الحـرب في الفضـاء الرقمي رؤيـة مستقبليـة

بحث مقدم من قبل
الاستاذ المساعد الدكتور سامر مؤيد عبد اللطيف
جامعة كربلاء/مركز الدراسات القانونية والدستورية

الخلاصــة.

مع التطور التقني المتسارع الذي عاشه العالم في العقود الأخيرة، زاد إعتماد الدول، بصورة كبيرة، على الحاسوب في إدارة وتوجيه أنشطتها المختلفة، وأصبحت الشبكة الدولية للمعلومات، من ثم، ليس فقط العمود الفقري لتبادل المعلومات على صعيد عالمي، بل انها قد اسهمت في ايجاد عالم آخر هو (العالم الرقمي). وقد انتقلت تداعيات هذه الثورة المعرفية، وما يرتبط بها من تكنولوجيا متطوِّرة بصورة فاعلة، إلى ميدان الحرب وأدواتها في إطار ما يعرف بالحرب الإلكترونية، الأمر الذي ادى إلى تنوع صور هذه الحرب وأساليب إدارتها وحتى أهدافها؛ إذ انتقلت العديد من وسائل السيطرة والتحكم الخاصة بمعظم العمليات الحربية الموجودة على الأرض إلى الحاسوب الآلي، مثلما انتقل جانب من المواجهات الحربية (غير الدامية) إلى العالم الافتراضي، حتى أمكن تبني إفراض مفاده أن الصيغة المستقبلية للحرب ستكون في الفضاء الرقمي وباستخدام الشبكة الدولية للمعلومات.

الكلمات المفتاحية:الحرب الإلكترونية ،الفضاءالرقمي، ألإستراتيجية والسياسة الدولية، والمستقبل.

Abstract.

With the rapid technological developments in the world in last decades, the states have adopted increasingly on the computer in management and guidance of its various activities. After that the international network of information has become, not only the backbone for the information s exchange on a global scale, but also contributed in creating another world is (Digital World). The repercussions of this revolution knowledge and its sophisticated technology that associated with it have moved effectively into the field of war and its tools, in the context of what is known as(cyber warfare), which led to the diversity of images and methods of this war and even its goals; since many means of control on military operations have moved into the cyber field, just as the military confrontations (non-bloody)have moved to the virtual world. At this point ,we can adopt the assumption that the future war will be in the digital space (cyber warfare).

Key words: Cyber warfare, strategy, international policy and the future.

المقدمـــة.

أولاً // أهمية البحث.

أحدث ظهور ثورة تكنولوجيا المعلومات واستخدامها في الأغراض العسكرية والحروب الحديثة تطوراً هائلاً في إدارة الصراع وبلوغ أهدافه؛ فقد منحت هذه الثورة، وما يرتبط بها من تكنولوجيا متطوِّرة الفرصة لمن يملكها بأن يكون له التفوق والسيطرة في ميادين الحروب؛ بالنظر لما تتميز به من قدرات للتأثير بفاعلية على إمكانات العدو، والحد من تأثير أسلحته في ساحة القتال بخلاف الحروب التقليدية، فإن الحرب الإلكترونية الحديثة لا تحتاج إلى كميات هائلة من الموارد مثل الأسلحة والأفراد والمعدات، بل تحتاج لشخص لديه معرفة واسعة في أحداث ضرر في الأنظمة، أو التسلل إلى الأجهزة البعيدة من خلال إستخدام الإنترنت أو أنظمة الإتصال الأخرى. وإذا كانت المعارك الحقيقية تخلف قتلى وجرحى، فإن المعارك الإلكترونية يمكن أن تتفوق على المعارك التقليدية من حيث الخسائر المادية والأضرار التي تتركها على الدول والمجتمعات؛ فبدلاً من استخدام الرصاص والقنابل تصبح لوحة المفاتيح والبرمجيات هي الأكثر ضرراً مجال الدمار الذي يلحق العدو. عليه فقد تعاظم دور الحرب الإلكترونية لتشكل البعد الرابع بين أسلحة القتال البرية، والبحرية، والجوية والدفاع الجوي في التأثير بفاعلية على كفاءة هذه النظم الإلكترونية، بل أنها مرشحة في المستقبل لأن تكون ميداناً مستقلا للمعارك بين الدول بعيداً عن الميادين والأسلحة التقليدية. ومع ندرة الدراسات الأكاديمية حول هذا النوع من الحروب، يوازيه غياب في الاستعداد لمواجهة التحديات التي تفرضها الحرب الإلكترونية، ولاسيما في ظل التطورات المتسارعة التي تخضع لها برامجيات الحاسوب والشبكة الدولية للمعلومات، تنبني الحاجة الماسة لخوض هذا الموضوع وسبر أغواره.

ثانياً // مشكلة البحث.

تنبع مشكلة البحث من سؤال محوري مفاده: كيف أثرت التقنيات الرقمية في مسار الحروب الحديثة؟ وما الصورة المستقبلية لهذه الحروب؟

ثالثاً // هدف البحث.

يسعى الباحث إلى إثبات فرضية مفادها: "أن استخدام الحاسبات الإلكترونية، سواء في إدارة الإشتباك المسلح أثناء المعارك الحربية او حتى أثناء الصراع غير المسلح، قد أحدث نقلة نوعية في فنون الحرب الحديثة ووسائلها، وسيكون لذلك تأثيرات عميقة على مستقبل الصراعات الدولية" .

رابعاً // منهجية البحث.

يستعين الباحث عند معالجته لمعطيات الموضوع بأدوات المنهجين الوصفي والوظيفي؛ لكشف ماهية هذا النوع من الحروب من جانب، ثم تبيان دورها في إدارة النزاعات المسلحة وغير المسلحة بين الدول وحسمها من جانب آخر، مع اعتماد منهج بناء المشاهد المستقبلية لمسار هذه الحروب في ظل المعطيات الميدانية الراهنة.

خامساً // خطة البحث.

تنقسم خطة البحث على ثلاثة مباحث رئيسة، يتصدى الأول منها إلى تبيان مفهوم الحرب الإلكترونية وتتبع تطورها التأريخي. وينصرف المبحث الثاني إلى توضيح صور الحرب الإلكترونية وأساليبها. وفي المبحث الثالث والأخير سيتم تسليط الضوء على الآفاق المستقبلية للحرب الإلكترونية، ثم خاتمة البحث التي سنضمنها أهم النتائج والمقترحات التي سنتوصل اليها الباحث.

المبحث الأول/ مفهوم الحرب الإلكترونية وتطورها التأريخي.

ارتبط مسار الحروب عبر تأريخها الطويل، بالتطورات التقنية التي عرفتها الجماعات البشرية، وسخرتها في سبيل تطوير قدراتها القتالية، وصولا لتحقيق أهدافها، وتامين مصالحها الحيوية المنشودة من خوض النزاع المسلح، فكانت الأخيرة بحق المختبر الواقعي والدموي لما دشنته تلك الامم من معارف. ومع ولوج الحضارة ألإنسانية عصر المعلومات والتقنيات الحديثة شهدت ساحات الحروب ولادة جيل جديد من المنظومات القتالية التي اعتمدت على التقنيات الإلكترونية والحاسوب في إدارة المعارك او اسنادها، والتي صارت تعرف بـ(الحرب الإلكترونية). ومما تقدم اضحى من الضروري الوقوف على تعريف مفهوم الحرب الإلكترونية وتتبع تطورها التأريخي في المطلبين ألآتيين:

المطلب الأول/ تعريف الحرب الإلكترونية وذاتيتها.

تعرض مفهوم الحرب الإلكترونية لجدل اكاديمي واسع عبّر عن تقاطع في الرؤى والخلفيات الايديلوجية والمعرفية؛ لمن تناوله بالبحث والتحليل والتطورات المتسارعة التي مر بها هذا المفهوم وإستخداماته المتنوعة، حتى اتسع نطاق هذه المفهوم ليتداخل في نطاقه مع مفاهيم مقاربة. ومن هذا المنطلق وجب الوقوف على تعريف الحرب الإلكترونية، تمييزها، ومن ثم، عن غيرها من المفاهيم المقاربة، في الفرعين ألآتيين:

الفرع الأول/ تعريف الحرب الإلكترونية.

من حيث الاصل والمبنى، أشتق مصطلح الحرب لغةً من الجذر (حرب حربا) اي تعب، وإذا اخذ جميع ماله فهو حريب، والحرب تعني المقاتلة والمنازلة.[i] وبوصف مقارب، حربه يحربه حربا أي أخذ ماله وحرب الرجل ماله، وحاربه حراباً أقام عليه الحرب. [ii] أما إصطلاحاً، فقد أخذت الحرب مساحة أكثر اتساعا وتعقيداً عند التعريف بها، لنجد من يعرفها على أنها (نزاع بين الوحدات السياسية تستعمل فيه القوة المسلحة)[iii]. وإذا كان اصطلاح النزاع يقترب من التوصيفات القانونية لأي خصومة بين طرفين، فإن الوحدات السياسية هي من ستخرجه من دائرة الصبغة القانونية لتدخله آتون المواجهة السياسية على إختلاف مستوياتها وأطرافها المحلية والدولية؛ شريطة ان يكون هذا النزاع مسلحا. وهنا يخفق التعريف في ادراك المستوى المنشود من الحرب غير الدامية التي يكون ميدانها الفضاء الرقمي - مجال البحث وغايته - على الرغم من كونه(أي التعريف)، قد أصاب في رسم الحدود التقليدية للحرب. ولا يبتعد باحث آخر عن المسار السابق في رسم ملامح الحرب عبر تضييق النطاق الواسع لمفردة الصراع ضمن حدود الإستخدام المسلح، فعرفها بكونها (صراع مسلح بين جماعات منظمة لكل منها هدف تعتبر أنه لا يمكن التوفيق بينها).[iv] ويبقى باحث آخر عند محور العنف في تشخيص ملامح الحرب مع تضييق نطاقها ضمن نطاق الدولة مستبعداً القوى والجماعات غير الدولية؛ فيعرف الحرب على أنها (عنف منظم تشنه

الدولة لمصلحة الدولة وضد الدولة)[v]. وبكل الأحوال والتوصيفات لم تخرج الحرب عن دائرة وصفها بكونها (مواجهة مسلحة بين طرفين- دول او جماعات - لتحقيق أهداف محددة). ومع اقتران الحرب بالتقنيات الإلكترونية التي افضت اليها ثورة المعلومات في القرن العشرين، ظهر مصطلح جديد هو (الحرب الإلكترونية) التي يمكن استخراج معناها باعتماد مدخلين، يعتمد الأول منهما، الوسائل الإلكترونية المستخدمة أثناء الاشتباك المسلح كدليل لتعريف الحرب الإلكترونية، انها: (ذلك الجزء من الاستخدام الإلكتروني العسكري الذي يتضمن الاعمال المتخذة او لتقليل الاستخدام الفعال من قبل العدو للطاقة الالكترومغناطيسية المشعة والاعمال المتخذة لضمان الاستخدام الايجابي من قبل القطعات للطاقة الالكترومغناطيسية)[vi] على أن ما ذكره أحد الباحثين في الشؤون الاستراتيجية والحربية، يجلي لنا بوضوح تعريف هذا المصطلح بقوله: «هو مجموعة الإجراءات التي تُنفذ بهدف الاستطلاع الإلكتروني للنظم والوسائل الإلكترونية المعادية، وإخلال عمل هذه النظم والوسائل الإلكترونية، ومقاومة الاستطلاع الإلكتروني المعادي، وتحقيق استقرار عمل النظم الإلكترونية الصديقة تحت ظروف استخدام العدو أعمال الاستطلاع، والإعاقة الإلكترونية».فهو يضيف بعدًا أكثر عمقًا من مجرد التصارع في إطار الفضاء اللاسلكي أو المجال الكهرومغناطيسي.[vii] وبتعبير جامع مانع ومختصر يقدمه الفقه الغربي للحرب الإلكترونية (Ew) بأنها "أي عمل عسكري ينطوي على استخدام الطيف أو الطاقة الموجهة للسيطرة على أو لمهاجمة العدو"[viii] . والملاحظ على هذا المستوى من التعريفات المختلفة للحرب الإلكترونية حرصها على عدم الخروج من ساحة الإشتباك المسلح من جانب، والتركيز المكثف على التحكم بمجالات الطاقة الكهرومغناطيسية؛ لتحقيق التفوق النوعي على الخصم، سواء مر ذلك عبر بوابة الحاسبة الإلكترونية او اكتفى بتوظيف أنظمة الدوائر الإلكترونية والموجات الكهرومغناطيسية التقليدية الموروثة من بدايات القرن السابق من جانب آخر. ومن هنا ينشأ الانفصال النوعي بين الجيل التقليدي للحرب الإلكترونية والجيل المعاصر والمستقبلي لمثل هذه الحروب بالاستعاضة عن الطيف الكهرومغناطيسي والاعتماد الكلي على الحاسبة الإلكترونية والفضاء الرقمي في إدارة الحرب وإخضاع الخصم، سواء تم اللجوء إلى الاشتباك المسلح ام لم يتم ذلك؛ إذ تعرف الحرب الإلكترونية، وفقا لهذا المدخل المعاصر بدلالة مفاهيم منها (الحرب الرقمية او السيبيرية او حرب الشبكات). إن هذا المفهوم الجديد، جرى تداوله لأول مرة، من قبل الباحث الاستراتيجي (جون اركيلا) في مقالة نشرت عام 1993 بعنوان "حرب الانترنت قادمة"، الذي عد فيها (حرب الانترنيت) ، شكلاً من أشكال الحرب التي يتم بوساطتها تعطيل، او حتى تدمير المعلومات ونظم الإتصالات. وفي خضم التطور الكبير في تكنولوجيا المعلومات والاستخدام الواسع لخدمات الانترنيت في كل مفاصل الدولة ومؤسساتها، رجح احتمال اللجوء إلى هذا النمط من الحرب الرقمية؛ لتكون النمط المهيمن من أنماط الحروب المستقبلية. [ix] وعندما تصدت الأكاديمية الحربية الأمريكية لتعريف هذا النوع من الحرب اشارت إلى أنه (نمط من هجمات الشبكات الكمبيوترية التي يتم إتخاذها للتأثير بشكل سلبي على المعلومات ونظم المعلومات للخصم، وفي الوقت نفسه الدفاع عن هذه المعلومات والنظم التي تحتويها). وحسب تعريف هذه الأكاديمية فإن العمليات الإلكترونية تتضمن أنشطة مثل (أمن العمليات، والعمليات النفسية، والخداع العسكري، والهجمات الفيزيائية، والهجمات على شبكات الكمبيوتر)، وتكون المعلومات بمثابة الهدف الرئيس لعملها ومجال تأثيرها. وبتوصيف مقارب عرفت لجنة الخدمات الحربية في الكونغرس الأمريكي (الحرب الإلكترونية)، وفق صورتها المعاصرة على أنها (توظيف قدرات الفضاء الإلكتروني في الهجوم والدفاع ضمن نطاق شبكة الكمبيوتر لتحقيق

أهداف العسكرية أو غيرها من الأهداف ألإستراتيجية).[x] وضمن الفضاء الإلكتروني ذاته قدم باحث آخر تعريفه للحرب الإلكترونية بأنها (مهاجمة شبكات العدو بهدف تعطيلها أو الحد من قدرتها على الهجومية والدفاعية على حد سواء بإستخدام الشبكة الدولية للمعلومات مع توفير القدرة على حماية الشبكات المحلية وحماية التواصل مع الجنود في الميدان، وحماية قدرات جمع المعلومات عن أنشطة العدو).[xi] وفي المكتبة العربية، عرفها أحد الباحثين في المجال الهندسي على أنها (إنتقال الهجمات إلى رحاب الفضاء التخيلي (مواقع الانترنت) بغرض تدميرها او تعطيلها او تشويه محتوياتها وتعطيل البريد الإلكتروني لجهات حساسة وشخصيات على مستوى القيادة السياسية) [xii] ما يسجل على ما تقدم من تعريفات الجيل الثاني للحرب الإلكترونية خروجها من مجال الطيف الكهرومغناطيسي وإستخدامها لأنظمة الكومبيوتر فضلاً عن خروجها النسبي عن دائرة الصراع المسلح وإقترابها من البعد غير المسلح للصراع بمداه الواسع؛ فحتى ساحة العمليات لم تعد ضمن الوصف المعاصر محددة بالميادين التقليدية للمواجهة المسلحة بل تعدتها إلى الفضاء الإلكتروني لشبكة المعلومات الدولية (الانترنيت). إزاء ما تقدم من تعريفات لمصطلح الحرب الإلكترونية، يمكن إستخلاص المزايا الإسترتيجية الأساسية لهذا النوع من الحروب وهي ألآتي:

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

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

3. تمتّع المهاجم بأفضلية واضحة في حروب الإنترنيت على المدافع، فهذه الحروب تتميز بالسرعة والمرونة والمراوغة وفي بيئة مماثلة يتمتّع بها المهاجم بأفضليّة، من الصعب جداً على عقليّة التحصّن لوحدها أن تنجح؛ فالتحصين بهذا المعنى سيجعل من هذا الطرف عرضة لمزيد من محاولات الاختراق، وبالتالي المزيد من الضغط.

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

5.حرب هلامية الشكل والملامح، فهي متعددة بميادينها، متنوعة ومتطورة بوسائلها المرتبطة بأكثر المجالات التقنية تطوراً وتبدلاً في الحياة المعاصرة للدول، وهي، فضلاً عن ذلك، غير محددة الأهداف والتأثيرات، إذ قد تتعدى مخاطرها ميادين القتال التقليدية لتطال بدمارها حتى أكثر المواقع السيادية والحساسة تحصيناً وبعداً عن دائرة القتال. [xv]

الفرع الثاني/ذاتيـة الحرب الإلكترونيـة.

يتم في أحيان استخدام مفهوم الحرب الإلكترونية بدلالة مفاهيم أخرى مقاربة بسبب التداخل الذي قد يحصل بينها من حيث الطبيعة والنطاق والوظيفة مع مفاهيم مقاربة من أهمها (حرب المعلومات وألإرهاب الإلكتروني). ولتثبيت الحدود الفاصلة بين تلك المفاهيم جرى تقسيم هذا الفرع على محورين.

أولا // تمييزهـا من حـرب المعلومـات.

للوهلة الأولى لا يمكن - بحال من ألأحوال- ايجاد الفارق النوعي، او فض الإشتباك والتداخل، بين المفهومين، لاسيما وأن العديد من الباحثين قد وظفوا هذين المفهومين بصورة متبادلة. وبتثبيت القاعدة المعرفية لمفهوم حرب المعلومات كمنطلق للتمييز بين المفهومين، نجد أن أحد الباحثين يعرف حرب المعلومات على أنها (أي عمل الغاية منه إرغام الخصم على الخضوع لإرادتنا الوطنية وتنفيذ برامج الغاية منها السيطرة على نظام معلوماته)، وعلى الطريق ذاته سار باحث آخر في تعريفها بكونها (نوع من حرب المعلومات التي تؤدي إلى أحداث خلل في أنظمة المعلومات للخصم) [xvi] وكان أحد علماء الرياضيات الأمريكيين، وهم الأكثر دقة في توصيف حرب المعلومات وتثبيت حدودها الموضوعية عبر إعتماد آلية متسلسلة لتصنيف أنواعها وفق السياق ألآتي [xvii].

1.الحرب الإلكترونية التقليدية (EW).
2. الحرب النفسية .
3. حرب القرصنة الإلكترونية
4. حرب المعلومات ألإقتصادية (EIW).

يتضح من هذا التصنيف أن حرب المعلومات، وإن كانت تشترك مع الحرب الرقمية بالمعلومة التي يجري توظيفها لتحقيق النصر، فإن حرب المعلومات (في الوقت عينه) أكثر اتساعا وشمولاً من الحرب الرقمية، سواء في أدواتها التي تتعدى الأنظمة الحوسبية لتشمل أنظمة الاتصال والإعلام والسيطرة وغيرها، أو في ساحاتها التي تشمل الفضاء الرقمي والكهرومغناطيسي أيضاً، أو حتى على صعيد أهدافها التي تتعدى أبعاد التدمير المادي لتصل إلى المعنويات، وما يلحقها من مستلزمات إدارة الحروب بكل أشكالها لتحقيق غاية النصر وإخضاع الخصم. فتكون الحرب الإلكترونية (الرقمية) التي يقتصر مضمارها على الشبكة الإلكترونية للمعلومات، وسلاحها وميدانها أيضاً هو الحاسبة الإلكترونية وسيلة من بين الوسائل المتعددة التي توظفها حرب المعلومات ضد ألأعداء . فتكون العلاقة بين هذين النوعين من الحروب على شاكلة العلاقة بين الجزء الذي تمثله الحرب الإلكترونية (الرقمية) والكل الذي تمثله حرب المعلومات، عبر رابطة تتكامل فيها ألأدوار بينهما لتتصل فيما بعد بوحدة الهدف.

ثانيا // تمييزها من الإرهاب الإلكتروني.

طبقا لتعريف وكالة المباحث الفيدرالية الأمريكيّة يعد ألإرهاب الإلكتروني: (كل هجوم مخطط له بدافع سياسي ضد المعلومات، وأنظمة الحاسب الآلي، وبرامج الحاسب، والبيانات مما يؤدي إلى العنف ضد أهداف غير حربية من قبل مجموعات وطنية فرعية أو عملاء متخفين).[xviii] وفي هذا التعريف يلاحظ أن ورود كلمة (الهجوم)، لم يقتصر على الهجوم المعلوماتي، فقد أطلق بصورة عامة ليشمل حتى الإرهاب بشكله التقليدي، ضد بنية المعلومات، وأورد التعريف أيضاً كلمة العنف ليؤكد على هذا المعنى، ويمكن أن نقول بأن تعريف الإرهاب الإلكتروني ينبغي أن يشمل أشخاص (مرتكبي) الأعمال، (وأدوات) تنفيذ الأعمال الإرهابية، من برامج، أو أجهزة، أو مستوى المعرفة الفنية، والعلمية الموظفة كما يلزم عند محاولة توصيف هذه الظاهرة التأكد من تحديد، وضبط (طبيعة) الأفعال التي يمكن أن تدخل تحت هذا المصطلح. وبتحليل ما تقدم، تضحى مهمة التفريق بين مفهوم الحرب الإلكترونية والإرهاب الإلكتروني، أكثر سهولة ويسر، عند تشخيص أطرافها وأهدافها، على الرغم من اتحاد عنصر الوسيلة بين المفهومين والمتمثلة بأنظمة الشبكة الإلكترونية للمعلومات. فعلى مستوى الأطراف او الفاعلين، نجد أن الإرهاب يقوم به افراد، أو جماعات، أو هيئات دون مستوى الدول، ومع دخول الدولة على خط المواجهة الإلكترونية، نكون أمام نمط من الحرب الإلكترونية. أما على مستوى الأهداف، فمن المؤكد أن أهداف الإرهاب الإلكتروني تفتقد بالضرورة إلى عنصر المشروعية، في الوقت الذي قد تكون فيه أهداف الحرب التي تخوضها الدول في الفضاء الإلكتروني مشروعة.

المطلب الثاني/التطور التأريخي للحرب الإلكترونية.

