الفضاء الإلكتروني ساحة حرب دولية مفترضة

تاريخ الاستلام:2014/4/8 تاريخ القبول: 2014/10/16

د. عصام فاعور ملكاوي (*)

الملخص

يعد الفضاء الإلكتروني في وقتنا الراهن وحسب المفهوم الأمريكي, البعد الخامس بعد حروب البر والبحر والجو والفضاء, كما أعلنت حكومة المملكة المتحدة قبل أشهر قليلة, أن استراتيجيتها للحرب الإلكترونية أخذت منحى أبعد من مجرد تأمين المملكة المتحدة ضد الهجمات الإلكترونية,لتصبح في الواقع استراتيجية تسعى لتطوير الأسلحة الإلكترونية لاستخدامات المستقبل.

وعلى الرغم من بقاء تعريف الحرب الإلكترونية محل اختلاف شديد, إلا انه وببساطة يمكن القول بأنها: عمل يقوم به سكان دولة ما , من خلال الإنترنت لمهاجمة أجهزة كمبيوتر أو شبكات معلومات لسكان دولة أخرى, مما يتسبب في أضرار ودمار في البنى التحتية الحساسة والمهمة, وعلى مدى عقد من الزمن , اعتبرت الحرب الإلكترونية جزءا من الصراعات المعاصرة.

(*) كلية العلوم الإستراتيجية – جامعة نايف العربية للعلوم الأمنية –الرياض – المملكة العربية السعودية.

وما زال العديد يتساءلون إذا كانت الأطر الأخلاقية التقليدية التي نفكر بها, كأخلاقيات الحرب التقليدية التي وضعت بعد الحرب العالمية الثانية مناسبة لتطبيقها على الأسلحة المستخدمة في عالم الإنترنت والحرب الإلكترونية.

Abstract

Cyber-space has recently been recognized as the fifth domain of warfare according to the American concept (alongside land, sea, air, and space) and the UK government has few months before announced that its cyber-strategy now simply goes beyond securing us against cyber-attacks but actually developing our own cyber-weapons for future employment.

Though the definition of cyber-war remains a matter of some intense dispute,tut it can simply be said that it is an action carried out by a nation-state, usually via the internet, to perpetrate another nation's computers or information networks for the purposes of causing damage and disruption to its critical infrastructure. Cyber-war has been considered a part of contemporary conflicts of at least a decade. Cyber-war is here and it is happening. Yet many are beginning to question whether our traditional ethical frameworks for thinking about the morality of warfare, frameworks that were developed after World War Two in response to conventional kinetic weapons, are suitable to be applied to weapons employed in the cyber realm and cyberwar.

المقدمة:

لم تعد مجالات المنافسة والمجابهة والاقتتال ,مجالات محصورة في ساحات القتال المتعارف عليها قي العلوم العسكرية والإستراتيجية, بل تعدتها إلى مجال آخر جديد,والذي أطلق عليه الخبراء الفضاء الإلكتروني, والذي أضيف في أواخر القرن العشرين إلى أدوات وساحات الصراع كحرب جديدة, وشَكّل في نظر البعض امتداداً للحرب الإلكترونية التي كانت سائدة مع نهاية الحرب العالمية الثانية، وخاصة خلال فترة الحرب الباردة.

فحرب الفضاء الإلكتروني لا تعد تعبيرا رديفا للحرب الإلكترونية بمعناها التقليدي المتعارف عليه، بل هي نوع من الحرب يستهدف الشبكات الإلكترونية،التي قد تكون مدنية أو عسكرية.

ويعد الفضاء الإلكتروني في وقتنا الراهن البعد الخامس للدفاع، بعد البر والبحر والجو والفضاء.(المرهون,عبد الجليل:2012م).ومع بداية القرن الحادي والعشرين أصبحت شبكة الإنترنت أساسية في استخداماتها للاتصالات والتعاملات وأجهزة التحكم والسيطرة، بالإضافة إلى أنها شكلت وسيلة تجسس لبعض الدول، كما تحولت إلى أداة استخدام في بعض الحروب ذات الصفة النوعية.

إن ما كشفه جوليان أسانغ، مؤسس موقع "ويكيليكس" ، في صيف عام2011م, يؤكد أن أجهزة الاستخبارات الأميركية يمكنها الحصول على معلومات عن أي مستخدم لمواقع الإنترنت الكبيرة في أي وقت تريده,مما جعل وكالة البحوث الدفاعية المتطورة ومراكز الدراسات الاستراتيجية والدولية في الولايات المتحدة الأميركية تفرد جزءاً مهماً

من أبحاثها ودراساتها لأسس الحروب عبر الشبكة العنكبوتية. وهكذا باتت الحرب الإلكترونية الشكل الرائج والأكثر احتمالية في حروب القرن الحادي والعشرين.

ومنذ ذلك الوقت انتقل العديد من وسائل السيطرة والتحكم الخاصة بمعظم العمليات الحربية والاستخباراتية الحيوية من الأرض إلى الفضاء في صورة أقمار صناعية ومحطات فضائية، وبذلك انتقلت من عالم الحواس إلى العالم الافتراضي الذي أوجده الإنسان باختراعه للكمبيوتر والذاكرات الإلكترونية الذكية وشبكات المعلومات، وأنشأ بداخله ساحات صراع بديلة سميت بالجغرافية الافتراضية الجديدة.

وهذا ما لاحظه الباحث من خلال دراسته واطلاعه ومتابعته لموضوع الدراسة في السنوات الأخيرة, وهو أنّ عدة دول في العالم أخذت تركز على تطوير قدرات حرب الفضاء الإلكترونية إضافةً إلى الولايات المتحدة الأمريكية التي تعد الأكثر تقدماً في هذا النوع الجديد من الحرب، مثل روسيا والصين وإسرائيل. وإن ما يثبت ذلك هو وجود ما بين عشرين وثلاثين جيشاً في العالم لديه قدرات يعتد بها في مجال حرب الفضاء الإلكتروني. وتركز حرب الفضاء الإلكتروني على استخدام تقنيات المعلومات والإنترنت كسلاح للحرب، وهذا النوع الجديد من الحرب ليس لعبة أو شطحة من شطحات الخيال، فمعظم الحروب الفعلية التقليدية في المستقبل ستصاحبها حروب فضاء إلكتروني، بل ستكون هناك حروب فضاء إلكتروني أخرى قائمة بذاتها، وإن امتلاك قدرات حرب الفضاء الإلكتروني يمكن أن يغير ميزان القوى العسكرية العالمية.(كلارك ريتشارد, وروبرت نيك: 2012م).

وفي ظل غياب التشريعات والقوانين الناظمة لاستخدام الفضاء الإلكتروني حتى وقتنا الحالي تبقى هناك أسئلة لا تزال دون حل بشأن آفاق حرب الفضاء الإلكتروني، ترتبط بصفة أساسية بماهية قوانينها، وقواعد الاشتباك الخاصة بها, وفي أي ظروف تشن؟ وكيف يمكن تجنيب المدنيين أضرارها الجانبية؟ وما هي مجالات استخدامها؟ وهناك أيضا سؤال حول من له الحق في الدول المختلفة باتخاذ قرار شن حرب الفضاء الإلكتروني، وعلى أي من المستويات يكون: السياسي أم العسكري؟

إن ماقامت به الولايات المتحدة من خلال عمليات التجسس الأخيرة على أصدقائها من زعماء بعض الدول, تشكل حسب رأي الباحث، نقلة نوعية في طبيعة العلاقات الإقليمية والدولية, تبيّنُ للجميع أن لا صديق ولا عدو في عالم السياسة, لأن "الميكافيلية" الأمريكية لا تؤمن إلا بلغة المصالح ولا شيء غيرها, إنها الغاية التي تبرر الوسيلة.

وهكذا أصبح الفضاء الإلكتروني, الساحة الجغرافية الافتراضية الجديدة في هذا النوع من الحروب الجديدة, التي قادت إلى المواجهات الافتراضية أو ستقود إليها مستقبلا، والتي لن تكون أدواتها ووسائلها وأهدافها تقليدية كما الحروب المتعارف عليها, إنها عدو كل ما يمكن أن تهاجمه أو تواجهه أو تجد فيه خطرا محتملا وإن كان افتراضيا وغير متوقع , إنها أسلوب جديد من الحرب الاستباقية أو بمعنى آخر العداوة الافتراضية.

مشكلة البحث

شكل التقدم العلمي في ثورته التكنولوجية الهائلة, ساحة جذب خصبة للدول المتقدمة, وبعض الدول ذات المصالح المتشابكة والمشتركة في المجتمع الدولي, سعيا للمنافسة والسيطرة على حيز من ساحة الفضاء الإلكتروني, بعدما ضاقت المساحات المكانية بطموح القوى العظمى فكان الفضاء اللاإلكتروني المكان الأرحب للتنافس الجديد في عصر الإنجازات الإلكترونية.

إن التطور الكبير الذي واكب ثورة تكنولوجيا المعلومات والاتصالات, والتوسع في استخدام شبكة المعلومات الدولية (الإنترنت), صاحبه تطور كبير في وسائل ارتكاب الجرائم. حيث ظهرت نوعية جديدة من الجرائم المستحدثة يتم ارتكابها من خلال استخدام التقنيات الحديثة والحاسبات الآلية عن طريق شبكة الإنترنت، أطلق عليها الجرائم المعلوماتية أو الجرائم الإلكترونية. ولقد أصبحت هذه الجرائم تهدد أمن وسلامة الأفراد والمؤسسات والدول ذاتها، فالمعلومات تتزايد يوما بعد يوم، ولا تتناقص بالاستخدام أو بالاستهلاك، وتعتبر المعلومات مصدر قوة اقتصادية وسياسية وعسكرية واجتماعية، ومع تزايد المعلومات واستخدام شبكة الإنترنت سوف تتزايد صور الاعتداءات والتهديدات, مما يعني ظهور العديد من أنماط الجرائم المختلفة، الأمر الذي يتطلب ضرورة التصدي لهذا النوع من الجرائم بالشكل الذي يحقق فاعلية في مواجهتها .

كما تبرز خطورة حروب الإنترنيت والشبكات, في كون العالم أصبح يعتمد أكثر فأكثر على الفضاء الإلكتروني (Cyberspace), لا سيما في البنى التحتية المعلوماتية العسكرية والمصرفية والحكومية, إضافة إلى المؤسسات والشركات العامة والخاصة, والذي يفرض بدوره القيام بدراسات وأبحاث تحول دون تخريب هذا الفضاء وإفساده.

ولما كانت حرب الفضاء الإلكتروني تدخل ضمن التصنيفات آنفة الذكر, إضافة لعدم وجود الضوابط والتشريعات القانونية الناظمة لاستخدام الفضاء الكوني لغير الأغراض الإنسانية, فإنها تعتبر حسب رأي الباحث من الجرائم المستحدثة, والتي تستهدف الشبكات الإلكترونية بشقيها المدني والعسكري. لذلك شكل التصدي لهذه الجرائم في الفضاء الإلكتروني في عصرنا الحاضر, بعدا خامسا في الأبعاد الدفاعية المتعارف عليها, البرية والبحرية والجوية والفضائية.

