أنماط الحروب الالكترونية وتداعياتها على الامن العالمي

Electronic warfare patterns and its repercussions on global security

م.د. الهام عطية عواد

PhD. Alham ateaa awaad

alham.ateaa@gmail.com

تاريخ الاستلام 2024/6/9 تاريخ القبول 2024/6/30 تاريخ النشر 2024/10/30

ملخص

تعد الحروب الإلكترونية شكلاً جديداً من الحروب التي تتطور في الوسائل والاساليب، وحتى النتائج التي تتوصل اليها الحروب العسكرية. إذ تتم في فضاء واسع للغاية تخترق الحدود الجغرافية بسرعة وسهولة بالإعتماد على تكنولوجيا المعلومات والاتصال بالاسلحة الالكترونية لإلحاق الضرر بالخصم. وتمتد ابعد من الجوانب العسكرية اذ يمكن ان تشمل استهداف البنية التحتية الحيوية مثل الكهرباء والمياه والاتصالات، وكذلك الهجمات التي تستهدف القطاعات الإقتصادية والمالية.

Abstract

Cyberwarfares are a new form of warfare that develops in means, methods, and even the results reached by military wars. It takes place in a very wide space, crossing geographical borders quickly and easily, relying on information like technology and communication with electronic weapons to harm the opponent. It extends beyond military aspects, as it can include targeting vital infrastructure such as electricity, water,

and communications, as well as attacks targeting the economic and financial sectors.

الكلمات المفتاحية: الحروب، الفضاء الالكتروني، الامن الدولي، التقدم التقني.

Keywords: wars, cyberspace, international security, technical progress.

المقدمة

دخل المجال الإلكتروني ميادين الحروب، كما البر والبحر والجو والفضاء، حيث السمة الغالبة إن لم تكن الرئيسة، ومن المتوقع أن تكون الحرب الإلكترونية للحروب المستقبلية في القرن الواحد والعشرين.

وكانت أساليب الحرب الإلكترونيَّة تستعمل منذ بداية هذا القرن، ولا سيّما عندما استُخْدِمت أجهزة الاتِّصالات اللاسلكية في الحروب، ولكن منذ الحرب العالمية الثانية أصبَح موضوع الحرب الإلكترونية محلَّ الاهتمام، من حيث المعدات والأساليب.

وتكمن خطورة حروب الإنترنيت والشبكات في كون العالم أصبح يعتمد أكثر فأكثر على الفضاء الإلكتروني لاسيّما في البنى التحتية المعلوماتية العسكرية، والمصرفية، والحكومية ، فضلاً عن المؤسسات والشركات العامة والخاصة. ولا شك أنّ ازدياد الهجمات الإلكترونية والتي نشهد جزءًا بسيطا منها اليوم يرتبط أيضا بازدياد هذا الاعتماد على شبكات الكومبيوتر والإنترنيت في البنية التحتية الوطنية الأساسية، وان شيوع البنى التحتية المعلوماتية الالكترونية الرقمية أدى إلى شراسة الهجمات المعلوماتية التي يمكن أن تمزق النسيج الاجتماعي للبلد المستهدف إلى جانب القدرة على إلحاق اضرار مادية واسعة بسبب الطاقات والقدرات التدميرية للهجمات المعلوماتية المتواصلة والمتاحة للجميع من افراد أو مؤسسات أو دول. وهو ما يعني إمكانية تطوّر الهجمات الإلكترونية اليوم لتصبح سلاحاً حاسماً في النزاعات بين الدول في المستقبل، علما أنّ أبعاد

مفهوم الحرب الإلكترونية لا تزال غير مفهومة لدى شريحة واسعة من المراقبين وحتى العامة.

أهمية البحث

ان السنوات الاخيرة شهدت تغييرات وتحولات جذرية في مفاهيم الحرب ونظرياتها والعقائد القتالية للجيوش، فقد شهد العقد الاول والثاني من القرن الحادي والعشرين مؤشرات ومتغيرات كثيرة افرزت بيئات عمل جديدة دفعت دول العالم الى إعادة بناء تصوراتها المستقبلية لأمنها القومي، وباتت تتكيف مع التغييرات الحاصلة في موازين القوى الدولية غير التقليدية وبالاخص التتكنولوجية منها والتي تتطلب ان يواجهها تخطيط استراتيجي متقن، فتجلت الحروب الالكترونية على ارض الواقع وهبطت من الفضاء النظري الذي رسم سناريوهاتها وتأثيرات المحتملة بما تترتب عليه من عمق الخطر الاستراتيجي المحدق بامنها القومي الشامل والتي دفعت الامن المعلوماتي ليشغل صدارة اولويات الامن القومي الدولي.

إشكاليه البحث

مع بروز الفضاء الالكتروني كساحة للصراع العالمي واجه الامن الدولي بصورة عامة تحديات واضحة خاصة لجهة مدى ملائمتها أو حتى تكيفها مع طبيعة التفاعلات في الواقع الافتراضي، لذا برزت الحاجة الى معرفة وتفسير طبيعة التغيرات التي ألحقتها الحقائق التكنولوجية بهذا المفهوم ومن هنا تدور المشكلة البحثيه حول **التساؤل الرئيسي** وهو **:كيف أثر الفضاء الالكتروني علي مفهوم الأمن الدولي ؟**

فرضية البحث

مفاد الفرضية "أن حروب المستقبل سوف تشهد تطورات جذرية تقلب المفاهيم والمقاييس العسكرية رأساً على عقب، بفعل تطور وتنوع تأثير مخرجات الثورة التقنية والمعلوماتية التي نشرت تأثيرا على كافة المجالات".

مناهج البحث

اعتمد البحث على أكثر من منهج كالآتي:

- المنهج الوصـفي: يقوم المنهج الوصـفي على تفسـير ظاهرة الفضـاء الإلكتروني والحروب التي تُدار فيه وتحديد خصـائص تلك الحروب، بالإضـافة إلى وصـف طبيعـة العلاقـة بين هذه الحروب والأمن القومي للدول، من خلال جمع البيانـات الوصفية حول واقع الحروب الإلكترونية.
- منهج دراسـة الحالة: من خلال إعتماد الحروب الإلكترونية في ميدان الفضـاء الإلكتروني الواسـع كنموذج؛ لتوضـيح مدى تأثير هذه الحروب على أمن الدول باستراتيجياتها المختلفة ورصد أبرز نماذج هذه الحروب.
- يمكن اسـتخدام منهج المقارنة لتوضـيح مدى التباين بين الحروب الالكترونية والحروب التقليدية القديمة.

هيكلية البحث

تم تقسـيم البحث الى ثلاث مطالب رئيسـة، المطلب الأول: يتناول مفهوم الحرب الالكترونية وخصـائصـها، المطلب الثاني: يتناول أنماط وتداعيات الحروب الالكترونيـة، المطلـب الثالـث: يتنـاول تـداعيـات الحروب الالكترونيـة على الأمن العالمي، والخاتمة، وقائمة المصادر.

المطلب الأول

مفهوم الحرب الإلكترونية وخصائصها

تختلط المفاهيم على الكثيرين ما بين الحرب الالكترونية والحرب السـيبرانية، فالأخيرة تشـكل جزءاً من الأولى، لكن ميدانها الطيف الكهرومغنطيسـي الموجود شـبكات الكومبيوتر والأجهزة المتصـلة بشـبكة الانترنت، بينما تأخذ الأولى طابعاً عسكرياً أكثر في المعارك ما بين القوى العسكرية.

