مجلة مدارات سياسية
EISSN: 2710 - 8341 ISSN: 2588 - 1825
المجلد (07) / العـدد: (02)، (2023)، ص 287 - 300

الحرب الباردة الأمريكية - الروسية في الفضاء السيبراني

The US-Russian Cold War in Cyberspace

عزالدين قطوش
جامعة الجزائر 3، (الجزائر)، guettouche.azeddine@univ-alger3.dz

تاريخ الإستلام: 2023/07/02 تاريخ قبول النشر: 2023/ 11/07 تاريخ النشر: 2023/ 12/31

ملخص:

أدت الثورة التكنولوجية والمعلوماتية إلى بروز ميدان جديد للتنافس والصراع بين القوى الكبرى وهو الفضاء السيبراني. وظهر معه مفهوم جديد للحروب وهي الحرب السيبرانية، والتي لا تقل خطورة عن الحروب التقليدية من حيث التهديد الذي تنطوي عليه وحجم التدمير الذي يمكن أن تؤدي إليه مع الأخذ بعين الاعتبار السرعة الفائقة في التنفيذ، باستخدام أساليب يصعب تتبعها أو معرفة مصدرها في أغلب الأحيان. وفي محاولة لمواجهة هذه التهديدات الأمنية الجديدة تسعى كل من روسيا والولايات المتحدة إلى صياغة استراتيجيات قومية مع اختلافات كبيرة بينهما في الرؤية والمبادئ والأهداف.

الكلمات مفتاحية:

الاستراتيجية؛ التهديدات؛ الحرب؛ الفضاء؛ السيبرانية.

Abstract:

The cyber conflict between the United States and Russia is still endemic and witnesses continuous transformation between the two countries. Both Russia and the United States enjoy advanced cyber capabilities, and the cyber conflict is consider the primary response to challenges in the twenty-first century. In this article, we will try to examine the cyber conflict between Russia and the United States, and their latest updates in this tense and dangerous cyber conflict.

Keywords:

Cyberwar; Russia; Strateg;, Threats; USA.

1. مقدمة :

برزت بعد نهاية الحرب الباردة تهديدات جديدة لم يشهدها النظام الدولي من قبل وهي ما تعرف بالتهديدات اللاتناظرية أو اللاتماثلية (Asymmetricthreats)، والتي لا تقر لا بالحدود الجغرافية ولا بالسيادة الوطنية، الأمر الذي أدى إلى حدوث تغير جذري في مجال الدراسات الأمنية والاستراتيجية.

من الثابت في تطور العلاقات الدولية أن مصادر قوة الدول غير مستقرة بل تتغير وفق تطور المجتمع، فإلى جانب القوة الصلبة (HardPower) ظهر اهتمام كبير بالقوة الناعمة (SoftPower). لكن بعد ظهور ثورة المعلومات برز شكل جديد من أشكال القوة وهي القوة السيبرانية (Cyber)Power التي أصبحت تؤثر في كل السياسيات العالمية؛ الأمر الذي أدى إلى التغير في موازين ومراكز القوى، وأصبح من يمتلك الآليات الإلكترونية الجديدة ويحسن توظيفها فستكون لديه القدرة على تحقيق الأهداف الاستراتيجية والتأثير في سلوك الفاعلين من الدول والأفراد والمنظمات، بالإضافة إلى حماية أمنه الحيوي وذلك فقط بوسائل بسيطة قد لا تتجاوز جهاز حاسوب أو هاتف نقال مرتبط بشبكة الأنترنيت.

تعتبر الحروب السيبرانية حاليا أهم العناصر الفعالة في السياسة الدولية وفي الاقتصاد بسبب تحول جزء كبير من الصراعات بين الدول الكبرى، خاصة بين روسيا والولايات المتحدة إلى الوسط الرقمي كميدان جديد للحروب.

الإشكالية: تحول الفضاء السيبراني إلى ساحة لحرب باردة متجددة بين الولايات المتحدة وروسيا، ومن أجل ذلك برزت اتجاهات جديدة للصراع الروسي – الأمريكي حول السيادة السيبرانية تحت مظلة التنافس لقيادة النظام الدولي أو التأثير في مساراته. فكيف سيؤثر كل ذلك على مستقبل الصراع السيبراني بين القوتين من جهة وتأثيره على الأمن الجماعي من جهة أخرى.

الفرضيات:

1-سباق التسلح السيبراني بين روسيا والولايات المتحدة قد يؤدي إلى حرب باردة جديدة بأدوات إلكترونية ويمكن أن تتطور لحروب تقليدية بالوكالة.

2-التطور التكنولوجي المتقارب نسبيا بين البلدين في المجال السيبراني من شأنه إعادة بعث نظرية الردع على غرار الردع النووي.

3-تيقن كل من روسيا والولايات المتحدة الأمريكية أن أي حرب سيبرانية بينهما ستكون نتيجتها صفرية فبالتالي سيسعى الطرفين الى امضاء معاهدات ثنائية أو دولية لاجتناب الصدام.

2.الحرب السيبرانية: التهديد الجديد للأمن الدولي.

خاضت العديد من دول العالم على مر العصور حروب دامية سواء بين بعضها البعض أو من خلال حروب أهلية، كما شهد العالم في القرن العشرين حربين عالميتين راح ضحيتها الملايين من القتلى، ودمرت مدن كاملة، وانهار الاقتصاد ومعه النسيج الاجتماعي بسبب الاقتتال بشتى أنواع الأسلحة.

في القرن الحالي تغيرت مفاهيم الحروب والنزاعات، وتغيرت نوعية السلاح واختلفت معها ساحات المعارك، فتحول القتال من الجيوش والآليات الثقيلة، ومن الطائرات والصواريخ وعبر السفن الضخمة والغواصات إلى مجرد جهاز حاسوب فقط تدار به الحروب.

