المؤتمر الفصلي لكلية العلوم السياسية في الجامعة المستنصرية

في ٢٠١٩/٢/٢٧

(الصراع السيبراني)

مفهومه واثره في العلاقات الدولية

الأستاذ الدكتور
موسى محمد آل طويرش
كلية العلوم السياسية- الجامعة المستنصرية

تطورت ادوات الصراع في العلاقات الدولية عبر الحقب الزمنية المختلفة طبقا لما انتجه العقل البشري من اساليب مختلفة للقتل والتدمير، لتتحول من اسلحة تقليدية الى نووية وصولا الى انواع اخرى اكثر تأثيرا كالبايلوجية والنترونية وغيرها.

الا ان القرن الحادي والعشرين شهد انواعا مختلفة من ادوات الصراع في العلاقات الدولية وتحولا في مفهوم القوة اتجاه القدرات (المعلوماتية) او ماطلق عليه بالصراع السيبراني **(cyber conflict)** مستفيدة من الفضاء الالكتروني. (١)

السؤال الذي ستحاول الورقة البحثيه الاجابة عليه هو كيف اثرت القدرات السيبرانية على احداث تحول في مفهوم القوة*،وماهي مكوناتها وادواتها، ومن هم الفاعلون في استخدامها؟ بدأ الاهتمام في هذا الموضوع بوضع فرضيات نظرية تدرس امكانية استخدام او تصميم اسلحة رقمية مستفيدين من الثورة العلمية الهائلة في مجال علم الحاسوب والانترنيت،تتفوق هذه الاسلحة على العتاد العسكري التقليدي المادي وتكون بديلة عنه لاحداث اكبر ضرر في منشئات العدو العسكرية والمدنية باساليب اكثر يسر واقل خسائر. ومن هنا عكف على وضع برامج متطورة تخترق بيانات الجهة المستهدفة ومعلوماتها ونشاطاتها العسكرية والتأثير على منشئاتها الحيوية واطلق على هذا النشاط بالقدرات السيبرانية. ويعرفه المختصون : بانه استخدام ذكي لتكنلوجيا الحاسوب في الفضاء الالكتروني لتقويض وضائف الشبكات الالكترونية للعدو ذات الاغراض القومية او السياسية من خلال التلاعب بالنظام او تدميره او انتهاك سيرته او تعديلها او منع الوصول اليه لاحداث تأثير او تغيير في التفاعلات السياسية والعسكرية بين الكيانات المختلفة بعيدا عن المعارك التقليدية واستخدام السلاح.(٢) اذ ان الصراع السيبراني لايدور في مساحة جغرافية محددة ولا زمان معين، فمساحته مفتوحة على كل المجالات والاماكن تبدأ من الاقمار الصناعية ووسائل التواصل الاجتماعي وليس انتهاءا بالطائرات المسيرة والروبوتات. وفقا لذلك فالصراع السيبراني يعني تلك الهجمات الالكترونية التي تعتمد برامج معقدة بهدف احداث خلل بمنشئات العدواو شلها كأمدادات الماء والكهرباء او تعطيل البنوك والمؤسسات المالية وتخريب البنى التحتية واختراق البيانات والمعلومات العسكرية،ويصنف هذا النشاط بانه من اساليب الحرب الناعمة او الحرب الذكية.

كان اول تطبيق عملي معلن لهذا النشاط عام ٢٠٠٥ عندما شنت الصين هجمات الكترونية ضد اجهزة كومبيوتر خاصة بوزارة الدفاع الامريكية،وكذلك الهجوم الالكتروني ضد الكلية البحرية الامريكية والذي عطل اجهزة الحاسوب فيها. كما شنت روسيا هجمات الكترونية على استونيا عام ٢٠٠٧ تعطلت خلالها لمدة ثلاث اسابيع التعاملات المصرفية ودمرت عدد من المواقع الرسمية والحزبية في استونيا، وكذلك الهجوم الروسي على جورجيا عام ٢٠٠٨ .(٣)

في حزيران عام ٢٠١٠ ظهرت الى العلن بوادر تأثيرتلك القدرات بشكل اكثر اتساعا وخطورة عندما اكتشف فايروس الكتروني مدمر باسم**(stuxnet)** والذي تمكن من اختراق اكثر من عشر مواقع صناعية ايرانية فائقة الحساسية كمعامل تخصيب اليورانيوم ،بهدف سحب المعلومات منها ومن ثم تدميرها. وقد وجهت اصابع الاتهام الى اسرائيل والولايات المتحدة . وعلى الرغم من نفيهما لتلك الاتهامات فقد مثلت هذه العملية نقلة نوعية في اساليب المواجهة في العلاقات الدولية كادوات فعالة في تحقيق الاهداف بعيدا عن استخدام الصواريخ والقنابل والطائرات.(٤)

يحدد الخبراء مجموعة من الاساليب التي تعمل عليها القدرات السيبرانية اهمها :

أ - تخريب ومهاجمة مواقع الانترنيت لتدمير او تشويه مواقع الخصم عبر نشر النصوص والصور المسيئة، كما حصل في الهجوم الالكتروني في استونيا عام ٢٠٠٧ عندما تعرضت