ان الحرب الالكترونية هي المسـتوى الأخطر للصـراع في الفضـاء الإلكتروني، وتعد جزءاً من الحرب المعلوماتية بمعناها الأوسع، وتهدف إلى التأثير

على إرادة الطرف المستهدف السياسية وعلى قدرته في عملية صنع القرار، وكذلك التأثير فيما يتعلق بالقيادة العسكرية وتوجهات المدنيين في مسرح العمليات الإلكتروني.

وتتضمن حرب الإلكترونية سلسلة هجمات تستهدف الأنظمة المعلوماتية للدول والجهات المعادية، وبحيث تشن عبر الفضاء الإلكتروني، بغرض سرقة أو تخريب البيانات أو المنشآت المرتبطة بها .وقد باتت الدول تعتمد وبشكل متزايد على اعتماد خيار الهجمات الإلكترونية وذلك في إطار الحروب والصراعات والأزمات المندلعة بينها، وبحيث باتت خياراً بديلاً يتم تفضيل اللجوء إليه في كثير من الحالات على اللجوء إلى استخدام ميدان القوة التقليدي .وهو ما يأتي بسبب من خصائص عديدة تتمتع بها هذه الحروب، تجعلها خياراً مفضلاً لدى الدول، فهي تبقى أقل كلفة، وأقل عبئا ًمن ناحية المسائلة والتبعات، نظراً لما تتسم به من سرية وغموض، وذلك مع قدرتها في كثير من الأحيان على تحقيق الأهداف المرجوة المتملتلفة في توجيه الضربات وإلحاق الضرر بالخصم.

أولاً: تعريف الحروب الإلكترونية

بفضل ما أحدثته الثورة التكنومعلوماتية من ثورة في المجال الإلكتروني، أصبح الفضاء الإلكتروني، تبعاً لذلك، مرشحاً بقوة لأن يكون ساحة جديدة لصراعات وحروب تُدار بأسلحة وأدوات مختلفة تماماً، بالشكل والمضمون عن تلك الحروب التي تعتمد على الأسلحة التقليدية .وهنا، جاء ظهور مسمى حروب الفضاء الإلكتروني، أو (الحروب السيبراني) ، والتي أصبح لها قواعد اشتباك خاصة مختلفة عن تلك الموجودة في الحروب التقليدية. وقد غيرت حروب الفضاء الإلكتروني من طبيعة الحرب ذاتها؛ فهي لا تستهدف في غاياتها تدمير الآلات والمعدات العسكرية والقوات البشرية للعدو، ولا تهدف للاستيلاء على أرض العدو واحتلالها، وانما إلحاق الضرر البالغ ببناه التحتية بأقل كلفة ممكنة. [1]

وتعرف الحرب الالكترونية بأنها "حرب تخيلية او افتراضية ذات طبيعة غير ملموسة تحاكي الواقع بشكل شبه تام، وهي حرب قد تكون بلا دماء، إذ تتلخص ادوات الصراع فيها بالمواجهات الالكترونية والبرمجيات التقنية وجنود من برامج التخريب المحوسب وطلقاتها لوحات المفاتيح ونقرات المبرمجين في بيئة اصطناعية تحاول ما امكن الوصول الى صورة حقيقية لملامح الحياة المادية والملموسة".[2]

وعند تعريف حروب الفضاء الإلكتروني، لا بد من الإشارة إلى الجهود الفكرية لعدد من المعنيين بدراسة حروب الفضاء الإلكتروني، منها ما تقدم به **(جون أركويلا وديفيد رون)**، اللذان عرفا حروب الفضاء الإلكتروني بأنها "اجراء، أو استعداد لإجراءات عمليات عسكرية بالاعتماد على المبادئ والآليات المعلوماتية، ما يعني تعطيل، أو تدمير، نظم المعلومات والاتصالات في الدولة العدو" [3]

كما عرفتها **(ماريا روزايا تاديو)**، الباحثة في معهد أكسفورد للإنترنت، بأنها " حرب تركز على استخدامات معينة لتكنولوجيا المعلومات والاتصالات ضمن استراتيجية عسكرية هجومية أو دفاعية، أقرتها الدولة، وتهدف إلى التعطيل الفوري أو السيطرة على موارد العدو، والتي تشن داخل بيئة المعلومات، مع أهداف تتراوح ما بين الصعيد المادي، والمجالات غير المادية، والتي قد يختلف مستوى الدمار فيها حسب طبيعة وحجم الهجوم [4]

فيما عرفت **(وزارة الدفاع الأمريكية)** حرب الإلكترونية بأنها "توظيف القدرات السيبرانية، وذلك بهدف تحقيق غرض أساس، يتمثل في تحقيق الأهداف أو الآثار العسكر ية في الفضاء السيبراني أو من خلاله.

وقد عرف **(مجلس الأمن الدولي)** حرب الإلكترونية بأنها "هي استخدام أجهزة الحاسوب، أو الوسائل الرقمية، من قبل حكومة، أو بمعرفة، أو موافقة صريحة من تلك الحكومة ضد دولة أخرى، أو مُلكية خاصة داخل دولة أخرى،

بما في ذلك :الوصـــول المتعمد أو اعتراض البيانات، أو تدمير البنية التحتية الرقمية، وانتاج وتوزيع الأجهزة التي يمكن استخدامها لتخريب النشاط المحلي"[5]

ومن هذه التعاريف يمكن أن نســتدل، أن حروب الفضــاء الإلكتروني لها أدوات جديدة ومســرح جديد، وميدان جديد، هو الفضــاء الإلكتروني والذي يمكن تعريفه بأنه: المجال الخامســة للحرب، يُضــاف إلى المجالات التقليدية الأربعة: البحر، اليابسة، الجو، الفضاء. وهو يشير إلى البيئة التي أنشأها التقاء الشبكات التعاونية لأجهزة الحاسوب، والبنى التحتية للاتصالات المستخدمة لربطها، وكل ما يتصل بهذه الشبكات من معدات وأجهزة يتم التحكم بها من خلالها. [6]

أما بخصـــوص طبيعة وماهية عمليات الهجوم الالكتروني فهي تشـــمل عمليات التســـلل إلى أنظمة الحاســـب الآلي، وجمع البيانات، أو تصـــديرها، أو إتلافها، أو تغييرها، أو تشـــفيرها، كما تشـــمل عمليات زرع برمجيات ضـــا رة للتجسـس . ان الهجمات الإلكترونية تشـمل أشـكال كثيرة، من سـرقة المعلومات، والتجسس، ونشر معلومات سر ية وفضـح الأنظمة السياسـة لأغراض التحريض، ونشر أفكار مضادة، وخلق تيارات معارضة، واثارة احتجاجات. وما زاد من تحدي الحروب الإلكترونية هو القدرة على توظيف الفضـــاء الإلكتروني من قبل فاعلين من غير الدول، يمتلك البعض منهم قدرات تقنية قد تفوق ما تمتلكه الحكومات؛ إذ أن أسلحة الفضاء الإلكتروني ليست حكراً على الدولة، قد يمتلكها فرد أو جماعة إرهابية وهي بذلك تعتبر إحدى أشكال الحرب اللامتناظرة. [7]

ثانياً: خصائص الحروب الالكترونية

وقد جاء التحول المتزايد من قبل الدول والفاعلين السـياسـيين نحو الاعتماد بصورة متزايدة على خيار المواجهة في الفضاء الإلكتروني بسبب ما تتمتع به من خصائص:

1- **تكلفتها:** قلة تكلفة المواجهة فيها نسبياً، بالمقارنة مع الحروب التقليدية فهي لا تحتاج لمعدات وجيوش مجهزة، كما أن احتمالية وقوع الضـحايا والخسائر البشرية

في صـــفوف القوة المهاجمة تكون منعدمة .وبالتالي، فإن التوجه المتزايد نحوها يأتي من مبدأ السعي لتحمل أقل كلفة، مع إلحاق أكبر ضرر بالعدو.[8]

