

انعكاسات تطور القوة المعلوماتية الأمريكية في البيئة الداخلية

أ.م.د. دنيا جواد مطلق* أحمد عبد الجبار عبد الله**
 باحثة من العراق باحث من العراق

* كلية العلوم السياسية - جامعة بغداد
 ** باحث دكتوراه - كلية العلوم السياسية - جامعة بغداد
 marfaa_albasra@yahoo.com

الملخص

تعتمد قوة الدولة فيما يطلق عليه بمجموعة العوامل الرمزية في التفاعلات الدولية، سواء كان ذلك على المستوى الإقليمي أم الدولي في البيئة الداخلية بالدرجة الأساس، إذ تعد الركيزة الأساس التي تعتمد عليها الدولة في بناء سياساتها العامة، وتأتي من بعدها البيئة الخارجية، لما تحيط به من متغيرات وأحداث مضطربة، وتشكل بمجموعهما البيئتين الداخلية والخارجية المجال الذي تنطلق فيه السياسة بشكلها العام، فان كانت البيئة صالحة ومستقرة وغير مضطربة وتتماشى مع الرؤية العامة للدولة، كانت سياسة الدولة قوية مستندة إلى أساس قوي، والعكس صحيح، وتتمتع الولايات المتحدة الأمريكية ببيئة داخلية مستقرة صالحة للعمل تنسجم مع رؤية الدولة في بناء استراتيجية تتماشى مع تطلعاتها، وبالنتيجة تتكيف مع البيئة الخارجية وفقاً لما تتطلبه مجموعة الأهداف القومية، وتعد القوة الجانب المهم في بناء الاستراتيجية، وركيزة مهمة في رسم السياسة الخارجية للدولة، ومن خلال مراحل تطور القوة وصولاً للمعلوماتية، كيفت الولايات المتحدة الأمريكية هذه القوة ووظفتها في سبيل تحقيق اهدافها العليا من خلال التأثير في البيئة الداخلية.

The Implications of The Development of the American Information Power in The Internal Environment

Prof. Asst. Dr. Dunia Jawad Mutlaq
 Researcher From Iraq
 College of Political Sciences

Ahmed Abdul-Jabbar Abdullah
 Researcher from Iraq
 University of Baghdad

Abstract

The strength of the state depends on what is called a set of symbolic factors in international interactions, whether at the regional or international level main-

ly in the internal environment, as the pillar is the basis upon which the state depends on building its public policies, and then comes the external environment, because of the surrounding Variables and turbulent events, and together their internal and external environments constitute the field in which politics is launched in its general form. If the environment is valid, stable, and not disturbed and in line with the general vision of the state, the state's policy is strong, based on a strong foundation, and vice versa.

The United States of America has a stable internal environment suitable for work that is consistent with the vision of the state in building a strategy that is in line with its aspirations, and as a result it adapts to the external environment according to the requirements of the national goals group. The power is the important side of building strategy, and a basic pillar in planning the state foreign policy. The evolution of power to informatics. The United States of America adapted and used this force to achieve its higher goals through influencing the internal environment. Therefore, the research will be addressed in two axes, as following: the first: the level of security, and the second: the military doctrine.

المقدمة:

تعد البيئة الداخلية من البيئات المهمة في سياسات الدول، وذلك لما تحتويه من أحداث ومتغيرات تؤثر في عملية صنع القرار السياسي، وبالنتيجة هي انعكاس لمتطلبات البيئة الخارجية استجابة للظروف المادية، فمجموعة الافكار والمعتقدات وكل المتبنيات المجتمعية التي تشكل على مر العقود، لاسيما في ظل التطور التكنولوجي، هي بمثابة بيئة تفاعل خصبة تعكس واقعاً مجتمعياً معيناً تشكل في ظله مجموعة عوامل تسهم في عملية صياغة استراتيجية معينة تتواءم وذلك الواقع، وبالنتيجة تسهم في عملية مستوى امن الدولة، وانسجاماً مع هذا الواقع الذي فرضته مجموعة العوامل البيئية الداخلية، فان القوة الامريكية لاسيما مع تطور قوتها المعلوماتية، احدثت تغيرات مهمة في بيئتها الداخلية، وفرضت واقعاً مغايراً لما كانت عليه فيما سبق في مستوى الامن وتبني عقيدة استراتيجية تنسجم وطبيعة هذه المتغيرات، وعليه سيتم تناول البحث في محورين، وكالاتي: الأول: مستوى الامن، والثاني: العقيدة العسكرية.

المحور الاول: مستوى الامن

أصبح (الفضاء الالكتروني) مجالاً جديداً للفعل والتأثير في النظام الدولي، ومع الانتقال من مرحلة النمو السريع الى مرحلة الاستعمال الكثيف لتكنولوجيا

المعلومات، أصبحت قضية (أمن الفضاء الإلكتروني) تحظى باهتمام متصاعد من اجندة الأمن الدولي، وزادت العلاقة بين الأمن والتكنولوجيا وثوقاً مع إمكانية تعضيد المصالح الاستراتيجية ذات الطبيعة الإلكترونية، إلى أخطار تهدد بتحول الفضاء الإلكتروني إلى ساحة للصراع الدولي متعدد الأطراف⁽¹⁾، وأصبح الأمن السيبراني يشكل جزءاً أساسياً من أي سياسة أمنية وطنية، وبات من المعلوم أن صناع القرار في الولايات المتحدة الأمريكية والاتحاد الأوروبي وروسيا والصين والهند وغيرها من الدول يصنفون مسألة الأمن السيبراني كأولوية في سياساتهم الدفاعية الوطنية⁽²⁾.

فمن جانب أصبحت قضية أمن الفضاء الإلكتروني تدخل في استراتيجيات الأمن القومي للعديد من الدول من أجل الاستحواذ على مصادر القوة في الفضاء الإلكتروني، وللحيلولة دون تعرض بنيتها التحتية الحيوية للخطر الذي ينجم جراء قطع خدمة الإنترنت أو ضرب مواقعها أو توقف رسائل البث الإذاعي أو التلفزيوني أو توقف موجات الراديو أو سقوط شبكات المحمول أو البث الفضائي، فقد أصبح لها تأثير عميق في المجتمع والاقتصاد على النطاق الدولي، وبذلك دخل المجال الإلكتروني ضمن المحددات الجديدة للقوة وأبعادها، من حيث طبيعتها وأنماط استخدامها وطبيعة الفاعلين، وهو ما كان له انعكاس على قدرات الدول وعلاقاتها الخارجية⁽³⁾.

وعليه دفعت التهديدات المتزايدة لأمن الفضاء الإلكتروني العديد من الدول للعمل على بذل الجهود فرادى وجماعات بشأن الحفاظ على أمن الفضاء الإلكتروني

(2) الهيئة المنظمة للاتصالات، لمحة عامة حول الأمن السيبراني، لبنان. متاح على الموقع:

<http://www.tra.gov.lb/Cybersecurity-in-few-words-AR>

للمزيد ينظر: تغريد معين حسن المشهدي، الأثر العسكري للأمن السيبراني في الجغرافيا السياسية للدولة، مجلة البحوث الجغرافية، جامعة الكوفة، كلية الآداب، العدد (30)، 2019، ص ص244-245.

(3) نورة شلوش، القرصنة الإلكترونية هي الفضاء السيبراني «التهديد المتصاعد لأمن الدول»، مجلة مركز بابل للدراسات الإنسانية، مركز بابل للدراسات الحضارية والتاريخية، جامعة بابل، العدد (2)، 2018، ص200.

(1) ما أن تم انتخاب الرئيس الأمريكي الاسبق (رونالد ريغان) (1981-1989) حتى قدم استراتيجية للأمن القومي تألفت من أربعة اتجاهات: دبلوماسية واقتصادية وعسكرية ومعلوماتية، تم التركيز فيها على العناصر المعلوماتية، وجرى المحافظة عليها في الوثائق اللاحقة لمسائل الأمن القومي، وفي كانون الثاني 1983 وقع (ريغان) على نظام قيادة الدبلوماسية الحكومية المرتبطة بأهداف الأمن القومي، وأعطى النظام حدوداً واسعة للنشاطات الدبلوماسية الحكومية، وأكد على أنه يتضمن إجراءات حكومة الولايات المتحدة الأمريكية الموجهة نحو دعم سياسة الأمن القومي الأمريكية أيضاً، وهذا يعني أن النظام أصبح يقوم بتنظيم وتنفيذ دائرة واسعة من الإجراءات المعلوماتية، والأكثر من ذلك وفر هذا النظام الظروف المناسبة لإعداد آليات تخطيط وتنسيق النشاطات الاجتماعية والمعلوماتية والسياسية لإدارة الولايات المتحدة الأمريكية، والمسائل المتعلقة بالثبوت الإذاعي المسموع والمرئي، كما جرت في نفس الوقت تبدلات جذرية في نظرية تطبيق التأثير المعلوماتي، وبدء عصر الصراع العالمي على الوعي الجماهيري للشعوب باستخدام أحدث تكنولوجيا المعلوماتية من خلال تنسيق نشاطات كل الأجهزة الحكومية والاتحادات العابرة للقوميات، وبذلك أصبحت الأجهزة الحكومية تستخدم إلى حد متنامي كمراكز تنسيق موجة التأثير المعلوماتي والنفسي والدور الرئيس في عملية تنسيق نشاطات أجهزة التأثير المعلوماتي والنفسي الذي أصبح يؤديه مجلس الأمن القومي في الولايات المتحدة الأمريكية، والذي كانت وظيفته عقيدة الدعاية النفسية للأمن القومي كفقرة مركزية في نظام العمليات النفسية إلى جانب الإدارة الحكومية، والمنظمات الدولية، وإدارة التجسس المركزية، ووكالة المعلومات في الولايات المتحدة الأمريكية (يوسيدا)، ورافقها ظهور آليات التنسيق العالمي للتأثير المعلوماتي والنفسي على المجتمع الدولي والتي شملت: رئيس الولايات المتحدة الأمريكية ومجلس الأمن القومي والوزارات (الإدارات) ومنظمات الولايات المتحدة الأمريكية العاملة في الساحة الدولية، كما جاءت نشاطات أجهزة المعلوماتية والنفسية (الحكومية، والمنظمات الاجتماعية والتجارية) بشمارها لتسيطر الولايات المتحدة الأمريكية على الساحة المعلوماتية العالمية، ولم تزل الولايات المتحدة الأمريكية اليوم تسعى بمساعدة شبكة الإنترنت المتطورة في فرض استراتيجية تفوقها على الساحة المعلوماتية العالمية خلال القرن الواحد والعشرين. المصدر: محمد البخاري، المعلوماتية والعلاقات الدولية في عصر العولمة، مجلة الفيصل، دار الفيصل الثقافية، الرياض، العدد (320)، 2003، ص43. للمزيد ينظر: عادل عبد الصادق، القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، مجلة السياسة الدولية، مؤسسة الاهرام، القاهرة، العدد (188)، 2012، ص28.