مواقع حكومية وموقع رئيس الوزراء للتضليل ونشر اخبار واقتباسات معادية. **ب-** الحرمان من الخدمة وتهدف الى غلق المواقع الالكترونية وتوقف الخدمة في الدوائر الحكومية والواقع الرسمية للدولة . **ج-** الاقتحام الفايروسي ،اذ ان هذا النوع من الهجمات يظل كامنا في اجهزة الحاسوب ويصعب الكشف عنه ويقوم بسرقة المعلومات وفق برامج معقدة ومن ثم تخريب البرامج* . د- عمليات التسلل(**Infiltrations**) اذ يقوم المهاجم بمحو جميع البيانات داخل الشبكة الالكترنية للخصم .ويمكن ايراد امثلة مختلفة عن مثل تلك الهجمات والتي اعلن عنها في وقت متاخر من وقوعها،ففي عام ٢٠٠٩ تم اختراق مواقع للبيت الابيض ووكالة الامن القومي والادارة الاتحادية للطيران في الولايات المتحدة ، وفي عام ٢٠١١ اعلن نائب وزير الدفاع الامريكي ان اكثر من ٢٤ الف ملف من ملفات وزارة الدفاع قد سرق ،وفي عام ٢٠١٢ تم تدمير ٣٥ الف جهاز كومبيوتر تابع لشركة ارامكو السعودية واتهمت ايران بتدبيرها .(٥)

ان اهم ميزات هذا الصراع انه نموذج للحرب غير المتكافئة وذلك لانه بامكان صغار الفاعلين دول او افراد او منظمات ممارسة التاثير في العلاقات الدولية، فينقسم الفاعلين الى الدول والحكومات اذ اصبح الفضاء الالكتروني مجالا مناسبا للصراع بهدف ردع الخصم وتعطيل قدراته من خلال استهداف بناه المدنية والعسكرية. وهناك فاعلون من غير الدول كالشركات المتعددة الجنسية اذ اصبحت شركات مثل غوغل وميكروسفت لها قدرات تسمح لها بامتلاك بيانات هائلة يستطيع من خلالها التاثير الاقتصادي والسياسي للدول (٦). وهناك الفصائل المسلحة والارهابية* والقراصنة الالكترونيين فضلا عن مايطلق عليهم (الانونيموس) او المجهولون والذين يمثلون جماعات احتجاجية حول العالم ينشطون في الفضاءات الالكترونية ولهم اهداف سياسية،وان انخراط الافراد فيها يكون بلا عضوية وبلا هوية ويوصفون بانهم (قيادة بلا جسد)، والمثال على ذلك الثورة المصرية عام ٢٠١١ والتي اشتعلت بفعل جهات قادت الجماهير الكترونيا (٧).

لقد اهتمت الدول بما اطلق عليه بالردع السيبراني ،اذ اهتمت الدول بشكل كبير جدا بتطوير قدراتها السيبرانية لتحقيق هدفين الاول حماية منظوماتها الالكترونية من الهجمات المعادية والثاني تعزيز القدرات الهجوميه السيبرانية لتحقيق اهداف يصعب تحقيقها بالاساليب التقليدية . فقد قامت الحكومة الايرانية عام ٢٠١٢ بتاسيس المجلس السيبراني الاعلى لتوحيد الانشطة الالكترونية ووضع خطة دفاعية للمنشئات الحيوية(٨). واعلن الرئيس الروسي بوتين في ٢٠٠٨ عن وضع استراتيجية القوة الهجومية والدفاعية الالكترونية ، كما سبق ذلك استحداث وزارة الامن الوطني في الولايات المتحدة بالتزامن مع اصدار قانون الامن الوطني عام ٢٠٠٢.وتشير الاحصاءات الى انفاق الدول مبالغ طائلة لتعزيز قدراتها كالولايات المتحدة واسرائيل والصين بما يقدر باكثر من مئة مليار دولار عام ٢٠١٥ فقط.

ان مايميزالصراع السيبراني فقدانه للمعاييرالتي تضبط مساراته وكيفية السيطرة على الانشطة الضارة كالانشطة الارهابية ، فضلا عن ذلك فان هناك عدم تمييز بين ماهو مدني او عسكري،فان احتمال وقوع الضر ر على المدنيين امر قائم عندما تستهدف البنى المدنية

كالكهرباء والمواصلات والبنوك بهجمات تخريبية .كما ان هذا النشاط غير مؤمن من العقوبات القانونية وانه يوفرمظلة تحمي الفاعلين وتخفي هوياتهم.

ان المستقبل يشير الى تصاعد حدة هذا الصراع بشكل خطيرلاسيما بعد اكتشاف تاثير القدرات السبرانية على تغيير الواقع الداخلي لدول كبرى كما حصل بالتدخل الروسي في الانتخابات الامريكية ، وكذلك المؤشرات التي دلت على التدخل الروسي في استفتاء خروج بريطانيا من الاتحاد الاوربي .بالمقابل فان الدول المتخلفة في هذا المجال ستكون عرضة للتاثير والتلاعب على مختلف الصعد كون العصر القادم هو عصر القدرات الالكترونية التي لامجال فيها للضعفاء والمتخلفين فيه.