2- مبدأ إخلاء المسؤولية: ولا يقف تدني الكلفة عند النواحي المادية والبشرية، وانما تكون كذلك أيضاً من ناحية المسؤولية. إذ أن هذه الهجمات تضمن تحقيق مبدأ إخلاء المسؤولية، وذلك بالنظر إلى صعوبة تحديد الجهة والمكان الذي صدر منه الهجوم .وكذلك إمكانية التلاعب والتمويه العالية فيما يتعلق بمصـــدر ومكان توجيه وشن الهجوم الإلكتروني، إضافة إلى إمكانية استخدام سلسلة من الوكلاء في شن الهجوم بما يبددا احتمالية تتبع مباشر للدولة صاحبة القرار في شن الهجوم[9]

3- احدثت تغيرات على مســتوى الأهداف وعلى مســتوى الفاعلين: من ناحية الأهداف، فإن هذه الحروب تتجه نحو اســتهداف بنك متنوع من الأهداف، فهي تستهدف البنى التحتية المدنية، ولا تقتصـر على العسكرية والأسـاس في الهدف بالنسبة لها هو أن يكون مرتبطاً بشبكات المعلومات، وهو ما بات يتوافر بشكل متزايد في شتى مناحي الحياة والمصـالح الحيوية حول العالم، وذلك بفعل التحول المتســارع نحو الرقمنة لمختلف الأنشــطة والمنشــآت. بحيث باتت التعاملات التجارية معتمدة على الفضـاء الإلكتروني، وكذلك الصـحة والتعليم، وصـولاً حتى شبكات المياه والكهرباء، والمؤسسات والمعاملات الحكومية وفي ظل القدرة على اســتهداف شــبكات الكهرباء، والمياه، والطاقة، وشــبكات النقل، والنظام المالي، والمنشآت الصناعية كل ذلك أدى إلى توسعة بنك الأهداف المتاحة أمام هجمات أسلحة الفضاء الإلكتروني، وبوساطة فيروس يمكنه إحداث أضرار مادية حقيقية تؤدي إلى وقوع انفجارات أو دمار هائل، وكل ذلك يتم دون إطلاق رصـــاصـــة واحدة. ما يمكن اعتباره بمثابة عملية تدمير صـــامتة وخفية. **وعلى مســـتوى الفاعلين،** تركت حروب الفضــاء الإلكتروني تاثيرات هامة في طبيعة المواجهات، حيث بات بالإمكان أن يكون هناك أطراف فاعلة من غير الدول، إذ أن الأسلحة

المستخدمة في هذه الحروب ليست حكراً بيد الدولة، إذ بات يتردد الوصف لحروب الفضاء الإلكتروني بأنها حروب غير تناظرية.[10]

4- فشل إمكانية تطبيق فكرة ومبدأ الردع في حروب الإلكترونية: والتي عادة ما تستخدم من قبل دولة ضد دولة أخرى في إطار منظومة الحروب التقليدية أو النووية، أما في الحروب الإلكترونية فهذا الجانب غائب إذ يتعذر إظهار القوة الإلكترونية المهاجمة، بحيث يتم ردع العدو عن الهجوم .فالردع بالانتقام أو العقاب لا ينطبق على هذه الحروب، وحتى إذا ما تم تتبع مصدر الهجمات الإلكترونية، وتبين أنها تعود إلى دول محددة، أو فاعلين غير حكوميين، فإنه في هذه الحالة لن يكون لديهم قواعد أو فضاءات مادية حتى يتم الرد إليها عبر استهدافها .كما أن بعض الهجمات قد تتطلب اشهرا ًلرصدها، وهو ما يلغي مفعول الردع بالانتقام، عبر توجيه ضربة تالية للضربة الأولى التي وجهها الطرف البادئ بالهجوم.[11]

5- انعدام الحدود والسيادة: وهي أنه لا توجد حدود جغرافية واضحة في هذه الحروب .كما لا يتواجد مفهوم" السيادة"، بمعناه السائد في العالم الواقعي، بحيث يتم منع الأطراف الأخرى من الدخول إلى المناطق الخاضعة لسيادة دولة ما مثلاً، بل إنه بالإمكان وصف الحدود في الفضاء الإلكتروني بأنها حدود مائعة . وبالأحرى، فإنه لا توجد حدود في العالم الافتراضي، إذ أن الحدود تتداخل مع بعضها، حيث كل الدول، صغيرة وكبيرة، تشترك في نفس الشبكات، التي يمكن اعتبارها بمثابة سحابة واحدة . وحتى خوادم الشبكات تكون في كثير من الأحيان موجود في بلدان أخرى، غير البلدان المستخدمة لها والمشغلة لها .وبالتالي فإنه بالإمكان التأكيد على أن مفهوم السيادة في العالم الإلكترونية مفهوم مائع، وذلك مما يقتضيه طبيعة العالم الافتراضي المتداخلة. [12]

المطلب الثاني

أنماط الحروب الإلكترونية

إن أشـــكال الحرب الإلكترونية على الإنترنت متعددة وأدواتها متغيرة، ويتفنن المحاربون في ابتكار أساليب جديدة يوماً بعد يوم ويجب على القطاعات العسكرية بشـــكل خاص أن تكون على معرفة كبيرة بطبيعة الحرب الإلكترونية، وأن تكون مستعدة لحروب من هذا النوع، وتشير العديد من التقارير إلى تزايد أعداد الهجمات الإلكترونية التي تتم في العالم اليوم والتي تقوم بها مجموعات أو حكومات تتدرج في الاستهداف من أبسط المستويات إلى أكثرها تعقيداً وخطورة.

أنماط الحروب الإلكترونية

قد تنوعت وســـائل الســـيطرة والتحكم الخاصـــة بمعظم العمليات الحيوية الموجودة على الأرض، وانتقلت إلى عالم الفضـــاء الالكتروني وفي صـــورة متعددة منها أقمار صناعية ومحطات فضائية، كما انتقل أيضاً قطاع واسع من الحروب والمعارك والصراعات والثورات إلى العالم الافتراضي، الذي خلقه الإنسان منذ اختراعه للكمبيوتر والذاكرات الإلكترونية وشـــبكات المعلومات، فأنشـــأ داخله جغرافية افتراضية جديدة ، وأخذ الصراع الالكتروني حيزاً واسعاً من خرائط الصراع الدولية ، وادخلت اساليب جديدة ومختلفة وهي مفاهيم بحاجة الى تقييم وصياغة، هذا ما سيتم التطرق إليه على وفق الشكل الأتي:

- **الحروب الموجهة:**

يســتند هذا النوع من الحروب على المعلوماتية ، إذ انه يكفي لقهر الخصـــم والنجاح فيها عن طريق الوصـــول الى هياكل القيادة ووســـائل الاتصـــال مع المؤســـســـات الفكرية لديه، و كذلك تســـتند هذه الحروب على القنابل الذكية التي اســـتخدمت في حرب الخليج الثانية عام (1991)، وقنابل الغرانيت القادرة على تصـفير دوائر المراكز الكهربائية والتي اسـتخدمت اخيراً ضـد الصـرب في حرب كوســـوفو، وكذلك القنابل التي اســـتخدمت في الحرب الامريكية على العراق عام

(2003)، اذ انه في حالة الصراع تصبح المعارك هدفاً للمواجهة وليس فقط ما يتيح الهجوم او الصدام في الظرف الملائم. [13]

