حرب الفضاء الإلكتروني
المفهوم - الأدوات والتطبيقات

Cyber Space War
Concept – Tools and Applications

الكلمة المفتاحية : **حرب الفضاء الإلكتروني، الأمن، التهديدات الإلكترونية، الردع.**

Keywords: Cyber Space War, Security, Electronic threats, Deterrence.

م. د. انمار موسى جواد

كلية اليرموك الجامعة

Lecturer Dr. Anmar Mosa Jawad
Yarmouk University College
E-mail: anmar.mosa@yahoo.com

ملخص البحث

في القرن الحادي والعشرين، وبسبب الاعتماد المتزايد للدول المتقدمة على شبكات الإنترنت، وبسبب ربط البنية التحتية على هذه الشبكات، برز الفضاء الإلكتروني ليشكل بعداً جديداً وتحدياً أخر للدول. فالدول لم تعد تتحسب للهجمات التي قد تقع على إقليمها البري والجوي والبحري فحسب، وإنما أصبحت تتحسب لنوع جديد من الحروب، وهو حرب الفضاء الإلكتروني الذي يتخذ من شبكات الإنترنت والحاسب الآلي مسرحاً له.

وأصبح لهذه الحروب مسارح وساحات وفاعلين جدد، وألغت هذه الحروب من الناحية الفعلية القيمة الدفاعية للحدود، كما ألغت من الناحية القانونية العلاقة بين السلم والحرب، وخلقت حالة من عدم الاستقرار، وزادت من حالة الإنكشاف الأمني ، مما تتطلب إعادة صياغة مفهوم الأمن ليتماشى مع التطورات الجديدة في مفهوم الفضاء الإلكتروني.

وتتمتع هذه الحروب بمجموعة من الخصائص تغري الأطراف على المبادأة بالهجوم، وتستخدم فيها أنواعاً معينة من الأدوات والأسلحة ذات المزايا الخاصة والتي لا تحتاج إلى تخزين وغير قابلة للضبط أو التخفيض أو النزع كالأسلحة التقليدية.

ولم تعد هذه الحروب مجرد مشاهد من الخيال، فقد وجدت هذه الحروب تطبيقها في الواقع بين الدول، فقد شهد العالم حروب فضاء إلكتروني مرافقة لحالات الصراع المسلح، وحروب فضاء إلكتروني قائمة بذاتها.

المقدمـــــة

بدأ عصر الفضاء الإلكتروني، وأصبحت حروب الفضاء الإلكتروني حقيقة واقعة، وأخذت مجموعة من الدول المتقدمة في مجال الحاسبات والانترنت والفضاء الإلكتروني تتحسب لهذا النوع من الحروب، وأصبحت قادرة على شن هذا النوع من الحروب ما يدمر غيرها من الدول. وحرب الفضاء الإلكتروني تتميز بمجموعة من الخصائص أهمها إنها حروب سريعة أي أنها تحدث بسرعة الضوء، وبالتالي خلقت مخاطر أمام صناع القرار في وقت الأزمات، بالإضافة إلى ذلك فإن أهم ما يميز هذه الحروب أنها لا تحتاج إلى ساحات معارك تقليدية، فالمصارف والرادارات و البنى التحتية يمكن الوصول إليها عبر الفضاء الإلكتروني، والسيطرة عليها و وتدميرها دون الحاجة إلى دحر الدفاعات التقليدية للدول.

وقد بدأت هذه الدول تعد ساحات معارك الفضاء الإلكتروني، وذلك من خلال اختراق شبكات الدول الأخرى و بنيتها التحتية ووضع ثغرات التسلل وزرع القنابل المنطقية، وهذا الطابع المتواصل لحرب الفضاء الإلكتروني يلغي الحدود الفاصلة بين السلم والحرب، ويخلق بعداً خطيراً في حالة عدم الاستقرار.

وتنطلق اشكالية البحث من أن هناك علاقة جدلية بين النمو السريع والاستخدام الكثيف للتكنولوجيا والمعلومات وبين حرب الفضاء الإلكتروني، ما جعل من قضية أمن الفضاء الإلكتروني تلقى اهتماماً متزايداً من قبل الدول وجعل حرب الفضاء الإلكتروني تكاد بديلاً عن الحروب المباشرة بين الدول. وتطرح إشكالية البحث مجموعة من التساؤلات، أهمها :

١- ما المقصود بحرب الفضاء الإلكتروني؟ وماهي خصائصها؟
٢- ما هي طبيعة هذه الحرب؟ وما هي أدواتها؟
٣- هل طبقت حرب الفضاء الإلكتروني؟ وماهي الدول الفاعلة في هذا ميدان الفضاء الإلكتروني ؟
٤- ماهي استراتيجيات وعقائد حرب الفضاء الإلكتروني ؟ وما هو مستقبل هذه الحرب؟

وجاءت فرضية البحث من فكرة اساسية مفادها أن حروب الفضاء الإلكتروني اصبحت حقيقة واقعة واصبح لها ساحاتها وادواتها واستراتيجياتها وعقائدها، واصبحت مجموعة من الدول المتقدمة تتحسب لهذا النوع من الحروب. لذلك جاءت هيكلية هذا البحث ليوضح ذلك في مبحثين، المبحث الأول ويتناول مفهوم وخصائص حرب الفضاء الإلكتروني، والمبحث الثاني يتناول أدوات و تطبيقات حرب الفضاء الإلكتروني.

المبحث الأول

مفهوم وخصائص حرب الفضاء الإلكتروني

المطلب الأول : مفهوم حرب الفضاء الإلكتروني

لقد أصبح الفضاء الإلكتروني مجالاً جديداً للفعل والتأثير والتغيير في النظام الدولي والعلاقات الدولية، ومع الانتقال من مرحلة النمو السريع إلى مرحلة الاستخدام الكثيف لتكنولوجيا المعلومات، أصبحت قضية أمن الفضاء الإلكتروني تلقى اهتماماً متصاعداً على أجندة الأمن الدولي، وزادت العلاقة بين الحرب والتكنولوجيا وثوقاً مع إمكانية تعرض المصالح الإستراتيجية ذات الطبيعة الإلكترونية إلى أخطار تهدد بتحول الفضاء الإلكتروني إلى ساحة للصراع والحروب الدولية[١].

فقد دخل المجتمع الدولي في مرحلة جديدة تلعب فيها هجمات الفضاء الإلكتروني دوراً أساسياً سواء في تعظيم القوة أو الاستحواذ على عناصرها الأساسية، وأصبح التفوق في مجال الفضاء الإلكتروني عنصراً حيوياً في تنفيذ عمليات ذات فاعلية على الأرض وفي البحر والجو والفضاء من خلال نظم التحكم والسيطرة[٢].

كل ذلك فرض إعادة التفكير في مفهوم الأمن والذي امتد إلى حماية الدولة من التعرض للهجوم العسكري إلى حماية المنشآت الحيوية للبنية التحتية من التعرض لأعمال عدائية من خلال استخدام تكنولوجيا الاتصال والمعلومات. وأصبحت قضية أمن الفضاء

الإلكتروني تدخل في استراتيجيات الأمن القومي للعديد من الدول المتقدمة للعمل على الحيلولة دون تعرض بيئتها التحتية الحيوية للخطر[٣]. وزادت حالة الانكشاف الأمني للدول نتيجة لاعتمادها المتزايد على الفضاء الإلكتروني في مختلف النشاطات مثل برامج[٤] الحكومة الإلكترونية والتي تصبح عرضة للاختراق والهجوم بالفيروسات وسرقة المعلومات وإتلافها[٥].

وظاهرة حرب الفضاء الإلكتروني برمتها تكتنفها اليوم السرية الحكومية، إلى الحد الذي يجعل الحرب الباردة كأنها عصر من عصور الانفتاح والشفافية[٦].

وليس من السهل تقديم تعريف محدد للفضاء الإلكتروني، فهناك من يرى أنه ذو طابع افتراضي، حيث يعرفونه بأنه ((تلك البيئة الافتراضية التي تعمل بها المعلومات الإلكترونية والتي تتصل عن طريق شبكات الكومبيوتر)). ويعرفه آخرون بأنه ((المجال الذي يتميز باستخدام الإلكترونيات لتخزين وتعديل وتغيير البيانات عن طريق النظم المرتبطة والمتصلة بالبيئة التحتية الطبيعية، ومن ثم فانه يشمل عملية الاندماج ما بين الإنترنت والمحمول وأجهزة الاتصالات والأقمار الصناعية)). وفي كل الأحوال فان المقصود بالفضاء الإلكتروني كما يراه الكثيرون مجال طبيعي ومادي[٧].