تعد الحرب السيبرانية من أخطر أنواع الحروب المعاصرة، خصوصا مع تطور وسائل الاتصالات ذات التكنولوجية العالية والمرتبطة بشبكة الأنترنيت، واقتحامها لكل ميادين حياة الأفراد والمؤسسات والدول، فباتت جزءا يتحكم في كل المجالات وفي كل الأرجاء سواءا في المساكن ووسائل النقل والقطاع الصحي، وصولا إلى قطاعات الكهرباء والطاقة والمياه وغيرها من خدمات البنى التحتية[1].

الأهمية الوظيفية الحساسة لهذه المرافق، دفعت أغلب دول العالم، إلى سن سياسات عسكرية وأمنية، لمواجهة هذا التهديد الجديد من الحروب، من خلال وضع خطط دفاعية وهجومية تؤمن هدف ردع الأعداء من تنفيذ أي هجوم على مصالحها الحيوية.

مفهوم الحرب السيبرانية هو استخدام التكنولوجيا الحديثة والإنترنت للقيام بالهجمات على الأهداف الحيوية الحكومية والتجارية والصناعية والعسكرية. وتشمل هذه الهجمات الاختراقات الإلكترونية للشبكات، والبرامج الخبيثة، وخدمات الإنترنت المشوهة، والحشرات الضارة، إلخ. وتهدف الحرب السيبرانية إلى تعطيل أو تدمير البنية التحتية الرقمية للأهداف المستهدفة، وعرقلة العمليات الحيوية اللوجستية للدولة أو الشركة أو المؤسسة المستهدفة. وتتطلب الحرب السيبرانية مهارات تقنية عالية وخبرة في الأمن السيبراني والحماية من الهجمات الإلكترونية[2].

تعطي مؤسسة راند (RAND) تعريفا للحرب السيبرانية بأنها: الإجراءات التي تقوم بها دولة أو منظمة لمهاجمة الحواسيب أو شبكات المعلومات في بلد آخر. قائمة على اعتداءات ذات دوافع سياسية على نظم المعلومات عبر الإنترنت، لتعطيل المواقع الرسمية وتعطيل الخدمات الأساسية للدول. فللحرب السيبرانية أهداف بعيدة المدى، وليس لخطورتها حد معين، ولا لأضرارها نطاق محدد، وتتمثل أهدافها أن الهجمات السيبرانية عابرة للحدود، فلا زمان ولا مكان يوقفها. كما يمكنها أن تصل لأي مكان في العالم بسرعة خيالية. ودمارها شديد، فقد تفجر محطات طاقة نووية، وقد تعطل كهرباء مدن كاملة. وقد تصل لأبعد من ذلك، كتعطيل أنظمة تحكم استراتيجية وتغير مسارات الصواريخ وتشوش عليها، وقد يتم اختراق البنوك والتلاعب بالتحويلات المالية وسرقتها. كما تؤدي الهجمات السيبرانية إلى تعطيل الرحلات الجوية والبحرية والبرية وتغيير مسارها[3].

تخصص العديد من الدول، ميزانيات كبيرة على مختلف الأنشطة السيبرانية استعدادا لحروب المستقبل، وأيضا من أجل بناء استراتيجيات جديدة لحرب المعلوماتية، والتي تهدف إلى إثارة الارتباك أثناء عملية صنع القرار لدى الأعداء، وذلك عبر عمليات الاختراق لأنظمتهم المعلوماتية. وهكذا أصبح النصر في الحروب ليس فقط لمن يملك القوة العسكرية، وإنما القادر على شل القوة والتشويش على المعلومة، وتغيير البيئة الثقافية والفكرية للخصوم والتأثير عليها.

فللفضاء السيبراني خصائص فريدة من نوعها في ميدان الحروب والنزاعات حيث تُمكن الدولة أو الأفراد من توجيه الهجمات بسرعة قصوى ضد أعداء يتواجدون على مسافات بعيدة جدا من دون تعرضهم للخطر، إذ تتسم الهجمات التي توجه من خلال هذا الفضاء الافتراضي بالصمت، قلة التكلفة، سرعة الأداء، قوة التأثير، صعوبة معرفة هوية المهاجم والخلفية الأيديولوجية له وغيرها من الصفات التي تجعل من هذه الهجمات شديدة الخطورة.

في أجواء شبيهة بالحرب الباردة يتصارع اليوم الغرب بقيادة الولايات المتحدة والشرق بقيادة روسيا والصين على فرض رؤيتهما لكيفية صياغة قواعد ومبادئ النظام الدولي، والتي من شأنها تنظيم عملية التعامل مع التهديدات الجديدة في الفضاء السيبراني، فالمشهد الدولي أصبح أكثر حساسية بعد تحول روسيا من سياسة العزلة إلى فاعل أساسي في المعادلات الدولية بل والانخراط بقوة من أجل بناء تكتل قوي لمواجهة الولايات المتحدة وحلفاءها.

أدى هذا الصراع بين القوتين والتباين في الرؤى والاستراتيجيات وكذلك المبادئ والأهداف وحتى المفاهيم، إلى عدم التوصل لاتفاق حول الأمن السيبراني، خاصة وأن الولايات المتحدة الأمريكية متمسكة بالهيمنة السيبرانية بعد تدشين قيادة عسكرية للفضاء الالكتروني عام 2009.

3.الاستراتيجية الأمريكية الجديدة للحروب السيبرانية:

جاء في تقرير للمعهد الدولي للدراسات الاستراتيجية لعام 2021، والذي يستعرض القدرات الإلكترونية لـ 15 دولة في العالم، أن الولايات المتحدة تتصدر قائمة هذه الدول، رغم أن أمنها السيبراني كان موضع تساؤلات بعد سلسلة من الهجمات الإلكترونية أطلقها ضدها قراصنة مرتبطين بروسيا والصين وإيران وكوريا الشمالية ودول أخرى. ويقيس المعهد قدرات كل بلد من خلال سبع خصائص أساسية، وهي الاستراتيجية والعقيدة، والحكم والقيادة والتحكم والقدرة الأساسية للاستخبارات الإلكترونية، والتمكين والاعتماد السيبراني، والأمن السيبراني والمرونة والريادة العالمية في شؤون الفضاء السيبراني، والقدرة الهجومية السيبرانية[4].

