ISSN: 3006-7812 (Print)
Al-Rafidain Journal of Political Science
ISSN: 3006-7820 (Online)
RJPS
مجلة الرافدين للعلوم السياسية
Al-Rafidain Journal of Political Science

Full Name, Academic Rank & Institutional Affiliation:
Prof. Dr. Iyad Abdel Karim Majeed
Kirkuk University, College of Law and Political Science
Asst lecturer. Donia Muhammad Ali Hassan
Kirkuk University, College of Law and Political Science

* *Corresponding author E-mail*:
albghdady79@yahoo.com

***Keywords*:**
Electronic warfare
Conflicts
Future

ARTICLE INFO

Article history:

Received:	**11 Sept 2023**
Received in revised form:	**27 Sep 2023**
Accepted:	**12 Nov 2023**
Final Proofreading:	**15 Mar 2024**
Available online:	

E-mail:
Rafjourpolsc@uomosul.edu.iq

Electronic warfare and the future of conflicts in the twenty-first century

Abstract:

The technological developments that the world has witnessed have brought about a major revolution in the means of combat and human conflicts, and have changed the nature of future wars and conflicts.

After armies, military mobilizations, and combat missiles were the language of conflict and traditional wars, scientific and technological progress came to change many aspects of life, and to show us a new field in The field of wars and conflicts is the field of cyberspace linked to digital networks, communications systems and the various Internet, which has become a strong candidate to be a new arena for electronic conflicts and wars managed with different weapons and tools, and relying on technological and technical superiority, after cyberspace has become a new field for action, influence and change, in Military, banking, and governmental information infrastructures, as well as private and public institutions and companies, remain connected to this space, making cyberwars the dominant form of conflicts and wars in the twenty-first century.

الحروب الإلكترونية ومُستقبل الصِراعات في القرن الحادي والعشرين

أ.د. أَياد عبد الكريم مجيد / جامِعة كركوك / كُلية القانون والعلوم السياسية / كركوك– العِراق
م.م. دُنيا محمد علي حسن / جامِعة كركوك / كُلية القانون والعلوم السياسية / كركوك– العِراق

المُلخص:

أحدثت التطورات التكنولوجية التي شهدها العالم ثورة كبيرة في وسائل القتال والصِراعات البشرية، وغيرت مِن طبيعة الحروب والصِراعات المُستقبلية، فبعد أَنَّ كانت الجيوش والحشود العسكرية والقذائف القتالية هي لُغة الصِراع والحروب التقليدية، جاء التقدم العلمي والتكنولوجي لتغير الكثير من مفاصل الحياة، وليظهر لنا حقلاً جديداً في ميدان الحروب والصِراعات وهو ميدان الفضاء الألكتروني المُرتبط بالشبكات الرقمية وأَنظمة الاتصالات والأنترنت المُختلفة، والذي أصبح مُرشحاً بقوة لأن يكون ساحة جديدة لصِراعات وحروب الكترونية تُدار بأَسلحة وأَدوات مُختلفة، وتعتمد على التفوق التكنولوجي والتقني، وذلك بعد أَنَّ أَضحى الفضاء

الألكتروني مجالاً جديداً للفعل والتأثير والتغيير، في ظل ارتباط البُنى التحتية المعلوماتية العسكرية والمصرفية والحكومية، فضلاً عن المؤسسات والشرِكات الخاصة والعامة بهذا الفضاء، لتكون الحروب الإلكترونية هي الشكل السائد للصِراعات والحروب في القرن الحادي والعشرين.

الكلمات المفتاحية: الحروب الالكترونية، الصراعات، المستقبل.

المُقدِمة:

أَحدثت التطورات التكنولوجية التي شهدها العالم ثورة كبيرة في وسائل القتال والصِراعات البشرية، وغيرت مِن طبيعة الحروب والصِراعات المُستقبلية، فبعد أن كانت الجيوش والحشود العسكرية والقذائف القتالية هي لُغة الصِراع والحروب التقليدية، جاء التقدم العلمي والتكنولوجي لتغير الكثير من مفاصل الحياة، وليظهر لنا حقلاً جديداً في ميدان الحروب والصِراعات وهو ميدان الفضاء الألكتروني المرتبط بالشبكات الرقمية وأنظمة الاتصالات والأنترنت المُختلفة، والذي أَصبح مُرشحاً بقوة لأن يكون ساحة جديدة لصِراعات وحروب ألكترونية تُدار بأَسلحة وأَدوات مُختلفة، وتعتمد على التفوق التكنولوجي والتقني، وذلك بعد أَنَّ أَضحى الفضاء الألكتروني مجالاً جديداً للفعل والتأثير والتغيير، في ظل ارتباط البُنى التحتية المعلوماتية العسكرية والمصرفية والحكومية، فضلاً عن المؤسسات والشرِكات الخاصة والعامة بهذا الفضاء، لتكون الحروب الإلكترونية هي الشكل السائد للصِراعات والحروب في القرن الحادي والعشرين.

إشكالية البحث:

إَنَّ الحروب الإلكترونية غيرت مِن طبيعة الصِراعات بين الدول والأطراف المُتصارِعة، في ظل تزايُد اعتماد الدول على التكنولوجيا في إدارة شؤَونها وتوظيفها في مُختلف قطاعات الحياة، مِما سبق ترتكز إِشكالية الدِراسة على سؤَال مِحوري وهو: هل الصِراعات المُستقبلية ستكون مُتأَثِرة بالتطور التكنولوجي؟ و يتفرع مِنه تساؤلات عدة منها:

- كيف أثرت الحروب الإلكترونية في مسار الصراعات الدولية؟ .
- وما هي الصور المُستقبلية لهذه الصِراعات؟.

فرضية البحث:

تنبثق فرضية البحث من مُعطيات الواقع الألكتروني وتسعى لإثبات فرضية مفادها: (كُلما ازداد التطور والتقدم التكنولوجي، كما أثر ذلك على نوع الصِراع في الفضاء الإلكتروني باستخدام أَدوات ووسائل الحروب الإلكترونية مِن قِبل الفواعل الدولية وغير الدولية).

أَهداف البحث:

يحاول البحث تحقيق جُملة من الأَهداف أَهمها:

١. التعرف على مفهوم الحروب الإلكترونية وخصائصها، فضلاً عن أَهم الأَدوات والأَسلحة الخاصة بالحروب الإلكترونية.
٢. التطرق إلى تأثير الحروب الإلكترونية على الصِراع الدولي، مع استعراض أَهم النماذج التطبيقية

للحروب الإلكترونية.

٣. رسم مشاهد مُستقبلية للصراع الإلكتروني في ظل الحروب الإلكترونية في القرن الحادي والعشرين.

منهجية البحث:

في سياق الفرضية والأسئلة المطروحة، فقد تمّ تبني أكثر من منهج حسب مُقتضيات موضوع البحث، إذ تمّ الاعتماد على المنهج الوصفي التحليلي من أجل وصف موضوع البحث بالاستناد على المعلومات الدقيقة عن الحروب الإلكترونية وتحليلها في الوقت الراهن، ومنهج الاستشراف المستقبلي لإعطاء سيناريوهات المستقبلية المحتملة للصراعات والحروب الإلكترونية.

هيكلية البحث:

في ضوء ما تقدم، فقد تم تقسيم هيكلية البحث إلى مبحثين فضلاً عن مُقدمة وخاتمة واستنتاجات، وجاء المبحث الأَول بعنوان: (الحروب الإلكترونية: دراسة في المفهوم والخصائص والأسلحة)،أَما المبحث الثاني فقد سلط الضوء على: (مُستقبل الصِراع الدولي في ظل الحروب الإلكترونية في القرن الحادي والعشرين).

المبحث الأَول:

الحروب الإلكترونية: دراسة في المفهوم و الخصائص و الأسلحة

تطورت ظاهرة الحرب عبر التاريخ وأخذت أشكالاً وصوراً مُختلفة حسب تطور المجتمعات البشرية، وازدادت حدة وتعقيداً مع تطور الأسلحة والمُعدات، ومن هنا تبلورت الحروب الإلكترونية بوصفها شكلاً جديداً مِن أشكال الصِراعات التي ارتبطت ظهورها ونشأتها بالتطور التقني المتسارع، وزيادة الاعتماد على شبكة الحواسيب والأنترنت، وتحولت فيها المواجهة بين الأطراف المتصارعة من مواجهة مباشرة بالأسلحة التقليدية إلى مواجهة غير مُباشرة بالأَسلحة الإلكترونية، كما اتّسمت الحروب الإلكترونية بمجموعة من الخصائص جعلتها مُختلفة عن نظيرتها التقليدية من حيثُ طبيعة الأنشطة العدائية والفواعل والآثار الناتجة عنها، وعليه سنعمد إلى دراسة هذا المبحث من خلال تقسيمه إلى المطالب الآتية:

المطلب الأول: مفهوم الحروب الإلكترونية:

المطلب الثاني: خصائص الحروب الإلكترونية:

المطلب الثالث: أدوات و أسلحة الحروب الإلكترونية:

المطلب الأول: مفهوم الحرب الإلكترونية:

أولاً: مفهوم الحروب الإلكترونية:

تعد الحرب الإلكترونية إحدى مجالات الحرب الحديثة الطرح والتطور على الساحة الأمنية والمعلوماتية، وذلك بعد أن تحولت الساحة الإلكترونية العالمية إلى أرض معارك حقيقية في عالم افتراضي تقني يعتمد على كل ما هو جديد فيما يخص التكنولوجيا الرقمية والاتصالية الحديثة، وتعددت أشكال هذه الحروب ما بين الفردي، الجماعي، الدولي، المؤسساتي، السياسي، الاقتصادي، والاجتماعي، وغيرها من أشكال الحروب الدائرة عبر الفضاء الألكتروني[١].

وقبل التطرق إلى مفهوم الحرب الإلكترونية لابد من الإشارة إلى مفهوم الحرب، فالحرب بمفهومها البسيط هي: الصراع المسلح بين وحدتين مستقلتين بواسطة القوات المسلحة النظامية للتوصل لتحقيق الخطوة الوطنية، وتعرف أيضا بأنها: "القتال المسلح الذي ينشب بين دولتين أو أكثر، في سبيل تحقيق هدف سياسي أو عسكري، وتخوض في غمارها جيوشها النظامية لحل النزاع القائم بينهما، بعد إخفاق جميع مساعي الدبلوماسية لإيجاد تسوية سياسية"[٢]، كما توصف الحرب بأنها: "استمرار للسياسة، ولكن بأدوات أخرئ"، كما تعرف أيضا بأنها: " نزاع بين الوحدات السياسية تستعمل فيه القوة المُسلحة"[٣].

وليس هناك إجماع حول مفهوم الحرب الإلكترونية وبالرغم من ذلك فقد ظهرت آراء تعطي مفهومها للحرب الإلكترونية، منها ما تقدم به كل من (ريتشارد كلارك) و(روبرت كنيك) اللذين عرفا الحروب الإلكترونية بأنها: "أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكومبيوتر والشبكات التابعة لدولة أخرئ، بهدف تحقيق أضرار بالغة أو تعطيلها"[٤].

في حين يعرفها (كينيث جريس) بأنها: القدرة على الدفاع والهجوم على المعلومات من خلال شبكات الحاسب الآلي عبر الفضاء الإلكتروني، فضلاً عن فشل قدرة الخصم على القيام بنفس هذه الهجمات[٥]، ويشير القاموس الدولي إلى الحروب الإلكترونية على أنها: "حرب يتم شنها من خلال أجهزة الحاسوب وشبكة الإنترنت، وهي تشمل إجراءات هجومية لإلحاق الضرر بنظم المعلومات عند الخصوم، وأخرى دفاعية لحماية النظم الخاصة بالمهاجمين، وقد تسبب الهجمات على هذه الأجهزة ضرراً مساوياً لما يسببه هجوم عسكري تقليدي"، وتعرف وزارة الدفاع الأمريكية الحرب الإلكترونية بأنها:"استخدام أجهزة الكومبيوتر والإنترنت لإجراء الحرب في الفضاء الإلكتروني"، كما تعرف الحروب الإلكترونية بأنها: "حرب افتراضية ذات طبيعة غير ملموسة تحاكي الواقع بشكل شبه تام، وهي حرب بلا دماء، بحيث تتلخص أدوات الصراع فيها بالمواجهات الإلكترونية، والبرمجيات التقنية، وجنود من برامج التخريب، وطلقات من لوحات المفاتيح ونقرات المبرمجين"[٦].