والفضاء الإلكتروني هو مجموع شبكات الحاسوب في العالم وكل ما ترتبط به وتتحكم فيه هذه الشبكات. وهو ليس الإنترنت فقط، فالإنترنت شبكة مفتوحة مكونة من عديد من الشبكات، ومن أي شبكة على الإنترنت تستطيع أن تتصل بأي كومبيوتر آخر متصل بأي شبكة من شبكات الإنترنت. أما الفضاء الإلكتروني فيشمل الإنترنت إلى جانب العديد من شبكات الحاسوب السرية الأخرى التي لا يمكن الوصول إليها عبر الإنترنت. وبعض هذه الشبكات الخاصة تشبه شبكة الإنترنت تماماً لكنها منفصلة عنه على الأقل نظرياً. كما يشمل الفضاء الإلكتروني الشبكات التجارية التي تقوم بمهام معينة من قبيل إرسال البيانات الخاصة بالتدفقات المالية والمعاملات في الأسواق المالية ومعاملات البطاقات الائتمانية. وبعض الشبكات هي نفسها نظم للتحكم، بمعنى أنها هي التي تسمح للأجهزة بمخاطبة غيرها من

الأجهزة مثل لوحات التحكم التي تخاطب المضخات والمصاعد ومولدات الطاقة والكهرباء[٨].

ويشير مصطلح حرب الفضاء الإلكتروني إلى الإجراءات التي تتخذها أي دولة 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 (*1-0*).

وكانت حرب الفضاء غير واضحة المعالم في تسعينات القرن الماضي، لأنها كانت مختلطة مع الحروب النفسية و الدعائية، في حين أن اتساع شبكة الإنترنت فتح آفاق كبيرة للأجهزة المخابراتية لإستغلال هذه الشبكة في حروبها الدولية، و التغلغل 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[٩].

واستخدم مفهوم حرب الفضاء على مستوى واسع في أجهزة الإعلام، ولكن مدلولات هذا المسمى قد اتسعت كثيراً عما قبل، فقد كان المفهوم مقصوراً على عمليات التشويش على أنظمة الاتصال والرادار وأجهزة الإنذار، بينما يكشف الواقع الحالي عن دخول شبكات الاتصال والمعلومات إلى بنية ومجال الاستخدامات الحربية. بالإضافة إلى ذلك فإن إطلاق مسمى الحرب، يعني استخدام جيوش نظامية وتحديد ميدان قتال محدد، أما هجمات حرب الفضاء الإلكتروني فأن ميدان القتال فيها مفتوح كونها تتحرك عبر شبكات المعلومات والاتصال المتعدية للحدود الدولية[١٠]. وقد دفع التطور في مجال الفضاء الإلكتروني إلى بروز ترسانة غير تقليدية لأسلحة الكترونية (*Cyber weapon*) متعددة كالفيروسات وهجمات إنكار الخدمة والاختراق وسرقة المعلومات والتشويش وشفرات التسلل والقنابل المنطقية[١١].

واتجهت الدول لتعزيز 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 عسكرة الفضاء الإلكتروني، خاصة وأن القدرة على السيطرة على هذا النوع من الأسلحة ضئيلة بالمقارنة مع الأسلحة التقليدية، وهناك مسألة صعوبة تحديد الأسلحة التي يمتلكها الآخرون ومن ثم يصبح لدى المجتمع الدولي قدرة سريعة على التدخل لاحتواء التقدم في مجال هذه الأسلحة[١٢].

وقد أدى تعدد أنماط استخدام الفضاء الإلكتروني وتداخلها ما بين ما هو مدني وما هو عسكري إلى عدم وجود إجماع على تعريف محدد ودقيق لمفهوم حرب الفضاء الإلكتروني، فهناك من عرفها بأنها أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكومبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها، بينما يعرفها آخرون بأنها مفهوم يشير إلى نزاع يحدث في الفضاء الإلكتروني ويكون له طابع دولي[١٣].

وهناك ثلاثة أمور في عالم الفضاء الإلكتروني تجعل من حرب الفضاء الإلكتروني أمراً ممكناً وهي[١٤]:

١. وجود ثغرات في تصميم الإنترنت.

٢. وجود ثغرات في المعدات والبرمجيات.

٣. الاتجاه لتوصيل المزيد من الأجهزة والقطاعات على شبكات الفضاء الإلكتروني.

وتتأثر الحرب في الفضاء الإلكتروني بما يحدث في البيئات الأخرى والنزاعات بين الأفراد والجماعات والصراعات بين الدول، ولأن الحروب الفعلية تستعمل شتى أنواع أسلحة التدمير فإنها لم تتوانى عن استخدام الفضاء الإلكتروني لما له من تأثير أمني وعسكري[١٥].

إن مصطلح حرب الفضاء الإلكتروني يغطي مجموعة واسعة من الإجراءات، تتراوح بين المجسات البسيطة المستخدمة لمحو المواقع على شبكة الإنترنت، والحرمان من الخدمة، والتجسس، والتدمير. وعلى نحو مماثل يستخدم لتغطية مجموعة واسعة من السلوكيات، وهو يعكس تعريفات قاموسية للحرب تتراوح بين الصراع المسلح إلى التسابق العدائي[١٦].

وعلى الطرف الآخر من النقيض، يستخدم بعض الخبراء تعريفاً ضيقاً لحرب الفضاء الإلكتروني: "حرب غير دموية" بين الدول تشتمل فقط على الصراع الإلكتروني في الفضاء

السيبراني. ولكن هذا يتجاهل الترابط المهم بين الطبقات المادية والافتراضية للفضاء الإلكتروني. وكما أظهر الفيروس (ستانكس نت) الذي أصاب البرنامج النووي الإيراني، فإن الهجمات التي تستخدم البرمجيات قد تسفر عن آثار مادية حقيقية[١٧].

وهناك تعريف أكثر فائدة لحرب الفضاء الإلكتروني : عمل عدائي في الفضاء الإلكتروني تؤدي التأثيرات المترتبة عليه إلى تضخيم العنف المادي أو تعادله. في العالم المادي، تفرض الحكومات ما يشبه الاحتكار على نطاق واسع من استخدامات القوة، ويتمتع المدافع بمعرفة وثيقة بالتضاريس، وتنتهي الهجمات إما بسبب الاستنزاف أو الإرهاق. وهنا تفرض عملية تدبير الموارد ونقلها تكاليف باهظة[١٨].

وبسبب حداثة التهديدات الإلكترونية، والتطور السريع لهذه التهديدات، وبسبب النقص في المصطلحات الفنية المتفق عليها لوصف هذه التهديدات، فلا يوجد هناك فهم كامل لهذه التهديدات، فالأمن الإلكتروني غالباً ما يجري تبسيطه كحماية الشبكات وأنظمة البيانات، لكن زيادة عدد الهجمات على الشبكات المالية والحكومية و العسكرية، جعل من الأمن الإلكتروني أسبقية في مجال الامن[٢٠]. وأصبحت حرب الفضاء الإلكتروني بديلاً عن الحرب المباشرة بين الدول، وأصبحت القدرة على القيام بهجمات الكترونية أداة سيطرة ونفوذ إستراتيجية بالغة الأهمية سواء في وقت السلم أو في وقت الحرب، بسبب زيادة علاقة الفضاء الإلكتروني بعمل المنشآت الحيوية للدول – سواء كانت مدنية أو عسكرية – مما أدى إلى إمكانية تعرضها لهجمات الكترونية تستهدف الشبكة كوسيط وحامل للخدمات أو يشل عمل أنظمتها المعلوماتية، مما يعرقل قدرتها على القيام بوظيفتها[٢١].

وبالنسبة لساحة حرب الفضاء الإلكتروني فنجد أن ساحة حرب الفضاء الإلكتروني هو جهاز الحاسوب المحمول الذي يرتبط بكابل يربطه بأجهزة الخوادم، واليوم أصبح الفضاء الإلكتروني ساحة حرب تشهد كثيراً من المعارك الحاسمة في القرن الحادي والعشرين. وما يجعل من هذه الأماكن ساحة لقتال قوات حرب الفضاء الإلكتروني، هو أن قوات حرب الفضاء الإلكتروني تستطيع أن تدخل في قلب هذه الشبكات وتسيطر عليها أو تدمرها، وإذا

استولت على شبكة ما فأنه يمكنها أن تسرق كل معلوماتها أو ترسل إليها تعليمات بتحويل الأموال أو تسريب النفط أو إطلاق الغاز أو تفجير المولدات أو إخراج القطارات عن قضبانها أو صدم الطائرات أو إرسال كتيبة لتقع في كمين أو تفجير قذيفة في المكان الخطأ أو إخراج الأقمار الصناعية عن مداراتها ليذهب في غير هدى في الفضاء السحيق أو إيقاف رحلات الخطوط الجوية تماماً. وهذه الأمور ليست افتراضات فقد حدثت مثلها أحياناً على سبيل التجريب وأحياناً أخرى على سبيل حرب الفضاء الإلكتروني. فالمعلومات التي تتعامل معها شبكات الحاسوب والتي تدير المرافق ووسائل المواصلات والمصارف يمكن استغلالها ومهاجمتها في ثوان ولا تستطيع الجيوش والأساطيل الدفاع عنها لأنها تقع في المجال الرقمي للفضاء الإلكتروني[٢٢].