تعتبر الولايات المتحدة، الدولة الأكثر تفوقا في مجال امتلاك القدرات السيبرانية والعسكرية منها، ولديها قيادة سيبرانية موحدة، هي وكالة الأمن السيبراني وأمن البنى التحتية بناء على استراتيجية وكالة الأمن القومي. وتعتمد القيادة السيبرانية الأمريكية على خمسة مكونات أساسية، هي: القيادة السيبرانية للجيش، وقيادة الأسطول السيبراني، والقيادة الإلكترونية للقوات الجوية، والقيادة الإلكترونية لقوات مشاة البحرية وخفر السواحل، إضافة إلى وحدات الحرس الوطني. ويبلغ عدد الفرق السيبرانية في هذه القيادة نحو 133 فريقا تضطلع بمهمات مختلفة في مجال حماية الأمن السيبراني.

تقدر ميزانية القدرات السيبرانية وتكنولوجيا المعلومات للجيش الأمريكي لسنة 2023 ما مقداره 16.6 مليار دولار. يخصص الجزء الأكبر منها والذي يساوي 9.8 مليار دولار تقريبا للقيادة التكنولوجية لشبكة الجيش الأمريكي (NETCOM)، ويخصص نحو 2 مليار دولار للعمليات السيبرانية الهجومية والدفاعية والبحث والتطوير الخاص بالأمن السيبراني.

عقد فريق عمل "مجلس الأمن القومي" العديد من الاجتماعات الرفيعة المستوى بين عامي 2012 و2014، وذلك من أجل صياغة مجموعة معقدة من السياسات، تعرف باسم التوجيه السياسي الرئاسي رقم 20 (Presidential PolicyDirective20)، تضع من خلاله مبادئ توجيهية بشأن متى يمكن للولايات المتحدة شن عمليات إلكترونية لردع الهجمات المستقبلية. من أجل ذلك كرست هيئة الأركان المشتركة في البنتاغون شهور متتالية من أجل تطوير بروتوكولات صارمة لحساب المدة الفاصلة بين وقوع هجوم سيبراني والتصدي له وردعه والوقت الذي يستطيع فيه وزير الدفاع الموافقة على القيام بهجوم إلكتروني موجه يهدف إلى تحييد هجوم معاد على أمريكا والتصدي له. وقد تم وضع ذلك التخطيط قيد الاختبار في عام 2014 عندما شن قراصنة كوريون شماليون أول هجوم سيبراني على الأراضي الأمريكية أين دمروا من خلاله شبكات سوني (Sony) الرقمية.

تولى الرئيس الأمريكي "دونالد ترامب" (DonaldTrump) منصب الرئاسة عام 2017 فكان أكثر صرامة من سلفه، حيث كان نهج إدارته تجاه أعداء الولايات المتحدة غير ثابت ولا يمكن التنبؤ به. لكن في عام 2018، وافق البيت الأبيض على رفع مستوى القيادة السيبرانية إلى قيادة قتالية كاملة، ما حررها من القيود التي كانت تفرض عليها العمل من خلال القيادة الاستراتيجية الأميركية. كما أعلن مستشار الأمن القومي "جون بولتون" (JohnBolton) أن الإدارة الأمريكية ستتخذ نهجا أكثر عدوانية تجاه العمليات الإلكترونية الهجومية عن طريق السماح للجيش بإجراء عمليات استباقية بعد موافقة وزير الدفاع.

بناءا على ذلك أقرت الولايات المتحدة عام 2018 استراتيجية جديدة للأمن السيبراني بعد التهديدات الإلكترونية والهجمات السيبرانية ضدها من قبل روسيا والصين وآخرين، حيث دخلت حيز التنفيذ بعد قرار الرئيس دونالد ترامب إلغاء كل القواعد التي حددها الرئيس السابق ب"اراك أوباما" (BarackObama) للعمليات السيبرانية عام 2012 والاتجاه للاستعداد للحرب السيبرانية من خلال بناء قوة أكثر بطشا، وأن قيام أي دولة بنشاط سيبراني ضد الولايات المتحدة الأمريكية سيكون الرد عليه بطريقة هجومية ودفاعية، ولن يتم بالضرورة في الفضاء السيبراني بل قد يتعداه ليشمل استخدام القدرات العسكرية التقليدية.

تعد الاستراتيجية السيبرانية الجديدة، أول استراتيجية مفصلة للولايات المتحدة منذ عام 2003 عندما أصدرت إدارة الرئيس الأمريكي الأسبق "جورج دبليو بوش" (GeorgeW.Bush) استراتيجيتها القومية لحماية الفضاء السيبراني من الهجمات السيبرانية. انطلاقا من قناعة بأن الولايات المتحدة هي التي أنشأت الإنترنت، وأن عليها أن تحافظ على

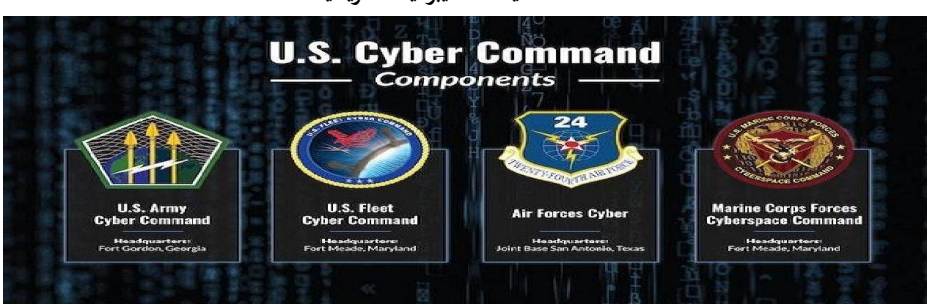
دورها المهيمن في تحديد الفضاء السيبراني وتشكيله وحمايته، لأنه الميدان الوحيد الذي يمكن فيه تحييد القوة العظيمة الاقتصادية والعسكرية والسياسية لأمريكا[5].

