حرب السيبرانو وأبعادها المستقبلية

الاستاذ المساعد الدكتور

حميد علوان محمد

جامعة ديالى / كلية التربية للعلوم الانسانية

قسم الجغرافية

المدرس

حسين عبد المجيد حميد

جامعة ديالى / كلية التربية الاساسية

قسم الجغرافية

موبايل / ٠٧٧٣٥٤٩٨٨٩٣

H_alsbaa2000@yahoo.com

٢٠١٦م

١٤٣٧هـ

الملخص

مع تزايد اعتماد معظم دول العالم في كافة انشطتها المختلفة على شبكة المعلومات الدولية، اتجهت معظم هذه الدول وبخطى حثيثة الى تطوير قدراتها الدفاعية في المجال الالكتروني للحد من تأثير خطر الهجمات السيبرانية التي تقوم بها بعض الدول المنافسة على مواقعها ومؤسساتها الالكترونية وبخاصة المواقع السياسية والعسكرية، وفي الوقت ذاته تقدمت عجلة تطور اساليب وطرق الهجمات والاختراقات السيبرانية، الامر الذي دفع الى تأسيس تشكيلات عسكرية الكترونية في مختلف دول العالم (وبخاصة الدول العظمى) مهمتها تعزيز دفاعات مؤسساتها الالكترونية ضد اي هجمات سيبرانية، وبذلك بدأت بوادر ما يعرف بحرب السيبرانو، ومن المتوقع ان تصبح الحرب السيبرانية نموذجاً تسعى اليه معظم دول العالم لإلحاق الاذى الاكبر بالدول المنافسة لها الامر الذي سيؤدي الى ظهور تحالفات دولية جديدة (تحالفات الكترونية) في المستقبل القريب .

Abstract:

With the growing majority of countries in the world to adopt all of the different activities on the internet, most of these countries tended and racing ahead to develop their own defense in the electronic field to reduce the impact of the risk of cyber-attacks carried out by some countries compete for positions, institutions and electronic especially political and military sites, and in the same time made the wheel evolution of techniques and methods of attacks and intrusions cyber, prompting the establishment of military formations electronic in various countries around the world (especially the great powers) mission is to strengthen the defenses of the electronic institutions against any cyber-attacks, and the beginnings of what is known as a war Alcyprano is expected to began the war become a cyber a model for most of the world is seeking to him to inflict the greatest harm countries competing which will lead to the emergence of new international alliances (electronic alliances) in the near future .

المقدمة

شكلت الثورة الرقمية التي بانت ملامحها في العقد التاسع من القرن العشرين طفرة هائلة في مجال الاتصالات وانظمة الحاسبات وتحول العالم بسرعة مذهلة ليعتمد عليها بشكل كبير في تسيير امور الحياة اليومية حتى اصبحت قدرات الدولة الالكترونية معياراً من معايير التطور وحساب القوة، وتحول التنافس الى حرب ولكنها حرب تختلف هذه المرة، فهي حرب الكترونية تسعى كل دولة من خلالها الى ابراز عضلاتها في مجال التقدم الالكتروني وغزو الانظمة الرقمية للدول المنافسة وهذا ما يطلق عليه (الحرب السيبرانية).

تناول هذا البحث الحرب السيبرانية كمصطلح حديث وكمحاولة لوضع اللبنة الاولى لدراسات اوسع عن هذا الموضوع، إذ ان المشكلة المطروحة تتمثل بـ(ماهي الحرب السيبرانية وما هو نطاقها الجغرافي وماهي انعكاساتها المستقبلية على العالم) على افتراض ان الحرب السيبرانية لا تستخدم فيها الاسلحة التقليدية ولكنها ستؤدي الى انعكاسات مستقبلية على العالم لا تقل عن الحرب العسكرية من ناحية الازمات السياسية والتحالفات الدولية والانفاق المالي، ان ما يبرر كتابة هذا البحث هو قلة ما كُتب عن هذا الموضوع الذي يعد موضوعا حديثاً، ويمكن ان يدخل في معايير قوة الدولة بالنسبة للجغرافية السياسية ليشكل عاملاً مضافاً، وقد انطوى البحث على ثلاثة مباحث وهي:

١-المبحث الاول مفهوم حرب السيبرانو وادواتها .

٢-المبحث الثاني النطاق الجغرافي لحرب السيبرانو واهم الجيوش السيبرانية .

٣-المبحث الثالث رؤية مستقبلية عن الابعاد الدولية لحرب السيبرانو .