وتعتمد الحروب الإلكترونية بشكل رئيس على الوسائل التكنولوجية وشبكات الإنترنت، والقوة الذهنية من خلال توظيف كفاءات بشرية قادرة على إدارة الحرب باستحواذها على المعلومات، وتلغى الخطوط الفاصلة ما بين السلم والصراع، والمدني والعسكري، مناطق المعارك والمناطق الآمنة، وقد ظهر هذا النوع من الحروب بسبب انتشار العولمة، وتصاعُد الصِراع العرقي والديني والثقافي، وتطور الوسائل التكنولوجية وانتشارها على نحو متزايد، ما أفرز حروباً لا تقع على أرض معركة مُحددة، والاستهداف فيها لا يطول الجنود فقط، وإنما يشمل الأفكار، والأطر القانونية، ووسائل الإعلام،والوكالات الدولية، والاتفاقيات والأنشطة الاقتصادية، والسلطة السياسية، وعقول الأفراد، بهدف التدمير المعنوي والمادي، وهنا تتجلى مظاهر مخاطر الحروب الإلكترونية، وخصوصاً وأنها تتم في فضاء مفتوح تتجاوز فيه الحدود الجغرافية الرسمية؛ إذ أن الحروب الإلكترونية أعادت هندسة مفهوم الحرب بإعادة هيكلة الفواعل، والأسلحة، وأساليب الحرب، واستراتيجياتها، فعلى الرغم من كون الحرب الإلكترونية هي عمل عسكري في الدرجة الأولى؛ إلا أن هذا لا يمنع توظيف

ألياتها من برمجيات تقنية، وشبكات الإنترنت، والوسائل التكنولوجية الحديثة؛ لاستهداف المجالين الاقتصادي والثقافي نظراً لتراجع الحروب العسكرية، وبروز أنماط جديدة من التهديدات العالمية.(٧)

ثانياً: آلية عمل الحروب الإلكترونية:

تقوم آلية عمل الحروب الإلكترونية على توافر ثلاثة عناصر رئيسة للتحكم في أي صراع إلكتروني قد ينشب في الفضاء الرقمي، وتكمن هذه العناصر في(٨):

القدرات العقلية والذهنية القادرة على الاستحواذ على المعلومة، وتوظيفها توظيفاً دقيقاً للتأثير على الطرف الآخر والوصول إلى الأهداف المرجوة.

توافر تكنولوجيا المعلومات والاتصالات الحديثة والمتطورة، وشبكات الإنترنت، وأجهزة اتصالات وحواسيب تتسم بأعلى معايير الدقة والكفاءة.

توافر المعلومات الصحيحة والدقيقة، مع التحري المستمر لمدى صحة المعلومات.

فبتوفر هذه العناصر تتم مجموعة من عمليات الحرب الإلكترونية والتي تتمثل في:

أ_ عمليات الهجوم الإلكتروني: تنطلق هذه الهجمات من قاعدة معلوماتية تقوم عليها معظم عمليات الحروب الإلكترونية في العالم، وهي العمليات المعلوماتية التي تهدف إلى السيطرة على معلومات الخصم، لمنعه من القيام بأي عمليات مسبقة، إذ يتم فيها التركيز على الحاق الضرر بالخصم، وضرب معلوماته السياسية والاقتصادية والعسكرية لإلحاق الأضرار المادية والمعنوية النفسية به(٩)، ويتم الهجوم الإلكتروني من خلال إعداد اعتداء مبرمج من حاسوب موجه نحو حاسوب أخر لاختراق جدار حمايته، وفتح ثغرة للبث فيه، وتكون على نوعين: الأول يكون مخصص في التركيز على حاسوب واحد ويكون ذلك سبب في توقفه عن العمل، أما الثاني يكون أخطر من الأول؛ وذلك لأن هدفه الأساسي ليس فقط إيقاف عمل نظام الجهاز بل اقتحامه والنيل من أدوات الحماية فيه، للتمكن من سرقة ما موجود فيه من بيانات(١٠).

ب_ عمليات الدفاع الإلكتروني: وتشمل الإجراءات والوسائل الوقائية وذلك للحد من ردة فعل الخصم المهاجم، وتتلخص هذه العمليات بالمنع والوقاية التي يهدف من خلالها حماية النظم المعلوماتية من الطرف المهاجم، وتحذير هذا الأخير وتنبيهه، وكشف الاختراقات الرقمية في حالة حدوثها، ووضع الخطط الاستباقية الرامية لمنع وقوع أي اختراقات معلوماتية، والدفاع عن أنظمة مؤسسات الدولة والمجتمع وأجهزتها ومعلوماتها(١١).

ج_ عملية الدعم إلكتروني: وهي عملية مكملة لعمليتي الهجوم والدفاع الإلكترونيين؛ للتعرف إلى التهديدات المباشرة، وتحديد الأهداف، والتخطيط لإدارة العمليات مستقبلاً، وتعد نظم دعم المعلومات مصدراً أساسياً للمعلومات، واتخاذ القرارات الفورية في عمليتي الهجوم والدفاع الإلكترونيين(١٢).

المطلب الثاني: خصائص الحروب الإلكترونية:

أولاً: تعد الحرب الإلكترونية حرب رقمية وتقنية متطورة، فقد جسدت قمة التطور الذي بلغته ثورة المعلومات وبوابتها الحاسبة الإلكترونية التي شكلت بدورها الأداة المحورية لهذا النوع من الحروب والميدان الرئيس لها(١٣).

ثانياً: تعتمد الحروب الإلكترونية على الفضاء الإلكتروني ميداناً وساحة للصراع؛ ويعود ذلك إلى عولمة تكنولوجيا الاتصال التي جعلت العالم قرية صغيرة يسهل التفاعل ضمنها[١٤].

ثالثاً: أن للحروب الإلكترونية تأثيرات مهمة على طبيعة المواجهات والأطراف المُشاركة في الصراعات الدولية، فقد بات بإمكان الأطراف والفواعل من غير الدول القيام بهجمات الإلكترونية؛ إذ أن الأسلحة المُستخدمة في الحروب الإلكترونية لم تعد حكراً على الدول ويمكن للفاعلين مِن غير الدول توظيف الفضاء الإلكتروني باستخدام أسلحة الحروب الإلكترونية لتحقيق أهدافهم[١٥].

رابعاً: تتميز الحروب الإلكترونية بأنها حروب غير تناظرية؛ إذ أن تكلفة الأدوات والوسائط اللازمة لشن مثل هكذا حروب هي تكاليف بسيطة مقارنة بتكاليف الحروب التقليدية، كما إنها لا تحتاج لدولة أخرى لتقوم بتصنيع أسلحة مُكلفة جداً مثل حاملات الطائرات والمقاتلات المتطورة لتفرض تهديداً خطيراً وحقيقياً على الدول الأخرى[١٦]، وإنما يكفي تطوير البرمجيات اللازمة لشن الهجمات، وامتلاك الأجهزة الحاسوبية، ومما تجدر الإشارة إليه، أن هذه الخاصية مرتبطة بقدرة الفواعل غير الدولية على شن الهجمات الإلكترونية؛ إذ أن سهولة الحصول عليها، وانخفاض تكلفتها هي ما تشجع على التوجه للصراع في الفضاء الإلكتروني، وتنفيذ الهجمات من خلال الأسلحة الإلكترونية.

خامساً: يتمتع الطرف المهاجم في الحروب الإلكترونية بأفضلية واضحة وكبيرة على الطرف المدافع؛ كون الطرف الذي يتمتع بقوة هجومية ويبادر باستخدامها هو الطرف الأقوى، بغض النظر عن حجم قواته التقليدية، فهذه الحروب تتميز بالسرعة والمرونة والمراوغة، كما أن البيئة التي يتمتع فيها المهاجم بأفضلية فإنه من الصعب جداً على عقلية التحصن لوحدها أن تنجح، فالتحصين بهذا المعنى سيجعل هذا الطرف عرضة لمزيد من محاولات الاختراق، وبالتالي المزيد من الضغط[١٧].

سادساً:أن الهجمات الإلكترونية التي تقوم بها دولة ضد أخرى أو الفواعل من غير الدول لا تستدعي استخدام الوسائل والمعدات العسكرية في الاشتباك مع قواتها والدخول إلى أراضيها أو القيام باحتلالها، إنما يمكن التعرض أو تنفيذ الهجمات والأهداف بواسطة الأنظمة الإلكترونية للمنشآت الحيوية للعدو، سواء كانت عسكرية أو مدنية، ما يعني أن منظومة الأسلحة الإلكترونية يكون بإمكانها القيام بهجوم مزدوج يستهدف المنشآت والمفاصل المدنية والعسكرية على حدٍ سواء[١٨].

سابعاً: أن أهداف الحروب الإلكترونية لا تنحصر في المواقع العسكرية فحسب، إذ تدخل ضمن أهدافها البنى التحتية المدنية الحساسة في البُلدان المُستهدفة، وهو أمر أصبح واقعياً في ظل القدرة على استهداف شبكات الكهرباء والطاقة، وشبكات النقل والنظام المالي، والمُنشآت الحساسة النفطية أو المائية أو الصناعية بواسطة فيروس يمكنه إحداث أضرار مادية وحقيقية تؤدي إلى انفجارات أو دمار هائل، دون الحاجة إلى دحر الدفاعات التقليدية للدول[١٩].

ثامناً: يعد مفهوم الردع الذي تم تطبيقه بشكل أساسي في الحرب الباردة غير ذي جدوى في الحروب الإلكترونية، فالردع بالانتقام أو العقاب لا ينطبق على سبيل المثال على الحروب الإلكترونية، فعلى عكس

الحروب التقليدية والتي عادة ما ينطلق الصاروخ فيها من أماكن يتم رصدها والرد عليها، فإنه من الصعوبة بمكان بل ومِن المُستحيل في كثير من الأَحيان تحديد الهجمات الإلكترونية ذات الزخم العالي، وفي بعض الحالات قد تتطلب أشهراً لرصدها، وهو ما يلغي مفعول الردع بالانتقام أو العقاب، وفي كثير من الحالات لا يمكن تتبع مصدرها، وحتى إذا تم تتبع مصدرها وتبين إنها تعود لفاعلين غير حكوميين فإنه في هذه الحالة لن يكون لديهم أصول أو قواعد حتى يتم الرد عليها.[٢٠]

تاسعاً: أن عمليات الهجوم الإلكتروني بالإضافة إلى قلة تكلفتها وانعدام ضحاياها البشرية، فإنها تكون مغرية لشن الهجوم في جميع الأوقات، وقد يسهل عملية توظيفها لأن تنفيذها لا يتطلب سوى وقت قصير؛ نظراً لسرعتها الفائقة لضرب الأهداف وفي أي مكان في العالم[٢١].

عاشراً: أن توظيف الفضاء الإلكتروني أصبح له تأثير كبير في تعظيم قوة الدول، وذلك من خلال التفوق والتأثير على بيئات مختلفة، وبالتالي أظهر ما يعرف باستراتيجية حروب الفضاء الإلكتروني التي تعني القدرة على تنمية القدرات في الفضاء الإلكتروني وتوظيفها، وذلك بالاندماج والتنسيق مع المجالات العملياتية لتحقيق أو دعم إنجاز الأهداف عبر عناصر القوة القومية[٢٢].

ومما تجدر الإشارة إليه، أن الحرب الإلكترونية قد تبدأ في الفضاء الإلكتروني بلا جنود وبلا إراقة الدماء؛ إلا أنه في بعض الأحيان قد لا تظل كذلك طويلاً، فقيام الدولة بزراعة الأسلحة الإلكترونية في شبكات البنية التحتية في غيرها من الدول يجعل فتيل الحرب سهل الاشتعال أكثر من أي وقت مضى في تاريخ الحروب، وقد يشعل فتيل حرب واسعة[٢٣].