على الرغم من التحاقها المتأخر بأدوات الحرب مع نهايات القرن التاسع عشر، إلا أن الحرب الإلكترونية، قد قطعت شوطاً كبيراً من التطور ما جعلها تحتل مكاناً متقدماً جداً من اهتمام القوى المتحاربة بسبب اعتماد الحرب الحديثة على هذا النوع من التسلح المعرفي والتقني لإدارة القتال وتحقيق الانتصار على الخصوم. ولتتبع مسار التطور التأريخي الذي قطعته الحرب الإلكترونية يمكن التمييز بين مرحلتين أساسيتين، مرحلة دارت وقائعها في نطاق سعي الأطراف المتحاربة لاستغلال موجات الطيف الكهرومغناطيسي للمساعدة في تحقيق النصر أثناء الإشتباك المسلح. واستمرت هذه المرحلة حتى إنتصاف القرن العشرين .أما المرحلة الثانية ، فقد اتسع فيها نطاق إستخدام المنظومات الإلكترونية وكانت الحاسبة الإلكترونية درة تاج التطورات التقنية التي أعانت المتحاربين على تحقيق النصر أثناء القتال المسلح، وستكون بدورها فاتحة عهد لخوض معارك وكسبها عبر الفضاء الرقمي. وعلى أساس هاتين المرحلتين التاريخيتين جرى توزيع الفروع في هذا المبحث.

الفرع الأول/الحرب الإلكترونية في النصف الأول من القرن العشرين.

أماطت الاكتشافات العلمية التي صاحبت عصر التنوير في القرن التاسع عشر، وما رافقها من حروب متفرقة، عن جيل جديد من أدوات الحرب يعتمد الطيف الكهرومغناطيسي، ليشهد هذا الأخير، أبان الحروب العالمية الكبرى، طفرات نوعية وتطورات في إستخداماته. ولدراسة التطورات التي لحقت بأدوات وفعاليات الحرب الإلكترونية، جرى تقسيم هذا الفرع على محورين، كرس المحور الأول منهما

للبحث في بدايات الحرب الإلكترونية، ومن ثم تم تناول التطورات التي مر بها هذا النوع من الحرب أثناء الحربين العالميتين في النصف الأول من القرن العشرين في المحور الثاني.

أولا // بدايات الحرب الإلكترونية.

عند تتبع تأريخ نشأة الحرب الإلكترونية في العالم، نجد أن الجذور الأولى لها تعود لمرحلة اندلاع الحرب الأهلية في الولايات المتحدة الأمريكية، في أبريل (1861)، فقد كان الرّئيس الأمريكي (إبراهام لينكولن) أول قائد عسكري يَستعملُ البرقيةَ لإصْدار الأوامر إلى جنرالاتِه المتواجدين في الخطوط الأمامية للقتال وبصورة فورية. حينها أضحت خطوط التلغراف [xix]هدفاً مهماً للقوات المتحاربة؛ إذ كان عمال الإشارة يتداخلون على خطوط المواصلات السلكية، من طريق توصيل هاتف على التوازي مع كل خط من هذه الخطوط للتنصت على المحادثات؛ ولهذا السبب، كان كل جانب يقطع المواصلات الخطية عند عدم الحاجة إليها، حتى لا يتداخل عليها الطرف الآخر.[xx] وفي عام (1888)، أثبت الالماني (هاينريش هيرتز) أن الطاقة الكهربائية تخلف ترددات في الفضاء تكون بمثابة اشارات يمكن اعتمادها ورصدها". وقد قاد هذا الاكتشاف إلى الاهتمام بما عرف فيما بعد بـ(الذبذبات الهرتزية) التي استخدمت في تطوير نظام الراديو في انكلترا. كان التطبيق العملي الأول لهذه التقنية أثناء الحرب الروسية – اليابانية عام (1904) حينما قصفت السفينتان اليابانيتان الحربيتان "كاسوجا ونيشين" القاعدة البحرية الروسية في ميناء"آرثر"، وكانت معهما سفينة صغيرة تصحح النيران بإستخدام الراديو "اللاسلكي"، وسمع أحد عمال الروس "الإشارة" بالمصادفة، وتضمنت تعليمات تصحيح النيران فإستخدم جهاز الارسال اللاسلكي في إعاقة الإتصال الياباني بالضغط على مفتاح الإرسال على تردد الشبكة اليابانية نفسها، مما عطل بلاغات تصحيح النيران من أن تُبّلغ لمدفعية السفينتين؛ وهكذا، لم ينتج عن هذا القصف البحري سوى إصابات طفيفة، لعدم دقة النيران في إصابة أهدافها. [xxi]

ثانيا // الحرب الإلكترونية أثناء الحربين العالميتين.

كانت الحربان العالميتان المناسبتان في الكشف عن دور التقنية في إدارة المعارك وتحقيق النصر فيها.ففي أثناء العمليات البحرية في الحرب العالمية الأولى، كان التشويش على الاتصالات اللاسلكية يستخدم من حين إلى آخر، ولكن وُجد أنه لكي ينفذ التشويش على أي اتصال لاسلكي، كان لا بد أن تسبقه عملية للتنصت، الأمر الذي تبين منه في أحيان كثيرة أهمية المعلومات التي يتبادلها الجانب المعادي،والتي يمكن عند الحصول عليها معرفة نواياه المستقبلية.ومن هنا ظهرت أهمية أعمال الاستطلاع اللاسلكي على شبكات العدو اللاسلكية، ففي الأشهر الأولى من عام (1915)، بدأت البحرية الملكية بإقامة سلسلة من محطات (DF) على طول الساحل الشرقي لإنجلترا، بهدف الحصول على المعلومات، وتحديد مواقع السفن، أو الطائرات، بإستخدام الموجات الراديوية ، كما أصبحت الوحدات البحرية على دراية بأن استخدام اللاسلكي أكثر مما ينبغي، يمكن أن يفصح عن حجم كبير من المعلومات المفيدة للعدو، حتى مع استخدام الكود والشفرة في الاتصالات اللاسلكية. وهذا ما تأكد بصورة جلية عندما تمكن الألمان من تمرير اتصالاتهم المشفرة بعيداً عن رقابة الروس في الوقت الذي تمكنوا فيه من اعتراض كل اتصالات الروس غير المشفرة، وكان ذلك من بين أهم عوامل النصر في معركة (تانينبرغ) الحاسمة بين الطرفين أبان الحرب العالمية الأولى[xxii]. وتشير التقديرات، أنه بانتهاء الحرب العالمية الأولى، كان هناك أكثر من (50) مركز اعتراض للموجات الراديوية تابعة للقوات الإنكليزية تمكنت من اعتراض

أكثرمن(15000)رسالة للقوات الألمانية خلال الحرب العالمية الأولى.[xxiii] بعد الحرب العالمية الأولى بذل مختبر البحوث البحرية الأمريكية (المختبر الوطني المرجعي) جهداً كبيراً في تحسين الاتصال بين المحطات الأرضية من جهة والسفن والطائرات من جهة أخرى. في الثلاثينيات من القرن العشرين تطورت أجهزة الإرسال بدرجة كبيرة وأُنتجت أجهزة استقبال ذات حساسية عالية وهوائيات دقيقة التوجيه، ما أدى إلى التفكير في التداخل اللاسلكي لإفشال أعمال التوجيه، فكان جهاز الرادار الأمريكي قادراً على اكتشاف الطائرات على مسافة (50) ميلاً. وفي هذه المدة، كان هناك عمل مشابه ينفذ في بريطانيا وألمانيا. وبحلول شهر يونيه 1935، أُنتج أول رادار نبضي للبحرية البريطانية يمكنه كشف الأهداف حتى مدى (17) ميلاً.[xxiv]

بعد هذه التطورات المهمة في مجال الرادار، بدأ الخبراء في التفكير في إمكانية مكافحة التشويش على البث الراديوي باستخدام منظومات متحركة، او محمولة. وهذا ما انجزته القوات البريطانية عبر اختبار التشويش المحمول جوا على الرادارات الالمانية من طراز (فريا)[xxv] من خلال تشتيت الموجة الارتدادية لهذه الرادارات ، وبالتالي اخفاء الهدف الجوي عنها[xxvi]وفي الوقت الذي توسع فيه الحلفاء باستخدام أدوات التشتيت الراداري المحمولة جواً، فإن الألمان قد وسعوا بالمقابل من نطاق تردد رادارات (فريا) وتخفيض قابلية التشويش عليها. هنا جاء نوع جديد من التشويش ضد الرادار جرى تطويره من قبل البريطانيين يدعى "النافذة" أثبت فعاليته ضد الرادارات الألمانية، يقوم على فكرة عكس قطب موجة الارتداد ليخلق صدى ارتداد قوي جداً يسهم في اضاعة فرصة اكتشاف الهدف الجوي من قبل الالمان.أصبح استخدام الخداع الإلكتروني جزءاً لا يتجزأ من التخطيط الاستراتيجي الحربي، وهذا ما كشف عنه الهجوم الياباني على الميناء الأمريكي (بيرل هاربور)؛ فقد أبحر الأسطول الياباني في المحيط الهادئ دون استخدام الموجات الراديوية للاتصال، وفي الوقت نفسه، كانت هناك شبكات إذاعية وهمية في بعض الجزر اليابانية للتمويه على نشاط الأسطول الياباني في البحر، وهو الفخ الذي وقع فيه الأمريكان.وفي وقت لاحق قادت جهود الحرب الإلكترونية ضد اليابان إلى تدمير الأسطول الياباني الناقل في منتصف الطريق إلى أوروبا، والنجاح، فيما بعد، في كسر شفرة الإتصالات الألمانية (ULTRA) مما سمح للحلفاء بإعتراض الإتصالات بين القيادة الألمانية والقطعات البحرية، الأمر الذي أدى إلى تدمير العديد من الغواصات الألمانية. والأكثر من ذلك، تأمين حركة القوافل البحرية للحلفاء عبر المحيط الأطلسي.[xxvii]

الفرع الثاني/الحرب الإلكترونية في النصف الثاني من القرن العشرين.

مثلت حرب الخليج الأولى عام 1991 التي خاضتها قوى التحالف الدولي ضد العراق علامةً فارقة في سياق تطور الحرب الإلكترونية. وعلى اساس من هذا جرى تقسيم هذا الفرع بين مرحلتين ما قبل حرب الخليج الأولى وما بعدها.

أولا // الحرب الإلكترونية قبل حرب الخليج الثانية عام 1991.

مع تزايد التدخل الأمريكي في حروب الهند الصينية للأعوام (1964- 1975)؛ بسبب ما أملته اعتبارات المواجهة مع الاتحاد السوفياتي (السابق)، تطورت منظومات التسليح واستخدام التقنيات الحديثة في أنظمة الإتصال والسيطرة والتحكم عن بعد. ومنذ بواكير التدخل الأمريكي في الحرب الكورية عبر إرسال أكثر من مئة قاذفة من طراز (B- 29.) في مسرح العمليات الكوري الشمالي، كان سلاح الجو

الكوري لا يملك أي وسيلة فعالة في مواجهة هذه القاذفات على الاقل خلال الأشهر الخمسة الأولى من الحرب، حتى تم تجهيزه بطائرات من طراز (ميج15) المقاتلة ذات السرعة الفائقة لسرعة الصوت، كما قامت القوات الكورية أيضاً بتثبيت رادارات الإنذار المبكر والقاذفات المضادة للطائرات من طراز (AAA) التي توجه باستخدام الرادار[xxviii]. وعلى الرغم من كل هذه التدابير المضادة من الجانب الكوري، لم تبادر القيادة الأمريكية بإعطاء الإذن لقواتها للتوغل في استخدام أهم التقنيات الحديثة المرافقة للحرب الإلكترونية في مواجهة الرادارات المعادية والصواريخ المضادة للطائرات من طراز(SAM-2) في محاولة لحجبها عن القوات السوفيتية؛ تحسباً لأي مواجهة مستقبلية مع الاتحاد السوفيتي (السابق). نتيجة لذلك، أصبحت الخسائر التي لحقت بسلاح الجو الأمريكي غير مقبولة، وكان من الواضح أن ظلام الليل في حد ذاته لم يكن غطاءً جيداً للاختفاء من الدفاعات الكورية. وكانت أجهزة الإستخبارات الاميركية - وقتذاك - في شغفٍ للتعرف على ما وصل اليه السوفيت من تطورات في مجال الرادارات، لاسيما بعد التطورات التي أضيفت اليها.عندها نجح الأمريكيون في تطوير طائرات الاستطلاع والمراقبة الجوية من طراز (. U -2)؛ لاستكشاف مواقع تمركز قوى الفيتنام الشماليين [xxix].

وفي مرحلة لاحقة من عام 1965، أدخلت الولايات المتحدة ولأول مرة في القرن العشرين منظومات التشويش التكتيكية ليتم تركيبها على الطائرات المقاتلة القاذفة بالتزامن مع تطوير نمط جديد من طائرات الاستطلاع المقاتلة وذات الامكانيات العالية على المناور الجوية من نوع (SR- 71 ، وB- 52 ، B -58). وبفضل هذه التقنية الجديدة تمكنت هذه الطائرات، ليس فقط من التشويش على القوات المعادية، بل والتملص من الصواريخ المضادة للطائرات.[xxx] هذا إلى جانب الاستخدام التقليدي لأطراف النزاع لأنظمة التصنت الراديوية والتشويش على الإتصالات التي جرى تطويرها منذ ايام الحربين العالميتين. وهكذا أضحت المنظومات الإلكترونية بكل توصيفاتها وإستخداماتها جزءاً لا يتجزأ من مناورات الخداع الاستراتيجي المرافق للإشتباك المسلح، بعد أن تم لأول مرة في التأريخ الحربي استحداث وحدات آلية مستقلة ومختصة بأنظمة الحرب الإلكترونية.[xxxi] أما على مسرح عمليات الشرق الاوسط، فقد استنفرت إسرائيل في المدة التي سبقت حرب (حزيران 1967) قدراتها في مجال الحرب الإلكترونية ضد الدول العربية في مجال إكتشاف منظومات القيادة والسيطرة التكتيكية والتعبوية العربية، وشبكات المطارات ومناطق تمركز الرادارات ووسائل الدفاع الجوي وغيرها من الأهداف، وكذلك نفذت جميع إجراءات الإخفاء والخداع الإلكتروني لخداع أنظمة الإستطلاع الإلكتروني العربية عن مناطق تمركز القوات الإسرائيلية التي يمكن ان يتم الحصول عليها بواسطة الإستطلاع الإلكتروني.وفور بدء العدوان الإسرائيلي على الدول العربية (مصر، سورية، الأردن) في (6 يونيو 1967م) قامت القوات الإسرائيلية بتنفيذ الإعاقة والخداع الإلكتروني على أنظمة الإتصال التكتيكية والتعبوية وألإستراتيجية، وكذلك ضد مختلف منظومات الدفاع الجوي العربية. وقد أدى ذلك إلى شل فعالية القيادة والسيطرة العربية، وكذلك إعماء الرادارات الخاصة بالقوات العربية. في حرب أكتوبر عام 1973، بدأت سوريا ومصر هجوماً واسع النطاق ضد إسرائيل لاستعادة الأراضي التي فقدت في حرب الأيام الستة عام1967، وقد أدارت في هذه الحرب كفة الحرب الإلكترونية لصالح الطرف العربي بعد أن تفاجئ الطيارون الإسرائيليون بالأنظمة الجديدة لصواريخ (SAM6) الموجهة بالرادار والأكثر دقة وقدرة على إصابة الأهداف الجوية من تلك التي إعتاد عليها الطيارون الإسرائيليون في المواجهة السابقة. وقد تفاعل هذا المعطى بصورة أكثر ضراوة عند مواجهة الإسرائيليين بنظام المقاومات المضادة

للطائرات المحلقة على إرتفاع منخفض (ZSU 23-4)، والتي كانت قد نشرت حديثا ضمن سلاح الدفاع الجوي المصري هذا إلى جانب منظومة الأشعة تحت الحمراء الموجهة. (MANPAD SAM) المحمولة والباحثة عن حرارة عادم الطائرات والصواريخ التي كانت فعالة ضد طائرات الهليكوبتر والطائرات المحلقة على إرتفاع منخفض. فكانت كلفة الدرس الإلكتروني الجديد باهضاً بالحسابات ألإستراتيجية العسكرية؛ فقد خسرت إسرائيل بفضل هذه التقنيات الإلكترونية أكثر من ثمانين طائرة خلال أسبوع من الحرب. [xxxii] وبعد أن تعلمت إسرائيل الكثير من التجربة السابقة في حرب 1973 اندفعت إلى الاستثمار المكثف في أنظمة الحرب الإلكترونية عبر التزود بنظم (C3I و EW) المحمولة جوا، والصواريخ والمدفعية ذاتية الدفع الذاتي لمواجهة واستئصال بؤر الدفاع الجوي للخصم فضلاً عن التركيز في مجال جمع المعلومات الإستخباري. فكانت المحصلة التجريبية لنجاعة هذه الإستعدادات، قد توضحت أثناء معركة وادي البقاع اللبناني عام 1982، والتي نفذتها إسرائيل ضد صواريخ الدفاع الجوي السورية، بعد أن قامت القوات الإسرائيلية خلال الفترة التحضيرية لهذه المعركة بتنفيذ إستطلاع الكتروني كثيف وتفصيلي لمختلف الأنظمة الإلكترونية السورية المتواجدة في سهل البقاع اللبناني، وكذلك داخل الأرض السورية. وقد تمكنت إسرائيل فعلاً من إكتشاف الاشعاعات الكهرومغناطيسية الخاصة بأنظمة الإتصال والرادارات ومختلف المنظومات الإلكترونية الأخرى الخاصة بالطيران والدفاع الجوي. وبالاستفادة من هذه الاشعاعات الكهرومغناطيسية، تمكنت القوات الإسرائيلية من اكتشاف الترددات الخاصة بالمنظومات الإلكترونية السورية، كما استخدمت إسرائيل الطائرات الموجهة بدون طيار كطعم من أجل إجبار السوريين على تشغيل الرادارات قبل تنفيذ هذه المعركة، وتمكنت إسرائيل فور بدء تنفيذ هذه المعركة من تنفيذ حرب الكترونية غير مسبوقة بإستخدام وسائل الحرب الإلكترونية الجوية المحمولة على الطائرات وطائرات الهيلوكوبتر، وكذلك بواسطة الوسائل الأرضية المتواجدة آنذاك في جبل الباروك اللبناني، وبهذا العمل تمكنت إسرائيل من تحقيق الاعماء الإلكتروني الكامل لجميع الوسائل والأنظمة الإلكترونية السورية اللاسلكية والرادارية، وقد تمكنت إسرائيل في هذه المعركة من تدمير (17) بطارية دفاع جوي من طراز سام (6) وكذلك حوالي (100) طائرة سورية. [xxxiii]

ثانيا // الحرب الإلكترونية بعد حرب الخليج الثانية.

على الرغم من أهمية حرب الخليج الثانية في حسابات الاستراتيجيات الإقليمية، وحتى العالمية، من منظور إعادة هيكلة الخارطة الدولية لمرحلة ما بعد انهيار الاتحاد السوفيتي. وما يرسخ هذا المدرك هو الكثافة النارية التي جرى تحشيدها لمواجهة القوات العراقية في أعقاب دخوله للكويت عام 1990، ومع ذلك كانت ألإستراتيجية العسكرية تنطلق من محددات بسيطة في بنيتها لكنها عميقة في تأثيرها، قوامها بناء قوات التحالف بما يكفي لإحتواء أي هجوم عراقي، ثم خفض فعالية القوات البرية العراقية على القتال بإستخدام الهجمات الجوية على نطاق واسع، وأخيراً الاجهاز الجوي والبري المتزامن على هذه القوات. ففي الوقت الذي حشد فيه العراق أنظمة الدفاع الجوي التقليدية والمكشوفة للحلفاء، المتمثلة بتشكيلة واسعة تجاوزت (17،000) صاروخ ارض جو من طراز (SA- 2، SA- 3، SA- 6، بطاريات صواريخ (SA- 8، ورولاند) تكملها باليد قاذفات صواريخ (SA- 7) مجهزة بشبكة واسعة ومعقدة من الإتصالات المعتمدة على نظام (AAA) الراداري، وجدت قوات التحالف الدولي، بقيادة الولايات المتحدة، بالمقابل فرصتها في إختبار الأجيال الجديدة لأسلحتها المتطورة والمعتمدة اعتمادا رئيساً على نظم الكومبيوتر في

جمع المعلومات والاستخبارات وتوجيه القوة النارية بدقة متناهية وتدمير واسع، هذا إلى جانب تجريب أنواع جديدة من الأسلحة المعتمدة على توظيف قدرات الطيف الكهرومغناطيسي في توليد الأثر التدميري والتي جرى تسليطها على شبكات إمدادات الطاقة وتوليد الطاقة الكهربائية وشبكات التوزيع والاتصال.كانت الأولوية الأولى بالنسبة لهذه القوات هي تعطيل مراكز القيادة والاتصالات ومهابط الطائرات ورادارات الدفاع الجوي، ومراكز العمليات التي جرى تدميرها بنجاح من دون أن يتم حتى إكتشافها من قبل الدفاعات الجوية العراقية، في الوقت الذي اعتقد فيه العراقيون أنهم أسقطوا عددا من الطائرات التي كانت، بواقع الحال، بدون طيار؛ بقصد كشف نقاط تمركز المقاومات الأرضية العراقية وتدميرها لاحقاً.والواقع أن هذه الحرب لم تؤشر الطفرة النوعية في مستوى دقة الإصابة وحجمها حتى مع بعد المسافة فحسب، وإنما أشرت أيضاً التنامي الملحوظ في القدرة على إحتواء وتحييد القوة النارية للخصم بإستخدام أدوات ووسائل الحرب الإلكترونية. وكان آخر العوامل الذي أسهم في نجاح الحملة الجوية للقوات المتحالفة، هو تركيب منظومات على الطائرات القاصفة لتشتيت الموجة الرادارية نوع (SIGINT)وإستخدام صواريخ مضادة للإشعاع (ALARM). (xxxiv) أما على مسرح العمليات الحربية البرية فكانت القطعات العراقية تحت نظر طائرات الإستطلاع الجوي الأمريكي الاواكس و E-8 وطائراتJSTARS التي كانت تجوب الصحراء بشكل متواصل ومتصل للكشف عن أي نشاط تقوم به القوات البرية العراقية. وعلى صعيد متصل نجحت القوات المتحالفة باستخدام المنظومات الإلكترونية من أمثال (RC -135 ، و RC- 135S) في التشويش على الإتصالات والتنصت عليها، وتفكيك شفراتها بصورة صعبت كثيرا مهمة الإتصالات التقليدية للقوات العراقية التي لجأت بالمقابل إلى أسلوب الإتصال السلكي القديمة للحيلولة دون إكتشافها من قبل قوات التحالف. وفي هذه الأثناء كانت أنظمة الدفاع للاتصالات الفضائية (DSCS) والأقمار الصناعية تستخدم على نطاق واسع لتوفير وصلات الإتصالات الحيوية، لإستكمال مهمات المنظومات الإلكترونية الأرضية في تعقب القوات وتوجيه الضربات اليها [xxxv]. كانت المناسبة الأخرى لامتحان القدرات الإلكترونية في المعارك الحربية، قد جرت في أثناء الضربات التي شنّتها قوات حلف شمال الأطلنطي ضد الصرب منتصف تسعينيات القرن المنصرم؛ وذلك حينما قصفت الطائرات الحربية الأمريكية محطات الكهرباء الصربية بقنبلة إلكترونية جديدة يطلق عليها اسم "CBU94"[xxxvi] أدّت إلى إغراق ثلاثة أرباع أراضي يوغسلافيا السابقة في الظلام.[xxxvii] وعلى الرغم من ان رغم أن هدف هذه القنابل الأساس هو تعطيل نظم الإتصالات العسكرية والتشويش على وسائل الدفاع الجوي، إلا أن الحياة المدنية تأثرت أيضاً نتيجةً لتوقف محطات توليد الطاقة الكهربائية عن العمل، والمؤكّد مما تسرَّب أن ذلك الهجوم قد أدى إلى توقّف الشبكة الرئيسة في يوغسلافيا(السابقة)، فتوقّفت فيها نظم الكمبيوتر الخاصة بالدفاع الجوي، ما سهّل على الأمريكيين مهمة إختراق المكالمات، وزرع معلومات مضللة وبث فيروسات تمحو ذاكرة الشبكة الرئيسة للسيطرة الإلكترونية للقوات المعادية.[xxxviii] مما تقدم يتضح أن حرب الخليج الثانية عام 1991، وما تلاها من حروب خاضتها القوى الكبرى في البوسنة وكوسوفو، قد كشفت بجلاء عن إرتفاع منحنى الارتباط بين أنظمة المعلومات والارتقاء النوعي لمفردات القوة وإستخداماتها، حتى تبدل الهدف النهائي للحرب من التدمير اللاإنساني للخصم إلى التحكم المفرط في تشكيل سلوكه؛ سبيلاً لتحقيق الغايات النهائية من فن إدارة الصراع؛ وهي أمور أضحت أكثر اعتمادية على الفضاء الرقمي، واقل إتكالا على مفردات ادارة الإشتباك المسلح للمعركة التقليدية. لقد كان ظهور "الإنترنت" وانتشاره أعظم إكتشاف اسهم في تغيير