المبحث الاول

مفهوم حرب السيبرانو

أولاً : ماهية الحرب السيبرانية

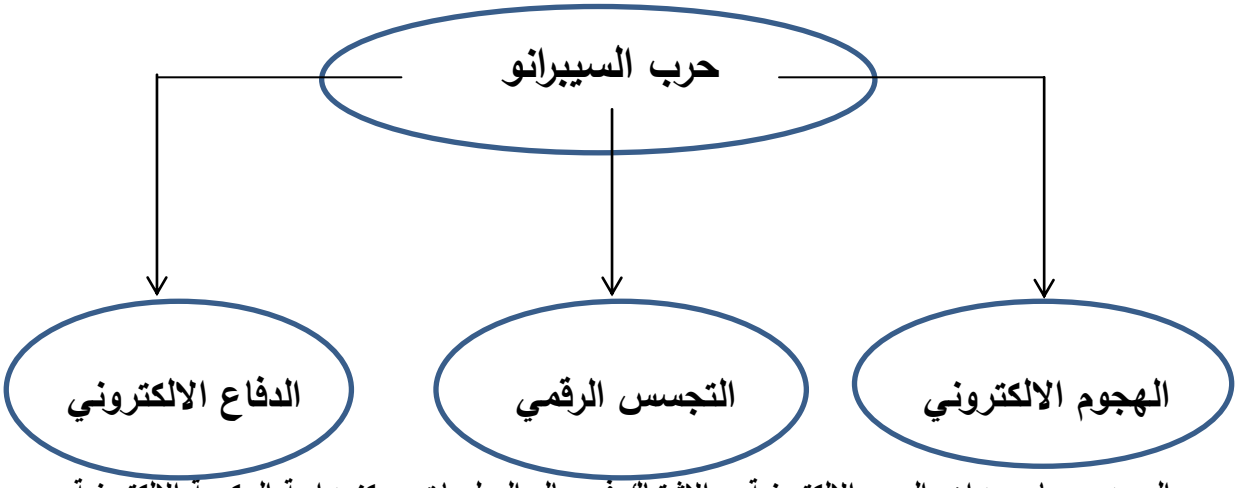
إن معظم الاشتباكات الالكترونية في الوقت الحاضر تتم من قبل منظمات وأفراد بغية الحصول على المال أو الانتصار لعقيدة معينة او الانتقام من منافسين، ولم يتطور هذا النوع من الحرب (الحرب السيبرانية) لكي يصل الى ان يكون جزءاً من حرب علنية تجري بين دولتين بالرغم من بدايات ظهور مؤشرات عليها في حرب روسيا– أستونيا، وحرب روسيا _ جورجيا، إذ تزامن هذا الهجوم الالكتروني بطريقة منظمة على البنية التحتية للمعلومات في جورجيا واستونيا مع العمليات العسكرية التي كانت تدور على الارض، وبالرغم من ان روسيا لم تعلن صراحة أنها قامت بتلك الهجمات الالكترونية، الا ان التقارير والمعلومات التي نشرت على شبكة الانترنت تشير الى ان مجموعات المهاجمين الالكترونيين الروس مرتبطة بطريقة او بأخرى بمنظومة السلطة والسيطرة الروسية وتتلقى تعليماتها وتوجيهاتها منها[١].

وتمثل الحرب السيبرانية خطورة كبيرة على كافة الدول وبخاصة الدول النامية التي ارادت توطين التكنلوجيا واحراز التقدم في المجال التقني من ناحية، ولكنها لم تتقدم في المجال المعلوماتي من ناحية اخرى، إذ لايزال التفوق في هذا المجال بيد الدول الكبرى والدول المصنعة لبرامج المعلومات . ويشهد العالم اليوم سباق نحو التسليح الرقمي بين الدول وعلى رأسها الولايات المتحدة الامريكية وروسيا الاتحادية وكوريا الشمالية والصين وبريطانيا واسرائيل من اجل توظيف تلك الامكانيات في اي حرب عسكرية قادمة[٢].

ومن الممكن تقسيم حرب السيبرانو الى عدة مجالات وكالاتي (انظر شكل ١)[٣] :-

١. مجال الدفاع الالكتروني : الذي يعنى بالدفاع عن انظمة واجهزة ومعلومات الدولة والجيش والمخابرات والمجتمع وكافة المؤسسات الاخرى .
٢. الهجوم الالكتروني : والذي يهدف الى التشويش على مصادر المعلومات وتدميرها وحرمان العدو من استخدامها لصالحه خلال اوقات الازمات او الحروب العسكرية .
٣. التجسس الرقمي : إذ شهدنا منذ مدة اكتشاف شبكة الشبح الرقمية الصينية التي تجسست على اكثر من ١٠٠ دولة ولم يتم اكتشافها الا مؤخراً.

شكل (١) مخطط يبّين مجالات الحرب السيبرانية



المصدر: عباس بدران، الحرب الالكترونية – الاشتباك في عالم المعلومات، مركز دراسة الحكومة الالكترونية، لبنان، بيروت، ٢٠١٠، ص٢٩ .

من الشكل (١) يمكن القول ان الهجوم الالكتروني لابد من ان يقابله استعدادات دفاعية من قبل الجهة الاخرى، لكن تبقى عملية التجسس الالكتروني المخابراتي هو المجال الاكثر تحقيقاً لأهدافه من خلال اختراق المواقع الالكترونية وسرقة المعلومات والبيانات ..... الخ، دون ان يكون للعدو اي علم الا بعد اتمام عملية الاختراق وبخاصة اذا كان قائد الهجوم الالكتروني من المتمرسين او من اصحاب الدراية والخبرة في هذا الجال .

ثانياً : مفهوم الحرب السيبرانية واهم معالمها

يعد مفهوم الحرب السيبرانية (Cyber War) احد اهم مفاهيم الحقبة المعاصرة والقادمة والتي ربما تشهد حروباً الكترونية تحل محل الحروب التقليدية لتصل الى مداها في الخسائر المادية وربما تتعداه، إذ يعتمد افراد الحرب السيبرانية (المجرمون، قراصنة الكمبيوتر، الحكومات) على حدٍ سواء على الاستفادة من نقاط الضعف البشرية والتقنية للوصول الى اجهزة الكمبيوتر الاخرى للقيام بهجمات سيبرانية، فالخطأ البشري هو جزء رئيس من اختراق أنظمة الامن السيبراني، كما ان الخطأ الفردي يمكن ان يكون كافياً لمنح فرصة للوصول الى شبكات بأكملها واختراقها من قبل الاشخاص المهاجمين بما في ذلك المواقع الحكومية والصناعية والمؤسسات العسكرية، وفي الوقت ذاته يصعب تتبع اصول وهوية مُطوّر البرامجيات الخبيثة او صاحب الهجوم الالكتروني المباشر[٤].