اثر الفضاء الإلكتروني في تغيير نمط القوة من حيث طبيعة وخصائص الامن والصراع في المشهد الدولي

لديها، سواء كان ذلك متمثلاً في انشاء هيئات لمواجهة الطوارئ المعلوماتية أو استحداث قوانين لمكافحة الجريمة الإلكترونية، أو إنشاء قيادة عسكرية لحماية الفضاء الإلكتروني، أو استحداث وحدات للحرب الإلكترونية داخل الجيوش العسكرية، أو المشاركة في مناورات إلكترونية لتحسين القدرات الدفاعية أمام الهجمات الإلكترونية، فضلاً عن إطلاق العديد من المبادرات التي تقوم بها

المنظمات الحكومية وغير الحكومية لدعم الأمن الإلكتروني، مثل الاتحاد الدولي للاتصالات الذي اطلق مبادرة للأمن الإلكتروني، وحلف شمال الأطلسي الذي أنشأ وحدة للدفاع الإلكتروني، كما أطلق الاتحاد الأوروبي مبادرة للأمن الإلكتروني، ومن ناحيتها تبنت الولايات المتحدة الأمريكية (الاستراتيجية الدولية للفضاء الإلكتروني)، وهي أول وثيقة سياسية من هذا النوع تبين الرؤية الشاملة لمستقبل التعاون الدولي المتعلق بالفضاء الإلكتروني⁽⁴⁾، فعلى سبيل المثال جرى خلال تسعينيات القرن الماضي في روسيا الاهتمام بهذه المسألة وأنشأت لجنة مشتركة من مختلف الإدارات الحكومية للاهتمام بالأمن المعلوماتي ضمن مجلس الأمن القومي الفيدرالي الروسي، وأعدت مشاريع عكست في مضمونها أساليب ووسائل وطرق حماية المصالح الحيوية للأفراد والمجتمع والدولة على الساحة المعلوماتية العالمية المفتوحة في عالم اليوم⁽⁵⁾.

بذلك اثر الفضاء الإلكتروني في تغيير نمط القوة من حيث طبيعة وخصائص الامن والصراع في المشهد الدولي، سواء كان على المستوى النظري أو التطبيقي، فقد كانت معادلة القوة الشاملة للدولة في السابق ترتبط بتزايد القوة العسكرية والاقتصادية والسياسية والدبلوماسية والمجتمعية، وهذه القوة تسير في اتجاه ردع الآخرين، إذ أصبح لها تأثيرات وشواهد واضحة في العلاقات الدولية، وتم ذلك عبر متغيرات ثلاث هي:⁽⁶⁾

1- إعادة التفكير في مفهوم الامن القومي للدولة، إذ ان الامن السيبراني لم يقتصر فقط على بعده التقني، بل تعداه الى ابعاد اخرى في ظل تراجع سيادة الدولة، وتزايد العلاقة بين الامن والتكنولوجيا، وتأثير ذلك في المصالح الاستراتيجية للدول.

2- تعظيم القوة أو الاستحواذ على عناصرها الاساسية في العلاقات الدولية، إذ أصبح التفوق في ذلك المجال عنصراً حيوياً في تنفيذ عمليات ذات فاعلية في الارض والبحر والجو والفضاء، واعتماد القدرة القتالية في الفضاء الإلكتروني

(4) عادل عبد الصادق، القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، مجلة السياسة الدولية، مؤسسة الاهرام، القاهرة، العدد (188)، 2012، ص28.

(5) محمد البخاري، الثورة المعلوماتية فجرت الحواجز القائمة بين الشعوب والدول، مجلة المعرفة، دمشق، العدد (576)، 2011، ص53.

(6) عبد الغفار رعيصفي الديوك، مستقبل الصراع السيبراني العالمي في القرن الـ 21، مجلة السياسة الدولية، مؤسسة الاهرام، القاهرة، العدد (214)، 2018، ص31.

على نظم التحكم والسيطرة التكنولوجية، وبات الفضاء الإلكتروني مسرحاً لشن هجمات مدمرة (مادياً ومعنوياً).

3- بروز أنماط جديدة من الصراع كمجال تنشأ فيه نزاعات بين الفاعلين المختلفين، وتعبيراً عن تعارض المصالح والقيم سواء بين الفاعلين من الدول أو الفاعلين من غير الدول.

فرض الفضاء الإلكتروني إعادة التفكير في مفهوم الامن

على اثر ذلك فرض الفضاء الإلكتروني إعادة التفكير في مفهوم الامن، الذي يتعلق بتلك الدرجة التي تمكن الدولة من ان تصبح في مأمن من خطر التعرض للهجوم العسكري او الارهابي، واجراءات الحماية ضد تعرض المنشآت الحيوية للبنية التحتية للأعمال العدائية، وأصبح الفضاء الإلكتروني يواجه بتهديدات متصاعدة نتيجة ارتباط العالم المتزايد به، مما عمل على زيادة خطر تعرض البنية التحتية الكونية للمعلومات لهجمات الكترونية، وكذلك استخدام الفاعلين من غير الدول الفضاء الإلكتروني لتحقيق اهدافهم وتأثير ذلك على سيادة الدولة⁽⁷⁾.

كما احدث الفضاء الإلكتروني ثورة في عمل اجهزة الاستخبارات الدولية، ودخلت في تحديد اهداف ومهام ومراحل تنفيذ الانشطة الاستخبارية سواء تلك التي تتم في المجال الخارجي او داخل الدول، واستفادت تلك الاجهزة بتوافر كم هائل من المعلومات التي كانت تعاني في السابق من شحتها وصعوبات في التحليل، مما زاد من اهمية العنصر البشري في العمل الاستخباراتي⁽⁸⁾، فحسب المدرسة الواقعية ان الدول تسعى إلى إتباع سياسة الاعتماد على النفس في المجال الأمني، وهي بذلك تخلق ردة فعل مقابل الدول الأخرى، وبالنتيجة ستخلق حالة من انعدام الأمن⁽⁹⁾، كل هذه الديناميكيات هي مثال على المعضلة الأمنية حسب راي المدرسة الواقعية، فعند اتخاذ الدولة تدابير دفاعية يمكن للدول الأخرى إدراك مثل هذا السلوك باعتباره تهديداً لها ومن ثم الاستجابة له وفقاً لذلك، إذ تكمن وراء هذه المعضلة صعوبة التمييز بين الهجوم والتحركات الدفاعية عند محاولة تقييم النوايا لدولة أخرى⁽¹⁰⁾.

وقبل الدخول في تعريف الامن الإلكتروني لابد من تعريف الامن القومي أولاً، فالأمن القومي يعرف انه: «مجموعة القواعد الحركية التي يجب على الدولة ان تحتفظ باحترامها وان تفرض لنفسها نوعاً من الحماية الذاتية والوقائية الاقليمية، وهو بهذا المعنى يصبح في جوهره مجموعة التقاليد القومية التي تسير عليها السياسة العملية بثبات في علاقاتها، بحيث تضمن الا تؤخذ على حين غرة من عدو محتمل

(7) عادل عبد الصادق، اسلحة الفضاء الإلكتروني في ضوء القانون الدولي الانساني، سلسلة أوراق، وحدة الدراسات المستقبلية، الاسكندرية، العدد (23)، 2016، ص 30-36.

(8) عادل عبد الصادق، اسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، مصدر سبق ذكره، ص 28.

(9) وصفي محمد عقيل، التحولات المعرفية للواقعية والليبرالية في نظرية العلاقات الدولية المعاصرة، مجلة دراسات للعلوم الإنسانية والاجتماعية، عمادة البحث العلمي، الجامعة الاردنية، العدد (1)، 2015، ص 110.

(10) Alyza Sebenius, Writing the Rules of Cyber war, Harvard Kennedy school belfer center Cyber war, June 28, 2017. Available on site :<https://www.belfercenter.org/publication/writing-rules-cyberwar>

(11) نقلا عن: عامر هاشم عواد، حدود الامن القومي الامريكي، مجلة المستنصرية للدراسات العربية والدولية، مركز المستنصرية للدراسات العربية والدولية، بغداد، العدد (42)، 2013، ص59.

(12) المصدر نفسه.

(13) جون باسيت، الحروب المستقبلية في القرن الحادي والعشرين، (ابو ظبي: مركز الامارات للدراسات والبحوث الاستراتيجية، 2014)، ص55.

(14) يونس مؤيد يونس، استراتيجية الولايات المتحدة الامريكية للأمن السيبراني، مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين، بغداد، العدد (55)، 2018، ص130.

(15) نورة شلوش، مصدر سبق ذكره، ص193.

يستطيع ان يستغل مواقف الضعف في طبيعة حدودها القومية⁽¹¹⁾، وهناك من عرفه بانه: «تامين كيان الدولة والمجتمع ضد الاخطار التي تهددها داخليا وخارجيا، وتأمين مصالحها وتهيئة الظروف المناسبة اقتصاديا واجتماعيا لتحقيق الاهداف والغايات التي تعبر عن الرضا العام في المجتمع»⁽¹²⁾. وبلاستناد الى تعريف الامن القومي يمكن تعريف الامن الالكتروني بانه: حماية البيانات الالكترونية والشبكات الالكترونية، وكذلك الاشخاص الذين يستخدمونها من اولئك الذين يعتمدون ممارسة الاذى او الضرر او السرقة او المضايقة او الاعمال المماثلة⁽¹³⁾، فالأمن الفضائي السيبراني هو مجموع القواعد التي يضعها مسؤولو الامن في اي مكان والتي يجب ان يتقيد بها جميع الاشخاص الذين يمكنهم الوصول اليه، فمفهوم الامن مفهوم واسع يطال جميع عمليات الدخول والخروج والبقاء او التصرف في مكان ما، وعليه يشمل الامن في الفضاء السيبري قواعد واصول ضبط الاتصال وانتقال المعلومات وتخزينها وحفظها، كما يشمل امن المواقع وامن الانظمة الالكترونية وعمليات استثمارها اضافة الى امن الاتصالات⁽¹⁴⁾.

وبذلك تصبح الدولة والافراد بمأمن من الاختراقات التي يتعرضون اليها سواء كان ذلك داخليا او خارجيا، ومن ثم يمكن للدولة الحفاظ على امنها القومي وتحقيق مصالحها الوطنية من خلال بناء منظومة امن متكاملة.

وبالاتساق مع ما تقدم أصبح الفضاء الإلكتروني يواجه تهديدات متصاعدة استجابة للبيئة الجديدة، وذلك من خلال:⁽¹⁵⁾

أولاً: ارتباط العالم المتزايد بالفضاء الإلكتروني، بما عمل على زيادة خطر تعرض البنية التحتية الكونية للمعلومات لهجمات إلكترونية.