مسار الحرب الإلكترونية في العقد الأخير من القرن الماضي، إذ بدأ بعض المفكرين العسكريين بأحداث ثورة في الشؤون العسكرية مدفوعةً بالتوظيف المكثف لإستخدامات ثورة المعلومات وشبكة المعلومات العالمية. وشهدت القواميس والموسوعات المعرفية ولادة مصطلحات من امثال (حرب المعلومات (IW) "الحرب الإلكترونية، والحرب الرقمية، وحرب الشبكات) للتعبير عن ثمرة المزاوجة الحاصلة بين أدوات التقنية الرقمية وأهداف الإشتباك المسلح للقوات العسكرية تركز.[xxxix] وبات الواقع الجديد يدفع إلى الإستنتاج بأن الشكل الجديد من الحروب قد تعدى، بفضل التقنيات الرقمية، حدود التوظيف الميداني لها في المواجهة المسلحة بعد إعادة دمجها في الفضاء الإلكتروني لضمان التفوق النوعي، ليصل إلى حد المجابهة الشاملة في الفضاء الرقمي بإستخدام الشبكة العنكبوتية للمعلومات، دون الحاجة إلى الإشتباك المسلح بتلك الأدوات الحربية الكلاسيكية.[xl] وقد توقع الخبراء في مجال الإنترنت أن أي اعتداء عسكري أوارهابي، قد يحدث ضد الولايات المتحدة الأميركية في حال وقوعه، لن يكون بإستخدام طائرات أو متفجرات كما حدث في 11 سبتمبر، أو حتى بانتهاك الحدود الأميركية، بل سيكون هجومًا في الفضاء الإلكتروني يشنه قراصنة الكمبيوتر، بحيث يكون قادرًا على تدمير الاقتصاد والبنية التحتية الأميركية القوة نفسها التي قد يتسبب بها تفجير مدمر. وعلى الرغم من صعوبة هذا التصور للوهلة الأولى فإن الولايات المتحدة بدأت بالفعل في إستخدام هذا السلاح للهجوم والحماية. وتشير بعض مواقع الإنترنت الأمريكية إلى أن أولى الحروب الإلكترونية جرت في أواخر العام (1990م)، إلا أن التأريخ يورد وقائع لحروب الكترونية أخرى قبل هذا التأريخ، ومنها الحرب الإفتراضية (الإختبارية) التي شنها مجموعة من قراصنة البرامجيات بتكليف سري من وزارة الدفاع الأمريكية بهدف التسلل لأنظمة كومبيوترات الوزارة نفسها، وسحب العديد من البيانات السرية، وإستغرق الأمر 3 أيام كي يتنبه الموظفون في الوزارة إلى حدوث هذا ألإختراق الأمني. وكانت المناورة الحربية الأخرى في الفضاء الإلكتروني، قد تمت من قبل لجان المقاومة الشعبية الصينية المرتبطة بالجيش الصيني في عام (1999) عندما قاموا بمهاجمة العديد من المواقع الحكومية الأمريكية في ردٍ غير معلن على قيام الولايات المتحدة بمهاجمة وتخريب الموقع الإلكتروني للسفارة الصينية في بلغراد في(7 أيار 1999). وبالمقابل إستخدمت أمريكا الإنترنت كطريقة للهجوم عدة مرات، وذلك حينما أطلقت حرباً إلكترونية على العراق وأفغانستان. في اطار حملتها الدولية لمواجهة ألإرهاب بعد أحداث ايلول عام (2001). وبعد هذا التأريخ، سجلت الحرب الإلكترونية حضوراً متصاعداً في بقاع أخرى من العالم كما حصل أثناء النزاع بين روسيا وجورجيا، وما حصل أيضاً بين الكوريتين في اطار الحرب الباردة بينهما.[xli] والملاحظ على سجل الوقائع الحربية في الفضاء الإلكتروني، حتى وقت قريب، إنه لم يتجاوز حدود التعرض السري وغير المباشر لبعض المواقع الحكومية المعادية؛ لتحقيق أهداف محدودة التأثير على شاكلة تشويه الموقع والحرمان من الخدمة، أو هجمات حجب الخدمة، مع إستمرار نشاط التجسس الإلكتروني من قبل جميع الدول التي دخلت هذا السباق الإلكتروني. وفي جميع ألأحوال لم تسجل، حتى يومنا هذا، هجمات الكترونية واسعة النطاق اسفرت عن إحداث اضرار بالغة بالبنى التحتية الحكومية للدول المعنية بهذا النوع من الحروب.

المبحث الثاني/صور الحرب الإلكترونية وأساليبها.

خضعت أدوات الحرب الإلكترونية لتطورات متسارعة بفعل عوامل عدة، من أهمها الثورة التقنية التي عاشها العالم في القرنين الأخيرين، وتنامي الإهتمام الرسمي والعلمي بهذا النوع من التقانات الحربية

بداعي الحاجة لتوظيفها في خدمة اغراض الصراع بين القوى السياسية وتنوع إستخداماتها التي افضت إلى تنوع صورها وأساليب ادارتها. ومن هذا المنطلق يمكن تحديد أهم صور الحرب الإلكترونية بالإعتماد على عاملي التطور التأريخي وظروف الإستخدام في نوعين رئيسين، هما (الحرب الإلكترونية التقليدية المصاحبة للإشتباك المسلح، والحرب الإلكترونية المعاصرة في الفضاء الرقمي).

المطلب الأول/الصورة التقليدية للحرب الإلكترونية أثناء الإشتباك المسلح.

منذ دخول الطيف الكهرومغناطيسي إلى ساحات المعارك الحربية، تنوعت صور وأساليب إستثماره بين تحقيق غايات دفاعية، وأخرى هجومية. وتأسيساً على ما تقدم يمكن تقسيم هذا المطلب، بالإستناد إلى أساليب إستخدام الطيف الكهرومغناطيسي ضمن نطاق الحرب الإلكترونية، على الفروع الآتية:

الفرع الأول/الدفاع او الإستطلاع الإلكتروني.

يؤدي هذا القاطع من العمليات دوراً مهماً في توفير مظلة الكترونية تتشكل في سياقها قاعدة معلوماتية تمكن القيادة من التقييم الدقيق والسريع للبيئة الإلكترونية للحرب.[xlii] فيكون هذا القاطع من العمليات جزءاً لا يتجزأ من التقنيات المصاحبة للحرب الإلكترونية التي تنطوي على إجراءات البحث عن الطاقة المشعة، وإعتراضها، وتحليلها لتوفير لمعلومات اللازمة؛ لأغراض التخطيط التكتيكي وتحديد التهديد والكشف المبكر عنه [xliii]؛ اي بعبارة أخرى عرض وتوسيع نطاق التقاط الترددات والاشارات المختلفة في بيئة دينامية.

أولاً // تعريف الدفاع (الإستطلاع) الإلكتروني.

يمكن تعريف الاستطلاع الإلكتروني على انه: ((العمل الذي تتحقق من خلاله المراقبة المستمرة للنظم والوسائل الإلكترونية المعادية، وتحليل مدلولاتها الفنية لصالح أعمال الإعاقة الإلكترونية خلال العمليات، وتحليل مدلولاتها التكتيكية لصالح أعمال قتال القوات الصديقة)). او هو برؤية أخرى: (**مجموعة الإجراءات المتخذة للبحث عن الانبعاثات الكهرومغناطيسية وإعتراضها لغرض تحديد التهديد الفوري سعيا إلى تقليل قدرة العدو على الاستغلال الامثل للطيف الإلكتروني في شن الهجمات على القوات الصديقة وحماية الأفراد ، والمرافق والمعدات للقوات الصديقة من الأثار المدمرة المترتبة على ذلك النشاط المعادي**). [xliv] مما تقدم يتبين أن الإستطلاع الإلكتروني يمثل وسيلة يتم من خلالها توفير مصدر للمعلومات المطلوبة للقيادة لمواجهة التهديدات القادمة من الأعداء عبر الفضاء الإلكتروني، وتهيئة الاستراتيجيات المناسبة للتكيف مع مختلف البيئات.

ثانياً // مزايا الإستطلاع الإلكتروني.

ثمة من يضع لهذا النشاط الإلكتروني أدوارا متعددة وحيوية ضمن هيكل البناء الإستراتيجي للمعلومات والفضاء الإلكتروني المرافق للعمليات الحربية تتمثل بالآتي.[xlv]:-

1. توفير مصادر بديلة للمعلومات أو الاستخبارات ضمن نطاق متقدم من السرعة والسرية. بما يحقق عمقاً استطلاعيا كبيراً.
2. تهيئة اجواء الشروع في تدابير الحماية الذاتية؛ كونه أقل أنواع الإستطلاع تعرضاً لتهديدات العدو، فهو يعمل من داخل أراضي القوات الصديقة.

3.تحديث قواعد البيانات بفضل المراقبة المستمرة لأي تغييرات تحدث في نظم السيطرة الإلكترونية المعادية، وبالتالي، لنشاط قواته، الأمر الذي يمَكِّن من جمع المعلومات عن العدو بطريقة منتظمة ومتتالية.
4.وضع أساس المبادرة بالهجوم الإلكتروني المباشر.

ثالثاً // أنـواع الإستطـلاع الإلكتـروني.

أصبح الاستطلاع الإلكتروني أحد المعالم الرئيسة في الحرب الحديثة، ويمكن تقسيمه على خمسة أنواع هي:

1.**الإستطلاع اللاسلكي:** وهي الطريقة التي تُراقب بها الإتصالات اللاسلكية المعادية؛ للحصول منها على المعلومات التكتيكية والفنية من خلال البحث عن الترددات في الحيز الذي يحتمل أن يستخدم في تشغيل وسائل الإتصال اللاسلكية المعادية، المطلوب إكتشافها، والحصول على معلوماتها. ثم يصار بعد ذلك إلى تصنيف المعلومات المتحصل عليها من أعمال البحث والتنصت اللاسلكي إلى معلومات خاصة بكل فرع من فروع القوات المسلحة (البرية، والبحرية والجوية، وقوات الدفاع الجوي). وبتحليل هذه المعلومات يتم الحصول على نوعين من المعلومات، أحدهما فني، والآخر تكتيكي.[xlvi]

الإسـتطلاع الـراداري: تجمـع معلومـات الإسـتطلاع الـراداري، وتحلـل، وتخـزن عـن الـرادارات المعاديـة مـن واقـع بصـماتها الخاصـة التـي تحـدد تـردد الإرسـال، التـي يمكـن أن نسـتخلص منهـا مقـدرة الـرادار ونظـام عملـه، والمعـدل التكـراري للنبضـات Pulses)Repetition Frequency:PRF)؛ وبـذلك فـإن بصـمة كـل رادار معـادي يعمـل لإدارة النيـران، أو الملاحـة أو المراقبـة، يـتم تجميعهـا وتحليلهـا وتخزينهـا، ثـم تسـتمر معـدات الإسـتطلاع الإلكترونـي فـي مداومـة المتابعـة والبحـث علـى حيـز التـردد بإسـتمرار، وتحديـد البصـمات المعاديـة ومقارنتهـا بالبصـمات المختزنـة للتعـرف علـى مـا يطـرأ مـن متغيـرات علـى الـرادارات المعاديـة وتحـديث إحـداثياتها لرصـد وهذه المتغيرات وتحليلها بإستمرار.[xlvii]

2.الإستطلاع الكهرو بصري (تليفزيوني/ حراري/ ليزري/ بصري).
3.الإستطلاع الصوتي.
4.إستطلاع الحاسبات الإلكترونية.

في أغلب الدول يقتصر الإستطلاع الإلكتروني على نوعين رئيسين، هما: (الإستطلاع اللاسلكي والإستطلاع الراداري). وينفذان بإستخدام وسائل (أرضية، أو محمولة بحراً/ جواً).[xlviii]

الفـرع الثاني/عمليـات التشويـش او الهجـوم الإلكترونـي.

تنطوي هذه العمليات على إستخدام الطاقة الكهرومغناطيسية في تحديد مواقع الأهداف المعادية وتوجيه الأسلحة لإصابتها بدقة عالية، مع محاولة التأثير الكترونيا على الأنظمة الإلكترونية للعدو؛ بقصد اعاقتها او التشويش عليها. او هي بعبارة أخرى (مجموعة الإجراءات المتخذة لمنع الإستخدام الفعال للطيف أو الحد منه من قبل العدو بإستخدام القدرات الإلكترونية).[xlix] وفي هذا السياق تُعد إعاقة نظم العدو ووسائله الإلكترونية، أحدى الإجراءات الإلكترونية المضادة المهمة، التي تقوم على فكرة إعاقة تشغيل النظم، والوسائل الإلكترونية المعادية بأنواعها المختلفة من خلال التأثير على كفاءتها في أداء مهامها الوظيفية بأساليب الإعاقة الإلكترونية ألآتية:

أولاً // الإعاقة الإلكترونية الإيجابية.

هي عملية توجيه حزمة من الأشعة الكهرومغناطيسية المتعمدة إلى مستقبلات النظم والوسائل الإلكترونية المعادية؛ للتأثير على أدائها بتعميتها، أو خداعها؛ بهدف شل عملها وإرباكها. وتعتمد في إعاقة تشغيل النظم والوسائل الإلكترونية المعادية المختلفة، ومنها (أنظمة وأسلحة الطاقة الموجهةDEW، والصواريخ المضادة للإشعاع) التي تقوم على خاصية إلتقاط أجهزة الإستقبال للإشارات المرغوبة، والإشارات الأخرى غير المرغوبة التي تكون على التردد نفسه.[l] ببساطة شديدة، يمكن القول، بأن الإعاقة الإلكترونية الإيجابية هي عملية إرسال إشعاع متعمد لموجات كهرومغناطيسية يتم إصداره من جهاز ما -لاسلكي، راداري،... الخ، وتوجيهه في اتجاه جهاز إستقبال معين؛ بغرض فرض هذا الشعاع دون سواه على هذا المستقبل. لقد أماطت التطورات التقنية في حقل الطاقة الميكروويفية، عن إمكانية تطوير جيل جديد من الأسلحة الإلكترونية وإستخدامها بصورة مباشرة في المعارك المسلحة عبر توجيه حزمة عالية من الطاقة الميكرويفيية المركزة (او ما يسمى سلاح النبضة الإلكترونية) إلى مرتكزات السيطرة وأنظمة الإتصالات الإلكترونية- العسكرية وحتى المدنية بهدف تعطيلها او على الحد من فاعليتها[li].

ثانيا // الإعاقة الإلكترونية السلبية.

هي عملية انعكاس متعمد للإشعاع الكهرومغناطيسي الصادر من أجهزة إرسال النظم والوسائل الإلكترونية المعادية، وخاصة الرادارية، نتيجة لإجبارها على الاصطدام بأجسام معينة دون سواها، فيرتد هذا الشعاع مرة أخرى نحو مستقبلات هذه النظم والوسائل المعادية مسبباً إرباكها، وتقليل كفاءتها، في تنفيذ مهامها، وذلك بقصد إرباك استخبارات العدو، ونظم المراقبة والإستطلاع لديه.[lii] وتعتمد الإعاقة السلبية في إعاقة تشغيل النظم والوسائل الإلكترونية المعادية المختلفة على خاصية انعكاس الإشعاعات الكهرومغناطيسية؛ سواء من الأجسام المرغوبة، أو غير المرغوبة التي تصطدم بها لترتد مرة أخرى إلى أجهزة استقبال هذه النظم والوسائل.[liii] ولتنفيذ هذا النوع من الاعاقة الإلكترونية، تم تطوير العديد من الأنظمة الإلكترونية من امثال (أجهزة تشتيت الموجات المضادة، أجهزة الانذار المبكر للتحذير من القذائف، وغيرها).[liv]

المطلب الثاني/الصورة المعاصرة للحرب الإلكترونية في الفضاء الرقمي.

مع تقدم الدول تقنياً في مجال الإلكترونيات، زاد إعتمادها بصورة كبيرة على الحاسوب في إدارة وتوجيه اعمالها المختلفة، وفي مقدمتها إدارة المعارك الحربية حتى أصبحت الشبكة الدولية للمعلومات ليس فقط العمود الفقري لتبادل المعلومات على صعيد عالمي، بل اسهمت في إيجاد عالم آخر هو العالم الرقمي او الافتراضي، الذي لا يقل خطورة عن واقع الحياة. وغدت حرب المعلومات بإستخدام الشبكة الدولية للحاسبات الميدان الاوسع، والوسيلة الافضل في تامين السيطرة والفاعلية وتحقيق الاقتدار الإلكتروني للقوى المتحاربة؛ فقد انتقلت العديد من وسائل السيطرة والتحكم الخاصة، بمعظم العمليات الحيوية الموجودة على الأرض، إلى الفضاء في صورة أقمار صناعية ومحطات فضائية، كما انتقل أيضاً

قطاع واسع من الحروب والمعارك والحوارات والثورات إلى العالم الافتراضي الذي خلقه ألإنسان منذ اختراعه للكمبيوتر والذاكرات الإلكترونية وشبكات المعلومات، فأنشأ داخله جغرافية افتراضية جديدة.[lv] وهكذا باتت الحرب الإلكترونية الشكل الأكثر إحتمالية على الرواج والفاعلية في حروب القرن الحادي والعشرين، مثلما امسى الفضاء الرقمي الميدان الجديد للمعارك المستقبلية.

والواقع ان خطورة الحروب في هذا الميدان الجديد (الفضاء الافتراضي) لاتقتصر على حجم الدمار الذي قد تخلفه الهجمات الرقمية على البنى التحتية وقواعد القدرة للدول المعادية؛ بسبب تعاظم درجة الإعتمادية على المنظومات الإلكترونية في إدارة الفعاليات المختلفة لمؤسسات الدولة، وتماهي الحدود المعلوماتية بين الكيانات الدولية في الفضاء الرقمي الجديد، بل تنبع خطورته كذلك من التنوع والتطور المستمر في صور وأساليب الهجوم الرقمي، وصعوبة، إن لم يكن استحالة الكشف عنها من قبل الدولة المعتدى عليها، ناهيك عن تنوع وإتساع قادة المشاركين في شن أمثال تلك الهجمات بين الجهات الرسمية او حتى الشعبية، الأمر الذي ينذر بعواقب وخيمة قد تتهدد البشرية من جراء هذا النمط من الحروب والتي قد تفتح أبواب خوض الحروب الحقيقية بين الدول.تأسيساً على هذا المدرك اتجهت الدول المتقدمة اليوم إلى تطوير أسلحتها الرقمية؛ لخوض معاركها الجديدة التي اتخذت أشكالا متنوعة، بعد ان ارتبطت - إلى حد كبير بالنزاعات الدولية؛ فقد بات متوقعاً أن يصاحب كل نزاع دولي حرب إلكترونية بين مؤيدي أطراف النزاع. وكما هي الحال في أية حرب، فإن الجيوش المتصارعة تستهدف دوما ثلاثة عناصر أساسية من أجل كسب المعركة، وهي (مراكز القيادة والتحكم العسكرية، ومراكز صنع القرار السياسي والمؤسسات ألإقتصادية الكبرى المتمثلة بـ(البنوك والمؤسسات المالية والمؤسسات الخدمية وما شاكل ذلك)؛ وذلك سعيا منها لتحقيق هدف أساس مفاده قهر إرادة الشعب. بالتزامن مع ما تقدم تنوعت أدوات وأساليب الهجوم والدفاع في حروبٍ كهذه، وفي مقدمتها (القرصنة الإلكترونية التسلل الإلكتروني والخداع الإلكتروني [lvi] والتحريض الإلكتروني)[lvii]. وعلى اساس من هذه الصور والأساليب للحرب الرقمية جرى تقسيم هذا المطلب على الفرعين الآتيين:

الفرع الأول / إختراق المواقع الإلكترونيةوتدميرها.

الاختراق، بصورة عامة، هو القدرة على الوصول لهدف معين بطريقة غير مشروعة، عن طريق ثغرات في نظام الحماية الخاص بجهاز الحاسب الآلي المستهدف؛ لتحقيق عدة أهداف تمس أمن الدولة وسيادتها عبر قيام المهاجمين بتغيير محتويات الموقع الإلكتروني المستهدف، أو سرقة معلومات سرية أوتعطيل الموقع عن العمل، أو الاستيلاء عليه بصورة عامة؛ بإستخدام ما بات يعرف ببرنامج (فيروس الحاسب) الذي أصبح - خلال السنوات القليلة الماضية- حقيقة واقعة ذات تأثير بالغ الخطورة، سواء على أنظمة الحاسبات، أو شبكات الحاسبات؛ نظراً للحجم الكبير لتبادل الملفات والبرامج بين مستخدمي الشبكة.[lviii] وفيروسات[lix] الحاسب "عبارة عن برامج تستنسخ نفسها في الجهاز المصاب عندما تنشط لتحدث تغييرات في البرامج أو البيئة التي تعمل فيها تلك البرامج مما يؤدي إلى أضرار مختلفة وتتراوح هذه الأضرار بين رسائل مزعجة تظهر للمستخدم، أو فقدان للملفات المخزنة، وقد تصل إلى تحطم نظام التشغيل في الجهاز". [lx] وعند تداخل البرنامج الفيروس مع نظام تشغيل الحاسب الآلي، يصبح هو المهيمن على الجهاز، ومن ثم يعطي أوامر مختلفة عن البرنامج الأصلي، فيستطيع، مثلاً، أن يعطي أمراً

بمسح جميع البيانات الخاصة بموضوع ما ذي نوعية خاصة، ويمكنه كذلك أن يضيف برنامجاً كبيراً لا يهم مستخدم الحاسب، بما يؤدي إلى خلق نوعٍ من الإرباك في عمليات الحاسوب المستهدف.

ومن أبرز خصائص فيروس الحاسب الآلي:-

(أ)القدرة على إخفاء نفسه.

(ب)خاصية التكاثر السرطاني.

(ج)القدرة على تنشيط نفسه ذاتياً دون تدخل من الخارج.

