# الفصل الثاني

## الحروب التكنولوجية وتواطؤ المعلوماتية

## المعارك الإلكترونية

تشير بعض الدراسات إلى أن نسبة مساهمة عنصر التكنولوجيا في العمليات الإنتاجية تقترب من 75% وترتفع النسبة في التكنولوجيا العسكرية. وقد مرت عملية تطور الحاسبات بخمس مراحل أو (أجيال): في الجيل الأول كانت الحاسبات تعتمد على مكونات ميكانيكية وكهربائية وكانت قدراتها الحاسبية محدودة، ورغم ذلك كان لها دور كبير في إدارة نيران المدفعية في الحرب العالمية الثانية، ومع ظهور الصمامات المفرغة ظهرت الحاسبات الإلكترونية فازدادت قدراتها الحسابية وتم تصنيعها في أحجام أصغر رغم ما بها من عيوب كالاستهلاك العالي من الكهرباء والحاجة لتبريد مكوناتها. وولد الجيل الثاني من الحاسبات بعد اختراع أشباه المواصلات (Semiconductors) لتحل محل الصمام الفرغ، وانطوى التغيير على ميزات عملية في القدرات الحسابية واستهلاك الطاقة والحجم الأصغر. وفي الستينيات حدث تطور آخر تمثل في جمع عدد من الدوائر الإلكترونية في وحدات مجمعة تسمى الدوائر المتكاملة(Integrated Circuits (IC ، ثم ظهرت المعالجات الدقيقة وتنوع استخدامها في منتجات أخرى كالطائرات والصواريخ ومعدات الاتصال وأجهزة السيطرة على النيران في الدبابات... وغيرها.

وكان من نتائج ذلك أيضاً ظهور الحاسبات الدقيقة Microcomputers التي استخدمت مشغلاً دقيقاً وبدأ إنتاج الحاسبات الخاصة بأجهزة الرؤية الليلية والصواريخ الموجهة وأجهزة الملاحة والطيران وأجهزة تحديد المواقع فلكياً، وفي عام 1978م ظهرت الحاسبات الشخصية وتنافست الشركات في إنتاجها بقدرات حسابية وسرعات وإمكانات برمجة متفاوتة، ويمكن وصف الجيل الرابع من الحاسبات بأنه ذو سرعات وقدرات حسابية وتخزينية عالية، لكن السمة الأهم فيه هي ظهور لغات برمجة حديثة وقوية وحزم برامج جاهزة تيسر لغير المتخصصين استخدام الحاسبات.

أدى التطور الذي بدأ يتنامى في عدة اتجاهات إلى توسع استخدام الحاسبات في كل التطبيقات تقريباً، واعتمدت فكرة حاسبات الجيل الخامس على استخدام تكنولوجيا الذكاء الصناعي في بناء تطبيقات مثل نظم الخبرة للمساعدة في اتخاذ القرار وعمليات التشخيص الآلي في المستشفيات وصولاً إلى الإنسان الآلي، وأثمرت هذه التطورات ثورة الوسائط المتعددة Multi Media ، ثم ظهور البنوك الآلية والأسلحة الذكية والصواريخ الموجهة تلفزيونيا والصواريخ ذات المستشعرات الكهرومغنطيسية وغيرها، ومع نهاية عقد الثمانينيات اتجهت اليابان للتفكير في أجيال أخرى من الحاسبات باستخدام تكنولوجيا الخلايا العصبية والمنطق المبهمNeutral and Fuzzy Technologies لإنتاج حاسبات الجيل السادس، وتقوم هذه التكنولوجيا بمحاكاة الجهاز العصبي للإنسان.

وتعد الحاسبات فائقة القدرة قمة تطور تكنولوجيا الحاسبات في نهاية القرن العشرين، وقد ظهرت استجابة للحاجة لقدرات حسابية فائقة لا تفي بها الأجيال التي ظهرت من الحاسبات العادية. ومن أهم تطبيقات هذه الأجهزة: مبادرة حرب النجوم الأمريكية، وعمليات حرب الخليج الثانية الخاصة بصواريخ سكود وصواريخ باتريوت، ونظم الصواريخ المضادة للصواريخ العابرة للقارات. ولتحقيق القدرة الحسابية الفائقة يستخدم مصمموها عددا من المعالجات الدقيقة تعمل بالتشغيل المتوازي أو المتعدد، حيث تعمل المعالجات في وقت واحد على مهمة واحدة يتم تقسيمها بينهم آليا. يتوقع أن يؤدي إلى إحلال الأساليب الرقمية محل الأساليب التناظرية في معظم المعدات الإلكترونية، وفوق ذلك فهي التكنولوجيا الأساسية في كل ما يتعلق بالحواسب الآلية، إذ أسهم استخدامها في تصغير حجم ووزن المعدات، مما سهل نقلها جواً، وإخفاءها، ورفع قدرتها على المناورة. وقد أصبح بالإمكان التعامل مع الخرائط رقمياً - كما في صواريخ كروز - وتبادل المعلومات بين القيادة والوحدات القتالية بشكل مستمر، وتلقي الصور من ميدان المعركة من صور الأقمار الاصطناعية أو الطائرات بدون طيار، حيث يتلقاها الحاسب العملاق فيقوم بعمليات فرز وتجنيب وتبويب ثم يوجهها إلى كل قائد ميداني فيما يخصه، وللتعامل مع هذا الكم الكبير من المعلومات وعمليات المعالجة المعقدة والمتعددة، هناك حاجة إلى حاسبات عسكرية ذات سرعات فائقة وذاكرة ضخمة جداً، وهذه الحاسبات العسكرية العملاقة ستكون أحد ظواهر القرن الحادي والعشرين، ولأجل التغلب على قيود اتفاقية حظر التجارب النووية طورت الدول المتقدمة حواسب قادرة على محاكاة التجارب النووية بشكل افتراضي، وهي حواسب تبلغ سرعتها أكثر من 100 ألف ضعف عن الحواسب الموجودة حالياً، ويطلق على مشروعها "المبادرة الاستراتيجية للحاسبات المتسارعة".

لذلك فإن الحرب الإلكترونية تكون السمة الغالبة إن لم تكن الرئيسة للحروب في القرن الواحد والعشرين. فالعالم أصبح يعتمد أكثر على الفضاء الإلكتروني لا سيما في البنى التحتية المعلوماتية العسكرية والمصرفية والحكومية إضافة إلى المؤسسات والشركات العامة والخاصة. ولا شك أنّ ازدياد الهجمات الإلكترونية والتي نشهد جزءًا بسيطا منها اليوم يرتبط أيضا بازدياد هذا الاعتماد على شبكات الكومبيوتر والإنترنت في البنية التحتية الوطنية الأساسية، وهو ما يعني إمكانية تطوّر الهجمات الإلكترونية اليوم لتصبح سلاحا حاسما في النزاعات بين الدول في المستقبل، علما أنّ أبعاد مفهوم الحرب الإلكترونية لا تزال غير مفهومة لدى شريحة واسعة من المراقبين وحتى العامة.

وقد اجتهد عدد من الخبراء من ضمن اختصاصاتهم في تقديم تعريف يحيط بمفهوم الحرب الإلكترونية، فعرّف كل من "ريتشارك كلارك" و"روبرت كناكي" الحرب إلكترونية

على أنها "أعمال تقوم بها دولة تحاول من خلالها اختراق الأجهزة والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها.
فيما يعرّفها آخرون بأنها "مفهوم يشير إلى أي نزاع يحدث في الفضاء الإلكتروني ويكون له طابع دولي". ولأن مثل هذه التعريفات فضفاضة ولا تعبّر بدقّة عن فحوى الموضوع، يقترح آخرون أن يتم التركيز بدلا من ذلك على أنواع وأشكال النزاع التي تحصل في الفضاء الإلكتروني، ومنها:
أ- القرصنة الإلكترونية: أو التخريب الإلكتروني، وتقع في المستوى الأول من النزاع في الفضاء الإلكتروني، وتتضمن هذه العمليات القيام بتعديل أو تخريب أو إلغاء المحتوى. ومن أمثلته القيام بعمليات قرصنة المواقع الإلكترونية أو بتعطيل الحواسيب الخادمة أو ما يعرف باسم الملقّمات من خلال إغراقها بالبيانات.
ب- الجريمة الإلكترونية والتجسس الإلكتروني: ويقعان في المستوى الثاني والثالث وغالبا ما يستهدفان الشركات والمؤسسات وفي حالات نادرة بعض المؤسسات الحكومية.
ج- الإرهاب الإلكتروني: ويقع في المستوى الرابع من النزاع في الفضاء الإلكتروني. ويستخدم هذا المصطلح لوصف الهجمات غير الشرعية التي تنفّذها مجموعات أو فاعلون غير حكوميون ضد أجهزة الكمبيوتر والشبكات والمعلومات المخزّنة. ولا يمكن تعريف أي هجوم إلكتروني بأنه إرهاب إلكتروني إلا إذا انطوى على نتائج تؤدي إلى أذى مادّي للأشخاص أو الممتلكات والى خراب يترك قدرا كبيرا من الخوف.
د- الحرب الإلكترونية: وهي المستوى الأخطر للنزاع في الفضاء الإلكتروني، وتعتبر جزءا من الحرب المعلوماتية بمعناها الأوسع، وتهدف إلى التأثير على إرادة الطرف المستهدف السياسية وعلى قدرته في عملية صنع القرار، وكذلك التأثير فيما يتعلق بالقيادة العسكرية أو توجهات المدنيين في مسرح العمليات الإلكتروني. وأوصل صاروخ "أر أس-20 دنيبر" الذي أطلقته قوات الصواريخ الاستراتيجية الروسية في مقاطعة أورينبورغ في جنوب منطقة الأورال، أقماراً صناعية خصصت لغرض استشعار الأرض عن بعد، إلى مواقعها المدارية في الفضاء.
وحمل الصاروخ 33 قمرا صناعيا تتبع لمختلف الدول بينها قمر "تابليتسات أفرورا" المملوك لإحدى الشركات الخاصة الروسية.
وصُمِّم صاروخ "أر أس-20 دنيبر" (أو "ساتان" /الشيطان/ بحسب مصطلحات حلف شمال الأطلسي) أصلاً لحمل رؤوس حربية إلى الأهداف المطلوب تدميرها، ولا يزال يعتبر أرهب صاروخ في العالم .
ويظل عدد كبير من صواريخ "الشيطان" في الخدمة في صفوف قوات الصواريخ الاستراتيجية الروسية، فيما تحوّل عدد من الصواريخ التي سُحبت من الخدمة العسكرية

للاستخدام المدني. وقام المهندسون الروس والأوكرانيون بإعادة تأهيلها لحمل الأقمار الصناعية إلى مدارات يتراوح ارتفاعها بين 300 و900 كيلومتر في الفضاء. وكان إطلاق صاروخ "أر أس-20 بي" الذي حمل الأقمار الصناعية الـ33، اختباراً جديداً لقدرات صواريخ "الشيطان."

وقال قائد الفرقة 13 من قوات الصواريخ الاستراتيجية الروسية، العقيد يفجيني كونوفالينكوف، مخاطبا الجنود والضباط الذين أداروا عملية إطلاق الصاروخ إن هذه العملية أكدت متانة وأمانة صواريخ "أر أس-20."

ومن المتوقع أن تصبح الحرب الإلكترونية نموذجا تسعى إليه العديد من الجهات نظرا للخصائص العديدة التي تنطوي عليها، ومنها:

1- الحروب الإلكترونية هي حروب لا تناظرية: فالتكلفة المتدنية نسبيا للأدوات اللازمة لشن هكذا حروب يعني أنّه ليس هناك حاجة لدولة ما مثلا أن تقوم بتصنيع أسلحة مكلفة جدا كحاملات الطائرات والمقاتلات المتطورة لتفرض تهديدا خطيرا وحقيقيا على دولة مثل الولايات المتّحدة الأمريكية على سبيل المثال.

2- تمتّع المهاجم بأفضلية واضحة: في الحروب التكنولوجية يتمتع المهاجم بأفضلية واضحة وكبيرة على المدافع، فهذه الحروب تتميز بالسرعة والمرونة والمراوغة. وفي بيئة مماثلة يتمتّع بها المهاجم بأفضليّة، من الصعب جدا على عقليّة التحصّن لوحدها أن تنجح. فالتحصين بهذا المعنى سيجعل من هذا الطرف عرضة لمزيد من محاولات الاختراق وبالتالي المزيد من الضغط.

3- فشل نماذج "الردع" المعروفة يعد مفهوم الردع الذي تمّ تطبيقه بشكل أساسي في الحرب الباردة غير ذي جدوى في الحروب الإلكترونية. فالردع بالانتقام أو العقاب لا ينطبق على سبيل المثال على هذه الحروب. فعلى عكس الحروب التقليدية حيث ينطلق الصاروخ من أماكن يتم رصدها والرد عليها، فإنه من الصعوبة بمكان بل ومن المستحيل في كثير من الأحيان تحديد الهجمات الإلكترونية ذات الزخم العالي. بعض الحالات قد تتطلّب أشهرا لرصدها وهو ما يلغي مفعول الردع بالانتقام وكثير من الحالات لا يمكن تتبع مصدرها في المقابل، وحتى إذا تم تتبع مصدرها وتبين أنها تعود لفاعلين غير حكوميين، فإنه في هذه الحالة لن يكون لديهم أصول أو قواعد حتى يتم الرد عليها.

4- المخاطر تتعدى استهداف المواقع العسكرية: لا ينحصر إطار الحروب التكنولوجية باستهداف المواقع العسكرية، فهناك جهود متزايدة لاستهداف البنى التحتية المدنية والحسّاسة في البلدان المستهدفة، وهو أمر أصبح واقعيا في ظل القدرة على استهداف شبكات الكهرباء والطاقة وشبكات النقل والنظام المالي والمنشآت الحساسة النفطية أو المائية أو الصناعية بواسطة فيروس – كمثال- يمكنه إحداث أضرار مادّية حقيقية تؤدي

إلى انفجارات أو دمار هائل.