تسمح الاستراتيجية السيبرانية الجديدة بأن تقوم المؤسسة العسكرية الأمريكية والوكالات الأخرى بعمليات سيبرانية، الهدف منها حماية أنظمة شبكاتها المعلوماتية لأن استهدافها من شأنه التأثير في المكانة الدولية لأمريكا وفي قوتها. كما تأتي الاستراتيجية السيبرانية الجديدة للولايات المتحدة في إطار المساعي لإنشاء فرع سادس للجيش الأمريكي يركز على الفضاء السيبراني ويحقق هيمنة أمريكية على هذا الميدان الجديد للحروب المستقبلية. ويكون ذلك من خلال تبادل المعلومات؛ وإعطاء وزارة الدفاع مزيدا من الصلاحيات لرقابة جهود الأمن السيبراني، ومكافحة الجرائم السيبرانية من خلال التعاون مع الدول الأخرى لتعقب منفذيها.

تعتمد الاستراتيجية الجديدة أيضا على تعزيز الاقتصاد الأمريكي الرقمي، بتشجيع الابتكار في قطاع التكنولوجيا والذكاء الاصطناعي، بالإضافة إلى بناء قوة عاملة حكومية في مجال الأمن السيبراني من خلال توظيف المتخصصين في مجال الأمن السيبراني في المؤسسات الأمريكية. فمن بين أهداف الاستراتيجية الجديدة للولايات المتحدة الأمريكية مكافحة التهديدات السيبرانية، من خلال استخدام كافة أدوات القوة لردع أي هجمات سيبرانية، وتعزيز المعايير الدولية في الفضاء السيبراني، كما تدعو إلى حرية الإنترنت في جميع أنحاء العالم وتزويد حلفاء الولايات المتحدة بقدرات سيبرانية؛ للتعامل مع التهديدات السيبرانية التي تستهدف مصالحهم المشتركة.

تعد كتيبة دعم الحرب الإلكترونية 915، أحد الكيانات الجديدة نسبيا. حيث تتكون الكتيبة والتي تم إنشاؤها في عام 2019، من 12 فريقا تدعم فرق الألوية القتالية أو غيرها من التشكيلات التكتيكية. كما تم إنشاء كتيبة هجومية جديدة للعمليات السيبرانية (ARCYBER) عام 2021 لدعم القوات الإلكترونية للجيش الأمريكي والدفاع عن البلاد من الهجمات السيبرانية. من أجل نجاح هذه الاستراتيجية تخصص وزارة الدفاع الأمريكية مبالغ كبيرة لهذا الغرض، فقد بلغت الميزانية الإجمالية لوزارة الدفاع الأمريكية لعام 2022، 778 مليار دولار، وشملت العديد من الأنشطة العسكرية والدفاعية، بما في ذلك الدفاع السيبراني، والذي خصص له أكثر من 100 مليار دولار[6].

القيادة السيبرانية الأمريكية



المصدر: وزارة الدفاع الأمريكية https://www.defense.gov/News

وتجدر الإشارة إلى أن الميزانية السيبرانية لوزارة الدفاع تعتمد على العديد من العوامل، بما في ذلك الحاجة إلى التكنولوجيا الحديثة والتدريب المتخصص والتحديث المستمر والبحث والتطوير، كتعزيز الحماية السيبرانية للأنظمة الدفاعية وتدعيم القدرة على استجابة الأمن السيبراني في حالات الهجمات الإلكترونية المحتملة. كما تتضمن الميزانية أيضا الجهود الداخلية لحماية البيانات الحساسة وسد الثغرات الأمنية والحفاظ على الأمان السيبراني العام للحكومة الأمريكية. كما تشمل الميزانية السيبرانية للدفاع الأمريكي أيضا تحديث وتطوير أنظمة الاتصالات السيبرانية واللوجستية وتطوير تقنيات الذكاء الاصطناعي والحوسبة السحابية لمساعدة القوات الأمريكية في القيام بمهامها بفعالية وكفاءة أكبر. ومعظم هذه الأمور تتضمن تكاليف عالية، وهو ما يؤدي إلى زيادة الميزانية السيبرانية للدفاع الأمريكي.

من هنا نستنتج أن استراتيجية الفضاء السيبراني الأمريكي تقوم على مبدأ الدفاع المتقدم لذا ينظر البعض إلى القوة السيبرانية الأمريكية على أنها قوة هجومية في المقام الأول تستند على دمج القدرات التكنولوجية في جميع مراحل العمليات التي تقوم بها. فوفقا لخارطة طريق أولية تمتد ما بين 2021 و2027، ستنشئ (ARCYBER) مركزا لعمليات حرب المعلومات، مما سيوفر قدرة غير مسبوقة لاستشعار وفهم والاستجابة لظروف الهجمات السيبرانية، كما يتيح للقيادة العليا للجيش خيارات متعددة وفرص مواتية لاتخاذ القرار الاستراتيجي الصائب في وقت قياسي.

4.الاستراتيجية السيبرانية الروسية

يختلف المنظور الروسي للحرب السيبرانية بشكل واضح عن نظيره الأمريكي، ويبدو ذلك واضحا من خلال الطريقة التي يعرف بها المنظرون الروس الحرب السيبرانية؛ على أنها كيفية استخدام الكرملين لقدراته في الإنترنت لتحقيق الأهداف القومية لروسيا الاتحادية.