ثانياً: استخدام الفاعلين من غير الدول للفضاء الإلكتروني لتحقيق أهدافهم وتأثير ذلك على سيادة الدولة.

ثالثاً: انسحاب الدولة من قطاعات استراتيجية مهمة لصالح القطاع الخاص ولاسيما المنشآت الحيوية، مما أدى الى تصاعد دور الشركات متعددة الجنسيات.

رابعاً: تأثير مواجهة الحرب الإلكترونية على حرية استخدام الفضاء الإلكتروني.

خامساً: إشكالية تعامل الدول مع الشركات التكنولوجية متعددة الجنسيات والتي أصبحت تفوق قدراتها، مثل: (الفيس بوك، وتوتر، واليوتيوب)، إذ أصبحوا فاعلين دوليين.

**أصبح الفضاء الإلكتروني
يواجه تهديدات متصاعدة
استجابة للبيئة الجديدة**

وعليه ازدادت حالة الانكشاف الأمني للدول باعتمادها المتزايد على الفضاء الإلكتروني، والتي أصبحت عرضة للاختراق والهجوم بالفيروسات وسرقة المعلومات أو إتلافها، وأصبحت معضلة جديدة للأمن بتحوله إلى نوع جديد يعتمد على الشبكات والإنترنت، وبرز مخاوف من ممارسة الدول لمثل تلك المعطيات إلى إمكانية اتجاه الجماعات الإرهابية في التأثير على أمن الفضاء الإلكتروني⁽¹⁶⁾، فالحكومات والقوات المسلحة ومراكز مراقبة حركة الطيران والبنية التحتية والصناعة وشركات التكنولوجيا وعالم الاستخبارات جميعها تعتمد وبشكل كبير على الحواسيب، كما ان هناك ملايين الاسرار والمشروعات فائقة التقدم مخزنة على أجهزة الحواسيب، وهذا يعني أن هذه المنظومات جميعاً معرضة للهجوم، ففي بريطانيا على سبيل المثال تتعرض حواسيب الحكومات والمنازل والشركات لديها لأكثر من 100 ألف هجوم سايري لكل 24 ساعة، وهذا يساوي 44 مليون هجوم لكل سنة،

(16) المصدر نفسه.

ازدادت حالة الانكشاف الأمني للدول باعتمادها المتزايد على الفضاء الإلكتروني

ويكبد ذلك الاقتصاد البريطاني خسائر هائلة تصل إلى 27 مليار جنيه استرليني، كما تعد مخاطر الوضع اشد سوءاً في الولايات المتحدة، إذ أن الحرب السيبرية وانقطاع الاتصالات والتجسس السائري يشكل أكبر تهديداً لها، وعلى اثر ذلك يسعى البتاجون وأجهزة الاستخبارات إلى تطوير القيادة السيبرية الأمريكية⁽¹⁷⁾، فعلى سبيل المثال تعمل منظومة الامن الأمريكية (التنفيذية والتطبيقية والرقابية) والتي هي مجموعة من الهيئات والوكالات الفيدرالية المسؤولة عن تطبيق وتنفيذ سياسات أمن المعلومات فيها، والتي لها ارتباطات مع باقي المؤسسات والوزارات القومية في الداخل الأمريكي، إذ تقدم لها الاستشارات والتطبيقات المعلوماتية والأمنية الإلكترونية، على ان يتم التنسيق مع العشرات من الوكالات الأمريكية، وعلى رأسها وكالة المخابرات الأمريكية ووكالة الأمن القومي، ووزارة الدفاع ومكاتب الاستطلاع الداخلية والخارجية والمكاتب المعنية بالشؤون الاقتصادية والاجتماعية، وغيرها من الجهات والوزارات القومية الأمريكية، بهدف إبقاء الوضع المعلوماتي متزن مع جميع الجهات، وبالنتيجة الحصول على قدر كاف من المعلومات المتعلقة بالأمن القومي الأمريكي⁽¹⁸⁾.

(17) مارك بيردسول، مستقبل الاستخبارات في القرن الحادي والعشرين، (ابو ظبي: مركز الامارات للدراسات والبحوث الاستراتيجية، 2014)، ص 16.

(18) وليد غسان سعيد، دور الحرب الإلكترونية في الصراع العربي الإسرائيلي، رسالة ماجستير (غير منشورة)، جامعة النجاح الوطنية، كلية الدراسات العليا، فلسطين، 2013، ص 46.

من هنا أصبحت مسألة الامن اكثر تعقيداً في ظل التكنولوجيا المتطورة التي يشهدها عالم اليوم، وذلك للأسباب الآتية:⁽¹⁹⁾

(19) روبرت كيوهان، مبني للمجهول: مآلات القيادة الأمريكية للنظام الدولي، ترجمة: أحمد محمد ابو زيد، مجلة المستقبل العربي، مركز دراسات الوحدة العربية، بيروت، العدد (404)، 2012، ص 53.

1 - استخدام تكنولوجيا الفضاء في امكانية اكتشاف الهدف وتتبعه والدقة في الوصول اليه والقدرة على تدميره.

2 - استخدام تكنولوجيا الفضاء في الاستطلاع والتصوير والمراقبة والاختراق والتجسس.

3 - استخدام تكنولوجيا التخفي والذكاء الصناعي واختراق الدفاعات المضادة والتهرب من الرادارات.

4- التفتن في الحصول على المعلومات والوصول إليها بسهولة ويسر.

**لعل الاشخاص هم اكبر
ثغرة امنية في امن الفضاء
الالكتروني**

ولعل الاشخاص هم اكبر ثغرة امنية في امن الفضاء الالكتروني سواء كانوا من العاملين داخل المؤسسة المستهدفة، ام من الاعضاء الموظفين الذين يرتكبون اخطاء حين تواجههم تدابير تكنولوجيا امن معلومات تتسم بالتعقيد وانعدام الترابط⁽²⁰⁾، لذلك تسعى الدول الى حماية الحسابات الإلكترونية والبريدية التابعة لها، حتى لا يتعرض أمنها القومي للخطر، إذ تمنح المسؤولين بموجبها حسابات بريدية رسمية، لكن في بداية العام 2015 وقبل أن تعلن وزيرة الخارجية الأمريكية السابقة (هيلاري كلينتون) عن نيتها لخوض الانتخابات الأمريكية، كشفت التقارير الصحفية عن استخدام (كليتون) (بريداً إلكترونياً)* خاصاً تستخدمه بدلاً من البريد الرسمي، وهو ما أثار المخاوف الأمريكية لتعرضه لعمليات قرصنة مما يهدد أمنها القومي⁽²¹⁾، إذ تعد مكافحة قرصنة الانترنت تحدياً كبيراً بالنسبة الى اجهزة الامن، ليس في مجال التجسس فقط، بل إن البنية التحتية الحيوية للعديد من الدول ومفاعلات الطاقة النووية ومحطات المياه وشبكات الغاز والكهرباء ووسائل النقل والمواصلات والمنشآت العامة الاخرى مثل المستشفيات وغيرها، جميعها تعتمد على منظومات حاسوبية، وهذه المنظومات كلها تعرضت في السنوات الاخيرة لهجمات سايبيرية⁽²²⁾.

فمن جانب مكنت العولمة الكوكبية التي يعيشها العالم قدرة الفواعل الدوليين ومنظمات دولية حكومية وغير حكومية وحركات تحررية واجتماعية دولية وحتى المنظمات الإرهابية على استخدام القوة الإلكترونية في تحقيق أهدافها. لذا، أصبحت هناك علاقة وثيقة بين الأمن الدولي والفضاء الإلكتروني، إذ يوجد المحتوى المعلوماتي العسكري والأمني والفكري والسياسي والاجتماعي والاقتصادي والخدمي والعلمي والبحثي في الفضاء الإلكتروني، لاسيما مع التوسع في تبني الحكومة الإلكترونية من جانب العديد من الدول، واتساع نطاق مستخدمي وسائل الاتصال وتكنولوجيا المعلومات في العالم، فقد أصبحت قواعد

(20) جون باسيت، حرب الفضاء الإلكتروني: التسليح واساليب الدفاع الجديدة، (ابو ظبي: مركز الامارات للدراسات والبحوث الاستراتيجية، 2014)، ص 58.

(21) عمرو صبحي، تكتيك الدرع والسيوف في استخدام القوة السيبرانية، دراسات، المركز العربي للبحوث والدراسات، القاهرة، 2018، متاح على الموقع: <http://www.acrseg.org/40716>

استغلت روسيا أمر البريد الإلكتروني الخاص بـ (هيلاري كلينتون)، في محاولة لتصفية الحساب معها نظراً لتشجيعها للاحتجاجات عقب فوز (فلاديمير بوتين) في العام 2012، وقامت بقرصنة ونشر رسائل البريد الإلكتروني الخاص بـ (كليتون)، لتلقي بالشك في نزاهة الانتخابات الأمريكية، وقد أكد مسؤولون في الإدارة الأمريكية وفقاً لـ (نيويورك تايمز) أنهم واثقون من أن القرصنة (الروس) قد تسلوا أيضاً إلى أنظمة الحاسوب التابعة للجنة الوطنية للحزب الجمهوري، كما فعلوا مع الحزب الديمقراطي. المصدر: عمرو صبحي، مصدر سبق ذكره.

(22) مارك بيردسول، مصدر سبق ذكره، ص 17.

البيانات القومية في حالة انكشاف خارجي، وهذا ما يعرضها لخطر هجمات الفضاء الإلكتروني، إلى جانب الدعاية والمعلومات المضللة ونشر الشائعات، أو الدعوة لأعمال تحريض أو دعم المعارضة الداخلية للنظام الحاكم⁽²³⁾، وعلى اثر ذلك صدر في العام 2003 توجيه رئاسي أمريكي بضرورة توفير مظلة الحماية المعلوماتية لشبكات الحاسوب في البنى التحتية الحرجة للولايات المتحدة بوصفها الحلقة الاضعف في بنية الأمن القومي الأمريكي، والأكثر عرضة لهجمات معلوماتية شرسة من قوى دولية وربما حتى هامشية، وفي العام 2007 دعت الإدارة الأمريكية وكالة الأمن القومي للتنسيق مع وزارة الأمن الداخلي لحماية الحكومة وشبكات الاتصالات المدنية من المتسللين ضمن اطار خطة تهدف إلى تعزيز الأمن السيبراني للمؤسسات الحكومية، وتعزيز الدفاعات لمكافحة الإرهاب، فقد خصص لهذا التوجه الاستراتيجي (144) مليون دولار من ميزانية الدفاع الأمريكي⁽²⁴⁾.

(23) رانيا عبد الله، القوة الإلكترونية وأبعاد التحول في خصائص القوة، أوراق، مجلة الشباب، 2014، متاح على الموقع: <http://shabab.ahram.org.eg/News/21761.aspx>

(24) سامر مؤيد عبد اللطيف، الحرب في الفضاء الرقمي رؤية مستقبلية، مجلة رسالة الحقوق، مركز الدراسات القانونية والدستورية، جامعة كربلاء، العدد (2)، 2015، ص 93.