المطلب الثالث: أدوات وأسلحة الحروب الإلكترونية:

تتسلح الحروب الإلكترونية بالعديد من الأدوات والوسائل التقنية والرقمية والتي يتم توظيفها في الصراعات الافتراضية الدائرة عبر الفضاء الإلكتروني في صورة مشابهة للحروب التقليدية التي تندلع على أرض الواقع[٢٤]، وسنتطرق بشكل موجز إلى أهم الأسلحة الإلكترونية من خلال: [٢٥]

أولاً: التجسُس المعلوماتي:

تمثل سلاح التجسس التقني والمعلوماتي أحد أشهر وأقدم أسلحة الحروب الإلكترونية، وتتخذ وسائل التجسس المعلوماتي عدة أشكال، منها ما يتم عبر التجسس والتنصت على المعلومات الصادرة من أجهزة الحواسيب، أو الصادرة عن المحطات الطرفية، أو يكون عن طريق اعتراض المراسلات الإلكترونية الصادرة عن الأقمار الصناعية، والهواتف المحمولة.

ثانياً: الاختراق الإلكتروني:

وهي عبارة عن إنشاء نظام أو برنامج إلكتروني تهدف إلى استغلال معلومات الخصم وتدميرها، إضافة إلى إفساد نظامه الحاسوبي والآلي، وذلك بهدف التقدم عليه أمنياً وعسكرياً واقتصادياً وسياسياً، وقد تكون هذه المواجهة على المستوى الفردي، أو المؤسساتي، أو على مستوى الدول، وللاختراق الإلكتروني أشكالاً عدة؛ لكن تتلخص جميعها بوظيفة واحدة وهي الدخول إلى قلب معلومات الخصم، والحصول عليها مستخدمة لأجل

ذلك نظام محوسب يضرب البنية المعلوماتية للفئة المستهدفة[٢٦].

ثالثاً: زرع الفيروسات التقنية في البيئات المعلوماتية

وهي عبارة عن برامج إلكترونية تصنع لغرض تغيير خصائص الملفات التي تستهدفها، وتقوم بتنفيذ بعض الأوامر إما بالإزالة أو التعديل أو التخريب وغيرها من العمليات الهجومية، إذ أن الغاية منها هو إلحاق الضرر بالحواسيب الأخرى أو السيطرة عليها،وتتم كتابتها بطريقة معينة، وهذه الفيروسات تستخدم لتعطيل الأجهزة المهاجمة عليها من شبكات الخدمة والبنية التحتية للطرف المستهدف، كأن يتم عن طريقها إحداث خلل أو توقف أوفشل في شبكة الاتصالات الدولية[٢٧].

رابعاً: القرصنة الإلكترونية

تعد القرصنة من أضخم وأشمل الأسلحة الإلكترونية المستخدمة عبر الفضاء الإلكتروني، ويشتمل هذا السلاح التقني على غالبية وسائل الصراع الإلكتروني، وذلك لشمولية مفهومه ومضمونه[٢٨]، وتقوم ألية عمله على تجنيد العديد من الأشخاص المؤهلين والقادرين على التعامل مع الحاسوب بخبرة ودراية عالية جداً، وبالشكل الذي تمكنهم من اقتحام مختلف الوسائل الاتصالية والنظم التكنولوجية من حواسيب وهواتف وموجات وألياف ضوئية وغيرها، كما ويطلق على هؤلاء الأشخاص اسم الهاكرز (Hackers)[٢٩].

خامساً: الرسائل الصامتة

وهي رسائل تبرمج بشكل لا يشعر حامل الهاتف النقال بوصولها، إذ إنها تساعد المرسل على التحديد الدقيق لمكان وجود الشخص المستلم للرسالة؛ وذلك عبر استخدام معادلة تقوم باحتساب قوة إشارة الموجات المنبعثة من الجهاز المحمول تبعاً لأقرب ثلاث مراكز مستقبلة لهذه الموجات[٣٠].

سادساً: وسائل الإعلام وشبكات التواصل الاجتماعي:

يعد وسائل الإعلام الحديث وشبكات التواصل الاجتماعي من الأسلحة إلكترونية أيضا؛ إذ يعتمد على استخدام أجهزة الحاسوب والاتصالات عن بعد في التعامل مع المعلومة التي يقدمها إلى الجماهير بشكل سهل وبأسعار منخفضة، ومن سماته أنه متعدد الوسائط؛ إذ أنه يعرض المعلومة على شكل نص وصورة وفيديو ما يجعل تأثيره كبير جداً[٣١]، وتضم شبكات التواصل الاجتماعي في طياتها مختلف الفئات العمرية،وجميع المستويات الاجتماعية والاقتصادية، وكافة الدرجات الثقافية والتعليمية، وتشمل شبكات التواصل الاجتماعي باقة من المواقع ذات النفوذ القوي عبر العالم من أشهرها: الفيسبوك(Facebook)، تويتر (Twitter)، اليوتيوب (YouTube) وغيرها الكثير من المنصات والمواقع الإلكترونية[٣٢].

سابعاً: الأقمار الاصطناعية:

وهي أسلحة ذات دلالات استحواذية تهدف إلى السيطرة على أكبر قدر ممكن من المعلومات، وذلك عبر التقاط ملايين الصور للهدف، وإرسالها للقاعدة المعلوماتية الموجودة على الأرض، وتعد الأقمار الاصطناعية من أكفئ الوسائل التقنية وأكثرها تعقيداً في حسم المعارك[٣٣]، فهي قادرة على توجيه الصواريخ والقاذفات النارية صوب أهدافها على الأرض، وتستخدم في التشويش على المحطات الفضائية ومنعها من البث، وذلك

لأغراض وأهداف سياسية، بالإضافة إلى ذلك تقوم الأقمار الاصطناعية باعتراض الرسائل وتشويش الاتصالات والتنصت على المكالمات[٣٤] .

ثامناً: الحقيبة الكهروستاتيكية:

وهي عبارة عن أجهزة صناعية على شكل حقائب صغيرة تقوم بتوليد نبضات كهرومغناطيسية فائقة القدرة، يمكن من خلالها تدمير الوحدات الإلكترونية في أية إدارة أو مؤسسة مالية أو محطة إرسال، مما يفقدها قدرتها العملية والإنتاجية والتشغيلية[٣٥].

تاسعاً: الخداع والتضليل الإلكتروني:

يشتمل هذا السلاح على عدة وسائل، أهمها: التقليد الصوتي، التشويش الإلكتروني، التضليل المعلوماتي، الخداع ونشر الشائعات، انتحال الشخصيات افتراضياً، الابتزاز الإلكتروني، وغيرها من أساليب الخداع الرقمية[٣٦].

عاشراً: الطائرات الإلكترونية:

وهي طائرات تبرمج وتوجه عن بعد، ويتحكم فيها خبراء متخصصون على الأرض، وتكون مجهزة بأدوات تسمح لها بأداء المهام المطلوبة، وقد تكون مزودة بأجهزة وكاميرات وبقذائف وصواريخ لاستخدامها ضد أهداف معينة[٣٧]، وتتميز هذه الطائرات بأنها من دون طيار وتمتلك قدرة عالية على الدقة في تحديد الهدف والمراقبة والقصف، وتشكل هذه الطائرات حلقات وصل بين القاعدة المعلوماتية الموجودة على الأرض، وساحة العمليات الحربية الكامنة في المجال الجوي الافتراضي عبر مختبر للتحليل المعلوماتي، والذي يمكنها من تحديد نيرانها بدقة[٣٨]

الحادي عشر: الإرهاب الإلكتروني:

يمثل الإرهاب إلكتروني أحد مظاهر الدمج والربط بين استخدام كل من العنف لتحقيق أهداف سياسية، وتوظيف التكنولوجيا الحديثة في مجالات الاتصال والمعلومات من خلال استخدام شبكة الإنترنت وشبكات المعلومات وأجهزة الكمبيوتر وما يرتبط بها من تطورات متسارعة من أجل التخويف والإرغام والتخريب لتحقيق أهداف سياسية، ويعرف الإرهاب الإلكتروني بأنه: " هجمة إلكترونية غرضها تهديد الحكومات أو العدوان عليها، سعياً لتحقيق أهداف سياسية أو دينية أو أيديولوجية، وتنتج عنها آثار تخريبية مدمرة مكافئة لآثار الأفعال المادية للإرهاب"، ويعرف أيضا بأنه: " استخدام أدوات شبكات الحاسوب في تدمير أو تعطيل البنى التحتية الوطنية المهمة، مثل الطاقة والنقل، أو بهدف ترهيب الحكومة والمدنيين"[٣٩].

الثاني عشر: قنابل التعتيم الميكروويفية:

يوجه هذا السلاح نحو مولدات الطاقة والرادارات ومحطات التزود بالإنترنت ومراكز الاتصالات؛ لإطلاق نبضات من الطاقة المغناطيسية لقطع جميع مصادر الطاقة والمعلومات؛ لفصل الجهة المستهدفة عن العالم الخارجي، ما يسهل السيطرة الكلية عليها[٤٠] .

المبحث الثاني: مستقبل الصراع الدولي في ظل الحروب الإلكترونية في القرن الحادي والعشرين:

مع التحول الذي طرأ على طبيعة الصراع بانتقالها من الصراع التقليدي إلى الإلكتروني؛ باتت الحروب والصراعات تجري في الفضاء الإلكتروني معتمدة على الهجمات الإلكترونية باستخدام أدوات الحروب الإلكترونية في إدارة صراعاتها وتحقيق أهدافها بأقل تكلفة، بعيداً عن التدخل والعمل العسكري التقليدي، من خلال استهداف الأنظمة المعلوماتية العسكرية الدفاعية أو الهجومية بالإضافة إلى البنى التحتية الحيوية للخصم، وباتت الحروب تجري في الفضاء الإلكتروني وتظهر نتائجها بصورة مادية على أرض الواقع، وهناك العديد من القوى الإقليمية والدولية فضلاً عن الفواعل غير الدولية لجأت إلى استخدام الحروب الإلكترونية في إدارة صراعاتها مع الأطراف الأخرى بغية الوصول إلى أهدافها، وبناء على ما سبق يمكن دراسة هذا المبحث من خلال تقسيمه إلى المطالب الآتية:

المطلب الأول: تحول الصراع الدولي في ضوء الحروب الإلكترونية

المطلب الثاني: أبرز نماذج الحروب الإلكترونية التي شهدتها الساحة الإقليمية والدولية

المطلب الثالث: مستقبل الصراع الإلكتروني في ظل الحروب الإلكترونية في القرن الحادي والعشرين

المطلب الأول: تحول الصراع الدولي في ضوء الحروب الإلكترونية:

ترتبط طبيعة الصراعات الدولية وأشكالها بعلاقة وثيقة مع التطورات المادية وغير المادية التي تشهدها الدول والمجتمعات، وذلك إنطلاقاً من أن التعارض كمضمون عام لفكرة الصراع يظل مرتبطاً في مسببات بروزه وتشكيل ملامح وأهداف أطرافه بما تطرحه السياقات الحاضنة له من مصادر وقضايا جديدة (قيم، ومصالح) تكون موضعاً للتنازع، فقد عرف العالم خلال التطورات المتعاقبة في القرنين العشرين والحادي والعشرين أنماطاً من الصراعات والتي تعددت قضاياها داخلياً وخارجياً، واختلفت فواعلها بين الدولية وغير الدولية، وتباينت دوافع نشوبها بحسب القوة الأكثر بروزاً التي يتصارع الأطراف المتنازعة على امتلاكها(سياسية، اقتصادية، عسكرية، ثقافية)، لتحقيق أهدافهم ومصالحهم.[٤١]

كانت الصراعات والحروب سابقاً وعلى مدى عصور وقرون عديدة تجري في الفضاء العام التقليدي(البري، البحري، الجوي)، فقد كان هذا الفضاء هو الميدان الرئيسي الذي يعبر فيه الفاعلون الدوليون عن مصالحهم ورغباتهم في الوصول إلى أهدافهم، فعلى سبيل المثال شهد العالم منذ ظهور الدول القومية حربين عالميتين تم فيه إدارة الصراع بين الدول بأدوات وأسلحة تقليدية(صواريخ، مدافع، طائرات... إلخ)، وبعد انتهاء الحرب العالمية الثانية وتأسيس منظمة الأمم المتحدة للحيلولة دون حدوث حروب عالمية أخرى في ظل وجود سباق دولي لامتلاك الأسلحة النووية لتحقيق قاعدة الردع النووي[٤٢]؛ أدى تصاعد شبح الحرب النووية إلى قيام الدول بالتفكير بوسائل جديدة للصراع تستثني المواجهة المباشرة، وذلك أن عدم اللجوء إلى استخدام السلاح النووي لا يعني بأي شكل من الأشكال توقف الدول عن التفكير بوسائل جديدة للمواجهة، وهذا بالضبط ما شهده العالم خلال الحرب الباردة والتي امتدت حوالي(٤٥) عاماً، فقد ظهرت خلال تلك المدة مصطلحات عدة كالحرب بالوكالة، والحرب الاقتصادية وغيرها، وآخر هذه الوسائل تمثلت في التركيز الكبير على تكنولوجيا(الحرب الإلكترونية)، والتي تعد أهم وأحدث تطور في ميدان الصراع والتنافس الدولي[٤٣]، إذ

شكلت التطورات التكنولوجية الهائلة في مجال الاتصال والمعلومات في أواخر القرن العشرين وبداية القرن الحادي والعشرين سياقات جديدة لنشوب صراعات حول النفوذ في الفضاء الإلكتروني، فقد عد هذا الأخير ساحة واسعة للتفاعلات الدولية، وبدأ مضمون الصراع يدور حول من يملك القدرة على التأثير في مسار تدفق المعلومات والاتصال في الفضاء الإلكتروني، وذلك انطلاقاً من أهمية ذلك في تقدم الدول والمجتمعات من جهة، وتوظيفها في صراعاتهم للوصول إلى أهدافهم وتحقيق مصالحهم من جهة أخرى[٤٤].