من هنا جاءت فرضية هذا البحث على النحو التالي:" إذا كانت الحرب بمفهومها العام عبارة عن اختبار شامل للقوى المادية والمعنوبة للدولة, فإن الأمر ليس كذلك بالنسبة لحرب الفضاء الإلكتروني, إنها حرب أدمغة بالدرجة الأولى, وهي ذات أهداف تجسسية أو تدميرية للشبكات الإلكترونية, مما يؤثر في طبيعة العلاقات الإقليمية والدولية, وتسهم في إعادة صياغة ضوابط النظام الدولي المعاصر وبحسب قدرات التكنولوجية للدول".

وعليه تبرز الفرضيات الفرعية التالية التي لابد من فحصها والتأكد منها :

- هناك علاقة طردية بين التقدم التقني الإلكتروني, وزيادة الفجوة الأمنية للدول.
- كلما تم التوصل لعمل دفاعي جديد لحماية الدول, كلما تسارعت وتيرة العمل المضاد لكسر هذه الحماية.
- يعتبر التجسس الإلكتروني شكلاً من أشكال الجرائم المستحدثة, تغذيه وتشجع عليه حروب الفضاء الإلكتروني.

- ليس هناك دولة أو أفراد أو مؤسسات مدنية أو عسكرية في مأمن من حروب الفضاء الإلكتروني سواء كانت خروقات للشبكات العنكبوتية أو تدميراً لها أو تجسساً عليها.

أهداف البحث

يهدف البحث للتوصل إلى فهم ماهية حروب الفضاء الإلكتروني, وكيف تدار إضافة إلى تحليل المخاطر الناتجة عنها والاحتياطات اللازمة لمواجهتها والسيطرة عليها, و ذلك من خلال:

- التعرف على العلاقة مابين زيادة التقدم التتقني الإلكتروني وتحقيق الأمن الدولي.
- التأكد من القدرة الحمائية للدول ضد الغزو الإلكتروني الجديد.
- التعرف على جاهزية الدول اللازمة لمقاومة حالات التجسس الإلكتروني عليها.
- التأكد من القدرات الدولية المضادة اللازمة لمقاومة الخروقات للشبكات العنكبوتية, وتحصين الفضاء الإلكتروني لمنع التجسس أو تدمير هذه الشبكات.

أهمية البحث

تبرز أهمية هذا البحث من الناحية العلمية والعملية كونه يشكل دراسة تشخيصية وتحليلية لما يعيشه عالمنا المعاصر اليوم من تخمة في التطورات التكنولوجية التي فاقت حد الحاجات الضرورية لواقع الإنسان في دوله المختلفة, الأمر الذي أغرى دولا وجماعات كثيرة على استغلال هذا الفائض من التقدم التكنولوجي والمعرفي ليصب في اتجاهات سلبية تعرض الكثير من دول العالم إلى القرصنة غير المحسوبة أو الخارجة عن نطاق قدراتها بما يغري الدول العظمى أو من يملكون مثل هذه القدرات أن يحققوا أهدافهم على حساب قوى لم تلحق بهذا التطور العلمي للحد من أثاره السلبية, وإعادة تشكيل العالم الافتراضي بما يخدم مصالحهم دون غيرهم. وتبرز هذه الأهمية حسب رأي الباحث من الدور الذي تلعبه الدول والمؤسسات المدنية والعسكرية, إضافة إلى بعض الأفراد والجماعات, فيما يختص بالاستخدامات السلبية للفضاء الإلكتروني,والذي يعد حافزا قويا لإعادة تشكيله ليكون فضاءً خدميا للبشرية لا كابوس خوف يؤرق مضاجعهم.

وتكمن أهمية البحث في دراسة المتغيرين الرئيسين في هذه الدراسة وهما: زيادة التقدم التقني الإلكتروني واستخداماته المختلفة, ومدى استفادة الدول والمؤسسات من هذا التقدم لتوفير الأمن وعدم انتهاك سيادة الدول وحقوق الناس وحرياتهم .

من هنا يمكن لهذا البحث أن يقدم توصيات مفيدة للعاملين في المجالات الأمنية والاستراتيجية, من أجل متابعة ما يستجد من اكتشافات وتطور إلكتروني غير محسوب, من ناحية طرق الاستخدام السلبية إضافة لتوفير التقنيات الحمائية المضادة.

منهج البحث

استخدم الباحث المنهج الوصفي المسحي, الذي يعتمد على وصف المتغيرات وصفا دقيقا, وتحليلها اعتماداً على تحليل الدراسات السابقة في هذا المجال, من خلال استقراء الواقع وأسلوب تحليل المضمون, حيث إنّ هذا المنهج يساعد في دراسة الواقع أو الظاهرة ويهتم بوصفها وصفا دقيقا ويعبر عنها كميا وكيفيا.

المفاهيم والمصطلحات

الفضاء الإلكتروني: هو الوسط الذي تتواجد فيه شبكات الحاسوب ويحصل من خلالها التواصل الإلكتروني.(http://ar.wikipedia.org/wiki/ php.index)

حرب الإنترنت أو **Cyberwarfare** :(http://ar.wikipedia.org/wiki)هي مصطلح يشير إلى استخدام الحواسيب وشبكة الإنترنت في مهاجمة الأعداء وهم يدعون بالمخترقين(hackers)

الحرب الإلكترونية:، عرّف كلٌّ من "ريتشارد كلارك" و"روبرت كناكي" الحرب إلكترونية بأنها "أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها. (Klarke &ekaneK:6P :2010)

فيما يعرّفها آخرون بأنها " أي نزاع يحدث في الفضاء الإلكتروني ويكون له طابع دولي". هذه التعريفات فضفاضة ولا تعبّر بدقّة عن الموضوع، يقترح آخرون (Dunn,Cavelty2010),أن يتم التركيز على أنواع وأشكال النزاعات التي تحصل في الفضاء الإلكتروني ومنها على سبيل المثال:

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 (Servers) من خلال إغراقها بالبيانات.

الجريمة الإلكترونية والتجسس الإلكتروني: ويقعان في المستوى الثاني والثالث وغالبا ما يستهدفان الشركات والمؤسسات، وفي حالات نادرة بعض المؤسسات الحكومية.

الإرهاب الإلكتروني: ويقع في المستوى الرابع من النزاع في الفضاء الإلكتروني. ويستخدم هذا المصطلح لوصف الهجمات غير الشرعية التي تنفّذها مجموعات أو فاعلون غير حكوميين (Non-State Actors) 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 وإلى خراب يترك قدرا كبيرا من الخوف.

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 و/أو توجهات المدنيين في مسرح العمليات الإلكتروني.

التجسس الإلكتروني :(http://ar.wikipedia.org/wiki/),"عبارة عن الطرق المستخدمة لاختراق المواقع الاكترونية , ومن ثم سرقة بعض المعلومات والتي قد تكون فائقة الأهمية والخطورة للطرف المتلقي والمسروق منه, وقد انتشرت في الألفية الجديدة بانتشار طرق الاختراق وأحيانا قد يكون الاختراق من اشخاص عابثين ليس إلا, وأحيانا بغرض سرقة معلومات".

من خلال ما تقدم يرى الباحث عدم وجود إجماع محددعلى تعريف دقيق لمفهوم الحرب الإلكترونية أو أحد مشتقاتها من المصطلحات ذات الصلة حتى الآن، بالرغم من اجتهاد العديد من الخبراء .

المستقبل بين الخيال والواقع

على مدار التاريخ الإنساني توالت الثورات العلمية في المجال الحربي والعسكري ,وهذه الثورات مصدرها الأول العقول المفكرة التي تستثمر طاقتها المبدعة في صنع تقنيات وتكنولوجيات جديدة تستطيع بها خدمة أوطانها وتوفير سبل الأمن لها, ولو تطرقنا إلى تاريخ الحروب التي عرفتها البشرية من القديم إلى الحديث لوجدنا أن العلم والحرب ربطت بينهما علاقة جدلية تظهر أحياناً وتختفي أحياناً أخرى, فالتلازم بين العلم والحرب كان في الماضي ويوجد في الحاضر وسيستمر في المستقبل, والقاسم المشترك بينهما يكمن في التخيلات المستقبلية لما يمكن ان يستجد ويكون عليه واقع الحال في كل زمان ومكان, ومن هنا ظهر، وحسب راي الباحث مفهوم أدب الخيال العلمي المحفز على التطوير والابتكار , وقد عرفته(سلامة,2006م):" بأنه ذلك الأدب الذي يتناول التقدم العلمي ومنجزات التقنية وتطورها، من خلال أحداث درامية، وينطلق هذا الأدب من حقيقة علمية ثابتة أو متخيلة، تكشف عن جانب مجهول من الكون أو لتصف حياة البشر في المستقبل القريب أو البعيد، أي إنّه خيال يشكل منطلقاً أساسياً في تكوين صور ذهنية جديدة لدى الأفراد لما ستكون عليه الأشياء في المستقبل".

إن كتابات عالم الاجتماع الأمريكي "الفين توفلر" شكلت علامة فارقة في التفكير العلمي في المستقبل، وقد ساعدت كتاباته في توفير كثير من المصطلحات الأساسية لكثير من المستقبليين خاصة ما ورد في كتابه "صدمة المستقبل" (Future Shock)

حيث اعتبر "توفلر" أن ما عاناه الأفراد والمجتمعات من اضطرابات سيكولوجية في الفترة الممتدة من أواخر القرن العشرين وأوائل القرن الحادي والعشرين شكلت حالة من الاضطرابات المتعارضة، تتراوح بين حالات حماس وانبهار، وحالات خوف وارتعاب، كان سببها التغير السريع والتغير العميق لما ألفه الأفراد والمجتمعات في الزمن الماضي.وحسب رأي " توفلر" فإن المستقبل هو أرض مجهولة يتطلب اكتشافها، ومن الأفضل أن يكون لدينا خريطة غامضة وناقصة ومعرضة لإعادة النظر والتعديل، بدلاً من أن لا يكون بين أيدينا شيء، ويجب القول أن المستقبل قابل للدراسة، وليس مغلقاً بالكامل أمام محاولات الإنسان.(توفلر: 1990م,ص 487).

وهذا يؤكد مالأفلام الخيال العلمي من دور مهم في التنبؤ بتقنيات حروب المستقبل وأسلحتها، حيث يذكر أن مبادرة الدفاع الاستراتيجي التي أعلن عنها الرئيس الأمريكي الأسبق رونالد ريجان عام 1983،(سلامة:2006م)والتي عرفت بين وسائل الإعلام بحرب النجوم، كانت مستمدة من فيلم "حرب النجوم" الذي أنتج عام 1977.كما أن فيلمي "المفترس" الذي أنتج عام 1987 م و"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" العالم 1995م .