وفي ديسمبر 2009، أوردت الحكومة الكورية الجنوبية تقريرا عن تعرضها لهجوم نفّذه قراصنة كوريين شماليين بهدف سرقة خطط دفاعية سريّة تتضمن معلومات عن شكل التحرّك الكوري الجنوبي والأمريكي في حالة حصول حرب في شبه الجزيرة الكورية.

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

ويجمع الخبراء على أنّ الهجوم الإلكتروني الذي استهدف استونيا في 2007، يكاد يكون الهجوم الإلكتروني الأول الذي يتم على هذا المستوى ويستخدم لتعطيل المواقع الإلكترونية الحكومية والتجارية والمصرفية والإعلامية مسببا خسائر بعشرات الملايين من الدولارات إضافة إلى شلل البلاد. وعلى الرغم من أنّ الشكوك كانت تحوم حول موسكو على اعتبار أن الهجوم جاء بعد فترة قصيرة من خلاف استوني-روسي كبير، إلا أنّ أحدا لم يستطع تحديد هوية الفاعل الحقيقي أو مصدر الهجوم الذي تم، وهي من المصاعب والمشاكل التي ترتبط بالحروب التكنولوجية. ومن أهم الأسلحة الحديثة القنبلة الكهرومغناطيسية،فهي من بين أهم وأخطر ما يهدد البشرية، لأنها من الأسلحة التي التى تهاجم الضحايا من مصدر مجهول يستحيل أو يصعب رصده مثل الأسلحة البيلوجية والكميائية.. والكهرومغناطيسية..وبالتحديد أسلحة موجات "الميكرو" عالية القدرة. في أقل من غمضة عين تستطيع "القنبلة الكهرومغناطيسية" أن تقذف بالحضارة والمدنية الحديثة مائتي عام إلى الوراء.

## التدمير الرقمي

يعيش العالم اليوم مرحلة جديدة من التطور التكنولوجي امتزجت فيها نتائج ثورات ثلاث، هى :ثورة المعلومات، أي ذلك الكم الهائل من المعرفة في صورة تخصصات ولغات عديدة، الذي أمكن السيطرة عليه بواسطة تكنولوجيا المعلومات، وثورة وسائل الاتصال المتمثلة في تكنولوجيا الاتصال الحديثة، وقوامها الأقمار الصناعية والألياف البصرية، وثورة الحواسيب الإلكترونية التي توغلت في مناحي الحياة كلها . وتمثل شبكة الإنترنت جوهر ذلك الامتزاج. وفيها يجرى تخزين المعلومات التي ترد من عدد هائل من شبكات المعلومات بشكل منظّم للغاية، ثم تنقلها بعد ذلك تقنيات الاتصال المتطوّرة، من أقمار صناعية وغيرها، إلى مئات الملايين من مستخدمي هذه الشبكة .وتجدر الإشارة إلى أن ثورة تكنولوجيا الاتصال سارت متوازية مع ثورة تكنولوجيا المعلومات، كما أن الخيرة جاءت محصلة لتفجّر المعلومات، وتضاعف الإنتاج المعرفي في مختلف المجالات والتخصصات . وأوجد ذلك الحاجة إلى ضرورة تحقيق أفضل سيطرة ممكنة على فيض المعلومات المتدفقة، وإتاحته للباحثين ومتخذي القرار في أسرع وقت وبأقل جهد، عن طريق استحداث أساليب تنظيمية جديدة تعتمد في الدرجة الأولى على الحاسوب، واستخدام التكنولوجيا الاتصالية لمساندة مؤسسات المعلومات، ونشر خدماتها وتطويرها عبر القارات .وهي ظاهرة فريدة، فزيادة المعلومات تدفع إلى المزيد من تطور تكنولوجيا المعلومات، الذي يقود بدوره إلى توالد المعلومات وتراكمها بصورة قياسية لا حدود لها . ومن ثم، فإنه لم يعد من الممكن الفصل بين تكنولوجيا المعلومات وتكنولوجيا الاتصال، فقد جمع بينهما النظام الرقمي الذي تطوّرت إليه نظم الاتصال، وبهذا ترابطت شبكات الاتصال مع شبكات المعلومات. تحتاج تقنيات المعلومات والاتصالات إلى توافر موارد رئيسية، هي تعليم متميز، وبنية تحتية ملائمة، ومنظومة من المؤسسات المستقرة . وبدون هذه الموارد الثلاثة سوف تزداد الفجوة المعلوماتية والرقمية بين الأغنياء والفقراء، والأخيرون، بطبيعة الحال، هم الأكثر تضرراً . ولم يعد خافياً أن استمرار وجود ما تعرف بالفجوة الرقمية على مستوى الدول سوف يصيب العالم بمشكلات كبيرة. ويلخص هؤلاء ما ينطوي عليه الموقف الراهن من سلبيات بقولهم: إن من بين أشد تلك الأخطار كلها خطر اللاوعي بطبيعة التحولات الجذرية العميقة، التي يعنيها انتقال المجتمع الدولي برمّته إلى عصر المعلومات . ثم يرد بعد ذلك الخطر الآخر المنبثق من الانضمام اللاواعي إلى شبكة معلومات واتصالات كونية لا تملك بعض الدول النامية القدرة على التعامل معها بكفاءة، وذلك بسبب النقص الذي تعانيه في كوادرها البشرية، ومهاراتها التنظيمية، وحصانتها الثقافية في وجه محاولات الاختراق الخارجي.. إلخ.

وسبب هذا الثراء اللامحدود في مصادر المعرفة بأشكالها ونوعياتها وتطبيقاتها كلها، فإن المؤسسات العسكرية والمدنية يجب ان تراجع المفاهيم التي سادت في مرحلة ما قبل هذه الثورة، وتعيد تقويمها.ثمة أهمية كبيرة للبحث المعمق في الظروف المستجدة بتأثير من الثورة

المعلوماتية والاتصالية الراهنة، فالحروب وما تخلفه من تدمير شامل، قد تستخدم فيه أحياناً الأسلحة النووية، ربما تلجأ إلى إحداث الخراب الواسع بواسطة الأسلحة المعلوماتية، بدلاً من الكلاسيكية المعروفة . ومثل هذا التحول إذا قدر له أن يحدث في الواقع، فسوف يكون انقلاباً ثورياً خطراً للغاية بكل المقاييس. وسوف يفرض التخطيط لهذه النوعية المتطورة من الحروب الدولية ( حروب الدمار المعلوماتي، وتوصف بالحروب الرقمية أيضاً ) التحول باتجاه تصميم منظومات مبتكرة من القواعد والآليات يمكن الاعتماد عليها في إدارة تلك الحروب، هجومية كانت أو دفاعية. ووفق ذلك، فإن حروب ما بعد الربع الثاني من القرن ال21 ستخاض بأسلحة تتسم بقدرات غير محدودة على إلحاق الأذى من دون أن تكون معلومة المصدر، وستبدو أقرب إلى حروب الأشباح إذا جاز التعبير، فهي تنطلق إلى تدمير أهدافها من قواعد غير منصوبة .كما أن في مقدور ترساناتها من الاسلحة ( غير المرئية أو المعروفة بدقة) أن تفلت من خطر الضربات الاستباقية أو الإجهاضية الساعية إلى تدميرها، وهي لا تزال قابعة بعد في مكامنها.

وهي حروب مباغتة وذكية بصورة لا عهد للبشرية بها . وذلك ما يجعل من القدرة على مواجهتها لتوقي أخطارها المدمرة أمراً بالغ الصعوبة. وتقوم على أسس انتقائية خالصة في إثارتها وإدارتها، وكذلك في التخطيط لها، وذلك من منطلق أنها لا تستغرق وقتاً على الانطلاق . وأهم ما فيها هو عنصر المفاجأة. ومن دون ذلك تفقد تلك الحرب (المعلوماتية ) واحداً من أهم مقومات فاعليتها التدميرية . كما تعتمد في التخطيط لها على محاولة إفقاد الخصم القدرة على التحسب المسبق لها بالسيناريوهات المضادة. ثمة ملاحظات يجب أن تُضاف إلى ما سبق، وهي:1- حروب المعلومات يمكن أن تلحق الدمار، خاصة بقطاعات حساسة للغاية، كقواعد البيانات الحيوية والمعلومات الاستراتيجية المتعلقة بالأمن القومي للدولة، وقد يستحيل إصلاحها إذا ما تم تعطيلها.

2- جهود التطوير غير المرئية ( لنا) تجرى حالياً على قدم وساق داخل مختبرات الأبحاث المعنية بابتكار أسلحة الحرب المعلوماتية وتطويرها وتنويعها، وزيادة درجة مناعتها في وجه محاولات الهجوم المضاد عليها . وهذا التطوير في مختلف صوره وأشكاله وأبعاده، وبكل ما يحمل من خفايا أسرار يسعى إلى إيجاد منظومة شاملة ومتكاملة من الأسلحة المعلوماتية، بحيث يخدم كل منها سيناريو خاصاً به. وتلك السيناريوهات كلها سوف

تتوزع بين ما يمكن أن يكون ملائماً لطبيعة الحرب المعلوماتية المحدودة ، أو للحرب المعلوماتية الشاملة.

وذلك ما يتماثل مع ما كان يحدث في الماضي، أو لا يزال، عندما كان يجرى التخطيط للحروب النووية التكتيكية الصغيرة أو المحدودة، والحروب النووية الاستراتيجية، أو الشاملة . وبالطبع، فإن لكل واحد من هذه السيناريوهات أسسه ومتطلباته وتكلفته وآلياته وتبعاته، مثلما له مخاطره وإشكالياته.

3- من أبرز خصائص حروب الدمار المعلوماتي أن في إمكانها تخطي الروادع كافة، التي حالت حتى دون نشوب حروب الدمار الشامل بأسلحتها الراهنة . ومن الأسباب التي تساعد على ذلك، الصعوبة في رصد مؤشرات قرب وقوع الحرب المعلوماتية، أو في اعتراضها عند انطلاقها، وتوقع مداها وتحديده، أو حتى في التيقن ممن يقفون وراءها ويتحملون المسئولية عنها. ومن شأن تلك الصعوبات والمحاذير التي تكتنف الحرب المعلوماتية أكثر من غيرها من حروب الدمار الشامل المعروفة، أن تشل كثيراً قدرة الخصم على المواجهة . بل ربما تفقده القدرة على اتخاذ القرار الذي يتيح له إدارة مثل هذا الموقف المعقد والمفعم بالاحتمالات.

4- تكلفة حروب المعلومات هي بالمقارنة أقل نسبياً مما يتكلفه إنتاج أسلحة الدمار الشامل الأخرى، ووسائط نقلها لإيصالها إلى أهدافها عبر القارات وتطويرها وإخفائها . وربما يرجع السبب في ذلك إلى أن الأسلحة المعلوماتية ليست كغيرها من الأسلحة التي تقوم على الإبادة الشاملة لكل مظاهر الحياة، إنسانية وغير إنسانية، إذ يتركز هدفها على محاولة تعطيل العقل الذي يفكر للمجتمع، وتدمير الشرايين التي تنبض بالحياة فيه.

## تكنولوجيا الخفاء

تعد تكنولوجيا الإخفاء من أهم تطورات تكنولوجيا الحرب الحديثة وتوفر نظم الإخفاء وسائل بسيطة وعالية الاعتمادية للأفراد والمعدات ومع تضاؤل الفجوة الزمنية بين اكتشاف الهدف وضربه أصبحت تكنولوجيا الإخفاء تقوم بدور متميز في تقليل الخسائر البشرية والمادية على السواء، وقد تطور الإخفاء من الوسائل التقليدية (شباك تمويه - طلاء بلون معين -..) ليتخذ مسارات مختلفة، أهمها: الإخفاء الحراري باختزال حجم ودرجة إشعاع المصادر الساخنة، حيث لايمكن فنيا إلغاء البصمة الحرارية للمعدات، بينما يمكن تخفيض مستواها بحيث لا تبدو لمن يرصدها واضحة، وهناك أيضاً الإخفاء الراداري من خلال امتصاص وتشتيت الموجات الرادارية وإضعافها إلى مستوى قريب من مستوى الموجات المرتدة من البيئة المحيطة. أما الطلاء ببويات خاصة فيختلف عن الطلاء ببويات التمويه التقليدية في أن بعضها له قدرة عاكسة للأشعة تحت الحمراء، وبعضها يمتص الأشعة تحت الحمراء، ولذا يستخدم لدهان جميع المعدات العسكرية (طائرات - قطع بحرية - مركبات بأنواعها) فيقلل بصورة ملموسة تعرضها للقذائف الحساسة للأشعة تحت الحمراء. وهناك نوع ثالث له قدرة على امتصاص أشعة الرادار ويستخدم في دهان الطائرات والقطع البحرية وهو ما يعني فاعليته في الإخفاء الحراري والراداري معاً، وخلال حرب الخليج الثانية تم طلاء الدبابات الأمريكية بإحدى تلك البويات التي تعكس 85% من الأشعة الساقطة عليها، مما أدى لتخفيض حرارة سطحها ب15 درجة مئوية.

