢٠ مصطفي علوي، مفهوم الأمن ، مصدر سبق ذكره، ٢٠٠٤ ، ص١٤

٢١) Martin C. Libicki, Conquest in Cyberspace: National Security and Information Warfare , Cambridge University Press, New York, 2007,pp 1-14.

٢٢) Morgane Fouch, Robert Macrae and Jon Danielsson, “Could a Cyber Attack Cause a Financial Crisis”WorldEconomicForum,2016,onlinee-article. https://www.weforum.org/agenda/06/2016/could-a-cyber-attack-cause-a-financial-crisis

٢٣ منى الاشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، بيروت، ٢٠١٧، ص٢٥

٢٤) Richard A. Kemmerer, Cyber security, University of California Santa Barbara, Department of Computer Science, California, 2003, P.3

3) Edward Amoroso, Cyber Security, Silicon Press, New Jersey, 2007 , P01.

٢٦) United Nation, Cyber security, International Telecommunication Union (ITU), Geneva, 2008.

٢٧) BLOCH.L & WOLFHUGET.C, « Sécurité Informatique principes et méthodes », Eyrolles, Paris, 2007.p251

٢٨) REFALO.P, « La Sécurité Numérique de l’Entreprise l’effet papion du hacker », Eyrolles, Paris, 2013, P : 27.

٢٩ الغثبر خالد القحطاني ، أمن المعلومات الإلكترونية بلغة ميسرة، مركز التميز لأمن المعلومات، ط ١ ، جامعة الملك سعو د، الرياض،٢٠٠٩، ص٣٢

٣٠ انظر : لجنة معايير نظام التشغيل والسرية والتأمين، " معيار قواعد الممارسة لإدارة أمن المعلومات" ، المركز القومي لإدارة المعلومات،٢٠١٠، ص ٤٧ .نقلا عن :المنظمة الدولية للقياس والهيئة الدولية للكهروتقنية

*لا بد من التنويه هنا، أن هذا الحديث لا ينطبق على أساليب المقاومة الإلكترونية التي ينتهجها الشارع الإسلامي والعربي بشكلٍ عام، والشارع الفلسطيني بشكلٍ خاص ضد الاحتلال الإسرائيلي، فذلك يدخل في مفهوم مقاومة الاحتلال، ول يس ضمن الأبعاد الإنسانية، والتي تخلو منها ساحات التصادم الدولية الإلكترونية الباحثة عن المصالح وكسب الأموال، وغير ذلك من الأبعاد غير الأخلاقية.

*المهاتما غاندي (M. Gandhi): الزعيم والأب الروحي للهند .سياسي هندي، قاد حركة استقلال الهند عن بريطانيا وهو رائد مقاومة الاستعمار من خلال العصيان المدني اللاعنفي .أنظر الرابط http://goo.gl/lzCUY يعرف هذا العصيان المدني اليوم في واقعنا الفلسطيني بـ(المقاومة الشعبية السلمية)، والذي يعاني الكثير من جدليات الرفض والقبول

٣١ جعفر الطائي، التطبيقات الاجتماعية لتكنولوجيا المعلومات ،دار المناهج للنشر والتوزيع، ط١،عمان ،٢٠٠٦ ص٢٧٣

٣٢ حسن مكاوي، تكنولوجيا الاتصال الحديثة في عصر المعلومات، الدار المصرية اللبنانية، ط١، القاهرة، ١٩٩٣، ص٣٥

٣٣ جمال غيطاس، أمن المعلومات والأمن القومي، شركة نهضة مصر للطباعة والنشر، ط١،القاهرة، ٢٠٠٧، ص ٦٣

٣٤ المصدر نفسه ، ص ص ٩١-٩٢

٣٥ جعفر الطائي، التطبيقات الاجتماعية ، مصدر سبق ذكره، ص١٤٩

٣٦ أبو بكر سلطان احمد، التحول إلى مجتمع معلوماتي، نظرة عامة، دراسات استراتيجية، العدد(٧٧)، مركز الامارات للدراسات والبحوث الاستراتيجية، ط١، ابو ظبي، ٢٠٠٢ ، ص ٤

٣٧ جمال غيطاس، امن المعلومات، مصدر سبق ذكره، ص٢٢٩

٣٨ المصدر السابق نفسه، ص ٢٣٦-٢٣٧

٣٩ المصدر نفسه، ص ٢٤٢-٢٤٤

٤٠ أبو بكر سلطان احمد، التحول إلى مجتمع معلوماتي ، مصدر سبق، ص ص ٤٨-٥٠

٤١ رأفت الكمار، الحاسوب والأمن القومي العربي، دار الكتب العلمية للنشر والتوزيع ، القاهرة، ٢٠٠٥، ص٣٥٧-٣٥٩

٤٢ نوران شفيق، "الفضاء الإلكتروني وأنماط التفاعلات الدولية، دراسة فى أبعاد الأمن الإلكتروني"، رسالة ماجستير (غير منشورة)، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة القاهرة. ص ص ١٠٥: ١٠٧.

٤٣ محمد محسن، الجيش الإلكتروني استراتيجية إسرائيل بالحرب الافتراضية، شبكة المعلومات الدولية، ٢٠١٣، متاح على : http://www.aljazeera.net

٤٤ مصطفى عبد الغني، الرقابة المركزية الأمريكية على الإنترنت في الوطن العربي، دار العين للنشر، ط١، القاهرة، ٢٠٠٦، ص ٩٩.

٤٥ يحيى اليحياوي، موقع العرب من شبكات المعرفة" ، ٢٠٠٨، شبكة المعلومات الدولية

http://www.elyahyaoui.org/ tijani_livre_talaa.htm

٤٦ عباس بدران،،" الحرب الإلكتروني ة :الاشتباك في عالم المعلوما ت"، مركز دراسات الحكومة الإلكترونية، بيروت، ٢٠١٠، ص٣٣.

٤٧سالم محمد، العصر الرقمي وثورة المعلومات :دراسة في نظم المعلومات وتحديث المجتمع، عين للدراسات والبحوث الانسانية والاجتماعية، ط١، القاهرة، ٢٠٠٢،ص١٤٧