وبالنسبة لطبيعة حرب الفضاء الإلكتروني، فإنها تتميز بطبيعة فريدة، فإنها قد تشجع على المبادرة إلى شن الهجوم، وأكثر الأهداف المحتملة التي تتعرض لها هي الأهداف المدنية، بالإضافة إلى ذلك فأن السرعة التي تتحرك بها والتي يمكن ضرب آلاف الأهداف في أي مكان بالعالم قد تؤدي إلى نشوب الأزمات الشديدة، فالقوة التي حالت دون وقوع الحرب النووية هي قوة الردع، لكنها لا تجدي في مجال حرب الفضاء الإلكتروني[٢٣].

المطلب الثاني : خصائص حرب الفضاء الإلكتروني

تدخل هجمات حرب الفضاء الإلكتروني في إطار الحروب غير المتكافئة (*Asymmetric War*) كون الطرف الذي يتمتع بقوة هجومية ويبادر باستخدامها هو الطرف الأقوى، بغض النظر عن حجم قواته التقليدية وهو ما يؤثر في نظريات الردع الاستراتيجي. ولا تستطيع الهجمات الإلكترونية التمييز بين المنشآت المدنية والمنشآت الأخرى ذات الطبيعة العسكرية، ولا تتطلب هذه الهجمات لتنفيذها سوى وقت محدد، وتمثل حرب الفضاء الإلكتروني أسلوباً عسكرياً غير نمطي لإدارة الصراعات المسلحة، حيث يشترك فيها دول وأفراد مدنيون عبر الفضاء الإلكتروني، وأصبح من الصعب التمييز وتحديد مواقع المتحاربين في ميدان هذه الحرب، وتتميز عملية استخدام حرب الفضاء الإلكتروني بسهولة الانتشار

والقدرة على التأثير في الأهداف الكترونياً كالبنية التحتية الحيوية والمؤسسات الاقتصادية والمالية والعسكرية[٢٤]. ويمكن القول أن أهم خصائص حرب الفضاء الإلكتروني هي[٢٥]:

- أولاً : إن حرب الفضاء حقيقة واقعة، ويلاحظ أن الولايات المتحدة وبعض الدول الأخرى قادرة على أن تشن من حروب الفضاء الإلكتروني ما يدمر غيرها من الدول الحديثة.
- ثانياً : إن حرب الفضاء الإلكتروني تحدث بسرعة الضوء، فعندما تتدفق فوتونات الحزم المهاجمة عبر الألياف الضوئية، فان الوقت المستغرق لشن الهجمة وتأثيرها يكاد يتعذر قياسه، مما يخلق المخاطر أمام صناع القرار في أثناء الأزمات.
- ثالثاً : إن حرب الفضاء الإلكتروني هي حرب عالمية الطابع، وفي نطاق أو صراع يستشري العدوان الإلكتروني على مستوى العالم سريعاً، لأن أجهزة الحاسوب والأجهزة الخادمة المخترقة خفية أو التي تم السيطرة عليها في شتى أنحاء العالم سرعان ما تنظم إلى الهجمات فتجر بلاد كثيرة إلى الصراع سريعاً.
- رابعاً : إن حرب الفضاء الإلكتروني لا تحتاج إلى ساحات المعارك التقليدية، فالأنظمة المختلفة التي يعتمد عليها الناس – من المصارف والمطارات والطائرات وبطاقات الائتمان وشبكات الكهرباء والطاقة والبريد وصولاً إلى رادارات الدفاع الجوي وأنظمة الصواريخ – يمكن الوصول إليها عبر الفضاء الإلكتروني والسيطرة عليها سريعاً أو تعطيلها دون الحاجة إلى دحر الدفاعات التقليدية للدول.
- خامساً : لقد بدأ عصر حرب الفضاء الإلكتروني، وصارت الدول تتحسب من وقوع الهجمات الإلكترونية فبدأت تعد ساحة المعركة وذلك بأن يحاول كل منها اختراق شبكات الدول وزرع ثغرات التسلل والقنابل المنطقية وكل هذا تم في وقت السلم، وهذا الطابع لحرب الفضاء الإلكتروني هو الذي يطمس الحدود الفاصلة بين السلم والحرب ويخلق بعداً جديداً في حالة انعدام الاستقرار.
- والفضاء الإلكتروني لا حدود له، حيث يتشارك كل الفاعلين بما فيهم الدول من الإستخدام الشخصي إلى البرامج الإقتصادية 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[٢٦].

يضاف إلى ذلك صعوبة التعرف على هوية المعتدي أو المهاجم في حرب الفضاء الإلكتروني، ومن الطرق التي يمكن إتباعها لتحديد هوية المعتدي استخدام برامج اقتفاء الأثر العكسي، ولكن هذه البرامج قد توصل إلى جهاز خادم لا يتعاون لمعرفة الهوية أو قد يكون المعتدي قد اتخذ من الاحتياطات ما يكفي لطمس أثر الاعتداء أو معالم المصدر[٢٧].

ويمكن استخدام أسلحة حرب الفضاء الإلكتروني بسرعة وسهولة وبدون الفهم الكامل للتفاقم التصاعدي الذي قد ينجم عنها، فعلى الرغم من أن الحرب قد تبدأ في الفضاء الإلكتروني بلا جنود وبلا إراقة دماء، إلا أنه في بعض الأحيان لا تظل كذلك طويلاً، فقيام الدول بزراعة الأسلحة الإلكترونية في شبكات البنية التحتية في غيرها من الدول يجعل فتيل الحرب سهل الاشتعال أكثر من أي وقت مضى في تاريخ الحروب، وبالنسبة لأثر أسلحة الفضاء الإلكتروني، فإن أثر أسلحة الفضاء الإلكتروني يقل عن أثر الأسلحة النووية، لكن استعمالها في ظروف معينة قد يحدث أضراراً فادحة، وقد يشعل فتيل حرب واسعة. ويمكن قياس القوة في مجال حرب الفضاء الإلكتروني من خلال تقييم ثلاثة عوامل : الأول : الهجوم، أي قدرة الدولة على شن هجمات الكترونية على الدول الأخرى. الثاني : القدرة على الدفاع، ويعني قياس قدرة الدولة على اتخاذ إجراءات عند تعرضها للعدوان لصد هجمة أو تخفيف آثارها. والثالث : الاعتماد، ويعني مدى اتصال الدولة بالإنترنت واعتمادها على الشبكات والأنظمة التي قد تكون عرضة للأخطار في حالة وقوع حرب الكترونية[٢٨]. ومع تطور حرب الفضاء ظهرت لنا عقائد أهمها عقيدة التعادل وهي سياسة التعامل مع هجمات حرب الفضاء الإلكتروني وكأنها معادلة لأي هجوم من نوع آخر، بما فيها الضربات الموجهة بالأسلحة المعتادة، ومن ثم الرد بالطريقة التي تختارها الدولة التي تعرضت للاعتداء بحسب حجم الضرر الذي لحق بها وغيره من العوامل المتصلة بالعدوان. ومن أهم الإشكاليات التي

تواجه المجتمع الدولي في طريقة التعامل مع الأسلحة الإلكترونية، فيما يتعلق بالجدل حول مدى اعتبار الأسلحة الإلكترونية مثل الأسلحة التقليدية، وإمكانية أن تخضع لقيود اتفاقيات الحد من التسلح، وهناك تساؤلات حول اعتبار الهجوم الإلكتروني هجوماً مسلحاً وفقاً للقانون الدولي والذي يشترط تحديد المسؤول عن الهجوم، إلا أنه في حالة استخدام أسلحة الفضاء الإلكتروني فأنه يصعب تحديد المسؤول. وتواجه الأسلحة الإلكترونية مشكلات في استخدامها حيث تكون هجماتها عشوائية وذلك لانطلاقها عبر الحدود الدولية، بما قد تعمل على الإضرار بطرف ثالث وبأمن الفضاء الإلكتروني بشكل عام، كما أن الاتفاقيات الدولية لا تحرم الهجمات الإلكترونية على الدول أو على البنية التحتية لهذه الدول[٢٩].

المبحث الثاني

أدوات و تطبيقات حرب الفضاء الإلكتروني

المطلب الأول : أدوات حرب الفضاء الإلكتروني

يتمثل استخدام أدوات حرب الفضاء الإلكتروني في القيام بعمل تخريبي عبر قطع كابلات الاتصالات أو تدمير أنظمة الاتصالات أو الأقمار الصناعية أو استخدام الأسلحة الإلكترونية المتقدمة كالفيروسات في تدمير الأنظمة المعلوماتية لمنشآت حيوية بشكل يؤثر في وظيفتها، ويهدد أمن الدولة أو السكان[٣٠].