ومن أشكال الإخفاء المهمة تقليل البصمة الرادارية من خلال تصميم المعدة نفسه طبقاً لزوايا انسيابية معينة لكل أنواع المعدات، فمثلاً أمكن تقليل المقطع الراداري للدبابة من حوال 50م2 إلى 1،0م2، واستخدمت هذه التقنية بنجاح في الطائرة F117 الشبح. وتعتبر المقاتلة F-117 بمثابة المقاتلة الأولى التي تم تصميمها خصيصاً للاستفادة من المراقبة الرادارية المنخفضة. تتميز الطائرة ببصمة رادارية . لا تزيد عما هو بين 0.01 و0.001 من المتر المربع .مما يجعلها تظهر على شاشات الرادار أنها طائرة صغيرة، فقط عند دخولها لمدى 8 – 16 ميل، وللطائرة كرسي قاذف لمقعد الطيار وعدة أنظمة تساند أعمال الطائرة في الأحوال الجوية الليلية، وتحتوي حاوية للتسليح، موقعها في وسط الطائرة تحمل من الذخائر حتى 5000رطل، ولها 2000 رطل من الذخائر الموجهة بالليزر (MK-84 ) عالية الانفجار، وأيضاً قذائف .(GBU-27) لم يكتفي الصانعون بتلك التقنيات فحسب، لننظر إلى محركات الطائرة، ليس محركاً عادياً، إنه من تصميم جنرال إلكتريك التوربيني المروحي، بدون احتراق، صممت هذه المحركات بحيث تحوي فتحتي دخول الهواء، وليس كالمحركات الأخرى، نظام امتصاص، فتحات خاصة لدخول الهواء

بنفسه، لأنه في المحركات العادية تدخل الموجات الرادارية مع دخول الهواء إلى المحرك الذي يمتصه، أما في هذه الطائرة (F-117) فهناك فتحات خاصة لدخول الهواء لا يمكن للموجات الرادارية الدخول منها.تم صنع هذه الطائرة من الألومينيوم مع بعض التيتانيوم المستخدم في المحركات النفاثة، صنع السطح الخارجي لبدن الطائرة منفصلاً عن الهيكل الخارجي، بمعنى أن هيكل الطائرة صنع، وفوقه طبقة منفصلة هي السطح الخارجي، صممت كذلك بغرض تقليل البصمة الرادارية، وكما أسلفنا، تم تغطية سطح الطائرة بمادة ماصة لأشعة الرادار التي يتم تصنيعها آلياً، السبب هو تفادي تأثير المادة على العاملين وقد لعبت المراقبة الرادارية المنخفضة دوراً هاماً في عدة تصاميم لعدة طائرات من مختلف المصانع.

أما شباك التمويه متعددة الأغراض فهي نوعية حديثة مصنوعة من النايلون وذات تركيب بتروكيماوي يجعلها قادرة على أن تعكس الأشعة تحت الحمراء إلى جانب تشتيت الأشعة الرادارية أو امتصاصها. كما أصبح بالإمكان القتال على الجبهة وفي العمق معاً إلى جانب التغلب على العقبات الطبوغرافية من خلال تطويع عدد من التكنولوجيات التي يمكن من خلالها القتال عن بعد وتستخدم هذه النظم الذكية الحواسب متناهية الصغر التي يتم تخزين بيانات الهدف فيها وتوضع في رأس القذيفة. ومستشعرات باحثة عن الحرارة أو الموجات الكهرومغنطيسية التي تجذبها للهدف، وتعد صواريخ كروز أبرز تطبيقات هذا النظام.

ومن التطبيقات المهمة أيضاً لهذه الثورة الذكاء الصناعي، وهو أحد علوم الحاسبات في مجال تصميم أنظمة ذكية لها القدرة على تفهم الكلام والقيام بعمليات استنتاج واستدلال وحل مسائل، ويعتمد تصميمها على توافر قاعدة معلومات في مجال التخصص تبنى على أساس اختزان الخبرات ومحاكاتها، فهي تحاول محاكاة العنصر البشري بالكفاءة نفسها، ولكن بسرعة ودقة أكبر، ويمكن تحويل أي من النظم المساعدة في إتخاذ القرار إلى نظام ذكي بإضافة قاعدة معلومات تحسن أداءه، وقد تم إنتاج نماذج كثيرة للنظم الذكية - تم استخدامها في حرب الخليج الثانية - تركزت في مجالات: المستشعرات متعددة الأغراض، وتحليل الرسائل والشفرات، وتحديد مواقع القوات، واختيار التكتيكات وطرق الاقتراب المناسبة وتمييز الأهداف وتفسير الخرائط والتوجيه الآلي. وقال علماء أمريكيون إنهم اقتربوا خطوة من تطوير مواد يمكن أن تمكن البشر من التواري.وطور علماء من جامعة بركلي بكاليفورنيا مادة يمكنها أن تحول الضوء عن الأشياء ثلاثية الأبعاد مما يخفيها عن الأنظار، وفقا لما يسمى بالانعكاس المقلوب أو السالب، وهو نفس مبدأ الفيزياء البصرية الذي يعطي الانطباع بأن قشة وضعت في كوب من الماء تبدو كما لو كانت منكسرة.

ولا توجد هذه المادة في شكل عادي، فقد أنتجت على قياس متناهي الصغر يناهز جزءا من مليار جزء من المتر. وقد استخدمت مقاربتان إحداهما استخدمت كمية متناهية الصغر من الفضة وفلورايد المجنيزيوم والأخرى استخدمت فيها حبال متناهية الصغر من الفضة.ولم تمتص هذه الأشياء الضوء كما لم تعكسه "مثل ماء ينساب حول صخرة". وكانت النتيجة أن الضوء الوحيد الذي يمكن رؤيته هو ضوء الخلفية. ويقول العلماء إن المبادئ التي يستند عليها الاكتشاف قد تمكن في المستقبل من صنع ملابس خفية ولكننا لانرجح ان هذا يتم استخداه او يدخل في حيز التنفيذ قبل نهاية منتصف القرن.وقد نشرت مجلتا ساينس ونيتشر الأمريكيتان بحث فريق العلماء هذا الذي يقوده جيان تسانغ. وقد أجريت من قبل تجارب على الانعكاس السالب استخدمت الأمواج الدقيقة (مايكرويف)، وهي أمواج ضوئية بالغة الطول بحيث تعجز العين البشرية المجردة عن رؤيتها. ومن خلال علوم النانو تكنولوجي يمكن استخدام شرائح من الأنابيب الكربونية فائقة الصغر (أنابيب نانو-كربونية) يتم طيّ مسار الضوء حول الجسم المراد إخفاؤه فيبدو وكأن الضوء قد مر من خلاله دون أي وجود له!. ومثال ذلك نراه في الصحراء حين ينقل لنا السراب أشياء توجد على مسافات بعيدة بسبب انكسار الضوء.

ومنذ الكشف عن المقاتلة الروسية سوخوي تي — 50 الخفية من الجيل الخامس والحديث عن اختلال ميزان القوى في لغرب لا يكاد يهدأ. وفي خضم فعاليات معرض ماكس 2011 الجوي، الذي أقيم في قاعدة جيكوفسكي بالقرب من ضواحي موسكو سمح الروس باستعراض المزيد من مميزات وقدرات طائرتهم الأخيرة التي حلق منها نموذجان في استعراض رائع أبهر الغرب أكثر من الروس أنفسهم، في مباردة من موسكو لتنبيه الغرب وعلى رأسهم الولايات المتحدة أن الصناعات الجوية الروسية قد بدأت تعيد هيبتها الصناعية من جديد. لكن الأبرز في ذلك هو الحديث عن تكنولوجيا للخفاء ومضادة للخفاء يزاح عنها النقاب حديثا، يمكنها أن تتسبب في أزمة حقيقية لقدرات الخفاء للطائرات الأمريكية التي طالما تمتعت بها لعقود.

ويذكر ان مفهوم الخفاء أصبح أمراً ملحّاً بالنسبة الى المخططين في سلاح الجو الامريكي، خصوصا بعد ان بينت حرب 1973 التي دارت بين مصر واسرائيل، مدى فتك انظمة الدفاع الجوي الصاروخية ورادارتها التي ازدادت تطورا بالطائرات المقاتلة. والحقيقة ان تاريخ تصميم طائرة غير قابلة للكشف تعود الى حقبة الحرب العالمية الثانية، الا انه في عام 1983 رسميا اعتبر بداية تلك التقنية واستخداماتها، حيث استلم سلاح الجو الامريكي أول سرب من طائرة إف - 117 ذات القدرات الخفائية عن الكشف بواسطة موجات الرادار الأمر الذي مكنها من التحليق من دون ان يتم رصدها او حتى كشفها، وفي

عام 1988 نشر سلاح الجو الامريكي صورا فنية لشكل قاذفة هي B-2 توضح ملامحها الرئيسية التي هي عبارة عن طائرة ذات حواف خلفية تشبه حرفي W باللاتينية وبفتحات دخول الهواء لمحركاتها مثبتة فوق جناحيها الكبيرين، كما لا يوجد فيها دفة رأسية ومجموعة ذيل خلفية، والطائرة بمجمل عام عبارة عن شكل جناح طائر، وبهذا يكون سلاح الجو الأميركي الرائد في هذا المجال قد افتتح رسميا عهد الطائرات الخفية.

ان استخدام الدهان الماص للاشعاع الراداري ليس بفكرة وليدة اليوم، فقد سبق لسلاح الجو الالماني في عهد هتلر أن أجرى تجارب لم تصب نجاحا كبيرا آنذاك على دهانات لجعل الطائرات المغيرة غير مرئية راداريا، كما ان تلك المادة تم استخدامها في مناظير الغواصات الالمانية النازية للحؤول دون تمكن الرادارات البريطانية من كشفها عند صعودها الى سطح الماء. وقد ظهرت اولى المواد الماصة للرادار الى العلن لاول مرة في عام 1982، عندما تقدمت السفارة الامريكية في طوكيو باليابان بطلب غريب من شركة TDKاليابانية وكذلك الاخرى NECالشهيرتين بصنع المعدات الالكتروني، وهو شراء صفيحة دهان تبين فيما بعد انها طورت لوقف رشح وتسريب الافران المنزلية العاملة بالموجات الصغرية المايكرويف MICROWAVES وهى تحتوي على صفائح مصنوعة من حبات او قشور لاكاسيد الحديد، وكانت تلك العينة لها اهمية بالغة بالنسبة للباحثين الاميركيين الذين كانوا يجرون أبحاثا حول صنع دهانات وأغلفة ماصة للاشعاع الراداري واستخدامها في الطائرات، لكن بعد ذلك تم الاعتماد على مادة اخرى أخف وزنا وأكثر فعالية.

وأمريكا والبديلة الجديدة للاتحاد السوفيتي السابق المتمثلة بروسيا عادتا الى التنافس في تقديم الاسلحة المتطورة كما في السابق، وان كان حظ روسيا هذه المرة أفضل، لكن المعارك هي خير دليل على نجاح السلاح فمن الناحية التجارية، فعلى الجانب التكنولوجي تميزت مقاتلة ‹السوخوي ‹Su-27 ومشتقاتها su-35/37/30MK/33K بكونها أخصب تصميم لطائرة مقاتلة من حيث امكانية تطورها ونموها، والسوخوي أو Su-27هى مقاتلة اعتراضية بعيدة المدى للقتال الجوي الصرف، وهي ذات مدى غير اعتيادي لمقاتلة تحمل جميع وقودها داخل البدن مثل.F-22 .

أيقنت القيادة التابعة لسلاح الجو الروسي أهمية المقاتلات القاذفة ذات المديات الطويلة والقدرات الادائية المتفوقة، مع خاصية التنوع في الحمولة التسليحية، وكان من نتاج ذلك المقاتلة القاذفة سوخوي34-Su ، بحيث بنيت على اساس المقاتلة الاصلية-Su 27، ولكن مع مقدمة جديدة وغريبة، أخذت شكلا مسطحا يعطي انطباعا بتمتع المقاتلة الجديدة بخاصية الخفاء الجزئي ويمكن لمقاتلة Su-34 حمل 8 اطنان من الاسلحة المتنوعة (صواريخ جو .جو بعيدة وقصيرة المدى، صواريخ وقنابل موجهة جو .أرض) مع

رادار ذي مسح الكتروني ورادار آخر مثبت في الجذع الخلفي الممتد، والخاص بالرؤية الخلفية للكشف واطلاق الصواريخ من نوع جو جو، اما ما يميز تلك المقاتلة القاذفة فهو في اعتمادها مبدأ الخفاء الالكتروني، وهو يتم بواسطة مولدات محمولة في الطائرة تستخدم البلازما (مادة عالية التأين) بحيث يقوم الغاز المؤين حول الطائرة بامتصاص موجات الرادار، وبالتالي حجب الطائرة عنه، الا ان له عيبا وهو ان الطائرة لا تتمكن من ارسال/ استقبال اي اتصال لاسلكي بسبب الحجب الالكتروني ذاك، لذلك فكر الروس في تقنية أخرى أكثر ثورية.

وظلت تكنولوجيا الخفاء أحد أعمدة القوة العسكرية الأميركية في مجال الحرب التكنولوجية المتطورة على مدى العقود الثلاثة الماضية، بيد أنه مع ظهور مقاتلة السوخوي تي — 50 في معرض موسكو الجوي الذي اقيم في الأسبوع الماضي، قد يعفى عليها الزمن. وتكنولوجيا الخفاء التي تتيح حاليا للطائرات الأميركية أمثال إف ـ 22 والقاذفة العملاقة بي — 2 قدرات لا مثيل لها في التسلل من دون رصدها من قبل رادارات العدو، قد لا تتمكن بعد سنوات قليلة من ذلك بسبب ظهور تكنولوجيا مضادة لها تتمثل في أنظمة استشعار ورادارات بطاريات الصواريخ سام الحديثة وكذلك رادارات المسح الإلكتروني المثبتة على كل من حواف أجنحة طائرتي سوخوي إس يو ـ 35 وتي ـ 50 الحديثتين والأخيرة من الجيل الخامس تم اعتماد تكنولوجيا النانو في طلائها مما أكسبها قدرة ليس على الخفاء وحسب، بل والتحكم في انسيابية الهواء على سطوحها بسلاسة تعمل على خفض معدل استهلاكها للوقود، الأمر الذي يمنحها مدى أطول من نظيرتها الأمريكية الإف — 22.