وكان اخر تطبيق عملي لهذه الحرب في العراق عام (2003)، من خلال اعتماد الولايات المتحدة على استراتيجية (الصدمة والترويع)، التي تقوم على قدرة تكنولوجية متطورة ومنظومات تسليحية متكاملة وقادرة على تطبيق التأثير المستهدف من اجل التأثير في ارادة الخصم وادراكه، وتتطلب هذه الاستراتيجية عدة عناصر لنجاحها، هي المعرفة الكاملة بالذات والخصم والبيئة، ويشمل ذلك معرفة كاملة بالعمليات الذهنية والمنظومات التقنية لقادة الخصم وجماهيره ، والسرعة في جميع مراحل العمل العسكري سواء في المناورات او التحركات داخل الميدان وضمان السيطرة على العمليات سواء على الارض او في مجال الاشارات اللاسلكية والبنية الاساسية للاتصالات بما يضطر الخصم الى الاستسلام خوفاً من تعرضه لدمار واسع. [14]

كما ان الحرب الموجهة تستخدم اكثر الاسلحة ذكاءاً وتتطلب وجود قوات ووحدات صغيرة ومترابطة لكي تتمكن من تنسيق هجماتها بشكل متكرر، ومن ابرز الدول التي تمتلك هذه القوات هي الولايات المتحدة وفرنسا وكندا وبريطانيا. [15]

ويجمع الخبراء على أنّ الهجوم الإلكتروني الذي استهدف أستونيا في العام 2007، يكاد يكون الهجوم الإلكتروني الأول الذي يتم على هذا المستوى ويستخدم لتعطيل المواقع الإلكترونية الحكومية والتجارية والمصرفية والإعلامية مسبباً خسائر بعشرات الملايين من الدولارات إضافة إلى شلل البلاد. وعلى الرغم من أنّ الشكوك كانت تحوم حول موسكو على اعتبار أن الهجوم جاء بعد فترة قصيرة من خلاف أستوني–روسي كبير، إلا أنّ أحداً لم يستطع تحديد هوية الفاعل الحقيقي أو مصدر الهجوم الذي تم، وهي من المصاعب والمشاكل التي ترتبط بحروب الإنترنيت إلى الآن. [16]

- **الحروب الشبكية:**

وهو شـكل جديد من اشـكال الحروب التي تمكن من التأثير على نشـاطات واعمال الخصـم ولا سـيّما إذا كان مجتمع الخصـم متطوراً ويعتمد بدرجة كبيرة على وسائل المواصلات والاتصالات، اما إذا كان الخصم اقل تطوراً في اعتماده التقنيات الحديثة فان اسـاليب حروب الشـبكات كالفعاليات التقنية والتشـويش لن يكون مؤثراً بالدرجة المطلوبة، ومن ثم سـيتم الاعتماد على الاسـلحة التقليدية المعروفة والتي تعتمد على الدقة في الاصابة والسرعة في الاستجابة، لذا فان حروب الشبكة موجهة بشـكل اسـاس نحو تحجيم العدو، ومن ثم هي تختلف عن الحرب الموجهة التي تكون نحو شل قدرة العدو العسكرية [17]

كالهجوم الذي وقع في السـابع والعشـرين من حزيران/يونيو عام 2017 م، وفي ظل الأزمة المسـتمرة بين روسـيا وأوكرانيا حول شـبه جزيرة القرم والمناطق الشـرقية والجنوبية الشـرقية من البلاد، بدأت سـلسـلة من الهجمات الروسـية الإلكترونية على مواقع المنظمات والمؤسـسـات الأوكرانية، بما في ذلك البنوك والوزارات والصـحف وشـركات الكهرباء، واسـتخدم المهاجمون الروس فيها برامج خبيثة من نوع (بيتا)، وأدى الهجوم إلى تعطيل أنظمة المعلومات وتوقف أجهزة الحاسـوب، مع مطالبة بدفع فدية بالعملة الإلكترونية (بيتكوين)، التي لا يمكن تعقبها .وأوضحت السلطات الأوكرانية لاحقاً أن طلب الفدية كان مجرد ستار، وأن الهجوم كان يهدف إلى تعطيل أعمال الشـركات الحكومية والخاصـة في أوكرانيا، واحداث زعزعة سياسية في البلاد. [18]

- **الحروب التجسسية:**

ان التقدم التقني اصـبح واحد من اهم مفاتيح المسـتقبل وعامل حاسـم للسـيطرة في النظام العالمي الجديد، لذا أصـبحت المنافسـة شـديدة في الميدان التكنولوجي والسـياسـي والاسـتراتيجي، لان من سـيحصـل على التكنولوجيا فانه سـيسـيطر في المجالات الاخرى, لذا يرى بان جزء كبير من الاتصـالات العالمية تسـيطر عليها

اجهزة الامن والاجهزة المخابراتية، إذ ان هذه الاجهزة تراقب كل شيء تقريباً وينتشر وكلاء متخصصون في كل بلدان العالم مدعومون بأقمار صناعية تجسسيه لجمع المعلومات والعمل مع الالاف من الاذاعات والقنوات، وكل ذلك يتجه لهدف واحد الا وهو التجسس على العالم، فالوكالات الامنية تنتشر في كل بلدان العالم وتسعى وتتنافس وبكل الطرق للحصول على المعلومات، مستخدمة كل الوسائل المتاحة بعملية تصارع اشبه بالحرب ذاتها من هنا انطلقت حرب التجسس هذه ، فالدول تسعى لانفاق ثروتها على قواعدها التنصتية ونصب وسائل ذات تقنية عالية الكفاءة للتجسس على العالم. (19)

وفي يوليو/ تموز 2010، أعلنت ألمانيا أنّها واجهت عمليات تجسس شديدة التعقيد لكل من الصين وروسيا كانت تستهدف القطاعات الصناعية والبنى التحتية الحساسة في البلاد ومن بينها شبكة الكهرباء التي تغذي الدولة.

ففي ديسمبر/كانون الأول من العام 2009، أوردت الحكومة الكورية الجنوبية تقريراً عن تعرضها لهجوم نفّذه قراصنة كوريين شماليين بهدف سرقة خطط دفاعية سريّة تتضمن معلومات عن شكل التحرّك الكوري الجنوبي والأمريكي في حالة حصول حرب في شبه الجزيرة الكورية. (20)

في التاسع عشر من كانون الأول /ديسمبر من العام 2018 ، ذكرت شركة (آريا سيكيوريتي) الأميركية المتخصصة في أمن المعلومات، ان وحدة إلكترونية تابعة لجيش التحرير الشعبي الصيني، تعمل بأوامر من الحكومة الصينية، اخترقت شبكة اتصالات يستخدمها الاتحاد الأوروبي لتنسيق السياسات الخارجية ، إذ تمكن القراصنة من الوصول إلى آلاف البرقيات الدبلوماسية، بحسب صحيفة نيويورك تايمز التي قدمت لها الشركة (1100) برقية نشرت مجموعة منها. ومن هذه التقارير ما يتضمن تحليلات لتوجهات السياسات العالمية والتجارة، وخصوصا دور الصين وتحولات سياساتها تحت حكم الرئيس (شي جينبينغ)، وكذلك علاقات

الاتحاد الاوربي مع كل من روســـيا والولايات المتحدة الأمريكية، ولمحات من اجتماعات مغلقة. [21]

- **الحرب النفسية:**

ففي عصـرنا الحالي لابد من القيام بحروب ذات وسـائل متطورة وجديدة، لها آثار كبيرة ليس على الجانب المادي بل تفتك قبل ذلك بالجانب المعنوي والروحي للإنسـان، ونحن لا نقول بأن هذا النوع من الحروب وليد هذا العصـر ولكنه أسلوب قديم، لكن التكنولوجيا هي من جعلت منه أشــد فتكاً بالبشــرية في الإعلام التقليدي بداية ووصــولاً إلى الأنترنت ومواقعها الإجتماعية التي تم الاسـتثمار فيها بكثرة في إحباط الروح المعنوية للأفراد عن طريق الدعاية، الإشـــاعة، الأخبار الزائفة، والتي كلها تعتبر أحد وسـائل الحرب النفسـية المتعلقة بالمعلومات الموجهة للسـيطرة على نفسية الإنسان.[22]