ومن أدوات حرب الفضاء هي البرامج الخبيثة، ويستخدم لفظ (*Malware*) أي البرامج الخبيثة للإشارة إلى مجموعة واسعة من البرمجيات كالفيروسات والديدان وحيل تصيد المعلومات. وتحاول هذه البرامج استغلال العيوب الموجودة في البرامج الأخرى والأخطاء التي يقع فيها مستخدمو الحاسوب قبل الدخول إلى المواقع المصابة بالعدوى الفيروسية أو فتح مرفقات الرسائل البريدية. والفيروسات هي برامج يتم تمريرها من مستخدم إلى آخر عبر الإنترنت أو الوسائط المحمولة مثل وحدات التخزين الصغيرة *Flash drivers*. أما الديدان

فلا تتطلب تمرير برنامج إلى مستخدم آخر لأنها قادرة على نسخ نفسها ذاتياً باستغلال عيوب معروفة ثم تزحف كالديدان عبر الإنترنت. أما حيل اصطياد المعلومات (*Phishing Scams*) فتقوم على خداع مستخدم الإنترنت للإدلاء بمعلومات مثل أرقام الحسابات المصرفية وشفرات المرور وذلك عن طريق إنشاء رسائل بريد إلكتروني ومواقع زائفة توهم المستخدم بأنها متعلقة بعمليات تجارية حقيقية كما في حالة المصرف الذي يتعامل معه[٣١].

وقد يقوم محاربو الفضاء الإلكتروني بإنشاء (ثغرة تسلل) أي إنها نفس فكرة حصان طروادة، وثغرة التسلل *Trapdoors* هي برنامج حاسوب غير مرخص يضاف إلى برنامج ما لأغراض خبيثة يسمح بالولوج غير المرخص به إلى شبكة أو برنامج حاسوبي، فغالباً بعد أن يقوم رجال الفضاء الإلكتروني باختراق النظام أو الشبكة لأول مرة فإنهم يتركون وراءهم ثغرة تسلل للسماح لهم بالدخول في المستقبل بطريقة أسرع وأسهل ويشار إليه أيضاً باسم (*Trojan*) نسبة إلى حصان طروادة، وهو استلهام للخدعة التي قام بها محاربو الإغريق لاقتحام طروادة عندما تظاهروا بالانسحاب تاركين وراءهم تمثالاً لحصان خشبي، وقد اختبأت داخله قوة من المحاربين الأشداء وتسللوا إلى طروادة واحتلوا المدينة[٣٢].

وأحياناً تسمح ثغرات التسلل لمقاتلي الفضاء الإلكتروني بالدخول إلى أجزاء معينة من الشبكة لا يسمح لهم بالدخول إليها عادة، وعندما يخترقون برنامجاً ما ولا يزال قيد التطور فأنه لا يسرق نسخة منه فحسب بل قد يضيف إليه شيئاً ما، وأحياناً تسمح لهم ثغرات التسلل بالوصول إلى الجذر (*Root*)، ومعنى ذلك أن لديهم السلطات والصلاحيات التي يتمتع بها مصمم البرنامج أو مدير الشبكة، وإنهم يستطيعون إضافة ما يشاؤون من برمجيات ويمحون أي دليل على وجودهم. وقد يذهب مقاتلي الفضاء الإلكتروني إلى ما هو أبعد من استغلال ثغرات التسلل، وذلك من خلال زرع قنبلة منطقية (*Logic Bomb*) وهو تطبيق من تطبيقات الحاسوب أو سلسلة من التعليمات تسبب توقف النظام أو الشبكة عن العمل و/أو حذف كل البيانات الموجودة على الشبكة، وأن الجيش الأمريكي هو الذي اخترع القنابل المنطقية. وهناك أدوات أكثر تقدماً من القنابل المنطقية يمكنها أن تبدأ بتوجيه أوامر لمعدات الحاسوب

لتقوم بشيء معين يؤدي إلى تدميرها، كأن تأمر شبكة الكهرباء بتوليد حمل كهربائي زائد يؤدي إلى حرق الدوائر الموجودة في محولاتها أو تجعل لوحات التحكم في الطيران تدفع الطائرة إلى السقوط المفاجئ، وبعد ذلك تمحو كل شيء ثم تمحو نفسها أيضاً[٣٣].

ومن أدوات حرب الفضاء الإلكتروني الاخرى، إرسال طوفان من طلبات الاتصال الكترونياً بالأجهزة الخادمة التي تدعم معظم صفحات الإنترنت المستخدمة، وإغراق الأجهزة بهذه الطلبات، وبالتالي تتعطل نتيجة عدم احتمال الحمل الشديد، وعجز عدد آخر من الأجهزة الخادمة نتيجة لتكدس نبضات واستدعاء صفحات لا يمكن الولوج إليها أساساً وبالتالي تسبب عجزاً عن إجراء أي معاملات مصرفية أو الدخول إلى مواقع الصحف أو الانتفاع بالخدمات التي توفرها الحكومة. أو عندما يقوم مستخدم الحاسوب بفتح صفحة على الإنترنت فقد تؤدي إلى تنزيل برنامج يحول هذا الحاسوب إلى جهاز مُستلب وخاضع للتحكم عن بعد، ويمكن للمرء أن يفتح رسالة بريد إلكتروني فيبدأ معها تنزيل البرنامج الذي يتحكم في الحاسوب، وفي بعض الأحيان يبقى الحاسوب المستلب كامناً في انتظار الأوامر، بينما يقوم في أحيان أخرى بالبحث عن أجهزة أخرى لمهاجمتها، وعندما ينشر عدواه إلى أجهزة أخرى تقوم هذه الأجهزة بنقل العدوى إلى أجهزة أخرى لتنشأ الظاهرة المعروفة باسم (العدوى الدودية) بمعنى أن العدوان يستشري ويتغلغل كالديدان من جهاز واحد إلى آلاف أو ملايين الأجهزة، وكل ذلك يمكن حصوله في بضع ساعات فقط[٣٤].

ومن أدوات حرب الفضاء الإلكتروني الأخرى، إنشاء شبكات تجبيرية (مسلوبة الإرادة) (*Botnet*)، وهي شبكة من أجهزة الحاسوب التي تجبر على العمل وفقاً لأوامر مستخدم بعيد غير مرخص له باستخدامها، وعادة ما يتم ذلك من دون علم أصحاب الشبكة أو مديرها، وتستغل هذه الشبكة المكونة من أجهزة الحاسوب الروبوتية في الهجوم على أنظمة أخرى، وعادة ما يتحكم في الشبكة المسيرة حاسوب واحد أو أكثر، وكثيراً ما يشار إلى أجهزة الحاسوب المتصلة بالشبكة المسيرة بكلمة (*Zombies*) أي مسلوبة الإرادة، وتستخدم الشبكات المسيرة لأغراض عديدة، مثل إغراق الشبكات بالرسائل. ومن الأدوات

الآليات الأخرى لحرب الفضاء الإلكتروني هي آلية تخطي الحاجز (*over flow Buffer*) وهي عبارة عن كتابة خطأ في شفرة الحاسوب يسمح لمستخدم غير مرخص له بالدخول إلى شبكة معينة. ويتمثل هذا الخطأ في عدم وضع حد لعدد الحروف والرموز التي يمكن إدخالها من جانب مستخدم غير موثوق به فيتمكن هذا الأخير من إدخال تعليمات إلى نظام البرنامج. ومن الأدوات الأخرى هو قطع خدمة الإنترنت عن طريق الإغراق الموزع (*Ddos*) (*Distributed Denial of Services*)، وهو أسلوب من الأساليب الأساسية لحرب الفضاء الإلكتروني يستخدم لإغراق مواقع معينة على الإنترنت أو جهاز خادم أو راوتر (*Router*) بطلبات للبيانات تفوق طاقة الموقع على الرد أو المعالجة، ونتيجة لهذا الطوفان تعجز التحركات المشروعة عن الوصول إلى الموقع فيصبح في حكم المغلق، وتستخدم الشبكات المسيرة لتنفيذ هذه الهجمات ومن ثم توزعها على آلاف الأجهزة المصدرة للرسالة والتي تعمل معاً في أن واحد. وهناك آلية أخرى وهي آلية التشفير (*Encryption*) وهي خلط المعلومات بطريقة لا يمكن قراءتها لمن ليس لديه مفتاح فك الشفرة، ويؤدي تشفير التحركات (البيانات الكامنة) إلى منع كل من يعترضها أو يحاول سرقتها من قراءتها[٣٥].