ثورة المعلومات والاتصالات أعادت صياغة عالمنا

بدأ الاتصال اللاسلكي الحقيقي في عام 1888م على يد الألماني هرتز، وفي منتصف عام 1897م استطاع المهندس والمخترع الإيطالي ماركوني تطوير جهاز لاسلكي يناسب الاستخدام في البحر؛ وكان من الطبيعي أن يظهر التشويش على الاتصالات اللاسلكية لتزايد الاستخدام في مساحة محددة, مما يعني التداخل البيني للموجات الكهرومغناطيسية عند إشعاعها بكثافة عالية في تلك المساحة المحددة، ومن هنا بدأ التدريب على العمل في ظل التشويش نتيجة الاستخدام اللاسلكي المكثف؛ ثم بدأ بعد ذلك الاستخدام المتعمد للتشويش لإعاقة الاتصالات اللاسلكية بين الوحدات العسكرية المعادية؛ وذلك لإرباكها وشل سيطرتها على قواتها وأسلحتها، وتجلت هذه الحرب منذ الحرب اليابانية الروسية في بداية القرن العشرين، وبدأت في الانتشار في الحرب العالمية الأولى (1914- 1918م)(http://www.moqatel.com).

في الحرب العالمية الأولى كان التشويش على الاتصالات اللاسلكية يستخدم من حين إلى آخر، ولكن وجد أنه لكي ينفذ على أي اتصال لاسلكي كان لابد أن يسبقه عملية التنصت الأمر الذي تبين منه، في أحيان كثيرة، أهمية المعلومات التي يتبادلها الجانب المعادي ومعرفة نواياه المستقبلية. من هنا ظهرت أهمية أعمال الاستطلاع اللاسلكي على شبكات العدو اللاسلكية بهدف الحصول على المعلومات. ومن المؤكد أن ثورة المعلومات والاتصالات أعادت صياغة عالمنا بما يفترض عقلية جديدة للتعامل مع الواقع الجديد، فالعالم يعيش تغيرا نوعيا في جميع أوجه الحياة: في الاقتصاد، والسياسة، والثقافة، والعلاقات الاجتماعية. وذلك يجري بتعجيل يفرضه زخم الثورة التكنولوجية في مجال المعلومات والاتصالات التي تتخذ طابعا كونيا حوّل العالم إلى قرية صغيرة، بينما تمر بعض من دول العالم في مرحلة متطورة من الثورة التقنية يقبع بعضه الآخر في الظلام ويتعثر منجزه التقني، بانتظار ردم، أو لنقل تقليص،

الفجوة الحضارية بين عالمين.ولا شك أن هذه الثورة المعلوماتية والتقنية استغلت في غير اهدافها أحيانا، وأحيانا تسببت في بعث شبح الرقابة.**(كاظم ,2007 بي بي سي العربية).**

تتحدث (سلامة:2006م) في كتابها " أسلحة حروب المستقبل بين الواقع والخيال", بأن حروب المستقبل تتميز باعتمادها على التكنولوجيات المتقدمة والمتطورة ,التي لم تعد ضرباً من ضروب الخيال العلمي، بل أصبحت حقائق قائمة في الكثير من جوانبها. ويرى الخبراء العسكريون أن الاستراتيجيات العسكرية الحديثة، والثورة في الشؤون العسكرية Revolution of Military Affairs,(RMA) ونظم القتال المستقبلية (Future Combat Systems) ستغير مفاهيم إدارة الصراع في المستقبل وستجعل حروب المستقبل غير تقليدية؛ إذ ستؤدي إلى تقليل الحاجة تدريجياً إلى البشر، وستحتوي على أسلحة ومعدات متقدمة جدا.

وعن أهمية استشراف المستقبل يشير الباحث إلى ماذكره الكاتب الأمريكي "ألفن توفلر" في مقدمة كتابه (صدمة المستقبل:1990م): "إن قراءة الخيال العلمي أمر لازم للمستقبل", مما يعني أن ما تتطلع إليه البشرية اليوم لما سيكون عليه المستقبل لا يكون إلا من خلال تخيلات يرسمها أصحاب الفكر المستقبلي, لتكون أمورا واقعية وحقيقية بأيدي صناع القرار لرسم خريطة المستقبل في التعامل الدولي خاصة فيما يتعلق بالعلاقات الإقليمية والدولية, لتحقيق المصلحة القومية العليا لدولهم ليس إلاَ.

وهكذا كان عندما تم إدخال علم التخيلات إلى قاعات الدراسة في المدارس والجامعات الأوروبية والأمريكية، وتم إنشاء مراكز متخصصة فيه، ومنها على سبيل المثال 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 كتّاب 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، حيث تمدنا بإنذار مبكر للقضايا العلمية والاجتماعية، وحث الناس على توقع تحدياتها ومفاجآتها، وبالتالي التهيؤ والاستعداد لمواجهتها قبل حصولها.(سلامة:2006م)

وهكذا يؤكد العلماء والخبراء العسكريون أن أسلحة المستقبل ستعتمد على تكنولوجيات متقدمة ومتطورة, ولم تعد ضرباً من ضروب الخيال العلمي, فمصانع السلاح لايقتصر أنتاجها على أسلحة تقليدية وأسلحة دمار شامل والأسلحة الأشد فتكاً وأقوى تدميراً, بل يرى العلماء أن أسلحة المستقبل لن تحتاج إلى بشر وستحمل مسميات مبتكرة , كالأسلحة غير الفتاكة والأسلحة النظيفة والأسلحة الذكية وغيرها من المسميات, التي تقود حروب المستقبل.(http://defense-arab.com)

ويرى الخبراء العسكريون في حديثهم عن العلم وأسلحة المستقبل(http://defense-arab.com): أن تقنية الروبوتات هي أول صورة من صور حروب المستقبل, وهذه الروبوتات عبارة عن كائنات إلكترونية شديدة التطور التكنولوجي , وينظر العلماء إليها باهتمام خاص, لاستخدامها في الحفاظ على حياة الجنود والقادة في ميدان الحرب, فقد استخدمت القوات الأمريكية في حرب أفغانستان عام 2001م الروبوت "باكيوس" الذي صممته شركة- آى روبوت - الأمريكية خصيصاً للمهام العسكرية,

مثل عمليات الاستطلاع ورصد السلاح الكيماوي والتمويه وتغطية المنطقة بالدخان, هذا إلى جانب قيام هذه الروبوتات بمهام أخربجديدة, مثل إزالة الألغام ونزع القنابل وقيادة الطائرات ونقل المؤن والذخيرة والأسلحة للجنود وتوفير المساعدة التلقائية لهم في ميدان المعركة, وأن ذلك يعني أن نصف وحدات الجيش في حروب المستقبل ستكون من البشر والنصف الأخر من المعدات الآلية، وبرغم هذه الآمال الكبيرة المعلّقة على الروبوتات في حروب المستقبل, ينتاب العلماء والخبراء المخاوف من المقاتل الآلى الذي يفتقر إلى المشاعر الإنسانية لأنه سيكون مقاتلاً أكثر وحشية من نظيره الجندي البشري الأمر الذي يشدد عليه العلماء بضرورة برمجة هذه الروبوتات العسكرية التي ستخوض حروب المستقبل للالتزام بالضوابط السلوكية نفسها التي يتحلى بها نظيره المحارب من البشر. وهنا يتساءل الباحث عن المشاعر الإنسانية التي يتحلى بها محارب اليوم, لتكون قدوة للمحارب الآلي الذي ينظر إليه العلماء, متناسين المجازر الرهيبة التي اقترفت بأيدي الجيوش النظامية, وكأنهم أمام صحوة ضمير مفاجئة تنتابهم ولا ترتاح ضمائرهم لأنّ الروبوتات لا مشاعر لديها, , لكن طغيان الحروب والمنافسة على المصالح أمات هذه المشاعر في نفوسهم وأعمى أبصارهم وبصيرتهم عن وحشية ماتقترف أيديهم من جرائم تتطور مع تطور فكر العلماء ووحشية المستخدمين لأفكارهم.

تطور الإنترنت وحروب المستقبل

إن أعظم اكتشاف ظهر في مسار الحرب الإلكترونية كان ظهور "الإنترنت" وانتشاره في العقد الأخير من القرن الماضي؛ فلقد توقع الخبراء في مجال الإنترنت أن أي اعتداء عسكري أو إرهابي قد يحدث ضد الولايات المتحدة الأمريكية في حال

وقوعه، لن يكون باستخدام طائرات أو متفجرات كما حدث في 11 سبتمبر أو حتى انتهاك للحدود الأمريكية، بل سيكون هجوما في الفضاء الإلكتروني يشنه قراصنة الكمبيوتر، بحيث يكون قادرا على تدمير الاقتصاد والبنية التحتية الأمريكية بنفس القوة التي قد يتسبب بها تفجيرمدمر (www.marefa.org/index.php).

ورغم صعوبة هذا التصور للوهلة الأولى, إلا أن الولايات المتحدة بدأت بالفعل في استخدام هذا السلاح للهجوم والحماية, وفي نفس الوقت يعكف الخبراء في وزارة الدفاع الأمريكية "البنتاجون" حاليا على تطوير قدرات الإنترنت لشن هجوم على أنظمة الحاسبات التابعة للدول الأخرى، وفي مقالته عن الحرب العالمية الإلكترونية 2011م, أشار دكتور حداد إلى أن بعض المسئولين العسكريين رفيعي المستوى يدفعون البنتاجون للمضي في الهجوم الإلكتروني عبر تطوير قدرات الإنترنت لشن هجوم على أنظمة الدول الأخرى الإلكترونية بدلا من التركيز على الدفاع عن الأمن الإلكتروني الأمريكي فقط. وهذا حسب رأي بعض العسكريين, سيمنحهم القدرة على التعرف على استخدام هذه التكنولوجيا للاستيلاء على طائرات العدو من دون طيار وشل قدرة طائرات العدو الحربية أثناء القتال، وقطع الكهرباء عن بعض المواقع الاستراتيجية. ولكن الاستراتيجية العسكرية الأمريكية لعمليات الإنترنت التي رفع عنها السرية العام الماضي، أثارت نقاشاً في البنتاجون مجددا وأعطت الجيش الضوء الأخضر للدفع نحو توسيع القدرات الإلكترونية, كما قال مايكل وين وهو مسؤول أمريكي سابق في القوات الجوية: "مع مرور الوقت سيكون عالم الإنترنت جزءا مهما من تكتيكات الحروب"(http://www.arabic-military.com)

وهكذا أصبحت القرصنة الإلكترونية حرباً يومية, و ليست مجرد عمليات عشوائية تتم بدافع الفضول، بل أصبحت جريمة منظمة ومتخصصة تعتمد على أحدث الوسائل

والبرامج للدخول إلى الأنظمة الإلكترونية وسرقة محتوياتها، وهذا ما قاد إلى نشوب حرب الفضاء الإلكترونى الباردة بين أمريكا والصين, التي تمثل اختبارا للعلاقات الثنائية بين البلدين خاصة أن الأعوام القادمة يرجح أن تشهد مزيدًا من عمليات القرصنة الإلكترونية التي تمهد لاشعال سباق حربي إلكتروني حول من يتزعم هذا المجال ومن يكون الرائد فيه، وكل المعطيات تشير إلى بداية الحرب الباردة هذه(اللواتى 2013م).

ولذلك أعلنت الصين عن إنشاء "الجيش الأزرق" وهى إدارة خاصة بجيش التحرير الشعبي الصيني، من أجل حماية الفضاء الإلكتروني الخاص بالجيش على شبكة الإنترنت، والعمل على زيادة مستوى أمن شبكة القوات المسلحة الصينية, والتي أولتها اهتماما بالغا وأصبحت موضوعا ساخنا للمناقشة بين المتحمسين وأصحاب الخبرات من العسكريين، ودخل هذا السلاح الجديد إلى كل دول العالم تقريبا، واستخدامه بالتأكيد متفاوت من حيث التقدم والتأخر بحسب تقدم وتأخر الدولة الراعية(موقع اليوم السابع المصري الإخباري).