وهناك من يرى ان الحرب النفســية "هي التي يســتخدمون فيها الدعاية من اجل التأثير على اشــخاص بين اوســاط العدو" وثمة من اعتبرها "عمليات تســتخدم فيها وسـائل الاقناع على نحو غير عنفي لتحقيق اهداف الحرب العسـكرية "، وقد حاول الباحث (بول الينبارجر) الذي عمل في مكتب المعلومات الحربية الامريكي خلال الحرب العالمية الثانية في كتابه (الحرب النفسـية) الاخذ بكل هذه التعاريف وتدوير رؤى النظر المختلفة، إذ عرف الحروب النفسية "بانها استخدام الدعاية ضد العدو مع اجراءات عملية اخرى ذات طبيعة عسكرية او اقتصاديه او سياسية" ، في حين ذهب الباحث (حامد ربيع) بتعريف الحرب النفســية "بأنها نوعاً من القتال لا يتجه الا الى العدو"، وهي بذلك خلاف الدعاية التي تتعدد فيها الرؤى ، كما انها تعد فناً حربياً لا يسعى الا للقضاء على الارادة الفردية والجماعية للعدو. [23]

ويتضـــح ان تنظيم داعش الارهابي قد أهتم بشـــكل كبير في حربه بالعراق بالجانب النفســي االعالمي حتى أصــبح له فرق كاملة متخصــصــة بنشــر اعماله الاجرامية مستغل وسائل العالم الالكتروني خاصـة شبكات التواصـل الرقمي كمنابر

لبث افكاره واخباره وتنفيذ اجندته بسبب الانتشار المكوكي لهذه الشبكات وامكانية تخطي الحواجز السياسية والجغرافية في عملية الاتصال وايصال رسائله لتحقيق استراتيجيته. وهكذا نرى أن التنظيم تنظيم داعش الإرهابي قد أهتم بشكل كبير في حربه بالعراق بالجانب النفسي العالمي حتى أصبح يوظف ويستغل وبشكل منهجي ومنظم حربه النفسية الالكترونية، وهو يعرف كيف يحصل على أفضل النتائج من الانفعالات الطبيعية لدى الجمهور وارباك صناع القرار. [24]

- **الحرب الفضائية:**

منذ عام (1983) سعت الولايات المتحدة الامريكية لتطوير برنامج حرب النجوم او منظومة الدفاع الاستراتيجي وامتلاك القدرة المطلقة على صد اي هجوم صاروخي، ومنذ ذلك الوقت طور الفضاء العمليات العسكرية الارضية في مجال المراقبة والاتصالات والملاحة والرصد الجوي بحيث عمقت التكنولوجيا مفهوماً جديداً يخص الميدان والجبهة على كل الابعاد يدعى بالجبهة متعددة الابعاد.

وان ظهور ما سمي بحرب النجوم التي ماهي إلا حرب اوسع تتضمن فقط البدء بوضع اسلحة في مدارات حول الارض تمكنها من تدمير القاذفات الاستراتيجية والصواريخ النووية خلال ثوان معدودة من اطلاقها، ومثل هذا الاحتمال اذا ما قدر له ان يتحول الى حقيقة فانه سيغير مشهد الحرب عامه، فتفتقد الصواريخ العابرة للقارات فاعليتها وجدواها وبذلك نكون قد انتقلنا الى مرحلة من الاسلحة الاستراتيجية مصممة لتدمير المجتمعات، اسلحة قادرة على تدمير اسلحة الدمار الشامل، وعلى الرغم من انتهاء الحرب الباردة قاد الى تراجع اهمية هذا المشروع للمؤسسة العسكرية – الصناعية الامريكية، إلا انه سرعان ما ان تصاعد وتيرة العودة للحديث عن هذا المشروع والبدء في عملية تطويره، وكذلك الكتمان الذي يحيط بالأبحاث الفضائية والمبالغ الضخمة التي تنفق على غزو الفضاء كافية لتثبت ان الامر ليس بحثاً علمياً خالصاً لمنفعة الإنسانية.[25]

وبذلك فإن التكنولوجيا المتقدمة قد بدلت من روحية وديناميةمنظومة القيادة والسيطرة والحاسبات والاتصالات والمراقبة والاستطلاع والاستخبارات في الحروب والعمليات العسكرية فضلاً عن ذلك اصبحت المسافة التي تفصل بين المستوى التكتيكي والاستراتيجي قليلة جداً ، إذ يمكن للمستوى الاستراتيجي قيادة العمليات التكتيكية مباشرة وعن بعد ، وتعد عملية قتل زعيم تنظيم القاعدة (إسامة بن لادن) في عام (2011)، مثالاً حياً على ذلك فقد كانت فرقة صغيرة من القوات الخاصة تقوم بالعملية والرئيس الامريكي مع طاقم مجلس الامن القومي الامريكي يتابعون العملية مباشرةً . [26]

وقد أحدث استخدام معدات الحرب الإلكترونية في الحروب الحديثة تطوراً هائلاً في مجالات هذه الحروب ومراحلها، وأصبح الحسم في المعارك الحديثة لصالح الجيوش والقوات التي تستخدم الحديث منها، وبقدر ما يمتلكه كل طرف من الأطراف المتصارعة، بعد أن كانت تحسم لمصلحة الطرف الذي يمتلك التفوق العددي، أو النوعي، أو يمتلك الأسلحة البعيدة المدى، والدليل على ذلك أن معدات الحرب الإلكترونية المستخدمة في الطائرات المقاتلة يقترب ثمنها من نصف قيمة الطائرة.[27]

في نهاية عقد التسعينات من القرن الماضي برزت الهجمات الإلكترونية المتبادلة بين الهند وباكستان، وذلك على خلفية النزاع طويل الأمد بين البلدين بشأن كشمير، إذ انتقلت المواجهات إلى الفضاء الإلكتروني، مع بدء المتسللين من كل دولة المشاركة في مهاجمة نظام قاعدة بيانات الحوسبة للدولة الأخرى . وقد زاد عدد الهجمات الإلكترونية سنويا ًبين البلدين تصاعادياً، من (45) هجمة في عام 1999 الى (133) في عام 2000 و (275) في عام 2001. [28]

وفي كانون الأول/ ديسمبر 2020 ، تعرضت الولايات المتحدة الأمريكية لهجمات إلكترونية واسعة، شملت عمليات قرصنة إلكترونية واسعة النطاق، استهدفت وكالات حكومية أميركية، من بينها إدارة الأمن النووي، ووزارات الدفاع

والخارجية والطاقة والخزانة، وشـــركات خاصـــة مرتبطة بالحكومة الفيدرالية إثر الهجوم نقلت صحيفة وول ستريت جورنال عن مسؤول أميركي استخباري قوله "إن التوصـــل إلى معرفة أبعاد عملية القرصـــنة الإلكترونية الأخيرة وتجاوُز تداعياتها يحتاج إلى أشـهر إن لم يكن سـنوات"، وأضـاف" إن أبعاد العملية مذهلة وكبيرة بالنظر إلى طبيعتها الحذرة والمتخفية، وأن أكثر ما يزعج فيها هو عدم القدرة حتى الآن على تحديد أنظمة الكمبيوتر المتأثرة" .[29]