المطلب الثاني : تطبيقات حرب الفضاء الإلكتروني

إن الفضاء الإلكتروني الذي يتألف من أجهزة كمبيوتر وأنشطة إلكترونية ذات صلة يشكل بيئة معقدة من صنع الإنسان، والخصوم من البشر يتسمون بالعزيمة والذكاء. من الصعب تحريك الجبال والمحيطات، ولكن من الممكن تشغيل أو إغلاق أجزاء من الفضاء الإلكتروني بكبسة زر. ومن المؤكد أن تحريك الإلكترونات عبر العالم أرخص وأسرع كثيراً من تحريك سفن ضخمة لمسافات طويلة. الأمر الذي يسمح للجهات الفاعلة غير الحكومية والدول الصغيرة بلعب دور كبير بتكاليف زهيدة. ويزعم (جوزيف ناي) أن انتشار القوة بعيداً عن الحكومات يُعَد من أعظم التحولات السياسية التي طرأت على العلاقات الدولية. ويشكل الفضاء الإلكتروني مثالاً ممتازاً. فالدول الكبيرة مثل الولايات المتحدة وروسيا وبريطانيا وفرنسا لديها قدرة أعظم من غيرها من الدول أو الجهات الفاعلة غير الحكومية على السيطرة على

البحر والجو والفضاء، ولكن من غير المنطقي أن نتحدث عن الهيمنة في العالم السيبراني. فمن الواضح أن الاعتماد على الأنظمة الإلكترونية المعقدة لدعم الأنشطة العسكرية والاقتصادية يخلق نقاط ضعف جديدة في الدول الكبرى تستطيع الجهات الفاعلة غير الحكومية استغلالها[٣٦].

وبدأت الولايات المتحدة تعمل على وضع خطط معقدة تمهيداً لهذا النوع من حروب الفضاء الإلكتروني، وبدأت قيادة حرب الفضاء الأمريكية والأجهزة المرتبطة فيها بالعمل على وضع المخططات وتجهيز القدرات اللازمة لتحقيق الهيمنة في الفضاء الإلكتروني. ولما كانت الولايات المتحدة هي التي اخترعت الإنترنت وهي الرائدة اليوم في مجال التجسس الإلكتروني وصنع أدوات حرب الفضاء الإلكتروني، فهي اليوم أصبحت تحمل شيئاً من الغطرسة إلى الحد الذي يجعلها تفترض أنه لا يوجد من يقدر على إخضاعها إلى حرب فضاء إلكتروني. فالولايات المتحدة تعتقد بأن أسلحة حرب الفضاء الإلكتروني تعتبر ميزة أمريكية ويجب استغلال هذه التقنية لتعويض ضعف انتشار القوات الأمريكية على مستوى العالم انتشاراً واسعاً، ولتعويض التطور الهائل في الأسلحة التقليدية الموجودة في يد الخصم المحتمل.

وتعد روسيا والصين من أكثر الدول تمكناً في مجال القوة الإلكترونية والقادرة على توفير أقصى حد من درجات الأمن الإلكتروني، وهو ما فرض على الولايات المتحدة تبني سياسات دفاعية ضد الأخطار المحتملة وحماية نظم المعلومات وتعزيز الأمن الإلكتروني بأبعاده المختلفة[٣٧].

وفي العقد الأول من القرن الحادي والعشرين، قامت الولايات المتحدة الأمريكية بتطوير نوع جديد من الأسلحة وهي أسلحة الفضاء الإلكتروني، وبدأت في استخدامه في صورة منهجية اعتماداً على تقنيات جديدة، وأنشأت قيادة عسكرية لخوض هذا النوع الجديد من الحروب (حروب الفضاء الإلكتروني *Cyber space war*) باستخدام أحدث التقنيات[٣٨].

وكتب العقيد (مايك تانكسلي *Mike Tanksley*) في مقال له في مجلة تايم، عن خوض الولايات المتحدة صراعاتها المستقبلية باستخدام قدرة أقل من القوة بحيث تجبر أعدائها على الخضوع من دون أن تطلق طلقة واحدة بإستخدام محاربو الفضاء الإلكتروني وسيطرتهم على العدو وشل حركته وتدميرهم لنظم التحكم والسيطرة وإصدارهم أوامر زائفة لجيوش العدو، ويصف (مايك تانكسلي) أثر استخدام هذه التكتيكات بأنه سيضع حداً للصراع قبل أن يبدأ، من خلال زرع قنبلة منطقية تظل خاملة داخل أنظمة العدو حتى تأتي اللحظة المطلوبة فتنشط وتبدأ بالتهام بياناته، وهذه القنابل يمكن أن تهاجم أجهزة الحاسوب التي تتحكم في نظام الدفاع الجوي أو الطيران أو المصارف... الخ[٣٩]. وفي عام ٢٠٠١ تم إنشاء مكتب خاص بالبيت الأبيض لتنسيق التعامل مع مشكلة الأمن الإلكتروني، ونتيجة لذلك تم وضع الإستراتيجية الوطنية لتأمين الفضاء الإلكتروني التي وقعها الرئيس الأمريكي (جورج دبليو بوش) عام ٢٠٠٣. وفي عام ٢٠٠٧ قام الرئيس الأمريكي (جورج دبليو بوش) بإصدار المبادرة الوطنية الشاملة لتأمين الشبكات (*PDD54*)، وهي وثيقة سرية تضم الخطوات الواجب إتباعها لتعزيز الدفاعات الحكومية ضد حرب الفضاء الإلكتروني، وطالب بوش بتدبير مبلغ (٥٠) مليار دولار على مدى خمسة سنوات للمبادرة الوطنية الشاملة لتأمين الشبكات[٤٠].

وفي الوقت الذي بدأ فيه (جورج دبليو بوش) رئاسته الثانية كانت أهمية حرب الفضاء الإلكتروني قد صارت واضحة تماماً للبنتاغون، من خلال إنشاء قيادة لحرب الفضاء الإلكتروني، تشترك فيها أفرع القوات المسلحة على أن تظل خاضعة للقيادة الإستراتيجية، وفي تشرين الأول ٢٠٠٩ فتح باب الانضمام إلى قيادة حرب الفضاء الإلكتروني الأمريكية والتي تشمل عدة أفرع رئيسة بالجيش. و تولى أحد جنرالات الجيش الأمريكي رئاسة هيئة عسكرية جديدة في الولايات المتحدة الأمريكية تعرف بقيادة (حرب الفضاء الإلكتروني)، مهمتها استخدام تقنيات المعلومات والانترنت كسلاح للحرب. وتقوم قيادة حرب الفضاء الإلكتروني في الولايات المتحدة الأمريكية بتجهيز ساحة حرب الفضاء الإلكتروني بما يطلق

عليه القنابل المنطقية (*Logic bombs*) وثغرات التسلل (*Trapdoors*)، ووضع متفجرات افتراضية في الدول الأخرى في وقت السلم[٤١].

وتسيطر على الولايات المتحدة بشأن موضوع حرب الفضاء الإلكتروني النظرية القائلة بأن الفضاء الإلكتروني (نطاق) أو ساحة تدور فيها رحى الحرب ويجب أن تهيمن عليها الولايات المتحدة. ويلاحظ أن ضرورة اتخاذ الولايات المتحدة المبادرة في حرب الفضاء الإلكتروني هي مسألة تمليها عدة عوامل منها : أن التحركات التي تتم في الفضاء الإلكتروني تتم بسرعة لم تشهدها حرب من قبل، الفضاء الإلكتروني يسمح بدرجة كبيرة من المناورات العملياتية وبسرعات تقترب من سرعة الضوء وتتيح دائماً للقادة فرصاً مختلفة للتأثير بسرعة لم يمكن لأحد أن يتصورها من قبل. كما تلاحظ الإستراتيجية أن المرء أن لم يسارع بالتحرك فربما لا يستطيع التحرك لأن الهدف الذي كان ضعيفاً من قبل قد يحل محله هدف آخر وقد يتم تزويده بدفاعات جديدة دون سابق إنذار، مما يجعل عمليات الفضاء الإلكتروني أقل فاعلية. أي أن المرء لو انتظر الجانب الآخر ليبدأ بالهجوم عليه في الفضاء الإلكتروني، فقد يكتشف أن غريمه في لحظة الهجوم نفسها لم يحذف قنابله المنطقية أو فصل الأهداف عن مسارات الشبكة التي أراد المرء استخدامها للوصول إلى هذه الأهداف.

ودعا الرئيس باراك أوباما أثناء حملته الانتخابية إلى وضع معايير جديدة صارمة لتوفير الأمن السيبراني وضمان قدرة البنية الأساسية الحرجة على الصمود في مواجهة الهجمات، كما وعد بتعيين مستشار للأمن السيبراني الوطني والذي سيكون تابعاً له مباشرة ومسؤولاً عن وضع الخطة السياسية اللازمة وتنسيق جهود الوكالة الفيدرالية. لكن لم تكن هذه بالمهمة السهلة، وذلك لأن القسم الأعظم من البنية الأساسية المطلوبة غير خاضع للسيطرة الحكومية المباشرة[٤٢]. وقد أوضح الرئيس (باراك اوباما) عام ٢٠٠٩ في المبادرة الوطنية الشاملة لأمن الفضاء الإلكتروني، بأن الأمن الإلكتروني هو أحد التحديات الوطنية الجادة التي تواجه الأمة الأمريكية. ووافق الرئيس (اوباما) عام ٢٠٠٩ على قبول التوصيات التي توصلت اليها مراجعة سياسة أمن الفضاء الإلكتروني، والتي تضمنت إنشاء فرع تنسيق تنفيذي لأمن الفضاء

الإلكتروني، والذي سيضمن إستجابة موحدة منظمة للحوادث المستقبلية لأمن الفضاء الإلكتروني، وإنشاء قوة لحماية أمن الفضاء الإلكتروني، وهذه المبادرة بنيت على المبادرة الوطنية الشاملة لأمن الفضاء الإلكتروني في عهد الرئيس (جورج دبليو بوش)[٤٣]. وقد ميّز الرئيس (باراك اوباما) أهمية الفضاء الإلكتروني، وحدد هيكلية ومصادر الأمن الإلكتروني القائم، وأعلن عن إنشاء مركز الفضاء الإلكتروني للإشراف على تهديدات الفضاء الإلكتروني المتصاعدة، وأمر الرئيس (اوباما) بمراجعة شاملة لسياسات وهيكليات أمن الفضاء الإلكتروني[٤٤].