(د) له هدف محدد، أو مجموعة من الأهداف: مثل التدمير، والتخريب، ويمكنه كذلك إظهار أخطاء خداعية، بمعنى، أنه ينبه مستخدم الحاسب الآلي إلى أن هناك خطأ في البرنامج، بينما لا يكون هناك أي خطأ، وذلك بهدف أحداث البلبلة والإرباك.[lxi]

لذلك أضحت كثير من الدول تخشى من استخدام الفيروسات ضدها في الحروب الإلكترونية نظراً للأضرار الفادحة التي تحدثها الفيروسات في الأنظمة المعلوماتية [lxii]، وإمكانية انتشارها بشكل سريع خاصة في الدول التي تعتمد إعتماداً كبيراً على التقنيات الحديثة في مؤسساتها المدنية والعسكرية. إن خطورة الأسلحة الفايروسية تتعدى حدود التدمير الذي تلحقه بالمواقع الإلكترونية الرسمية وغير الرسمية التابعة لدولة ما على الشبكة الدولية للمعلومات [lxiii]، كالتي جرى إستخدامها في الصراع العربي الصهيوني الرقمي مع بدء انتفاضة الأقصى؛ فقد تم إستهداف المواقع الإلكترونية الحكومية، بصورة رئيسة، في هذه الحرب، فسقط تبعا لذلك أكثر من موقع إسرائيلي وعربي على حد سواء، من هذه المواقع على سبيل المثال: (موقع رئيس الوزراء الإسرائيلي، والكنيست، وبعض البنوك). [lxiv] إلى إمتلاك تلك الأسلحة الفايروسية القدرة على تدمير أنظمة السيطرة الإلكترونية المتحكمة بالمؤسسات والمرافق الحيوية للدولة؛ والدليل على ذلك ينهض مما أطلق عليه خبراء الشبكة (سلاح الفضاء الإلكتروني الكبير الأول) الذي اكتشف مؤخرا، وكان الهدف من ايجاده اختراق أنظمة التحكم في المنشآت الصناعية والتقنية لاسيما تلك المصنعة من قبل شركة سيمينز الالمانية، إضافة لسرقة المعلومات الهامة عن البرامج الصناعية المهمة كالبرنامج النووي الإيراني مثلاً وإرسالها لجهات محددة مما يخول "القراصنة" من السيطرة على الأجهزة والمعدات الصناعية عن بعد، الأمر الذي يعني تعريض العديد من الأجهزة الصناعية للخلل الخطير كمثل تعطيل المضخات بمختلف أنواعها والمحركات، وأجراس الإنذار، وأنظمة إطفاء الحريق ويمكن أن يؤدي، من الناحية النظرية على الأقل، إلى انفجار الغلايات الضخمة في المصانع ومحطات تحلية المياه وإصابة خطوط الغاز والنفط بأضرار بليغة، بل وتعطيل محطات توليد الكهرباء النووية التي يبدو أنها هي المستهدف الأول للفيروس. والأكيد أن هذا الفيروس الذي وجد في الأصل لمهاجمة مواقع تصنيع أسلحة الدمار الشامل سيتحول، هو وأضرابه، إلى سلاح دمار إلكتروني شامل.[lxv] ووفقا لخبراء التنسيق في أمن المعلومات بجامعة كارنيجي - ميلون الاميركية، فانه لا توجد طريقة فعالة سريعة، على المدى القريب، للقضاء على هذه الهجمات، وافضل الطرق المتوافرة حاليا هي تعزيز الكومبيوترات لتمكينها من مجابهة هذه الهجمات.[lxvi]

الفرع الثاني/التجسس الالكتروني.

برعت حكومات كثيرة في إستخدام تقنيات متطورة للتجسس على شبكة الإنترنت، لا سيما وأن المعلومات التي تنتقل عبر الشبكات يمكن إعتراضها والتجسس عليها. والأخير لايختلف عن ألإختراق إلا

في الهدف، مع ثبات الأساليب المتبعة في تنفيذ عمليات ألإختراق .[lxvii] ويمكن تعريف التجسس في مجال الحاسب الالي على انه (إختراق هادف يراد من خلاله تمكين المتجسس من التعرف على محتويات جهاز الحاسب الالي المستهدف دون الاضرار بها بإستخدام برامج الفايروسات المنقولة إلى الحاسب المستهدف)[lxviii]وقد نشطت حركات التجسس بعد هجمات الحادي عشر من سبتمبر في الولايات المتحدة عندما كثفت أجهزة الأمن الأمريكية تجسسها على شبكة الإنترنت، وبدأت عمليات موسعة لاصطياد من أسمتهم بالجماعات ألإرهابية، فقد أثيرت شكوك كثيرة حول إستخدام تلك الجماعات المعادية للولايات المتحدة لشبكة الإنترنت في إصدار الأوامر إلى الخلايا النائمة، على حد تعبيرهم. وقد أعطت الحكومة الأمريكية أجهزتها الأمنية صلاحيات واسعة للتجسس على مستخدمي الإنترنت ومراقبتهم أثناء تصفح الشبكة النسيجية وتبادل الرسائل الإلكترونية. وأصبح من المتوقع أن يتم اصطياد رسائل الكترونية تحتوى على كلمات مثل جهاد، انتفاضة، حرب مقدسة، بحيث يتم بعد ذلك تعقب أثرها الإلكتروني للوصول إلى المصدر الذي انطلقت منه تلك الرسائل. ولا يقتصر الأمر على أمريكا فحسب، فالحكومة الإسرائيلية لها تأريخ حافل في عمليات التجسس الإلكتروني، وقد دعمت ذلك مؤخراً بإنشاء قسم خاص في هيئة أركانها للتصنت على شبكة الإنترنت للحصول على معلومات تساعدهم في إتخاذ احتياطات وتدابير أمنية.وصاحب إنشاء القسم المذكور أنباء عن صفقة كبيرة مع شركة مايكروسوفت الأمريكية لشراء برنامجاً حاسوبياً للتصنت على الإنترنت بقيمة (217)مليون دولار.[lxix]

وكان الهجوم الإلكتروني على "المواقع الإلكترونية الرسمية للحكومة الاستونية، وأحدا من أكثر الهجومات شهرة في التأريخ المعاصر للحرب الإلكترونية، على الرغم من كونه ليس الهجوم الأول الذي يشن بقصد التجسس على مثل هذه المواقع الحكومية. ولعل وصف الخبير الأمني ورئيس وكالة الدفاع الإلكتروني في البنتاغون (O. Saydjari)، لهذا الهجوم على انه "غيض من فيض من كمية ونوعية الهجمات التي تجري"، هو الاقرب إلى الواقع في ظل تنامي حالات اللجوء إلى هذا النوع من الهجمات والحروب[lxx]، ومن ذلك أيضاً سلسلة الاختراقات الإلكترونية التي تعرض لها البرنامج النووي الايراني باستخدام فيروسات من امثال (ستكسنت والشعلة[lxxi]، ومهدي تروجان)، والتي تم تطويرها بصورة تسمح للمهاجمين عن بعد بسرقة ملفات من أجهزة الكمبيوتر المصابة بالفيروس ومراقبة رسائل البريد الإلكتروني والرسائل الفورية.[lxxii]

المبحث الثالث/الآفاق المستقبلية للحرب الإلكترونية.

يجمع خبراء عصر المعلومات على أن العقود القليلة القادمة قد تشهد تحولاً مدهشاً للعالم الذي سيتخذ شكل مدينة ذكية صغيرة مرتبطة بالكامل بالأقمار الصناعية[lxxiii]. وإذا كانت عجلة التقدم في مجال التقانات الرقمية، قد تسارع ايقاعها باتجاهات ومجالات مختلفة في عالم اليوم حتى صارت عنواناً للعصر ومفتاحاً لتقدم الأمم، فإن مسيرة التقدم الرقمي في طريق تعزيز قدرات الأمم على إدارة الحروب وتحقيق السيطرة والنصر، سيكون لها تداعيات مستقبلية أكثر خطورة وتأثيرا نتيجة لمتغيرات عدة من أهمها حجم الدعم المادي الكبير الذي تخصصه الدول للاستثمار في هذا القطاع من جانب، وأهمية الأهداف الحيوية المراد تحقيقها بإستخدام هذه الوسائل من جانب آخر. بيد أن تبني فرضية التحول الجزئي، او الكلي، في مسار الحروب المستقبلية باتجاه الافراط في الإعتماد على المتغير التقني الرقمي، يستلزم إستكشاف حدود البنية والإمكانات الواقعية لتحقق ذلك، سواء على مستوى التخطيط الإستراتيجي أو حتى على مستوى

التعرض الفعلي بإستخدام الوسائل الإلكترونية في مجال إدارة الحروب. وهذا ما سيتم تناوله تباعا في المطلبين ألآتيين:

المطلب الأول/ مرحلة التخطيط وبناء الاستراتيجيات.

تؤشر الدراسات ألإستراتيجية المعاصرة تزايداً ملحوظا في درجة الإهتمام بموضوع الحرب على الشبكة العنكبوتية، لاسيما بعد عام (2009). وقد انعكس ذلك على أعداد ما ينشر عن هذا الموضوع من بحوث ودراسات وورش عمل ومؤتمرات دولية. ولم يقتصر ذلك على الجانب العسكري فحسب، بل اتسع ليشمل المؤسسات الإقتصادية والمجتمع المدني. تبعا لذلك انتقلت وتوسعت دائرة الإهتمام بهذا الموضوع لتطال المستويات الرسمية، حينما بدأت العديد من الدول تأخذ الموضوع على درجة متقدمة من الجدية عبر بناء الاستراتيجيات وتهيئة القدرات النوعية في مواجهة سيناريوهات الهجمات الإلكترونية المعادية او حتى التهيئة لشن أخرى مضادة عبر الإنترنت.[lxxiv] وللوقوف على الأبعاد الواقعية لاستعدادات الدول في هذا المضمار ينبغي تحري مضمون وأبعاد عقيدتها ألإستراتيجية للحرب الإلكترونية. ونظراً لكثرة الدول المهتمة بتطوير ترسانتها الحربية الإلكترونية ، جرى التركيز على أهمها، سواء على مستوى العالم او حتى على مستوى إقليمنا الشرق أوسطي.

الفرع الأول/البنية ألإستراتيجية للحرب الإلكترونية للقوى الكبرى.

جرى تقسيم هذا الموضوع على القوى العالمية المتطلعة والمرشحة لممارسة دور الريادة في مجال حرب الفضاء الرقمي؛ بحكم معطيات القدرة والامكانات المتاحة لها في هذا المجال، وهي كل من (الولايات المتحدة الأمريكية، وروسيا الاتحادية، وجمهورية الصين الشعبية).

أولا// الولايات المتحدة الأمريكية.

مع تصاعد التهديداًت ألإرهابية داخل الولايات المتحدة الأمريكية بعد هجمات سبتمبر 2001 تنبهت الإدارة الأمريكية – في عهد بوش الابن – إلى خطورة الهجمات والتحديات غير التقليدية، بما فيها حرب المعلومات التي تواجه الأمن القومي الأمريكي، وتستدعي إتخاذ الإجراءات الحاسمة للتصدي لها، لاسيما مع انتشار مثل هذه القدرات (الإلكترونية) في أيد الخصوم المحتملين، وتزايد احتمال لجوئهم إلى إعتماد مثل هذه الوسائل في وجه الهيمنة الساحقة التقليدية للولايات المتحدة. وكان الاطار الرسمي الذي تضمن الاشارة الأولى لمثل تلك الاحتمالات، قد جاء في تقرير المراجعة الرباعية الذي قدمته وزارة الدفاع الأمريكية للكونغرس، وتكلل بالإشارة التي اوردها نائب وزير الدفاع الأمريكي عام 2001 ولفوتز إلى: "ضرورة تبني الولايات المتحدة لاستراتيجيات جديدة للدفاع ضد أنماط غير تقليدية من الحروب في مقدمتها حروب الشبكة الدولية للمعلومات ".[lxxv] ومع حلول عام 2003 صدر توجيه رئاسي أمريكي بضرورة توفير مظلة الحماية المعلوماتية لشبكات الحاسوب في البنى التحتية الحرجة للولايات المتحدة بوصفها الحلقة الاضعف في بنية الأمن القومي الأمريكي والأكثر عرضة لهجمات معلوماتية شرسة من قوى دولية هامشية، او معزولة، لدوافع شتى. في نوفمبر 2007 دعت إدارة بوش وكالة الأمن القومي للتنسيق مع وزارة الأمن الداخلي لحماية الحكومة وشبكات الإتصالات المدنية من المتسللين، ضمن اطار خطة تهدف إلى تعزيز "الأمن السيبراني [lxxvi]للمؤسسات الحكومية، وتعزيز الدفاعات لمكافحة ألإرهاب، وقد خصص لهذا التوجه الاستراتيجي (144) مليون دولار من ميزانية الدفاع الأمريكي. ومع تزايد حجم الإعتمادية الأمريكية على شبكة المعلومات وتعرض الجيش الأمريكي عام 2008 لعدد كبير من هجمات

الانترنت، أعلن الرئيس الأمريكي باراك أوبأما : "ان تهديد الانترنت وأحدا من أخطر التحديات التي تواجها بلاده، وأن الأسلحة التي تستخدم في هذه الحرب هي أسلحة الدمار الشامل الحقيقية". اتبع ذلك اعلان قادة في البنتاغون: "أن شنّ هجوم سيبراني مضرّ بما فيه الكفاية على الولايات المتحدة قد يُنظَر إليه على أنه (عمل من أعمال الحرب)، يستدعي الرد عليه بالصورة نفسها.ولن يأخذ هذا الرد بالضرورة شكل هجوم سيبراني مضاد من جانب الولايات المتحدة".

نتيجة لذلك التحدي تحركت الإدارة الأمريكية على طريق الأمن الإلكتروني بخطى أكثر جدية وشمولية في اطار ما يعرف بـ(المبادرة الوطنية الشاملة للأمن السيبراني)، التي خصص لها مبلغ قدر بنحو (6) مليار دولار من ميزانية عام (2009)."إذ قدمت (القيادة الإلكترونية[lxxvii] لتطوير "تكنولوجيات الانترنت)، تصوراتها للكونغرس حول السياسة الإلكترونية لوزارة الدفاع والإدارة القومية لمكافحة التجسس، وتوجهات سياسة واشنطن في هذا المجال للمستقبل المنظور.[lxxviii] وكان من بين ما تضمنته هذه ألإستراتيجية الجديدة، بمفاصلها الرئيسة، توحيد نظم (القيادة والتحكم والإتصالات والاستخبارات) تحت إدارة واحدة تسمى (القيادة الفضائية الأمريكية)، التي تخضع للإشراف المباشر من قبل مساعد وزير الدفاع الأمريكي. وتتولى هذه القيادة مسؤولية إدارة شبكات الحاسوب في كل صنوف الجيش الأمريكي، يتقدم ذلك دورها المحوري في مجال تأمين الحماية الإلكترونية لها في مواجهة ألإرهاب المعلوماتي، أو حتى تحقيق هجمات معلوماتية إستباقية ضد خصوم الولايات المتحدة، فضلاً عن مهامها التقليدية في تقديم الخدمات لأنشطة القوات المسلحة الأمريكية ايام الحرب والسلم [lxxix]. وفي سياق متصل بهذا الجهد المعلوماتي، عملت عدد من الشركات الدفاعية تحت اشراف وكالة البحوث الدفاعية المتقدمة (Darpa)، على تأسيس نماذج افتراضية مما يسمى بـ"ميادين رماية" في إطار "معارك الحرب الاليكترونية". إذ يسمح هذا النظام للباحثين بمحاكاة هجمات من قبل قوى أجنبية، ومن قراصنة الحواسيب داخل الولايات المتحدة. وبذلك يكون هذا النموذج بعد تجهيزه، بمثابة إختبار لتطوير التكنولوجيات الدفاعية، وربما هجومية أيضاً على غرار أنظمة حماية الشبكات. وقد أعد البنتاغون - لهذا الغرض- قائمة خاصة بالأسلحة السيبرانية تشتمل على (ديدان وفيروسات عدة)، تُستَخدم أما لدعم حملة عسكرية قائمة، أما لإستخدامها، بموافقة رئاسية، على الصعيد الإستراتيجي . وطبقاً للمبدأ الناشئ، سيكون بمقدور قادة الجيش الأميركي الموجودين في مناطق الحروب أن يستخدموا أسلحة سيبرانية لتجميع معلومات استخباراتية من شبكات العدو، ودعم العمليات التكتيكية في الحملات العسكرية الأوسع في النطاق، أو حتى شنّ هجمات ضد البنية التحتية الصناعية للعدو، مثل دودة ستوكسنت، التي إستخدمت ضد مجمع إيران النووي على الصعيد الاستراتيجي، لكن بموافقة رئاسية.[lxxx]

ثانيا // الاتحاد الروسي.

لم تخف الحكومة الروسية نشاطها في مجال الحرب الإلكترونية، حينما أعلنت عن برنامج ما يسمى بـ"أسلحة المعلومات". علما أن لدى المخابرات الروسية تأريخ يمتد حتى عام 1985 في إستخدام القرصنة الإلكترونية ضد الولايات المتحدة، عندما استأجرت (الكي جي بي) القرصان الالماني الشرقي (ماركوس هيس)؛ لمهاجمة وكالات وزارة الدفاع الأمريكية في نطاق عملية مخابراتية سميت بـ"بيضة الوقواق".ومنذ عام 1999أصبح أمن المعلومات وأسلحة البرمجيات في روسيا مسألة لها الأولوية في حزمة إهتمامات الأجهزة الأمنية والمخابراتية الروسية، فانصرفت الجهود الحكومية إلى تأمين الفضاء الإلكتروني بعد ان تم تخصيص إدارة مسؤولة عن أمن المعلومات تتصل بوكالة الأمن الروسي(FSB)

بلغت ميزانيتها السنوية نحو(2.5%) من إجمالي التمويل لبرنامج التدابير ذات الصلة لتطوير نظم المعلومات وحماية البيانات في عام (2002). وفي هذا السياق، أشارت الدراسات إلى قيام وزارة الدفاع بالتعاون مع بعض شركات البرامجيات والأوساط ألأكاديمية بوضع عقيدة (الحرب الإلكترونية) التي إنطوت على سلسلة من التدابير الهجومية والدفاعية لضمان نجاحها". من ضمنها بناء الخطط ووضع الاستراتيجيات المتعددة الأبعاد وتحديد الأهداف التي يتقدمها في المجال الهجومي تهيئة الأجواء لتنفيذ "ما يسمى بـ الضربة الأولى" ضد العدو، او" بيرل هاربور الرقمية " من خلال تنفيذ عملية إختراق واسعة وخفية لشبكات الحاسوب وقواعد البيانات في وقت مبكر قبل بداية العمليات القتالية للعدو، واستزراع كم هائل من الفيروسات الدقيقة القادرة على ألإختراق والإنتشار، والتخفي داخل رقائق الذاكرة لحاسبات الخصم بما يسهم بفقدان البيانات المخزنة فيها على المدى الطويل، إلى جانب إمكانية إعادة كتابة البرامج بأسلوب:(باسلوب من؟!)؛ سبيلاً لحرمان العدو من الوصول إلى قواعد بياناته والتحكم بمنظومات السيطرة والتوجيه لكل مؤسساته وبناه ألإستراتيجية، بما يساعد على إيقاع الصدمة النفسية بالسكان والتأثير العميق في معنوياتهم. يستخلص مما تقدم، أن الطابع الهجومي الإستباقي القائم على إمتلاك زمام المبادرة في إنتقاء الوقت الأمثل لتنفيذ الهجوم المعلوماتي الأول والكاسح، يمثل المحور الأساس في صياغة هذه العقيدة ألإستراتيجية دون إهمال الجانب الدفاعي المتمثل بشبكة واسعة من محطات المراقبة والتتبع والتصدي لمحاولات إختراق المنظومات المعلوماتية الروسية. بعبارة أخرى إن حدود الهدف الاستراتيجي من إمتلاك وخوض الحرب الإلكترونية، وفقا للعقيدة ألإستراتيجية الروسية، يتاتى من تحقيق إمكانية النصر المعلوماتي الشامل وتحطيم العدو معلوماتيا ومعنويا قبل تحريك القطعات العسكرية، اي تحقيق النصر من دون حرب، او إشتباك مسلح. والواقع أن السجل التأريخي من محاولات ألإختراق الإلكتروني الذي نفذته الأجهزة الأمنية الروسية، متفاعلاً مع اعلان الحكومة الروسية في الوقت الحاضر عن برنامجها الحربي الإلكتروني، قد أثار الشكوك لدى الكثير من الدول، بما فيها الولايات المتحدة، حول الطبيعة العدائية ذات الأبعاد الهجومية لهذا البرنامج، لاسيما بعد الكشف في عام 1998 عن محاولتين لإختراق قاعدة بيانات وزارة الدفاع الأمريكية، كان مصدرها مختبر ألأكاديمية الروسية للعلوم. وكان النزاع القائم بين روسيا والمنطقة الشيشانية الإنفصالية الروسية، المناسبة التي مكنت الروس من تجربة إستخدام حرب المعلومات كجزء من استراتيجية مواجهة النزعات الانفصالية، إذ دأبت وكالة الأمن الروسي (FSB) على مهاجمة المواقع التي يستخدمها المتمردون (مثل kavkaz.org)، وذلك بإستخدام سلاح (القصف الإلكتروني) بهدف تعطيل الموقع، او الحد من إمكانية الوصول اليه. [lxxxi]

ثالثا // جمهوريــة الصين الشعبيــة.

منذ بدايات العقد التاسع من القرن السابق شهدت جمهورية الصين الشعبية [lxxxii] ثورة في الشؤون العسكرية نشأت عن الحاجة إلى التكيف مع المعطيات الجديدة لعصر المعلومات، بعد أن تقبل قادة جيش التحرير الشعبى الصينى فكرة أن يستند نجاح القتال في الحرب التقليدية على القدرة على بسط السيطرة وبشكل إستباقي، على نظم المعلومات لدى العدو. وهنا غدت قوة المعلومات المفصل الجوهري في تطوير البنية ألإستراتيجية للجيش الصيني، من دون التفريط بهيكل القوة السائد. عندها بدأ جيش جمهورية الصين الشعبية بوضع عقيدة الحرب السيبرانية التي تركز الى تطبيق تكنولوجيا المعلومات للقيادة والاستخبارات والتدريب، والتسليح بما يؤمن التكيف مع التغيرات في البيئة الأمنية الدولية والتحديات المتزايدة، والتحول التدريجي من الاعتماد على العقيدة التقليدية للحشد الشعبي الماوي إلى الاعتماد على القوة النوعية للتقانات

الحديثة وشبكة الحاسبات الإلكترونية. فعمل هذا الجيش بنشاط على تطوير قدرات شبكة الحاسوب الصينية مستثمرا الدعم المالي المتزايد المخصص له من الموازنة العامة للبلاد، ومستفيدا من الخبرات والامكانات التي جندت له بالتعاون مع خبراء الشركات الخاصة؛ لتجنيد خبراء التقنية من أجل تطوير منظومات وأسلحة الحرب الإلكترونية كهياة احتياط عسكري مخصص لهذا الغرض.[lxxxiii] وضمن سياق الإعداد الاستراتيجي لمنظومة الحرب الإلكترونية الصينية حضي التدريب على عمليات الهجوم السيبراني المستقبلي بأهمية قصوى لدى الجيش الصينى بإستخدام مراكز التدريب الخاصة بالحرب الإلكترونية التابعة للجيش، وأكاديمية القيادة للاتصالات في مقاطعة (ووهان)، وجامعة هندسة المعلومات في (تشنغتشو)، وجامعة العلوم والهندسة والجامعة الوطنية للعلوم والتكنولوجيا في الدفاع تشانغشا.[lxxxiv] وقد إعتمدت استراتيجية الحرب الإلكترونية الصينية ما يسمى بـ"شبكة الحرب الإلكترونية المتكاملة (INEW)".وهذه الإستراتيجية تسعى إلى تطوير البنية الشاملة للشبكة الإلكترونية القادرة على التنسيق بين العمليات العسكرية (في البر والبحر والجو عبر السيطرة على الطيف الكهرومغناطيسي، كما تتميز بقدرتها العالية على التوظيف الشامل لقدرات الحرب التقليدية والإلكترونية [lxxxv]، بصورة تكاملية يعاد فيها تركيب الهيكل النوعي المعاصر للتقنية الحوسبية المتطورة على الهيكل التقليدي لمفردات القوة المعبر عنها بالعدة والعتاد، بعد إعادة تحديثها وربطها بالمنظومة التقنية المعلوماتية الجديدة. [lxxxvi] يؤكد ذلك ما قاله قائد جيش التحرير الشعبى الصينى (بو شيونغ) "ان على الجيش الصيني تحسين قدرته على النصر بإستخدام التكنولوجيا العالية والحرب الإلكترونية لمواجهة الهيمنة العسكرية التقليدية الأميركية". وبتحليل مفردات القوة الإلكترونية للجيش الصيني، وجد المحلل الاستراتيجي الأمريكي (توماس) أن جيش التحرير الشعبى الصينى يوزع المهام القتالية في الحرب الإلكترونية ضمن ثلاثة مديات، هي: **(المراقبة، والهجوم، وشبكة الحماية)**:

1.نطاق المراقبة الكهرومغناطيسية بما يسمح للجيش الصيني بجمع معلومات عن الأهداف المحتملة ووضع خطة الهجوم على البنية التحتية الحيوية للعدو.