ومع تزايد حجم الاعتمادية الأمريكية على شبكة المعلومات وتعرض الجيش الأمريكي في العام 2016 لعدد كبير من هجمات الانترنت، أعلن الرئيس السابق (باراك أوباما) ان: «تهديد الانترنت اصبح واحداً من أخطر التحديات التي تواجهها بلاده، وأن الأسلحة التي تستخدم في هذه الحرب هي أسلحة الدمار الشامل الحقيقية»⁽²⁵⁾، واتبع ذلك اعلان قادة في البنتاغون: «أن شن هجوم سيبراني مضر بما فيه الكفاية على الولايات المتحدة، قد ينظر إليه على أنه عمل من أعمال الحرب يستدعي الرد عليه بالصورة نفسها، ولن يأخذ هذا الرد بالضرورة شكل هجوم سيبراني مضاد من جانب الولايات المتحدة»⁽²⁶⁾، ونتيجة لذلك التحدي تحركت الإدارة الأمريكية من خلال الأمن الإلكتروني بخطى أكثر جدية وشمولية في اطار ما يعرف بالمبادرة الوطنية الشاملة للأمن السيبراني، والتي خصص لها مبلغ قدره 8 مليار دولار من ميزانية العام 2019، كما قدمت القيادة الإلكترونية لتطوير تكنولوجيات الانترنت تصوراتها للكونغرس حول السياسة الإلكترونية لوزارة الدفاع والإدارة القومية لمكافحة التجسس، وتوجهات سياسة واشنطن في هذا المجال للمستقبل المنظور، وكان من بين ما تضمنته هذه الاستراتيجية الجديدة بمفاصلها الرئيسة، هو توحيد نظم القيادة والتحكم والاتصالات والاستخبارات تحت إدارة واحدة تسمى (القيادة الفضائية الأمريكية)، والتي تخضع للإشراف المباشر من قبل مساعد وزير الدفاع الأمريكي، وتتولى هذه القيادة مسؤولية إدارة شبكات الحاسوب في كل صنوف الجيش الأمريكي، يتقدم ذلك دورها المحوري في مجال تأمين الحماية الإلكترونية لها في مواجهة الإرهاب المعلوماتي، أو حتى تحقيق هجمات

(25) نقلاً عن: المصدر نفسه.

(26) المصدر نفسه.

معلوماتية استباقية ضد خصومها، فضلاً عن مهامها التقليدية في تقديم الخدمات لأنشطة القوات المسلحة الأمريكية أيام الحرب والسلام⁽²⁷⁾.

(27) المصدر نفسه، ص 88.

وبالاستناد الى ما تقدم، فقد اصبح إدماج الفضاء الإلكتروني ضمن الأمن القومي للدول حاجة ملحة، من خلال تحديث الجيوش وتدشين وحدات متخصصة للحروب الإلكترونية، وإقامة هيئات وطنية للأمن والدفاع الإلكتروني، والقيام بالتدريب وإجراء المناورات من اجل تعزيز الدفاعات الإلكترونية، وكذلك العمل على تعزيز التعاون الدولي في مجالات تأمين الفضاء الإلكتروني، والقيام بمشروعات وطنية للأمن الإلكتروني⁽²⁸⁾.

(28) عادل عبد الصادق، أنماط

من هنا تأتي أهمية تعاون كافة الفاعلين لترسيخ ثقافة عالمية لأمن الفضاء الإلكتروني، وأهمية الموازنة بين اعتبارات الأمن وحرية استخدام الفضاء الإلكتروني، والاحتكار العالمي للتكنولوجيا والعمل على انتقالها في دول العالم، ومن ثم فإن التعامل مع النمط الجديد من التهديدات يتطلب تعاوناً دولياً، وكذلك أهمية الحاجة إلى فتح الطريق أمام التعاون المثمر بين الحكومات والأفراد والشركات العاملة في تكنولوجيا الاتصال والمعلومات، كما يجب تعزيز دور الفضاء الإلكتروني في النمو الاقتصادي وتحسين حياة المواطنين، وحرية الرأي والتعبير، وتعزيز التسامح بين الثقافات، وبذل جهود دولية عاجلة ومتكاتفه لمواجهة تهديدات أمن الفضاء الإلكتروني بإمكانية العمل على حل الصراعات على أرض الواقع لمنع انتقالها إليه، والعمل على توافق القوانين المتعلقة بالصراع الإلكتروني مع القانون الدولي وأهمية المبادرات الدولية لحماية الفضاء الإلكتروني، فضلاً عن البحث والتطوير في مجال الدفاعات ضد الأخطار الإلكترونية، وتعزيز أشكال التعاون الدولي في سبيل مكافحتها من أجل تعزيز أمن الفضاء الإلكتروني باعتباره مرفقاً دولياً وتراثاً مشتركاً للإنسانية⁽²⁹⁾.

(29) عادل عبد الصادق، القوة الإلكترونية: أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، مصدر سبق ذكره، ص 29.

لكن بالمقابل يعد امن الفضاء الالكتروني بطبيعته مشكلة دولية كما هو واضح في سلسلة من المؤتمرات الدولية المعنية بأداة الفضاء الالكتروني التي بدأت في (لندن) في العام 2011، وتواصلت في (بودابست) للعام 2012 ومضت قدماً في (سيؤول) للعام 2013، إذ ان احتمالات تحقيق تقدم مبكر في مجال الاتفاقات الدولية لمراقبة استخدام اسلحة الفضاء الالكترونية وتنظيمها تبدو ضئيلة، وعلى اية حال فمن المرجح انه حتى في ظل وجود بيئة حميدة فان مفاوضات الحرب الالكترونية قد لا تتسم بالتوصل الى حل شامل واحد، وانما بسلسلة من

يعد امن الفضاء الالكتروني بطبيعته مشكلة دولية

الاتفاقات المحدودة التي يتم التوصل اليها على امتداد مدة من الزمن، ونظراً الى احتمال تطور سريع لأسلحة الفضاء الالكتروني من الجيل الثاني الشديدة التأثير

وانتشار المنظومات المنخفضة التأثير، قد يكون من الأفضل ان تركز المفاوضات على الحد من الاضرار الجانبية والتأثيرات الانسانية، وعلاوة على ذلك يبدو من الصعب جداً التغلب على تحديات التحقق الفعال وتطبيق العقوبات، إذ تعتمد نظم الرقابة على الاسلحة التقليدية على التحقق من خلال التفتيش واحتمال فرض عقوبات تأديبية على المخالفين، كما يمكن ان تشكل سهولة اخفاء تطوير اسلحة الفضاء الالكتروني بالإضافة الى مشكلة الاستخدام المزدوج عقبة أداء امام نظام تحقق ذي مصداقية، بالإضافة الى ذلك فان تطبيق العقوبات التأديبية من الممكن ان تعرقه صعوبات تحميل المسؤولية بصورة ذات مصداقية في اي حادثة من هذا النوع⁽³⁰⁾. لذلك اصبح الفضاء السيبراني اكثر عرضة للهجمات السيبرانية فيما يتعلق بعملية تزايد البنية التحتية الكونية للمعلومات دولياً نتيجة عدد من المتغيرات اهمها:⁽³¹⁾

(30) جون باسيت، مصدر سبق ذكره، ص 54-66.

(31) عبد الغفار رعيضي الدويك، مصدر سبق ذكره، ص 34.

- 1- باتت العلاقة بين الامن والتكنولوجيا علاقة طردية مع امكانية تعرض المصالح الاستراتيجية ذات الطبيعة السيبرانية الى اخطار الكترونية، واعادة التفكير في مفهوم الامن القومي الذي يعنى بحماية قيم المجتمع الاساسية ومن ثم يعد رافداً جديداً له.
- 2- يهتم الامن السيبراني بعملية وضع المعايير والاجراءات لمنع الاستخدامات غير السلمية للفضاء السيبراني، وما يمثله ذلك من تهديد للأمن العالمي والبنية التحتية الكونية للمعلومات، إذ اصبح امن الدول جزء من الامن الجماعي.
- 3- اصبحت قضية امن الفضاء السيبراني قضية دولية تتطلب استراتيجية مرنة تتواءم مع المتغيرات المستمرة سواء في الآليات او التكتيكات الخاصة بالأمن مقابل التطور المستمر في الاخطار.
- 4- لم يتم الاقتصار في عملية الاهتمام بالأمن السيبراني على البعد التقني وحسب، بل تجاوزوه الى ابعاد اخرى اصبحت ذات علاقة في تفسير القضية، مثل الابعاد الثقافية والاجتماعية والاقتصادية والعسكرية.
- 5- تصاعد دور الفاعلين من غير الدول في العلاقات الدولية اثر بدوره على سيادة الدولة، لاسيما مع بروز الشركات التكنولوجية عابرة للحدود الدولية.

المحور الثاني: العقيدة الاستراتيجية

برزت في مرحلة ما بعد الحرب الباردة، ولاسيما في منتصف عقد التسعينيات من القرن الماضي، اتجاهات فكرية أمريكية تطالب بضرورة تغيير مفاهيم وعقائد

الاستراتيجية الأمريكية بما ينسجم مع متطلبات المرحلة، وعلى اثر ذلك طرح تيار المحافظين الجدد رؤية جديدة لأداء الاستراتيجية الأمريكية تتمثل في توظيفها لمقومات قوتها الشاملة وفرض هيمنتها على العالم، وقد استند هذا الطرح إلى مقارنة مشروع القرن الأمريكي الذي يهدف إلى ترويج الأفكار المتعلقة بالقيادة الأمريكية بشكل يتوافق مع المبادئ والمصالح الأمريكية الجديدة، لاسيما وإن تيار المحافظين الجدد استطاع توظيف أحداث 11 أيلول عام 2001 في تحقيق أهدافه المتمثلة في تغيير مفاهيم وعقائد واستراتيجيات جديدة تمايزت عن مرحلة الحرب الباردة، ويبدو إن هذا المذهب يحوي تطلعات مستقبلية للأعوام المقبلة من القرن الحادي والعشرين، إذ يتجه الفكر الاستراتيجي الأمريكي إلى إدامة القوات المسلحة الأمريكية وتطوير أداؤها من خلال إجراء بعض التعديلات على عناصر الجيش، لاسيما في هيكله القوات ومدى حجمها وتسليحها، وانطلاقاً من إن الجيش ذو العدد الكبير أصبح يكلف ميزانية الدولة أموالاً طائلة تصل ما بين 70-80 % من ميزانيتها على الإنفاق العسكري، تم استحداث استراتيجية بناء جيش صغير وذكي⁽³²⁾.