وقبل أيام من الحملة العسكرية على ليبيا في مارس ٢٠١١ قامت الولايات المتحدة بتحريك ترسانتها الإلكترونية صوب ليبيا وتجري الولايات المتحدة سنوياً محاكاة التعرض لحرب الفضاء الإلكتروني وتم تخصيص (٥٠٠) مليون دولار في ميزانية عام ٢٠١٢ لمواجهة التهديدات الإلكترونية وتطوير أسلحة وأدوات لحرب الفضاء الإلكتروني[٤٥].

وجاء الهجوم الإلكتروني بفيروس (ستانكس نت) على برنامج إيران النووي عام ٢٠١٠ ليمثل نقلة مهمة في مجال تطور أسلحة الفضاء الإلكتروني[٤٦]. ويمثل النموذج الإيراني حالة فريدة لتحول الفضاء الإلكتروني لساحة قتال بأشكال متعددة في إطار المواجهة بين الولايات المتحدة وإيران، فقد استخدم الفضاء الإلكتروني في شن هجمات تخريب للبرنامج النووي الإيراني للعمل على تعطيله، ففي ١٧ فبراير ٢٠١٢ أعلنت الاستخبارات الإيرانية أن فيروس (ستانكس نت) أصاب ما يقدر بستة عشر ألف جهاز كومبيوتر[٤٧].

وفي عام ٢٠٠٧ تعرضت (استونيا)؛ إحدى جمهوريات الاتحاد السوفيتي السابق، والتي تتميز بتوافر خدمات الإنترنت فيها وانتشار الشبكات ذات السرعة العالية واستخدام تطبيقات الإنترنت في مجال الحياة اليومية؛ إلى هجوم من مجموعة واسعة من الأجهزة لتعطيل خدمة الإنترنت فيها، ويتلخص هذا الهجوم في كونه طوفاناً مبرمجاً من الحركة المصممة عبر شبكة الإنترنت بغرض تعطيل الشبكات عن العمل أو خنقها وهي موسعة أو منسقة، بمعنى أن آلافاً أو مئات الآلاف من أجهزة الحاسوب الموزعة في أماكن مختلفة من العالم تستغل في

إرسال نبضات الاستدعاء الإلكترونية إلى مجموعة من مواقع الإنترنت المستهدفة، ويطلق على أجهزة الحاسوب المهاجمة لفظ (*robotic network*) أي شبكة مسيرة (مسلوبة الإرادة) مكونة من مجموعة من أجهزة الحاسوب الخاضعة للتحكم عن بعد في هذه الأجهزة المستلبة، وتتبع تعليمات تم إدخالها إلى الأجهزة دون علم أصحابها، وصاحب الجهاز لا يعرف متى أستلب جهازه ومن قام باستلابه. وسرعان ما بدأت الشبكات المستلبة في (استونيا) في استهداف عناوين الأجهزة الخادمة التي تدير شبكات الاتصال الهاتفية في البلاد، ونظام التحقق من هوية مستخدمي البطاقات الائتمانية، وقد بدأ مصرف هانز بانك (*Hans bank*) في الترنح وتأثرت التجارة والاتصالات. وزعمت (استونيا) أن أجهزة التحكم النهائية كانت في روسيا، وان الشفرة الحاسوبية المستخدمة في هذه العملية كانت مكتوبة بالألفبائية السلافية، من جانبها أنكرت الحكومة الروسية باستياء شديد أن لها يداً في حرب الفضاء الإلكتروني على استونيا، كما رفضت طلباً دبلوماسياً رسمياً من استونيا بمساعدتها في تعقب المعتدين على الرغم من وجود اتفاقية ثنائية بين البلدين[٤٨].

وعندما احتدم الصراع على بعض الأقاليم الصغيرة المتنازع عليها بين جورجيا (وهي إحدى جمهوريات الاتحاد السوفيتي) وبين روسيا الأم، في تموز ٢٠٠٨، قامت جورجيا بغزو (أوسيتا الجنوبية) وسارع الجيش الروسي بإخراج الجورجي من إقليم (أوسيتا الجنوبية)، وفي نفس الوقت الذي تحرك فيه الجيش الروسي تحرك محاربوه الإلكترونيون أيضاً. فقبيل اندلاع القتال في عالم الواقع وفي المراحل الأولية، وجه محاربو الفضاء الإلكتروني الروس ضربات لتعطيل خدمة المواقع الحكومية الجورجية، واخترقوا جهاز الخادم الخاص بموقع الرئيس لتشويهه بوضع صور تقارن بين الرئيس الجورجي (ميخائيل ساكاشفيلي) و (أدولف هتلر)، ومع اندلاع القتال البري اشتدت الهجمات الإلكترونية في حدتها ودرجة تعقيدها[٤٩]. وفي شهر آب ٢٠٠٨ عندما تحركت القوات الروسية إلى داخل جورجيا، هاجم المتخصصون في اختراق أنظمة الحاسب الآلي مواقع الحكومة الجورجية على شبكة الإنترنت في الأسابيع التي

سبقت اندلاع الصراع المسلح. وهذا الصراع بين روسيا وجورجيا يمثل أول الهجمات السيبرانية (الإلكترونية) التي تصاحب صراعاً مسلحاً. مرحباً في القرن الحادي والعشرين[٥٠].

وقد اتجه حلف الناتو بعد عجزه عن مواجهة الهجمات على استونيا عام ٢٠٠٧ وجورجيا عام ٢٠٠٨ إلى تكوين وحدة للدفاع الإلكتروني مقرها (تالين) عاصمة إستونيا، كما تم تطوير المفهوم الاستراتيجي للحلف بحيث أصبح الفضاء الإلكتروني منطقة لعملياته، ومن مهامه تطوير قدراته الدفاعية الإلكترونية بما يشمل مساندة ودعم حلفائه الذين يتعرضون لهجمات الكترونية[٥١].

وفي تموز ٢٠٠٩ أرسلت كوريا الشمالية رسالة مشفرة إلى (٤٠٠) ألف حاسوب حول العالم وهي محملة بفايروس للسطو على الشبكات، وتضمنت الرسالة مجموعة من التعليمات التي تجعل الحاسوب يبدأ في إرسال النبضات المطالبة بالاتصال بقائمة من مواقع الإنترنت الخاصة بالولايات المتحدة الأمريكية وحكومة كوريا الجنوبية وعدد من الشركات الدولية، وعندما يتم تشغيل الأجهزة فإنها تنظم إلى الهجوم. فتعرضت المواقع الأمريكية لحمل بلغ مليون طلب في الثانية مما أدى إلى اختناق الأجهزة الخادمة، فتعطلت الأجهزة الخادمة للخزانة العامة والخدمة السرية وهيئة التجارة الفيدرالية ووزارة النقل وبورصة نيويورك وموقع هيئة البريد بواشنطن. ويبدو أن هجوم كوريا الشمالية هو لم يكن مجرد عدوى دودية انطلقت في غياهب الإنترنت وسمح لها بالانتشار، بل أن هناك من يتحكم في الهجوم ويوجه ويعدل قائمة الأهداف. وقد أعلنت كوريا الشمالية عن مخططات لإنشاء قيادة للحرب الإلكترونية بحلول عام ٢٠١٢، ولو شنت كوريا الشمالية ضربة الكترونية فان خيارات الرد عليها ستكون قليلة نسبياً، فليس من الممكن تشديد العقوبات أكثر مما هي عليه اليوم، كما أن أي عمل عسكري غير وارد على الإطلاق، كما أن احتمالات الرد بالطريقة نفسها محدودة للغاية، لأن كوريا الشمالية ليس لديها الكثير مما يستحق المهاجمة من جانب الولايات المتحدة أو كوريا الجنوبية[٥٢].

(١) هذه الوقائع تشير إلى أنها أول صدام علني بين الدول في عالم الفضاء الإلكتروني، وهناك أمثلة أخرى لعمليات قامت بها الصين وتايوان و(إسرائيل) وغيرها. وقد أطلق البعض على حادثة استونيا مصطلح (*WWI*) وهو مختصر (*Web War One*) أي الحرب الأولى على الشبكة العنكبوتية والذي يتطابق مع المختصر الشهير للحرب العالمية الأولى (*WWI*) مختصر (*World War One*).