2.ويشير نطاق الهجوم "إلى عمليات لتعطيل وتخريب وتدمير المعلومات في أنظمة شبكة الكمبيوتر للعدو بإستخدام معدات متخصصة، أو برامج، أو حتى قوة النيران.

3.نطاق الحماية: ويشير إلى الوقاية من خيارات المراقبة و الهجوم المضادة.

من ذلك يلاحظ تركيز العقيدة القتالية الصينية على السير في طريق تعزيز إمكانية هزيمة العدو قبل أن ينزل إلى المعركة؛ بتحقيق التفوق والسيطرة في مجال المعلومات في معارك المستقبل؛ سبيلاً لتحديد نتيجة الإشتباك سلفاً.[lxxxvii] وهذا الأمر يتأتى من خلال تنفيذ هجمات منسقة؛ لإختراق أنظمة حاسبات الخصم المحمية كوسيلة لمواجهة عدو متفوق تقنياً داخل وخارج ميدان المعركة بإستهداف بناه التحتية وألإستراتيجية وقدراته المختلفة، وأهمها العسكرية، وذلك قبل حتى إنطلاق العمليات العسكرية التقليدية. وقد وصف الصينيون هذا الأمر بما يسمى نهج "حرب الوخز بالإبر"، اي شل العدو بمهاجمة الحلقة الضعيفة له المتمثلة بأنظمة القيادة والسيطرة والإتصالات والمعلومات قبل مبادرته بالهجوم [lxxxviii]. وفي هذا السبيل لاتستبعد العقيدة القتالية للصين إستخدام المدنيين كقراصنة لمساعدة القوات العسكرية في شن الهجمات الإلكترونية إنطلاقاً من منازلهم؛ ومن ثم فأن أي شخص لديه جهاز كمبيوتر يمكن أن ينضم في المعركة ضد قوة المنافس بوصفها قوة مضاعفة؛ تحقيقاً لهذه الغاية.

الفرع الثاني/البنية ألإستراتيجية للحرب الإلكترونية في الشرق الاوسط.

لم يخرج الشرق الاوسط من سباق التطورات المتسارعة في أنظمة الحرب الإلكترونية العالمية؛ نظراً لإستمرار عقد الصراع والتنافس بين قواه الإقليمية. فتجهزت هذه الأخيرة بالإرادة والقدرة ألإستراتيجية على خوض غمار هذه الأشكال المتطورة من القتال بعد إعادة النظر والتطويرفي بنيتها ألإستراتيجية وعقيدتها القتالية،وهوالأمرالذي أخذ حيزاً متقدماً من الإهتمام في الدوائر الرسمية للقوى الفاعلة في هذا الإقليم، تتقدمها إسرائيل وايران. وهو ما سيتم تناوله تباعاً.

أولا // إسرائيـل.

إتجهت إسرائيل إلى الفضاء الإلكتروني الحربي حينما أعلن فيها عن إنشاء فريق من الخبراء مهمته بلورة خطة إستراتيجية دفاعية لمواجهة هجمات إلكترونية معادية تستهدف شبكات الحواسيب الإسرائيلية.وكشف ديوان رئيس الوزراء أن نتنياهو بادر إلى إنشاء الطاقم نهاية 2010 بعد شهور من إكتشاف "فيروس الحواسيب"، والذي أعطب منشآت إيران النووية ومس شبكات حاسوب كثيرة في العالم. وكان وزير الدفاع (إيهود باراك) أعلن، في (6 حزيران) من العام نفسه: "أن إسرائيل تعمل لكي تحتل موقعاً قيادياً في الحرب الإلكترونية الأمنية عالمياً داعياً لتعاون دولي مكثف للتصدي لحرب إلكترونية محتملة".[lxxxix]وقال باراك، خلال مؤتمر أمني عقد في جامعة تل أبيب، إن "الدمار الذي يمكن أن تسببه الحرب الإلكترونية في مكان ما يمكن أن تمس تأثيراته أماكن أخرى"، لافتاً إلى أن "الصعوبة تكمن في تحديد إذا ما وقعت قرصنة إلكترونية، وأن تتوقف أنظمة الحاسوب عن العمل؛ بسبب ذلك الهجوم وألإختراق ألإرهابي، وليس تعطل بريء.". وهو الأمر الذي يصعب إلى حد كبير مهمة وضع خطط دفاعية وحماية ضد الهجمات الإلكترونية المحوسبة. من هنا، لا يبتعد أحد الخبراء الاستراتيجيين عن مدار الحقيقة - بقطع النظر عن النوايا الكأمنة خلفها - حينما يعلن: "إن الدفاع عن الحدود من خلال الدبابات والمدفعية بعيدة كل البعد عن حقيقة ما نحن فيه، فإرهاب الهاكر(أي قراصنة الكومبيوتر) لا يقترب من الحدود ولا يدخل عن طريقها، لكنه يدخل إلى صميم الدولة من مكان بعيد في العالم، لاسيما وأن هناك مؤسسات مثل البنوك تنفق أموالاً طائلةً من أجل توفير الحماية لها، ولكن هذا الأمر يبقى خاصاً، خلافاً للمؤسسات العامة والمؤسسات الأمنية التي باتت في أمس الحاجة لتوفير المظلة المعلوماتية الأمنة. إن الإستنتاج الذي يستخلص من واقع تلك التصريحات الإسرائيلية المتلاحقة، إنعقاد العزم على إستباق إسرائيل خطى تأهيل منظومة الحرب الإلكترونية لقواتها المسلحة، مع الحرص على إظهار هذا المسعى للعالم على إنه نوع من رد الفعل على إحتمالية تعرضها للعدوان من جيرانها العرب، بما يعطيها الشرعية، ويسهم بتحقيق الردع عبر خلق حالة التفوق النوعي الإلكترونية لإسرائيل على القوى الشرق أوسطية المنافسة لها. وبالفعل خطت إسرائيل خطوات أخرى أكثر واقعية في هذا المضمار،عندما شرعت قيادة نظم الإستخبارات في الجيش الإسرائيلي بإعداد مقرر تدريبي للقادة الميدانيين حول الحرب الإلكترونية وتأثيراتها على عمليات الحرب البرية القادمة، بعد أن أنهت شركة "البت سيستمز" تطوير برنامج جديد يمكن إستخدامه لتدريب القوات العسكرية والطواقم الحكومية على حماية البنية التحتية المعلوماتية وشبكات الحواسيب الحساسة ضد أي حرب الكترونية.[xc]على صعيد متصل كشف رئيس الوزراء الإسرائيلي (بنيامين نتياهو) أن طاقماً من الخبراء يشمل كافة المؤسسات الحكومية المعنية بالبحث والتطوير وكافة أجهزة الأمن، يتطلع إلى تطوير قدرات إسرائيل في "حرب الحواسيب"، وتابع "في حال إمتلكنا أجهزة دفاع قوية سيصاب المهاجمون باليأس، ونحن مستعدون لبذل الكثير من أجل

حرق حواسيب من يهاجم إسرائيل ومن أجل الدفاع عنها لا مفر من انتهاك حقوق الآخرين[xci]"، مؤكدا أنه "إذا وجدت ضرورة لحرب تدور رحاها في الفضاء الإلكتروني، فإن الجيش جاهز للقيام بهجمات وعمليات استخبارية مركزة." وإعترفت قيادة عمليات الجيش الإسرائيلي في تقرير خاص، صدر في (3 حزيران/ يونيو الجاري)، ولأول مرة، أن الجيش إستخدم الحرب الإلكترونية لجمع معلومات إستخبارية، والقيام بعمليات هجومية عسكريةضدالخصوم الذين تم جمع المعلومات حولهم بتلك الوسيلة.[xcii]

ثانيا // الجمهوريـة الاسلاميـة في إيران.

إتجهت إيران إلى تطوير قدراتها الإلكترونية على خلفية تعرض برنامجها النووي لغزوات الكترونية موجهة بعد عام 2010. ليصبح ذلك في صلب أولويات القيادات العليا في إيران، بما في ذلك المرجع الأعلى السيد (علي خامنئي)، والذي أمر قبل أعوام بإنشاء (مجلس أعلى للفضـاء الإلكتروني) يتولى الإشراف على سياسات التعامل مع الإنترنت، ورصد لذلك مئات الملايين من الدولارات لتدريب الكوادر المختصة في هذا المجال، وتطوير قدراتهم بإستمرار لمجاراة القدرات الغربية. وتشير تقارير أن إيران باتت في المراحل النهائية لشن هجمات إلكترونية محتملة، وخاصة بعد أن أعدت قوات الحرس الثوري الإيراني جيشاً من القراصنة الإلكترونيين، حسب تعبير التقرير، قوامه عدة آلاف من المختصين في مجال الحرب الإلكترونية، وهو جزء من خطة إستراتيجية جديدة لتطوير شعبة الجيش الإلكتروني التي أنشأت في العام 2010. وقد تم تقسيم الشعبة على ثلاث مجموعات:

المجموعة الأولى//مهمتها دفاعية، وتقوم على أساس مراقبة ورصد وتحديد هوية المهاجمين في الفضاء الإلكتروني، وصد أي هجوم إلكتروني محتمل، أو مباغت على إيران. وقد تمكنت هذه الوحدات بالفعل من إكتشاف عدد من الفيروسات، وتحجيم مخاطرها في بداية نشوئها، كما تمكنت أيضاً من تطوير فيروسات مضادة لها.

المجموعة الثانية// مهمتها هجومية عبر شن هجمات إلكترونية على مراكز التحكم في البنى التحتية لشبكات الطاقة والمياه والقطارات والمطارات في المناطق التي تعد معادية لإيران، في حال إضطرت لذلك.

المجموعة الثالثة// وتختص بإختراق وتحليل الشفرة الإلكترونية الخاصة بنقل المعلومات، وقد طوّرت هذه المجموعة مباشرة بعد إنشاء قوات حلف شمال الأطلسي (الناتو) قاعدة رصد استخباراتي في تركيا. وقد تمكنت هذه المجموعة في وقت سابق من إختراق الشفرة الإلكترونية لأحدى طائرات الإستطلاع الأميركية بدون طيار، وأرغمتها على الهبوط في أحدى قواعدها العسكرية. مما تقدم يمكن ملاحظة الانخراط المكثف للقوى الإقليمية الرئيسة في الشرق الاوسط في سباق نوعي وغير مسبوق للقوة يتشكل في حيز الشبكة الدولية للحاسبات ميدانا وإستخداماً. الأمر الذي قد يؤدي إلى انهيار البنية المفاهيمية الأساسية لتوازن القوى بين تلك الاقطاب الإقليمية ومن قبلها الدولية، وينذر بإحتمالات التأزم والتصعيد في مستويات الصراع بينها بما يهدد الأمن الهش في الإقليم الشرق الاوسطي في المستقبل القريب، حتى تعيد حسابات ومفردات القوة الإلكترونية الجديدة إنتاج معادلة جديدة للتوازن الإقليمي بين تلك القوى.

المطلب الثاني/ مرحلـة التعرض الإلكتروني المباشر.

تتصل حلقة إعداد وتطوير البنية ألإستراتيجية والقتالية لأي دولة بحلقة أخرى أكثر أهمية، مجالها الإختبار الفعلي لمدى فاعلية تلك القدرات في ادراك الغاية المنشودة من إعتمادها؛ فتضحى تلك القدرات المعبر الأساس لإنجاز الأهداف ألإستراتيجية للدولة وتحقيق النصر لها بأقل الأكلاف، وأفضل الوسائل تقليدية كانت أو نوعية. وعند المحطة الأخيرة من الوسائل النوعية تبرز قدرات الحرب الإلكترونية كأفضل خيار للدول لتحقيق أهدافها بإستخدام أهم نمطين من أنماط الحرب، او التعرض (الجزئي او ما يعرف بحرب الإستنزاف) او الكلي . وهذا ما سيتم تناوله في الفرعين ألآتيين.

الفرع الأول / مرحلـة التعرض الإلكتروني الجزئي (الإستنزاف الإلكتروني).

تعرف حرب الإستنزاف في الادبيات العسكرية بأنها "السعي المستمر من القائد لإيقاع الخسائر في أفراد الخصم ومعداته وأسلحته ومؤسساته الإدارية والفنية وجبهته الداخلية ومعنوياته، بهدف كسب التفوق، الكمي والمعنوي، عليه، توطئة لدحره في معركة حاسمة تالية " [xciii] يستشف من ذلك، إن حرب الإستنزاف تمثل أحدى صور الصراع العسكري التي تتضمن معنى التعرض الجزئي، أو غير المباشر، وتنطوي على إستراتيجية تستهدف إضعاف العدو ودفعه إلى الإنهيار عن طريق أحداث الخسائر البشرية، أو العسكرية بين صفوفه سبيلاً لتحقيق النصر. فهي من نمط الحروب التي تُدار ،سياسياً وعسكرياً؛ لتغطية المدة بين السلم والحرب الشاملة، أما بهدف الوصول في النهاية إلى سلم أفضل، أو إلى وضع إستراتيجي أكثر مناسبة لخوض الحرب. وتدل مصادر التأريخ الحربي أن حرب الإستنزاف تتم بعد أن يدرك أحد أطراف الصراع العسكري، بأنه المتضرر الأكبر من حروب المناورة، والأكثر عرضة للهزيمة إذا ما أقدم على خوضها، نظراً لتفوق خصمه، فيسعى إلى هذه الحرب بغية إستنزاف هذا الأخير مادياً ومعنوياً، بتدمير قواته وإلحاق أكبر قدر من الخسائر بين صفوفه؛ سبيلاً لتحقيق النصر بثمن باهظ ."[xciv] وشأنها شأن اي صورة أخرى من صور الحرب. وتقوم حرب الإستنزاف على جملة من المبادئ الرئيسة التي يمكن تأشيرها بألآتي[xcv]:

1- أن تسير الحرب ضمن مخطط عام يشمل التصعيد والتهدئة.

2- أن تشمل نقاط القوة لدى الجانب المهاجم، وتوجه بتركيز حاسم ضد نقاط الضعف والمراكز الحساسة لدى العدو، لتغيير ميزان القوى. لاسيما إذا كان العدو أكثر قوة أو عدداً.

3- أن تتناسب مكاسب الإستنزاف مع تكاليف وردود فعل العدو.

4- أن يحقق تشتيت انتباه العدو ومجهوده إلى أكثر من اتجاه.

5- أن يصاحب بخطة إعلامية واقعية مدروسة، من دون تقليل أو تهويل. وبفحص المزايا ألإستراتيجية التي يمكن ان تؤمنها هذه الحرب، يتحدد الفارق النوعي بينها وبين غيرها من أنماط الحروب، ففي المقام الأول، والأهم، تسلك هذه الحرب سبيل أنهاك الجانب المعادي، بشرياً ومعنوياً واقتصادياً، كغاية أولى وتهدف في المقام الثاني إلى إكتساب الخبرة الميدانية ومواصلة الإستعداد لحرب جديدة تحت ظروف أفضل، أي أنها، بعبارة أخرى، تتبلور فيها خبرات القوات المتحاربة عبر زجها في مهام قتالية واقعية تنطوي على مستوى من الجدية والمخاطرة يفوق ما يمكن إدراكه من خلال التدريب. وهي من جانب آخر المناسبة التي يتم فيها إختبار كفاءة الأسلحة، وكذا أساليب القتال وإختبار الأنسب منها من أجل تطوير هذه الأسلحة والخروج بعقيدة قتالية فاعلة مستقبلا. ومن المزايا الأخرى التي يمكن تحصيلها من هذه الحرب

أنها توفر المناخ المثالي لتطوير القدرة القتالية والأداء الميداني للقيادة والمقاتلين على حدٍ سواء، مثلما تعمل على شحذ الهمم وادامة حالة التأهب والاستعداد للمعركة.[xcvi] ولا تبتعد تلك القواعد والمزايا ألإستراتيجية لحرب الإستنزاف التقليدية الميدانية عن الصورة الرقمية لها في الفضاء الافتراضي (الانترنت)، وان إختلفت أدواتها وتعقدت أساليبها، إذ أنها تشترك مع نظيرتها التقليدية في إستخدامها من قبل الطرف الأضعف الذي يخشى المواجهة لإستنزاف الطرف الاقوى وتدمير قواه، او على الاقل إنهاكه؛ بإستهداف وتخريب المفصل الأكثر دقة في بنيته القتالية المتمثل بقواعد البيانات ومراكز السيطرة والتوجيه الإلكتروني بإستخدام الحاسبة الإلكترونية وشبكة المعلومات الدولية. وهكذا فان أي دولة ليس بمقدورها مواجهة القوى الكبرى، ولاسيما إذا كانت تمتلك أسلحة الدمار الشامل مثل الولايات المتحدة وغيرها، قد تستطيع أن تنال منها بهجوم إلكتروني، يفوق ما تحققه حرب الإستنزاف التقليدية بحسابات الضرر والدمار، والأكثر من ذلك أنها تستطيع أن تقوم بالإغارة عليها دون أن تترك أثراً يشير إليها، أو يشي بها. وبهذا تتحاشى الضربات الانتقامية التي تردع عادة، وتجعل مجرد التفكير في مثل ذلك ضرباً من المستحيل[xcvii]. وبمسح سريع تشير بعض الدراسات العالمية إلى أن أكثر من (23) دولة لديها حالياً إمكانيات شن غارات إلكترونية سرية، والعدد قابل للزيادة بصورة تفوق كل التوقعات، ومن ثم، كل الإستعدادات من جانب الدول المستهدفة. وإذا كانت دولة عظمى مثل الولايات المتحدة قد تفوقت في ميادين القتال والإشتباك المسلح، وحققت لنفسها تفوقا موازيا على مسرح العمليات الإلكترونية، فأنها لن تستطيع بأي حال من الأحوال أن تحتكر لنفسها الريادة والتفرد في هذا المضمار، بل والأكثر من ذلك عندما تتحول نعمة تفوقها الإلكتروني إلى نقمة انكشافها وسهولة إستهدافها وإستنزافها الكترونيا من القوى المعادية؛ كونها الأكثر انغماسًا وإعتماداً على الأنظمة الإلكترونية المفتوحة نسبياً، لاسيما إذا ما علمنا أن أكثر (46%) من إمكانيات العالم الإلكترونية مركزها أمريكا. [xcviii] يؤكد ذلك ما اثاره مدير الاستخبارات الوطنية (مايكل ماكونيل) في تقييمه السنوي في (فبراير 2008)، من مخاوف عن "التهديدات السيبرانية" مشيراً "لدينا معلومات بأن البنية التحتية مستهدفة على نحو متزايد لأغراض الاستغلال وربما للتعطيل أو التدمير من قبل طائفة من خصوم الدولة وغير الدولة،... نقدر ان الدول، بما فيها روسيا والصين، لديها قدرات تقنية لإستهداف وتعطيل البنية التحتية للمعلومات في الولايات المتحدة".وهو الأمر الذي يفسر هوس الإهتمام الأمريكي بوسائل تحصين نظمها الإلكترونية، التي تعدت كلفتها حاجز المليارى دولار سنويا.[xcix] وبتسليط الضوء على ما تمتلكه هذه الحرب من أساليب ومزايا للإستنزاف عبر ألإختراق والتدمير، والتي جرى إستخدامها على ارض الواقع من قبل القوى المتفوقة تقنيا، لتدشن بذلك حقبة جديدة وغير مسبوقة من حقب المواجهات الحربية، ولكن بأساليب نوعية متقدمة غير قاتلة وفي ميادين لم ولن تطأها أقدام الإنسان، يتضح الآتي:

1.التجسس بإستخدام "برامج متسللة إلى أنظمة الحاسوب؛ لسرقة معلوماتها دون علم المستخدم كما حصل في عام 1998، عندما هوجمت - لأول مرة في التأريخ - عدد من شبكات وزارة الدفاع عبر المنافذ الرخوة لنظام سولاريس الكمبيوتري. وقد تمكن المهاجمون من زرع برنامج لجمع البيانات في حاسبات الوزارة. وبعد سلسلة من الهجمات التجسسية وأنشطة التسلل على شبكة الإنترنت لبعض قواعد سلاح الجو وعشرات المواقع العسكرية الأمريكية الأخرى والجامعات، تم ألقاء القبض على اثنين من طلاب مدرسة ثانوية في كاليفورنيا، ليتأكد للمعنيين هشاشة منظومة الحماية الخاصة بقواعد بيانات البنتاغون والمؤسسات المهمة في الولايات المتحدة وانكشافها، لاسيما مع إعتماد أنظمة التشغيل فيها على