بالمقابل شهد العقد الاخير من القرن العشرين تطورات سريعة في مجالي الحوسبة وتكنولوجيا المعلومات، مما افضى الى تغييرات بعيدة المدى في جميع مجالات الحياة، ولاسيما في المجالين العسكري والامني اللذين شهدا تغييرات تتعلق بطرق القتال وبناء الجيوش القوية، ويعزى ذلك جزئياً الى المستجدات التي طرأت على انماط التفكير الاستراتيجي وعلى بلورة عقيدة قتالية تتلائم مع الواقع المتغير⁽³³⁾.

إن حالة انعدام الثقة واللايقين في العلاقات الدولية هو ما شجع تزايد النزاعات في العالم، فضلاً عن التطورات السريعة في الفضاء السيبراني، وهذا ما جعل الدول تسارع إلى تبني تغييرات في العقيدة الامنية، وذلك بإدراج القوة السيبرانية كمحدد رئيس لمدى قوة الدولة وقدرتها على حسم النزاعات لصالحها، وعلى اثر ذلك نجد أن كلاً من والولايات المتحدة الأمريكية، والصين، واسرائيل، وبريطانيا، وفرنسا، وإيران، وكوريا الشمالية، قد طوروا من عقيدتهم الامنية، وأصبح الفضاء السيبراني مسرحاً للعمليات العسكرية لكل منهم، كما أوجدوا قيادة خاصة ومستقلة لقيادة العمليات السيبرانية⁽³⁴⁾.

بذلك افرزت القوة الالكترونية التي اثرت من ناحيتها في علاقات القوة في السياسة الدولية، داخلياً من خلال توزيع القوة بين اكبر عدد من الفاعلين مع ضعف السيطرة الدولية، وخارجياً من خلال زيادة قدرة الفاعل الاصغر في السياسة الدولية على

(32) عمار حميد ياسين، مكانة القوة في المدرك الاستراتيجي الأمريكي دراسة في التأصيل النظري والتوظيف الاستراتيجي، مجلة السياسية والدولية، كلية العلوم السياسية- الجامعة المستنصرية، العددان (35-36)، 2017، ص ص-405 406.

(33) نقلاً عن: جيل برعام، تأثير تطور تكنولوجيا الحرب السيبرانية على بناء القوة في اسرائيل، مجلة الدراسات الفلسطينية، مؤسسة الدراسات الفلسطينية، بيروت، 2014، ص2. متاح على الموقع: <http://www.pales-tine-studies.org>.

(34) اسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، جامعة محمد بوضياف، المسيلة، الجزائر، العدد (1)، 2019، ص26.

ممارسة أنواع مختلفة من القوة في الفضاء الإلكتروني. وعلى اثر ذلك أصبح تامين الفضاء الإلكتروني جزءاً من استراتيجيات الامن القومي للعديد من الدول، فقد قام البعض منها بإنشاء هيئات الطوارئ لمواجهة المعلوماتية الإلكترونية، وقيادات عسكرية لحماية الفضاء الإلكتروني⁽³⁵⁾.

(35) نقلاً عن: صباح عبد الصبور عبد الحي، استخدام القوة الإلكترونية في التفاعلات الدولية، بحوث ودراسات سياسية، المعهد المصري للدراسات السياسية والاستراتيجية، اسطنبول، 2016، ص4.

من هنا يجب النظر إلى استراتيجية الفضاء الإلكتروني على أنها مكون لا يتجزأ من مشاركة الدولة في مجال الإنترنت في هذا الإطار، إذ يجب أن تتم عملية تعزيز القوة للفضاء الإلكتروني والتي تشمل خمس عناصر رئيسة هي: الأول صياغة استراتيجية وعقيدة للسلوك في الفضاء الإلكتروني، والثاني تطوير التكنولوجيا التي تدعم تحقيق أهداف واتجاهات النشاط السيبراني على النحو المحدد في الاستراتيجية، والثالث يتعلق بتنمية الموارد البشرية لتشغيل الأدوات التكنولوجية، والرابع يكمل الآخرين بشكل كبير ويتعلق بتنظيم الموظفين في الأطر التشغيلية ذات الصلة على أساس المزايا النسبية في العملية، والعنصر الخامس يتعامل مع التدريبات الخاصة بالتكنولوجيا للتركيز على بناء البرامج المهمة وممارستها في الواقع⁽³⁶⁾.

Gabi Siboni and Ofer Assaf, (36) Guidelines for a National Cyber Strategy, the institute for national security studies, strategic studies center, 2014. Available on the site: <http://www.inss.org.il>

ان الخلفية الفلسفية والفكرية لاستراتيجية وسائل الاتصال والاعلام التي تتبناها وزارة الخارجية الأمريكية هي نفسها خلفية المدرسة الأمريكية الكلاسيكية التي صاغها المفكر (مارشال مكلوهان)، والتي تنص على ان: «شكل وطبيعة وسائل الاتصال والاعلام في اي مجتمع واي عصر هي التي تصوغ شكل التنظيم الاجتماعي والسياسي وليس العكس، وان نشر وتعميم وسائل الاتصال والاعلام في المجتمعات هو هدف في حد ذاته، لان ادوات ووسائل الاتصال والاعلام تخلق شروط نمو البيئة الليبرالية التحررية والديمقراطية في المجالات السياسية والاجتماعية والاقتصادية»⁽³⁷⁾.

(37) نقلاً عن: مركز الحرب الناعمة للدراسات، شبكات التواصل الاجتماعي منصات للحرب الأمريكية الناعمة، (شبكة المعارف الإسلامية، 2016)، ص91.

هذا التقدم في المجال التكنو-معلوماتي أسهم في إعادة صياغة الاستراتيجية العسكرية الأمريكية، حيث كشفت خبرة الحروب التي خاضتها الولايات المتحدة في عقد التسعينيات من القرن المنصرم (حرب الخليج الثانية 1991 في إطار التحالف الدولي، وحرب كوسوفا 1999 في إطار حلف الناتو، والحرب ضد أفغانستان، والحرب ضد العراق في العام 2003)، عن جملة حقائق تشكل اليوم أساس العقيدة العسكرية للقوات المسلحة الأمريكية ومذهبها القتالي، فقد أتاح تنامي وتائر الثورة التقنية العسكرية فرصاً للتفكير بترجيح خيار حروب تستخدم فيها أسلحة تقليدية ذات خصائص تقنية-معلوماتية على درجة عالية من الكفاءة القتالية تحقيقاً لمبدأ الحسم السريع لأية عملية عسكرية تشارك فيها القوات الأمريكية⁽³⁸⁾، إذ سعت

(38) عبد القادر محمد فهمي، الفكر السياسي والاستراتيجي للولايات المتحدة الأمريكية: دراسة في الأفكار والعقائد ووسائل الامبراطوري، (عمان: دار الشروق للنشر والتوزيع، 2009)، ص175-171.

المؤسسة العسكرية الأمريكية إلى توظيف الثورة التكنو- معلوماتية لخدمة أهدافها الاستراتيجية العسكرية من خلال تطوير كفاءتها القتالية وضبط أدائها العملياتي. وان نظرية الاشتباك الآمن ما هي إلا نتيجة لمثل هذا التوظيف، فقد انطوت هذه النظرية على تحول مهم في مجال الأسلحة المستخدمة بهدف توسيع مداها القتالي المؤثر وزيادة قدرتها التدميرية، فمنظومات الأسلحة التقليدية التي تعتمد على تكنولوجيا المعلومات والأجهزة الكمبيوترية لم يعد مداها مقتصرًا على مسارح العمليات، بل امتد أثرها المدمر إلى أهداف استراتيجية خارج نطاق النشاط الميداني أو التعبوي للقوات المتحاربة، لتصل إلى داخل العمق الاستراتيجي للعدو.⁽³⁹⁾ من هنا جاء في تقرير المراجعة الرباعية الذي قدمته وزارة الدفاع الأمريكية للكونغرس، وتكلم بالإشارة التي أوردها نائب وزير الدفاع الأمريكي السابق (بول ولفويتز) في العام 2001 إلى: «ضرورة تبني الولايات المتحدة لاستراتيجيات جديدة للدفاع ضد أنماط غير تقليدية من الحروب يأتي في مقدمتها حروب الشبكة الدولية للمعلومات»⁽⁴⁰⁾.

(39) عبد القادر محمد فهمي، مصدر سبق ذكره، ص171.

(40) نقلاً عن: سامر مؤيد عبد اللطيف، مصدر سبق ذكره، ص93.

وهذا ما اكدت عليه الاستراتيجية القومية العسكرية الامريكية لعمليات الفضاء الالكتروني الصادرة في العام 2006 من خلال تأكيدها السيطرة على المعلومات وتبادلها وتوظيفها بما يخدم الاهداف المرسومة دون التلاعب فيها او تدميرها، والقدرة على الاختراق ومراقبة بيانات العدو، والتطبيقات الحركية، وحرية الحركة داخل الفضاء الالكتروني سواء كانت حركات هجومية او دفاعية، وتطبيق القانون من خلال سرعة اجراء التحقيقات في الاعمال الاجرامية لردع الجناة، ومكافحة التجسس من خلال معرفة الخصم ومدى نواياه واهدافه وقدرته في استغلال المجال الالكتروني⁽⁴¹⁾.

(41) يونس مؤيد يونس، مصدر سبق ذكره، ص141.

بذلك جاءت استراتيجية الأمن القومي الأمريكي للعام 2010 لتؤكد أن: «التحديات الإلكترونية تمثل واحدة من أخطر التهديدات التي تواجه الأمن القومي والسلامة العامة للمواطنين، فضلاً عن أنها أحد أهم التحديات التي تواجه الاقتصاد القومي، ومن ثم يجب تأمينها، كما يجب أن تكون جديرة بثقة مستخدميها، ويمكن تحقيق ذلك عبر الاستثمار في الناس والتكنولوجيا، وعبر تدعيم قدرات الشركات مع القطاعات المختلفة، سواء كانوا أفراداً أو مؤسسات خاصة»⁽⁴²⁾. بناء على ذلك فقد اكدت استراتيجية الأمن القومي الأمريكي للعام 2010 التي أعادت تأكيد الأولويات الطويلة الأمد في السياسة الخارجية الأمريكية على الآتي:⁽⁴³⁾

(42) نقلاً عن: إيهاب خليفة، أبعاد التحول في استراتيجية الدفاع الأمريكية، مركز المستقبل للأبحاث والدراسات المتقدمة، ابو ظبي، 2014، متاح على الموقع: <https://futureuae.com/ar/Mainpage/Item/856/cy-ber-defense>

(43) Kristin M. Lord and Travis Sharp, America's Cyber Future: Security and Prosperity in the Information Age, center for a new American security, Francisco in February 2011, p12

1 - أمن الولايات المتحدة ومواطنيها وحلفائها وشركائها.

2 - اقتصاد أمريكي قوي مبتكر ومتنامي في ظل نظام اقتصادي دولي مفتوح يعزز الفرص والازدهار.