بالرغم من أن روسيا نفت مسؤوليتها عن الهجوم، فإن عدداً من المسؤولين الأميركيين أصـــروا على اتهامها بالســـؤولية عن هذا الاختراق الكبير، ومنهم من أشار إلى أن مجموعة" كوزي بير" المرتبطة بأجهزة الاستخبارات الروسية، هي من قامت بالهجوم. وفي موقف يؤيد ما ذهب إليه العديد خبراء الاستخبارات الأمريكية، قال السـيناتور الجمهوري، ماركو روبيو، أنه "يتضـح بشـكل متزايد أن المخابرات الروسـية هي من نفذت أخطر اختراق إلكتروني في تاريخ الولايات المتحدة" وعقب الهجوم توعد الرئيس المنتخب حديثاً في وقتها، جو بايدن، توعد الروس، باعتبار أنهم يقفون وراء الهجوم الإلكتروني الواسـع، وأكد أن الأمن السـيبراني سـيكون من بين أولويات إدارته . كما وجه وزير الخارجية الأمريكي (مايك بومبيو) الاتهام إلى روســيا والرئيس الروســي (بوتين) بالوقوف وراء الهجمات، وقال "يمكننا أن نقول بوضـوح تام أن الروس هم من شاركوا في هذا النشاط"، بالرغم من عدم تقديمه أي تفاصيل تعزز اتهامه. [30]

المطلب الثالث

تداعيات الحروب الإلكترونية على الأمن العالمي

تزايـدت العلاقـة بين الأمن والتكنولوجيـا ومعهـا تزايـدت إمكـانيـة تعرض المصـــالح الإســـتراتيجية للدول للتهديدات الســـيبرانية بل وهددت بتحول الفضـــاء الإلكتروني لوسـيط ومصـدر لأدوات جديدة للصـراع الدولي متعدد الأطراف. ومع تزايد النزاعات والصـــراعات في الفضـــاء الإلكتروني؛ بســـبب حالة إنعدام الثقة بين

الدول إضـــافة إلى التطورات الهائلة في الفضـــاء الإلكتروني، التي جعلت الدول تُســارع لتبني تغيرات في العقيدة الأمنية لديها وذلك بإدراج القوة الســيبرانية كمحدد رئيســي لمدى قوة الدولة وقدرتها على حســم الصــراعات، مما ســاعد على وجود الصـــراعات والحروب في الفضـــاء الإلكتروني بين الفواعل الدولية والفواعل غير الدولية وعلى إثر ذلك أصـــبح هناك أمننة لقضـــية الحروب الإلكترونية، وجعلها قضية هامة تمس الأمن القومي للدول.

1. ســـببت الحروب الإلكترونية العديد من المخاطر والتهديدات للأمن القومي للدول سواء من خلال أساليب عملها مثل التجسس الإلكتروني والهجوم الإلكتروني أو من خلال النتائج المادية التي تُحدثها؛ فعلى **المســتوى العســكري** أدت الحروب الإلكترونية إلى تصاعد المخاطر السيبرانية خاصة مع قابلية المنشآت الحيوية في الدولة للهجوم وبالتالي التأثير في وظائف تلك المنشـــآت والتحكم في تنفيذ هذه الهجمات يُعد أداة اســـتراتيجية، ولعبت الحروب الإلكترونية دوراً هام في عســـكرة الفضاء الإلكتروني وبالتالي تصاعدت القدرات في سباق التسلح السيبراني وتبني سياسات دفاعية سيبرانية في مجال تطوير أدوات الحرب الإلكترونية داخل الجيوش الحديثة، عملت الحروب الإلكترونية على إختراق المخططات العسكرية للدولة، مما ساعد على التعرف على طبيعة القوة العسكرية للدولة وتكتيكها العسكري وبالتالي ذلك يســـاعد على التحكم في مواجهة الدول المســـتهدفة ســـواء في ميدان الحرب التقليدي أو في الفضاء الإلكتروني. [31]

2. على **المستوى الإقتصادي**، قد تستهدف الهجمات الإلكترونية توقف الإنترنت كلياً في الدولة المُستهدفة، مما يؤدي لتوقف المعاملات البنكية ومعاملات الحكومة الإلكترونية وســـرقة أرقام وتفاصـــيل بطاقات الائتمان التي يتم التســـوق بها عبر الإنترنت، مما ينتج عن ذلك تعطل تدفق الأموال في الدولة وبالتالي توقف أهم القطاعات في الدولة مثل الصـــناعة وغيرها من قطاعات الدولة، على **المســـتوى النفســـي**؛ قد تســتهدف الهجمات الإلكترونية إحداث حالة من الهلع في الدولة مثل

إختراق المواقع الإلكترونية وإعلان حالة الطوارئ مما يثير القلق لدى المواطنين ويتسبب في إحداث حرب نفسية. [32]

3. على **المستوى الثقافي**، قد تستهدف الحرب الإلكترونية مسخ هوية الدولة من خلال الترويج لأفكار الدولة المُهاجمة بأساليب تستهدف شباب الدولة وتُأثر على أفكاره ومعتقداته وهذا ما يُعرف بالغزو الثقافي الذي يستهدف إختراق البنية الفكرية للمجتمعات من خلال إختراق العقول عبر زرع أفكار تُدمر الإبداع وتُعرقل التنمية الشاملة في الدولة، وهذا ما تستخدمه العديد من الفواعل غير الدولية مثل التنظيمات الإرهابية التي تستهدف الشباب وتجعله يتخذ مسلكاً وطريقاً ضد دولته وغمسه في الأفكار المُتطرفة، وكل هذا يتم عن طريق مواقع التواصل الإجتماعي والقنوات الفضائية .

4. **على المستوى السياسي**، قد تستهدف الحرب الإلكترونية إثارة الفتن في الدولة وشحن الشعب ضد السلطة الحاكمة وخطابات بث الكراهية من خلال مُخاطبة الشعب بأن هناك العديد من المخاطر التي تُحيط بالدولة وأن السلطة الحاكمة لا توفر الإحتياجات الأساسية للشعب وكذلك مُطالبة شعب الدولة المُستهدفة بالحصول على حقوقه المنهوبة، مما يؤدي إلى خروج الشعب إلى مظاهرات وقد تتطور لثورات غير سلمية هدفها التخريب وتدمير الدولة المُستهدفة وكل ذلك يكون بفعل منصات التواصل الإجتماعي، ولعب هذا الهدف دوره في ثورات الربيع العربي عام 2011 التي تسببت في سقوط أنظمة حُكم العديد من حُكام الدول العربية بل هناك دول لم تستطيع استرجاع عافيتها بعد هذه الثورات مما جعلها مناطق تنافس بين الدول الكُبرى بل وجعلت التنظيمات الإرهابية من هذه الدول مكاناً لها. [33]

لم تَعد القوة العسكرية وحدها هي المُهدد الوحيد للدول بل أصبح إمتلاك الدول للقوة الإلكترونية يُمثل خطراً أكبر على الدول المُستهدفة ومن هنا جاء التحول في مفهوم الأمن، بحيث لم يعد أمن الدولة القومي مُقتصر على الأمن العسكري، بل أصبح هناك **الأمن القومي السياسي**، والذي يتلخص في المحتوى الأمني للبيانات

الرقمية والمعلومات الإلكترونية التي تخص الأحزاب في الدولة، فضلاً عن المعلومات التي تتعلق بالبرلمانات وأجهزة الدولة السيادية هي كلها معلومات حساسة قد يؤدي العبث بها لحروب أهلية داخل الدولة، وكذلك **الأمن القومي الفكري والثقافي** والذي يُمثل ذروة الإنتاج الفكري لأي دولة والتي قد تُساهم في رفع أو خفض مظاهر الأمن القومي للدولة، كالمظهر المادي المتعلق باستقرار المواطنين أو رفع الهواجس الأمنية في الدولة.[34]