من هنا تكون السيبرانية مجموعة واسعة من الإجراءات والتي تتراوح بين استخدام المجسات البسيطة المستخدمة لمحو المواقع على شبكة الإنترنت وبين الحرمان من خدمة الشبكة والتجسس والتدمير، وعلى نحو مماثل يستخدم مصطلح "الحرب السيبرانية" لتغطية مجموعة واسعة من السلوكيات وهو يعكس تعريفات للحرب تتراوح بين الصراع المسلح وبين التسابق العدائي (على سبيل المثال "الحرب ضد المخدرات")، وعلى الطرف الآخر النقيض يستخدم بعض الخبراء مفهوماً ضيقاً للحرب السيبرانية "حرب غير دموية" تنشأ بين الدول والتي تشتمل فقط على الصراع الإلكتروني في الفضاء السيبراني، ولكن هذا التعريف يتجاهل الترابط المهم بين الطبقات المادية والافتراضية للفضاء الإلكتروني، وكما أظهر الفيروس "ستوكسنت"

الذي أصاب البرنامج النووي الإيراني فإن الهجمات التي تستخدم البرمجيات قد تسفر عن آثار تدميرية مادية حقيقية[٥].

وهناك مفهوم أكثر فائدة للحرب السيبرانية يؤكد على انها عمل عدائي في الفضاء الإلكتروني والذي تؤدي التأثيرات المترتبة عليه إلى تضخيم العنف المادي أو تعادله. وفي العالم المادي تفرض الحكومات ما يشبه احتكار واسع النطاق من استخدامات القوة ويتمتع المدافع بمعرفة وثيقة بالتضاريس، وتنتهي الهجمات إما بسبب الاستنزاف أو الإرهاق وهنا تفرض عملية تدبير الموارد ونقلها تكاليف باهظة، أما في العالم السيبراني فإن الجهات الفاعلة متنوعة (ومجهولة في بعض الأحيان) والمسافات المادية تصبح بلا أهمية ولا تكلف بعض أشكال الهجوم سوى تكاليف زهيدة، ولأن شبكة الإنترنت كانت مصممة لتيسير الاستخدامات وليس توفير الأمن فإن المهاجمين يتمتعون بميزة تجعلهم متفوقين على المدافعين[٦].

ولابد هنا من التمييز بين الحرب المادية (الحرب التقليدية) والحرب السيبرانية، فمفهوم الحرب يستخدم لوصف مجموعة متنوعة من الظروف والسلوكيات بدايةً من حالة النزاع المسلح بين الدول (كالحرب العالمية الثانية) وصولاً الى الحروب الرمزية ، اما الحرب السيبرانية فهو مصطلح يستخدم لوصف كل شيء متعلق بحملات التخريب وتعطيل الانترنت وصولاً الى حالة الحرب الفعلية باستخدام الوسائل الالكترونية، ويذهب بعض الخبراء لتوسيع هذا المفهوم ليشمل عمليات تزوير بطاقات الائتمان .

ويمكن توضيح مصطلح الحرب السيبرانية من خلال ثلاثة معالم رئيسة هي[٧]:

١. الحرب السيبرانية تمتلك فضاءً مستفيضاً لها وهو الفضاء الالكتروني، كما هو الحال بالنسبة للحرب المادية التي يشمل فضاؤها البر والبحر والجو .

٢. الحرب السيبرانية تهدف الى تحقيق مآرب سياسية ومخابراتية محددة (وهو ما يميزها عن الجرائم الالكترونية الاخرى) .

٣. الحرب السيبرانية دائما ما تمتلك وحدة عنف اساسية .

ثالثاً : ترسانة الحرب السيبرانية:

من المعلوم ان اي حرب من الحروب سواء كانت عسكرية مادية او الكترونية رقمية بحاجة الى عدت عناصر مجتمعة من اجل اطلاقها وادارتها ويعتمد النصر فيها او الهزيمة على عدد من الاستراتيجيات والتكتيكات على العنصر البشري، واهم من ذلك على ترسانة السلاح المتوفرة بيد ذلك العنصر البشري، فالحرب السيبرانية (الرقمية) لا تختلف كثيراً في هذا المجال إذ انها تعتمد على التخطيط والستراتيجية والتنظيم والتدريب وعلى ترسانة سلاح آخر (ترسانة السلاح الرقمي)، إذ بدأت الدول الكبرى في الوقت الحاضر بناء ترسانة سلاح رقمي بكل ما للكلمة من معنى وتسعى ان تكون تلك الترسانة سرية وجاهزة لدعم ومؤازرة اي حرب او اشتباك سياسي عسكري مستقبلي، ولا تقتصر ترسانة السلاح الرقمي على اسلحة التعطيل والتخريب بل تتعداها الى الاسلحة التجسسية وادوات ووسائل محاربة الاعتراضات والتجمعات الالكترونية ضد الدولة[٨].

ومن الجدول (١) يمكن ان نتعرف على اهم ما يميّز اسلحة الحرب السيبرانية عن اسلحة الحروب التقليدية من حيث الخسائر بالأرواح والمدى الذي يمكن ان تصل اليه والتكاليف وتأثيرها بالراي العام والمهارات المطلوبة من العنصر البشري في مثل هذه الحروب.