وعليه فقد تعرضت ظاهرة الصراع إلى تحولات عدة مع بروز الفضاء الإلكتروني كمجال حيوي تجري فيها الصراعات والنزاعات بين الفواعل الدولية وغير الدولية، خاصة مع الاعتماد الكثيف على تكنولوجيا الاتصال والمعلومات، وهنا ظهر الصراع الإلكتروني كحالة من التعارض في المصالح والقيم بين الفاعلين المختلفين في الفضاء الإلكتروني[٤٥]، وأصبح هذا الأخير يشكل ساحة جديدة للصراع بشكله التقليدي ولكنه ذو طابع إلكتروني يعكس النزاعات التي تخوضها الدول أو الفاعلين من غير الدول بسبب خلفيات دينية أو عرقية أو أيديولوجية أو اقتصادية أو سياسية، وبات الصراع الإلكتروني يتمدد داخل شبكات الاتصال والمعلومات متجاوزاً الحدود التقليدية وسيادة الدول، وهو ما أوجد نوعاً جديداً من الضرر من خلال قابلية التعرض للهجوم دون الحاجة إلى الدخول الطبيعي والمادي لإقليم الدولة؛ وذلك لاعتماد الدول على الأنظمة الإلكترونية في كافة منشآتها الحيوية؛ بما يجعل من تلك الأنظمة هدفاً للهجوم، وخاصة أن تلك الأنظمة تحمل طابعاً مدنياً عسكرياً مزدوجاً وذلك بعد أن تمخض عن الثورة التكنولوجية ثورة أخرى؛ وهي الثورة في الشؤون العسكرية وتطور تقنيات الحرب، بالإضافة إلى ما سبق، يعد الفضاء الإلكتروني أحد العناصر الرئيسة المؤثرة في عملية التعبئة وتحشيد الجماهير، فضلاً عن التأثير على القيم السياسية وأشكال القوة والصراعات، كما يمكن أن يستخدم كوسيلة من وسائل الصراع داخل الدولة بين مكوناتها على أساس طائفي أو اقتصادي أو ديني، وهو ما يساعد على كشف ديناميكيات التفاعل الداخلي إلى الخارج؛ بما يسهل من عملية الاختراق الخارجي عبر شبكات الاتصال بدعم أحد أطراف الصراع بأدوات غير قتالية[٤٦].

وبما أن المتنازعين يلجئون في الصراعات التقليدية إلى استخدام شتى أنواع أسلحة التدمير الممكنة؛ فقد انتقلت جبهات القتال بشكل مواز إلى ساحة الفضاء الإلكتروني، وكان هذا التغير سببا في التفكير في ديناميكية وحركية الصراع، وظهور وبروز ما يعرف بـ"عصر القوة النسبية" والتي تعني أن القوة العسكرية قد لا تكفي وحدها لتأمين البنية التحتية للدول، الأمر الذي يخلف آثاراً استراتيجية هائلة على مستوى تركيبة وتوازنات النظام الدولي[٤٧].

ومن الجدير بالذكر أن هناك عوامل ساهمت في انتقال الصراع إلى الفضاء الإلكتروني وبالتالي إفساح المجال لنشوب الحرب الإلكترونية ومنها[٤٨] :

اولاً: تغير منظور الحرب جذرياً، إذ انتقلت من نسق الحرب بين الدول إلى وسط الشعوب، وبمعنى أخر انتقالها من حرب بين الدول إلى الحروب البينية (الحروب الأهلية).

ثانياً: بروز الصراعات ذات الأبعاد المحلية_ الدولية، إذ ساعد تزايد الصراعات الداخلية في المرحلة ما بعد

الحرب الباردة وكذلك طبيعة السياق الدولي للفضاء الإلكتروني في توفير بيئة مناسبة لدمج الفئات والقوى المهمشة في السياسة الدولية، إضافة إلى خلق شبكة تحالفات مؤيدة أو معارضة ذات نطاق دولي عريض، إما على أساس قيم حقوقية أو انتماءات عرقية أو دينية. وقد ساعد تحول الصراع التقليدي إلى صراع إلكتروني نتيجة للتطور التكنولوجي واستخدام الفضاء الإلكتروني إلى ظهور أساليب جديدة للصراع الدولي تباينت بين الطابع السياسي والاقتصادي والعسكري، وعليه فقد ظهرت أنواع للصراع الإلكتروني تختلف باختلاف المجالات التي تستهدفها ومنها(٤٩):

١. **صراع إلكتروني ذو طبيعة سياسية:** وهو صراع تحركه دوافع سياسية، وقد يأخذ شكلاً عسكرياً، ويتم فيه استخدام قدرات هجومية ودفاعية عبر الفضاء الإلكتروني؛ وذلك بهدف افساد النظم المعلوماتية والشبكات والبنية التحتية، ويتضمن هذا النوع من الصراعات استخدام أسلحة إلكترونية من قبل الفاعلين داخل المجتمع المعلوماتي، أو من خلال التعاون مع قوى أخرى لتحقيق أهداف سياسية.
٢. **صراع إلكتروني ذو طبيعة ناعمة:** ويدور هذا النوع من الصراع حول الحصول على المعلومات، والتأثير في المشاعر والأفكار، وشن حرب نفسية وإعلامية، ويتم ذلك من خلال تسريب المعلومات واستخدامها عبر منصات إعلامية، بما يؤثر على طبيعة العلاقات الدولية، كالدور الذي لعبه موقع ويكليكس في الدبلوماسية الدولية.
٣. **صراع إلكتروني على التقدم التكنولوجي والاقتصادي:** ويأخذ هذا النوع من الصراع الإلكتروني طابعاً تنافسياً حول الاستحواذ على سباق التقدم التكنولوجي، وسرقة الأسرار الاقتصادية والعلمية، وقد يمتد إلى محاولة السيطرة على الإنترنت من خلال السعي للسيطرة على أسماء النطاقات، وعناوين المواقع والتحكم بالمعلومات، والعمل على اختراق الأمن القومي للدول بدون استخدام طائرات أو متفجرات أو حتى انتهاك حدود السيادية للدول، كهجمات قراصنة الكومبيوتر، وتدمير المواقع والتجسس بما قد يكون له من تأثيرات مدمرة على الاقتصاد والبنية التحتية بنفس القوة التي قد يسببها تفجير تقليدي مُدمر.

بناءً على ما تقدم يمكن القول بأن دائرة الصراعات الإلكترونية اتسعت، وزاد عدد المهاجمين، وصار الصراع بين الفاعلين المختلفين حول امتلاك أدوات الحماية والدفاع، وتطوير القدرات الهجومية الإلكترونية بهدف حيازة القوة والتفوق والهيمنة، وتعزيز التنافس حول السيطرة والابتكار والتحكم في المعلومات، وتنظيم وتعظيم القدرات القادرة على زيادة النفوذ والتأثير في المستويين المحلي والدولي(٥٠).

المطلب الثاني: أبرز نماذج الحروب الإلكترونية التي شهدتها الساحة الإقليمية والدولية:

شهدت الحروب الإلكترونية منذ نهاية التسعينيات وبداية القرن الحادي والعشرين تطوراً هائلاً بفعل ما أحدثته شبكة الإنترنت من تسهيل لعمليات الدخول للأنظمة المختلفة واقتحام شبكات المعلومات، والذي نتج عنه خسائر مالية كبيرة قدرت بالملايين، كما توسعت جرائم نشر الفيروسات عبر الإنترنت لسهولة وصوله إلى الملايين من المستخدمين في الوقت ذاته، إذ تطورت الهجمات الإلكترونية بنحو أوسع من خلال

استهداف البنى التحتية للدول الأخرى سواء كانت مرافق عامة، أم خدمات البنى العسكرية والاقتصادية وغيرها[٥١]، وقد ساهمت أحداث وتطورات السياسة الدولية في تكثيف الهجمات الإلكترونية بين العديد من الدول ومن أبرز هذه الهجمات، الهجمة التي تعرضت لها أنظمة الاتصال الإلكترونية التابعة لوزارة الدفاع الأمريكية (البنتاغون)، ووكالة الفضاء الأمريكية(ناسا)، ووكالة الطاقة الأمريكية بين الأعوام (١٩٩٨_٢٠٠٠)، ووجهت الولايات المتحدة الأمريكية الاتهام رسمياً إلى روسيا الاتحادية، في حين انكرت الأخيرة مسؤوليتها عن هذا الهجوم[٥٢].

وفي الوقت الذي أعلنت فيه الصين عن إنشاء وحدات الفضاء الإلكتروني عام ٢٠٠٣؛ تعرضت الولايات المتحدة الأمريكية في العام نفسه لواحدة من أسوأ حلقات التجسس الإلكتروني، ويطلق عليها اسم" Titan Rain"، وفيها تم سحب ما يتراوح بين(١٠_٢٠) تيرابايت_ وهي وحدة قياس لسعة التخزين في الكومبيوتر_ من المعلومات من شبكة البنتاغون غير السرية[٥٣]، كما قام قراصنة إلكترونيون صينيون بشن بضع هجمات على المواقع الإلكترونية لشركة "لوكهيد مارتين" الأميركية، وسرقوا معلومات عن تكنولوجيا تصنيع مُقاتلة "إف_٣٥" التي استخدمتها الصين في ما بعد لدى تصميم وتصنيع مُقاتِلة "تي ٢٠" الصينية، وشملت الهجمات أيضا مقاولين لدى وزارة الدفاع الأمريكية الذي يعملون على صناعة وتطوير طائرات من دون طيار الأمريكية، بهدف سرقة المعلومات حول هذه الطائرات وكيفية صناعتها وتطويرها[٥٤] .

وفي عام ٢٠٠٧، تعرضت استونيا لهجمة إلكترونية واسعة النطاق من قبل روسيا والتي أدت إلى توقف خدمات الدولة، وجاءت هذه الهجمة كنتيجة لقيام الحكومة الاستونية بإزالة تمثال الجندي البرونزي وجثث جنود الجيش الأحمر في الحرب العالمية الثانية من حديقة عامة في العاصمة "تالين"، وقد تسبب هذا الهجوم في حدوث خلافات بين روسيا واستونيا، وقد تأثرت مواقع الوكالات الحكومية بهذه الهجمة أيضا، وبعد ذلك تم ضرب المواقع الخاصة بالخوادم والبنوك والصحف، وعلى الرغم من عدم وجود خسائر بشرية؛ إلا أن الإغلاق المطول للخدمات العامة تسبب في اضطرابات في الاقتصاد الاستوني، وكان لذلك تأثير على البنية التحتية المدنية[٥٥] .