(٢) وبالنسبة للصين، فقد عملت الصين على الاستثمار في التقنيات الجديدة ومنها تقنية بناء الشبكات للتعامل مع ساحة حرب الفضاء الإلكتروني، وبنهاية عقد التسعينات كان الخبراء الإستراتيجيون الصينيون قد اتفقوا على فكرة مفادها أن الصين يمكن أن تستخدم حرب الفضاء الإلكتروني تعويضاً عن قصورها العسكري الكيفي مع الولايات المتحدة الأمريكية. وبحلول عام ٢٠٠٣ أعلنت الصين عن إنشاء وحدات حرب الفضاء الإلكتروني، وهاتان الوحدتان هما المسؤولتان على الهجوم والدفاع على شبكة الإنترنت. وفي الوقت الذي أعلنت فيه الصين عن إنشاء وحدات حرب الفضاء الإلكتروني، تعرضت الولايات المتحدة لأسوأ عملية تجسس إلكتروني أطلق عليه اسم (مطر العمالقة *Titan Rain*) وفيها تم سحب ما يتراوح من (١٠–٢٠) تيرا بايت من المعلومات من شبكة البنتاجون وشركة المقاولات الدفاعية (لوكهيد مارتن *Lockheed Martin*) وغيرها من المواقع العسكرية. وبحلول عام ٢٠٠٧ بدا أن الحكومة الصينية منخرطة في سلسلة واسعة من عمليات اختراق الشبكات الأمريكية والأوربية، ونسخ وتصدير وإتلاف كميات كبيرة من البيانات[٥٣]. وقد اتهمت الولايات المتحدة الصين مراراً وتكراراً باختراق شبكاتها الإلكترونية، حيث اتهمتها باختراق نظم المعلومات لأقمارها الصناعية في الفضاء الخارجي، لكن مسؤولي الاستخبارات الأمريكية لا يعتبرون أن الصين هي التهديد الأول للولايات المتحدة الأمريكية في مجال حرب الفضاء الإلكتروني لأنهم يعتبرون الروس أفضل منهم، بل ويفوقون الولايات المتحدة في قدراتهم[٥٤].

الخاتمـــــة

مما تقدم نجد أن حروب الفضاء الإلكتروني انتقلت من مجرد فكرة خيالية إلى تطبيق مادي ملموس وأصبحت بعض الدول المتقدمة في مجال الحاسبات والأنترنت والفضاء الإلكتروني قادرة على شن هجمات على غيرها من الدول، وأصبح الفضاء الإلكتروني أحد أبرز القضايا على الصعيد الدولي، وفرض إعادة التفكير في مفهوم الامن. فقد أدى التطور الكبير والاستخدام الكثيف للتكنولوجيا إلى وزيادة اعتماد الدول على شبكة الإنترنت إلى زيادة احتمالات تعرض الدول لهجمات وحروب الفضاء الإلكتروني، وساعد على ذلك وجود عيوب في تصميم الإنترنت والمعدات والبرمجيات والإتجاه المتزايد لتوصيل القطاعات والخدمات والبنى التحية على شبكات الفضاء الإلكتروني، و لجأت الدول المتقدمة إلى هذه النوع من الحروب، لمجموعةٍ من الأسباب، أهمها محاولة تجنب العمل العسكري المباشر، ومحاولة تقليل الخسائر المادية والبشرية التي تترتب على العمل العسكري المباشر، وتجاوز الرأي العام الداخلي و الدولي، فضلاً عن أن هذه الحروب لا تحتاج إلى ساحات معارك كبيرة مثل المعارك التقليدية.

وتتميز هذه الحروب بأنها لا تحتاج إلى ساحات معارك تقليدية، وتمتاز بالسرية التامة، وأنها تشجع على شن الهجوم، فهي تتحرك بسرعة الضوء ومن الصعوبة تقفي اثر المعتدي، كما أنها لا حدود لها، حيث يتشارك الافراد والدول الفضاء الإلكتروني، وهذا الطابع المميز اطمس الحدود الفاصلة بين حالة السلم وحالة الحرب، وخلقت مجالاً لعدم الاستقرار في العلاقات الدولية.

وخلقت هذه الحروب نوعاً من التحديات أمام الدول، من حيث طريقة التعامل مع هذه الحروب، ومدى اعتبار الأسلحة الإلكترونية مثل الاسلحة التقليدية، ومدى إمكانية أن تخضع لقيود وإتفاقيات، ومدى إمكانية اعتبار الهجوم الإلكتروني هجوماً مسلحاً وفقاً لقواعد القانون الدولي العام.

ولعل أكبر أسرار عالم حرب الفضاء الإلكتروني يتلخص في أن بعض الدول بينما لديها القدرة على خوض حرب الفضاء الإلكتروني ولكنها ليست متفوقة في الدفاع الإلكتروني، فالبنية التحتية (بما في ذلك الطاقة الكهربية والتمويل والاتصالات السلكية واللاسلكية والرعاية الصحية والنقل والمياه والدفاع والإنترنت) عرضة للأخطار بسبب ارتباطها واعتمادها على شبكات الإنترنت. وفي مجال الفضاء الإلكتروني، فالغلبة لتلك الدول التي لاتعتمد بصورة كبيرة على الفضاء الإلكتروني، أو تلك الدول التي تستطيع فصل شبكاتها عن الإنترنت.

وهناك مجموعة من الدول الفاعلة في مجال الفضاء الإلكتروني، في مقدمتها الولايات المتحدة والصين وفرنسا، إلا أنه توجد عشرين دولة أخرى لديها بعض القدرات في هذا الصدد مثل إيران وكوريا الشمالية وكوريا الجنوبية وتايوان. وقد شهد العالم نماذج عديدة من حروب الفضاء الإلكتروني، مثل هجوم الصين على الولايات المتحدة عام ٢٠٠٧، وهجوم روسيا على إستونيا عام ٢٠٠٧، وعلى جورجيا ٢٠٠٨، وهجوم كوريا الشمالية على الولايات المتحدة عام ٢٠٠٩، وهجوم الولايات المتحدة على مفاعل ايران النووي عام ٢٠١٠.

إن الحكومات تتعلق بالأمل في ردع حروب الفضاء الإلكتروني تماماً كما تعمل على ردع الهجمات النووية أو غيرها من الهجمات المسلحة. بيد أن الردع يتطلب فرض تهديد أو رد فعل قوي في مواجهة المهاجمين. وهذا النوع من الردع يصبح أكثر صعوبة في عالم حيث تجد الحكومات صعوبة بالغة في تحديد مصدر هجمات الفضاء الإلكتروني، وما إذا كانت قادمة من دولة معادية أو مجموعة إجرامية تتخفى في هيئة حكومة أجنبية. وبالتالي فقد أصبح الفضاء الإلكتروني مصدراً رئيسياً لانعدام الأمن.

الهـــوامـــش

(١)عادل عبد الصادق، القوة الإلكترونية :أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، السياسة الدولية، مركز الأهرام للدراسات السياسية والإستراتيجية، مصر، العدد ١٨٨، ٢٠١٢، ص٢٨.

(2) *Arsenio T. Gumahad , Cyber Troops and Net Wars : The Profession of Arms in The Tnformation Age , Air war college , April , 1996 , p57-66.*

(3) *Tim Jordan, Cyber Power: The Culture and Politics of Cyberspace and the internet, Rutledge, 2000, p160-175.*

(4) *Tim Jordan, Cyber Power: The Culture and Politics of Cyberspace and the internet, Rutledge, 2000, p160-175.*

(5) *Gabriel Weismann, Terror on The Internet: The New Arena, The New Challenges, United States institute of peace press, 2006, p243.*

(٦) ريتشارد كلارك وروبرت نيك، حرب الفضاء الإلكتروني : التهديد التالي للأمن القومي وكيفية التعامل معه، مركز الإمارات للبحوث والدراسات الإستراتيجية، الإمارات العربية المتحدة، ٢٠١٢، ط١،ص٨.

(٧) عادل عبد الصادق، القوة الإلكترونية :أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، مصدر سبق ذكره، ص٢٨.

(٨) ريتشارد كلارك وروبرت نيك، المصدر السابق، ص٩٣.

(٩) المصدر نفسه، ص٥٣.

(١٠) عادل عبد الصادق، القوة الإلكترونية :أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، مصدر سبق ذكره، ص٣١.

(11) *Martin C. Libicki , Conquest in Cyber Space : National Security and Warfare , New York , Cambridge University press , 2007 , p13.*

(١٢) عادل عبد الصادق، المصدر السابق، ص٣٣.

(١٣) علي حسين باكير، الحروب الإلكترونية في القرن الحادي والعشرين، مركز الجزيرة للدراسات، قطر، ٧ ديسمبر٢٠١٢.