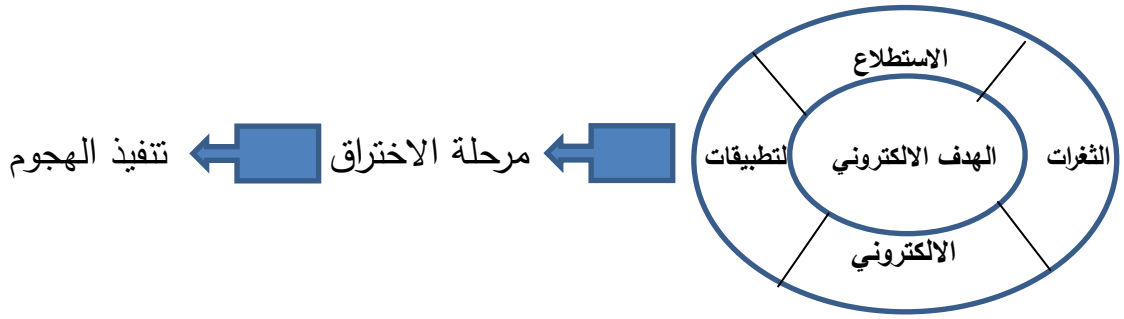
جدول (١) يبيّن الفرق بين الاسلحة الرقمية والاسلحة التقليدية

المميزات	السلاح الرقمي	السلاح التقليدي
خسائر الارواح	محدودة	عالية جداً
المدى بالكيلومتر	تطال اي نقطة وصلت اليها شبكة الانترنت	تعتمد على نوع السلاح – محددة بقياس بالكيلومترات
التأثير بالراي العام	عالي	منخفض
الحرب النفسية	عالية	عالية
كلفة الاقتناء والصيانة	منخفضة	عالية
الاستخدام للتجسس	عالية	منخفضة
المهارات البشرية المطلوبة	مهارات ناعمة	مهارات خشنة
عدد مرات الاستخدام	مرات عديدة – طالما بقى السلاح الرقمي تحت سيطرة القيادة	مرة واحدة – اطلاق ثم تفجير

المصدر : عباس بدران، الحرب الالكترونية – الاشتباك في عالم المعلومات، مركز دراسة الحكومة الالكترونية، لبنان، بيروت، ٢٠١٠، ص٤٥ .

كما ويمكن تجسيد الهجوم السيبراني ومراحله بالشكل (٢)، إذ تبدأ بعملية الاستطلاع الالكتروني ومعرفة الموظفون والمختصون واوقات تواجدهم وتحديد الثغرات الالكترونية ومن ثم فرز الهدف المراد غزوه وبالتالي تأتي مرحلة الاختراق ومن ثم تنفيذ الهجوم .

شكل (٢) مراحل الهجوم السيبراني



المصدر : عباس بدران، الحرب الالكترونية – الاشتباك في عالم المعلومات، مركز دراسة الحكومة الالكترونية، لبنان، بيروت، ٢٠١٠، ص٤٧.

المبحث الثاني

المجال الجغرافي لحرب السيبرانو واهم الجيوش السيبرانية

يعد الفضاء الالكتروني هو الميدان الرابع للحروب الحديثة بعد ان كانت تقتصر على البر والبحر والجو ومن المتوقع ان تكون الحرب السيبرانية (Cyber War) احدى اشكال الحرب الحديثة والمستقبلية، إذ تكمن الخطورة في حروب الانترنت والشبكات في كون العالم اصبح يعتمد اكثر فاكثر على الفضاء الالكتروني لاسيما في البنى التحتية والمعلوماتية العسكرية والمصرفية والحكومية فضلاً عن المؤسسات والشركات العامة والخاصة . ان زيادة الهجمات السيبرانية جاءت نتيجة لزيادة الاعتماد على شبكات الانترنت والكمبيوتر، وهذا يعني امكانية تطور الهجمات والاختراقات الالكترونية لتصبح سلاحاً حاسماً في النزاعات بين الدول في المستقبل، لذلك شرعت العديد من الدول وبخاصة الدول العظمى الى تشكيل جيوش الكترونية يقع على عاتقها اختراق الدفاعات الالكترونية لمواقع العدو والعمل على تحصين دفاعات مواقعها الالكترونية لصد اي هجوم سيبراني من قبل الدول الاخرى[٩].

ومن المتوقع ان يؤدي تحديد استخدام الاسلحة النووية الى احتلال الحرب السيبرانية المشهد والتي لا تقل خطورة عن السلاح النووي، حيث يمكن ان تحدث خسائر بالمليارات دون اطلاق رصاصة واحدة، وكان هذا السبب وراء اتجاه العديد من الدول لتشكيل وحدات خاصة لهذه الحرب الجديدة التي تتخذ من الفضاء الالكتروني مسرحاً لعملياتها وهجماتها .

ومن اهم هذه الوحدات والتشكيلات السيبرانية العسكرية في دول العالم هي (انظر خريطة ١) :

(خريطة ١) اهم الوحدات والتشكيلات السيبرانية العسكرية في دول العالم

المصدر: من عمل الباحثان بالاعتماد على اطلس العالم السياسي ٢٠١٣ .

أولاً : الوحدات الست في الولايات المتحدة الامريكية[١٠]

هناك ست وحدات الكترونية تعتمد عليها الولايات المتحدة الامريكية وهي :

١. الوحدة الامريكية لقيادة الفضاء الالكتروني: تختص هذه الوحدة بإدارة الحروب السيبرانية والتخطيط والتنسيق لها مع باقي الفروع التي تتبعها .
٢. وحدة الجيش الامريكي الالكتروني : وتتكون من ثلاثة وحدات اصغر .
٣. وحدة السايبر بقوة المارينز : والتي تختص بحماية وتامين منشآت المارينز من الهجمات الالكترونية .
٤. وحدة الجيش الالكتروني البحرية : ويقع على عاتقها تامين وصد الهجمات على المواقع والمنشآت البحرية الالكترونية فضلاً عن جمع المعلومات عن حروب السايبر.
٥. وحدة القوة الجوية ٢٤ : وتختص بالطيران والقوات الجوية الامريكية وتتفرع الى ثلاثة اجنحة .
٦. الاسطول العاشر الامريكي : ومهمته التخابر لصالح البحرية الامريكية .