ونظراً لتعرض المنظومة الإقتصادية والعلمية في الدولة لمثل هذه الحروب كان لابد من وجود **الأمن القومي الإقتصادي**، حيث أنه أكثر القطاعات الأمنية عِرضةً للهجمات الإلكترونية؛ نظراً لتحول الإقتصاد العالمي لإقتصاد رقمي معتمد على تكنولوجيا المعلومات وبالتالي تعرض تلك المنظومة لمثل هذه الهجمات قد يتسبب في خسائر إقتصادية وقومية هائلة، وأيضاً **الأمن القومي العلمي والبحثي** الذي يتعلق بالبيانات والمعلومات الخاصة بالمؤسسات البحثية والعلمية والجامعات والتي تُشكل ثروة قومية مستقبلية تحوي العديد من الاكتشافات وبراءة الاختراع المُعرضة للسرقة عن طريق القرصنة الإلكترونية.[35]

الخاتمة

يتبين أن تطور وسائل تكنولوجيا المعلومات أصبح سلاح ذو حدين للدول؛ فمن ناحية يُمكنها من تطوير إستراتيجياتها الأمنية والتحول الرقمي في جميع المجالات مما قد يجعلها قوة تكنولوجية كبيرة ومن ناحية أخرى قد يُمكن الدول من شن هجمات إلكترونية تلحق الأذى بالخصوم وترغمهم على الإذعان لمطالب الدولة المُهاجمة مما أدى لحدوث تحول كبير في مفهوم الأمن، فلم يعد يقتصر الأمن على بُعد واحد بل أبعاد متعددة تهدف لحماية الفضاء الإلكتروني، وأصبحت الدول لا تعتمد على التنافس المباشر التقليدي بل تعتمد على المواجهة الغير مباشرة في الفضاء الإلكتروني، مما جعل العديد من الدول تضع الأمن الإلكتروني الذي يهدف لحماية فضاءها الإلكتروني في مقدمة استراتيجياتها الوطنية؛ بهدف الحفاظ على

الأمن القومي، وكذلك كما يأتي اللجوء لخيار الحرب الإلكترونية اغتناماً، واستفادة من الغياب للأنظمة التشريعية اللازمة لردع وتقييد هذا النوع من الهجمات، فضلاً عن ما توفره الطبيعة والخصـــائص التقنية لهذه الهجمات من إمكانية ومجال للتملص من المسؤولية والمحاسبة لأن ليس هناك تفعيل للقوانين الرادعة لمثل هذه الحروب.

إلا ان الاستخدام الواسع للوسائل والشبكات الالكترونية من قبل الدول لاستهداف دولٍ أخرى يعد تهديداً للامن الدولي باكمله مما يستوجب ويستدعي التعاون الدولي من اجل وضـــع اســتراتيجيات تكون قابلة للتطبيق والتنفيذ على الصعيد العالمي الى جانب التشريعات القائمة على الصعيدين الوطني والإقليمي، ومنها ما وقع في استونيا عام 2007 الهجوم الالكتروني، والذي ادى الى تعطيل المواقع الالكترونية الحكومية والتجارية والمصرفية والاعلامية مسبباً خسائر مادية فادحة ادت الى الاضرار بالبلاد.

وفي عامي 2009 و 2010، برزت الهجمات التي نفذتها الوحدة (8200) الإسرائيلية بالتعاون مع (وكالة الأمن القومي الأمريكية)، على المنشأة النووية الإيرانية في نطنز، إذ تمكنت الوحدة من نشر فيروس حاسوبي يطلق عليه اسم ستوكسنت Stuxnet داخل المرفق، واستهدف الفيروس نظام التشغيل لأجهزة الطرد المركز ي المستخدمة في تخصيب اليورانيم، ما أدى إلى جعلها تتحرك بوتيرة خارجة عن السيطرة، وأدى بالنهاية إلى تكسرها وكانت هذه الأجهزة من طراز (سيمنز سي 1000) وهي أجهزة متطورة، واتجهت الاتهامات الإيرانية مباشرة إلى الولايات المتحدة الأمريكية و(إسرائيل)، إلا أنهما نفتا الاتهامات.

الاستنتاجات

في ضوء الاجابة على أسئلة الد راسة توصلت الد راسة إلى الاستنتاجات التالية:

1. تزايد عدد الهجمات الإلكترونية خلال العقدين الأخيرين، حتى باتت إحدى أهم الوسائل والتكتيكات المعتمدة بين الأطراف المتصارعة حول العالم، وذلك نظراً

لتدني كلفتها والخسائر التي قد تنجم عنها للطرف المهاجم مقارنة مع حجم ما يمكن تحقيقه والحاقة من أضرار بالخصم عبر توظيفها .إضافة إلى أ ن الفضاء الإلكتروني يحرر الدولة المهاجمة من تبعات المساءلة القانونية الدولية، ويضعف احتمالية توجيه الإدانة اليقينية لها بشكل مباشر.

2. هناك تنوع في الأدوات والوسائل وأشكال الهجمات الإلكترونية، بما في ذلك على سبيل المثال، بث فيروسات والبرامج التخريبية والمدمرة للأنظمة والشبكات الحاسوبية، أو إختراق حسابات والوصول إلى معلومات سرية وتسريبها، أو الاستفادة منها لاغراض عسكرية وامنية عدائية. كما أن هناك تنوع في الأهداف التي تتعرض لها الهجمات الالكترونية، وهي لا تقتصر على الأهداف العسكرية، إذ يمكن إن تستهدف الضربات الإلكترونية أهداف مدنية وقطاعات خدمية وانتاجية.

3. من أهم عناصر ومميزات هجمات الفضاء الإلكتروني أ ن الدول تلتزم في معظم الأحيان بعدم الاقرار بالهجوم وتعمد إلى استخدام وسائل لإخفاء هوية الفاعل، كما في حالة اللجوء إلى استخدام (سيرفرات) خوادم من دول أخرى، وكل ذلك يؤكد على خاصية عدم إمكانية تحديد مصدر الهجوم، التي يتميز بها هذا النوع من الحروب، ويجعله مختلفاُ عن الحروب التقليدية، الأمر الذي يؤدي إلى زعزعة قواعد الاشتباك التقليدية واضعاف الردع.

4. التحدي الأكبر الذي يواجه التنظيم القانوني للهجمات في الفضاء الإلكتروني هو عدم وجود ارادة دولية على صعيد المفاوضات، أو على صعيد قرارات مجلس الأمن، حيث تغيب الارادة الدولية اللازمة للدفع باتجاه ذلك، ولا سيّما من قبل الدول المهيمنة في هذا المجال. وما زاد من التحدي هو ان القانون الدولي يذهب إلى تنظيم استخدام الأسلحة بصورتها التقليدية وغير التقليدية، في حين لا يبدو أن الهجمات الإلكترونية، حتى الآن، تصنف على هذا النحو، باعتبارها أسلحة مادية، وذلك باعتبار بقاء النظر لها باعتبارها تعمل في الحيز الافتراضي غير المادي.

5. بات من غير المختلف عليه ان أمن الدول لم يعد متعلقاً فقط بحمايتها من الهجمات العسكرية، بالأسلحة التقليدية أو غير التقليدية، وانما امتد واتسع ليشمل الحاجة لحماية مجتمعاتها ومنشآتها الحيوية وبنيتها التحتية من التعرض للهجمات باستخدام تكنولوجيا الاتصال والمعلومات.