التوصيات :

اذ ان القدرات السيبرانية اصبحت من اهم الادوات التي تستخدمها دول ومنظمات وافراد في نشاطها لتهديد الامن الوطني للدول بكافة مفاصله ،واذ ان العراق يعد بحكم موقعه الاستراتيجي فاصلا او حاجزا لقوى متنافسة اقليمية ودولية وهو معرض لمخاطر وتهديدات مختلفة، لذا فانه يستوجب على الحكومة العراقية الاهتمام بشكل مركز لبناء وتطوير القدرات السيبرانية بكفاءات عراقية باعتبار تلك القدرات اداة وسلاح اساسي لحماية امنه الوطني بمختلف تفرعاته الاقتصادية منها او العسكرية او الاجتماعية ، ويكون ذلك وفق ثلاث اتجاهات :

أ- بناء منظومة الكترنية دقيقة ومتطورة لمنع الهجمات الالكترونية التي تستهدف مفاصل الدولة المختلفة لاسيما المتعلقة بالامن الوطني العسكرية منها والمدنية كالنشاط المصرفي والمالي والمؤسسات الاخرى .
ب- ايجاد قدرات الردع اللازمة ليس للحماية من الهجمات الالكترونية فحسب وانما القدرة على الرد المباشر .
ت- تطويرالقدرات العراقية في شن هجمات سيبرانية ضد قوى معادية بغية الحد من مخاطرها ومعرفة نواياها العدوانية .

ويتطلب ذلك اجراءات عدة :

أ- توفير التخصيصات المالية اللازمة وتحديدها في الميزانية العامة لتطويرالقدرات السيبرانية اسوة بباقي الدول التي ترصد مليارات الدولارات لهذا النشاط لارتباطه بامن الدولة بكل مفاصلها .
ب- بناء منظومة الكترنية متكاملة تابعة للامن الوطني او وزارة الدفاع تضع الدراسات والخطط والتنفيذ للنشاط السيبراني، مع تدريب الكفاءات العراقية وتوفير كل الامكانات المادية لذلك .
ت- وضع مناهج متكاملة في الجامعات العراقية مع توفير المختبرات اللازمة لتوسيع القاعدة الشبابية العلمية بين طلبة الجامعات للنشاط الالكتروني البناء.

الهوامش:

(١) يشير الباحثين الى ان استخدام مصطلح القوة السيبرانية اكثر دقة من القوة الاكترونية التي تترجم الى (Electronic power) اذ ان المقصود هو (Cyber power) وهي اكثر شمولية في مانقصده في التعاملات الدولية. ينظر : ايهاب خليفه،القوة الالكترونية ..كيف يمكن ان تديرالدول شؤونها في عصر الانترنيت،القاهرة-٢٠١٧ ،ص٥.

(*)تعرف القوة على انها القدرة على التأثير في الاخرين للحصول على نتائج محددة يسعى لها طرف ما ، وتربط القوة بمفهوم التحكم والمكاسب .للمزيد ينظر :القوة : كيف يمكن فهم تحولات القوة في السياسة الدولية،ملحق مجلة السياسة الدولية، القاهرة ،العدد ١٨٨ ،ابريل-٢٠١٢ .

(٢)سماح عبد الصبور،الصراع السيراني، طبيعة المفهوم وملامح الفاعاعلين ،ملحق مجلة السياسة الدولية ، القاهرة ،العدد ٢٠٨ ، ابريل-٢٠١٧، ص.٥

(٣) ايهاب خليفة ، المصدر السابق، ص٢١.

(٤) برنامج (ستاكسنت) يستهدف اجهزة الحاسوب للبرنامج النووي الايراني واشارت الاجهزة الاستخبارية الايرانية انه اصاب اكثر من ستة عشر الف جهاز كومبيوتر، ينظر: جريدة الشرق الوسط، ٣ اذار -٢٠١٣.

(*) من اشهر الفايروسات التي استخدمت في الهجمات السيبرانية اضافة الى ستاكسنت يوجد فايروس يسمى (Flam) والذي صمم لسرقة المعلومات للانظمة المستهدفة في الملفات المخزونة والمحتويات المعروضة على الشاشة وحتى النسجيلات الصوتية.

(٥) احمد زكي عثمان ،تأثيرات القدرات السيبرانية في الصراعات الاقليمية ، ملحق مجلة السياسة الدولية،القاهرة العدد ٢٠٨ في ابريل ٢٠١٧، ص١٧ .

(٦) كان من تائج الخلاف الصيني مع شركة كوكل توتر العلاقات الامريكية الصينية في عهد الرئيس اوباما.لمزيد عن طبيعة الخلاف ينظر ايهاب خليفة ، المصدر السابق ، ص ٦٩ .

(٧) تكاثرت المواقع التي توصف بالجهادية الى ٦ الاف موقع عام ٢٠١٠ ،

(٨) احمد زكي عثمان ، المصدر السابق ،