وقد استطاعت هذه الوحدات السيبرانية قطع خدمات الانترنت تماماً عن كوريا الشمالية في ديسمبر ٢٠١٤ ليوماً كاملاً رداً على اختراقات كوريا الشمالية لمواقع تابعة لشركة سوني الامريكية .

ثانياً : الكتيبة ١٢١ في كوريا الشمالية : أنشأت كوريا الشمالية (Bureav121) عام ١٩٩٨ وهو عبارة عن وحدة خاصة بالحروب السيبرانية واهدافه الرئيسة كل من الولايات المتحدة الامريكية وكوريا الجنوبية واليابان، ومن اهم اعماله هو اختراق شركة سوني الذي تسبب بخسائر تقدر بملايين الدولارات[١١].

ثالثاً : اللواء ٧٧ البريطاني : في بداية عام ٢٠١٥ اقدمت بريطانية على تشكيل اللواء ٧٧ معلنةً عن دخولها مضمار الحرب السيبرانية، ويركز هذا اللواء في عمله على الحسابات المؤيدة للمتشددين على تويتر ويتكون هذا اللواء من ٢٠٠٠ جندي.

رابعاً: مخابرات الاشارة الروسية : من الاعمال التي قامت بها هذه الوحدة هو الهجوم على المواقع الالكترونية لأوكرانيا بالتزامن مع انفصال شبه جزيرة القرم وانضمامها الى روسيا الاتحادية، اما عن احدث الهجمات السيبرانية التي شنها الروس هو اختراق وزارة الخارجية الامريكية وانظمة البيت الابيض لدرجة تسريب جدول اعمال الرئيس الامريكي باراك اوباما(١٢).

خامساً : الوحدة ٦١٣٩٨ الصينية : يؤكد بعض الخبراء على امكانيات هذه الوحدة الالكترونية والتي استطاعت سرقة اسرار عسكرية امريكية واختراق شبكات الطاقة النووية في مايو ٢٠١٤ .

سادساً : كومندوز الجيش الاسرائيلي : تركز هذه الوحدة الالكترونية على ٣٠ موقعاً، فضلاً عن بعض مواقع التواصل الاجتماعي، وقد ابقت هذه الوحدة الالكترونية على تغطية شبكة الانترنت في قطاع غزة آبان الحرب الاسرائيلية عليها عام ٢٠١٢ بهدف اختراق الاتصالات بين اعضاء حركة حماس فضلاً عن اهداف اخرى(١٣).

سابعاً : جيش ايران الالكتروني : ظهرت امكانيات ايران في الهجمات الالكترونية من خلال اختراق ٣٠ الف كمبيوتر تابع لشركة آرامكو السعودية للبترول واختراق شركة هولندية وسحب شهادات رقمية منها حتى تؤمن وسائل اتصالات الانترنت كما استطاع هذا الجيش الالكتروني من التجسس على جنرالات في الجيش الاسرائيلي وفيزيائيين وعلماء ذرة ومجموعة من الاكاديميين وعلماء الاقتصاد(١٤).

ثامناً : المجموعات الدولية الخاصة (جماعة أنو نيموس) مثالاً : وهي شبكة دولية لنشطاء من جنسيات متنوعة متخصصين في التسلل عبر الانترنت وقامت بعدد كبير من الهجمات الالكترونية ضد مواقع الكترونية لحكومات وشركات ومواقع دينية متعددة ومنها مواقع اسرائيلية بخاصةً في فترة العدوان الاسرائيلي على قطاع غزة عام ٢٠١٢، وبعد هجمات باريس (تشرين الثاني ٢٠١٥) هددت هذه الجماعة تنظيم داعش الارهابي باختراق مواقعه بهجمات سيبرانية متعددة كردّ على الاعمال الاجرامية التي يقوم بها هذا التنظيم[١٥].

تاسعاً : الهجمات الالكترونية للتنظيمات المتطرفة حول العالم

تستخدم معظم التنظيمات الارهابية والمتطرفة الانترنت في الوقت الحاضر كوسيلة للاتصال وتبادل المعلومات، فعلى سبيل المثال نادراً ما استخدم تنظيم القاعدة الانترنت خلال سنواته التكوينية في تسعينيات القرن الماضي، إذ كانت الرسائل التهديدية لزعمائه تنشر عن طريق تسجيلات صوتية او شرائط فديو تبث على بعض القنوات الفضائية، ولكن منذ مطلع القرن الواحد والعشرون وبعد وقوع احداث (١١ سبتمبر) واحتلال الولايات المتحدة لأفغانستان أفقدت العمليات العسكرية للجيش الامريكي تنظيم القاعدة ملاذاته الآمنة للتدريب والتنظيم، مما دفعه للتركيز على استخدام التكنلوجيا السيبرانية، الامر الذي أفرز تنظيماً يتبنى افكار القرون الوسطى باستخدام تكنلوجيا القرن الواحد والعشرين، ولكن لم تستخدم القاعدة الفضاء الالكتروني للقيام بعمليات ارهابية سيبرانية، بل لتمرير المعلومات والوصول الى العالم الواسع بشكل لم يحدث من قبل لمثل هذه الجماعات، كما سمحت ثورة الانترنت للجماعات الارهابية بالقيام بعملياتها بطرق جديدة اكثر تعقيداً عن سابقتها التقليدية، وعند ذلك ادركت هذه التنظيمات اهمية الانترنت من خلال ما يوفره من