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

- **حروب الإنترنيت هي حروب لاتماثلية** (Asymmetric): (J.William 2010p.98). تتميز بالتكلفة المتدنية نسبيا للأدوات اللازمة لشن مثل هذه الحروب بمعني أنّه ليس هناك حاجة لدولة ما مثلا أن تقوم بتصنيع أسلحة مكلفة جدا كحاملات الطائرات ومقاتلات متطورة لفرض تهديدٍ خطيرٍ وحقيقي على دولة مثل الولايات المتّحدة الأمريكية وتتصف بما يلي:

– **فشل نماذج "الردع" المعروفة:**(Martin C. Libicki, 2009, p:39) يعد مفهوم الردع الذي تمّ تطبيقه بشكل أساسي في الحرب الباردة غير ذي جدوى في حروب الإنترنت.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. وبعض الحالات قد يتطلّب 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، فانه في هذه الحالة لن يكون لديهم أصول أو قواعد حتى يتم الرد عليها.

– **المخاطر تتعدى استهداف المواقع العسكرية:** لا ينحصر إطار حروب الإنترنت 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 يمكنه إحداث أضرار مادّية حقيقية تؤدي إلى انفجارات أو دمار هائل.وتشير بعض التقارير إلى تزايد أعداد الهجمات الإلكترونية التي تتم في العالم اليوم, والتي تقوم بها مجموعات أو حكومات تتدرج في مستويات الاستهداف من أبسطها إلى أكثرها تعقيدا وخطورة.ففي ديسمبر/كانون الأول من العام 2009، نشرت الحكومة الكورية الجنوبية تقريرا عن تعرضها لهجوم نفّذه قراصنة كوريّون شماليون يهدف لسرقة خطط دفاعية سريّة تتضمن معلومات عن طبيعة التحرّك الكوري الجنوبي والأمريكي في حالة نشوب حرب في شبه الجزيرة الكورية.وفي يوليو/ تموز 2010، أعلنت ألمانيا أنّها واجهت عمليات تجسس شديدة التعقيد لكل

من الصين وروسيا كانت تستهدف القطاعات الصناعية والبنى التحتية الحساسة في البلاد ومن بينها شبكة الكهرباء التي تغذي الدولة.(Guardian Newspaper, 3 , Feb. 2010)

ويؤكد الخبراء أنّ الهجوم الإلكتروني الذي استهدف أستونيا في العام 2007، يكاد يكون الهجوم الإلكتروني الأول الذي تم على هذا المستوى، فتمّ تعطيل المواقع الإلكترونية الحكومية والتجارية والمصرفية والإعلامية وسبب خسائر بعشرات الملايين من الدولارات, إضافة إلى شل البلاد وإيقافها عن العمل. وعلى الرغم من أنّ الشكوك كانت تدور حول موسكو, على اعتبار أن الهجوم جاء بعد فترة قصيرة من خلاف أستوني–روسي كبير، إلا أنّ أحدا لم يستطع تحديد هوية من قام بالفعل حقيقة, أو مصدر الهجوم الذي حدث، وهذا من المصاعب والمشاكل التي ترتبط بحروب الإنترنت إلى الآن(Bruno, 27 Feb. 2008)

إن من شأن التلويح بقدرات الهجوم عبر الإنترنت أن يؤدي إلى ثلاثة أمور(ليبيكي, 2014,ص 14):إعلان القدرات, الإيحاء بإمكانية استخدامها في ظرف معين, وإيضاح أن مثل هذا الاستخدام سيسبب الأذى بالفعل.

أسلحة وتقنيات عسكرية مستقبلية

تستعرض (سلامة:2006م)ما يجري تطويره في المؤسسات العسكرية والعلمية في الدول المتقدمة، خصوصاً الولايات المتحدة الأمريكية، من أسلحة ومعدات متقدمة جداً في مجال الروبوتات والنانوتكنولوجي والليزر والفضاء والمعلومات والموجات الكهرومغناطيسية والتقنية الحيوية. ففيما يتصل بحقل الروبوت (الإنسان الآلي) فإن المخططين العسكريين يعتبرون هذه التقنية أول صورة من صور حروب المستقبل،

وينظرون إليها باهتمام خاص لاستخدامها في الحفاظ على حياة الجنود والقادة في ميدان الحروب.

ومن أسلحة المستقبل (http://defense-arab.com/vb/threads) استخدام الموجات الكهرومغناطيسية كي تلحق الضرر بالإنسان والأشياء المحيطة به وشل حركة العدو وذلك عبر استخدام نبض كهرومغناطيسي قوي جداً, وتعتبر هذه التقنية العالية إحدى أسلحة المستقبل لدى كلٍّ من الولايات المتحدة الأمريكية وروسيا والصين وبريطانيا والمانيا وهولندا وفرنسا وإيطاليا. وكذلك استخدام ما يطلق عليه تكنولوجيا النانو,إضافة إلى سلاح البلازما الأحدث في المجال العسكري والذي يعتمد على حزمة من البلازما لها كتلة يمكنها التحرك في الفضاء كالبرق، وتتولد البلازما على شكل طاقة مركزة بواسطة موجات المايكروويف أو بأشعة الليزر إلا أنها أبطأ من شعاع الليزر ومن موجات المايكروويف، لكنها تسبب أضراراً أكبرمن غيرها وتسعى القوات الأمريكية إلى تطوير هذه التكنولوجيا وتشجع البحوث العلمية الجديدة في هذا المجال للمحافظة على تفوقها العسكري، كما تسعى روسيا إلى تطويرهذا السلاح الجديد

من خلال هذه النظرة السريعة لأسلحة وتقنيات المستقبل, يحاول الباحث بيان دور أسلحة المستقبل باستخدام تكنولوجيا المعلومات في حروب الفضاء ودورها في تحقيق الأهداف بطرق مختلفة عن الطرق التقليدية المتعارف عليها.

الفيروسات الإلكترونية.. حروب العالم المقبلة

يخوض العالم منذ سنوات حروباً «فيروسية» خرجت من دائرة الخيال العلمي والحروب التقليدية، إلى عالم التقنيات الإلكترونية, وحوّلت الحواسيب إلى جواسيس أشد فتكاً

وأكثر أمناً وأقلّ خسائر في الأرواح. في المقابل أصبح الأمن الإلكتروني هدفاً تسعى إليه الدول عبر تأسيس برامج متطّورة لردّ التهديدات وتحصين الشبكات، إذ يتوقّع أن تصل قيمة سوق الأسلحة الإلكترونية والأمنية إلى 100 مليار دولار بحسب شركة نورثروب كينت شنايدر، في حين ستُنفق الولايات المتّحدة وحدها أكثر من 10,5 مليار دولار على الأمن الإلكتروني بحلول العام 2015، وتُضاعف عدد خبراء الحرب الإلكترونية لديها البالغ عددهم 14 ألف خبير.(عطوي:2012م)

وفي تقرير أمني أعدته شركة مكافي يقول(ديفيد لي,2012م) إنّ إسرائيل وفنلندا والسويد تصدّرت استطلاعاً يقيس مدى جاهزية الأجهزة الأمنية في العالم في التعامل مع التهديدات والهجمات الإلكترونية، وأبهرت هذه الدول الخبراء، مع الإشارة إلى تعرّض إسرائيل لأكثر من 1000 هجوم إلكتروني كلّ دقيقة، ووضع التقرير الصين والبرازيل والمكسيك ضمن قائمة أقلّ الدول في مجال الحماية الأمنية ضدّ الهجمات الإلكترونية.

واختتم التقرير بتوصية تشير إلى أهمية تبادل المعلومات بشكل كبير بين الدول على مستوى العالم للتحصّن من التهديدات الإلكترونية قبل حدوثها, واقترح التقرير أيضا تطبيق تشديد قوانين الجرائم الإلكترونية العابرة للحدود. وجاءت كل من بريطانيا والولايات المتحدة وألمانيا وأسبانيا وفرنسا في مراكز متقدمة من التقرير الأمني.

وجاءت هذه التصنيفات بناءً على إدراك الخبراء لمدى تأهب الدول أو قدرتها على مواكبة عدد من المخاطر والهجمات الإلكترونية. ويقول راج ساماني كبير موظفي شركة مكافي للتكنولوجيا: "إن موضوعية التقرير هي أكبر قوة له. وما يقدمه التقرير هو إدراك هؤلاء الخبراء لمدى التأهب الأمنى والعمل في مجال الأمن الإلكتروني

بشكل مستمر ".وأضاف بقوله:" يتواصل المجرمون الإلكترونيون فيما بينهم عبر العديد من الدول المختلفة. وهم يختارون دولاً يعلمون جيداً أنها لا تتعاون بشكل جيد مع الدول الأخر, كما أن الشركاء الأشرار يتبادلون المعلومات, ونحن نحتاج أن نقوم بالمثل أيضا."(ديفيد لي,2012م)

الفضاء الإلكتروني – الإيجابيات، والسلبيات، وسبل التصدي للمشكلات

وفي مقالها عن الفضاء الإلكتروني تحدثت مجلة الناتو(review/docu/int.nato.www/2013)عن طبيعة الفضاء الإلكتروني والتوجهات الدولية لاستثمار هذا الفضاء في الأغراض العسكرية وما هي السلبيات والإيجابيات المتوقعة, إضافة إلى سبل التصدي لها ,واعتبرت أنه عندما وقعت أحداث الحادي عشر من سبتمبر 2001، كانت أعداد مستخدمي الإنترنت لا تتجاوز 513 مليون مستخدم "لا تتجاوز نسبة 8% من سكان العالم". وقد أدت أحداث سبتمبر 2001, إلى القيام بعمليات عسكرية في أفغانستان, ولا تزال مستمرة حتى يومنا هذا. لكن أعداد مستخدمي الإنترنت في عالمنا اليوم أصبحت تتجاوز 2,7 مليار مستخدم " أو ما يعادل 39% تقريبًا من سكان العالم", وغني عن القول أنه لو تم شن هجوم إلكتروني في عام 2001 فإنّه كان سيشكل عملاً مضادًا، لكن لم يكن له أدنى تأثير

على أكثر من 90 بالمائة من سكان العالم. ولكن الحال لم تعد كذلك في وقتنا الحاضر, ومثلما استخدم منفذو هجمات الحادي عشر من سبتمبر أساليب مبتكرة، يجد الإرهابيون الشغوفون بالوسائل المبتكرة في عالمنا اليوم في الفضاء الإلكتروني مجالاً حافلاً بالثغرات التي يمكن استغلالها, وبناء عليه يتساءل الباحث : هل الفضاء الإلكتروني بإيجابياته وسلبياته يقودنا إلى مواجهة من نوع آخر, مواجهة لاتفرق بين عدو وصديق, مواجهة لا تقبل القسمة على اثنين, مواجهة المنتصر غير آمن , والمهزوم فيها دائما مقاوم ؟

بناء على ذلك هل نحن أمام حرب إلكترونية؛ يقول جوناثان ماركوس مراسل بي بي سي للشؤون الدبلوماسية(arabic/uk.co.bbc.www), تتزايد المخاوف من أن تقع أجهزة الحواسيب في الولايات المتحدة فريسة لهجمات قرصنة، شأنها في ذلك شأن كل أنظمة الدعم الإلكتروني التي يعتمد عليها المجتمع الحديث. كما أن الرئيس الأمريكي أوباما كان قد حذر في خطاب عن"حالة الأمة"، من وقوع مثل تلك الهجمات.