وعندما احتدم الصراع على بعض الأقاليم الصغيرة المتنازع عليها بين جورجيا وروسيا في تموز عام ٢٠٠٨، قامت جورجيا بغزو إقليم (أوسيتا الجنوبية)، وسارع الجيش الروسي على إخراج جورجيا من إقليم(أوسيتا الجنوبية)، وفي الوقت نفسه الذي تحرك فيه الجيش الروسي؛ تحرك محاربو الروس الإلكترونيون بتوجيه ضربات الإلكترونية لتعطيل خدمة مواقع الحكومية الجورجية، واخترقوا جهاز الخادم الخاص بموقع الرئيس لتشويهه، ومع اندلاع القتال البري اشتدت الهجمات الإلكترونية في حدتها ودرجة تعقيدها، وفي أب ٢٠٠٨ ومع تحرك القوات الروسية إلى داخل جورجيا؛ هاجم المتخصصون في اختراق أنظمة الحاسب الآلي مواقع الحكومة الجورجية على شبكة الانترنت في الأسابيع التي سبقت اندلاع الصراع المسلح، وهذا الصراع بين روسيا وجورجيا يمثل أول الهجمات الإلكترونية التي تصاحب صراعاً مسلحاً في القرن الحادي والعشرين[٥٦].

تجدر الإشارة إلى أيضا إلى أحد الهجمات إلكترونية الشائعة على البنية التحتية الحيوية، والمتمثلة في الهجوم على خط أنابيب النفط التركي في عام ٢٠٠٨، والذي اشتعلت فيه النيران بطريقة غامضة دون إطلاق أي مستشعرات أو إنذارات، وعلى الرغم من أن الانفصاليين الأكراد زعموا بأنهم من تسبب بالهجوم؛ إلا أن عدد من مسؤولي المخابرات الأمريكية قد أدانوا روسيا التي عارضت إنشاء خط أنابيب الغاز "باكو_ تبليسي_ جيهان"؛ لأنه خارج أراضي الروسية، ومن شأنه تقويض قدرتها على التحكم في تدفق الطاقة باتجاه أوروبا[٥٧].

في تموز ٢٠٠٩ أرسلت كوريا الشمالية رسالة مشفرة إلى(٤٠٠) ألف جهاز حاسوب حول العالم، وهي محملة بفايروس للسطو على الشبكات، وتضمنت الرسالة مجموعة من التعليمات التي تجعل الحاسوب يبدأ في إرسال النبضات للمطالبة بالاتصال بقائمة من مواقع الانترنت الخاصة بالولايات المتحدة الأمريكية وحكومة كوريا الجنوبية وعدد من الشركات الدولية، وعندما يتم تشغيل الأجهزة فإنها تنظم إلى الهجوم[٥٨].

وجاء الهجوم الإلكتروني بفايروس ستاكسنت على برنامج إيران النووي عام ٢٠١٠ ليمثل نقلة مهمة في مجال تطور أسلحة الفضاء الإلكتروني، ويمثل النموذج الإيراني حالة فريدة لتحول الفضاء الإلكتروني لساحة قتال بأشكال متعددة في إطار المواجهة والصراع بين الولايات المتحدة الأمريكية وإيران، فقد استخدم الفضاء الإلكتروني في شن هجمات تخريب للبرنامج النووي الإيراني للعمل على تعطيله، وشكل فايروس ستاكسنت آلة حرب معقدة جداً ومعززة بمئات الآلاف من خطوط البرامج، ويستغل هذا الفايروس عدة خطوط للانتشار، ويتمتع بنظام تخفي يجعل اكتشافه عسيراً جداً، ويختص فايروس ستاكسنت بقدرته على تغيير قواعد إحكام العمل بكيفية تجعله يحدث اضطرابات في عمل الحواسيب، ويرسل في الوقت ذاته إلى قاعات المراقبة معلومات كاذبة ومطمئنة، وقد يكون قادراً على الدخول في حالة نوم والعودة إلى النشاط والعمل من جديد، وقد أعلنت الاستخبارات الإيرانية في عام ٢٠١٢ أن فيروس ستانكسنت أصاب ما يقدر بـ(١٦) ألف جهاز كمبيوتر[٥٩]، وأدى إلى تعطيل حوالي ألف جهاز من أجهزة الطرد المركزي في منشأة لتخصيب اليورانيوم في مفاعل "ناتانز" في وسط إيران[٦٠]، إذ هاجم هذا الفايروس أنظمة التحكم المركزية والذي كان مصمماً للعمل فقط عند وصوله إلى المفاعل النووي الإيراني، وأتضح في عام ٢٠١٢ أن الولايات المتحدة الأمريكية وإسرائيل عملاً بشكل مشترك على تطوير هذا الفايروس على الرغم من عدم اعتراف أيا منهما بالمسؤولية، إلى جانب هذا الهجوم، تعرضت إيران لهجمات عدة كان أخرها في عام ٢٠٢٠ عندما تعطلت شبكة الاتصالات لساعات، لكن إيران التزمت الصمت حول الجهة التي شنت هذا الهجوم[٦١].

وفي كانون الثاني ٢٠١١ أعلنت الحكومة الكندية تعرض وكالاتها لهجوم إلكتروني ضخم من بينها وكالة البحث والتطوير الدفاعي الكندية، وقد أجبرت هذه الهجمات وزارة المالية ومجلس الخزانة الكنديين على فصل اتصالهما بالإنترنت[٦٢]، بالإضافة إلى الهجمات التي سبق ذكرها، هناك مجموعة من الهجمات قامت بها الـ(أنونيموس) وهي مجموعة من القراصنة المحترفين التي تعرف بأنها من أكبر المجموعات الإلكترونية تأثيراً في العالم، وهي المسؤولة عن مجموعة من الهجمات الإلكترونية التي طالت البنتاغون، فضلاً عن مجموعة

من الهجمات والعمليات التي تعرضت لها بعض الشركات والمنظمات في مختلف أنحاء العالم، إلا أن أشهر العمليات التي قامت بها(أنونيموس) هي الهجمة إلكترونية على إسرائيل(أوب_ إسرائيل #OP_ Israel) في عام ٢٠١٣، وهي أكبر عملية قرصنة استهدفت مواقع إلكترونية إسرائيلية حساسة بلغت خسائرها ما يقارب ثلاثة مليار دولار أمريكي، بينما أوردت تقارير أخرى بأن خسائرها وصلت إلى خمسة مليار دولار أمريكي، وأعلنت المجموعة الدولية المكونة من آلاف قراصنة الكومبيوتر العرب والأجانب عن هدف الهجوم وهو محو إسرائيل من على الانترنت والرد على سياساتها ضد الفلسطينيين[٦٣]، بشن هجوماً على مواقع إسرائيلية، وشملت الهجمات مواقع البورصة الإسرائيلية، ورئيس الوزراء ووزارة الدفاع وموقع جهاز الأمن الداخلي الشاباك والصناعات العسكرية الإسرائيلية إضافة إلى موقع مكتب الإحصاء الرسمي ووزارة التربية والتعليم وعشرات المواقع الأخرى، وبالمقابل أعلنت مجموعة قراصنة إسرائيليين إنها تمكنت من شن هجوم إلكتروني مضاد واختراق موقع انونيموس[٦٤].

كما أجرت كوريا الشمالية هجوماً إلكترونياً ضد شركة "Sony Pictures Entertainment" في عام ٢٠١٤، مما جعل الآلاف من أجهزة كمبيوتر الخاصة بتلك الشركة غير صالحة للعمل، وتم اختراق المعلومات التجارية السرية للشركة، بالإضافة إلى الطبيعة المدمرة للهجمات؛ سرقت كوريا الشمالية نسخا رقمية لعدد من الأفلام التي لم يتم إطلاقها، بالإضافة إلى آلاف المستندات التي تحتوي على بيانات حساسة تتعلق بالشخصيات الشهيرة وموظفي الشركة، وقد كان هذا الهجوم من أكثر الهجمات تأثيراً على الولايات المتحدة الأمريكية[٦٥].

وقد تعرضت روسيا للاتهام بالقرصنة الإلكترونية في الانتخابات الأمريكية في عام ٢٠١٦ لدعم المرشح الجمهوري "دونالد ترامب" في مواجهة منافسته الديمقراطية "هيلاري كلينتون"، والتسلل إلى خوادم البريد الإلكتروني للجنة الوطنية الديمقراطية، كما تم اختراق البريد الإلكتروني الخاص بـ (جون بوديستا)_ رئيس الحملة الانتخابية الرئاسية لهيلاري كلنتون_ وعلى أثرها تم طرد(٣٥) دبلوماسياً روسياً[٦٦].

كما تعرضت أوكرانيا لهجوم من قبل روسيا في عام ٢٠١٧ بسبب الخلاف المستمر حول شبه جزيرة القرم، وبعض المناطق الشرقية والجنوبية للبلاد، حيث بدأت الهجمات الروسية على المواقع الإلكترونية للمنظمات والمؤسسات الأوكرانية باستخدام إصدارات "بيتا" من البرامج الضارة، وأدى الهجوم إلى اختراق أنظمة المعلومات وإغلاق أجهزة الكمبيوتر، والمطالبة بتقديم فدية بالنقود الإلكترونية "بيتكوين"، وبعد ذلك أوضحت السلطات الأوكرانية أن هدف الفدية هو التستر على الهجوم والغرض الأساسي من الهجمات هو تعطيل أعمال الشركات الحكومية والخاصة وزعزعة الأمن والاستقرار في أوكرانيا[٦٧]

وفي عام ٢٠١٩ تعرضت السعودية لانفجار أصاب محطتين للنفط بسبب هجمات مباشرة بواسطة طائرات مسيرة انفجارية تابعة للحوثيين، كما سجلت عام ٢٠١٩ عدة غارات بطائرات مسيرة على قاعدة حميميم متسببة في إصابة طائرات الميغ الروسية وأجهزة الرادار في المطار بعدة قذائف صاروخية[٦٨] .

وفي الصراع الروسي الأوكراني الحالي أيضا اعتمدت روسيا على الهجمات الإلكترونية وعمليات

القرصنة لتعزيز موقفها في الصراع الدائر بينهما، إذ أكدت السلطات الأوكرانية تعرض المواقع الإلكترونية الخاصة بالحكومة والبرلمان والمصارف الكبيرة في البلاد لهجوم إلكتروني واسع النطاق، وأن الخدمات الإلكترونية الخاصة بالعديد من المؤسسات الإلكترونية بما في ذلك وزارات الصحة والخارجية تعطلت، وأن العديد من البنوك تأثرت بهذا الهجوم، وأوضحت السلطات أن الهجوم يعرف باسم " دي دي أو إس" أو الحرمان المتوزع من الخدمات،عملت على إغراق المواقع الإلكترونية بحركة زائفة مكثفة ومنعها من التواصل بالطريقة المعتادة، وبحسب وسائل إعلام دولية فإن خدمات الإنترنت انقطعت من عدة مواقع شبكية تابعة لدوائر حكومية أوكرانية؛ وذلك بفعل هجمات إلكترونية من فئة الهجمات المتخصصة في الحرمان من خدمات الإنترنت[٦٩] ومن الجدير بالذكر أن الهجمات المذكورة بدراستنا هذه ليست الوحيدة في العالم الافتراضي لكنها الأهم والأشهر.

المطلب الثالث: مستقبل الصراع الالكتروني في ظل الحروب الإلكترونية في القرن الحادي والعشرين:

أولاً: مشهد استمرار الوضع القائم:

يقوم هذا المشهد على فرضية مفادها: أن التطور التكنولوجي والمعلوماتي أثرت على طبيعة الصراعات التي تحولت من صراع تقليدي يدور في ساحات القتال التقليدية إلى صراع إلكتروني يدور في الفضاء الإلكتروني من خلال أسلحة الحروب الإلكترونية لتقوم الدول بتوظيفها في صراعاتها وحروبها جنباً إلى جنب مع الأسلحة التقليدية، وذلك بالتزامن مع زيادة وكثافة الاعتماد على التكنولوجيا والمعلومات في مختلف مجالات الحياة المعاصرة.