التوصيات

في ضوء النتائج الحالية توصي الدراسة بما يلي:

1. فهم وإدراك طبيعة الفضاء الإلكتروني واعتباره عنصر رئيسي في الأمن القومي، إذ أن لها علاقة وطيدة بقضايا التنمية السياسية والإقتصادية والاجتماعية وضرورة إدماجه في العقيدة الأمنية للدولة ووضع إستراتيجية قادرة على التعامل التهديدات والهجمات التي يكون مصدرها الفضاء الإلكتروني.

2. ضرورة تفعيل التشريعات والقوانين التي تُنظم الفضاء الإلكتروني، خاصةً قوانين الحروب الإلكترونية.

3. ضرورة نشر التوعية بخطورة هذه الحروب والأهداف منها؛ حتى يكون هناك فهم وإدراك لدور الأفراد في بناء الأمن. إعداد برامج توعوية حول الأمن الإلكتروني يتم تقديمها وبثها بطريقة واضحة ومبسطة لعامة الناس.

4. ضرورة التعاون الدولي والإقليمي في مجال مكافحة الحروب الإلكترونية وحق الدول على فرض هيمنتها على فضاءها الإلكتروني.

5. تطوير برامج حماية إلكترونية لمواجهة الهجمات الإلكترونية، وفي سبيل ذلك عقد شراكات بين الدول والقطاع الخاص في كل دولة لتطوير البنية التحتية.

المصادر

1. فهمي، عبد القادر، "الحروب التقليدية وحروب الفضاء الإلكتروني؛ دراسة مقارنة في المفاهيم وقواعد الاشتباك"، مجلة العلوم القانونية والسياسية، العراق ، جامعة بغداد ، المجلد 16السنة الثامنة، العدد 2، كانون الأول 2018.ص18

2. كمال مساعد ،"الحرب الافتراضية وسيناريوهات محاكاة الواقع" ، مجلة الجيش اللبناني ، لبنان ، قيادة الجيش اللبناني ، العدد(253) , 2006 .

3. Arquilla, John, Ronfeldt, David (1993). Cyberwar is coming! .Rand Corporation. At: www.rand.org.

4. Taddeo, Mariarosaria (2012). "An analysis for a just cyber warfare," 4th International Conference on Cyber Conflict .(CYCON 2012), Tallinn, 2012, pp. 1-10

5. Schreier, Fred (2015). On Cyber Warfare. 1st edition. DCAF. .Switzerland: Geneva

6. Wingfield, T. C. (2000). The law of information conflict: national security law in cyberspace. 1st edition. USA - Virginia: .Falls Church: Aegis Research Corporation

7. مصدر سبق ذكره ، ص 22.

8. كلارك، ريتشارد، وكنيك، روبرت ،"حرب الفضاء الإلكتروني: الخطر القادم على الأمن القومي وسُبُل مواجهته" ،الطبعة الأولى، الإمارات العربية المتحدة - أبو ظبي: مركز الامارات لدراسة السياسات.2012.ص 287.

9. مصدر سبق ذكره ، ص 289.

10. مصدر سبق ذكره ، ص 18.

11. مصدر سبق ذكره ، ص 24.

12. صلاح حيدر عبد الواحد ،رسالة ماجستير" حروب الفضاء الإلكتروني؛ د راسة في مفهومها وخصائصها وسبل مواجهتها"، قسم العلوم السياسية كلية الآداب والعلوم جامعة الشرق الأوسط تموز، 2020.ص 44.

13. جون باسيت ومجموعة باحثين، حرب الفضاء الالكتروني : التسلح واساليب الدفاع الجديدة ، في كتاب : الحروب المستقبلية في القرن الحادي والعشرين ، مركز الامارات للدراسات والبحوث الاستراتيجية ، أبو ظبي، 2014، ص53.

14. رياض مهدي عبد الكاظم و الاء طالب خلف ، المعلوماتية و الحروب الحديثة – دراسة حالة الحرب الامريكية على العراق عام 2003، مجلة واسط للعلوم الانسانية ، جامعة واسط ، العدد (29)، 2015 ، ص194-195.

15. خورشيد دلي , الاذاعات الموجهة مثالية في السياسة بدلا من الحرب ، شبكة البيان ، تاريخ النشر 25 / 9/ 2000

16. Greg Bruno, The Evolution of Cyber Warfare, Council on Foreign Relations, 27 Feb. 2008,

17. مصدر سابق رقم 14 ص 195.

18. Saalbach, Klaus-Peter (2019). Cyber war Methods and Practice. Germany - Osnabrueck: Osnabrueck University.

19. مصدر سابق رقم 14 ص 196.

20. Simon Tisdall, Cyber-warfare 'is growing threat', Guardian Newspaper, 3 February 2010,

21. فرانس 24، الاتحاد الأوروبي يحقق في قرصنة" آلاف "البرقيات الدبلوماسية2018/12/19، ربط الموقعhttps://www.france24.com :

22. وليد شاب الدراع و جهاد الصحراوي ، " الفضاء السيبراني وإشكالية الحرب النفسية للمعلومات عبر وسائل التواصل الاجتماعي" ، مجلة الف باء للغه والاعلام والمجتمع، تاريخ النشر أكتوبر/3/2021.

23. يوسف نصر الله ، الحرب النفسية – قراءات في استراتيجيات حزب الله ، دار الفارابي للنشر والتوزيع ، ط 1 ، بيروت، 2012 ، ص 25.

24. اســـماعيل محمود عبد الرحمنا االرهاب والثقافة البديلةا مكتبة الوفاء القانونيةا االسكندرية ا 2014 ا ص .81

25. مصدر سابق 14 ص 197.

26. الياس حنا واخرون ، مســتقبل الحرب في القرن الحادي والعشــرين – الشــرق الاوسط نموذجاً ، في كتاب : الحروب المستقبلية في القرن الحادي والعشرين، ط1 مركز الامارات للدراسات والبحوث الاستراتيجية ، 2014 ، ص80.

27. فيصل محمد عبد الغفار ، الحرب الالكترونية ، ط1، الجنادرية للنشر والتوزيع عمان ، 2016 ، ص30.

28. عبد الصــادق، عادل ،"أسـلحة الفضــاء الالكتروني في ضـوء القانون الدولي الإنســاني".الطبعة الأولى .مصــر – القاهرة :المركز العربي لأبحاث الفضــاء الإلكتروني .2018

29. Wall Street Journal, 17/12/2020. Hack Suggests New Scope, Sophistication for Cyberattacks. At: https://www.wsj.com/. Accessed on: 25/4/2021.

30. بي بي ســـي، 2020/12/19، " الهجوم الإلكتروني على الولايات المتحدة : بومبيو يتهم روســـيا ويصـــف رئيســـها بأنـه خطر حقيقي. ربط الموقع : https://www.bbc.com /.

31. ســليم دحماني، أثر التهديدات الســيبرانية على الأمن القومي: الولايات المتحدة الأمريكية نموذجا، رسالة ماجستير، جامعة محمد بوضياف، الجزائر، 2017

32. سـهيلة هادي، الحروب التكنولوجية في ظل عصـر المعلومات، جامعة بسـكرة، الجزائر، 2020

33. سـليم دحماني، أثر التهديدات السـيبرانية على الأمن القومي: الولايات المتحدة الأمريكية نموذجا، رسالة ماجستير، جامعة محمد بوضياف، الجزائر، 2017

34. خينش ماجدة، الحروب الإلكترونية وتأثيرها على سيادة الدول، مجلة الدراسات القانونية والسياسية، العدد 7 ، يناير 2018

35. محمد عاطف إمام إبراهيم، "الفضـــاء الإلكتروني وأثره على الأمن القومي للـدول: الحروب الإلكترونيـة نموذجـاً" ، المركز الـديمقراطى العربى .23أبريـل 2022.