مكونات مصنعة خارج البلاد؛ نظراً لرخص تكاليفها. وهو الأمر الذي خلق ثغرة أمنية إستغلتها الدول الاجنبية المصنعة لهذه المكونات لغرض زرع مكونات وبرامج التجسس داخل هذه الاجزاء المصنعة فيها، مما يجعل أجهزة الكمبيوتر عرضة للهجوم و/ أو التجسس.[c] وإذا كانت المحاولة السابقة لإختراق منظومة المعلومات الأمريكية والتجسس عليها، قد جرت على ايد هواة اميركيين، فان ما تبعها من محاولات إختراق وتجسس كانت مدبرة؛ ولتحقيق أهداف تنسجم مع أهداف التعرض غير المباشرة كأسلوب من أساليب حرب الإستنزاف في اطار ما يسمى بـ(عملية ضوء القمر المتاهة) التي تم فيها التسلل إلى شبكات البنتاغون وسرقة بيانات منها حول تقنيات الدفاع الإلكتروني لصالح روسيا. وفي حادث ذي صلة وقع في شهر فبراير من عام 1999، كانت مراكز القيادة البحرية والحرب البحرية (Spawar) في سان دييغو هدفاً لهجمات أخرى؛ لغرض سرقة بعض الوثائق وإرسالها إلى مكان بعيد في روسيا.[ci] وفي ميدان آخر جرى تجريب أسلوب التعرض الإلكتروني الجزئي، أو ما يسمى بالإستنزاف الإلكتروني من قبل الجيش الصيني كثمرة متحصلة من جهود الإعداد والتطوير الذي أقدم عليه هذا الجيش في مجال الحرب الإلكترونية، حينما أطلق عددا غير معروف من الهجمات التجسسية المخفية في عام (2005) ضد شبكات الكمبيوتر من وزارة الدفاع الأمريكية[cii]، كما أثبت مبرمجو القبعة السوداء التابعون لبرنامج الحرب الإلكترونية الصيني قدراتهم الفعلية على تنفيذ هجمات ضد أهداف معادية حقيقية مرة أخرى حينما تسللوا (بخفية) عام (2009) إلى المواقع الإلكترونية لعدد من الشركات التجارية الأمريكية. وذلك بتضمين بعض البرامج الوثائقية المنشورة على الشبكة الدولية للمعلومات من نوع (PDF) امتدادات ترافقية مخفية، تتضمن فايروسات وحصان طروادة لها القدرة على الاختباء بفعالية في ملفات المشغلين وبرامج، وشبكة اتصالاتهم وإعدادات التسجيل الخاص بهم؛ سبيلاً للتجسس على برامجهم، والسيطرة على محتويات حاسباتهم، وإكتشاف اي شفرة سرية يجري تثبيتها لحماية المعلومات فيها مستقبلا.[ciii] والواقع ان خطورة التعرض هذه المرة تتأتى من تمكن المهاجمين لأول مرة من تأسيس خط تواصل مخفي ومستمر مع برامج الحاسبات المستهدفة والتأثير فيها عن بعد، بل انه قد أمن لنفسه مواقع مستقبلية متقدمة للالتفاف وتفتيت إجراءات الحماية لهذه الأجهزة. وفي وقت سابق كشفت صحيفة "نيويورك تايمز" أن الولايات المتحدة كانت اللاعب الرئيس في الهجوم الإلكتروني ضد إيران، وذلك ضمن حملة تستهدف تدمير برنامجها النووي، وأشارت الصحيفة إلى أن الرئيس الأمريكي أوباما يهتم شخصياً بتسريع وتيرة إستخدام الفيروسات الإلكترونية في الهجوم على برنامج تخصيب اليورانيوم الإيراني، وتؤكد الصحيفة أن الولايات المتحدة وإسرائيل هما اللذان قاما بإستخدام فيروس "س" تكسنت الذي دمر بعضاً من الأنظمة التي تشغل منشآت تخصيب اليورانيوم في إيران، كما أن الولايات المتحدة إستخدمت فيروس فليمر ضد المنشآت النووية الإيرانية وألحقت بها أضراراً بالغة. ويعتقد المراقبون أن الفيروس فليمر نجح في سرقة كم هائل من المعلومات السرية عن المفاعل النووي الإيراني[civ]. ولقد استطاعت الولايات المتحدة أخيراً إصدار نسخة جديدة من أسلحتها الإلكترونية الفتاكة التي تحمل إسم اللهب (Flamer) ويجوب هذا السلاح الفضاء الافتراضي، وتتفوق قوته على السلاح النووي فوق التقليدي، ولا تقتصر أهدافه على شن هجمات على منشآت ذات حساسية بالغة كالبرنامج النووي الإيراني، وإنما يتجاوز ذلك مستهدفاً جميع القطاعات في أي دولة دون استثناء، كما يتيح للدولة التي تطلقه أن يكون بمثابة جاسوس غير تقليدي؛ إذ بمقدوره تجنيد أي جهاز كمبيوتر ليتحول، بدوره، إلى جاسوس مطيع يسجل المحادثات التي تتم على مقربة منه ويلتقط الصور التي تظهر على شاشات الأجهزة، وكذلك اقتحام ما يدور من دردشات وصولاً إلى تجميع

ملفات البيانات وتغيير برمجيات الأجهزة..[cv] وحتى الآن، فإن السلاح الإلكتروني الأقوى وصل إلى بعض الدول في الشرق الأوسط، ممن لها عداوات ومواجهات مثل إسرائيل وإيران. ونعترف بأنه ليس لدينا معلومات كافية عن مدى متابعة السعودية لهذه الحرب الإلكترونية العالمية، ولا نعرف مدى الاستعداد للدخول في سباقاتها، ولكن الذي نعرفه، حتى الآن، أن أسلحة هذه الحرب الإلكترونية العالمية ما زالت وقفا على الدول المتقدمة، وعلى رأسها الولايات المتحدة التي ما زالت تمسك بإدارتها وقيادتها.[cvi]

2. تخريب المواقع الإلكترونية والبنى التحتية العسكرية والمدنية: تستهدف هذه النوعية من الهجمات عادة، الأهداف العسكرية والمدنية المرتبطة بشبكات المعلومات. مع التأكيد ان النوع الأول من الهجمات التي تستهدف المواقع العسكرية نادر الحدوث عادة لعدة أسباب: أولها، هو أنه يتطلب معرفة عميقة بطبيعة الهدف، وطبيعة المعلومات التي يجب النفاذ إليها، وهي معرفة من العسير الوصول اليها. وثانيها، أن الحكومات تقوم عادة بعزل المعلومات العسكرية الحساسة عن العالم، ولا تقوم بوصل الأجهزة التي تحملها بالعالم الخارجي بأي شكل من الأشكال. ومن السيناريوهات التي تمثل هذا النوع من الهجمات، هو النفاذ إلى النظم العسكرية وإستخدامها لتوجيه جنود العدو إلى نقطة غير أمنة قبل قصفها بالصواريخ مثلا.بدأ الإختبار العملي في أول ممارسة مباشرة لحرب إلكترونية لهذا النوع من الهجومات الإلكترونية أثناء الإشتباكات المصاحبة للغارات التي شنّها حلف الأطلنطي على كوسوفا في ربيع 1999، حينما نفذت الولايات المتحدة الأمريكية هجمات معلوماتية مركزة استهدفت نظم كمبيوتر الصرب أدى إلى توقّف الشبكة الرئيسة في يوغسلافيا، وبخاصة نظم الكمبيوتر الخاصة بالدفاع الجوي والتي كانت مهمتها إستهداف طائرات حلف الأطلنطي لضربها بالصواريخ. بالمقابل تعرض نظام البريد الإلكتروني غير السري لوزارة الدفاع الأمريكية "البنتاجون في عام 2002 لهجوم نفذه قراصنة ، أدى إلى تعطيل الخدمة لنصف الطاقم الخاص بوزير الدفاع (روبرت جيتس).[cvii] وفي مناسبة أخرى جرى فيها إختبار سلاح التدمير الإلكتروني التابع لمنظومات حرب الإستنزاف الإلكتروني، كان ذلك أثناء الصراع الروسي مع المتمردين في الشيشان منتصف التسعينيات. إذ برهن هذا الصراع على أهمية الدور الذي تمارسه قدرات الحرب الإلكترونية في التأثير على مجريات المواجهة بين الطرفين؛ فإستخدم الأخيران المواقع الإخبارية لترجيح كفتهم في الصراع وتثبيت مواقفهم بمؤازرة حلفاء خارجيين على خط الترويج الإلكتروني لمواقف أحد الطرفين مثل ما فعل موقع (qoqaz.net.my)، ومقره في ماليزيا، بالترويج لموقف المتمردين الشيشان ونشر رسالتهم مشفوعة بتحميل ملفات الفيديو حول الهجمات الشيشانية على الروس وبث المقابلات المصورة مع قادة التمرد الشيشاني وعرض صور من تعاملهم مع أسرى الحرب الروس إلى جانب التغطية الاخبارية المستمرة لمجريات النزاع، بالمقابل إستخدمت الحكومة الروسية عقوبات البث الإذاعي والتلفزيوني التي تسيطر عليها الدولة لاظهار جانبها من الأحداث إلى جانب تجنيد الموقع الإلكتروني (infocentre.ru) لتدعيم موقفها من هذا النزاع والرد على الطرف الآخر الذي امتد بالخفاء ليأخذ مسار الهجمات الإلكترونية الموجهة لإختراق وتدمير المواقع الإلكترونية المؤيدة للمتمردين الشيشان، والتي راح ضحيتها موقعان الكترونيان تابعان للمتمردين الشيشان الذين عمدوا إلى اتباع استراتيجية المواقع الإلكترونية البديلة، وطوروا من وسائل حمايتها أمام محاولات الإختراق. التي وصلت إلى نحو (472) هجمة فقط على موقع (chechenpress.com) ، مثلما سجلت هجمات أكثر ضراوة على موقع (kavkaz.org) الشيشاني، والتي وصلت إلى حد اختطاف الموقع من قبل الروس في خطوة غير مسبوقة في عالم التقنيات الرقمية، وذلك عن طريق تغيير تسجيل نطاق الموقع، ومن ثم، القضاء

على بياناته بعد اضافته إلى خادم آخر.في خضم تلك الصور من التعرض الجزئي والإستنزاف الإلكتروني، لم يترك الشرق الاوسط فرصة الدخول إلى عالم المواجهة الافتراضية هذا عبر بوابة الصراع العربي الإسرائيلي الذي اتخذ مستويات متنوعة من التصعيد والتعرض الإلكتروني تارة من قبل الافراد والجماعات غير الرسميين، وتارة أخرى من قبل الجهات الرسمية، وان تم ذلك بصورة خفية.فاستهدفت الهجمات العربية على الانترنت في أولى هجماتها النظامية، وتحت شعار (الدرة ينتقم من قتلته)، موقع جهاز المخابرات الإسرائيلية الموساد (http://www.m0sad.com) الذي دمر تماما واختفت صفحة البداية فيه بفعل ضربات الحجارة الإلكترونية على الانترنت. بإستخدام برنامج "الدرة" الشهير الذي صممه مبرمج سعودي اسمه (عمران) كما كشفت صحيفة "يديعوت أحرنوت" (2012/1/17) الذي غزا به عدة مواقع إلكترونية "إسرائيلية" حساسة . وقد نفذت هذه الهجمات عبر إرسال كميات هائلة من المعلومات (ping وThreads) لتوجه إلى الخادم الحامي للموقع المستهدف (Web Server) لتعمل على أنهاكه بكميات الطلبات العالية، وتراجع سرعته واجابته لتلك البيانات الضخمة، مما يشله في النهاية ويجعله عاجزا عن اداء عمله بالشكل المطلوب، وقد يجعل المشرفين على الموقع يقومون بإيقافه تماماً عن العمل. ويقوم مايطلق عليهم بقادة الكتائب بتوجيه المشاركين من خلال المنتديات العربية والرسائل البريدية الإلكترونية واشعارهم عن الهدف المحدد عن طريق النقر على أمر تحديث؛ ليقوم البرنامج بالإتصال بموقع مخفي على الانترنت، وتحديث بيانات الموقع الجديد المراد ضربه لالحاق الإذى به وشله عن العمل وغالباً ما تكون تلك العمليات ناجحة بسبب العدد الكبير من المستخدمين المشاركين في الهجمات والذين لا يتطلب الأمر منهم سوى تنزيل تلك البرامج في اجهزتهم وتشغيلها طيلة بقائهم متصلين بشبكة الانترنت. بإستخدام تلك البرامج التي تصنف ضمن برامج الاغراق المعلوماتي (DOS Attack). جدير بالذكر ان الهجمات الاغراقية، والتي تستهدف المواقع الشبكية على الانترنت، تعد من الهجمات الخطرة؛ لأنها لا يمكن التنبؤ ببدئها، ولا بموعد انتهائها، ولا حتى توقع مصدرها، وقد سبق ان اسقطت هجمات كبيرة من هذا النوع مواقع شهيرة مثل(yahoo.com وhotmail.com) وغيرهما [cviii] وفي جولة أخرى من حرب الإستنزاف الإلكتروني العربي ضد إسرائيل، قامت مجموعة من "قراصنة" شبكة الإنترنت (هاكرز) تسمي نفسها "جماعة الكابو nightmare group" مناصِرة لكفاح الفلسطينيين ضد "إسرائيل" بإختراق المواقع الإلكترونية للبورصة "الإسرائيلية" وشركة "إلعال" للطيران وعدة مصارف كبرى، وتسببت بوقفها عن العمل فترة من الزمن. اللافت في ألإختراقات الإلكترونية التي نجح فيها "القراصنة" العرب أن "هيئة الحرب السيبرنتيكية" التي كان رئيس حكومة "إسرائيل" بنيامين نتنياهو قد أعلن عن تشكيلها في أغسطس/آب الماضي، لم تستطع أن تفعل شيئاً لحماية المواقع الإلكترونية الرسمية والخاصة، الأمر الذي أدى إلى توجيه انتقادات شديدة لها من جانب المؤسسات الخاصة والمعلّقين السياسيين من المواقع الأخرى.[cix] وبالمقابل رد "قراصنة" إنترنت "إسرائيليون" على "الهاكرز" العرب بإختراق الموقع الإلكتروني للبورصة السعودية. غير أنه اتضح من اسم مجموعة القراصنة "الإسرائيلية" ("IDFTeam"طاقم جيش الدفاع "الإسرائيلي") أنها مجموعة نظامية، وأن قرصنتها تمت على ما يبدو، بقرار رسمي "إسرائيلي".[cx] ان مثل تلك الجولات من الحرب الإلكترونية الإستنزافية بين طرفي الصراع تؤشر من جانب اتساع نطاق هذا الصراع ليضم بين صفوفه المدنيين من الشباب المتحمس لعدالة قضيته، كما يؤشر، من جانب آخر، تنوع أدوات هذا الصراع بعد ان استطالت حلقاته التأريخية، بما ينذر بالوقت بإحتمالية التصعيد غير المنضبط لمستوياته

بصورة قد تخلق مضاعفات وتداعيات خطيرة على الإستقرار الهش في منطقة الشرق الاوسط يقدم ما حدث مؤخراً من "معارك" إلكترونية ضد "إسرائيل" مسألة الحرب الإلكترونية على صعيدي الدول والتنظيمات الشعبية في المنطقة. صحيح أن أشكالاً من الحرب الإلكترونية جرى إعتمادها بين "إسرائيل" وحزب الله في حرب،2006 وبعدها ضد قطاع الإتصالات في لبنان، إلا أنه لم يُبلّغ رسمياً عن قيام حرب إلكترونية بين "إسرائيل" وايّ دولة عربية أخرى، في حين أن"إسرائيل" والولايات المتحدة منخرطتان في حرب إلكترونية ضد إيران. وقد تسبّبت هذه الحرب، مرة أو مرتين، في تعطيل أجهزة الطرد المركزي الإيرانية ذات الصلة بالمنشآت النووية.[cxi] مما تقدم تتضح ملامح الدور المتزايد للتقنية الرقمية في شن الحروب الإلكترونية والتوسع في مداراتها وضراوة تأثيراتها ليس بالترويج لموقف وتحشيد المؤيدين له فحسب، بل ومهاجمة الآخرين بإستخدام أكثر من وسيلة. يلاحظ، مما تقدم، وجود علاقة طردية وثيقة بين الاقدام على خوض تجربة الحرب بكل صورها والتطور في أساليبها الذي برز على وجه الخصوص في مجال التقنيات الرقمية التي ترافقت مع اطلالة عصر المعلوماتية في نهايات القرن المنصرم. وعلى الرغم من ذلك، تبقى مفردة الحرب الإلكترونية بكل صورها والياتها في الوقت الراهن، وحتى المستقبل القريب، أحدى المفاصل، او الجزئيات التابعة لاستراتيجية الصراع الشاملة، التي تقدم وسائل الدمار المادي المسلح على ما سواها من وسائل، دون ان نسقط من حساباتنا المستقبلية إحتمالية التحول الكلي في مسار الصراع الدولي باتجاه الفضاء الرقمي مع التقدم المستمر في تقنياته واستراتيجيات خوضه وإرتفاع سقف الأهداف المنشودة من إستخدامه من جانب أطراف الصراع.

الفرع الثاني/مرحلة التعرض الإلكتروني الشامل.

إزدادت القناعة بأن الحرب الإلكترونية لم تعد ضرباً من الخيال العلمي، خصوصا في ظل إمكانية تطوير برامج تزداد تعقيدا - يوما بعد آخر- يمكن أن تستخدم كأسلحة فتاكة، بل لا يستبعد حدوث كارثة جراء "قيام دولة ما بشل الخدمات في دولة أخرى "، مما يمهد لحرب حقيقية على حد اعتقاد وتعبير خبير الحاسبات التونسي (هيثم المير) المدير الفني في شركة "مينا ليغيز" [cxii]. وفي سياق متصل رفع الخبير الاستراتيجي الأمريكي اللواء (فلاديمير بيلوس) سقف القناعة بقوله: "أن تبدأ المعركة في المستقبل في التحول أكثر وأكثر باتجاه الفضاء الافتراضي، مع تنامي قدرة الدول المهاجمة على تطوير وإدارة سيناريو حرب المعلومات ضد دول أخرى في محاولة تدميرها من الداخل دون الحاجة لشن حرب دامية او مكلفة على المستوى الاستراتيجي اي سيضحى بالإمكان إجبار العدو على الاستسلام دون إستخدام الأنواع التقليدية من الأسلحة".[cxiii] وإذا سلمنا بان ما تقدم لا يعدو ان يكون مجرد توقعات لخبراء مهتمين ومتحمسين لهذا النوع من الحرب، فان الاستعدادات ألإستراتيجية ذات التوجه التقني للدول الأكثر تقدما في مجال المعلوماتية يفصح عن مستوى اكبر من الجدية والعزم في التوجه لخوض الحروب المستقبلية في الفضاء الرقمي، لاسيما إذا ما علمنا ان الولايات المتحدة قد أقرت استراتيجية جديدة في العام 2010 تحضر فيها لإمكانية خوض حرب إلكترونية شاملة، وتعد بموجبها أن العالم الافتراضي ميدانا حقيقيا لحرب محتملة لا تقل أهمية عن المجال الجوي والبري والبحري. وفي هذا السبيل جهز البنتاغون لذلك (15) ألف شبكة حاسوب يعمل على ادارتها(90) ألف خبير في الكمبيوتر، إضافة إلى نحو ألف خبير عسكري في القرصنة والجاسوسية الإلكترونية. وتنحصر المهمة الرئيسة لهذا الجيش الكبير من المختصين في المجال الإلكتروني، في التصدي للهجمات الرقمية على الولايات المتحدة، وتسديد

الضربات الإستباقية إلى الجهات التي تحضر تلك الهجمات.[cxiv] في سياق متصل كشفت "ريغينا دوغان" مدير وكالة الدفاع الأميركية للتقنيات الواعدة، عن جهودٍ إضافية ستبذل لإنشاء سلاح إلكتروني هجومي يشكل عنصراً جوهرياً في الآلة العسكرية الأمريكية، مع ضرورة معرفة الإمكانات الإلكترونية للدول الأخرى بهدف التحصن ضدها. مما يعني اكتمال اضلاع الحرب التعرضية الشاملة من ناحيتي الدفاع والهجوم"[cxv] وتشير الوقائع إلى ان الاستعداد والتجهيز لحرب شاملة مداها الفضاء الرقمي، قد تجاوزت نطاق الدول الكبرى لتصل إلى دول نامية، مثال ذلك ما سجلته التقارير من أن ايران تستعد لخوض حرب إلكترونية مع الولايات المتحدة وإسرائيل اللتين وجهتا هجمتين الكترونيتين لشبكتها الرقمية مستهدفة برنامجها النووي. ولهذه المهمة أعدت هي الأخرى (أي ايران) جيشا من قراصنة الإنترنت؛ لإستهداف شبكات الكهرباء والمياه الأمريكية والإسرائيلية والعديد من منشآت البنية التحتية انتقاما للهجمات الإلكترونية التي تعرضت لها في السنتين الأخيرتين. وتحدثت تقاريرسابقة عن تخصيص إيران نحو مليار دولار لقراصنة مختصين من أجل توجيه هذه الضربات، ويوضح المهندس سأمر سفاريني لموقع "روسيا اليوم"، أنه على الرغم من التفاوت بين قدرات إيران والولايات المتحدة فإن "جمع جيش إلكتروني وأسلحة رقمية ليس بالأمر الصعب في حال توافرت الرغبة والامكانات المادية"، ورغم أن الخبير في الإتصالات وبرامج الكمبيوتر يعتقد بأنه "لا يوجد حتى الآن فيروس جاهز في العالم يستطيع تعطيل خدمات حكومة بأكملها، وأن معظمها يستخدم لأغراض التجسس"، فإنه يتفق مع الرأي بأن "العالم في القرن الحادي والعشرين يواجه خطر كوارث كبيرة قد تصل إلى تدمير معظم منجزات الحضارة ألإنسانية في حال انتشار وباء بيولوجي نعجز عن إيجاد علاج له، أو فيروس إلكتروني يؤثر في شبكات الخدمات المدنية ويصل إلى الشبكات العسكرية. ويذهب باحث آخر إلى ابعد من ذلك في بناء نظرته إلى مستقبل الحرب الإلكترونية على قاعدة ما أطلق عليه (سيناريو اليوم الاسود) والذي توقع بموجبه إستمرار التطور في مجال المواجهات الإلكترونية بين الدول والافراد، إلى المستوى الذي تبدأ فيه صفحات الانترنت في بلد ما بالإختفاء، او إعلان شركات النقل الجوي والبري والمائي عن تغيير جميع مواعيد رحلاتها من دون سابق إنذار، بعد ذلك يتم مسح معلومات بعض الشركات من الأسواق المالية، الأمر الذي سيؤدي إلى سحب ملايين المستثمرين لأموالهم من السوق المالي؛ خوفاً عليها من أمثال هذه الهجمات، وصولاً إلى الإفلاس التام لنظام البورصات في دولة معينة، ناهيك عن مخاطر التدمير للبنى التحتية والمؤسسات السيادية والأمنية عبر إختراق مواقعها على الشبكة، والايعاز الكاذب إلى انظمتها المرتبطة بالحاسوب بالتوقف عن العمل، او تغيير نمط العمل بصورة تؤدي إلى التخريب التام للمؤسسة مثل اعطاء ايعاز الإطلاق للصواريخ - بضمنها الصواريخ النووية - المرتبطة بالحاسوب، وما شاكل ذلك. وهكذا قد تندفع دول إلى خوض حروب حقيقية والإنتصار فيها على الرغم من صعوبة الانتصار التام او الحسم في أمثال هذه المواجهات الإلكترونية؛ بسبب عدم معرفة ما سيحدث، ومن أين، ومتى، وكيف، وما هو حجم ونوع تلك المخاطر والأسلحة والهجمات والجيش، وحتى الجهة التي ستشن الهجمات؟ لاسيما مع انفتاح حدود المواجهة على دخول أطراف أخرى غير معروفة ولديها مصلحة ادامة الصراع او حسمه لصالح طرف على آخر[cxvi]". إن المزايا التي تقدمها الحرب الإلكترونية بصورتها الشاملة عبر الفضاء الرقمي لشبكة الإنترنيت، تفتح أفقاً ذهنياً أكثر إتساعاً لترجيح إحتمال حصولها في المستقبل، حتى مع قطع النظر عن الاستعدادات التي تجريها الدول على منظوماتها الرقمية في الوقت الراهن. وهو الرأي الذي لاقى رواجاً لدى جمهرة من الباحثين ممن وجدوا في الهجوم بالسلاح الإلكتروني خياراً آخر للحروب دون إراقة نقطة

دماء، فلا دمار في المدن، ولا إنهيارات في المباني، ولا صواريخ ولا قنابل، ولا ضحايا في الأرواح على النحو المعهود في المعارك والحروب [cxvii] إن تنوع أسلحة الفتك الرقمي، وسهولة وقلة كلفة تصنيعها وتواضع البنية التحتية لبناء جيش رقمي شديد الفتك، وسهولة المناورة والاختفاء في إدارة مفاصل الحرب الرقمية مع إرتفاع حجم الدمار والاضرار التي تسببها هذه الحرب في البنى التحتية للخصم، لاسيما مع انفتاح حدود المشاركة فيها أمام فئات الشعب للأطراف المتحاربة، هو بعينه ما يفسر إقدام الكثير من الدول التي لم تساعدها ظروفها على التسلح بالأسلحة التقليدية، على بناء ترسانة لها في ميادين الحرب الإلكترونية العالمية القادم؛ لتعوض تخلفها في مجالات الأسلحة التقليدية. [cxviii] كل هذه المزايا وغيرها متفاعلة مع التقدم التكنلوجي المتسارع، وتزايد الإعتمادية على المنظومات الحوسبية سيغري دول العالم في المستقبل على خوض صراعاتها في الفضاء الرقمي بشكل كلي بعيداً عن مخاطر الصراعات المسلحة الدامية والمكلفة. وبذلك ستكون الحرب الإلكترونية الشكل الرائج، والأكثر فعالية في حروب القرن الحادي والعشرين. وليس من قبيل المبالغة التوقع بأن تكون الحرب الرقمية هي البديل المستقبلي للحروب التقليدية الحالية، وغداً لناظره لقريب.