3 - احترام القيم العالمية.

ففي ذات السياق اشارت وثيقة الامن القومي الامريكي عن حماية الولايات المتحدة من الحرب الالكترونية لتحسين الامن الامريكي في بنيتنا التحتية الحيوية، إذ تقوم الاستراتيجية بتقييم المخاطر في ست مجالات رئيسة هي: (الامن الوطني، والطاقة، والاعمال المصرفية المالية، والصحة والسلامة والاتصالات، والنقل)، إذ تعمل الاستراتيجية على مواجهة التهديدات الالكترونية، داخلياً من خلال فرض الولايات المتحدة الامريكية عواقب سريعة ومكلفة على الحكومات الاجنبية والمجرمين والجهات الفاعلة الاخرى التي تضطلع بأنشطة الكترونية خبيثة، وخارجياً من خلال العمل مع الحلفاء والاصدقاء لتوسيع وعيها بالأنشطة الخبيثة، من اجل تحسين تبادل المعلومات مع الدول الصديقة⁽⁴⁴⁾، ويمكن القول إن السطور الأولى من هذه الاستراتيجية تلخص أزمة العقل السياسي الأمريكي المعاصر الذي مازال أكثر تمسكاً بمشروع السيطرة على العالم، وهي السيطرة التي أطلق عليها الحزب الجمهوري تسمية (الهيمنة الأمريكية على العالم)، وأطلق عليها الحزب الديمقراطي تسمية (قيادة أميركا للعالم)، ورغم الفرق الشكلي بينهما إلا ان المضمون نفسه بين القيادة والهيمنة⁽⁴⁵⁾.

(44) يحيى سعيد قاعود وعلا عامر الجعب، وثيقة الامن القومي الامريكي 2017، قراءة تحليلية في استراتيجية دونالد ترامب، مجلة قراءات استراتيجية، منظمة التحرير الفلسطينية، مركز التخطيط الفلسطيني، العدد (20)، 2018، ص44.

(45) الحرب الناعمة الاسس والنظرية والتطبيقية، مصدر سبق ذكره، ص72.

بناء على ذلك اوجدت ثورة المعلومات بيئة استراتيجية من الصعب توظيفها، إذ يمكن من خلالها صياغة مفهوم جديد للاستراتيجية العسكرية، إذ في هذا الصدد يذكر (الفن توفلر): «ان الاهتمام بالحرب والحرب المضادة -حرب المعلومات- يبدأ من اعادة صياغة استراتيجية المعرفة العسكرية والمخابراتية، حيث لا تعتمد الاستراتيجيات اليوم على القوة العسكرية فحسب، وانما على القدرة الشاملة للدولة، والتي تكمن في القدرات المتوفرة والكامنة والمحتملة، ويأتي في مقدمتها العقل والمعلومة»⁽⁴⁶⁾، بذلك اخذ مصطلح استراتيجية حرب المعلومات منحاً جديداً يقتضي محاولة معرفة كل شيء عن الخصم ومنعه في الوقت نفسه من الحصول على المعلومات، وهذا يعد جزءاً أساسياً من الاستراتيجية العسكرية التي يطلق عليها (توفلر): «تغيير توازن المعلومات والمعرفة لصالحك»⁽⁴⁷⁾.

(46) نقلاً عن: جهاد عودة، المعلومات وصناعة القرار الاستراتيجي، (القاهرة: المكتب العربي للمعارف، 2018)، ص282. للمزيد ينظر: Isaac Bin Tabansky, An Interdisciplinary View of Security Challenges in the Information Age, Military and Strategic Affairs, Center for Strategic Studies B, Institute for National Security Studies cd, Volume 3, No. 3, December 2011, p13.

(47) جهاد عودة، مصدر سبق ذكره، ص282.

من هنا تأسست العقيدة الاستراتيجية للولايات المتحدة في ظل الظروف الموضوعية للبيئة الدولية للرد على أي هجوم سيبراني بأي سلاح، وبما يتناسب

Joseph S. Nye, Is Cyber the (48) Perfect Weapon, the world's opinion page, July 05, 2018 <https://www.project-syndicate.org/commentary/detering-cyber-attacks-and-information-warfare-by-joseph-s-nye-2018-07>.

(49) إيهاب خليفة، أبعاد التحول في استراتيجية الدفاع الأمريكية، مركز المستقبل للأبحاث والدراسات المتقدمة، أبو ظبي، 2014، متاح على الموقع: <https://futureuae.com/ar/Mainpage/Item/856/cyber-defense>.

(50) نقلاً عن: ريتشارد كلارك وروبرت نيك، حرب الفضاء الإلكتروني: التهديد التالي للأمن القومي وكيفية التعامل معه، (أبو ظبي: مركز الإمارات للدراسات والبحوث الاستراتيجية، 2012)، ص 190-191.

والضرر المادي الناجم عن إصرار أن القانون الدولي - بما في ذلك الحق في الدفاع عن النفس - ينطبق على النزاعات السيبرانية⁽⁴⁸⁾، وعليه فقد أعدت الإدارات المتعاقبة على البيت الأبيض في إطار مواجهة التهديدات الإلكترونية المختلفة، سواء في مدة رئاسة الرئيس الأمريكي السابق (جورج دبليو بوش) أو في مدة رئاسة الرئيس الأمريكي السابق (باراك أوباما)، العديد من الخطط والاستراتيجيات التي تتنوع ما بين، الدفاع مثل: الاستراتيجية القومية للحماية المادية للبنية التحتية الحيوية والأصول الرئيسة، والاستراتيجية القومية لتأمين الفضاء الإلكتروني الصادرين في العام 2003، والهجوم مثل: الاستراتيجية القومية العسكرية لعمليات الفضاء الإلكتروني الصادرة في العام 2006، وإنشاء قيادة عسكرية في الفضاء الإلكتروني تابعة لوزارة الدفاع والصادرة في العام 2009، وتعظيم التعاون الدولي في مجال مكافحة الهجمات الإلكترونية مثل: الاستراتيجية الدولية للفضاء الإلكتروني الصادرة في العام 2011⁽⁴⁹⁾.

إن الغرض الأساس من أي استراتيجية أمنية وطنية أمريكية هي الدفاع عن الولايات المتحدة، فالولايات المتحدة الأمريكية لا تصنع الأسلحة بغرض بسط الهيمنة على مختلف المجالات (البحار والفضاء الخارجي والفضاء الإلكتروني) فحسب، وإنما للدفاع عن أمنها القومي، وإذا كان هذا القول يبدو بسيطاً لأول وهلة فإنه سرعان ما يصبح معقداً بسبب من يعتقدون أن أفضل السبل للدفاع هو الهجوم وتدمير الخصم، وفي هذا الصدد يذكر الجنرال (روبرت الدر) عندما كان على رأس قيادة حرب الفضاء الإلكتروني التابعة للقوات الجوية، إذ ذكر لعدد من الصحفيين أن قيادته على الرغم من تمتعها بقدرات هجومية كانت تخطط لشل شبكات الحاسوب لدى العدو بقوله: «إننا نريد أن نقض عليهم لنضربهم الضربة القاضية في الجولة الأولى»⁽⁵⁰⁾.

ونتيجة لذلك أقرت الولايات المتحدة الأمريكية في العام 2018 استراتيجية جديدة للأمن السيبراني اتخذت فيها موقفاً أكثر شراسة في الحرب السيبرانية، في مقابل

تهديدات كل من روسيا والصين، ودخلت حيز التنفيذ بعد قرار الرئيس (دونالد ترامب) بإلغاء قواعد حدها سلفه الرئيس (باراك أوباما) للعمليات السيبرانية، والاتجاه لاستعدادات الحرب السيبرانية من خلال بناء قوة أكثر فتكاً، وتوسيع التحالفات والشراكات، وهي ترى أن الفضاء السيبراني يجب أن يعزز بالتفوق العسكري وممارسة الأنشطة الاستخباراتية، وحماية الأمن القومي، والعمل على ردع

أقرت الولايات المتحدة الأمريكية في العام 2018 استراتيجية جديدة للأمن السيبراني اتخذت فيها موقفاً أكثر شراسة في الحرب السيبرانية

القوى الدولية المنافسة، ومواجهة سرقة الأسرار الصناعية، وتهديد البنية التحتية المعلوماتية والنظام الديمقراطي، وذلك من خلال العمل على: (51)

1 - ضمان قدرة الجيش الأمريكي على القتال وكسب الحروب في أي مجال، بما في ذلك الفضاء السيبراني، وحماية الأمن القومي وردع العدوان الذي قد يشنه الأعداء، والاستجابة السريعة للهجمات السيبرانية التي تمثل استخداماً للقوة ضد مصالح الولايات المتحدة وحلفائها وشركائها الاستراتيجيين.

2 - السعي لشن هجمات استباقية وردع الأنشطة السيئة عبر الإنترنت، التي تستهدف البنية التحتية، والتي قد تؤثر في قدرة وزارة الدفاع للدفاع عن المصالح الوطنية، واعتماد أسلوب الدفاع إلى الإمام من خلال ضرب مصادر الخطر خارج حدود الولايات المتحدة قبل أن تصل إلى الداخل.

3 - تعزيز التعاون مع الهيئات المعنية بالدفاع مع القطاعين العام والخاص لتنسيق أنماط الاستجابة، ونقل الخبرات والتعاون في تنفيذ الاستراتيجية القومية للأمن السيبراني.

4 - التعاون مع الحلفاء من أجل تعزيز القدرة على مواجهة الهجمات السيبرانية، وتعزيز جاهزيتها في مجال الدفاع السيبراني والردع ومواجهة الهجمات، وتشارك المعلومات للعمل على فاعلية مواجهة التهديدات السيبرانية وتعزيز وضع الأمن السيبراني.

5 - تعزيز قواعد السلوك الرسمي للدولة في الفضاء السيبراني من أجل العمل على تبني المبادئ الطوعية وغير الملزمة لسلوك الدولة في الفضاء السيبراني، وتأييد عمل لجنة فريق الخبراء الحكوميين التابع للأمم المتحدة المعني بالتطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي.