خدمات موثوق بها وشروط ميسرة وهويات افتراضية، كما استطاعت الجماعات الارهابية من التواصل مع بعضها البعض عبر القارات، الامر الذي كان يستغرق شهوراً في الماضي، كما سمحت شبكات الانترنت لهذه التنظيمات المتشددة من تبادل الخبرات في صناعة المتفجرات واساليب اخفائها وعمل الخلطات التفجيرية من خلال ما يسميه خبراء الامن (TTPS) وهو اختصار لـ(تكتيكات وتقنيات واجراءات)، ومن الجدير بالذكر ان شبكة المعلومات الدولية (الانترنت) وفرت لهذه التنظيمات مصدراً منخفض التكلفة لجمع المعلومات الاستخباراتية حول اهدافهم، فمثلاً مكنت تقنية (Google Earth) لجماعة (شكر طيبة) الباكستانية من التخطيط لهجمات مومباي عام ٢٠٠٨، وكذلك في عام ٢٠٠٧ عندما قام مجموعة من الجنود الامريكان بالتقاط صور تذكارية في قاعدة عسكرية في العراق وكان خلفهم مجموعة من طائرات الهليكوبتر ثم قاموا بتنزيلها على الانترنت، عند ذلك استطاعت بعض الجماعات المسلحة من استغلال العلامات الجغرافية (Geo tags) التي شملت عليها تلك الصور التذكارية لتتمكن هذه الجماعات المسلحة من تحديد موقع القاعدة العسكرية وتدمير اربعة طائرات هليكوبتر من خلال هجوم بقذائف الهاون[١٦].

وفي الوقت الحاضر تبيّن ان تنظيم داعش الارهابي يستخدم الانترنت ومواقع التواصل الاجتماعي لنشر أفكاره الاجرامية والمتطرفة لاستمالة من يوافقونه على جرائمه للعمل معه في هذا النهج الاجرامي، كما استخدم هذا التنظيم الانترنت لنشر افعاله وجرائمه ضد المناوئين له ومن يتعارضون معه في الايديولوجيات التي يتبناها.

المبحث الثالث

رؤية مستقبلية عن الابعاد الدولية لحرب السيبرانو

يجمع خبراء عصر المعلومات على ان العقود القليلة القادمة قد تشهد تحولاً مدهشاً للعالم الذي سيتخذ شكل قرية ذكية صغيرة مرتبطة بالكامل بالأقمار الصناعية، واذا كانت عجلة التقدم في مجال التقنيات الرقمية قد تسارع ايقاعها باتجاهات ومجالات مختلفة في عالم اليوم حتى صار عنواناً للعصر ومفتاحاً لتقدم الامم، فأن مسيرة التقدم الرقمي في طريق تعزيز قدرات الامم على ادارة الحروب وتحقيق السيطرة والنصر ستكون لها تداعيات مستقبلية اكثر تأثيراً وخطورة نتيجة لمتغيرات عدة من اهمها حجم الدعم المادي الكبير الذي تخصصه الدول في الاستثمار في هذا القطاع من جانب، واهمية الاهداف الحيوية المراد تحقيقها باستخدام هذه الوسائل من جانب اخر، بيد ان تبني فرضية التحول الجزئي او الكلي في مسار الحروب المستقبلية باتجاه الافراط في الاعتماد على المتغير التقني الرقمي يستلزم استكشاف حدود البنية والامكانيات الواقعية لتحقيق ذلك سواء كان على مستوى التخطيط الاستراتيجي او حتى على مستوى التعرض الفعلي باستخدام الوسائل الالكترونية في مجال ادارة الحروب[١٧].

والى الوقت الحاضر لاتزال الهجمات السيبرانية ليس لها قانون دولي رادع كون القوى السيبرانية الثلاثة الاكبر في العالم (الولايات المتحدة الامريكية والصين وروسيا الاتحادية) لم تتفق على معاهدة مشتركة لموائمة القوانين الوطنية او تسهيل التعاون فيما بينهم، كما أنها لا تتعاون فيما بينها في هذا المجال من خلال مؤسسات عالمية أخرى باستثناء مجموعة العشرين + الامم المتحدة[*]، وقد ولدت حالات التجسس الالكتروني في السنوات الاخيرة قدراً متنامياً من انعدام الثقة حتى بين

الحلفاء التقليديين مثل الاتحاد الاوربي والولايات المتحدة، إذ يهدد الفضاء السيبراني بالتحول في المستقبل القريب الى ميدان معركة، حيث تشتبك الحكومات والكيانات الفاعلة والمجموعات الدولية غير التابعة للحكومات والقطاع الخاص (الافراد) فيما بينهم لتحقيق منافع عامة (وطنية) او خاصة، وربما يكون الهجوم الذي قام به متشددون على القناة الفضائية الفرنسيةٌ (TV5) واختراق شركة سوني من قبل كوريا الشمالية نذيراً بما سوف يحدث في المستقبل القريب[١٨].