الخاتمـــة.

أولاً //النتائج.

1- في ضوء ما تقدم من معطيات، يمكن تأشير النتائج ألآتية:

2- كان أثر ثورة المعلومات واضحاً ومتسارعاً في الميدان العسكري أكثر من غيره؛ نظراً لإرتباطه بالقضايا والمصالح الحيوية التي تدافع عنها الدول عند الدخول في اي نزاع مسلح.

3- تعقدت مهمة ايجاد تعريف متفق عليه لمصطلح الحرب الإلكترونية؛ نظراً لتعدد إستخداماته، وتنوع أهدافه، والتطورات المعرفية التي مرت به، وإستخدامه من قبل المعنيين والباحثين، بدلالة عدد غير محدود من المفاهيم المقاربة.

4- يمكن التمييز بين نسختين أو صورتين للحرب الإلكترونية بالنظر لدرج التطور وميدان التوظيف ووسيلته، النسخة أو الصورة التقليدية القديمة للحرب الإلكترونية التي نشأت في ميدان القتال؛ لغرض الدعم والإسناد عبر توظيف موجات الطيف الكهرومغناطيسي، وهي نسخة لم يتم الإستغناء عنها في الحروب حتى يومنا هذا. والنسخة الثانية من الحرب الإلكترونية التي نشأت حديثاً في كنف الحاسب الإلكتروني، وما رافقه من تطور في مضمار الشبكة الدولية للمعلومات لتحاكي النسخة الحديثة والمستقبلية من الحرب الإلكترونية بإستخدام قدرات هذه الشبكة في إيقاع أكبر خسائر ممكنة بالخصم من دون إمكانية اللجوء إلى إستخدام القوة. ومن هنا أضحى الحاسوب أداتها وميدانها لتحقيق الأهداف من دون الحاجة إلى الإشتباك المسلح.

5- إن ألأدوار التي تقوم بها وسائل الحرب الإلكترونية، بصورتيها التقليدية والحديثة، تؤدي، على التوالي، ألأدوار ذاتها والغايات التي تستخدم فيها وسائل الإشتباك المسلح، سواء في مجال الدفاع او الهجوم، مع حفظ الفوارق المذكورة انفا بين الصنفين.

6- إكتسبت الحرب في الفضاء الرقمي بإستخدام شبكة المعلومات الدولية ميزة إستراتيجية نوعية قدمتها في المكانة والأهمية على الصورة التقليدية للحرب الإلكترونية لدى صناع القرار الاستراتيجي، بفعل التطورات المتسارعة التي تحققت في مضمار الحاسوب من جانب وسهولة مهمة التجهيز لها وادارتها

بنفقات محدودة الكلفة من جانب آخر، وميزتها الحاسمة في تحقيق أكبر قدر ممكن من الدمار للبنى التحتية للخصم ومفاصل القوة لديه، مع احتمال عدم كشف هوية المهاجم، ومن ثم تضاؤل إحتمالية تعرضه لأعمال إنتقامية من العدو.

7- إن المزايا ألإستراتيجية التي تنطوي عليها حرب الشبكات، لم تلغ بالمقابل ما يمكن أن تحمله من آثار جانبية وأبعاد سلبية، نتيجة لغياب القواعد القانونية المنظمة لأنماط إستخدامها، والفوضى العارمة التي يصاحبها دمار يخرج عن نطاق الحدود المرسومة بفعل دخول قوى وأطراف أخرى، او لجوء الأطراف ذاتها إلى وسائل اشد فتكاً ودهاءً وخفاءً، ناهيك عن إحتمالية إندفاع أطراف النزاع الإلكتروني إلى الحرب المسلحة نتيجة الدمار الذي سببته المواجهة الإلكترونية غير المنضبطة.

8- تؤشر التجارب التأريخية للدول- لاسيما المتقدمة منها - في مجال تطوير ترسانتها الحربية، مهما كانت صورتها وأدواتها، إستبعاد إحتمالية تخليها عن تطوير أي سلاح دمار، مهما كان ضرره تحت أي ظروف؛ مادام توافر لها القدر الادنى من الشك بنوايا المنافسين على دخول المضمار نفسه، حتى مع انخفاض منسوب عمليات وتجارب التطوير فيه تحت وطأة المطالبات والمطالبات الدولية الضاغطة بهذا الاتجاه. لنتذكر على سبيل التدليل والتأكيد التجارب العالمية في مجال الأسلحة (الكيمياوية، والجرثومية، والنووية بكل اجيالها).

ثانياً // التوصيات.

إن هذا الجيل المعاصر من الحروب يحث على تقديم جملة من التوصيات لصانع القرار وكألآتي:

1- الدعوة إلى تأسيس هيئة عليا في الدولة او فرع في القوات المسلحة له إرتباط مباشر بالقيادة العامة للقوات المسلحة، يتولى مهمة وضع الخطط ألإستراتيجية وتهيئة الكوادر وإدارة الحرب الإلكترونية في الجوانب الدفاعية والهجومية على حدٍ سواء.

2- مضاعفة الإهتمام بالأنشطة والفعاليات والبحوث في المجال الإلكتروني سواء في الجوانب السلمية او العسكرية، ومن صور ذلك:

أ- استحداث قسم لدراسات الحرب الإلكترونية في الجامعات العسكرية او المدنية.

ب- تنظيم المسابقات والمعارض والندوات والمؤتمرات العلمية والدولية في المجالات الإلكترونية لاستقطاب وتشجيع الموهوبين في مجال الحاسبات الإلكترونية وتقديم الرعاية لهم؛ لغرض الاستفادة من خبراتهم في سبيل بناء قوة ردع الكتروني او ما يسمى بـ(الجيش الإلكتروني).

ت- إرسال البعثات الدراسية والزمالات البحثية المتخصصة في مجال حرب الشبكات والوقاية منها .

3- وضع إستراتيجية مستقبلية لتشجيع الاستثمار في مجال صناعة الأجهزة والمنظومات الإلكترونية محليا؛ بغية التقليل من الإعتماد على استيرادها من الخارج، لتعزيز عوامل الأمان الإلكتروني لدينا، واستبعاد خطر إرسال أجهزة مصممة في الدول الاجنبية لإختراق منظوماتنا الحوسبية.

4- السعي لإبرام اتفاقيات تعاون مشترك مع الدول التي لها خبرة كبيرة في مجال البرامجيات الإلكترونية؛ للإفادة منها في تطوير كوادرنا الوطنية. وبالمثل يمكن للعراق تبني مبادرة دولية لإبرام إتفاقية دولية متعددة الأطراف في سبيل تطوير قواعد القانون الدولي في مجال مواجهة مخاطر الحرب الإلكترونية، أو تحديد نطاقها وضبط مساراتها على أقل تقدير.

5- ضرورة عزل المنظومات الأمنية والسيادية الحيوية بشبكة داخلية مستقلة ومحمية من الحاسبات لمنع إختراقها او التأثير عليها تحت أي ظرف، مع عمل نسخ احتياطية، لكل ملفات المعطيات والبرامج العاملة، ومراعاة تجديدها بإستمرار.

6- إستخدام أنواع مختلفة من الرادارات والترددات والتغيير المستمر لها، مع تخصيص ترددات إحتياطية، يمكن المناورة بها، عند وجود إعاقة، او اعمال تعرضية لها.

7- إستخدام إتصالات لاسلكية حديثة يصعب إعاقتها، للتقليل من إشعاع الفصوص الجانبية للهوائيات، مع إستغلال طبيعة الأرض في حجب الإشعاع في إتجاه العدو.

8- وضع القيود الزمنية على تشغيل بعض الوسائل الإلكترونية، لصالح الوسائل الإلكترونية الأكثر أهمية، مع الحرص على إستخدام أقل قدر ممكن من قدرة الإرسال، سواء من خلال إستخدام الهوائيات الموجهة ذات الإشعاع الضيق (Narrow Beam) أو من خلال تشغيل الأجهزة والمحطات اللاسلكية لفترات قصيرة.

9- فرض الصمت اللاسلكي للأجهزة، والمحطات اللاسلكية، وإستخدام الوسائل التي تكفل سرية المعلومات المتداولة لاسلكياً... والله ولي التوفيق .

الهوامـش.

(i) احمد بن محمد بن علي الفيومي ، المصباح المنير في غريب الشرح الكبير للرافعي ، ج1 ، المكتبة العلمية ، بيروت ، بلا سنة طبع ، ص 127 .

(ii) بطرس البستاني ، محيط المحيط ، مكتبة لبنان ناشرون ، بيروت ، 1979 ، ص 157.

(iii) د. وضاح زيتون ، المعجم السياسي ، دار اسامة للنشر والتوزيع ، عمان ، 2006 ، ص138 .

(iv) فرانك بيلي ، معجم بلاكويل للعلوم السياسية ، مركز الخليج للأبحاث ، دبي ، 2004، ص 689 .

(v) مارتن فان كريفلد ، حرب المستقبل ، ترجمة د. السيد عطا ، الهيئة المصرية العامة للكتاب ، القاهرة ، 1995 ، ص 52 .

(vi) سامي عوض ، معجم المصطلحات العسكرية ، دار اسامة للنشر والتوزيع ، عمان ، 2008 ، ص 186 .

(vii) محمد شعبان أيوب ، قصة الحرب الإلكترونية ، مجلة الوعي الاسلامي ، وزارة الاوقاف والشؤون الاسلامية ، دولة الكويت ، العدد 564 ، يونيو 2012 ، ص 63.

(viii) Ali Can Kucukozyigit, ELECTRONIC WARFARE (EW) HISTORICAL PERSPECTIVES AND ITS RELATIONSHIP TO INFORMATION OPERATIONS (IO)—CONSIDERATIONS FOR TURKEY, THESIS Introduced to: NAVAL POSTGRADUATE SCHOOL , CALIFORNIA , September 2006,p.32

(ix) Francis Rico C. Domingo, Chinese Cyber Warfare and its Implications on Selected Southeast Asian States , International Studies Department, De La Salle University, Manila,p.2

(x) ELECTRONIC WARFARE : DOD Actions Needed to Strengthen Management and Oversight,Report to the Committee on Armed Services, House of Representatives, United States Government Accountability Office, July 2012,p.5

(xi) Robert F. Erbacher, Extending Command and Control Infrastructures to Cyber Warfare Assets Department of Computer Science, Utah State University, Logan, USA,p.1.

(xii) اشرف صلاح الدين ، الانترنت في عالم متغير ، مجلة معلومات ، المركز العربي للمعلومات ، بيروت ، العدد 80 ، تموز 2010 ص 34

(xiii) د.اشرف السعيد احمد ، القرصنة الإلكترونية ، دار النهضة العربية ، القاهرة ، 2013 ، ص 47.

(xiv) د. اشرف السعيد احمد ، مصدر سابق ، ص 45.

(xv) مفهوم الحرب الإلكترونية ، منتدى طلاب جامعة القاهرة ، الأحد 10يونيو، 2012

(16) Johnny Heikell, ELECTRONIC WARFARE SELF-PROTECTION OFBATTLEFIELD HELICOPTERS: A HOLISTIC VIEW, Helsinki University of Technology, Applied Electronics Laboratory, Series E: Electronics Publications E18, 2005,p.27

(xvii) Clay Wilson, Information Operations, Electronic Warfare, and Cyberwar Capabilities and Related Policy Issues, Congressional Research Service Report RL31787, February 2, 2009,p.3.

(xviii) الجريمة في عصر وسائل الإتصال الحديثة ، صحيفة الجزيرة الإلكترونية ، المملكة العربية السعودية ، العدد 11426 ، بتأريخ 2004/1/10

(xix) بدأت الإتصالات بين أرجاء العالم المختلفة بإستخدام المواصلات السلكية من طريق المورس "جهاز البرق الصوتي" عام 1837؛ ولم يتحقق أي اتصال آخر في ذلك الوقت إلا من طريق تبادل المراسلات؛ بإستخدام السفن في نقل الرسائل بين الموانئ البحرية.

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

(xxi) المهندس مختار علي حيدر ، نشأة الحرب الإلكترونية وتطورها ، مقال منشور على موقع منتدى التكنلوجيا العسكرية والفضاء بتأريخ 5 ابريل 2014 ، على الرابط : http://army-tech.net/forum/index.php

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

(xxiii) James T. Westwood, Electronic Warfare and Signals Intelligence at the Outset of World War I, USN,p.24

(xxiv) Ali Can Kucukozyigit, op.cit, p.47

(xxv) نوع من رادارات الإنذار المبكر التي جرى إستخدامها من قبل ألمانيا لإعتراض الهدف .

(xxvi) H.Banks, R. Mc Quillan, Electronic Warfare Test and Evaluation, Flight Test Techniques Series, RESEARCH AND TECHNOLOGY ORGANIZATION- NORTH ATLANTIC TREATY ORGANIZATION,Canada,2000,p.2

(xxvii) OFFENSIVE ELECTRONIC WARFARE, ,United States Army Signal Center and Fort Gordon Fort Gordon, Georgia, Sub-course Number SS0134, September 1994,p.1.

(xxviii) H.Banks, R. Mc Quillan, op.cit, p.2.

(xxix) محمد شعبان أيوب ، قصة الحرب الإلكترونية ، مجلة الوعي الاسلامي ، وزارة الاوقاف والشؤون الاسلامية الكويتية ، العدد 564، يوليو 2012 ، ص 67 .

(xxx) Ali Can Kucukozyigit, op.cit,p.56

(xxxi) OFFENSIVE ELECTRONIC WARFARE, op.cit,p.4.

(xxxii) د.مصطفى طلاس وآخرون ، ألإستراتيجية السياسية العسكرية ،ط2، دار طلاس للدراسات والترجمة والنشر ، دمشق ، 2003 ، ص ص 262-263

(xxxiii) العقيد سالم احمد القليبي ، الحرب الإلكترونية الإسرائيلية ومستجداًتها ، صحيفة 26سبتمبر اليمنية

(xxxiv) OFFENSIVE ELECTRONIC WARFARE, op.cit,p.4.

(xxxv) وليامسون مورأي ، حرب العراق : تأريخ عسكري وميداني يومي ، ترجمة مركز التعريب والبرمجة ، الدار العربية للعلوم ، بيروت ، 2005 ، ص ص 255-256.

(xxxvi) توجد بداخل القنبلة "CBU94" عدة قنابل أخرى تنطلق من داخلها في الجو، وكل وأحدة منها مزوَّدة بمظلة صغيرة، ثم تخرج من هذه القنابل أيضاً ملفات مصنوعة من الرصاص الكربوني تُكَوِّن شبكة الكترونية كشبكة العنكبوت عند إقترابها من الأرض؛ بحيث تصيب محطات الطاقة الكهربائية والإتصالات التليفونية بالشلل التام وعلى إرتفاع معيَّن انفجرت القنبلة وخرجت منها ملفات سلكية خاصة انتشرت في الجو فوق خطوط الضغط العالي فعطلتها، مما أدى إلى اشتعال النيران في المحطات، وتوقفت مراكز توزيع الطاقة اليوغسلافية عن العمل.

(xxxvii)Jeffry T.Kelsey, Hacking into international Humanitarian Law: The principles of distinction and neutrality in the age of cyber warfare, Michigan law review,VOL106,P14.

(xxxviii) Ali Can Kucukozyigit,op.cit,p.63

(xxxix) للمزيد من التفاصيل حول أثر التقنية في سير المعارك الحديثة وتطورها ينظر : بيتر سينجر ، الحرب عن بعد : دور التكنلوجيا في الحرب ، مركز الأمارات للدراسات والبحوث ألإستراتيجية ، ابو ظبي ، 2010 ، ص 555 وما بعدها .

(xl) Jon M. Anderson, THE NEW WIZARD WAR: CHALLENGES AND OPPORTUNITIES FOR ELECTRONIC WARFARE IN THE INFORMATION

AGE, A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations. November 2007,pp.5-11.

(xli) الحرب الإلكترونية العالمية الأولى.. هل هي قادمة بالفعل؟ مقال منشور على موقع لها أون لاين، بتأريخ 05 - مايو – 2012 على الرابط: www.lahaonline.com/articles/view/40730.htm

(xlii) Anthony E. Spezio, Electronic Warfare Systems, IEEE TRANSACTIONS ON MICROWAVE THEORY AND TECHNIQUES, VOL. 50, NO. 3, MARCH 2002,p. 63

(xliii) الحرب الإلكترونية : مفهوم وأهداف ، منتدى الجيش الوطني الشعبي ، بتأريخ 20 تشرين الأول 2014 ، على الرابط: http://www.anp-dz.com/t6294-topic

(xliv) LÁSZLÓ KOVÁCSop.cit,pp.145-146.

(xlv) Canadian National Defense-LAND FORCE INFORMATION OPERATIONS, ELECTRONIC WARFARE, B-GL-321-004/FT-001 2004-03-02, pp.17-18.

(xlvi) Keith B .Alexander, Electronic Warfare in Operations (Final Approved Draft), Department of the Army, Washington, DC, No. 3-36,p.8

(xlvii) Ali Can Kucukozyigit, op.cit, pp. 36-38

(xlviii) Canadian National Defense ,op.cit,p.17-20

(xlix) LÁSZLÓ KOVÁCS, op.cit, p.143

(l) Keith B .Alexander, op.cit,p.9

(li) OFFENSIVE ELECTRONIC WARFARE, op.cit,8

(lii) Canadian National Defense-LAND FORCE INFORMATION OPERATIONS, op.cit, p.19

(liii) LÁSZLÓ KOVÁCS, op.cit,p.143

(liv) Anthony E. Spezio, Electronic Warfare Systems, IEEE TRANSACTIONS ON MICROWAVE THEORY AND TECHNIQUES, VOL. 50, NO. 3, MARCH 2002,p.633

(lv) Evan Baun, The Digital Underworld Cyber Crime and Cyber Warfare, HUMANICUS, issue 7, 2012,p.1.

(lvi) الذي يعرف بإرسال معلومات خاطئة بهدف الحصول على أخرى صحيحة ومهمة.

[lvii] رضاب نهار، الحرب الإلكترونية: مئة هجوم في الثانية بأسلحة مدمّرة ، ميدل ايست أونلاين ، مقال منشور على الرابط : http://www.middle-east-online.com/?id=134762

[lviii] نهلة عبد القادر المومني ، الجرائم المعلوماتية ، دار الثقافة ، عمان ، 2008 ، ص 22.

[lix] سُمي بالفيروس؛ لأنه لا يستطيع أن يعمل بمفرده بل هو في حاجة إلى برنامج وسيط آخر يستضيفه حتى يكون له مفعول تمأما مثل الفيروس البيولوجي الذي لا بد له من وسيط كي يبدأ نشاطه الفعال ينظر في ذلك : Clay Wilson, op.cit ,pp.4-6.

[lx] تجدر الإشارة إلى انه ليس من الضروري أن يكون الفيروس على شكل برنامج دخيل، إذ يمكن أن يكون جزءاً من نظام التشغيل المصاحب للحاسب، وهذا مكمن الخطورة، خاصة للدول التي تعتمد على استيراد هذه الحاسبات ضمن أنظمة متكاملة تامة التصنيع بالدول الأجنبية، التي قد تكون حليف اليوم وعدواً مباشراً أو غير مباشر غداً.

[lxi] الحرب الإلكترونية ، بحث منشور على موقع المقاتل العربي ،على الرابط : http://www.moqatel.com/openshare/Behoth/Askria6/ElectroWar/sec04.doc_cvt.htm

[lxii] لا تقتصر الاضرار الناجمة عن تدمير المواقع على الاضرار بسمعة الجهة المستهدفة نتيجة تغيير الصفحة الرئيسة فقط ، بل قد تتبع ذلك خسائر في مجال التعاملات المالية بالنسبة للمؤسسات ألإقتصادية ، او مخاطر بالنسبة للمؤسسات الأمنية : ينظر في ذلك د.اشرف السعيد ، مصدر سابق ، ص 49.

[lxiii] ومن الأساليب الإلكترونية الأخرى لتدمير المواقع ، تنفيذ ما يسمى بـ(هجمات منع الخدمة) التي تعني في ابسط امثلتها، إرسال دفق هائل من البيانات من عدة مواقع، عبر الشبكة يؤدي إلى اختناقها، او توجه عدد من المهاجمين إلى إرسال حزم خاصة تقود إلى شل أجهزة الخادم الكومبيوترية او تعطيل خدماتها. راجع حول ذلك : حاتم عبد الرحمن منصور ، الاجرام المعلوماتي ، دار النهضة العربية ، القاهرة ، 2002، ص174.

[lxiv] د. محمد بن عطية الحارثي ، الحرب الإلكترونية على الإنترنت، ص ص 2- 3 ، دراسة منشورة على الرابط: http://faculty.ksu.edu.sa

[lxv] د.سامي سعيد حبيب في مجابهة الحرب الإلكترونية ، صحيفة المدينة ،السعودية ، العدد : 18057 ، الأحد 2012/9/30م

[lxvi] الحرب الإلكترونية والتجسس الصناعي ، مقال منشور على موقع مجلة المنتدى العامة (كوكتيل) على الرابط: http://www.jableh.com/vb/showthread.php?t=6386

[lxvii] د. اشرف السعيد احمد ، مصدر سابق ، ص 17.

[lxviii] Samuel Liles, Cyber Warfare as A form Of Low Intensity conflict And Insurgency, Conference on Cyber Conflict ,Proceedings 2010,C. Czosseck and CCD COE Publications, Tallinn, Estonia, 2010,p.50.)K. Podins (Eds

[lxix] Clay Wilson, op.cit ,p.8.

([lxx]) محمد عطية الحارثي ، مصدر سابق ، ص ص 7- 8

([lxxi]) سأمر الياس ، هل العالم على أعتاب "الحرب الإلكترونية"؟ على الرابط :
alkompis.se/interesting/did-you-know/1056

([lxxii]) الحرب الإلكترونية على إيران تتواصل من خلال فيروس (مهدي تروجان)، صحيفة الدستور الاردنية ، الأربعاء 29/أغسطس/2012

([lxxiii]) عمر حرز الله ،الحرب الإلكترونية.. صراع في العالم الافتراضي ، مقال منشور على موقع البيان الإلكتروني الأماراتي ، بتأريخ: 04 مارس 2012 ، على الرابط :
http://www.albayan.ae/five-senses/mirrors/2012-03-04-1.1604787

([lxxiv]) وهو الأمر الذي اكده(جريغ داي) أحد المحللين الأمنيين التابعين للفرع الأوروبي من شركة مكافي للبرامجيات بالقول: "هناك على الأقل خمسة بلدان هي بريطانيا وفرنسا وألمانيا والصين وكوريا الشمالية من المعروف أنها تسلح نفسها استعداداً لهذا الصنف من الصراعات". هذه البلدان

([lxxv]) Steven A. Hildreth, Cyber warfare, CRS Report for Congress ,Received through the CRS Web, Congressional Research Service, The Library of Congress, June 19, 2001,p.6

([lxxvi]) السبرانية في اللغة مشتقة من الكلمة الاغريقية (Kybernetike) وتعني فن القيادة ، وفي الإصطلاح تعني علم الإتصال وتنظيم المعلومات ، كما أطلق المصطلح على العلم المؤلف من مجموعة النظريات والدراسات المتعلقة بعمليات الإتصال بين اجزاء الكائن الحي او اجزاء الالة وقيادتهما ذاتياً . نقلا عن : مصطفى طلاس ، الثورة العلمية التقنية وتطور القوات لمسلحة ، ط3 ، دار طلاس للدراسات والترجمة والنشر ، دمشق ، 2003، ص 318.