وقال: "نحن نعلم أن هناك مجموعة من قراصنة الإنترنت تقوم بسرقة الحسابات الإلكترونية للناس، ويمكنها التسلل إلى بريدهم الإلكتروني الخاص, كما ندرك أيضا أن بعض الدول والشركات تتلصص لمعرفة أسرارنا الداخلية. ويعمل أعداؤنا الآن للوصول إلى ما يمكنهم من تهديد شبكات الطاقة، ومؤسساتنا المالية، وأنظمة المراقبة الحيوية لدينا".

لذلك فإن البعض يعتقد أن التهديد الإلكتروني الذي قد أصبح شديد الخطورة هو أن لغة قراصنة الشبكة مدمرة, إلا أن توماس ريد، وهو محاضر في قسم دراسات الحروب

بكلية "كينغز لندن"، له نظرة أخرى حول مدى إمكانية وقوع ذلك الخطر، ويحمل عنوان كتابه الجديد اسم "الحرب الإلكترونية لن تحدث, ويرى أن الحديث عن وقوع سيناريو هجمة إلكترونية عارمة أمر مبالغ فيه. وقال: "إذا ما تحدثت إلى بعض المسؤولين في البنتاغون، فمن الممكن أن يعترفوا أن مثل تلك التصريحات مبالغ فيها، حيث إنها مفيدة للأغراض السياسية، وذلك للضغط على الكونغرس من أجل تمرير قانون الأمن الإلكتروني(arabic/uk.co.bbc.www)

لذا، فإن المخاوف من حدوث هجمة إلكترونية مدمرة دفعت الولايات المتحدة لتعزيز دفاعاتها، ويعمل البنتاغون على تكليف 4000 من موظفيهم لمجابهة تلك الهجمات الإلكترونية, كما وقع

طلب رئاسي من شأنه أن يعمل على حماية البنية التحتية الأساسية في الولايات المتحدة من هجمات قراصنة الإنترنت، إذ إنّ مجال الحماية في مواجهة هجمات القرصنة آخذ في الاتساع بطريقة تتنافس فيها الشركات الخاصة والعسكرية على الاستئثار بالنصيب الأكبر, ويرى الباحث في هذا الشأن أن التهويل المبالغ فيه له أسبابه داخل الولايات المتحدة , لكن التقليل من شأنه إلى حد الركون إلى أن لا خطر محتملاً منه يعد سذاجة أيضا, وهذا يتفق مع ماذكره (مارتن سي ليبيك) في كتابه" التلويح بقدرات الهجوم عبر الإنترنت" عندما تحدث عن بث الخوف والغموض والشكوك في نفوس الأعداء, وبيَن أن حروب الفضاء الإلكتروني على عكس الحروب النووية من حيث إثارة الرعب حيث "إنها غير قادرة على بث رعب حقيقي بصورة مباشرة, بل قادرة على إثارة شبح الشكوك والغموض, ولا سيما في عقول الذين يمكن أن يتساءلوا عما إذا كانت أنظمتهم العسكرية ستعمل عند الحاجة إليها"(ليبيكي, 2014م,ص 28)

الفضاء الإلكتروني وبناء الجيوش الحديثة

اختلف الفقهاء والخبراء العسكريون حول مستقبل الجيوش, وما يمكن أن تكون عليه القدرات العسكرية التقليدية في المستقبل, ويرى الباحث أنهم انقسموا إلى فريقين: فريق مازال يؤمن بالقدرات العسكرية التقليدية, وأن مايشاع حول انحسار دورها لصالح التكنولوجيا والجيوش الإلكترونية ما هو إلا محض تضخيم وتهويل أساسه بث الرعب والخوف لدى الدول التي ليس لها القدرة على اللحاق بالقدرات العسكرية التقليدية وغير التقليدية للدول المتقدمة, حتى لا تتجه نحو التصنيع الإلكتروني أو البحث والتطوير فيه, وهو أقل كلفة ولا يحتاج إلى ما تحتاجه القدرات العسكرية التقليدية أو غيرها للوصول إلى ما يسمى توازن القوى.

بينما يتجه الفريق الثاني إلى تأكيد أن دور الجيوش التقليدية قد أخذ في الانحسار وأن الجيوش الإلكترونية قادمة لامحالة في تصدر الموقف في ساحات الحروب القادمة والتي ستكون في الفضاء , والذي من شأنه أن ينعكس على سكان الأرض سلبا ,من حيث تعطيل سبل الحياة المتقدمة والرفاهية اللامتناهية, والتي قادت معظم شعوب الأرض للاعتماد عليها, ونسي هؤلاء أن حروب الفضاء القادمة باستخدام التقنيات الإلكترونية ستحرمهم مماهم فيه بضغطة زر.

ويميل الباحث للأخذ بالرأي الثاني على اعتبار ماكان من استخدامات تقنية إلكترونية عالية الدقة وما نتج عنها بعد استخدامها, وما سيكون عليه الحال في المستقبل إذا ما استمر العالم نحو تطلعاته للسيطرة على الفضاء الكوني بعدما سيطر على الأرض

ومن عليها واستطاع أن يبني مخزونا هائلا من المعلومات القيمة عن طريق الرصد والتنصت والتجسس.

فكيف سيكون عالم الغد وجيوشه في ظل هذا التقدم التقني المستمر, وهل ستحل جيوش الروبوتات محل الجنود الحقيقيين, وهل ستكون الحرب الإلكترونية القادمة ساحتها فضائية وأرضية ؟ وهل باستطاعة الأفراد الانخراط في هذه الحرب؟

نعم هناك من يقول أنّ باستطاعة مجموعة من الأشخاص ذوي المعرفة والخبرة والمتمرّسين والمزودين بالمتطلبات الأساسية, استهداف بعض القطاعات التي تستهدفها الحرب الإلكترونية وتحقيق بعض ما يمكن أن تحققه الحروب الإلكترونية أيضا، إلا أنّ الفارق كبير بين الحالتين: فمجال الحرب الإلكترونية أرحب من أن يتولاه مجموعة أشخاص, والقطاعات المستهدفة أكبر والأضرار الناجمة أضخم والقدرات المستخدمة هائلة، وهي لا تتوافر إلا لدول بعينها لديها القدرة والقابلية على استثمار مواردها في هذا الإطار واستخدامها فيه.

لذلك ينشط العديد من الدول ولا سيما الصين وروسيا والولايات المتّحدة الأمريكية وفرنسا وانكلترا وإسرائيل وبعض الدول من الصف الثاني والثالث كالهند وباكستان وكوريا الشمالية وإيران بصورة غير معلنة, لتطوير قدراتها في الحرب الإلكترونية وبناء جيوش من الخبراء الذين قد يشكّلون مستقبلا نواة الجيش الإلكتروني للدولة.

لذلك فعندما يتحدث أخصائيو حرب الفضاء الإلكتروني الأمريكيون عن "الصراع الأكبر" فإنهم يعنون دائما الصراع في الفضاء الإلكتروني مع روسيا أو الصين, وهما الدولتان الوحيدتان بخلاف الولايات المتحدة، اللتان تملكان قدرات هجومية متطورة في

هذا المجال, إن التفكير في حرب الفضاء الإلكتروني بغرض فهمها لا يزيد احتمال وقوعها(كلارك,و نيك 2012,ص 215).

ولأنّه ليس هناك قانون يحكم عمل أو يحدد إطار الحرب الإلكترونية في الفضاء الإلكتروني، فإنّ 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 والصينيّون، 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 أستونيا ربيع عام 2007 وجورجيا صيف عام 2008. أمّا الصينيون فقد شنوا العديد من الهجمات الشرسة المعروفة حتى اليوم في مجال التجسس لعل أهمّها محاولات اختراق البنتاغون في العام 2007. انظر (blogs.com.weeklystandard.www)

الإجراءات الدفاعية

تقوم العديد من الدول خاصة تلك التي تعتمد على الإنترنت وعلى الشبكات والمعلوماتية بتطوير قدراتها الدفاعية إلى جانب امتلاكها قدرات هجومية متطورة،ذلك لكون الدولة الأكثر اعتمادا على استخدامات شبكات الإنترنت هي الأكثر عرضة للنتائج الكارثية لأي حرب إلكترونية تشن على مستوى عالٍ ودقيق. ولأن الأفضلية في

حروب الإنترنت هي للمهاجم عادة وليس للمتحصّن، أو المدافع, ولإن ميدان حروب الإنترنت هو ميدان لا تماثلي أو لا تناظري، فإن بعض الدول قامت ببناء استراتيجياتها الدفاعية من خلال التحصين الإلكتروني ومثال ذلك ما قامت به كل من:

- انجلترا: وقامت على سبيل المثال بإصدار استراتيجية الأمن الإلكتروني القومية في حزيران/يونيو 2009(www.cabinetoffice.uk.gov)، كما قامت انجلترا بإنشاء وحدة الأمن الإلكتروني ومركز العمليات, ومقرّه وكالة الاستخبارات القومية ، وبدأت عملها فعليا في شهر آذار/مارس 2010.(www .zdnet.co.uk/news/security-threats/2009/11/13/uk-)

– الولايات المتّحدة: بالرغم من كونها الدولة الأكثر امتلاكا للقدرات والتقنيات الهجومية العالية المطلوبة في الحروب الإلكترونية، إلا انّه من الواضح أنّ اهتمامها يتركز على تعزيز القدرات الدفاعية في هذا المجال. وكونها الدولة الأكثر اعتمادا في العالم على شبكات الإنترنيت و في مختلف القطاعات المدنية والعسكرية, فإن اهتماما بالجانب الدفاعي فيما يتعلق بالحروب الإلكترونية كان كبيرا مقارنة بالدول الأخرى. ففي أيار/مايو 2009، صدّق البيت الأبيض على وثيقة "مراجعة سياسة الفضاء الإلكتروني" (www.whitehouse.gov/assets/documents)التي قدمت من قبل لجنة خاصة إلى الرئيس الأمريكي أوباما، وهي تلخّص الخطوات الواجب على الولايات المتّحدة اتّباعها للبدء في تفعيل الأمن الإلكتروني ومتطلّباته الأساسية والأوّلية.كما كشفت وكالة الاستخبارات المركزية الأمريكية, عن مبادرة جديدة لمحاربة الهجمات

الإلكترونية وضعت من خلالها الخطط العريضة المناسبة لخمس سنوات قادمة.(www.cia.gov/news-information)

وفي مايو/أيار 2010, قامت الولايات المتّحدة بإنشاء قيادة الإنترنت "سايبركوم" وعيّنت الجنرال كيث أليكساندر– مدير وكالة الاستخبارات القوميّة – قائدا عليها مهمته تأمين حماية الشبكات العسكرية الأمريكية على الدوام.(The Economist, July 3rd, 2010, p:25). وقد بدأت هذه القيادة عملها الفعلي في الأول من تشرين الأول/أكتوبر 2010 , بعد أن تمّ الإعلان عن ضرورة إنشائها في عهد الرئيس أوباما في العام 2009، و ضمت 1000 فرد من نخبة القراصنة والجواسيس المحترفين والمميزين إلكترونيا(www.rawstory.com)،

وتشير بعض التقديرات إلى أنّ الولايات المتّحدة بحاجة إلى قوة تعدادها حوالي 20 إلى 30 ألف فرد لهم نفس المميزات والصفات,لضمان تنفيذ المهام الدفاعية الإلكترونية على أفضل وجه لحماية كافة منشأتها الحيوية .(http://www.npr.org/templates/story/story.php?)