بالطبع لم يقف الأميركيون مكتوفي الأيدي إزاء هذا الخرق الروسي، فهناك فرصة بالنسبة لهم للاستمرار في الاعتماد على تكنولوجيا الخفاء، خاصة مع تطوير المقاتلة إف ـ 35 الحالية، التي لم تدخل الى الخدمة حتى الآن نظرا لتأخر طرأ على برنامج تطويرها المكلف؛ والتي يعتمد على تفوقها في أنظمة الاستشعار واستخدام الكمبيوتر الخاص برادارها العتيد. ويمكن لذلك الرادار نظريا أن يستخدم للتشويش كما الرصد على رادارات العدو مهما بلغت من قوة، وتسريب برامج مدمرة في نظام السيطرة الخاص بها، مما قد يتسبب في شلل تام للعدو، الأمر الذي يسهل تدميره.

وما هو احدث اجهزة الاستشعار والاجهزة الالكترونية القابلة للارتداد والتي تصبح جزء من عالمنا حتى اننا نلحظ وجودها،فانت تمشي في غرفة تتحرك كل اجزائها وتتفاعل معك وفق اوامرك.هذه النوعية من التقدم التقني قد تقضي على الانترنت او تضعف من اهميته إلى حققها على الاقل.

## التوازن الإلكتروني والدفاعي

إن سعي الدول إلى حيازة أسلحة للهجوم أو الردع النووي يصبح بلا معنًى، إذ ان التطور المثير سيفرض على الدول التحول باتجاه الاستثمار في صناعة المعلومات بكل تقنياتها فائقة الحداثة والتطور، بدلاً من أن تستثمر في برامج مكلفة للغاية لتطوير طاقاتها النووية العسكرية من دون أن تتوافر فرصة حقيقية لاستخدامها بصورة فعلية. وعلى صعيد آخر، فإن ماسيتحقق من تحولات بعيدة المدى بفعل هذه الثورة من شأنه أن ينقل قريباً علاقات توازن القوى، خاصة بين الدول الكبرى، من مرحلة التوازن الاستراتيجي العسكري إلى مرحلة التوازن الاستراتيجي المعلوماتي. وهو تحول سوف تكون له دلالات وانعكاسات على كل ما يتعلق بحماية الأمن

القومي للدول .وهكذا، فإن تقويم ما تحويه ترسانات الدول من الأسلحة سيكون على اساس ما تضمّه من أسلحة معلوماتية متنوعة ومتطورة .ومثل هذا التقويم سيكون أمراً صعباً نظراً إلى الطبيعة الغامضة للكثير من هذه الأسلحة ولمنظومة الوسائط المتعدّدة المستخدمة في تمكينها من اختراق أهدافها وتدميرها.

وسيترتب على ذلك، ارتفاع هامش الخطأ المحتمل في عمليات الحساب والتقويم .كما سيتفرّع عنه أن أي محاولة لفرز نوعيات هذه الأسلحة المعلوماتية، وتصنيفها على أساس ما هو دفاعي، أو ما هو هجومي منها، قد تكون أمراً متعذراً أيضاً .ومعنى أن الأسس التي تقوم عليها حسابات هذا النوع من أسلحة حروب المعلومات تفتقر إلى الدقة والموضوعية .وهو ما قد يقود في النهاية إلى استنتاجات مضلّلة .وتلك هي إحدى أخطر معضلات التعامل مع حروب المعلومات، التي تجعلها مختلفة عن الحروب الأخرى، بما فيها الحروب النووية نفسها. وبالنظر إلى الطبيعة التقنية الفائقة، وتطور الحروب المعلوماتية، فإن الوضع الراهن صار يحتم إعادة النظر في نوعية المهمات المسندة إلى المؤسسات العسكرية بمستواها الحالي من الإمكانات والقدرات .

بعبارة أخرى، يجب أن يُترَك التخطيط لحروب المعلومات لكوادر ومؤسسات تكون أقدر على الوفاء بمتطلبات هذا العمل الأمني القومي الحساس، وليس لمؤسسات عسكرية فقط تحكمها مفاهيم وعقائد وتقاليد قتالية بعيدة تماماً عما نتحدث عنه هنا. كما أن إسناد مهمات التعامل مع حروب المعلومات، بتقنياتها المعقدة، إلى كوادر ومؤسسات مؤهلة ومتخصصة ومدرّبة لن يكون أمراً سهلاً، وذلك من واقع أن مرحلة التحول بكل تبعاتها سوف تستغرق الكثير من الوقت .وكذلك فإن تصميم بنية معلوماتية فائقة التطور سيكلف الكثير من الموارد والطاقات القومية .ولا بد أن يستند مثل هذا التحول الجذري الشامل إلى ثقافة مجتمعية ومعرفية متطورة تحفز على هذا التغيير وتسانده وتدعمه. استراتيجيات الدفاع من الواجب أخذ الحقائق التالية في الاعتبار لدى تصميم

استراتيجيات فعّالة للدفاع ضد الحروب المعلوماتية: أولاً :إن قدرة أي دولة، مهما كان مستوى تطورها المعلوماتي، على مواجهة المخاطر، التي تسببها الحروب المعلوماتية، تخرج عن حدود الواقع والممكن، ويترتب على ذلك أن أقصى ما يمكن للدولة أن تفعله هو أن تزيد بدرجة ما من قدرتها على الدفاع والردع للحدّ من التهديد المعلوماتي الذي يشمل مداه العديد من المحاور، لكي تُبقي هذا التهديد ضمن حدود يمكن تحملها .وربما يزيد من صعوبة تلك المهمة أن الهجوم على نظم المعلومات وقواعدها في الدولة الخصم قد يصل في شموله إلى مستوى التهديد الاستراتيجي، وهو الأشد فتكاً، وتصعب مقاومته . وسيفضي أي هجوم معلوماتي شامل إلى نتائج كارثية .

ومن أضراره الهبوط بمستوى الأداء العسكري، وشلّ السياسة الخارجية للدولة عن سعيها إلى تدارك الكارثة، وذلك غير ما يتسبب به من دمارين اقتصادي ومعنوي، وانعدام ثقة المجتمع بالحكومة المسؤولة عنه.

ثانياً :يصبح خطر الحرب المعلوماتية أكثر فتكاً بقدرات الخصم في غياب المؤشرات الدالة إلى أنه في طريقه إلى الحدوث .وإذا كانت هذه هي الطبيعة المميزة للحرب المعلوماتية( كحرب مباغتة وغامضة وربما مجهولة المصدر والاتجاه)، فإن الدفاع ضدها سواء كانت شاملة أو محدودة، يفرض على الدول التي تحس بخطرها أن تكون على أعلى درجة من الحيطة والحذر المستمر تحّسباً للأسوأ.

ثالثاً :الأطراف التي يقع عليها عبء الدفاع في حروب المعلومات، باحتمالاتها اللامحدودة،ستكون في الموقف الأصعب نسبياً بالمقارنة مع ما يمكن أن يكون عليه موقف المهاجمين، فهؤلاء يمكنهم الإمساك دائماً بزمام المبادرة، خاصة في كل ما يتعلق بتحديد توقيت الهجوم ومكانه وآلياته وأسلوب تنفيذه .وبالنسبة إلى الأطراف المدافعة، فسيكون من الصعب عليها تطوير دفاعاتها، والتحول عن سيناريوهاتها إلى أخرى مختلفة .كما لن يكون هيناً بالنسبة إليها تغطية كل نقاط الانكشاف في مختلف أجهزتها ومؤسساتها، بما يضمن إغلاقها بإحكام

في وجه محاولات اختراقها. وسيترتب على وجود هذه الفجوة التكنولوجية بين المهاجمين والمدافعين أن التخطيط لاستراتيجيات الدفاع ونظمه في حروب المعلومات المقبلة يجب أن

يكون مستمراً حتى تتوافر للدولة جاهزية أعلى للرد على أي هجوم معلوماتي تتعرض له.

رابعاً :يجب أن يشمل توزيع الدولة لمهمات الدفاع في حروب المعلومات القطاعين الحكومي والخاص .ويعني ذلك أن ثمة مناطق يحتم الدفاع عنها أن يكون مس ؤولية الحكومات وحدها .وبالمستوى نفسه، ستكون هناك مناطق أخرى يتولاها القطاع غير

**الحكومي، خاصة إذا كانت بعض أجهزته ومؤسساته تزاول أنشطة فائقة الأهمية بالنسبة إلى الأمن القومي.**

**وعلى الرغم من أهمية ماسبق، فالموقف قد يقتضي الذهاب إلى أبعد من ذلك، وإعادة النظر في الكثير من النظم التشريعية الحالية الموروثة من مرحلة ما قبل عصر المعلومات وثورة الاتصالات .ويتوقع أن تكون المهمة العاجلة لهذه النظم الجديدة التوصل إلى منظومات مختلفة من المعايير القادرة على توفير الحماية المناسبة لأمن المعلومات، وتحصين الخدمات المعلوماتية على اختلاف مواقع الأطراف المشاركة فيها أو المتعاملة معها .وباختصار، فإن الهدف النهائي هو إيجاد بيئة معلوماتية محصنة بكل الوسائل والآليات الفعّالة. العالم يقف أمام مشكلة تتفاقم بحدة لم يسبق لها مثيل . وتبدو فظاعة المشكلة أكثر وضوحاً في ظل عدم وجود ملاذات آمنة يمكن الاحتماء بها في مواجهة الهجمات المباغتة والمدمرة للحروب المعلوماتية.**

**ولعل مما يزيد من مؤشرات الخطر الداهم، هو ما نشهده من تطور متسارع في مجال تكنولوجيا المعلومات، مقروناً بالتوسع المستمر في كل مكان في تطبيقها في جميع المجالات المتصلة بأمور الدفاع والتخطيط الاستراتيجي،ونظم التسليح، ومحطات إنتاج الطاقة، والمفاعلات النووية، وتشغيل المطارات، والقواعد الجوية، ووسائل النقل، ومراكز القيادة والسيطرة والاتصال، ومراكز الأبحاث، ومؤس سات الصناعة والإنتاج وتقديم الخدمات، والمعاهد التعليمية والجامعات، فضلاً عن الشبكات الدولية للمعلومات، وغيرها. ومع كل هذه الاستخدامات والتقاطعات المتشابكة بين كل تلك المواقع والخطوط، فلا بد أن تتزايد مخاطر الانكشاف والتعرض للاختراق بصورة تبعث على الخوف مما يمكن أن يحمله المستقبل من محن.و أكثر ما يكشف عنه هذا التطور المثير في طبيعة حروب المستقبل المحتملة وصراعاته، هو الحاجة الماسة إلى طبقة جديدة من الجنرالات الجدد الذين لا ينتمون، بطبيعة تكوينهم وتأهيلهم وثقافتهم، إلى سلك العسكريين المحترفين،بل يكونون من سلك مختلف من المبدعين والمبتكرين الذين يعيشون المستقبل أكثر مما يعيشون الماضي أو الحاضر، ويخططون لحروب مقبلة، هجوماً ودفاعاً، بسيناريوهات لم يسبقهم إليها أحد في التاريخ.**

## الجيوش الإلكترونية

على الرغم من استطاعة مجموعة من الأشخاص المحترفين والمتمرّسين والمزودين بالمتطلبات الأساسية استهداف بعض القطاعات التي تستهدفها أي حرب إلكترونية وتحقيق بعض الجوانب التي تحققها الحروب الإلكترونية أيضا، إلا أنّ الفارق كبير بين الحالتين. فمجال الحرب الإلكترونية أوسع من أن يتولاه بضعة أشخاص والقطاعات المستهدفة أكبر والأضرار الناجمة أضخم والقدرات المستخدمة هائلة، وهي لا تتاح إلا لدول لديها القدرة والقابلية على استثمار مواردها في هذا الإطار واستخدامها في هذا المجال.

وإدراكا منها لهذا الواقع، تنشط العديد من الدول ولا سيما الصين وروسيا والولايات المتّحدة الأمريكية وفرنسا وانجلترا وإسرائيل والهند وباكستان وكوريا الشمالية وإيران بصورة صامتة لتطوير قدراتها في الحرب الإلكترونية وبناء جيوش من الخبراء الذين قد يشكّلون مستقبلا نواة الجيش الإلكتروني للدولة.

ولأنه ليس هناك قانون يحكم عمل أو يحدد إطار الحرب الإلكترونية في الفضاء الإلكتروني، فان الأعمال الهجومية والدفاعية التي تتم فيه إنما تعكس شخصية وصفات النظام الاستخباراتي القائم في ذلك البلد وتوجهاته العامة.

فالألمان على سبيل المثال يتمتعون بقدرات عالية ومتطورة، ولكنها مقيّدة ويتم كبحها بدافع ذاتي خاصة في الأعمال السريّة. أمّا الروس والصينيين، فهم ليسوا كذلك على الإطلاق وهناك نزعة هجومية واضحة في عملهم، وتنسب إليهم معظم الهجمات التي تتم اليوم في الفضاء الإلكتروني من خلال تنظيمهم آلاف الهجمات على مواقع أجنبية كل عام. فقد كانت الشكوك تحوم حول الروس في أشهر حالتين معروفتين في هجمات استونيا ربيع 2007 وجورجيا صيف 2008. أمّا الصينيين فقد شنوا العديد من الهجمات الشرسة المعروفة حتى اليوم في مجال التجسس لعل أهمّها محاولات اختراق البنتاجون في 2007.

أولا: تطوير الاستعدادات الهجومية:على الرغم من أنّ معظم الدول تعمل حثيثا على تطوير قدراتها الهجومية في المجال الإلكتروني، إلا أن الصين وروسيا تعتبر الدول الأبرز في هذا المجال لدوافع ومبررات مختلفة.