([lxxvii]) انشات هذه الإدارة كمؤسسة تابعة لوزارة الدفاع الأمريكية (البنتاغون) منذ ربيع عام 2010 وتعنى بشؤون الحرب الإلكترونية والاستراتيجيات والبرامج المرتبطة بها لمواجهة التطورات الحاصلة في نظم المعلومات العالمية .

([lxxviii]) ذهبت مصادر موثوقة إلى ان الولايات المتحدة الأمريكية ستنفق أكثر من (10) مليارات دولار على الأمن الإلكتروني بحلول عام(2015) .

(79) Steven A. Hildreth, Cyberwarfare, lbid,p.8.

([lxxx]) أشرف أبوجلالة الكشف عن ملامح مبدأ الحرب الإلكترونية الخاص بالبنتاغون ، جريدة ايلاف لندن ، العدد 4146 الخميس 27 سبتمبر 2012

([lxxxi])Marty Lyons, THREAT ASSESSMENT OF CYBER WARFARE ,University Of Washington,Homeland Security - CSE P590TU,7 December 2005,pp.16-19 .

(lxxxii) لا يمكن رصد او تحديد الملامح الرئيسة لاستراتيجية الحرب الإلكترونية الصينية دون المرور بالمرتكزات والمحددات الرئيسة التي تقوم عليها العقيدة ألإستراتيجية الصينية بكل توجهاتها والمتأتية من السعي إلى تامين الأهداف الرئيسة الثلاثة للأمن القومي الصيني وهي :

1- الحفاظ على بقاء النظام (حكم الحزب الشيوعي الصيني)،

2- الدفاع عن السيادة الوطنية والسلامة الإقليمية،
3- إقامة الصين كقوة على الصعيدين الإقليمي والعالمي.
ينظر حول ذلك : منير شفيق ، ألإستراتيجية والتكتيك في فن علم الحرب من السيف والدروع إلى الصاروخ والانفاق ، الدار العربية للعلوم ناشرون ، بيروت ، 2008 ، ص ص 70-71.

([lxxxiii])Charles Billo, CYBER WARFARE AN ANALYSIS OF THE MEANS AND MOTIVATIONS OF SELECTED NATION STATES,INSTITUTE FOR SECURITY TECHNOLOGY STUDIES,AT DARTMOUTH COLLEGE,November 2004,p.25

([lxxxiv]) يشمل منهاج التدريب : النظرية الأساسية ، بما في ذلك أساسيات الكمبيوتر والتطبيقات؛ الإتصالات تكنولوجيا الشبكة ؛ طريق المعلومات السريع ؛ وحدات متصلة بواسطة تكنولوجيا المعلومات ؛ إلكتروني المضادة ؛ تكنولوجيا الرادار ؛ القواعد و اللوائح الحرب الإلكترونية ؛ استراتيجية الحرب الإلكترونية والتكتيكات ؛ المسرح والحرب السيبرانية ألإستراتيجية؛ نظم المعلومات ، بما في ذلك جمع ، والمنأولة، و نشر وإستخدام المعلومات و الأوأمر القتالية ، والرصد، و إتخاذ القرارات ، والسيطرة systems.81تدريب رسمي لضباط جيش التحرير الشعبى الصينى أخرى تشمل إستخدام أسلحة المعلومات، محاكاة الحرب الإلكترونية ، وحماية نظم المعلومات ، والكمبيوتر هجمات الفيروسات و الهجمات المضادة ، و التشويش ومكافحة التشويش على الإتصالات

(lxxxv) Deepak Sharma, Integrated Network Electronic Warfare: China's New Concept of Information Warfare ,Focus, Vol 4. No 2. April 2010,p.38.

([lxxxvi])Greg Bruno, Staff Writer, The Evolution of Cyber Warfare, Feburary 27, 2008,p.67

([lxxxvii]) يرى خبير استراتيجية الحرب الإلكترونية الصينية انغ باوكن ،ان العقيدة ألإستراتيجية السيبرانية الصينية استمدت رؤيتها من مبدأ المفكر الصيني القديم صن تزو بضرورة" إخضاع العدو دون قتال. "

(lxxxviii) وهي عقيدة قتالية مستمدة من أحدى أهم الفنون القتالية الصينية القديمة المعروفة بفن (الكونغ فو) .

([lxxxix]) لقد كانت إسرائيل اسبق من غيرها من دول الشرق الاوسط في تجنيد التقنيات الحديثة خدمة لأغراضها ، وهذا أمر تأكد في الخطاب السياسي للقادة الإسرائيليين ومنهم شيمون بيريز الذي أعلن " المعلومة اقوى من المدفع " ، قبل ان يتأكد أكثر عملياً من خلال الاقمار الاصطناعية التجسسية التي ارسلتها إسرائيل إلى الفضاء منذ عام 1990 ، والمواقع الإلكترونية العربية التي اخمدتها قوى القرصنة الإسرائيلية الموجهة من الموساد الإسرائيلي . ينظر للتفاصيل: بيخال محمد مصطفى ، دراسة حول فكرة القانون في الدستور ، مكتبة زين الحقوقية والادبية ، بيروت ، 2013، ص ص 213- 216.

([xc])القوات الإسرائيلية تطور قدرات الحرب الإلكترونية تدريبياً ، منتدى الجيش العربي ، الرابط:
http://www.sdarabia.com/preview_news.php?id=26598&cat=2

[xci] إسرائيل تواجه الهجمات الإلكترونية ، مقال منشور على شبكة الجزيرة بتأريخ 2011/4/5 على الرابط : http://www.aljazeera.net/home/print/

[xcii]القوات الإسرائيلية تطور قدرات الحرب الإلكترونية تدريبياً ، منتدى الجيش العربي ، الرابط : http://www.sdarabia.com/preview_news.php?id=26598&cat=2

(xciii) محمد المحيمد ، حرب الإستنزاف والابتزاز ، جريدة اخبار الخليج البحرينية ، العدد 11638 ، الثلاثاء 2 فبرأير 2010

(xciv) منير شفيق ، مصدر سابق ، ص 72

(xcv) حرب الإستنزاف من وجهة نظر مصرية ، دراسة نشرت على موقع وزارة الدفاع السودانية بتأريخ 13 فبرأير، 2010، على الرابط : http://mod.gov.sd/index.php/section-blog/80

[xcvi] المصدر السابق .

[xcvii] الحرب الإلكترونية.. إلى أين؟ ، مقال منشور على موقع الاسلام اون لاين بتأريخ 30 نوفمبر 2004 ، على الرابط : http://www.islamonline.net/iol-arabic/dowalia/scince-13/scince1.asp

[xcviii] المصدر السابق

[xcix] عصام نعمان ، الحرب الإلكترونية بديلاً من المقاومة المسلحة ، *نقلا عن صحيفة "الخليج" الأماراتية ، السبت 21 يناير 2012م

Deepak Sharma, op.cit,p.41. c

[ci] العقيد سالم احمد القيشي ، الحرب الإلكترونية الإسرائيلية ومستجداًتها ، صحيفة 26سبتمبر اليمنية ،

[cii]Greg Bruno, Staff Writer, The Evolution of Cyber Warfare ,Feburary 27, 2008,p.36

[ciii] Deepak Sharma, op.cit, p.41.

[civ] عماد غنيم ، اهوال الحرب الإلكترونية ، صحيفة الاهرام ألإقتصادية ، القاهرة ، 2012 /4/30

[cv] أمريكا تدق طبول الحرب الإلكترونية ، صحيفة الاهرام الاقتصادي ، القاهرة ، 2012 /6/18

[cvi] د. أمين ساعاتي ، **الحرب الإلكترونية العالمية القادمة** ، صحيفة ألإقتصادية السعودية ، العدد 6887 ، الأحد 19 أغسطس 2012

[cvii] ذكرت مصادر البنتاجون أن ما يقرب من 1500 مستخدم من إجمالى 3000 موظف الذين يعملون مباشرة مع مكتب وزير الدفاع، لم يتمكنوا من الدخول إلى البريد الإلكتروني بعد إختراق جهاز الكمبيوتر الرئيسي المزود بالخدمة "السيرفر".

[cviii] اشرف صلاح الدين ، مصدر سابق ، ص 34 .

[cix] ايمان الحمود ، الحرب الإلكترونية بين السعودية وإسرائيل ... من المستفيد؟ ، مقال منشور على موقع شبكة مونت كارلو ، بتأريخ 2012 /1/20 ، على الرابط :

http://www.mc-doualiya.com/articles/20120119-israel-saudi-arabia-hacker-cyber-war

([cx]) هشام منوّر ، الحرب الإلكترونية... المعترك الجديد ، جريدة المستقبل اللبنانية ، العدد 4226 ، السبت 14 كانون الثاني 2012.

([cxi]) عصام نعمان ، مصدر سابق .

(cxii) سأمر الياس ، هل العالم على أعتاب "الحرب الإلكترونية"؟ ، مقال منشور على موقع الكومبس الإلكتروني بتأريخ 2012/1/1 ، على الرابط :
/http://alkompis.se/interesting/did-you-know/1056

([cxiii]) Samuel Liles, op.cit,p.51.

([cxiv]) هل يودع العالم الأسلحة التقليدية؟ ، مقال منشور على موقع ميدل ايست أونلاين ، على الرابط : http://www.middle-east-online.com/?id=132743 2012-06-08

(cxv) الحرب الإلكترونية.. إلى أين؟ ، مصدر سابق .

([cxvi]) خلدون غسان سعيد ، ألإرهاب والجرائم المعلوماتية .. اختطاف وتسميم يومي للمواقع والملفات ، مجلو معلومات ، المركز العربي للمعلومات ، بيروت ، العدد 80 ، تموز 2010 ، ص ص 102-103 .

(cxvii) الحرب الإلكترونية.. إلى أين؟ ، مصدر سابق

([cxviii]) عمر حرزالله ، الحرب الإلكترونية.. صراع في العالم الافتراضي ، 4 مارس2012 http://www.albayan.ae/one

المصادر.

أولاً // الكتب.

1.احمد بن محمد بن علي الفيومي ، المصباح المنير في غريب الشرح الكبير للرافعي ، ج1 ، المكتبة العلمية ، بيروت ، بلا سنة طبع .

2.د.اشرف السعيد احمد ، القرصنة الإلكترونية ، دار النهضة العربية ، القاهرة ، 2013

3.بطرس البستاني ، محيط المحيط ، مكتبة لبنان ناشرون ، بيروت ، 1979 .

4.بيتر سينجر ، الحرب عن بعد : دور التكنلوجيا في الحرب ، مركز الأمارات للدراسات والبحوث ألإستراتيجية ، ابو ظبي ، 2010 .

5.بيخال محمد مصطفى ، دراسة حول فكرة القانون في الدستور ، مكتبة زين الحقوقية والادبية ، بيروت ، 2013 .

6.حاتم عبد الرحمن منصور ، الاجرام المعلوماتي ، دار النهضة العربية ، القاهرة ، 2002،

7.سامي عوض ، معجم المصطلحات العسكرية ، دار اسامة للنشر والتوزيع ، عمان ، 2008

8.فرانك بيلي ، معجم بلاكويل للعلوم السياسية ، مركز الخليج للأبحاث ، دبي ، 2004

9.نهلة عبد القادر المومني ، الجرائم المعلوماتية ، دار الثقافة ، عمان ، 2008 .

10. cxviii مارتن فان كريفلد ، حرب المستقبل ، ترجمة د. السيد عطا ، الهيئة المصرية العامة للكتاب ، القاهرة ، 1995 .
11. مصطفى طلاس ، الثورة العلمية التقنية وتطور القوات لمسلحة ، ط3 ، دار طلاس للدراسات والترجمة والنشر ، دمشق ، 2003
12. د.مصطفى طلاس وآخرون ، ألإستراتيجية السياسية العسكرية ،ط2، دار طلاس للدراسات والترجمة والنشر ، دمشق ، 2003 .
13. منير شفيق ، ألإستراتيجية والتكتيك في فن علم الحرب من السيف والدروع إلى الصاروخ والانفاق ، الدار العربية للعلوم ناشرون ، بيروت ، 2008.
14. د. وضاح زيتون ، المعجم السياسي ، دار اسامة للنشر والتوزيع ، عمان ، 2006 .
15. وليامسون مورأي ، حرب العراق : تأريخ عسكري وميداني يومي ، ترجمة مركز التعريب والبرمجة ، الدار العربية للعلوم ، بيروت ، 2005.

ثانياً // البحوث.

1.اشرف صلاح الدين ، الانترنت في عالم متغير ، مجلة معلومات ، المركز العربي للمعلومات ، بيروت ، العدد 80 ، تموز 2010 .
2.خلدون غسان سعيد ، ألإرهاب والجرائم المعلوماتية .. اختطاف وتسميم يومي للمواقع والملفات ، مجلة معلومات ، المركز العربي للمعلومات ، بيروت ، العدد 80 ، تموز 2010 .
3.محمد شعبان أيوب ، قصة الحرب الإلكترونية ، مجلة الوعي الاسلامي ، وزارة الاوقاف والشؤون الاسلامية ، دولة الكويت ، العدد 564 ، يونيو 2012.

ثالثاً // الصحف والدوريات.

1.أشرف أبو جلالة الكشف عن ملامح مبدأ الحرب الإلكترونية الخاص بالبنتاغون ، جريدة ايلاف لندن ، العدد 4146 الخميس 27 سبتمبر 2012
2.الجريمة في عصر وسائل الإتصال الحديثة ، صحيفة الجزيرة الإلكترونية ، المملكة العربية السعودية ، العدد 11426 ، بتأريخ 2004/1/10
3.الحرب الإلكترونية على إيران تتواصل من خلال فيروس (مهدي تروجان)، صحيفة الدستور الاردنية ، الأربعاء 29/أغسطس/2012
4.أمريكا تدق طبول الحرب الإلكترونية ، صحيفة الاهرام الاقتصادي ، القاهرة ، 18/6/ 2012
5. د. أمين ساعاتي ، **الحرب الإلكترونية العالمية القادمة** ، صحيفة ألإقتصادية السعودية ، العدد 6887 ، الأحد 19 أغسطس 2012
6. سالم احمد القيشي ، الحرب الإلكترونية الإسرائيلية ومستجداتها ، صحيفة 26سبتمبر اليمنية.
7.د.سامي سعيد حبيب في مجابهة الحرب الإلكترونية ، صحيفة المدينة ،السعودية ، العدد : 18057 ، الأحد 2012/9/30م
8.عصام نعمان ، الحرب الإلكترونية بديلاً من المقاومة المسلحة ، *نقلا عن صحيفة "الخليج" الأماراتية ، السبت 21 يناير 2012م

9. عماد غنيم ، اهوال الحرب الإلكترونية ، صحيفة الاهرام ألإقتصادية ، القاهرة ، 30/4/ 2012
10.محمد المحيمد ، حرب الإستنزاف والابتزاز ، جريدة اخبار الخليج البحرينية ، العدد 11638 ، الثلاثاء 2 فبرأير 2010

رابعاً // مواقع الشبكة الدولية للمعلومات.

1.مفهوم الحرب الإلكترونية ، منتدى طلاب جامعة القاهرة ، الأحد 10يونيو، 2012
مختار علي حيدر ، نشأة الحرب الإلكترونية وتطورها ، مقال منشور على موقع منتدى التكنلوجيا العسكرية والفضاء بتأريخ 5 ابريل 2014 ، على الرابط : http://army-tech.net/forum/index.php
2.الحرب الإلكترونية العالمية الأولى.. هل هي قادمة بالفعل؟ مقال منشور على موقع لها أون لاين، بتأريخ 05 - مايو – 2012 على الرابط: www.lahaonline.com/articles/view/40730.htm
3.الحرب الإلكترونية : مفهوم وأهداف ، منتدى الجيش الوطني الشعبي ، بتأريخ 20 تشرين الأول 2014 ، على الرابط : http://www.anp-dz.com/t6294-topic
4.رضاب نهار، الحرب الإلكترونية: مئة هجوم في الثانية بأسلحة مدمّرة ، ميدل ايست أونلاين ، مقال منشور على الرابط : http://www.middle-east-online.com/?id=134762
5.الحرب الإلكترونية ، بحث منشور على موقع المقاتل العربي ،على الرابط : http://www.moqatel.com/openshare/Behoth/Askria6/ElectroWar/sec04.doc_cvt.htm
6.د. محمد بن عطية الحارثي ، الحرب الإلكترونية على الإنترنت، دراسة منشورة على الرابط : http://faculty.ksu.edu.sa
7.الحرب الإلكترونية والتجسس الصناعي ، مقال منشور على موقع مجلة المنتدى العامة (كوكتيل) على الرابط : http://www.jableh.com/vb/showthread.php?t=6386
8.سأمر الياس ، هل العالم على أعتاب "الحرب الإلكترونية"؟ على الرابط :
9. alkompis.se/interesting/did-you-know/1056
10.عمر حرز الله ،الحرب الإلكترونية.. صراع في العالم الافتراضي ، مقال منشور على موقع البيان الإلكتروني الأماراتي ، بتأريخ: 04 مارس 2012 ، على الرابط : http://www.albayan.ae/five-senses/mirrors/2012-03-04-1.1604787
11.القوات الإسرائيلية تطور قدرات الحرب الإلكترونية تدريبياً ، منتدى الجيش العربي ، الرابط : http://www.sdarabia.com/preview_news.php?id=26598&cat=2
12.إسرائيل تواجه الهجمات الإلكترونية ، مقال منشور على شبكة الجزيرة بتأريخ 2011/4/5 على الرابط: http://www.aljazeera.net/home/print/
13.القوات الإسرائيلية تطور قدرات الحرب الإلكترونية تدريبياً ، منتدى الجيش العربي ، الرابط : http://www.sdarabia.com/preview_news.php?id=26598&cat=2
14. حرب الإستنزاف من وجهة نظر مصرية ، دراسة نشرت على موقع وزارة الدفاع السودانية بتأريخ 13 فبرأير،2010، على الرابط: http://mod.gov.sd/index.php/section-blog/80

15. الحرب الإلكترونية.. إلى أين؟ ، مقال منشور على موقع الاسلام اون لاين بتأريخ 30 نوفمبر 2004 ، على الرابط : http://www.islamnli

16. ايمان الحمود ، الحرب الإلكترونية بين السعودية وإسرائيل ... من المستفيد؟ ، مقال منشور على موقع شبكة مونت كارلو ، بتأريخ 2012 /1/20 ، على الرابط : http://www.mc-doualiya.com/articles/20120119-israel-saudi-arabia-hacker-cyber-war

17. هشام منوّر ، الحرب الإلكترونية... المعترك الجديد ، جريدة المستقبل اللبنانية ، العدد 4226 ، السبت 14 كانون الثاني 2012.

18. سأمر الياس ، هل العالم على أعتاب "الحرب الإلكترونية"؟ ، مقال منشور على موقع الكومبس الإلكتروني بتأريخ 2012/1/1 ، على الرابط :

19. http://alkompis.se/interesting/did-you-know/1056/

20. هل يودع العالم الأسلحة التقليدية؟ ، مقال منشور على موقع ميدل ايست أونلاين ،

21. على الرابط : http://www.middle-east-online.com/?id=132743 2012-06-08

22. عمر حرزالله ، الحرب الإلكترونية.. صراع في العالم الافتراضي ، 4 مارس2012 http://www.albayan.ae/one

BOOKS // FIRST.

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

2. Francis Rico C. Domingo, Chinese Cyber Warfare and its Implications on Selected Southeast Asian States , International Studies Department, De La Salle University, Manila

3. H.Banks, R. Mc Quillan, Electronic Warfare Test and Evaluation, Flight Test Techniques Series, RESEARCH AND TECHNOLOGY ORGANIZATION-NORTH ATLANTIC TREATY ORGANIZATION,Canada,2000

4. The Evolution of Cyber Warfare, Feburary 27, Greg Bruno, Staff Writer, 2008

5. James T. Westwood, Electronic Warfare and Signals Intelligence at the Outset War I, USN of World

6. Johnny Heikell, ELECTRONIC WARFARE SELF-PROTECTION OFBATTLEFIELD HELICOPTERS: A HOLISTIC VIEW, Helsinki University of Technology, Applied Electronics Laboratory, Series E: Electronics Publications E18, 2005

7. Dr Rex Hughes, Towards a Global Regime for Cyber Warfare, Cyber Security Project, Chatham House, London

8. Robert F. Erbacher, Extending Command and Control Infrastructures to Cyber Warfare Assets Department of Computer Science, Utah State University, Logan, USA .
9. Samuel Liles, Cyber Warfare as A form Of Low Intensity conflict And Insurgency, Conference on Cyber Conflict ,Proceedings 2010,C. Czosseck and K. Podins (Eds)CCD COE Publications, Tallinn, Estonia, 2010 .

Second : Thesis

1- Ali Can Kucukozyigit, ELECTRONIC WARFARE (EW) HISTORICAL PERSPECTIVES AND ITS RELATIONSHIP TO INFORMATION OPERATIONS (IO)—CONSIDERATIONS FOR TURKEY, THESIS Introduced to: NAVAL POSTGRADUATE SCHOOL , CALIFORNIA , September 2006

Third: Articles

1. Anthony E. Spezio, Electronic Warfare Systems, IEEE TRANSACTIONS ON MICROWAVE THEORY AND TECHNIQUES, VOL. 50, NO. 3, MARCH 2002
2. Anthony E. Spezio, Electronic Warfare Systems, IEEE TRANSACTIONS ON MICROWAVE THEORY AND TECHNIQUES, VOL. 50, NO. 3, MARCH 2002. Canadian National Defense-LAND FORCE INFORMATION OPERATIONS, ELECTRONIC WARFARE, B-GL-321-004/FT-001 2004-03-02
3. Charles Billo, CYBER WARFARE AN ANALYSIS OF THE MEANS AND MOTIVATIONS OF SELECTED NATION STATES,INSTITUTE FOR SECURITY TECHNOLOGY STUDIES,AT DARTMOUTH COLLEGE, November 2004
4. Clay Wilson, Information Operations, Electronic Warfare, and Cyberwar Capabilities and Related Policy Issues, Congressional Research Service Report RL31787, February 2, 2009 .
5. Deepak Sharma, Integrated Network Electronic Warfare: China's New Concept of Information Warfare ,Focus, Vol 4. No 2. April 2010 .
6. ELECTRONIC WARFARE : DOD Actions Needed to Strengthen Management and Over sight,Report to the Committee on Armed Services, House of Representatives, United States Government Accountability Office, July 2012.

7. Evan Baun, The Digital Underworld Cyber Crime and Cyber Warfare, HUMANICUS, issue 7, 2012 .
8. Jeffry T.Kelsey, Hacking into international Humanitarian Law: The principles of distinction and neutrality in the age of cyber warfare, Michigan law review,VOL106 .
9. Jon M. Anderson, THE NEW WIZARD WAR: CHALLENGES AND OPPORTUNITIES FOR ELECTRONIC WARFARE IN THE INFORMATION AGE, A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations. November 2007 .
10. Keith B .Alexander, Electronic Warfare in Operations (Final Approved Draft), Department of the Army, Washington, DC, No. 30-36
11. Marty Lyons, THREAT ASSESSMENT OF CYBER WARFARE ,University Of Washington,Homeland Security- CSE P590TU,7 December 2005
12. OFFENSIVE ELECTRONIC WARFARE, ,United States Army Signal Center and Fort Gordon Fort Gordon, Georgia, Sub-course Number SS0134, September 1994 .
13. Steven A. Hildreth, Cyber warfare, CRS Report for Congress ,Received through the CRS Web, Congressional Research Service, The Library of Congress, June 19, 2001