وإذا كانت معظم الدول تعمل على تطوير قدراتها الهجومية في المجال الإلكتروني، فإن الصين وروسيا تعتبر الدول الأبرز في هذا المجال لأسباب مختلفة, فالصين هي من أكثر الدول التي تعمل على تطوير قدراتها الهجومية في المجال الإلكتروني، إضافة إلى أنها من الدول القليلة التي تدمج مفهوم "الثورة في الشؤون العسكرية" , في عقيدتها العسكرية، وخاصة في مجال الحروب الإلكترونية. وتؤكد الورقة الصينية البيضاء المسماة "الدفاع القومي" للعام 2006 على أنّ الهدف الرئيسي من بناء

الجيش الحديث، هو جعله قادرا على كسب الحروب المعلوماتية بحلول منتصف القرن ال 21. وهو الأمر الذي أكدته ورقة عام 2009.(Solan 2010 : 8p).

ولأن الصين ليست على المستوى العسكري لكل من أمريكا وروسيا، فهي تحاول على الأرجح استغلال البُعد الإلكتروني لتطوير قدراتها "اللاتناظرية" أو "اللاتماثلية" لتحقيق تفوقها في هذا المجال, وبالتالي ضمان قدرات رادعة تتيح لها توفير مزيد من الوقت اللازم لبناء قدراتها التقليدية من جهة، وتتيح لها أيضا اكتشاف نقاط ضعف خصومها في المجال الإلكتروني للتركيز عليها من جهة أخرى.(4p 2009 (Shackelford,

أما روسيا فتتبنّى كذلك تطوير قدراتها في الحرب الإلكترونية خاصة في الشق الهجومي، واتهمت بأنها تقف وراء العديد من الحالات الهجومية المشهورة , دون أن يكون هناك دليل مادي قوي على ذلك. لكن الواضح أنّ روسيا ومنذ انهيار الاتحاد السوفيتي, تعتمد على وسائل ذات كلفةأقل ولكنها أكثر فاعلية في مواجهة الولايات المتّحدة وحلف شمال الأطلسي؛ إذ تعتبر القدرات اللاتناظرية أو اللاتماثلية, ومن ضمنها الحرب الإلكترونية, إحدى أهم وسائل المواجهة التي تستخدمها, في ظل التفوق العسكري للناتو وواشنطن.(Shackelford, 2009 5p)

من خلال ما تقدم يرى الباحث أن جميع الإجراءات التي اتخذتها الدول المهتمة بهذا النوع من الحروب أو الإجراءات التي ستتخذها, ما زالت تفتقر إلى قوة الردع, وأنها مازالت مكشوفة لهجمات العديد من الدول وخاصة الولايات المتحدة الأمريكية، ولعل حالات التنصت على زعماء الدول الأوروبية والدول الصديقة شكلت صدمة مذهلة

لهذه الدول, وهي التي تعتبر نفسها دولاً حليفة , وأنها في مأمن من أن تتلقى أجهزتها هذا النوع من التجسس ومن أقرب حلفائها.فإذا كان هذا الوضع بالنسبة للدول الحليفة , فكيف هو بالنسبة للدول غير الصديقة أو التي في حالة عداء مع الولايات المتحدة؟

وهذا يتفق مع ما ذهب إليه كل من ريتشارد كلارك وروبرت نيك في كتابهما " حرب الفضاء الإلكتروني –التهديد التالي للأمن القومي وكيفية التعامل معه" عندما ذكرا أنّ تقنية المعلومات تتطور بمعدل أسرع من تقنية أمن نظم المعلومات, وأن أمن ونظم المعلومات والشبكات هو التحدي الأمني الأساسي في هذا العقد أو القرن القادم, إضافة إلى عدم وجود وعي كاف بالمخاطر الجسيمة التي نواجهها في هذا المضمار.(كلارك, و نيك2012م, ص 132).

وحتى تتغلب الولايات المتحدة على هذا القصور في أمن نظم المعلومات , وحتى تبقى متفوقة على خصومها وحلفائها في نفس الوقت , يعرض الباحث هنا مختصرا لما قامت يه الولايات المتحدة من تجسس تجاه حلفائها, وردة الفعل الدولي على ذلك, إضافة إلى التبريرات الأمريكية لما حصل, مما يشكل لدى الباحث قناعة مفادها أن الاستراتيجية الكونية الأمريكية, استراتيجية ميكافيلية, لا تستثني أي أسلوب يمكن استخدامه إذا كان الهدف منه تحقيق مصالحها، رغم الحرج الشديد الذي رافق اكتشاف عمليات التنصت على هواتف زعماء العالم وإن دل هذا على شيء, فإنما يدل على أن الولايات المتحدة لا تعترف إلا بمصالحها, وأن ما يقال في العلاقات الدولية عن العلاقات الحميمية والصداقة المتينة شيء, والمصالح شيء آخر. لذلك لابد أن يدرك الجميع أن علم السياسة لايعترف بصداقات دائمة, أو عداوات دائمة؛

الشيء الثابت في علم السياسة أنها متغيره, المهم وفي المحصلة النهائية هي المصالح ولا شيء غير المصالح.

إن قيام الولايات المتحدة بتجسسها عبر جهاز استخباراتها (C.I.A), على 35 دولة من دول العالم, بينهم الكثير من زعماء دول العالم الأول, كالتجسس على المستشارة الألمانية أنجيلا ميركل, والرئيس الفرنسي السابق ساركوزي وعلى خلفه الحالي أولاند, ولمدة تزيد على سبع سنوات ومنذ عام 2006, يعني في الحسابات الاستراتيجية الأمريكية وحسب رأي الباحث أن لاخطوط حمراء تقف أمام هذه الإستراتيجية الكونية لأمريكا, على اعتبار أن الفضاء الكوني ومساحاته الجغرافية الاقتراضية, لابد أن تكون في مجملها منطقة تحت السيطرة والمراقبة الإلكترونية الأمريكية وأن لا ينازعها عليها أحد , وإن قامت إحدى الدول أو بعض منها بالعمل لدخول مضمار المنافسة , كان لابد أن تكون تحت الرقابة الإلكترونية الأمريكية. حتى وإن وصل الحال للتنصت على مكالمات زعمائها.

ويرى الباحث أن هذا ساعد وبشكل مباشر على ظهور الجريمة الإلكترونية, والتجسس الإلكتروني , والاقتراب من شبح الحرب الإلكترونية, لذلك تحاول دول عدة أن تراقب وتتدخل وتسيطر على شبكة المعلومات وتدفقها في فضائها الجغرافي وربما تمتد إل فضاءات جغرافية دولية أكبر, وبذلك تنازع الولايات المتحدة سيطرتها على هذا الفضاء. وهذا ما ذهب إليه روبرت كينك في حديثه عن دور الدولة في مواجهة مصممي الإنترنت الذين سعوا للحد من دور الحكومات في تصميم الشبكات وعملها وإدارتها, مما يسمح للإنترنت أن يتطور وينمو ليشمل المشهد الدولي دون مشاركة

حكومية, وكان موقف أمريكا يقوم على أن دور الحكومات في إدارة الشبكة يجب أن يبقى محدودا(كنيك, 2011,ص 13).

ما يدعو للتدبر في الوثائق التي كشفها المحلل الاستخباراتي السابق لدى وكالة الإستخبارات الأمريكية إدوارد سنودن (عوض الله, 2013م), أن وكالة الاستخبارات الأمريكية في تجسسها على 35 دولة وعلى العديد من الزعماء, كانت تفرض بالأمر على المسؤولين البارزين في مواقع مختلفة في الإدارة الأمريكية, كالبيت الأبيض والبنتاجون, والوكالات الحكومية, وتأمرهم بأن يقدموا لوكالة الاستخبارات الأمريكية مالديهم من أرقام هواتف تخص السياسيين حول العالم, لإضافتها إلى قاعدة بيانات الوكالة. وقدم حسب الوثيقة المنشورة أحد المسؤولين الأمريكيين البارزين أكثر من 300 رقم هاتف من بينها أرقام ل 35 من زعماء العالم, وفورا تم تكليف موظفين في C.I.A, بمراقبة إتصالات هذه الأرقام. والأشد خطورة حسب الوثيقة أن تاريخها يعود إلى عام 2006 م, مما يعني أن التجسس كان قائما قبل ذلك بكثير.

اللافت للنظر في هذه الأمور كلها هو ردة الفعل الصادرة عن الخبراء الأمنيين الأمريكان, ويمكن ملاحظة ذلك في ماكتبه" إيفودالدر", رئيس مجلس شيكاغو للشؤون العالمية, وكان أيضا سفيرا للولايات المتحدة الأمريكية لدى حلف الناتو من 2009م-2013م, في جريدة الفايننشال تايمز, تناول فيه قضية التنصت الأمريكي على الزعماء الأوروبيين وقال:" إن من حق الحكومات جمع المعلومات حول أنشطة وأفكار الحكومات الأخرى , حتى في الدول الصديقة والحليفة, كما أنها مهمة يقوم بها الدبلوماسيون لمساعدة حكوماتهم في فهم ما يحدث في البلدان التي يخدمون فيها". ويطرح دالدر التساؤل التالي بقوله:" السؤال لاينصب على ما إذا كان ينبغي أو

لاينبغي للحكومات جمع المعلومات بعضها عن بعض, فهي تفعل ذلك, وينبغي لها أن تفعله. كما أنها تجمع المعلومات عن الدول الصديقة وغيرها, ويجب أن تفعل ذلك, لكن السؤال هو ما إذا كان التنصت على هواتف الرؤساء هو الوسيلة الأكثر فاعلية وجدوى, وما إذا كانت تكلفة اكتشاف الأمر للرأي العام تستحق كل هذا العناء (صحيفة الشروق, 7نوفمبر 2013م).

وفي هذا السياق قال" جوناثان لورانس", الأستاذ المساعد في العلوم السياسية في بوسطن كوليدج والمتخصص في العلاقات الأميركية الألمانية :«إن علينا مسؤولية تقديم اعتذار صادق وطمأنة حقيقية، ولكن لا يمكننا أن نغفل حقيقة أننا لسنا العدو وأن لديهم أعداء... يجب علينا ألا نغفل أن الدول الأوروبية ليست تابعة لنا ولكنها بدرجة ما خاضعة لحمايتنا... نحن نوفر مظلة أمن على امتداد العالم ومصالحنا تتداخل كثيراً مع مصالحهم«(صحيفة الإتحاد الإماراتيه2013/11/22).