(١٤) ريتشارد كلارك وروبرت نيك، مصدر سبق ذكره، ص٩٨.

(١٥) عادل عبد الصادق، القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، مصدر سبق ذكره، ص٢٩.

(16) *Joseph S. Nye, Cyber War And Peace, project syndicate, 10April 2012, http//:www.project-syndicate.org/commentary/cyber-war-and-peace*

(١٧) جوزيف س. ناي، الحرب والسلام في الفضاء الإلكتروني، بحث منشور على شبكة المعلومات الدولية، ٢٠٠٥/٢/٢٤، ص ١، الموقع :

(18) *http//www.project-syndicate.org/commentary/presedent-push-gose-soft/Arabic*

(19) *Ibd.p1*

(20) *Michael Chertoff, The Cyber Domain And The Evolution of Smart Power , in: Dealing with Today's Asymmetric Threat to U.S And Global Security, Symposium Three, :Employing Smart Power, March 24,2009,Co-Sonsored by U.S Naval Institute,p28-30,The Internet : http: // www. asymmetricthreat.net.*

(21) *Jenn M. Williamson , Information Operations : Computer network attack in the 21st century , US Army War college , 2002 , p15.*

(٢٢) ريتشارد كلارك وروبرت نيك، مصدر سبق ذكره، ص٩٣ – ٩٤.

(٢٣) المصدر نفسه، ص٩٠.

(٢٤) عادل عبد الصادق، القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، مصدر سبق ذكره، ص٣٢.

(٢٥) ريتشارد كلارك وروبرت نيك، المصدر السابق، ص٤٨–٤٩.

(26) *Michael Chertoff, op.cit.p 25.*

(٢٧) ريتشارد كلارك وروبرت نيك، مصدر سبق ذكره، ص٢٥٣.

(٢٨) المصدر نفسه، ص٢٤٩.

(٢٩) عادل عبد الصادق، القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، مصدر سبق ذكره، ص٣٤.

(٣٠) عادل عبد الصادق، الإنترنت والإتصالات : ساحة جديدة للتجسس الدولي، المركز العربي لأبحاث الفضاء، ٢٠١١، *http//www.accr.com.co1/= p341.*

(٣١) ريتشارد كلارك وروبرت نيك، مصدر سبق ذكره، ص١٠٧.

(٣٢) المصدر نفسه، ص٣٣٥.

(٣٣) المصدر نفسه، ص١١٩–١٢٠.

(٣٤) المصدر نفسه، ص٢٨.

(٣٥) المصدر نفسه، ص٣٢٤–٣٢٧.

(36) *Joseph S. Nye, Cyber War And Peace, op.cit.p1-2.*

(٣٧) عادل عبد الصادق، القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، مصدر سبق ذكره، ص٣١.

(٣٨) ريتشارد كلارك وروبرت نيك، مصدر سبق ذكره، ص٨.

(٣٩) نقلاً عن : المصدر نفسه، ص١٣٢.

(٤٠) المصدر نفسه، ص١٤٢–١٤٣.

(٤١) المصدر نفسه، ص٥٣.

(42) *Joseph S. Nye, Cyber Insecurity, project syndicate,p1, Dec10, 2008, http//:www.project-syndicate.org/commentary/cyber-insecurity*

(43) *The Comprehensive National Cyberspace Security Initiative ,Published by : Executive Office of The President Of the United States,2009,p1.See also :www.whitehose.org/issues/foreign-policy/cybersecurity/national-initiative*

(٤٤) عادل عبد الصادق،القوة الإلكترونية : أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني،المصدر السابق،ص٢٨.

(٤٥) عادل عبد الصادق، القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، مصدر سبق ذكره، ص٣٣.

(٤٦) عادل عبد الصادق، الإنترنت والدبلوماسية ومعركة القوة الناعمة بين الولايات المتحدة وإيران، مختارات إيرانية، مركز الأهرام للدراسات السياسية والإستراتيجية، مصر، ٢٠١١،ص٢٢.

(47) *Michael Chertoff, , op.cit.p30.*

(٤٨) ريتشارد كلارك وروبرت نيك، مصدر سبق ذكره، ص٢٨–٣١.

(٤٩) المصدر نفسه، ص٣٢–٣٤.

(50) *Joseph S. Nye, Cyber Insecurity, op.cit.p2.*

(٥١) عادل عبد الصادق، القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، مصدر سبق ذكره، ص٣٣.

(٥٢) ريتشارد كلارك وروبرت نيك، مصدر سبق ذكره، ص٣٩-٤٣.

(٥٣) المصدر نفسه، ص٧٠-٧٢.

(54) *Misha Glenny, The Cyber Arms Race Is On, October 23, 2011, www.post-gexzettle. Com/p8/113849/11-109-MTY.*

المصـــــادر

(١) جوزيف س. ناي، الحرب والسلام في الفضاء الإلكتروني، بحث منشور على شبكة المعلومات الدولية، ٢٠٠٥/٢/٢٤، ص ١، الموقع :-*http//www.project-syndicate.org/commentary/presedent-push-gose-soft/Arabic*

(٢) ريتشارد كلارك وروبرت نيك، حرب الفضاء الإلكتروني : التهديد التالي للأمن القومي وكيفية التعامل معه، مركز الإمارات للبحوث والدراسات الإستراتيجية، الإمارات العربية المتحدة، ط١، ٢٠١٢.

(٣) عادل عبد الصادق، الإنترنت والإتصالات : ساحة جديدة للتجسس الدولي، المركز العربي لأبحاث الفضاء، ٢٠١١، *http//www.accr.com.co1/= p341.*.

(٤) عادل عبد الصادق، القوة الإلكترونية :أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، السياسة الدولية، مركز الأهرام للدراسات السياسية والإستراتيجية، مصر، العدد ١٨٨، ٢٠١٢.

(٥) عادل عبد الصادق، الإنترنت والدبلوماسية ومعركة القوة الناعمة بين الولايات المتحدة وإيران، مختارات إيرانية، مركز الأهرام للدراسات السياسية والإستراتيجية، مصر،٢٠١١.

(٦) علي حسين باكير، الحروب الإلكترونية في القرن الحادي والعشرين، مركز الجزيرة للدراسات، قطر، ٧ ديسمبر٢٠١٢.

(7) Arsenio T. Gumahad , Cyber Troops and Net Wars : The Profession of Arms in The Tnformation Age , Air war college , April , 1996.

(8) Gabriel Weismann, Terror on The Internet: The New Arena, The New Challenges, United States institute of peace press, 2006.

(9) Jenn M. Williamson , Information Operations : Computer network attack in the 21st century , US Army War college , 2002.

(10) *Joseph S. Nye, Cyber Insecurity, project syndicate,p1, Dec10, 2008, http//:www.project-syndicate.org/commentary/cyber-insecurity*

(11) *Joseph S. Nye, Cyber War And Peace, project syndicate, 10April 2012, http//:www.project-syndicate.org/commentary/cyber-war-and-peace.*

(12) *Martin C. Libicki , Conquest in Cyber Space : National Security and Warfare , New York , Cambridge University press , 2007.*

(13) *Michael Chertoff, The Cyber Domain And The Evolution of Smart Power , in: Dealing with Today's Asymmetric Threat to U.S And Global Security, Symposium Three, :Employing Smart Power, March 24,2009,Co-Sonsored by U.S Naval Institute,p28-30,The Internet: http://www.asymmetricthreat.net.*

(14) *Misha Glenny, The Cyber Arms Race Is On, October 23, 2011, www.post-gexzettle. Com/p8/113849/11-109-MTY.*

(15) *The Comprehensive National Cyberspace Security Initiative ,Published by : Executive Office of The President Of the United States,2009,p1.See also :www.whitehose.org/issues/foreign-policy/cybersecurity/national-initiative.*

(16) *Tim Jordan, Cyber Power: The Culture and Politics of Cyberspace and the internet, Rutledge, 2000.*

Cyber Space War
Concept – Tools and Applications

Lecturer Dr. Anmar Mosa Jawad
Yarmouk University College

Abstract

In the twenty first century, due to the increasing reliance of developed countries on the Internet networks, and infrastructure's link with these networks. Cyberspace has emerged to form a new dimension and another challenge for the countries. Countries are no longer afraid of attacks that might occur on land, air or sea territory only, but they become alarmed by a new kind of war, a cyberspace war that take the Internet networks and computer as a scene of war.

These wars have new effective theaters and arenas that ceased the actual defensive value-border point of view. Furthermore, it legally terminate the relationship between war and peace creating a state of instability and increased state of security disclosure. Which require a reformulation of the concept of security in line with new developments in the concept of cyberspace.

These wars has a range of features motivating parties initiating attack using certain types of tools and weapons with special properties that do not need to store and cannot be controlled, reduced or removed just like traditional weapons.

These wars are not just scenes of fiction, but they have been applied in reality among nations. World has witnessed cyber space wars that accompanied to with states of an armed conflict, and cyber space war by itself.