لذا فان الحرب السيبرانية ستكون مرهقة اقتصادياً للدول المهاجمة والدول المستهدفة على حدٍ سواء، لان الدول المستهدفة ستصرف مبالغ طائلة لحماية انظمتها ومؤسساتها الالكترونية، وفي الوقت ذاته ستعمل الدول المهاجمة على شراء العديد من الانظمة والبرامجيات من الشركات والمؤسسات الالكترونية العالمية لتطوير اساليب هجماتها السيبرانية، كما ستلجأ الدول الصغيرة المستوردة لأنظمة الحاسوب الى الانخراط في معسكرات الدول الكبرى، لأنها غير قادرة على انتاجها وحمايتها، فمثلاً يذهب العراق الى الولايات المتحدة لاستيراد انظمة تشغيل الحاسبات ووسائل حمايتها، في حين تلجأ سوريا مثلاً الى روسيا الاتحادية، وغيرها الى الصين، وهكذا سيتولد حلف ثالث جديد (التحالفات الالكترونية) يضاف الى الاحلاف الدولية التقليدية (العسكرية والاقتصادية).

كما ويرى الباحثان ان على الشركات الالكترونية العالمية ومنظمات المجتمع المدني العالمية ان تلعب أدواراً كبيرة لضمان بقاء ادارة الفضاء الالكتروني مفتوحة وشاملة ومرنة بالقدر الكافي لتكيف نفسها مع المخاطر والتحديات المتغيرة، ولابد من تطوير النهج الحالي للإدارة الفنية للفضاء السيبراني والعمل على اكتشاف مقترحات اخرى مبدعة قد تساهم في تحسين إدارة مجلس الاستقرار السيبراني التابع

لمجموعة الدول العشرين + الامم المتحدة، اذ تشير العديد من التقارير ومنها تقرير التنمية البشرية للأمم المتحدة لعام ٢٠١٤[*] الى ان عام ٢٠٢٠ سيشهد اتصال ثلثا سكان العالم بالإنترنت (جدول ٢ و ٣) ، لذا سيحتاج العالم الى اجراء حوار سلس وصريح بين الدول واشراك المنظمات والمؤسسات والقطاع الخاص بهذا الحوار من اجل الوصول الى تحقيق امن الفضاء السيبراني واستخدام طرق واساليب ترقى لان تعالج التهديدات السيبرانية في القرن الواحد والعشرون، حيث نرى ان المجتمع الدولي يضع العديد من الانظمة والقوانين والمعايير لتنظيم مجالات متعددة منها الصحة (منظمة الصحة العالمية) وانتشار الاسلحة النووية، لذلك لابد من الاستعانة بالنهج ذاته في التعامل مع الفضاء السيبراني، فالمجتمع البشري جميعاً لديه مصلحة مشتركة في الحفاظ على انفتاح الفضاء السيبراني واعطاءه الشخصية العالمية، وسوف يتطلب القيام بذلك ان نضع المصالح الفئوية الضيقة جانباً لضمان الامن والتقدم الجماعي العالمي في المضمار الالكتروني .

جدول(٢)النسبة المئوية لمستخدمي الانترنت من مجموع السكان في بعض دول العالم لعام ٢٠١٢

ت	الدول	مستخدمو الانترنت بالنسبة المئوية % من مجموع السكان في عام ٢٠١٢
١	المملكة المتحدة	%٨٧
٢	كوريا الشمالية	%٨٤،١
٣	الولايات المتحدة الامريكية	%٨١
٤	اسرائيل	%٧٣،٤
٥	روسيا	%٥٣،٣
٦	الصين	%٤٢،٣
٧	ايران	%٢٦

المصدر: تقرير التنمية البشرية للأمم المتحدة ٢٠١٤، برنامج الامم المتحدة الإنمائي، مسجل في المكتبة البريطانية ومكتبة الكونغرس، ص٢٠٦-٢٠٩ . الرابط الالكتروني http://hdr.undp.org

جدول(٣) النسبة المئوية لمستخدمي الانترنت من مجموع السكان في بعض المناطق والجهات في العالم لعام ٢٠١٢

ت	المناطق والجهات في العالم	مستخدمو الانترنت بالنسبة المئوية % من مجموع السكان في عام ٢٠١٢
١	الدول العربية	٣٤،٢
٢	شرق اسيا والمحيط الهادي	٣٦،٧
٣	اوربا واسيا الوسطى	٤١،١
٤	امريكا اللاتينية والبحر الكاريبي	٤٣،٤
٥	جنوب اسيا	١٢،٣
٦	جنوب الصحراء الافريقية الكبرى	١٥،٢
٧	العالم	٣٥،٥

المصدر: تقرير التنمية البشرية للأمم المتحدة ٢٠١٤، برنامج الامم المتحدة الإنمائي، مسجل في المكتبة البريطانية ومكتبة الكونغرس، ص٢٠٦-٢٠٩. الرابط http://hdr.undp.org

الاستنتاجات والتوصيات:

توصل الباحثان الى ان منظومة السلاح السيبراني الذي تمتلكه اي دولة ستكون في المستقبل القريب سلاح ردع يضاهي السلاح النووي في فاعليته وقيمته في المحافل الدولية، ولن تنجح معظم الاتفاقيات العالمية بهذا الجانب، لان الهجمات السيبرانية غالباً ما يكون فاعلها مجهول الهوية، ولذلك ستضطر الدول لعقد اتفاقيات ثنائية لحماية منظوماتها الالكترونية، كأن تعقد الولايات المتحدة الامريكية اتفاقية مع الصين وتعطيها تنازلات معينة مقابل ان تقوم الصين بالتهدئة في مجال حربها السيبرانية اتجاه الولايات المتحدة ، كما يرى الباحثان ان الحرب السيبرانية ستكون مكلفة جدا من الناحية الاقتصادية للدول التي ستعمل على تدعيم دفاعاتها الالكترونية والدول الي يتسارع الى تطوير اساليبها الهجومية .