وقد عبرت ألمانيا وفرنسا عن رفضهما للممارسات المزعومة لعمليات التجسس الأميركية وجمع المعلومات واسع النطاق الموجه ضدهما، مما دفعهما إلى إرسال وفودٍ استخبارية من البلدين بسرعة إلى واشنطن لمعالجة القضية والسعي للتوصل إلى ما وصفه "فرانسوا أولاند" بأنه «ميثاق شرف» جديد للعمل الاستخباراتي (صحيفة الإتحاد الإماراتيه2013/11/22). وكذلك قالت أشيلي ديكس, أستاذ القانون في جامعة فيرجينيا، "إن إحدى السلبيات الكبيرة لدخول الولايات المتحدة في اتفاق استخباراتي ملزم مع ألمانيا ستكون إرساء سابقة قد تدفع دولاً أخرى للسعي إلى اتفاقات مشابهة", مضيفة أيضا " أن الولايات المتحدة لن تخسر معلومات استخباراتية بتوسيع الاتفاقات الملزمة فحسب، بل سيتعين عليها أيضاً أن تفكر في احتمال أن ينتخب بلد مثل ألمانيا في

مرحلة ما حكومة غير صديقة, مما يعقد عمل الحكومات الأمريكية المقبلة ",(صحيفة الإتحاد 2013).

وبرغم كلمات التهدئة الصادرة من البيت الأبيض، يُشكك بعض الخبراء في العلاقات الأمريكية الألمانية, في احتمال أن يبرم أوباما مع ألمانيا أو أي حليف آخر اتفاقاً طويل الأمد مثل المبرم مع بريطانيا, حيث يقول الخبراء "إن هذا صحيح بشكل خاص مع الأخذ في الاعتبار الخلافات المحورية بين ألمانيا وأمريكا، ومنها العلاقات التجارية الألمانية بالصين وإيران والتعامل مع روسيا في ظل قيادة بوتين".(owshart/ralbashee/net.isslamtoday)

وتقول أشيلي ديكس "برغم سلبيات توسيع الاتفاقات الملزمة التي تقيد جمع المعلومات في دول أخرى، فإن تكلفة عدم فعل هذا سترتفع، لأن هناك دولاً تهدد برد أكثر تكلفة مثل تقييد التعاون الاستخباراتي, كما قالت "إن الولايات المتحدة ربما تستطيع تقليص الضرر وتهدئ حدة المخاوف على الجبهة الأوروبية بفرض بعض القيود، ولكن هذا لن يهدّئ غضب دول مثل البرازيل والمكسيك التي يرجح أن تتمسك بالمطالبة بإبرام اتفاقات خاصة بها هي أيضاً مع الولايات المتحدة ".(owshart/ralbashee/net.isslamtoday)

ويرى الباحث أن التجسس الأمريكي رغم الإجراءات الدفاعية والحمائية المتوافرة لدى الدول الصديقة أو المعادية للولايات المتحدة , ما زالت تقف عاجزة عن صد الهجمات التجسسية الأمريكية عليها, وأن الباعث لهذا الحماس لدى الولايات المتحدة في المضي قدما في تجسسها, مرده الرغبة الجامحة لديها في معرفة ماذا يفكر أصحاب الرأي وصناع القرار في هذه الدول, وما هي احتمالات أعمالهم القادمة تجاه قضايا

إقليمية أو دولية , وترى الولايات المتحدة أنها مسائل وقضايا تعنيها وتهمها. وبالتالي تستطيع وضع الخطط اللازمة لمجابهة كل الاحتمالات الممكنة, دون الخوف من الفشل في التنفيذ, كون ما يتوافر لديها من معلوات يشكل تفوقا على الخصم من حيث معرفة مايريده الخصم وما يحاول أن يذهب إليه, مقابل جهله لما تريده الولايات المتحدة أو ما تحاول أن تقوم به.

وهذا ما ذهب إليه أحد مسؤولي الاستخبارات الأمريكية عندما قال:" إن التجسس على قادة أجانب أمر مألوف ". في حين قال مدير الاستخبارات القومية الأميريكية جيمس كلابر في جلسة استماع أمام لجنة الاستخبارات في مجلس النواب لدى استجوابه بشأن العمليات الاستخباراتية التي أثارت سخطا بين الحلفاء الأوروبيين: "أعمل في الاستخبارات منذ 50 عاما، ومعرفة نوايا القادة هو مبدأ أساسي في ما نحاول جمعه وتحليله".وأضاف: أنّ "نوايا القادة تمثل تخوفا أبديا بالنسبة للمعلومات الاستخباراتية، ومراقبة قادة أجانب ليس أمرا جديدا، وهو أحد أوائل الأشياء التي تعلمتها في مدرسة الاستخبارات عام 1963".وأوضح أن الهدف خصوصا هو: "تحديد إذا كان ما يقولونه مطابقا لما يحصل. من الحيوي بالنسبة لنا أن نحدد الاتجاه الذي تسلكه الدول وماهية سياساتها وتداعيات ذلك علينا في سلسلة من المجالات".وتابع أن معظم القلق يأتي من الساسة الذين ربما لا يألفون حجم عمليات بلدانهم الاستخباراتية، مؤكدا أن دولا حليفة مارست أنشطة تجسس على الولايات المتحدة أو قادتها.(http://www.aljazeera.net/news)

ويبدو أن التساؤل المنطقي هنا يكمن في لماذا تتجسس الدول الصديقة بعضها على بعض ولعل العلاقة بين أمريكا وألمانيا، وهما دولتان حليفتان, وحصل ما حصل

بينهما نتيجة التجسس الأمريكي، يقود إلى هذا التساؤل، إلا أن الجواب قد لا يكون معلنا بشكل مباشر لكن مؤشراته تدل عليه، مثل: الخلافات بينهما فيما يتعلق بملف التبادل التكنولوجي مع إيران, و كيفية مواجهة التجسس الإلكتروني الصيني، وأخيرا قيام الولايات المتحدة بالتنصت على الاتصالات في ألمانيا وخاصة التجسس على هاتف المستشارة الألمانية ميركل, يدل دلالة واضحة أن ما ذكر آنفا من خلافات بين أمريكا وألمانيا ليس إلا ذريعة لما فعلته أمريكا من أجل معرفة ما يمكن أن تقوم به ألمانيا في تصرفاتها وسلوكها الدولي.

التجسس الأمريكي وأثره على العلاقات الدولية

لا شك أن ما أسفرت عنه فضيحة التجسس الأمريكي على الدول الحليفة وزعمائها, شكل ضربة قوية للسياسة الدولية, وطبيعة العلاقات الدولية القائمة على مبدأ احترام سيادة الدول, وعدم التدخل في شؤونها أو التجسس عليها, مما أعاد إلى الأذهان مرة أخرى التساؤل الذي يطرح دوما حول المباديء الأساسية التي تقوم عليها العلاقات الدولية, وهل مازالت المصالح تحتل المرتبة الأولى في أجندة الدول في ممارساتها السياسية , أم أن هناك تحولاً جديداً نحو الالتزام بالقواعد والقوانين الدولية التي تحظر الأساليب و الممارسات التي تخترق وتستبيح خصوصيات الدول, كما حصل مؤخرا بالتنصت والتجسس الأمريكي. والظاهر للعيان أن الممارسات السياسية مازالت تتخذ من مقولة ميكافيلي "الغاية تبرر الوسيلة" منهجا متبعا لا يمكن أن تحيد عنه, ففي السياسة الجميع يتجسس على الجميع وفي كل الأوقات: في الحرب وفي السلم، والكل على علم بذلك ولهم قواعدهم في الممارسة, أما المخالفة فيها فإنها تكمن في أن يكتشف الطرف الآخر أنه وقع ضحية هذا التجسس.

لذلك اتسعت قاعدة الدول التي تطالب الولايات المتحدة باستفسارات تخص إمكانية التنصت عليها، التي فجرها الموظف السابق في وكالة الأمن القومي الأمريكية، إدوارد سنودين، بعد اكتشاف عمليات مماثلة على هواتف عدد من قادة الدول، خصوصا في الاتحاد الأوروبي. صحيفة "لوموند" الفرنسية، إلى جانب عدد من المنابر الإعلامية العالمية، خصصت حيزا من أخبارها طيلة الفترة الأخيرة لتداعيات هذه العمليات التي تنذر بأزمات دبلوماسية متبادلة بين واشنطن وعدد من عواصم حلفائها.

أزمة في الأفق بين باريس وواشنطن

قالت صحيفة "لوموند"، إن وكالة الأمن القومي الأمريكية، تجسست على دبلوماسيين فرنسيين في واشنطن وفي الأمم المتحدة، وحصلت الصحيفة على وثائق تثبت استخدام برنامج مراقبة متطور يعرف باسم "جيني"، من قبل وكالة "إن إس آ". وأشارت "لوموند" في تقريرها إلى أن الجواسيس الأمريكيين يقومون بتثبيت برامج تنصت عن بعد في أجهزة حاسوب في الخارج، بما فيها أجهزة في سفارات أجنبية، مؤكدة أن مثل هذه البرامج ثبتت في أجهزة حاسوب بسفارة فرنسا في واشنطن، وفي جهاز حاسوب تابع للبعثة الفرنسية في الأمم المتحدة. وتضيف الصحيفة، في مقالات تحليلية نشرتها الأسبوع الماضي، أن الولايات المتحدة خصصت سنة 2011 ميزانية قيمتها 652 مليون دولار لتوفير برامج التجسس، وشملت العملية عشرات الملايين من الأجهزة، وتبين وثيقة مؤرخة في 2010 أن معلومات سرقت من أجهزة حاسوب لسفارات أجنبية سمحت لواشنطن معرفة مواقف أعضاء في مجلس الأمن من العقوبات على إيران، قبل الإعلان عنها

وقال الرئيس الفرنسي فرانسوا هولاند حسب صحيفة الصباح، إن هذا الأمر "غير مقبول بين أصدقاء وحلفاء"، وطلب استفسارا بشأنه، وأعرب هولاند في اتصال هاتفي مع نظيره الأمريكي باراك أوباما عن "استنكاره الشديد" لما أثير حول تجسس وكالة الأمن القومي الأمريكية على مضامين عشرات ملايين المكالمات الهاتفية لمواطنين فرنسيين، معتبراً أنها "ممارسات مرفوضة" بين الحلفاء، وأضافت الرئاسة الفرنسية في بيان لها، أن هولاند طلب تقديم كل التوضيحات اللازمة، إضافة إلى مجمل المعلومات التي قد تكون في حوزة المستشار السابق في وكالة الامن القومي الأمريكي إدوارد سنودين (www.assabah.press.ma/index.php?)

كما نقلت وكالة الأنباء الفرنسية "أ. ف. ب"، عن مسؤول الدبلوماسية الفرنسية أن هذا النوع من الممارسات بين الحلفاء الذي يحمل جانبا من المس بالحياة الشخصية أمر غير مقبول، مضيفا أنه يجب التأكد في أسرع وقت من أنه لن تتم إعادة مثل هذه الممارسات، مبينا أن باريس قد تفاعلت حتى الآن مع هذه المسألة. وفي السياق ذاته، لوحت مصادر دبلوماسية فرنسية، بأزمة منتظرة في الدبلوماسية القائمة بين باريس وواشنطن.