1- الصين: وتعتبر من أكثر الدول التي تعمل على تطوير قدراتها الهجومية في المجال الإلكتروني، وهي واحدة من الدول القليلة التي تدمج فعلا مفهوم "الثورة في الشؤون العسكرية" (RMA) في صلب العقيدة العسكرية، وخاصة في مجال الحروب الإلكترونية. وتؤكد الورقة الصينية البيضاء عن "الدفاع القومي" لعام 2006 على أنّ

**الهدف الرئيسي من بناء جيش حديث، هو جعله قادرا على الفوز في حروب المعلوماتية بحلول منتصف القرن الواحد والعشرين. وهو الأمر الذي أعادت تأكيده عام 2009.**

**ولأن الصين ليست على المستوى العسكري لأمريكا وروسيا، فهي تحاول على الأرجح استغلال البُعد الإلكتروني لتطوير قدراتها "اللاتناظرية" لتحقيق تفوق في هذا المجال وبالتالي ضمان قدرات ردعيّة تتيح لها توفير الوقت اللازم لبناء قدراتها التقليدية من جهة، وتتيح لها أيضا استكشاف نقاط ضعف خصومها في المجال الإلكتروني للتركيز عليها.**

**2- روسيا: وتتبنى كما الصين تطوير قدراتها في الحرب الإلكترونية لاسيما في الشق الهجومي، واتهمت بأنها تقف وراء العديد من الحالات المشهورة من دون أن يكون هناك دليل مادي قوي على ذلك. لكن الواضح أنّ روسيا ومنذ انهيار الاتحاد السوفيتي تعتمد على وسائل أقل تكلفة وأكثر فاعلية في مواجهة الولايات المتّحدة وحلف شمال الأطلسي. إذ تعتبر القدرات اللاتناظرية ومن ضمنها الحرب الإلكترونية إحدى أهم وسائل المواجهة في ظل التفوق العسكري للناتو وواشنطن.**

**ثانيا: تطوير الاستعدادات الدفاعية: ولأنّ الدولة الأكثر اعتماداعلى الشبكات والمعلوماتية تعتبر الأكثر عرضة في المقابل للنتائج الكارثية لأي حرب إلكترونية تشن على مستوى عالي ودقيق. ولأن الأفضلية في الحروب الإلكترونية هي للمهاجم عادة وليس للمتحصّن، ولان ميدان حروب المعلومات هو ميدان لا تناظري، تعكف العديد من الدول على تطوير قدراتها الدفاعية إلى جانب امتلاكها قدرات هجومية متطورة، ومنها:**

**1- انجلترا: وقامت على سبيل المثال بإصدار إستراتيجية الأمن الإلكتروني القومية في يونيو 2009، كما قامت بإنشاء وحدة الأمن الإلكتروني ومركز العمليات ومقرّه وكالة الاستخبارات القومية (GCHQ)، وبدأت وظيفتها عمليا في مارس 2010.**

**2- حلف شمال الأطلسي (ناتو): وكذلك ناقش الحلف الشكل والحد الذي يمكن عنده اعتبار الهجمات الإلكترونية بمثابة إعلان حرب أو شكل من أشكال الاعتداء العسكري الذي يفرض على الدول الأعضاء الالتزام بتقديم المساعدة والدفاع عن الحليف الذي يتعرّض لذلك الهجوم. وقد ذكر تقرير الناتو الصادر في مايو 2010 والمعد لبلورة مفهوم جديد ودور جديد للحلف عام 2020 أنّ هناك ضرورة لتكثيف الجهود وتعزيز قدرات الرد على الهجمات الإلكترونية التي تترك مخاطر متزايدة على أن تتضمن مساعدة الحلفاء على تطوير قدرات دفاعية تضمن الردع المناسب.**

**3- الولايات المتّحدة: وعلى الرغم من أنّها تبقى الدولة الأكثر امتلاكا للقدرات والتقنيات الهجومية العالية المطلوبة في الحروب الإلكترونية، إلا انّه من الواضح أنّ اهتمامها ينصبّ مؤخرا على تعزيز القدرات الدفاعية في هذا المجال. ونظرا لأنها الدولة الأكثر**

**اعتمادا في العالم على الإنترنت وعلى الشبكات في مختلف القطاعات المدنية والعسكرية تبدو الأكثر اهتماما بالجانب الدفاعي فيما يتعلق بالحروب الإلكترونية مقارنة بالدول الأخرى.**

**وفي مايو 2009، صدّق البيت الأبيض على وثيقة "مراجعة سياسة الفضاء الإلكتروني" التي تمّ تقديمها من قبل لجنة خاصة إلى الرئيس الأمريكي أوباما، وهي تلخّص الخطوات التي يجب على الولايات المتّحدة اتّباعها في مجال البدء بتفعيل الأمن الإلكتروني ومتطلّباته الأوّلية الأساسية.**

**وفي 26 أبريل 2010كشفت وكالة الاستخبارات المركزية الأمريكية (CIA) عن مبادرة جديدة لمحاربة الهجمات الإلكترونية، وضعت من خلالها العناوين العريضة للخطط المناسبة لخمس سنوات قادمة.**

**كما قامت الولايات المتّحدة في مايو 2010 بإنشاء قيادة الإنترنت "سايبركوم" وعيّنت مدير وكالة الاستخبارات القوميّة الجنرال كيث أليكساندر قائدا عليها مهمته الحرص على حماية الشبكات العسكرية الأمريكية على الدوام. وقد بدأت هذه القيادة العمل فعلا بعد أن كان قد تمّ الإعلان عن ضرورة إنشائها في عهد الرئيس اوباما في العام 2009، وهي تضم اكثر من 1000 فرد من نخبة القراصنة والجواسيس الإلكترونيين المحترفين والمميزين يعملون تحت إمرة الجنرال أليكسنادر، علما أنّ بعض التقديرات تشير إلى أنّ الولايات المتّحدة بحاجة إلى قوة قوامها حوالي 20 ألف إلى 30 ألف فرد بنفس المميزات والصفات حتى تضمن تنفيذ المهام الدفاعية الإلكترونية على أكمل وجه في حماية الولايات المتّحدة بأسرها.**

**وفي 25 سبتمبر 2010، أكدت إيران أن العديد من وحداتها الصناعية وقعت ضحيت إرهاب إلكتروني بعد إصابتها بفيروس "ستكسنت" ويعد هذا الفيروس وفق العديد من التقارير التي صدرت مؤخرا واحد من أعقد الأدوات التي تم استخدامها. فـ"ستكسنت" عبارة عن برنامج كومبيوتر خبيث يهاجم أنظمة التحكم الصناعية المستخدمة على نطاق واسع في مراقبة الوحدات التي تعمل آليا. وكان الخبراء بداية يعتقدون أنّ مهمّة البرنامج هي التجسس الصناعي ونقل المعلومات التي تساعد على تقليد المنتجات.**

**لكن تبيّن لخبراء الهندسة العكسيّة فيما بعد أنّ الأمر مختلف كليّا. فالبرنامج -وعلى عكس الكثير من البرامج المعروفة - ليس مخصصا للتجسس وسرقة المعلومات الصناعية لمحاولة كسب المال أو لسرقة الملكية الفكرية. فبعد حوالي أربعة أشهر من العمل، ظهر أن الأمر أكثر تعقيدا مما كان متصورا، وأننا نقف أمام نوع جديد من البرامج التي من الممكن أن تتحول إلى نموذج للأطراف التي تنوي إطلاق هجمات إلكترونية تؤدي إلى دمار حقيقي واقعي في البلد المستهدف حتى دون الحاجة إلى الإنترنت.**

فالبرنامج لا يعمل بشكل عشوائي كما هي العادة وإنما بشكل محدد جدا. إذ يقوم بعد اختراق الأجهزة والحواسيب بالتفتيش عن علامة فارقة تتعلق بأنظمة صنعتها شركة "سيمنز الألمانية"، فإذا ما وجدها يقوم عندها بتفعيل نفسه ويبدأ بالعمل على تخريب وتدمير المنشأة المستهدفة من خلال العبث بأنظمة التحكم وقد تتعدد المنشآت التي يستطيع مهاجمتها من خطوط نقل النفط إلى محطات توليد الكهرباء وحتى المفاعلات النووية وغيرها من المنشآت الإستراتيجية الحسّاسة، وإذا لم يجدها، فيترك الحاسوب وشأنه.

البرنامج كبير ومشفّر جدا ومعقد جدا ويوظّف تقنيات ذكية وجديدة، ولا يلزمه للعمل أي تدخل بشري في أي مرحلة من المراحل، ويكفي أن يكون هناك بطاقة ذاكرة تخزين إلكترونية مصابة به حتى يبدأ عمله.

ولأنه على هذه الدرجة من التعقيد والتطور ولأنّه يعمل بشكل محدد جدا، فمن البديهي أن يكون من صنع دولة، ومن البديهي أن تكون المنشأة أو المنشآت الأساسية التي يبحث عنها لتدميرها أو تخريبها قيّمة للغاية وعلى درجة عالية من الأهمية. وبناء على هذا الاستنتاج، ذهبت العديد من المصادر إلى التخمين بأنّ مفاعل بوشهر الإيراني قد يكون الهدف الأساسي الذي يبحث البرنامج عنه لتدميره.

ففي دراسة لها، أشارت شركة "سيمناتيك" التي تعمل في مجال برامج الأمن الإلكتروني والبرامج المضادة للفيروسات أنّ إيران تأتي في طليعة الدول المستهدفة من ناحية الإصابات التي حققها برنامج "ستكسنت" وأنّ ما يقارب 60% من أجهزة الكمبيوتر التي تعرضت لهجوم من هذا التطبيق الخبيث كانت في إيران.

وعلى الرغم من أنّ إيران نفت عبر مدير مشروع بوشهر محمود جعفري أن يكون الفيروس قد أصاب المفاعل أو تسبب في أي ضرر في أنظمة التحكم فيه، إلا أنها كانت قد أقرت إصابة بعض الحواسيب الشخصية المحمولة لموظفي المحطة بهذا الفيروس إضافة إلى إصابته أكثر من 30 ألف نظام حاسوبي لمنشآت صناعية متعددة داخل إيران.

وهناك عدد من الخبراء يعتقد بالفعل أنّ هدف الفيروس الأساسي قد يكون مفاعل بوشهر، وأنّ الفيروس قد حقق هدفه من التخريب بدليل أنّ إيران أعلنت أنها ستؤجّل العمل في المفاعل عدّة أشهر حتى بداية عام 2011، في وقت يرى فيه آخرون أنّ الهدف هو منشأة ناتانز لتخصيب اليورانيوم بدليل أنّ المنشأة عانت مشكلة ظلّت طي الكتمان وأدت إلى انخفاض أجهزة الطرد المركزية القادرة على العمل بنسبة 15% فجأة وذلك في نفس الفترة التي ظهر فيها الفيروس لأول مرّة.

وبالرغم من أنّه قد تمّ اكتشاف "ستكسنت" لأول مرة من قبل شركة بيلاروسية تدعى VirusBlockAda قالت أنها عثرت على التطبيق الخبيث في جهاز كمبيوتر يعود

لأحد عملائها الإيرانيين، إلاّ أنّ أصابع الاتهام لم تتّجه إليها، وتمّ إطلاق العديد من التخمينات حول الجهة التي قد تكون أطلقت هذا الهجوم بالفعل، ومنها:

1- روسيا: على اعتبار أنّه سبق وان كانت موضوع شبهة في أكبر هجومين وقعا حتى فترة ما قبل "ستكسنت" في استونيا وجورجيا. وفي حالة إيران، فالإيرانيين استخدموا الروس لتركيب أنظمة سيمينز الألمانية، والعلماء الروس كانوا الجهة الأجنبية الوحيدة المسؤولة عن بوشهر والمخولة أيضا الدخول إلى كافّة الأنظمة، وعليه فالروس يعلمون جيدا مكمن الضعف، ومن الممكن جدا لأسباب مختلفة أن يكونوا الجهة التي أدخلت الفيروس عبر استخدام بطاقة ذاكرة مصابة. وتشير بعض التقارير الاستخباراتية الصادرة مؤخرا إلى أنّ عددا من العلماء والتقنيين الروس المشاركين في مشروع بوشهر بدؤوا في مغادرة إيران خوفا من اعتقالهم واستجوابهم خاصة بعدما تمّ احتجاز بعض من زملائهم لاستجوابهم من قبل السلطات الإيرانية.

2-الصين: وفي المقابل، يشير عدد من خبراء الأمن الإلكتروني إلى أنّ الصين قد تكون المصدر المحتمل للفيروس، وانّ الهدف المقصود منه كان الهند وليس إيران مستندين في ذلك إلى أنّ الهند وحتى نهاية سبتمبر 2010 تعد الدولة الأكثر تعرّضا للفيروس وفقا لإحصاءاتهم، وهي وتأتي في المرتبة الأولى من حيث عدد الحواسيب المصابة بالفيروس متخطّية كل من إيران وإندونيسيا وبواقع 60 ألف جهاز. وذلك في سياق التوتر الذي تشهده العلاقة بين البلدين على خلفية نزاعات حدودية وسياسية متزايدة مؤخرا.

3-أمريكا: ولا تستبعد جهات أخرى أن تكون الولايات المتّحدة الدولة المصنّعة للفيروس نظرا لتعقيده وتطوره ولما يحتاجه من خبرات وموارد هائلة. ويربط البعض بين هذا الفيروس وبين النزاع الأمريكي-الإيراني حول الملف النووية، وأنّ الهدف منه هو تخريب المجهود النووي الإيراني خاصّة أنّ الرئيس جورج بوش الابن كان قد سمح -وفقا لتقارير صحفية نقلا عن مسؤولين حكوميين- بإطلاق جهود تتضمن العديد من الخطوات التي تهدف إلى تخريب البرنامج النووي الإيراني من خلال استهداف أنظمة الحواسيب والكهرباء والشبكات وكل ما يخدم البرنامج النووي الإيراني. ووفقا لأصحاب هذا التصوّر، فقد استكمل الرئيس أوباما هذا المجهود فيما بعد، خاصّة أنّ عملية تخصيب اليورانيوم كانت قد عانت مصاعب تقنية كبيرة.وما زال من غير المعروف إذا ما كان السبب هو العقوبات الاقتصادية أم التصنيع الرديء أم عمليات التخريب الأمريكية.

4- ومع ذلك تبقى إسرائيل وفق كثير من الخبراء والمتخصصين المرشح الأكثر احتمالا كمصدر لفيروس "ستكسنت".