يعد ظهور البعد الإلكتروني في الصراع الدولي هو جزء من سلسلة طويلة من التطورات التي شهدتها هذه الظاهرة منذ الحرب العالمية الثانية حتى الآن، وقد كان للتطورات التكنولوجية دوراً مهماً في تطوير الأسلحة التقليدية واستراتيجيات إدارة الحروب العسكرية، إذ بات الفضاء الإلكتروني ساحة جديدة للصراع، وبدأت الدول وحتى الفاعلين من غير الدول تلجأ في إدارة صراعاتها مع خصومها إلى توظيف الحروب الإلكترونية كأدوات إضافية في حروبها، وأصبح البعد الإلكتروني حاضراً في أغلب الصراعات والحروب المسلحة في العصر الحديث[٧٠]، فعندما تنشب حروب تقليدية بين الدول؛ تصبح قطاعات الاتصالات والمعلومات والبنى التحتية والمعلوماتية ضمن الأهداف العسكرية، خاصة مع ارتباط تلك القطاعات بالأمن الوطني للدول، ومن ثم أصبحت هناك أسلحة ذات طبيعة الكترونية ضمن الحروب مثل الفايروسات وبرامج التجسس والتخريب، ووسائل التواصل الاجتماعي، والاقمار الصناعية، والطائرات من دون طيار، والأسلحة الروبوتية، الأمر الذي أدى إلى تعرض مختلف دول العالم إلى عمليات الاختراق والتجسس الإلكتروني، للحصول على معلومات عسكرية كانت أو مدنية، فضلاً عن القيام بعمليات التعرض للبيانات واتلاف المنشآت؛ نظراً لاختلاف الدول من حيث أنظمة الحماية والدفاع الإلكتروني[٧١].

ومن أهم المعطيات والدلائل التي تشير إلى استخدام الأسلحة التقليدية والإلكترونية جنباً إلى جنب في الصراعات والحروب الجارية في الوقت الراهن، واستمرار هذا النوع من الصراعات، هو ما يحدث الأن في

الحرب الروسية_ الأوكرانية، والتي تستخدم فيها روسيا مختلف قدراتها الإلكترونية، وتعمل على توظيفها بالشكل الذي يدعم موقفها في الجانب التقليدي من الحرب، للوصول إلى تحقيق غاياتها وأهدافها بأقل الخسائر البشرية والمادية.

فضلاً عن ذلك، أن أدوات الحروب الإلكترونية لا تخدم أهداف الحروب والصراعات الجارية بين الدول فحسب؛ بل تستخدم حتى في تأجيج وتحريك الصراعات الداخلية في الدول من قبل الأطراف المتنازعة والمتعارضة في أهدافها وتوجهاتها ومتطلباتها، وخير دليل على ذلك الاحداث التي شهدتها الدول العربية عام ٢٠١١ وما بعدها في سوريا وليبيا وتونس ومصر وغيرها من الدول، وتعد وسائل التواصل الاجتماعي من أسرع الوسائل لتحشيد وتعبئة الجماهير وخاصة في البلدان النامية.

ووفقاً لهذا المشهد من الممكن أن يبقى الصراع على ما هو عليه الآن وهو ما يشير إليه معطيات والأحداث الجارية على أرض الواقع، إذ تبدو ملامح الحروب الحديثة في القرن الحادي والعشرين مزيجاً من تكنولوجيات متطورة عالية التقنية، ولا يعني ذلك استبعاد المفاهيم والنظريات العسكرية التقليدية المعروفة جملة وتفصيلاً، فمبادئ الحرب ثابتة في معظمها لكسب بعض مضامينها، كما أن المفاهيم الهجومية والدفاعية أيضا تظل سارية مع تطوير أدواتها واساليبها من خلال توظيف ما تم الوصول إليه من تكنولوجيات جديدة[٧٢]، كما أن الفضاء الإلكتروني ستبقى آمنة للأعمال والتواصل مع الأخرين، وفي الوقت ذاته يتم توظيفها في الصراعات الإلكترونية لسرقة البيانات الشخصية للأفراد، أو الحرمان من الخدمة، كما ستستمر الدول باستخدام الأسلحة الإلكترونية في الصراعات والحروب، وهذا يؤدي إلى استمرار الدول بتعزيز قدراتها للحد من هجمات الفضاء الإلكتروني،والإرهابيين سيسعون إلى مزيد من التقنيات لتطوير الهجمات الإلكترونية على الدول عبر تكثيف الاعتماد في استراتيجياتهم على الخدمات الإلكترونية والبريد الإلكتروني وكل هذه التطورات ستجعل الصِراع مُستمر على الوضع الحالي بما يشمله من هجمات الإلكترونية متبادلة[٧٣].

ثانياً: مشهد تراجع الصِراع الإلكتروني:

ينطلق هذا المشهد من فرضية مفادها: أن الصِراع الإلكتروني قد تتراجع في الفضاء الإلكتروني عن طريق إيجاد سبل للتعاون في هذا الفضاء، وعقد اتفاقيات إقليمية ودولية للحد من الأنشطة الإلكترونية، فضلاً عن اختراع برامج تكنولوجية عالية في مجال الدفاع بالشكل الذي يطغى فيه الوضع الدفاعي على الهجومي، أي كلما تمكنا من احتواء وتقليل العوامل الدافعة باتجاه زيادة الصراع في الفضاء، كلما تراجع الصراع الإلكتروني، وبالعكس كلما كان هناك فشل في معالجة العوامل المحفزة للصراع في الفضاء كلما تزايد الصراع الإلكتروني.

يرتكز هذا المشهد على ضرورة مُعالجة التحديات الناجمة عن ظهور الأسلحة الإلكترونية، وضرورة التعاون بين القوى الإقليمية والدولية لتبني اتفاقية دولية شاملة تتعامل مع مخاطره، فضلاً عن تحديث مواد القانون الدولي التي تحرم استخدام القوة أو التهديد بها عبر الفضاء الإلكتروني، إلى جانب أهمية قيام الدول بتعزيز دورها في صنع السياسات المتعلقة بوضع حد للأخطار والتهديدات الناتجة عن الحروب والصراعات

الإلكترونية وذلك من أجل حماية سيادتها أولاً، وحفظ السلم والأمن الدوليين ثانياً[٧٤]، وأمام هذا الواقع الذي تخطى الحدود الوطنية، حاولت مؤخراً عدة دول من خلال عدد من المعاهدات معالجة هذه التحديات والمخاطر التي فرضتها الحروب الإلكترونية، لأنه لا يوجد حتى هذه اللحظة نظام عالمي لمكافحة مساوئ الإنترنت، وفي الواقع لا يمكن معالجة التحديات القانونية والفنية والتنظيمية المتعلقة بالحروب الإلكترونية بشكل صحيح إلا من خلال اعتماد استراتيجية على المستوى الدولي يشارك فيها جميع ذوي العلاقة لمعالجة الأمر[٧٥]، ومن الجدير بالذكر أن التعاون الدولي في مجال مواجهة التهديدات الإلكترونية يرتكز على الأسس الآتية: [٧٦]

١. إنشاء مركز دولي للمعلومات والبيانات الخاصة بتلك التهديدات على مختلف صورها وأنماطها
٢. التنسيق بين المؤسسات الأمنية بأليّاتها المختلفة في الساحات الأمنية الإقليمية والدولية، بما يحقق حصر معدلات التهديدات.
٣. تحديد سبل التعاون في مجال التدريب والتعاون التقني، وتحقيق التكامل الأمني بين الأجهزة الأمنية على المستوى الدولي.
٤. إعداد مدونة دولية تتضمن توحيد المعايير والأركان القانونية التي تقوم عليها هذه الهجمات.
٥. وضع استراتيجيات وقائية قادرة على خلق مناخ ملائم لأعمال المكافحة، وتضييق الخناق على أنشطة تلك المنظمات وحرمانها من البيئة الملائمة لممارسة انشطتهم الإجرامية، وزيادة الوعي العام لدى الجماهير.

كما أن فرضية هذا المشهد مدعومة بمجموعة من العوامل أهمها: [٧٧]

أ- وجود توجهات باتجاه تشكيل تحالفات إقليمية ودولية لاسيما في موضوع مكافحة الإرهاب الإلكتروني، إذ أن التحالفات والشراكات الدولية تدفع باتجاه تفضيل التعاون على الصراع.

ب- تراجع خطر الجماعات الإرهابية وتحجيم قدراتها على إمكانية شن الهجمات؛ بسبب التحالف الدولي على الإرهاب.

ت- إدراك الدول لحجم المخاطر والكلف العالية المترتبة على الحروب والصراعات الإلكترونية، إذ إنها تستهدف قطاعات الحيوية المهمة داخل الدولة، ومنها الطاقة والكهرباء والمنشآت النووية والبنى التحتية والمعلوماتية، فلا ترغب أي دولة من الدول في إحداث حرب نووية مجهولة المصدر بسبب قرصنة تلك المنشآت النووية، فقد أشار (جيمس أكتون) المدير المشارك في برنامج السياسة النووية في مؤسسة(كارنيغي) للسلام الدولي، إن القلق لا يتركز في الهجمات على الأسلحة النووية نفسها، بل في أنظمة القيادة والتحكم المحيطة بها(قيادة الأسلحة النووية والتحكم بها هو كل شيء؛ لأنها ضرورية لتشغيل السلاح)، لذا فإن تعاظم الخطر النووي، ووجود الإدراك بها سيدفع إلى الحد من الهجمات الإلكترونية، ويشجع على إيجاد حلول للتحكم والسيطرة على الفضاء الإلكتروني، وكل ذلك يؤدي في النهاية إلى تراجع الصراعات الإلكترونية.

ثالثاً: مشهد تصاعد الصراع الإلكتروني:

يستند هذا المشهد على افتراض مفاده: إن التقدم المستمر في مجال الأسلحة الإلكترونية، وظهور أجيال جديدة للحروب مع استمرار التطور التكنولوجي، إلى جانب تسابق الدول للحصول على التقنيات المتطورة، في ظل عدم وجود ردع حقيقي للهجمات الإلكترونية يؤدي إلى تصاعد حدة الصراع الإلكتروني، أي كلما كان هناك فشل في معالجة العوامل المحفزة للصراع في الفضاء، كلما تزايد الصراع الإلكتروني.

إن المتتبع لسير الأحداث في النظام العالمي يلاحظ أن العالم يتجه نحو التطور التكنولوجي السريع، والذي قد يؤثر سلباً على الجانب العسكري ومستقبل الحروب والصراعات بين القوى المتعارضة [٧٨]، إذ يوفر هذا التطور مزايا عديدة للفاعلين الدوليين وغير الدوليين وتشجعهم على خوض صراعاتهم في الفضاء الإلكتروني بعيداً عن مخاطر الصراعات المسلحة الدامية والمكلفة، ومنها تنوع أسلحة الحروب الإلكترونية، وسهولة وقلة كلفة تصنيعها، وتواضع البنية التحتية لبناء جيوشها، وسهولة المناورة والاختفاء في إدارة مفاصل الحرب الالكترونية، مع ارتفاع حجم الدمار والأضرار التي تسببها في البنى التحتية للخصم، لاسيما مع انفتاح حدود المشاركة فيها من قبل الفاعلين من غير الدول، كل ذلك يفسر إقدام الكثير من الدول على التسابق لبناء ترسانة لها في ميادين الحرب الإلكترونية؛ لتعوض تخلفها في مجالات الأسلحة التقليدية، وبذلك ستكون الحرب الإلكترونية هي الشكل الرائج والأكثر فعالية في حروب القرن الحادي والعشرين، وهي البديل المستقبلي للحروب التقليدية الحالية[٧٩]، إذ يشير سيناريو حروب المستقبل بأنه لن يكون للأسلحة التقليدية الدور الرئيس في الصراعات والحروب، فمعظم الأسلحة التقليدية وهياكل القوات المسلحة مرشحة للاستبدال والاستغناء عنها مستقبلاً بأعداد صغيرة من الجنود، تكون على درجة عالية من الاستعداد، وذات روح معنوية مرتفعة، ومزودة بأجيال جديدة ومتطورة من الأسلحة والمعدات[٨٠]، كما أن آلة الحرب قد تكون باستخدام كبسة زر واحدة من لوحة مفاتيح أجهزة الحواسيب، والتي قد تدمر دولاً عديدة؛ نظراً للتطور الحاصل في توجيه الصواريخ وإمكانية التدمير.[٨١]

بالإضافة إلى ما سبق، هناك مجموعة من العوامل تساعد على تنامي التهديدات الإلكترونية لمصالح الدول، وتحفز تصاعد الحروب والصراعات الإلكترونية، ومن أهمها[٨٢]:

١. تزايد ارتباط العالم بالفضاء الإلكتروني، وهوما أدى إلى توسع خطر تعرض البنية التحتية للمعلومات إلى خطر التعرض للهجمات الإلكترونية، فضلاً عن استخدامه من قبل الفاعلين من غير الدول لتحقيق أهدافها.