وفي هذا السياق ثمة مبادئ أساسية من مبادئ الاستراتيجية السيبرانية ربما تساعد في الموازنة الجديدة لعملية التحول في النسق الدولي تتمثل في:

المبدأ الأول: إدراك أن المفاهيم الاستراتيجية لم تعد تحمل المعنى نفسه بسبب التغيير التكنولوجي، فالعملة النقدية على سبيل المثال تعد لاعباً في الاستراتيجية المالية لأي دولة أو شركة أو فرد، ومع ذلك فقد تبدل شكل هذه العملة على مر الزمن، إذ كانت في السابق تصنع من المعادن، أصبحت ورقية، وفي عالم اليوم باتت قطع عملة رقمية على الانترنت، وأدى هذا التحول بدوره إلى تغييرات في الاستراتيجيات نفسها التي يمكن استخدامها لرفع قيمة هذه العملات. (52)

(51) نقلاً عن: المركز العربي لأبحاث الفضاء الإلكتروني، عادل عبد الصادق، صراع السيادة السيبرانية بين التوجهات الروسية والأمريكية، التقرير الاستراتيجي العربي 2018، مركز الأهرام للدراسات السياسية والاستراتيجية، القاهرة، 2019، ص 26-29. متاح على الموقع: http://accronline.com/article_detail.aspx?id=29415

(52) بيتر سنجر، التكنولوجيا العسكرية.. دورها حاسم في الحروب، مجلة آفاق المستقبل، مركز الامارات للدراسات والبحوث الاستراتيجية، ابو ظبي، العدد (27)، 2015، ص 90.

المبدأ الثاني: إدراك أن الأدوات الموثوق بها ربما لا تخدم الأهداف الاستراتيجية بالسبل عينها، فقد نرى اليوم تحولاً مماثلاً في طور الحدوث، فعلى سبيل المثال في الأشهر التسعة الأولى من عمليات الولايات المتحدة الأمريكية وحلفائها ضد تنظيم (داعش) أصيب أكثر من 5548 هدفاً خلال ما يقرب من 3300 ضربة جوية، ويعد هذا المستوى عالٍ من الدقة تاريخياً مقارنة بالاختبارات التي أجريت إبان الحرب العالمية الثانية، إذ كان معدل الإصابة أقل من 4 % من خلال الضربات الصاروخية ضد أهداف ثابتة كانت مطلية باللون الأبيض.

المبدأ الثالث: هو معاينة إمكانية تسبب التحولات التكنولوجية في تغيير الأهداف نفسها التي تنطوي عليها استراتيجية ما، فهناك هدف محوري يتمثل في بحث الكيفية التي يمكن من خلالها زيادة قدرتنا في الجانب الهجومي، حتى نصل إلى مرحلة الردع، لكن بالمقابل هناك تحدٍ كبير يتمثل في حالة الصراع الإلكتروني، إذ ان معرفة من يتعرض للهجوم والتعرف إلى الذي يشن هذا الهجوم، يعدان مسألة بالغة الأهمية⁽⁵³⁾.

من هنا نصت سياسة الردع في الفضاء الإلكتروني التي انتهجتها إدارة الرئيس السابق (باراك أوباما) من أن: «الردع في الفضاء الإلكتروني في عصر المعلومات يختلف اختلافاً جوهرياً عن مفاهيم عصر الحرب الباردة التي تهدف إلى ردع استخدام أسلحة الدمار الشامل»⁽⁵⁴⁾. ووفقاً لذلك فإن الفضاء الإلكتروني يتمتع بخصائص فريدة بما في ذلك طبيعته العالمية والمتراصة، والملكية الخاصة إلى حد كبير، وإمكانية عدم الكشف عن الهوية، والحوافز المنخفضة أمام دخول أولئك الذين يرغبون في إحداث الضرر، وهي خصائص تشكل تحديات للردع تختلف في نوعها ونطاقها عن الردع في الجانب التقليدي بنسبة أكبر⁽⁵⁵⁾، يتضح من ذلك ان (الردع السيبراني) أصبح مفهوماً عصرياً ذو اتجاهات متعددة، فهناك مجموعة كبيرة من الأدبيات والجدل الذي يسعى إلى تبسيطه وجعله كنظرية قابلة للتطبيق في سبيل إدراجه في استراتيجيات الأمن القومي، لاسيما التهديدات التي طرأت في العصر الحديث من خلال المجالات السيبرانية (التجسس الإلكتروني، الحرب الإلكترونية، الهجمات الإلكترونية، القرصنة والتخريب الإلكتروني، سرقة الصناعة)، فقد اضطر استراتيجيو ومخططو الأمن القومي في البحث من ردع أعمال القوة السيبرانية، ليس فقط على الشبكات الحكومية ولكن أيضاً على الشركات والأفراد عبر تشكيل دفاع قوي قائم على التهديد بالانتقام⁽⁵⁶⁾.

(53) بيتر سنجر، مصدر سبق ذكره، ص90.

الردع السيبراني هو استراتيجية تسعى من خلالها الدولة المدافعة للحفاظ على الوضع الراهن من خلال الإشارة إلى نواياها لردع نشاط سيبراني عدائي، عبر استهداف جهاز صنع القرار لدى الخصم، والتأثير عليه لتجنب الانخراط في نشاط سيبراني مدمر، خوفاً من الانتقام الأكبر من جانب المعتدي الأول، ويختلف الردع في التفاعلات الدولية على أرض الواقع جزئياً منه في حالة الردع في الفضاء الإلكتروني، كون أن أحد الفاعلين غير قادر على إزالة أو تدمير الطرف الآخر كلياً، كما في حالة الردع النووي مثلاً، كذلك ليس من السهولة تحقيق الردع في الفضاء الإلكتروني بسبب خاصية التخفي، والتي تجعل من الصعوبة بمكان على متخصصي الأمن الإلكتروني أن يتعرفوا على خصومهم أو أن يتوقعوا من أين سوف تأتيهم الهجمة الإلكترونية القادمة، وهو ما يلحح سؤالا حول إمكانية أن تقوم الهجمات الإلكترونية بتهديد السلم والأمن العالمي؟ ولتحقيق الردع الإلكتروني يجب أن تعمل الدول على زيادة قدراتها الدفاعية من خلال حائط صد للهجمات الإلكترونية، ووضع أجهزة استشعار على بنيتها التحتية للكشف المبكر عن الأخطار الإلكترونية، وتطوير قدراتها في مجال تتبع العكسي للهجمات الإلكترونية لمعرفة مكان إطلاقها. المصدر:

A A Ghonis, The Limits of Deterrence in the Cyber World An Analysis of Deterrence by Punishment, university of Sussex, 2013, p12. Available on the site: <http://www.inss.org.il>.

(54) نضلاً عن: يوشياكي ناكاجاوا وسكوت ديليو هارولد وآخرون، التحالف الأمريكي الياباني ومواجهة ضغوطات النزاع البارد (المنطقة الرمادية) في مجالات البحر والفضاء الإلكتروني والفضاء الخارجي، مؤسسة (راند)، سانتا مونيكا، كاليفورنيا، 2017، ص43-42. متاح على الموقع: www.rand.org.

(55) يوشياكي ناكاجاوا وسكوت ديليو هارولد وآخرون، مصدر سبق ذكره.

(56) A A Ghonis, The Limits of Deterrence in the Cyber World An Analysis of Deterrence by Punishment, university of Sussex, 2013, p9. Available on the site : <http://www.inss.org.il>.

وبالاستناد الى ما تقدم فان العقيدة الاستراتيجية للردع السيبراني في الفضاء الالكتروني تركز الى ثلاث ركائز هي: (57)

(57) رغبة البهي، الردع السيبراني: المفهوم والاشكاليات والمتطلبات، مجلة العلوم السياسية والقانون، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين، العدد (17)، 2017، ص 52، 61

الاولى: مصداقية الدفاع عن انظمة المعلومات وردع اي محاولة لاختراقها وتوافر انظمة نسخ احتياطية اخرى، مما يعني ان اي هجوم ناجح عليها لن يسفر عن التدمير التام لها او الفقدان الكلي لما تحويه من معلومات، ورغم تزايد تكلفة هذا الحل الا انه الحل العملي الاكثر فعالية.

الثانية: الرغبة في الانتقام، إذ على من تعرض للهجوم ان يعلن عن رغبته في الانتقام من المهاجم، كون ان امتلاك القدرة على الانتقام لا تكفي بمفردها لردعه، كما يختلف الردع في عصر المعلومات كثيراً عنه في عصر الحرب الباردة الذي تميز بقلّة عدد الدول المالكة للسلاح النووي، لكن في عالم اليوم فان عدد الدول التي تسعى لتطوير اسلحتها السيبرانية بلغ حوالي 140 دولة، كذلك ادخلت 30 دولة الوحدات السيبرية في جيوشها.

في عالم اليوم فان عدد الدول التي تسعى لتطوير اسلحتها السيبرانية بلغ حوالي 140 دولة، كذلك ادخلت 30 دولة الوحدات السيبرية في جيوشها.

الثالثة: القدرة على الانتقام، إذ لا بد من ان يتكبد المهاجم ضرراً يفوق ما وقع على المدافع من اضرار، ولكن هذا يتطلب القدرة على الانتقام وتنفيذ هجمة سيبرانية ضد المهاجم الاول بعد التعرف عليه وهو امر صعب التحقق.

مما تقدم يمكننا القول: تغيرت الرؤية الامريكية بالنسبة الى بيئتها الداخلية، وانعكست تلك الرؤية بالتفكير على المستوى الامني بأبعاده الداخلية، فاصبح يشكل تهديداً كبيراً على امن الدولة، لاسيما في ظل التقنية المتاحة والمتوفرة للأفراد والشركات والتنظيمات الارهابية، فأصبحت حرية الراي والمشاركة متاحة للجميع في الفضاء الالكتروني، وبالنتيجة انعكس ذلك عن تبني نوع معين من العقيدة الاستراتيجية تتماشى وواقع هذه البيئة، والتي جاءت مصاحبة ومتزامنة مع التطور الحاصل للقوة في مفهومها الشامل والمتمثلة بالقوة المعلوماتية.

الخاتمة:

يمكن القول تغيرت الرؤية الامريكية بالنسبة الى بيئتها الداخلية، وانعكست تلك الرؤية بالتفكير على المستوى الامني بأبعاده الداخلية، فاصبح يشكل تهديداً كبيراً على امن الدولة، لاسيما في ظل التقنية المتاحة والمتوفرة للأفراد والشركات والتنظيمات الارهابية، فأصبحت حرية الراي والمشاركة متاحة للجميع في الفضاء

الالكتروني، وانعكس ذلك عن تبني نوع معين من العقيدة الاستراتيجية تتماشى وواقع هذه البيئة، والتي جاءت مصاحبة ومتزامنة مع التطور الحاصل للقوة في مفهومها الشامل والمتمثلة بالقوة المعلوماتية. بالاستناد الى ما تقدم يتضح ان القوة المعلوماتية الامريكية قد تطورت بشكل كبير نتيجة لعوامل عدة اثرت في البيئتين الداخلية والخارجية، اي على الصعيدين المحلي والدولي، وانعكس ذلك وبالشكل الكبير والمباشر في رسم الاستراتيجيات التي تنسجم مع متطلبات التحول التي يشهدها عالم اليوم في ظل تسارع تكنولوجيا المعلومات، بالنتيجة احدثت هذه التحولات نقلة نوعية في حركة التفاعلات الدولية من سباق تسلح وحروب وصراعات دولية، كان لها الدور الكبير في اختلالات ميزان القوى الدولي.