وفي أواخر التسعينات نجح خبير في مجال الحواسيب يعمل في جهاز الأمن الداخلي الإسرائيلي (شين بيت) من خلال تقنيات القرصنة في اقتحام نظام الكمبيوتر الخاص

بمستودع (بي جالوت) للوقود شمالي تل أبيب. كان الهدف إجراء اختبار روتيني لتدابير الحماية بالموقع الاستراتيجي، لكن هذه العملية نبهت الإسرائيليين أيضا إلى الإمكانية التي توفرها هذه التسللات عالية التقنية للقيام بأعمال تخريبية حقيقية، وأدركوا حينها أنه بخلاف الاطلاع على البيانات السرية، فإنهم يستطيعون أيضا تنفيذ تفجيرات متعمدة بمجرد برمجة تغيير في مسار خطوط الأنابيب".

ومنذ ذلك الوقت تبلورت الحرب الإلكترونية شيئا فشيئا لتصبح ركنا رئيسيا في التخطيط الاستراتيجي لإسرائيل. وتعتبر الوحدة 8200 في الجيش الإسرائيلي أكثر الوحدات تطورا من الناحية التقنية والتكنولوجية ولها نشاطات واسعة في حروب الإنترنت والشبكات، وقد انضم إليها الآلاف من العقول الإسرائيلية منذ إنشائها نظرا لشهرتها الواسعة حيث تعمل على ضمان التفوق النوعي لإسرائيل من خلال عمليات دفاعية أو هجومية في الفضاء الإلكتروني.

وعلى الرغم من أنّه قد تمّ تصنيف الوحدة 8200 من قبل بعض المؤسسات المعنيّة بأنها أكبر سادس مطلق لهجمات الإنترنت في العالم، فان هذه الوحدة ليست الوحيدة التي تتمتع بهذه القدرات التقنية العالية في إسرائيل، فهناك العديد من الوحدات الأخرى التي تتمتع بقدرات متطورة جدا في مجال تكنولوجيا المعلومات في جميع التخصصات. ويتم استقطاب وتجنيد الأطفال الإسرائيليين من النخبة حتى قبل إنهائهم دراستهم الثانوية، عندما يبلغ هؤلاء سن الـ25 عاما، يكون لديهم أكثر من 7 سنوات خبرة عملية في مجال التكنولوجيا.

ولا يقتصر الأمر على الجيش الإسرائيلي في توظيف الأدمغة وبناء قدرات عالية في مجال الحروب الإلكترونية وإنشاء وحدات قوات نخبة خاصة كوماندوس بحروب الإنترنت وتكون مهمتها التعامل مع أصعب وأخطر وأعقد الحالات المتعلقة بهذه الحروب، وإنما تدخل الاستخبارات الشين بيت على الخط أيضا للقيام بنفس المهمة، ويتم الاستفادة في هذا الإطار من العناصر المخضرمة أيضا، ومن المؤسسات التقنية والمعلوماتية الإسرائيلية ومن العاملين فيها كرافد مهم.

وتتجه أصابع الاتهام إلى إسرائيل فيما يتعلق بفيروس "ستكسنت" اعتمادا على عدد من المؤشرات منها,توافر القدرات التقنية اللازمة للقيام بمثل ذلك العمل,وتعقيدات العمل العسكري التقليدي وتردد الأمريكيين في الدخول بحرب جديدة أو السماح لإسرائيل بفعل ذلك,وتوافر سوابق لإسرائيل في هذا المجال، لعلّ أبرزها كما يقول الصحافي في مجلة "جينز ديفنس"، طوني سكينر نقلا عن مصادر إسرائيلية، أن قصف إسرائيل العام 2007 لمفاعل نووي مزعوم في سوريا، كان مسبوقا بهجوم إلكتروني عطّل الرادارات الأرضية والراجمات المضادة للطيران.

**لكن الأهم من كل ما تمّ ذكره أعلاه والمثير للاهتمام في نفس الوقت في الموضوع أنّ رئيس شعبة المخابرات العسكرية الإسرائيلية الميجر جنرال "عاموس يادلين" كان قد كشف في خطوة نادرة أنّ مجال الحرب الإلكترونية يناسب تماماً عقيدة الدفاع في إسرائيل، وأنّ القوات الإسرائيلية أصبح لديها الوسائل الكافية لإطلاق هجمات إلكترونية استباقية من دون أي مساعدات خارجية، وهي تدرس بهدوء استخدام هذه التقنيات ضدّ الآخرين بهدف التسلل إلى معلومات أو القيام بتخريب من خلال زرع برامج في أنظمة السيطرة والتحكم في المنشآت الحساسة للأعداء في المنطقة مثل إيران. بالاضافة إلى ان إسرائيل توصّلت إلى أنّ نقطة ضعف إيران الكبرى إنما تكمن في معلوماتها المحملة إلكترونيا، وهو ما يتيح استهدافها. وعندما سئل سكوت بورج مدير الوحدة الأمريكية لتبعات الإنترنت "وهي وحدة استشارية تقدم خدماتها في مجال الأمن الإلكتروني لمختلف الوكالات الأمنية الوطنية الأمريكية" عن السيناريو الذي يمكن أن تلجأ إليه إسرائيل لاستهداف إيران، أجاب انه "من الممكن استخدام "البرامج الخبيثة" لإفساد أو تعطيل أو السيطرة على أجهزة التحكم في المواقع الحساسة مثل محطات تخصيب اليورانيوم، وبما أن الأصول النووية لإيران ستكون في الغالب غير متّصلة بالإنترنت، فلن يتسنى للإسرائيليين زرع الفيروس عبر الإنترنت وسيكون عليهم دسه في البرامج التي يستخدمها الإيرانيون أو في أجهزة محمولة يدخلها فنيون دون علم الإيرانيين. ويكفي توافر أي وحدة تخزين بيانات متنقلة ملوثة لإتمام هذه المهمة". وهو سيناريو شبيه بما حصل مؤخرا في إيران. كما يقوم "ستكسنت" عندما يجد هدفه بعرض رقم من ثماني خانات (19790509)، وهو على الأرجح تاريخ 9 مايو 1979. وفقا للأرشيف، فان هذا التاريخ شهد موت حبيب الغانيان، وهو أول إيراني تم إعدامه في إيران بعد الثورة الإسلامية بتهمة التجسس.**

**وعلى الرغم من كل هذه التخمينات فليس هناك من دليل قاطع على الجهة التي قامت بإطلاق هذا الفيروس أو المستهدف الحقيقي، فكل ما هو موجود هو مجرد مؤشرات قد تدل على هذه الدولة.**

## التقدم التقني في الشئون العسكرية

الاستراتيجيات العسكرية الحديثة والثورة في الشؤون العسكرية ونظم القتال المستقبلية ستغير مفاهيم إدارة الصراع وستجعل حروب المستقبل غير تقليدية؛ إذ تؤدي إلى تقليل الحاجة تدريجياً إلى البشر. ونتناول الآن جوانب من التقدم العلمي والتقني في الشؤون العسكرية، وتستعرض ما يجري تطويره في المؤسسات العسكرية والعلمية بالدول المتقدمة من أسلحة ومعدات متقدمة جداً في مجال الروبوتات (الإنسان الآلي) والنانوتكنولوجي (التقنية المتناهية الصغر) والليزر والفضاء والمعلومات والموجات الكهرومغناطيسية والتقنية الحيوية.

والخيال العلمي لعب دوراً مهماً في تحقيق الكثير من الاكتشافات والإنجازات العلمية في عصرنا الحالي، والتي كانت في كثير من جوانبها أحلاماً وخيالات في أذهان الأدباء والعلماء الذين حاولوا بخيالهم الخصب استشراف آفاق المستقبل واقتحام عوالمه المغلقة.

وأدب الخيال العلمي يشكل منطلقاً أساسياً في تكوين صور ذهنية جديدة لدى الأفراد لما ستكون عليه الأشياء في المستقبل, فقراءة الخيال العلمي أمر لازم للمستقبل. وهذا الأدب تم إدخاله في قاعات الدراسة في المدارس والجامعات الأوروبية والأمريكية، وتم أيضاً إنشاء مراكز متخصصة فيه، ومنها مركز لدراسة الخيال العلمي في جامعة كانساس الأمريكية الذي تأسس عام 1982، وأيضاً قسم العلم والخيال العلمي في جامعة جلامورجان البريطانية الذي افتتح عام 1999.فقد أدركت هذه الدول أن كتاب الخيال العلمي يسبقون العلماء دائماً في صياغة الأفكار، بل كثيراً ما تكون قصص الخيال العلمي قادرة على المساهمة في اكتشاف المستقبل والتأثير فيه والتخطيط له، كما أنها قادرة على التنبيه والتحذير من آثار التقنية المستقبلية وأخطارها، وبالتالي التهيؤ والاستعداد لمواجهتها قبل حصولها.

فقد تنبأ كاتب الخيال العلمي البريطاني إتش جي ويلز في راويته (العالم تحرر) التي صدرت عام 1913باكتشاف الطاقة الذرية وتحررها وتطوير القنابل الذرية، كما تنبأ بأسلحة الليزر - التي سماها "أشعة الموت" - بروايته (حرب العوالم) التي صدرت عام 1898.كما أن كاتب الخيال العلمي الأمريكي روبرت هينلين قد تناول في روايته (جيوش سفينة النجوم) الصادرة عام 1959الحديث عن زي روبوتي لجندي المستقبل يظهر فيه الجنود مسلحين بهياكل خارجية تلبي طلباتهم، وهو ما تقوم وكالة مشاريع أبحاث الدفاع المتقدمة "داربا (DARPA) "بإجراء الأبحاث عليه حالياً.

أفلام الخيال العلمي لعبت دوراً مهماً في التنبؤ بتقنيات حروب المستقبل وأسلحتها، حيث يذكر أن مبادرة الدفاع الاستراتيجي التي أعلن عنها الرئيس الأمريكي الأسبق رونالد

ريجان عام 1983، والتي عرفت بين وسائل الإعلام بحرب النجوم، كانت مستمدة من فيلم "حرب النجوم" الذي أنتج عام 1977.كما أن فيلمي "المفترس" الذي أنتج عام 1987و"ماتريكس" الذي أنتج عام 1999قد تناولا الحديث عن زي جندي المستقبل، حيث يظهر البطل في درع مرن، يمكن تحويله بشكل فوري إلى درع خفيف عند الطلب، والذي تجري الأبحاث عليه حالياً في الولايات المتحدة الأمريكية. ولم تخلُ أيضاً أفلام الخيال العلمي من الحديث عن الأسلحة البيولوجية والتنبؤ بأخطارها، مثل "رجل الأوميجا" لعام 1970و"خلية أندروميدا" لعام 1971، المقتبس عن رواية بالاسم نفسه لكاتب الخيال العلمي الأمريكي مايكل كرايتون، و"انفجار" لعام 1995م.

وفيما يتصل بحقل الروبوت (الإنسان الآلي) فإن المخططين العسكريين يعدون هذه التقنية أول صورة من صور حروب المستقبل، وينظرون إليها باهتمام خاص لاستخدامها في الحفاظ على حياة الجنود والقادة في ميدان الحروب. استخدمت القوات الأمريكية في حرب أفغانستان عام 2001الروبوت "باكبوتس"الذي صممته شركة "آي روبوت"الأمريكية خصيصاً للمهمات العسكرية مثل عمليات الاستطلاع ورصد السلاح الكيماوي والتمويه بتغطية المنطقة بالدخان.

ستواجه الدول العربية في القرن الحادي والعشرين تحديات تفرضها تقنيات الحرب الحديثة، خصوصاً أن التقدم العلمي والتكنولوجي أسفر عن فجوة كبيرة بين الدول المتقدمة، التي اهتمت بتنظيم قدراتها العلمية والتكنولوجية وتطويرها وجعلها مكوناً أساسياً لأمنها القومي، وبين الدول النامية المتطلعة إلى تحقيق أمنها بحسب ما تملكه من قدرات وإمكانيات متاحة، مما أدى إلى حدوث صراع شديد نشأ عن احتكار الدول المتقدمة للتكنولوجيا الجديدة المتطورة، بينما تحاول الدول الأقل تقدماً نقل هذه التكنولوجيا، وما يؤدي إليه ذلك من إذعان وتبعية للدول المتقدمة.

ولا شك في أن الثورة العلمية والتكنولوجية قد أحدثت نقلة نوعية في الفكر العسكري المعاصر، إذ قام العديد من الدول بوضع مجموعة من البرامج والخطط بهدف إعادة تنظيم القوات المسلحة، بحيث تغدو قادرة على مواجهة التحديات في القرن الحادي والعشرين. ففي سيناريو حروب القرن لن يكون للأسلحة التقليدية الدور الرئيسي، فمعظم الأسلحة التقليدية وهياكل القوات المسلحة مرشحة للاستبدال والاستغناء عنها مستقبلاً بأعداد صغيرة من الجنود تكون مدربة تدريباً فائقاً، وجاهزيتها عالية، ومزودة بأجيال جديدة ومتطورة من المعدات والأسلحة الفتاكة. إلا أن التطور التكنولوجي الكبير في نظم التسليح وأدوات الحرب، وفي الفكر الاستراتيجي والمذاهب العسكرية تبعاً لذلك، من الصعب أن يشكل نمطاً يمكن احتذاؤه بواسطة جميع الدول، كبيرها وصغيرها، لأن فارق الإمكانيات التكنولوجية والاقتصادية والبشرية المؤهلة لا بد من أن يقف حائلاً دون

ذلك. ولكن التغيرات الحادة في طبيعة الحروب الحديثة وسماتها تفرض ضرورة البحث في الوقت ذاته عن الأساليب المختلفة لمواجهتها، وهو إعداد الدولة المسبق للعديد من الإجراءات لدرء أو تقليل الآثار الناجمة عنها.