تراجع دور الدولة في ظل العولمة والتطور التكنولوجي، وذلك بالتزامن مع تصاعد دور الشركات متعددة الجنسيات خاصة الشركات العاملة في مجال التكنولوجيا كفاعل مؤثر في الفضاء الإلكتروني، لاسيما مع امتلاكها قدرات تقنية تفوق الحكومات.

٢. نشوء نمط جديد من الضرر على خلفية الهجمات الإلكترونية التي يمكن أن تسببها دولة إلى أخرى، دون الحاجة للدخول المادي إلى أراضيها؛ وذلك يعود إلى تزايد اعتماد الدول على الأنظمة الإلكترونية

في جميع منشأتها الحيوية جعل هذه الأخيرة عرضة للهجوم المزدوج، لما لها من سمات مدنية وعسكرية متداخلة.

٣. قلة تكلفة الحروب الإلكترونية مقارنة بنظيرتها التقليدية، مع إمكانية شن الهجوم في أي وقت، بحيث لا يتطلب تنفيذه سوى وقت محدود.

٤. تحول الحروب الإلكترونية إلى إحدى أدوات التأثير في المعلومات المستخدمة في مستويات ومراحل الصراع المختلفة سواء على الصعيد الاستراتيجي أو التكتيكي العملياتي، بهدف التأثير بشكل سلبي في هذه المعلومات ونظم عملها. عادل عبد الصادق أنماط الحرب السيبرانية وتداعياتها على الأمن العالمي.

أن الموضوعية العلمية تفرض علينا ترجيح المشهد الأكثر احتمالاً للحدوث، والأقرب إلى الواقع طبقاً لمعطياته السائدة والمتوافقة مع الواقع العملي، وفي ضوء ذلك نجد أن المشهد الأكثر قرباً للواقع هو مشهد تصاعد الصراع الإلكتروني في القرن الحالي؛ بسبب الدلائل والمعطيات التي تشير إلى أن العالم يسير باتجاه ابتكار تكنولوجيات حديثة يوم بعد يوم، ولاسيما في مجال الأسلحة الإلكترونية، فالتطوير والبحث العلمي لن يتوقف ولن ينتهي عند حد معين، كما أن البيئة الدولية ليست مثالية لتنتهي فيها الصراعات والنزاعات بين القوى المتعارضة، بل إنها تشتد وتزداد قرن بعد قرن .

الخاتمة:

يتبين لنا من كل ما تقدم، أن الحروب الإلكترونية ظهرت كنوع جديد من أنواع الحروب في القرن الحادي والعشرين، إذ أن طبيعة الحرب لا تتغير ولكن سمات الحرب تتغير مع تطور أدوات الحرب، وخاصة في ظل التقدم التكنولوجي والتقني الذي تشهده العالم، والذي أضحى فيه الفضاء الإلكتروني ساحة جديدة للصراع والقتال بين الفواعل الدولية وغير الدولية، وبات يشكل الخيار المفضل للدول التي تعمل على نقل الصراعات نحو ميدان الفضاء الإلكتروني، والذي يعد فضاء مثالي لتوجيه الضربات للخصوم بأقل الكلف والتبعات، بالإضافة إلى ما سبق تميزت الحروب الإلكترونية بسرعة انتشارها وانتقالها إلى مختلف الدول، إذ أن أغلب الدول والفواعل غير الدولية لجأت إلى استخدامها، وباتت حتى الدول النامية وذات القدرة المحدودة تتوجه للحصول عليها وتوظيفها في صراعاتهم، وذلك بخلاف الأسلحة النووية التي تمتلكها عدد محدود من الدول، وهي تستهدف الأهداف المدنية والعسكرية على حد سواء، وتعمل وفق ألية معينة يمكن فيها استخدامها للدفاع وللهجوم على المؤسسات والبنى التحتية الحيوية للخصم، فضلاً عن توظيفها لدعم قطعات الجيوش في الحروب التقليدية.

الاستنتاجات

١. أن التطورات التكنولوجية غيرت من الأشكال التقليدية للصراع وأدخلت مفاهيم وأدوات جديدة للحروب والصراعات لم تكن موجودة من قبل، وظهر نوع جديد من الصراع وهو الصراع في الفضاء الإلكتروني

٢. على الرغم من تعدد واختلاف التعاريف التي تطرقت لمفهوم الحروب الإلكترونية وفسرت طبيعتها وألية عملها؛ إلا أن جميعها اتفقت على ارتباطها الوثيق بالتطور التكنولوجي وشبكات الانترنت وتزايد اعتماد الدول على تكنولوجيا في مختلف المجالات.

٣. تتنوع الأهداف التي تتعرض لها الهجمات الإلكترونية إذ أنها لا تقتصر على الأهداف العسكرية فحسب؛ بل تستهدف أيضا أهداف اقتصادية وسياسية وثقافية وقطاعات خدمية وانتاجية.

٤. تتمتع الحروب الإلكترونية بمجموعة من الخصائص تمنحها نوع من الجاذبية لتوظف من قبل الدول أو الفواعل من غير الدول، فمنظومة الأسلحة الإلكترونية لا تحتاج إلى أموال طائلة أو تقنيات وأجهزة معقدة يصعب اقتناؤها أو استخدامها، كما يسهل توفير الخبرات والكوادر المتخصصة لإدارتها وبرمجة وتنظيم عملها.

٥. أن حروب الفضاء الإلكتروني لا تحتاج إلى ساحات المعارك التقليدية؛ فالأنظمة المختلفة التي يعتمد عليها الناس من المصارف والمطارات والطائرات وبطاقات الائتمان وشبكات الطاقة والكهرباء، وصولاً إلى رادارات الدفاع الجوي وأنظمة الصواريخ يمكن الوصول إليها عبر الفضاء الإلكتروني والسيطرة عليها أو تعطيلها دون الحاجة إلى دحر الدفاعات التقليدية للدول.

٦. يصعب تحديد مصدر الهجمات الإلكترونية فقد تشن من داخل الدول دون علمها من لدن مجاميع صغيرة لكن لديها إمكانيات وقدرات إلكترونية مؤثرة، وهو ما أدى إلى قيام الفواعل غير الدولية بالعديد من النشاطات والهجمات من خلال الإمكانيات والتقنيات التي وفرتها الحروب الإلكترونية بالشكل الذي أصبح لهم دوراً في التأثير على سياسة الدول.

٧. في ضوء التطور التكنولوجي ظهرت أنواع متعددة من الأسلحة الإلكترونية التي يمكن استخدامها بسهولة لتنفيذ الهجمات وتحقيق الأهداف بدقة مثل الطائرات من دون الطيار والروبوتات والتي سوف تؤدي دوراً كبيراً ومُهِماً في حروب المُستقبل، فضلاً عن بث الفايروسات والبرامج التخريبية للأَنظمة والشبكات الحاسوبية والوصول إلى المعلومات السرية والاستِفادة مِنها لأَغراض عسكرية وأَمنية.

٨. غياب اتفاقية دولية شامِلة ومُلزمة في إِطار القانون الدولي تنطوي احكامها على ترتيب جزاءات وعقوبات على الأطراف التي تلجأَ إِلى شن هجمات إِلكترونية التي تخترق كُل الحواجز والحدود، وهو ما أَدى إِلى انكشاف أمن سيادة الدول، وتحرر الأطراف المُهاجمة مِن المُساءلة القانونية الدولية.

٩. أن الصراعات الإلكترونية سوف تتصاعد وتزداد في القرن الحادي والعشرين وذلك مع استمرار التقدُم العلمي وظهور الابتكارات التقنية الحديثة، وعدم وجود رادع قوي يحد من قدرة وإِمكانيات الدول في هذا المجال.

الهوامش والمصادر:

(١) غريب حكيم، شرقي صبرينة، تداعيات الحروب الإلكترونية على العلاقات الدولية: دراسة في الهجوم الألكتروني على إيران٠ فيروس ستكنست، مجلة دفاتر السياسة والقانون، العدد(٢)، كلية الحقوق والعلوم السياسية – جامعة قاصدي مرباح ورقلة، الجزائر، حزيران٢٠٢٠، ص٩٤.

(٢) محمد فتحي أمين، موسوعة أنواع الحروب، ط١، الأوائل للنشر والتوزيع، دمشق، ٢٠٠٦، ص١٦.

(٣) غريب حكيم، شرقي صبرينة، مصدر سبق ذكره، ص٩٤.

(٤) ريتشارد إيه كلارك– روبرت كيه كنيك، حرب الفضاء الألكتروني التهديد التالي للأمن القومي وكيفية التعامل معه، ط١، مركز الإمارات للبحوث والدراسات الاستراتيجية، الإمارات، ٢٠١٢، ص ٢١ .

(٥) إيهاب خليفة، مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي، ط١، العربي للنشر والتوزيع، مصر، ٢٠١٧، ص٤٧.

(٦) غريب حكيم، شرقي صبرينة، مصدر سبق ذكره، ص _ ص ٩٤_ ٩٥ .

(٧) سهيلة هادي، الحروب الإلكترونية في ظل عصر المعلومات، مجلة رؤى استراتيجية، العدد(١٤)، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبوظبي، يونيو ٢٠١٧، ص_ ص ١٢٦_ ١٢٧ .

(٨) المصدر نفسه، ص ١٢٨.

(٩) عبد الفتاح الطاهري، الأمن المعلوماتي وعلاقته بالأمن القومي، مجلة الباحث للدراسات القانونية والقضائية، العدد(١٠)، المغرب، فبراير٢٠١٩، ص ٣٤.

(١٠) شيماء جمال محمد، الحرب الإلكترونية واستراتيجية الدول لمواجهتها، مجلة كلية القانون للعلوم القانونية والسياسية، العدد(٣٦)، كلية القانون والعلوم السياسية_ جامعة كركوك، شباط ٢٠٢١، ص ٢٤٧.

(١١) عبد الفتاح الطاهري، مصدر سبق ذكره، ص ٣٤.

(١٢) سهيلة هادي، مصدر سبق ذكره، ص ١٢٨.

(١٣) حنان دريسي، الحرب السيبرانية: تحول في أساليب القتال وثبات في المبادئ والأهداف، مجلة الفكر القانوني والسياسي، العدد(١)، كلية الحقوق والعلوم السياسية_ جامعة عمار ثليجي الأغواط، الجزائر، ماي ٢٠٢٢، ص ٩١٨ .

(١٤) المصدر نفسه، ص ٩١٧.

(١٥) عبد القادر محمد فهمي، الحروب التقليدية وحروب الفضاء الإلكتروني: دراسة مقارنة في المفاهيم وقواعد الاشتباك، مجلة العلوم القانونية والسياسية، العدد(٢)، الجمعية العلمية للبحوث والدراسات الاستراتيجية، كانون الأول ٢٠١٨، ص٢٢.

(١٦) غريب حكيم، شرقي صبرينة، مصدر سبق ذكره، ص ٩٦ .

(١٧) فيصل محمد عبدالغفار، الحرب الإلكترونية، ط١، الجنادرية للنشر والتوزيع، عمان_ الأردن، ٢٠١٦، ص_ ص ١١_١٢.

(١٨) عبد القادر محمد فهمي، مصدر سبق ذكره، ص٢٢.

(١٩) حنان دريسي، مصدر سبق ذكره، ص٩١٨.

(٢٠) فيصل محمد عبدالغفار، مصدر سبق ذكره، ص ١٢.

(٢١) عبد القادر محمد فهمي، مصدر سبق ذكره، ص ٢٣ .

(٢٢) المصدر نفسه، ص ٢٣.

(٢٣) ريتشارد إيه كلارك_ روبرت كيه كنيك، مصدر سبق ذكره، ص ٢٤٩.

(٢٤) عبد الفتاح الطاهري، مصدر سبق ذكره، ص ٣٥.

(٢٥) حمدان محمد الطيب، خينش ماجدة،الحروب الإلكترونية وتأثيرها على سيادة الدول، مجلة الدراسات القانونية والسياسية، العدد(٧)،جامعة عمار ثليجي الأغواط، الجزائر،جانفي٢٠١٨، ص٢٣.