ولما كانت المعلومات تعتبر جزءا مهما من مفهوم القوة في العلاقات الدولية, لذلك فإن أمريكا تعتبر الدولة الأكثر هوسا بالمعلومات التي تهم الجميع، وتمتلك المؤسسة المخابراتية الأكثر نشاطا وفاعلية في العالم، بل الأكثر اختراقا للحركات السياسية سواء السرية منها كالجماعات الإسلامية بما في ذلك القاعدة وغير السرية كالأحزاب والجمعيات الخيرية، أو الدول والكيانات السياسية الإقليمية.

لذلك يرى الباحث أن المعلومات أضحت بالنسبة للولايات المتحدة الأمريكية بمثابة القوة الناعمة التي تريد أن تنفرد في جمعها عن العالم , لكي تكون على دراية بكل مايمكن أن يحدث على الساحة الدولية.

لذلك نجد أن العديد من مؤسسات وأجهزة التجسس والتنصت الأمريكية لا تتوانى عن عمل ذلك أو الإفصاح عنه خدمة للأمن القومي الأمريكي كما يقولون، ولو على حساب انتهاك خصوصيات الدول والأفراد . وهذا ما نلاحظه في برامج وخطط وكالة الأمن القومي الأمريكي تحت شعار: "أسمعك أينما كنت", واستخدام وكالة الفضاء الأمريكية (ناسا) للتنصت على أحاديث العالم, إضافة إلى وكالة الإستخبارات الأمريكية (C.I.A) , إضافة إلى النظام السري الذي كشف عنه مؤخرا وهو (eXKeyscor) الذي استخدمته أمريكا للتجسس على دول العالم.

وبحسب رأي الباحث فإن الولايات المتحدة لا تعدم الوسيلة في الحصول على المعلومة حيثما وجدت, ولكن ما الذي يمكن أن تقود إليه حرب المعلومات هذه على صعيد العلاقات الدولية, خاصة ونحن نعيش حقبة تراجع أمريكي وانبعاث روسي جديد وتخلخل في العلاقات الأوروبية الأوروبية, والأوروبية الأمريكية, مما يشي بمستقبل جديد من حرب باردة جديدة قد تستعر بين لحظة وأخرى في عالمنا المعاصر.

الخلاصة:

مما تقدم يخلص الباحث إلى أن الجرائم الإلكترونية أصبحت تمثل خطرا كبيرا على استقرار الدول، بعد أن استطاع الإنترنت اختراق جميع الحواجز والقيود التى تسيطر على المجتمعات. ولمواجهه الجرائم والهجمات الإلكترونية يجب تفعيل التعاون الدولى فى العديد من دول العالم من خلال:

-عقد الاتفاقيات الدولية لضبط وتسليم المجرمين.

- إصدار مجموعة من القوانين التشريعية الجديدة الناظمة لاستخدام الإنترنت ولتجريم أي استخدام غير آمن لتكنولوجيا المعلومات والاتصالات.

- التعاون والتنسيق الدائم مع الإنتربول الدولى فى مجال تبادل المعلومات والخبرات الأمنية والفنية.

- رصد ومتابعة كافة الأنشطة الإجرامية والإرهابية، خاصة فيما يتعلق بالنشاط الإرهابى التكنولوجي، نظرا لتزايده المستمر من خلال عناصره الإجرامية المحترفة والمنتشرة فى العالم.

- محاولة تجسير الفجوة بين سرعة تطور تقنية نظم المعلومات وتقنية أمن المعلومات

- متابعة كل مايستجد من تطور في علوم الكمبيوتر والإنترنت, واستحداث وحدات علمية دفاعية مضادة في دولنا العربية لكل ما يهدد أمننا,على غرار" الجيش الأزرق " في الصين,

المراجع:

1. باكير, علي حسين(2011م), " البعد الخامس...الحرب الإلكترونية في القرن ال21 ", انظر الرابط: studies.aljazeera.net/issues
2. بي بي سي العربية(2013م)," بريطانيا تنشيء وحدة جديدة للدفاع الإلكتروني", آخر تحديث الأحد26 سبتمبر/أيلول 2013م, انظر الرابط:
www.bbc.co.uk/arabic/worldnews/cyber-shtml.unit

3. توفلر, ألفن(1990م), " صدمة المستقبل: المتغيرات في عالم الغد", ط2, ترجمة محمد علي ناصيف, تقديم أحمد كمال أبو المجد, القاهرة, نهضة مصر.
4. حداد, فايز (2011م)," الحرب العالمية الإلكترونية ", انظر الرابط:
http://www.assakina.com/news/news1/11414.html
5. الفضاء الإلكتروني – الإيجابيات والسلبيات وسبل التصدي للمشكلات. انظر الرابط:
www.nato.int/docu/review/2013/Cyber/AR/index.htm
6. سلامة, صفات أمين(2006م)," أسلحة حروب المستقبل بين الخيال والواقع", مركز الإمارات للدراسات والبحوث الاستراتيجية
7. عطوي, ثناء(2012م)," الفيروسات الإلكترونية...حروب العالم المقبلة", النشرة الإلكترونية أفق, مؤسسة الفكر العربي, العدد 208, 2012/6/18
8. عوض الله, أسامة(2013م)," من هم الزعماء والرؤساء العرب الذين تجسست عليهم CIA الأمريكية", صحيفة أخبار اليوم السودانية , الأحد 27 تشرين أول 2013م
8. كلارك, ريتشارد, روبرت , نيك(2012م), "حرب الفضاء الإلكتروني: التهديد التالي للأمن القومي وكيفية التعامل معه", أبو ظبي, منشورات مركز الإمارات للدراسات والبحوث الاستراتيجية.
9 . كلابر, جيمس(2013م), "التجسس من أجل الأمن القومي الأمريكي", الجزيرة نت, آخر تحديث الأربعاء, 10/30 /2013 , tnews/twww. aljazeera.ne
10 . كاظم, مصطفى(2007م), " ثورة المعلومات والاتصالات إعادة صياغة عالمنا ",أنظر الرابط:
news.bbc.co.uk/hi/arabic/news/newsid_7166000/7166241.stm
11 . كلارك, ريتشارد, نيك روبرت (2012م),"حرب الفضاء الإلكتروني– التهديد التالي للأمن القومي وكيفية التعامل معه",ط1, مركز الإمارات للدراسات والبحوث الاستراتيجية, أبو ظبي

12 . كينك, روبرت(2011م), "حوكمة الإنترنت في عصر انعدام الأمن الإلكتروني", سلسلة دراسات عالمية, العدد95,ط1, مركز الإمارات للدراسات والبحوث الاستراتيجية, أبو ظبي

13 .اللواتي, نسرين فوزي(2013م),"**الفضاء الإلكترونى حرب باردة جديدة بين أمريكا والصين**"انظر الرابط:http://loghatalasr.ahram.org.eg/NewsContent/5/25/6168/

14 . لي, ديفيد(2012م)," إسرائيل تتصدر تقريرا لجاهزية التعامل مع الهجمات الإلكترونية والصين تتراجع", آخر تحديث , الثلاثاء 31 يناير 2012, انظر الرابط: www.bbc.co.uk/arabic/scienceandtech/2012/.../120131_**israel**_cyber.sht

15 . ليبيكي, مارتن سي(2014م)," التلويح بقدرات الهجوم عبر الإنترنت" سلسلة دراسات عالمية, العدد 12, ط1,مركز الإمارات للدراسات والبحوث,أبوظبي

16 . مقلد, ديانا(2012م)," الحرب الإلكترونية...الجبهة الجديدة",صحيفة الشرق الأوسط, 23ذوالحجة 1433هـ, 8 نوفمبر 2012, العدد 12399

17 www.bbc.co.uk/arabic/scienceandtech/2013/.../130307_cyber_**war**.shtml

16. المجذوب, محمد(2007م)," القانون الدولي العام ", ط6, بيروت, منشورات الحلبي الحقوقية.

17. المركز العربي لأبحاث الفضاء الإلكتروني, "مفهوم الحرب الإلكترونية", أنظر الرابط: www.accronline.com

18. المرهون, عبد الجليل(2012م)," عصر الردع الإلكتروني" انظر الرابط: www.moslimonline.me/?p**age**=articals&id

19. لافرانشي, هاوارد(2013م)," التجسس الأمريكي ... واتفاق العيون الخمس", صحيفة الإتحاد الإماراتية, الأحد 22 تشرين ثاني, 2013م

المراجع الأجنبية

1. Bruno Greg(2008)," The Evolution of Cyber Warfare on foreign relations",27Feb.2008, at the link: www.Cfr.Org/publication cyber-warfare.html-evolution

2. Dunn Kavelty, Myriam(2010)," Cyber War Concept Status Quo",CSS Analysis in Security Policy, CSSETH. Zurich,No71

3. Klarke, Richard, Robert, Knake(2010), " Cyber War", Harber Collins.

4. Lynn, William J.(2010), " Defending a New Domain: The Pentagon's Cyber Strategy", Foreign Affairs, Sept- Oct. 2010

5. Libicki, Martin c.(2009), rand corporation, library of congress, Arlington. VA222o2-5050

6. Panetta, Leon E. CIA Director, Unveils Blueprint for Agency's Future, at this link: https://www.**cia**.gov/news.../press.../press-release-2010/

7. Shackelford, Scott(2009)," Estonia Two-and-A-Half Years Later: A progress Report on Combating Cyber Attacks", Indiana University, Kelly school of Business, University of Cambridge - Department of Politics and International Studies; Stanford Law School, November 4, 2009

8. Sloan, Elinor(2010)," China's Strategic Behaviour", Canadian defence: Foreign Affairs Institute, June, 2010,at this link: www.cdfai.org/.../**China**%20**Strategic**%20**Behaviour**.pdf

9. Space Policy Security Review: Assuring a Trusted and Resilient Cyber information, at this link:http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

10. Simon, Tisdall(2010), " Cyber – War: is growing threat", Guardian Newspaper, 3 Feb.2010

المواقع الإاكترونية:

1. موقع اليوم السابع المصري," الصين تستحدث الجيش الأزرق لحماية شبكتها من القرصنة الإلكترونية", آخر تحديث: 2011/5/26

2. موسوعة المعرفة." حرب الإنترنت", الرابط:php.index/org.awww.maref

3. منتدى الجيش العربي. أنظر الرابط: com.military.www.arabic

4.www.weeklystandard.com/blogs/does-stuxnet-mean-cyb...

5.www.zdnet.co.uk/news/security-threat/2009/11/13/uk

6.pentagon-weighs-applying-preemptive-warfare-tactics-internet/
http://www.rawstory.com/rs/2010/08/29/

7. Cyber warrior Shortage Threatens U.S. Security, at the link:

http://www.npr.org/templates/story/story.php?storyId=128574055

الصحف:

1 . صحيفة العالم، يومية، عراقية، الثلاثاء 26 تشرين الثاني 2013, الستة الرابعة, العدد 917 2 . صحيفة الحياة اللندنية, السبت 31 آب 2013م الطبعة الدولية, العدد 16955

3 . صحيفة الشروق," تكلفة التجسس على هواتف الحلفاء", الخميس 7 تشرين الثاني 2013
4 . صحيفة الاتحاد الإماراتية," التجسس الأمريكي...واتفاق العيون الخمس", الأحد 22 تشرين الثاني 2013م