وتوظيف الأسلحة الذكية(حروب الفضاء والمقاتل الروبوت الذي يقوم برصد الألغام وحراسة الحدود وشل الطائرات والدبابات). وقد كانت حرب الخليج 1991 أول تطبيق عملي لهذه الحرب، إنها حروب الموجة الثالثة المعتمدة على الذكاء البشري والمعرفة المدمجة في الأسلحة والتي تتراجع امامها الحروب التقليدية التي عرفها الإنسان: حروب الموجة الأولى التي خاضها قبل قرون جنود مسلحون بالسيوف والرماح ومدربون على الالتحام, وحروب الموجة الثانية بجيوشها المسلحة بالدبابات والمدافع والطائرات أي الحروب التي لم نعرف سواها.

المنهج الجديد لإعداد الدولة للحرب الحديثة لا يعني تجاوز المفاهيم التقليدية، وإنما تطوير تلك المفاهيم والإضافة إليها بما يتماشى والتقنيات الحديثة التي تم التوصل إليها في شتى المجالات، وهذا يعني إدخال مفاهيم جديدة على الأسلحة والمعدات الموجودة فعلاً في الخدمة بدلاً من شراء أسلحة ومعدات جديدة للقيام بالمهام المطلوبة، ويعني أيضاً ضرورة الإدراك العام لمدى أهمية التطور التكنولوجي للدولة في إطاره الشامل وما يواكبه من تطور وانعكاسات على المجالات الاستراتيجية العسكرية على وجه الخصوص.

الدول العربية ماتزال تبتاع أسلحة من الدرجة الثانية ولا تنتجها، كما أن بحوث التطوير والتحديث العسكرية العربية لا تزال متأخرة عن التقدم العلمي والتكنولوجي الذي تم إنجازه في الشؤون العسكرية في الدول المتقدمة، إلا أننا ندعو الدول العربية إلى التفكير بجدية في أساليب مواجهة التهديدات التي قد تتعرض لها نتيجة للتطورات العسكرية، والسعي بكل قواها إلى بناء القدرات الذاتية التي تمكنها من تحقيق أمنها القومي، ودون الاعتماد على قوى خارجية، والذي لن يتحقق إلا بتعاون قوي وفعّال بين الدول العربية، ومواكبة الثورات العلمية والتكنولوجية، والاستفادة إلى أقصى حد من الثورة في الشؤون العسكرية المصرية بصفة خاصة.وكذلك ضرورة مضاعفة الجهود لتوليد التكنولوجيا، بمعنى ابتكارها وإنتاجها بدلاً من شرائها واستهلاكها، والاستغلال الأمثل للثروات الطبيعية والبشرية، بما يحقق قدراً من الاكتفاء الذاتي. إن الدول العربية بحاجة ضرورية إلى استراتيجية عسكرية مشتركة لمواجهة حروب القرن، تتعاون من خلالها وتنسق خططها واستراتيجياتها تحقيقاً للتوازن التكنولوجي العسكري، واستعداداً لمجابهة أي أخطار أو تهديدات في الحاضر والمستقبل.

## قواعد وقيادات

استحداث قيادة عسكرية مهمتها الرد على هجمات قراصنة المعلوماتية وتنفيذ عمليات في الفضاء الإلكتروني كان إعلان لوزارة الدفاع الأمريكية في 22 يونيو 2011، وأردف الإعلان أن تلك القيادة دخلت حيز العمل في أكتوبر 2012، ويعكس ذلك تأكيدا على الأهمية القصوى التى تلعبها شبكة الإنترنت فى حياة الشعوب سلما أو حربا ويقدم إنذار بامكانية عسكرة الفضاء الإلكتروني والذي أصبح يتعلق بالبنية التحتية الكونية للمعلومات.

وكان البنتاجون قد أكد أن الأخطار المرتبطة بأمن الفضاء الإلكتروني هي من أخطر التحديات التي يواجهها الاقتصاد والأمن القومي في القرن الحادي والعشرين. وكانت شبكات رقمية عسكرية أمريكية تعرضت لعدد كبير من الهجمات من قبل خبراء معلوماتية موهوبين، صينيين أو روس في الغالب، بحسب تقارير أمريكية عديدة. وجاء قرار البنتاجون بإنشاء تلك القيادة ليمثل طورا جديدا في مجال الحرب الإلكترونية عن طريق الفضاء الإلكتروني، وتم استحداث تلك القيادة للمرة الأولى في تاريخ الولايات المتحدة لتعمل تحت لواء القيادة الاستراتيجية الأمريكية وتباشر عملها من مقر القيادة الجديدة في فورت ميد بولاية ميريلاند. وتستهدف وزارة الدفاع الأمريكية من تلك القيادة الجديدة أن تشرف على مختلف الجهود المتعلقة بالإنترنت في كل أجهزة القوات المسلحة، مع التاكيد أنها لن تصل إلى مستوى عسكرة فضاء الإنترنت. بل إنها تعمل على حماية شبكات الجيش الأمريكي التي تتكون من 15 ألف شبكة ونحو سبعة ملايين جهاز كومبيوتر ,حيث تحاول أكثر من 100 وكالة استخبارات أجنبية دخول الشبكات الأمريكية بشكل غير مشروع ,حيث تتعرض لهجمات مستمرة ويتم محاولة دخولها عدة مرات يوميا ويتم مسحها ملايين المرات يوميا، مع تكرار وتعقيد هذه الهجمات.

ويتراوح هذا التهديد من قراصنة الانترنت من الهواة المراهقين إلى العصابات الإجرامية التي تعمل كمرتزقة إنترنت لحكومات أجنبية، وترصد تقارير أمريكية أن الصين بنت برنامجا متطورا لحرب الإنترنت.

وكان الرئيس باراك أوباما قد أعلن اعتزامه تعيين منسق لشبكات الإنترنت للبيت الأبيض لكي يقوم بتنسيق الجهود الأمريكية من أجل حماية شبكات الكومبيوتر والتعاون الوثيق مع الشركات التي تملك أو تتحكم في الأنظمة المالية والكهربائية وغيرها.

تعد هجمات شبكات الكمبيوتر والتي يطلق عليها حرب الفضاء الإلكتروني جزءاً من عمليات المعلومات والتي يمكن أن يتم استخدامها في مستويات ومراحل الصراع

المختلفة سواء كان ذلك على الجانب التكتيكي أو الاستراتيجي أو العملياتي، ويتم استخدام تلك الهجمات في أي وقت سواء أكان وقت سلم أم حرب أم أزمة.
والحرب الرقمية هي الإجراءات التي يتم اتخاذها للتأثير بشكل سلبي على المعلومات ونظم المعلومات، وفي الوقت نفسه الدفاع عن هذه المعلومات والنظم التي تحتويها. وتوجد طرق عديدة يمكن من خلالها تنفيذ الهجمات عبر الفضاء الإلكتروني، منها الهجمات المباشرة من خلال التدمير الفيزيائي لأجهزة الخصم، أو نقاط الاتصالات الهامة ضمن شبكاته، وذلك باستخدام القوة العسكرية المباشرة.
وهناك أيضا سرقة المعلومات من أجهزة الخصم، ومن ثم اتخاذ قرارات أفضل في المعركة، إضافة إلى تخريب قواعد بيانات الخصم والتلاعب بها، لجعل الخصم يخطئ في اتخاذ القرارات. وبالطبع هناك استخدام الفيروسات والأساليب الإلكترونية مثل هجمات الحرمان من الخدمات للتأثير على مواقع الخصم، مما يؤدي إلى التقليل من مقدرة الخصم على الاتصال وإبطاء قدرته لاتخاذ القرار.
وتتضمن هجمات الكمبيوتر حدوث هجوم على خطوط الاتصالات وتأتي تلك الهجمات من مسافة بعيدة عن مصدر الهجوم وذلك عبر الشبكات الدولية للمعلومات العابرة للحدود ومن خلال موجات الراديو أو الشبكات الدولية للاتصالات بدون تدخل مادي أو طبيعي في الأراضي الخاصة بدولة أخرى أو القيام بغزوة تقليدية.
وعلى الرغم من الاستخدامات الحديثة لهجمات الفضاء الإلكتروني في الصراعات الحديثة في عصر المعلومات إلا انه لم يتم إدماجها بشكل كامل في العقيدة العسكرية للجيوش الحديثة. غير أن هناك جهودا تبذلها بعض القوى الكبرى لتطوير أسلحة الفضاء الإلكتروني لكي يتم استخدامها في حروب القرن، وهو امر سينطوى حتما على تغيير المبادئ الخاصة بشن الحروب وتغيير طبيعة ميادينها الفعلية أو الافتراضية.
وعلى مدار التاريخ البشرى لعبت المعلومات والمعرفة دورا هاما وحيويا في تشكيل القوة، وأحدث التطور السريع لتكنولوجيا الكمبيوتر وخاصة في الشبكات تحولا كبيرا في مفهوم القوة ترتب عليه دخول المجتمع الدولي في مرحلة جديدة تلعب فيها هجمات الفضاء الإلكتروني دورا أساسيا سواء في تعظيم القوة أو الاستحواذ على عناصرها الأساسية. وأصبح التفوق في مجال الفضاء الإلكتروني عنصرا حيويا فى تنفيذ عمليات ذات فاعلية في الأرض وفي البحر والجو والفضاء. وتعتمد القدرة القتالية في الفضاء الإلكتروني على نظم التحكم والسيطرة.
وقد أوجدت ملايين أجهزة الكمبيوتر المنتشرة فى كل مكان عالما افتراضيا نشأ نتيجة عملية الاتصال، ومثل وسيطا جديدا للقوة حيث يمكن للقراصنة دخول الفضاء الإلكتروني بهدف محاوله السيطرة على الاجهزة وسرقة المعلومات وإفسادها أو تعطيلها.

ومع زيادة اعتماد المجتمعات والجيوش الحديثة على أجهزة الكمبيوتر، أصبح الإنترنت مرادفا لاستخدام الذكاء الاصطناعي. وهكذا ظهرت مخاطر جديدة، كما ظهرت أسلحة إلكترونية جديدة ومتعددة كالفيروسات وهجمات إنكار الخدمة والاختراق وسرقة المعلومات والتشويش.

وهناك ما يعرف بالقنابل الإلكترونية والتى تستهدف تعطيل الاتصالات والتشويش عليها والتنصت على المكالمات، وبث معلومات مضللة عبر شبكات الحاسب والهاتف، ومنها تقليد بصمات الأصوات وخاصة أصوات القادة العسكريين وعن طريق ذلك يمكن إصدار أوامر ضارة بالقوات، واستهداف شبكات الحاسب بالتخريب عن طريق نشر الفيروسات ومسح الذاكرة الخاصة بالأجهزة المعادية، ومنع تدفق الأموال وتغيير مسار الودائع، وإيقاف محطات الكهرباء عن العمل.

ونظرا لدور مراكز الاتصال والشبكات فى الحروب، فقد صممت لذلك أسلحة خاصة تعتمد على الطاقة الموجهة ومنها أسلحة الميكروويف عالية القدرة. والمعروفة اختصارا بـ (HPM)ويمكن استخدامها لاختراق الأهداف عالية التحصين لتدمير وشل أسلحة الدفاع الجوي والرادارات وأجهزة الاتصال والحاسبات التي تعمل ضمن منظومة القيادة والسيطرة. وتنتج هذه الأسلحة شحنات عالية من الطاقة تؤدي للإضرار بالأدوات الإلكترونية وتقوض ذاكرة الحواسيب، وتتميز بالدقة الشديدة في إصابة الهدف. وهناك نحو 120 دولة تقوم بتطوير طرق لاستخدام الإنترنت كسلاح لاستهداف أسواق المال ونظم الكمبيوتر الخاصة بالخدمات الحكومية. وتقوم أجهزة الاستخبارات الدولية بالفعل باختبار شبكات الدول الأخرى بصورة روتينية بحثاً عن ثغرات لتوظيفها عند الضرورة. كما أن هناك ما يشبة تشكيل قوات الكترونية.

يعد الإنترنت وسيطاً مفيداً بسبب التنوع والاتساع للأنشطة التي تجري من خلاله والتي تعد جزءا لا يتجزأ من طبيعة العصر الحديث، والتي يتزايد دورها فيما يعرف بالاقتصاد الرقمي والحكومات الإلكترونية والتجارة الإلكترونية، فضلا عن دوره في وسائل الإعلام والاتصالات الدولية والمصارف والمنشآت الحيوية. ومن ثم فإن أي عملية هجوم قد تستهدف الإنترنت كوسيط وحامل للخدمات وناقل لها من شأنه فشل الإنترنت في القيام بوظيفته ومن ثم فإن التحكم في تنفيذ هذا الهجوم يعد أداة سيطرة ونفوذ استراتيجية بالغة الأهمية سواء فى زمن السلم أو الحرب.

وتعتمد القوات المسلحة على الإنترنت في الاتصالات العسكرية بين وحدات الجيش والأجهزة الحكومية المعنية وأجهزة الاستخبارات، ويستخدم الجيش الإنترنت كمصدر للمعلومات والصور الفضائية. وفى الجيوش المعاصرة يوجد اتصال بين الإنترنت الداخلي للجيش وبين الشبكة الدولية، ومن ثم يمكن أن يتعرض الجيش للهجوم عن طريق

الإنترنت بعدة طرق كاختراق شبكات الجيش الداخلية وشن هجمات إنكار الخدمة للتأثير على عملية المعلومات واتخاذ القرار. ويؤدي التعرض لهجوم مباشر إلى إتلاف كم هائل من أوامر السيطرة على أجهزة الكمبيوتر ونظم ربط الشبكات، ومن ثم يحدث شلل تام أو جزئي في قدرة النظام على الردّ على طلبات المستخدمين المدنيين أو العسكريين. ويمكن لشخص واحد أن يحدث مثل هذا الشلل في شبكة أو مجموعة شبكات مترابطة.

وفي خلال السنوات الماضية تمكنت فيروسات سارس ولف من الانتشار في نصف مليون جهاز كمبيوتر في أقل من أربع ساعات، وأصبحت هذه الهجمات تستخدم في سياق صراعات دولية، فقد استخدم الناتو تقنيات الحرب الاليكترونية على صربيا وفي الحرب في كوسوفا، وغالبا ما يحدث محاولات للتأثير على شبكات مدنية او عسكرية فيما بين الصين وروسيا والولايات المتحدة واستراليا. كما استخدمت حروب شبكة الإنترنت في حرب العراق وفي الصراع العربي الإسرائيلي.