فالمسؤولون الروس مقتنعون بأن موسكو تخوض عملية صراع وجودي مستمر مع قوى داخلية وخارجية تسعى إلى تحدي أمنها في عالم المعلوماتية، ويرون في الإنترنت والتدفق الحر أنها تشكل تهديدا وفي نفس الوقت فرصة يمكن استغلالها بصورة ايجابية لخدمة الأهداف القومية على حد سواء، كما أنهم يصورون العمليات الإلكترونية ضمن الإطار الأوسع لحرب المعلومات، والذي هو عبارة عن مفهوم شامل يتضمن عمليات شبكة الحاسوب والحرب الإلكترونية والعمليات النفسية. كما ترى موسكو الصراع داخل مجال المعلومات هو عملية مستمرة ولا تقف عند حدود معينة، بالتالي فإن للكرملين عقيدة معينة في استخدام الإنترنت تختلف عن تلك المتبعة في الولايات المتحدة والدول الأوروبية.

ومن أبرز منظري الاستراتيجية الروسية الجنرال "فاليري غيراسيموف" (ValeryGherassimov) الرئيس الحالي لهيئة الأركان العامة للقوات المسلحة الروسية ونائب وزير الدفاع الأول. فوفق عقيدته للاستراتيجية الروسية السيبرانية (TheGherassimovdoctrine) التي أصدرها عام 2013: فإن الخطوط بين السلم والحرب غير واضحة المعالم في العالم المعاصر، وغالبا ما تكون الصراعات غامضة وغير معروفة المصدر، فمهما بلغ حجم القوات التي يملكها

العدو، ومهما بلغت درجة تطور قواته ووسائله الحربية فإنه من الممكن إيجاد السبل والأدوات الازمة للتغلب عليه، إذ سيكون دوما لدى الخصم نقاط ضعف مما يعني البحث عن سبل ووسائل مناسبة لمحاربته[7].

وفي دراسة للمفكر الأمريكي "دافيد سميث" (DavidJ.Smith) " بعنوان كيف تستخدم روسيا الحرب السيبرانية؟ يرى أن موسكو تعتمد على مفهوم واسع للحرب المعلوماتية، يشمل الاستخبارات والتجسس المضاد، والخداع والتضليل وتدمير الاتصالات وأنظمة دعم الملاحة الجوية والبحرية والضغوط النفسية، بالإضافة إلى الدعاية وإلحاق الضرر بنظم المعلومات.

سارعت روسيا في سياق حربها الباردة في الميدان السيبراني مع الولايات المتحدة الأمريكية إلى تعزيز أمنهما في مواجهة أي هجمات محتملة من الأطراف الأخرى، حيث أنشأ جهاز الأمن الفيدرالي الروسي عام 2018 تزامنا مع اعتماد الاستراتيجية الأمريكية في الفضاء السيبراني، مركزا وطنيا لتنسيق مكافحة الهجمات السيبرانية على البنية التحتية الحيوية في روسيا، يتولى مهام الكشف والوقاية والقضاء على تداعيات الهجمات الإلكترونية، وتبادل المعلومات بين الهيئات المتخصصة في الداخل والخارج وتحليل الهجمات السيبرانية الماضية وتطوير أساليب مكافحتها[8].

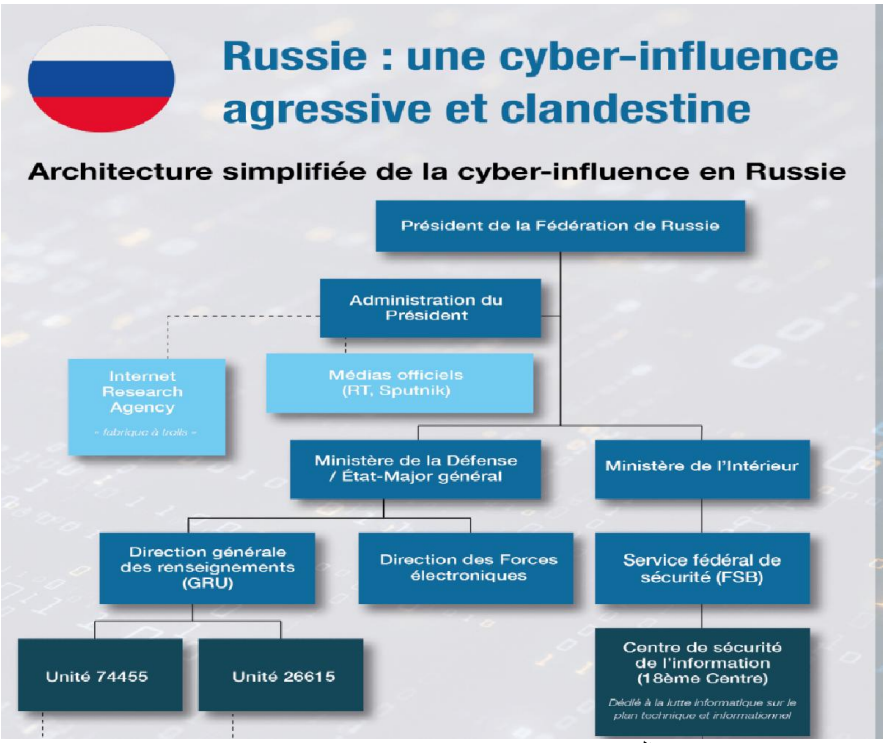
ومن أجل التطبيق الناجح للاستراتيجية الروسية في الحرب السيبرانية، وافق البرلمان الروسي في 12 فيفري 2018 على قانون عزل البلاد عن شبكة الإنترنت العالمية، لجعل روسيا في موقع أفضل لصد أي هجمات إلكترونية محتملة من الخارج، خاصة من قبل الولايات المتحدة الأمريكية. فالهجمات الإلكترونية وفق استراتيجية الأمن الروسي تأتي الأولى ضمن قائمة أكثر المخاطر التي تهدد البنية التحتية الروسية، بينما تأتى في المرتبة الثانية عملية تطوير القدرات التكنولوجية للقوات المسلحة حتى يتحقق الردع الإلكتروني.