(٢٦) عبد الفتاح الطاهري، مصدر سبق ذكره، ص ٣٥_ ٣٦ .

(٢٧) إيهاب خليفة، القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت، ط١، العربي للنشر والتوزيع، القاهرة، ٢٠١٧، ص٨٣.

(٢٨) شيماء جمال محمد، مصدر سبق ذكره، ص ٢٤٥.

(٢٩) حمدان محمد الطيب، خينش ماجدة، ، مصدر سبق ذكره، ص_ ص٢٣_٢٤.

(٣٠) عبد الفتاح الطاهري، مصدر سبق ذكره، ص ٣٧.

(٣١) سهيلة هادي، مصدر سبق ذكره، ص ١٢٩.

(٣٢) حمدان محمد الطيب، خينش ماجدة، ، مصدر سبق ذكره، ص ٢٤.

(٣٣) شيماء جمال محمد، مصدر سبق ذكره، ص_ ص ٢٤٥_ ٢٤٦.

(٣٤) حمدان محمد الطيب، خينش ماجدة، ، مصدر سبق ذكره، ص_ ص ٢٤_ ٢٥.

(٣٥) عبد الفتاح الطاهري، مصدر سبق ذكره، ص ٤٠.

(٣٦) المصدر نفسه.

(٣٧) جبارة نورة، الطائرات بدون طيار: التنظيم والمسؤولية المدنية، مجلة دراسات وأبحاث: المجلة العربية للأبحاث في العلوم الإنسانية والاجتماعية،العدد(٤)، جامعة زيان عاشور الجلفة، الجزائر، جويلية ٢٠٢١، ص ٤٠٩ .

(٣٨) عبد الفتاح الطاهري، مصدر سبق ذكره، ص٤٠.

(٣٩) إنجي المهدي، الإرهاب الإلكتروني: الظاهرة والتداعيات: "الاستخدام من قبل التنظيمات الجهادية"، المجلة الاجتماعية القومية، العدد(١)، المركز القومي للبحوث الاجتماعية والجنائية، القاهرة، يناير ٢٠٢١، ص_ ص ٣٨_ ٣٩ .

(٤٠) سهيلة هادي، مصدر سبق ذكره، ص ١٢٩.

(٤١) خالد حنفي علي،إشكاليات تداخل الصراعات السيبرانية والتقليدية،ملحق مجلة السياسة الدولية، العدد(٢٠٨)،مركز الأهرام للدراسات السياسية والاستراتيجية، القاهرة، ابريل٢٠١٧،ص٣

(٤٢) علي عبد الرحيم العبودي، هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين، مجلة قضايا سياسية، العدد(٥٧)،كلية العلوم السياسية،جامعة النهرين،حزيران٢٠١٩، ص٩٥.

(٤٣) قاسم خضير عباس العزاوي، ديناميكيات الحروب الإلكترونية وأثرها في الصراع الدولي، دراسة بحثية منشورة في موقع مركز الديمقراطي العربي، تاريخ النشر: ٢٠٢١/٢/٢٢، تاريخ الزيارة: ٢٠٢٢/٨/٢٢، متاح على الرابط الآتي: https://democraticac.de/?p=73151

(٤٤) خالد حنفي علي، مصدر سبق ذكره، ص ٣.

(٤٥) محمود علي عبدالرحمن، أسامة فاروق مخيمر، الفضاء الإلكتروني وأثره على مفاهيم القوة والأمن والصراع في العلاقات الدولية، مجلة كلية السياسة والاقتصاد، العدد(١٥)، كلية السياسة والاقتصاد_ جامعة بني سويف، مصر، يوليو ٢٠٢٢، ص ٤٣٢.

(٤٦) نورة شلوش، القرصنة الإلكترونية في الفضاء السيبراني" التهديد المتصاعد لأمن الدول"، مجلة مركز بابل للدراسات الإنسانية، العدد(٢)، مركز بابل للدراسات الحضارية والتاريخية_ جامعة بابل، حزيران ٢٠١٨، ص_ ص ١٩٣_١٩٧.

(٤٧) بشلالق ليلى، تأثير الحروب الإلكترونية على العلاقات الأمريكية الروسية، رسالة ماجستير غير منشورة، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف_المسيلة، الجزائر، ٢٠١٩، ص٣٣.

(٤٨) عادل عبد الصادق أنماط "الحرب السيبرانية" وتداعياتها على الأمن العالمي، ملحق مجلة السياسة الدولية، العدد(٢٠٨)، مركز الأهرام للدراسات السياسية والاستراتيجية، القاهرة، أبريل ٢٠١٨، ص ٣٣ .

(٤٩) عادل عبد الصادق، مصدر سبق ذكره، ص ٣٤.

(٥٠) محمود علي عبدالرحمن، أسامة فاروق مخيمر، مصدر سبق ذكره، ص ٤٣٣ .

(٥١) علاء الدين فرحات، الفضاء السيبراني: تشكيل ساحة المعركة في القرن الحادي والعشرين، مجلة العلوم القانونية والسياسية، العدد(٣)، كلية الحقوق والعلوم السياسية_ جامعة الشهيد حمه لخضر_ الوادي، الجزائر، ديسمبر ٢٠١٩، ص ٩٢.

(٥٢) بسمة يونس محمد الرفادي، الحروب السيبرانية وأثرها في التنظيم الدولي، مجلة العلوم والدراسات الإنسانية، العدد(٤٩)، كلية الآداب والعلوم_ المرج، جامعة بنغازي، ليبيا، فبراير ٢٠١٨، ص ٧ .

(٥٣) أنمار موسى جواد، حرب الفضاء الإلكتروني المفهوم_ الأدوات والتطبيقات، مجلة العلوم القانونية والسياسية، العدد(٢)، كلية القانون والعلوم السياسية_ جامعة ديالى، كانون الأول ٢٠١٦، ص ١٤٣.

(٥٤) شريفة كلاع، الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الإنسانية، العدد(١)، كلية الحقوق والعلوم السياسية_ جامعة زيان عاشور، الجزائر، أبريل ٢٠٢٢، ص ٣٠٢.

(٥٥) حسين قوادرة، منى كحلوش، التداعيات الاقتصادية لحرب المعلومات السيبرانية، مجلة الناقد للدراسات السياسية، العدد(١)، كلية الحقوق والعلوم السياسية_ جامعة محمد خيضر بسكرة، الجزائر، أبريل ٢٠٢١، ص_ ص ٢١٠_٢١١.

(٥٦) أنمار موسى جواد، مصدر سبق ذكره، ص_ ص ١٤١_١٤٢ .

(٥٧) شريفة كلاع، مصدر سبق ذكره، ص ٣٠١ .

(٥٨) ماجد محمد الحنيطي، الحرب الإلكترونية وأثرها على الصراعات الدولية المعاصرة، أطروحة دكتوراه غير منشورة، كلية الدراسات العليا_ جامعة مؤتة، الأردن، ٢٠١٧، ص٨٧.

(٥٩) ماجد محمد الحنيطي مصدر سبق ذكره، ص_ ص ٨٥_٨٦.

(٦٠) شريفة كلاع، مصدر سبق ذكره، ص_ ص٣٠٠_٣٠١ .

(٦١) لمى عبد الباقي محمود، اسراء نادر كيطان، المسؤولية الدولية عن الأضرار التي تحدثها الهجمات الإلكترونية، مجلة العلوم القانونية، العدد الخاص لبحوث التدريسيين مع طلبة الدراسات العليا، الجزء الثاني، المجلد(٣٦)، كلية القانون_ جامعة بغداد، أيلول ٢٠٢١، ص ٣٥٥ .

(٦٢) ماجد محمد الحنيطي، مصدر سبق ذكره، ١٠٤.

(٦٣) المصدر نفسه، مصدر سبق ذكره، ص_ ص ٨٨_٨٩.

(٦٤) المصدر نفسه، ص ١٠٤.

(٦٥) علاء الدين فرحات، مصدر سبق ذكره، ص ٩٣ .

(٦٦) ساسوي خالد، بن حسين محمد، الحروب السيبرانية والأمن العالمي التحديات والمواجهة، رسالة ماجستير غير منشورة، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجزائر، ٢٠٢٠، ص ٤١ .

(٦٧) صلاح حيدر عبدالواحد، حروب الفضاء الإلكتروني: دراسة في مفهومها وخصائصها وسبل مواجهتها، رسالة ماجستير غير منشورة، كلية الآداب والعلوم_ قسم العلوم السياسية، جامعة الشرق الأوسط، الأردن، ٢٠٢١، ص ٢٩.

(٦٨) معيزي ليندة، دهقاني أيوب، الثورة الرقمية في المجال العسكري وتداعياتها على الحروب الحديثة (الحروب السيبرانية نموذجاً)، المجلة الجزائرية للحقوق والعلوم السياسية، العدد(١)، كلية الحقوق_ جامعة أحمد بن يحيى الونشريسي، الجزائر، حزيران ٢٠٢٢، ص ٩.

(٦٩) الصراع بين روسيا والغرب يدخل العالم عصر الحروب السيبرانية، صحيفة أخبار اليوم، تاريخ النشر: ٢٠٢٢/٣/١٣، تاريخ الزيارة: ٢٠٢٢/٨/٢٨، متاح على الرابط الآتي: https://m.akhbarelyom.com/news/newdetails/3699585/1

(٧٠) تغريد صفاء مهدي، توظيف القوة السيبرانية في الأداء الاستراتيجي الأمريكي، أطروحة دكتوراه غير منشورة، كلية العلوم السياسية_ جامعة النهرين، ٢٠٢١، ص_ ص ٢٠٠_ ٢٠١.

(٧١) شريفة كلاع، الصراع الروسي_ الصيني_ الأمريكي للاستحواذ على الهيمنة في الفضاء السيبراني، مجلة السياسة العالمية، العدد(١)، مخبر الدراسات السياسية والدولية، جامعة محمد بوقرة_ بومرداس، الجزائر، حزيران٢٠٢٢، ص_ ص١٠١٤_١٠١٥.

(٧٢) تغريد صفاء مهدي، مصدر سبق ذكره، ص٢٠١.

(٧٣) ياور عمر محمد، استراتيجية الحرب في القرن الحادي والعشرين، حرب الفضاء الإلكتروني نموذجاً، رسالة ماجستير غير منشورة، كلية القانون والعلوم السياسية_ جامعة كركوك، ٢٠٢٠، ص_ ص ١٩١_١٩٢ .

(٧٤) عادل عبد الصادق، استخدامات الفضاء الإلكتروني من منظور التدخل الخارجي، مجلة السياسة الدولية، العدد (٢١٠)، مركز الأهرام للدراسات السياسية والاستراتيجية، القاهرة، أكتوبر ٢٠١٧، ص ٣٢.

(٧٥) تغريد صفاء مهدي، مصدر سبق ذكره، ص ٢١٢.

(٧٦) عادل عبد العال إبراهيم، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة للنشر والتوزيع، ط١، الإسكندرية، ٢٠١٥، ص ١٩٣.

(٧٧) مهند جبار عباس، الحروب السيبرانية ومستقبل الأمن الدولي، أطروحة دكتوراه غير منشورة، كلية العلوم السياسية_ جامعة النهرين، ٢٠٢٢، ص_ ص٢٣٦_٢٣٧.

(٧٨) ياور عمر محمد، مصدر سبق ذكره، ص ١٨٦ .

(٧٩) سامر مؤيد عبد اللطيف، الحرب في الفضاء الرقمي رؤية مستقبلية، مجلة رسالة الحقوق، العدد(٢)، كلية القانون_ جامعة كربلاء، آب ٢٠١٥، ص _ ص١٠٥_ ١٠٦ .

(٨٠) صفات أمين سلامة، أسلحة حروب المستقبل بين الخيال والواقع، دراسات استراتيجية، مركز الإمارات للدراسات والبحوث الاستراتيجية، ابوظبي، ٢٠٠٥، ص ٣٠ .

(٨١) ياور عمر محمد، مصدر سبق ذكره، ص ١٨٦ .

(٨٢) ليلى بشلالق، مصدر سبق ذكره، ص_ ص ٣٩_ ٤٠ .