وقد تستخدم الدول هجمات الإرهاب الإلكتروني ضد دول أخرى، أو قد تستخدمها الجماعات الإرهابية، وفي السيناريو الأول قد تقوم إحدى الدول باستخدام هجمات الفضاء الإلكتروني ضد دولة أخرى دون أن تتورط بشكل رسمي ومباشر في حرب معلنة. وقد تقوم دولة باستخدام هجمات الفضاء الإلكتروني كجزء من الاستعداد لنشوب صراع وحرب وهجوم تقليدي ضد دولة معادية. وتعد هجمات الفضاء الإلكتروني أقرب إلى مفهوم الحرب غير المتماثلة، وهو مفهوم عسكري يشير إلى الاستخدام غير المباشر للقوة وذلك بدلا من استخدام القوة بصورة مباشرة في مواجهه قوة مقابل قوة أخرى. وتتضمن عمليات استغلال الفضاء الإلكتروني القدرة على توظيفة لخدمة وحماية نظم المعلومات ومنع تعرضة لعمليات هجومية معادية، وتعزيز الأمن الإليكتروني بأبعاده المتعلقة بالبرمجيات والبنية التحتية. ومنع استغلاله في الحرب النفسية. أما الدفاع عن الفضاء الإليكتروني فيعني القدرة على الحماية ضد هجوم أو استغلاله من قبل الخصم، وتأتي أهمية ذلك في ضوء احتمال استخدام الفضاء الإليكتروني من قبل الجريمة المنظمة أو القراصنة أو جماعات إرهابية وبما يؤثر على الاستقرار الاقتصادي والاجتماعي للدول التي تعتمد على الفضاء الإلكتروني في تسيير بنيتها التحتية. ومن ثم يصبح من مصلحة كل الدول أن تتعاون من أجل ضمان أمن وسلامة الفضاء الإلكتروني. لاشك أنه كما كان للفضاء الإلكتروني استخدامات سلمية كان له استخدامات عسكرية أيضا لأنه ارتبط باستخدام متعدد من قبل الدول والأفراد والجماعات الإرهابية بهدف تحقيق أهداف سياسية وبما عزز في الوقت نفسه من فرص ذلك الاستخدام عدم وجود اتفاقية دولية تنظم الفضاء الإلكتروني واستخداماته وتحدد الواجبات والمسؤليات في العمل على حفظ أمنه، ودخل ذلك في موضوع تنافسي بين العديد من الدول من أجل

**الاستحواذ على مصادر القوة داخل الفضاء الإلكتروني والتي أصبح يتعلق بعمل البنية التحتية الكونية للمعلومات والمرافق الحيوية كمحطات الطاقة والمحطات النووية وسدود المياه وخدمات الحكومة الإلكترونية والمصارف والبنوك والبورصات العالمية وأصبح كل ذلك يشكل عنصر هام من عناصر الأمن القومي الجديد.**

**وكما هو الحال في أية حرب، فإن الجيوش المتصارعة تستهدف دوما ثلاثة عناصر أساسية من أجل كسب المعركة؛ وهي العناصر العسكرية، والاقتصادية، والسياسية أو بكلمات أخرى إرادة الخصم، وفي عالم حروب المعلومات نجد العناصر الثلاثة ذاتها وعلى رأسها مراكز القيادة والتحكم العسكرية، والبنوك والمؤسسات المالية، ومؤسسات المنافع كمؤسسات المياه والكهرباء وذلك لإخضاع إرادة الشعوب. وكل ذلك دفع العديد من الدول إلى الاهتمام بأمن الفضاء الإلكتروني سواء أكان متمثلا في إنشاء هيئات لمواجهة الطوارئ او استحداث قوانين لمكافحة الجريمة الإلكترونية وصورة ثالثة ظهرت في الاهتمام به عسكريا والذي ظهر في مبادرة الولايات المتحدة في إنشاء قيادة عسكرية لحماية الفضاء الإليكترونى وهذه المبادرة من المتوقع أن تسري أيضا في العديد من الدول والولايات المتحدة وحلف الأطلسي يدرسان إمكانية صنع السلاح النفسي الإلكتروني.ويعد الإشعاع الترسيوني (إشعاع فيزيائي ينتج في المختبرات بشكل اصطناعي) ذروة الاختراعات الروسية في هذا المجال، ومن المستحيل على الإنسان بمساعدة الوسائل العادية واحتياطات الجسم الداخلية الدفاع بها عن نفسهِ ولا يجد الخبراء صعوبة في استخدام هذا الإشعاع لرفع حالة التهيج غير المرغوب فيها وتقليل النشاط النفسي والفيزيائي وإحداث خلخلة بكل الرغبات الإنسانية المعروفة، كالشرب مثلا، ويؤدي بالإنسان إلى الاعتراف بمختلف الأسرار التي يمتلكها وتدفعه على الانتحارِ ومن الضروري إدخال برنامج في العقل الباطن من دون تأثيرات التنويم المغناطسي المعروفةِ والأجهزة المرتبطة بهذا السلاح واستخدامه العملي سرية للغاية وتتطلب مهارة عالية في تشغيلها وما زالت الأعمال مستمرة في روسيا لتطوير هذا النوع من الأسلحة النفسية . الإلكترونيةِ. الأسلحة السايكوترونية Psychotronic weapons الأسلحة السايكوترونية هي تلك المصنّفة ضمن النوع المسمى بالأسلحة "غير المميتة-Non " ( lethal weaponsمع أنها مميتة جداً). تستطيع عناصرها الخفية أن تقتل عبر مسافة غير محدودة، يمكنها تجسيد أو التسبب بأي مرض مزمن، يمكنها جعل الشخص يتحوّل إلى مجرم أو أبله عديم المسؤولية، التسبب حوادث طيران أو سير أو سكك حديدية خلال ثوانٍ، تدمير البُنى الأساسية لأي شيء مادي أو حيوي، خلق أو استثارة أي كارثة بيئية/جوية، التحكّم بأكثر الآلات أو الأدوات تعقيداً التحكّم في سلوك البشر وأي كائن حيوي آخر وكذلك تغيير نظرة الواقع لمجتمع بكامله.**

## الأسلحة غير المميتة والضربات الانتقائية

لم يكن الهدف من كتابنا حرب اللاعنف وعلاقتها بالفوضي الخلاقة مجرد فضح المخططات وإنما أيضا استخدام هذا العلم وتحويله إلى طريقة لحروب وصراعات المستقبل، بحيث مهما كانت أي حرب أو صراع لا يقتل فيه بشر، خاصة وأن حقوق الإنسان ومواثيقة وقوانينه في ازدياد وتقدم. والأسلحة غير المميتة أحد التصنيفات الحديثة للأسلحة التي تعد أقل فتكاً، حيث لا تكون مميتة للأفراد بل تستهدف إضعافهم أو تعطيل معداتهم. وقد ظلت تستخدم هذه الأسلحة لفترة طويلة بشكل أساسي في الشرطة والقوات شبه النظامية ثم أنتجت منها نوعيات أكثر تطوراً للاستخدام العسكري، ويؤدي استخدامها لتقليل الخسائر البشرية والمادية للحروب؛ وتقليص تكاليف إعادة الإعمار، وتضم هذه الأسلحة: الأسلحة الصوتية، والأسلحة الصوتية البصرية، والحواجز، والهراوات، ومضادات القتل، والتقنيات الحيوية، والأسلحة المكهربة، الأسلحة الكهرومغنطيسية، والأسلحة الرغوية اللزجة.

وتعد القنابل النيوترونية سلاحاً لاستهداف الأفراد دون المنشآت، إذ صمم لتقليل الصدمة الحرارية المتولدة من القنابل النووية الكبيرة، بينما يقدم الطاقة القاتلة للنيوترونات السريعة ذات الطاقة العالية، وهو ما يؤدي إلى التحكم في حدود التدمير الإنشائي الناتج عن التفجير مع زيادة قدرتها على قتل الأفراد، ولذا يطلق عليها القنبلة الصديقة للمباني ويتم إنتاجها من الزئبق الأحمر وتبلغ قوتها كيلو طناً واحداً، وكما تم إنتاج نموذج مصغر منها يتميز بدقة التصويب.

والنتيجة الطبيعية لآلية المعركة هي تقليل العناصر البشرية نتيجة إحلال الآلة محلها جزئياً ونتيجة قيام المعدة المتطورة بمهام كانت تقوم بها قبلا عدة معدات، وسيفرض هذا التطور الاستعانة بقوة بشرية مؤهلة علمياً لتستوعب أنظمة التسليح المتطورة، كما أن هذه الأنظمة أصبحت تبنى بشكل متكامل يشتمل على مكون حرب المعلومات، وأدى تقدم تكنولوجيا التصغير في كل المجالات تقريباً إلى تقليص حجم المعدات العسكرية بدرجة ملحوظة، وستؤدي تكنولوجيا الإخفاء لإطالة عمر نظم التسليح على نحو سيؤثر في اقتصاديات التسليح، وسيؤدي هذا التطور لإعادة تنظيم الوحدات المقاتلة باستحداث وحدات جديدة (فضائية - حرب معلومات - دفاع ضد الصواريخ - وحدات ليزر) ومقابل ذلك سيتم تقليص حجم وحدات المشاة التقليدية والاعتماد على قوات المشاة الميكانيكية والمدرعة، مع زيادة حجم القوات الخاصة. ومن المنتظر أيضاً زيادة عدد وحدات الصواريخ أرض-أرض،والصواريخ المضادة للصواريخ التكتيكية والعملياتية والاستراتيجية على السواء، وكذلك عناصر المدفعية ذات المقذوفات الذكية والموجهة ذاتياً على حساب عناصر المدفعية التقليدية المجرورة، وتخفيض حجم وحدات الإشارة والاستطلاع التقليدية اعتماداً على نظم الاتصال التي توفرها ثورة المعلومات. وهناك صنف الاسلحة السمعية غير القاتلة أو قنابل صوتية . بصرية صادمة، كما أن هناك نظما سمعية توجه ضد الأفراد والمعدات والآليات، ومولدات

**سمعية ترسل موجات صوتية وفوق صوتية تصيب الإنسان بالألم والغثيان وتشوش حركته. وفيما يتعلق بالتأثير السياسي والأخلاقي لاستخدام الأسلحة غير القاتلة سواء كانت قنابل صوتية أو بصرية أو كهرومغناطيسية أو موجات ميكرويف حارقة فإن بعض الخبراء يقارن تأثيرها بتأثير القنبلة الذرية التي كانت أشنع أسلحة قاتلة يخترعها الإنسان حتى الآن، ولم تستخدم أبدا بعد إسقاطها على كل من هيروشيما وناجازاكي. ومثلما غير السلاح النووي التفكير الاستراتيجي الدولي وخلق إلى الوجود مصطلح جديد هو الردع النووي الذي حكم العلاقات الدولية لأربعة عقود، فإن الأسلحة غير القاتلة يمكن أن تدشن مرحلة جديدة من العلاقات الدولية تقوم على مفاهيم التدخل الوقائي المحدود والضربات الانتقائية. ويبدو أن الولايات المتحدة بالذات تعول على هذا النوع من الأسلحة كثيرا لتسهيل تنفيذ سياساتها في الخارج من دون احتجاج داخلي أو خارجي كبير. ولا يستبعد المحللون الاستراتيجيون أن تتولى كتيبة أمريكية واحدة أو حتى فصيلة، تنويم أو شل حركة فرقة أو فيلق من الحرس الخاص لرئيس هذه الدولة أو تلك ثم إلقاء القبض عليه بكل يسر وسهولة، لمحاكمته بتهمة دعم الإرهاب أو ارتكاب جرائم حرب. وقد يؤدي تطور هذا النوع من الأسلحة التي يحرص البنتاجون الأمريكي على وضع أبحاثه عليها في منتهى السرية، إلى تغيير كبير في مفهوم السيادة بحيث تتلاشى سيادة الدول على أراضيها. وقبل أن يصل العالم إلى تلك النتيجة فإن منظمات حقوق الإنسان تحاول أن تنبه إلى خطورة الأسلحة غير القاتلة ومن بين هذه المنظمات اللجنة الدولية للصليب الأحمر، ومعهد استوكهولم الدولي لأبحاث السلام، إضافة إلى منظمات أخرى، ولكن الاهتمام بهذه القضية لم يصل إلى درجة تكفي للتحذير منه، إذ أن الكثير من البشر مازالوا يجهلون خطورة هذه الأنواع من الأسلحة إن لم يعرفوا بوجودها أصلا. وقد انتقدت منظمات حقوق الإنسان استخدام الليزر على سبيل المثال كسلاح يتسبب في العمى المؤقت وربما الدائم، كما حذرت من استخدام أي أسلحة تسبب عاهات مستديمة بدنية أو عقلية حتى وإن لم تكن قاتلة. وطالبت اللجنة الدولية للصليب الأحمر بسن قوانين دولية تنظم أو تمنع صنع واستخدام أو إساءة استخدام الأسلحة غير القاتلة.**

**من هنا يأتي التسريع في استخدام الروبوت في الحرب كبداية لجيوش بدون جنود.فباستطاعة الروبوت الواحد أن يحل محل 2و7 عامل،أي أن 100 ألف روبوت تكفي لإلغاء 270 الف وظيفة عمل،بينما يتطلب إنتاجها هي نفسها 50 ألف من العمال.ويتطلب استخدامها حوالي 50 ألف آخرين.والمحصلة النهائية هي أن تشغل مائة ألف روبوت يعني تأهيل مائة ألف عامل وبطالة 170 ألف آخرين.وهذه النسب ستتضاعف أكثر من 20 مرة خلال ال20 سنة الأولي من القرن ال21.كل هذا بالطبع مع تطور العامل وتحديثه وتمكينه بأحدث وسائل وعلوم العصر.**