أنشأت روسيا الاتحادية وكالة أبحاث الانترنت، أو ما يعرف باسم "جيش المتصيدين" (Army Troll) تابع لوكالة الأمن الاتحادي الروسي، يضم آلاف الموظفين، ويخصص له سنوياً نحو300 مليون دولار من ميزانية الدفاع الروسية، إذ يعد الجيش الالكتروني الروسي خامس أقوى جيوش العالم الالكترونية بعد كل من: الولايات المتحدة والصين وبريطانيا وكوريا الشمالية على التوالي.

وتتلخص مهمات الجيش الالكتروني الروسي في القيام بعمليات التجسس على الخصوم والقيام الهجمات الإلكترونية التي تسبب الضرر للبنى التحتية والاقتصاد والمواقع الحكومية في الدول الأجنبية المعادية. كما تشن حروب معلوماتية في وسائل الإعلام والشبكات الاجتماعية عن طريق القيام بعمليات اختراق الحسابات والبريد الالكتروني، وانشاء حسابات وهمية على شبكة المعلومات الدولية وفتح الآلاف من الحسابات المزيفة على مواقع التواصل الاجتماعي للرد على الآلاف من التعليقات والمقالات، ونشر الشائعات وتظليل الحقائق في محاولة لدعم الموقف الروسي وتوجيه الرأي العام ضد الخصوم.

تلعب السيبرانية الهجومية دورا أكبر في العمليات العسكرية الروسية التقليدية، وربما ستلعب دوراً أكبر في المستقبل في إطار استراتيجية الردع الروسية، بالرغم من أن الجيش الروسي كان بطيئاً في اعتناق العقيدة السيبرانية لأسباب هيكلية وعقيدية على حد سواء، فقد أشار الكرملين إلى أنه يعتزم تعزيز القدرات الهجومية السيبرانية فضلاً عن الدفاعية للقوات المسلحة الروسية. تعتمد الاستراتيجية الروسية الخاصة بالحروب السيبرانية على استخدام الأسلحة الإلكترونية الهجومية باعتبارها قوة مضاعفة (Multiplier Force) في الحروب، حيث تزيد من القدرات القتالية للدولة إذا ما تم استخدامها إلى جانب القدرات العسكرية أخرى[9].

هياكل التأثير السيبراني الروسي



المصدر: Focus stratégique, n° 104, mars 2021

كما تعتمد أيضا على محاولة تعطيل البنية التحتية والمعلوماتية للخصم والاتصالات المدنية والعسكرية له قبل البدء في العمليات العسكرية التقليدية. فوفقا للعقيدة العسكرية الروسية، لابد أن يسبق الهجوم العسكري الناجح عمليات أخرى تهدف إلى منع الخصم من الحصول على معلومات من المصادر الخارجية، وتعطيل عمليات التداولات المالية والائتمانية ومحاولة التأثير في الرأي العام في دول الخصم عن طريق المعلومات الخاطئة والدعاية التي تخدم المصالح الروسية. فخلافا للنسخ السابقة من استراتيجية الأمن القومي الروسي، أعارت النسخة المحدثة منها التي وقعها الرئيس

"فلاديمير بوتين" (VladimirPoutine) سنة 2021 اهتماما خاصا بملف الأمن السيبراني، الذي بات يشغل أولوية قصوى ليس فقط على المستوى الخارجي، بل على المستوى الداخلي أيضا.

بالاستناد إلى نص الوثيقة، فإن التوجهات الرئيسة، التي برزت في الاستراتيجية الروسية الجديدة تشمل أيضا التحذير من أن التطور السريع لتكنولوجيات المعلومات والاتصالات يزيد من احتمالات ظهور مخاطر على أمن المواطنين والمجتمع والدولة، وأن توسيع نطاق استخدام تكنولوجيات المعلومات والاتصالات للتدخل في شؤون دول وتقويض سيادتها ووحدة أراضيها بات يشكل خطرا على الأمن والسلام الدوليين. وهنا توقفت الاستراتيجية الروسية عند تزايد عدد الهجمات على الموارد المعلوماتية ومعظمها ينفذ من خارج البلاد، لتلفت الأنظار إلى أن المبادرات الروسية الرامية إلى ضمان الأمن المعلوماتي الدولي تواجه معارضة من قبل دول أجنبية تسعى إلى الهيمنة في الفضاء المعلوماتي العالمي.

يظهر نص الوثيقة أيضا معارضة روسيا الكاملة للاتهامات الغربية لموسكو، وفي المقابل تتهم أجهزة استخباراتية أجنبية بتكثيف أنشطتها الرامية إلى تنفيذ عمليات في المجال المعلوماتي الخاص بروسيا. فحسب الوثيقة فإن روسيا تواجه حملات تضليلية وتخريبية في الإنترنت تستهدف بالدرجة الأولى الشباب، مع اتهام شركات دولية عملاقة مثل «غوغل» على ترسيخ احتكارها في الإنترنت والسيطرة على كل الموارد المعلوماتية من خلال فرض الرقابة غير القانونية وإغلاق موارد معلوماتية بديلة. بهذه التحذيرات والاتهامات للغرب، تدفع استراتيجية الأمن القومي الروسي عمليا إلى وضع ملف المواجهة السيبرانية وأمن المعلومات في مقدمة معركتها الحالية مع الغرب. من بين الآليات التي وضعتها الاستراتيجية الروسية لتحقيق هذا الهدف هو إنشاء فضاء آمن لتداول المعلومات الموثوق بها وكذلك تحصين البنى التحتية الخاصة بالمجال المعلوماتي في روسيا منع التأثير التخريبي بالوسائل التكنولوجية على الموارد المعلوماتية الروسية مع تهيئة الظروف الملائمة لكشف ومنع الجرائم في الإنترنت أو السيطرة الأجنبية على أنشطته.