ان التطورات التي يشهدها النظام الدولي من تقدم تكنولوجيا اثرت في ميزان القوى، وجعلت من القوة شيئاً نسبياً يختلف عما كان عليه فيما مضى، فقد اصبح امتلاك القوة وتوظيفها وممارسة التأثير والنفوذ في السياسة الدولية امر متاح، لاسيما مع دخول فواعل من غير الدول في النظام الدولي وممارستهم لأنواع عدة من القوة في الفضاء الالكتروني. لذلك، وانسجماً مع متطلبات المرحلة التي يشهدها النظام الدولي والتي تعد منعطفاً خطيراً في العلاقات الدولية، اخذت الدول على عاتقها تبني القوة المعلوماتية، وتأثرت في مقدمتها الولايات المتحدة الامريكية، سيما وانها تبحث دوماً عن متطلبات الهيمنة.

قائمة المصادر والمراجع:

اولاً: الكتب

- 1 - جهاد عودة، المعلومات وصناعة القرار الاستراتيجي، (القاهرة: المكتب العربي للمعارف، 2018).
- 2 - جون باسيت، الحروب المستقبلية في القرن الحادي والعشرين، (ابو ظبي: مركز الامارات للدراسات والبحوث الاستراتيجية، 2014).
- 3 - _____، حرب الفضاء الالكتروني: التسليح واساليب الدفاع الجديدة، (ابو ظبي: مركز الامارات للدراسات والبحوث الاستراتيجية، 2014).
- 4 - ريتشارد كلارك وروبرت نيك، حرب الفضاء الالكتروني: التهديد التالي للأمن القومي وكيفية التعامل معه، (ابو ظبي: مركز الامارات للدراسات والبحوث الاستراتيجية، 2012).
- 5 - عبد القادر محمد فهمي، الفكر السياسي والاستراتيجي للولايات المتحدة الامريكية: دراسة في الافكار والعقائد ووسائل البناء الامبراطوري، (عمان: دار الشروق للنشر والتوزيع، 2009).

- 6 - مارك بيردسول، مستقبل الاستخبارات في القرن الحادي والعشرين، (ابو ظبي: مركز الامارات للدراسات والبحوث الاستراتيجية، 2014).
- 7 - مركز الحرب الناعمة للدراسات، شبكات التواصل الاجتماعي منصات للحرب الامريكية الناعمة، (شبكة المعارف الإسلامية، 2016).

ثانياً: الدوريات والمجلات

- 1 - اسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية، جامعة محمد بوضياف المسيلة، الجزائر، العدد (1)، 2019.
- 2 - إيهاب خليفة، ثورة قادمة: ابتكارات تكنولوجية تغير نمط حياة الأفراد وأوضاع الدول، تحليلات المستقبل، مركز المستقبل للأبحاث والدراسات المتقدمة، ابو ظبي، العدد (16)، 2016.
- 3 - بيتر سنجر، التكنولوجيا العسكرية.. دورها حاسم في الحروب، مجلة آفاق المستقبل، مركز الامارات للدراسات والبحوث الاستراتيجية، ابو ظبي، العدد (27)، 2015.
- 4 - تغريد معين حسن المشهدي، الأثر العسكري للأمن السيبراني في الجغرافيا السياسية للدولة، مجلة البحوث الجغرافية، جامعة الكوفة، كلية الآداب، العدد (30)، 2019.
- 5 - رغدة البهي، الردع السيبراني: المفهوم والاشكاليات والمتطلبات، مجلة العلوم السياسية والقانون، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين، العدد (17)، 2017.
- 6 - روبرت كيوهان، مبني للمجهول: مآلات القيادة الامريكية للنظام الدولي، ترجمة: أحمد محمد ابو زيد، مجلة المستقبل العربي، مركز دراسات الوحدة العربية، بيروت، العدد (404)، 2012.
- 7 - سامر مؤيد عبد اللطيف، الحرب في الفضاء الرقمي رؤية مستقبلية، مجلة رسالة الحقوق، مركز الدراسات القانونية والدستورية، جامعة كربلاء، العدد (2)، 2015.
- 8 - صباح عبد الصبور عبد الحي، استخدام القوة الالكترونية في التفاعلات الدولية، بحوث ودراسات سياسية، المعهد المصري للدراسات السياسية والاستراتيجية، اسطنبول، 2016.
- 9 - عبد الغفار رغيبي، مستقبل الصراع السيبراني العالمي في القرن الـ 21، مجلة السياسة الدولية، مؤسسة الاهرام، القاهرة، العدد (214)، 2018.
- 10 - عادل عبد الصادق، القوة الالكترونية: اسلحة الانتشار الشامل في عصر الفضاء الالكتروني، مجلة السياسة الدولية، مؤسسة الاهرام، القاهرة، العدد (188)، 2012.
- 11 - _____، اسلحة الفضاء الالكتروني في ضوء القانون الدولي الانساني، سلسلة اوراق، وحدة الدراسات المستقبلية، الاسكندرية، العدد (23)، 2016.
- 12 - _____، أنماط الحرب السيبرانية وتداعياتها على الأمن العالمي، ملحق مجلة السياسية الدولية، مؤسسة الاهرام، القاهرة، العدد (208)، 2017.
- 13 - عامر هاشم عواد، حدود الامن القومي الامريكي، مجلة المستنصرية للدراسات العربية والدولية، مركز المستنصرية للدراسات العربية والدولية، بغداد، العدد (42)، 2013.

- 14 - عمار حميد ياسين، مكانة القوة في المدرك الاستراتيجي الأمريكي دراسة في التأصيل النظري والتوظيف الاستراتيجي، مجلة السياسية والدولية، كلية العلوم السياسية، الجامعة المستنصرية، العددان (35-36)، 2017.
- 15 - نورة شلوش، القرصنة الالكترونية في الفضاء السيبراني «التهديد المتصاعد لأمن الدول»، مجلة مركز بابل للدراسات الانسانية، مركز بابل للدراسات الحضارية والتاريخية، جامعة بابل، العدد (2)، 2018.
- 16 - محمد البخاري، الثورة المعلوماتية فجرت الحواجز القائمة بين الشعوب والدول، مجلة المعرفة، دمشق، العدد (576)، 2011.
- 17 - _____، المعلوماتية والعلاقات الدولية في عصر العولمة، مجلة الفيصل، دار الفيصل الثقافية، الرياض، العدد (320)، 2003.
- 18 - 18-وصفي محمد عقيل، التحولات المعرفية للواقعية والليبرالية في نظرية العلاقات الدولية المعاصرة، مجلة دراسات للعلوم الإنسانية والاجتماعية، عمادة البحث العلمي، الجامعة الاردنية، العدد (1)، 2015.
- 19 - يحيى سعيد قاعود وعلا عامر الجعب، وثيقة الامن القومي الامريكي 2017، قراءة تحليلية في استراتيجية دونالد ترامب، مجلة قراءات استراتيجية، منظمة التحرير الفلسطينية، مركز التخطيط الفلسطيني، العدد (20)، 2018.
- 20 - يونس مؤيد يونس، استراتيجية الولايات المتحدة الامريكية للأمن السيبراني، مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين، بغداد، العدد (55)، 2018.

ثالثاً: الرسائل

- 1 - وليد غسان سعيد، دور الحرب الإلكترونية في الصراع العربي الإسرائيلي، رسالة ماجستير (غير منشورة)، جامعة النجاح الوطنية، كلية الدراسات العليا، فلسطين، 2013.

رابعاً: الانترنت

- 1 - الهيئة المنظمة للاتصالات، لمحة عامة حول الأمن السيبراني، لبنان. متاح على الموقع: <http://www.tra.gov.lb/Cybersecurity-in-few-words-AR>.
- 2 - إيهاب خليفة، أبعاد التحول في استراتيجية الدفاع الأمريكية، مركز المستقبل للأبحاث والدراسات المتقدمة، ابو ظبي، 2014، متاح على الموقع: [https://futureuae.com/ar/](https://futureuae.com/ar/Mainpage/Item/856/cyber-defense).
- 1 - المركز العربي لأبحاث الفضاء الالكتروني، عادل عبد الصادق، صراع السيادة السيبرانية بين التوجهات الروسية والأمريكية، التقرير الاستراتيجي العربي 2018، مركز الاهرام للدراسات السياسية والاستراتيجية، القاهرة، 2019. متاح على الموقع: http://accronline.com/article_detail.aspx?id=29415.
- 2 - جيل برعام، تأثير تطور تكنولوجيا الحرب السيبرانية على بناء القوة في اسرائيل، مجلة الدراسات الفلسطينية، مؤسسة الدراسات الفلسطينية، بيروت، 2014. متاح على الموقع: <http://www.palestine-studies.org>.

- 3 - رانيا عبد الله، القوة الإلكترونية وأبعاد التحول في خصائص القوة، اوراق، مجلة الشباب، 2014، متاح على الموقع: <http://shabab.ahram.org.eg/News/21761.aspx>.
- 4 - عمرو صبحي، تكتيك الدرع والسيف في استخدام القوة السيبرانية، دراسات، المركز العربي للبحوث والدراسات، القاهرة، 2018. متاح على الموقع: <http://www.acrseg.org/40716>.
- 5 - يوشياكي ناكاغاوا وسكوت دبليو هارولد وآخرون، التحالف الأمريكي الياباني ومواجهة ضغوطات النزاع البارد (المنطقة الرمادية) في مجالات البحر والفضاء الإلكتروني والفضاء الخارجي، مؤسسة (راند)، سانتا مونيكا، كاليفورنيا، 2017. متاح على الموقع: www.rand.org.

Books:

- 1 - Isaac Bin Israel and Lior Tabansky, An Interdisciplinary View of Security Challenges in the Information Age, Military and Strategic Affairs, Center for Strategic Studies B,institute for National Security Studies cd, Volume 3, No. 3, December 2011.
- 2 - Kristin M. Lord and Travis Sharp, America's Cyber Future: Security and Prosperity in the Information Age, center for a new American security, Francisco in February 2011.

Internet:

- 1 - A A Ghionis, The Limits of Deterrence in the Cyber World An Analysis of Deterrence by Punishment, university of Sussex, 2013. Available on the site: <http://www.inss.org.il>.
- 2 - Gabi Siboni and Ofer Assaf, Guidelines for a National Cyber Strategy, the institute for national security studies, strategic studies center, 2014. Available on the site: <http://www.inss.org.il>.
- 3 - Alyza Sebenius, Writing the Rules of Cyber war, Harvard Kennedy school belfer center Cyber war, June 28, 2017. Available on site: <https://www.belfercenter.org/publication/writing-rules-cyberwar>.
- 4 - Joseph S. Nye, Is Cyber the Perfect Weapon, the world's opinion page, July 05, 2018 <https://www.project-syndicate.org/commentary/deterring-cyber-attacks-and-information-warfare-by-joseph-s--nye-2018-07>.