ويوصي الباحثان على ضرورة الابقاء على حيادية الفضاء السيبراني وان يكون متاحاً للجميع وتفعيل دور المنظمات العالمية المختصة بهذا المضمار ، كما ويؤكد الباحثان على ضرورة إنشاء كتيبة عسكرية الكترونية عراقية تعمل على صدّ الهجمات السيبرانية التي قد تتعرض لها المواقع الالكترونية العراقية لمنع تسريب المعلومات العسكرية والاستراتيجية في المنظومات الالكترونية التابعة للوزارات والمؤسسات السياسية والعسكرية الى جهات وجماعات قد تستخدمها للقيام بأعمال عدائية .

الهوامش :

---

[١] عباس بدران، الحرب الالكترونية – الاشتباك في عالم المعلومات، مركز دراسة الحكومة الالكترونية، لبنان، بيروت، ٢٠١٠، ص٢٩.

[٢] خالد وليد محمود، الهجمات عبر الانترنت : ساحة الصراع الالكتروني الجديدة، المركز العربي للأبحاث ودراسة السياسات، سلسلة دراسات، سبتمبر ٢٠١٣، ص٩-١١.

[٣] روز تسانغ، الاخطار الالكترونية والنقاط المعرضة للخطر والهجمات، بيركلي كاليفورنيا، جامعة كاليفورنيا، كلية غولدمان للسياسة العامة، ٢٠٠٩، ص٦-١٠

[4] Pw singer and Allan friedman , Cyber security and Cyber war : what everyone needs to know , Newyork oxford university press , 2014

[٥] أمل خيري، اسرائيل وقراصنة الانترنت : جولة جديدة في الحرب السيبرانية، ٢٠١٣/٤/١١، الرابط الالكتروني:

htt://www.alamatonline.net/13php?id=56608

[٦] جوزيف س. ناي، مقالة بعنوان الحرب والسلام في الفضاء الإلكتروني، جريدة الغد الالكترونية، كمبريدج، ٢٠ نيسان ٢٠١٢ الرابط الالكتروني : http://www.alghad.com/articles/617909

[٧] بيتر سيبنجر وآلان فريدمان، كيف سيواجه العالم تحديات الامن السيبراني، عرض محمد محمود السيد، مجلة السياسة الدولية، الرابط الالكتروني: www.siyassa.org.eg/newscontent/4/96/4925.

[٨] خالد بن سلطان بن عبد العزيز، موسوعة مقاتل من الصحراء، الاصدار السادس عشر، ٢٠١٥، الرابط الالكتروني : http://www.moqatel.com/openshare/Behoth/Askria6/ElectroWar/sec03.doc_cvt.htm

[٩] الحرب في الحيز الافتراضي، مجلة قضايا اسرائيلية، العدد ٤٣-٤٤، شتاء ٢٠١٢، ص٣ .

[١٠] ضياء الدين زاهر، الحروب غير المتكافئة :الجيل الرابع وما بعده، مقال منشور على الرابط الالكتروني www.acrseg.org21410، ٢٠١٤ .

[١١] خالد وليد محمود، مصدر سابق، ص٣١ .

[١٢] شبكة المعلومات الدولية (الانترنت)،الموقع الرسمي لإذاعة CNN بالعربية، الرابط الالكتروني: http://www.arabic.cnn.comhgl,ru

[١٣] محمود محارب، اسرائيل والحرب الالكترونية، المركز العربي للأبحاث ودراسة السياسات، معهد الدوحة، الدوحة، ٢٠١٢، ص٤-٨ .

[١٤] عادل شهبون، حروب السايبر- المعارك الجديدة بين الدول، الاهرام الرقمي، ٢٠١١/٦/٤ الرابط الالكتروني :

http:\\www.digital.ahram.org.eg\articles.asx?serial=52342eid=110

[١٥] أحمد ابو طالب، أنو نيموس : القرصنة السياسية عبر الفضاء الالكتروني، الاهرام الرقمي ٢٠١٢/١/١ الرابط الالكتروني :

http://www.digital.ahram.org.eg\politcly.aspx?serial=780539

[١٦] هلجا طويل الصوري، الاحتلال الرقمي الاسرائيلي لغزة، سلسلة دراسات انظمة المراقبة في الوطن العربي، مجلة عمران للعلوم الاجتماعية والانسانية، المركز العربي للأبحاث ودراسة السياسات، العدد/٧، المجلد/٢، شتاء ٢٠١٤،ص١-٢٤.

[١٧] سامر مؤيد عبد اللطيف، الحرب في الفضاء الالكتروني رؤية مستقبلية، مجلة رسالة الحقوق، السنة السابعة، العدد الثاني، مركز الدراسات القانونية والدستورية، جامعة كربلاء، ٢٠١٥، ص٩٢-٩٣ .

(*) مجموعة العشرين + الامم المتحدة : تم تشكيل هذه المجموعة لوضع القوانين الخاصة بالفضاء الالكتروني ليكون متاحاً لجميع الافراد وعلى مستوى العالم وفق بعض الضوابط والقواعد المهنية العالمية .

(١٨) خافيير سولانا، الحرب والسلام في الفضاء السيبراني، مقال تم نشره في جريدة الغد الالكترونية، ٨ آيار ٢٠١٥ . الرابط الالكتروني :

www.alghad.com/articles/869054

(*) تقرير التنمية البشرية للأمم المتحدة ٢٠١٤ وهو من سلسلة تقارير تصدر سنوياً عن برنامج الامم المتحدة الانمائي منذ عام ١٩٩٠، وهي تقارير موضوعية تتضمن تحاليل مدعّمة بالوقائع وتتناول القضايا والاتجاهات والسياسات الانمائية . للاطلاع على التقرير كاملاً من خلال الرابط الالكتروني:

http://hdr.undp.org