تمثلت أهداف الاستراتيجية الروسية أيضا في تقليص عدد حالات تسرب البيانات السرية والشخصية إلى أدنى حد ممكن، وتعزيز الأمن المعلوماتي الخاص بقوات الجيش الروسي ومنتجي الأسلحة والمعدات العسكرية، وتطوير وسائل وأساليب ضمان الأمن المعلوماتي باستخدام تكنولوجيات حديثة، منها الذكاء الاصطناعي وأخيرا، تعزيز التعاون مع الشركاء الأجانب في مجال ضمان الأمن المعلوماتي، بما يخدم خاصة إنشاء نظام دولي جديد خاص بهذا الشأن.

مما تقدم يتضح بأن القيادة الروسية عملت في السنوات القليلة الماضية بشكل دؤوب على تنمية قدرات روسيا في المجال السيبراني وتطويرها بشكل كبير، وسخرت تلك القدرات بصورة ذكية كسلاح فعال لإيقاع الضرر المطلوب في قدرات خصومها، بالشكل الذي جعل من تلك القدرات السيبرانية أحد عناصر الردع الاستراتيجي للدولة الروسية[10].

5.الصدام الأمريكي الروسي في الفضاء السيبراني:

أخذت الحرب الأمريكية الروسية منحنى جديد، فبعد عهد الحرب الباردة، ظهرت أواخر عام 2020 حرب إلكترونية بين أكبر قوتين عسكريتين في العالم، ليعيد الصراع من جديد بين واشنطن وموسكو من أسلوب الحرب

التقليدية إلى الصدامات الإلكترونية. فقد كشفت جولات الحوار الروسي الأميركي التي جرت خلال عام 2021 في مدينة جنيف السويسرية، أن الاهتمام الرئيس لم ينصب على ملفات الأزمات الإقليمية الساخنة، رغم أهميتها ولا على ملفات التسلح ونزع السلاح والمعاهدات. بل أن الملف الأساسي الذي فرض نفسه على برنامج النقاشات يتعلق بأمن المعلومات الذي بات يتخذ في الآونة الأخيرة بشكل متزايد صفة العنصر الرئيس للاستقرار الاستراتيجي.

إبان الانتخابات الأمريكية لسنة 2016، تم اتهام روسيا باستخدام الاختراق السيبراني كوسيلة للتأثير في نتائج تلك الانتخابات، لصالح الرئيس "دونالد ترامب". ورغم أنه لم يتم الحسم بعد في ذلك الاتهام، لكن الحرب السيبرانية اشتعلت من جديد بسبب تعرض العديد من الوزارات والهيئات ومؤسسات أمريكية حساسة عام 2020، لهجمات سيبرانية تم استهداف من خلالها، المكتب الذي يدير الأسلحة النووية، التابع لوزارة الطاقة الأمريكية وأيضا وزارتا التجارة والخزانة ولم يقتصر تأثيرها فقط على الإدارة الأمريكية بل امتد ليشمل الشعب الأمريكي كافة. الهجوم نفذته مجموعة هاكرز تدعمهم روسيا، وفق تصريح لوزير خارجية الولايات المتحدة الأميركية السابق "مايك بومبيو"(Mike Pompeo) رغم النفي الرسمي الروسي لتورطها في هذه الهجمات.

لقد قام الروس باستعراض تقنياتهم في الحرب الإلكترونية منذ الهجوم الإلكتروني على إستونيا عام 2007 ثم أثناء الحرب في القرم 2014 وسوريا والحرب الأخيرة في أوكرانيا 2022 من خلال تعطيل الأجهزة اللاسلكية ومنع الاتصال بالطائرات بدون طيار. وقد فاجأ الجيش الروسي الخبراء في ميدان الحرب الإلكترونية لاستخدامهم أسلحة وآليات قائمة على التكنولوجيا العالية القادرة على اختراق أنظمة الطائرات بدون طيار والتشويش على الرادارات، مما جعل كبار الضباط في الجيش الأمريكي يعترفون بأنهم قد تأخروا على الروس في هذا المجال. فعندما يتمكن بلد أجنبي من التسلل إلى المنشآت الأمريكية وينفذ هجمات سيبرانية ويخترق أنظمتها فهذا يشير إلى ضعف أنظمة الدفاع السيبراني في الولايات المتحدة.

هناك العديد من أوجه التشابه بين واشنطن وموسكو فيما يخص الردع الإلكتروني رغم اختلاف القدرات لذلك ينظر كل منهما إلى الآخر على أنه عدو ذو قدرة عالية في المجال السيبراني، ورغم أوجه التشابه التي يتشاركان فيها في مجال الاستهداف الإلكتروني، إلا أن كل من موسكو وواشنطن مرتا بمسارات مختلفة في تطوير القدرات والسياسات الخاصة بالحرب الإلكترونية، ويعزى ذلك في جزء كبير منه إلى التفسيرات المختلفة لكلا الطرفين للأحداث العالمية ومقدار الموارد المتاحة أمامهما، مما خلق فجوة في مجال استخدام العمليات الإلكترونية والقدرة على إطلاقها. ففي حين فشلت الولايات المتحدة في مواكبة القدرات الجديدة في مجال العمليات الإلكترونية، خاصة داخل جيشها، فقد تفوقت روسيا في استخدام العمليات الإلكترونية ضد الخصوم المحتملين، من خلال تعزيز قدراتها العسكرية الإلكترونية وتوسيع مبادرات التجنيد وتطوير البرمجيات الضارة والفيروسات[11].

لا يكمن خطر الردع السيبراني في إرادة كلا الطرفين وقدراتهما المتقاربة فقط بقدر ما هو متجذر في سوء التفاهم المتبادل. فالسلطات السيبرانية في الكرملين تملك وجهة نظر ثابتة، مفادها أن الولايات المتحدة الأمريكية تسعى إلى تقويض مكانة روسيا العالمية في المجال الرقمي. بينما السلطات في واشنطن لا تبذل جهدا كبيرا لفهم مدى تعقد الرؤية الاستراتيجية الروسية للحرب السيبرانية خاصة إذا علمنا أن المخترقين في موسكو غير مقيدين نسبيا بالحدود القانونية أو المعيارية. فمن أجل التغطية عن هذا العجز في المجال السيبراني تقوم إدارة "جو بايدن" (JoeBiden) بعملية التصعيد من خلال التهديد بفرض عقوبات إضافية على روسيا في المستقبل، وممارسة المزيد من الضغوطات الاقتصادية ومحاولة إقامة حصار شامل ضدها.

ففي الحروب السيبرانية تستخدم أربع وسائل رئيسية، أولا أنها حرب بالوكالة، ثانيا هدم الدولة من الداخل، ثالثا الحصار الاقتصادي المؤسسي، ورابعا الحرب النفسية، وقد ظهرت كل هذه الأدوات بشكل واضح في الصراع السيبراني الدائر بين روسيا وأمريكا، لا سيما فيما يتعلق بالحصار الاقتصادي المؤسسي كسلاح في تلك الحرب، بالتوازي مع توظيف التقنيات التكنولوجية والهجمات السيبرانية كأداة من أدوات الحرب لتدمير المجتمع من الداخل وإضعاف قدرات الطرف الآخر[12].

إن ثمة حربا باردة جديدة بين الولايات المتحدة وروسيا تفرض نفسها على الساحة بأدوات مختلفة وفي فضاء جديد، وهي حرب مستمرة وستستمر خاصة مع التطور الهائل والسريع في ميدان تكنولوجيات الاتصال وكذا الذكاء الاصطناعي. لكن وعند النظر إلى القواعد التي تحكم العلاقات الروسية الأمريكية في الوقت الراهن، نجد أنه من الصعب أن تهزم أمريكا روسيا في الحرب السيبرانية كما أن روسيا لا تسعى لهزيمة الولايات المتحدة، لأنها تدرك أنها تفتقر إلى القوة المطلوبة، فكل ما في الأمر أنها تريد احتواء الولايات المتحدة في إطار نظام دولي مرن متعدد الأقطاب يبقي على التوازنات في النظام الدولي.

6. مستقبل الصراع السيبراني الأمريكي–الروسي.

استمرار الصراع السيبراني بين الولايات المتحدة الأمريكية وروسيا قد يؤدي إلى تصاعده والانتقال به من الصراع على السيادة والهيمنة في الفضاء السيبراني الى ميدان الفضاء الخارجي خاصة مع التداخل والتكامل بين كلا المجالين. فروسيا تدرك جيدا أن القدرة الفضائية المتفوقة لأمريكا هي نقطة ضعفها. حيث تعتمد القوات الأمريكية في مناطق الحرب على كوكبة من 31 قمرا صناعيا لتحديد المواقع العسكرية المستهدفة وتحديد حتى أماكن الأفراد. هذا ما يجعل روسيا أول دولة تطور وتختبر نظام الصواريخ المضادة للأقمار الصناعية (ASATS) والتي تم تصميمها خصيصا لضرب الأقمار الصناعية للعدو، فالتفوق في ميدان الفضاء الخارجي معناه التفوق في الفضاء السيبراني وعلى الأرض.

الصراع بين الولايات المتحدة الأمريكية وروسيا من أجل تعزيز القيادة والسيطرة قد ينتقل من الصراع الناعم المقتصر فقط على المجال المعلوماتي إلى الصراع الصلب من خلال الاستحواذ على القوة السيبرانية ذات الطابع التدميري،

وبناء القدرات في مجال شن الهجمات السيبرانية المنظمة والتحول من تبني السياسات الدفاعية إلى أخري هجومية ذات طابع استباقي مما يهدد بعسكرة الفضاء السيبراني وتحوله إلى ميدان حرب حقيقية.

من أجل كل ذلك تسعى كل من روسيا والولايات المتحدة الأمريكية إلى إيجاد الدعم لسياساتهما السيبرانية عبر تكتلات دولية وإقليمية تضمن لهما المساندة والضغط على الطرف الآخر من خلال سلاح العقوبات. لقد تم توظيف الفضاء السيبراني لتحقيق أهداف خارجية والتدخل في الشئون الداخلية للدول من خلال دعم حركات معارضة سياسية أو مسلحة سواء عبر تقديم الدعم التقني او السياسي أو الإعلامي. فالولايات المتحدة الأمريكية تعمل على توظيف الفضاء السيبراني لفرض العقوبات الدولية على كل من يهدد أمنها، وذلك بمنع تصدير التكنولوجيا العسكرية وقطع كابلات الانترنت الواصلة للدول العدوة أو حجب المواقع المساندة للأنظمة المعادية.

7.الخاتمة

من خلال هذه الدراسة المقارنة نستنتج أن تصاعد حدة الصراع بين القوتين الأمريكية والروسية في الفضاء السيبراني سيعمل على تهديد الأمن الجماعي الدولي مثلما كان الحال عليه إبان الحرب الباردة وهو ما يعزز اتجاه إعادة الاعتبار للقانون الدولي والمنظمات الدولية في حفظ الأمن والسلم الدوليين.

فإذا كانت التهديدات المرتبطة بالأمن السيبراني العالمي تجعل جميع الدول متساوية فلا بد من مناقشتها ليس ضمن دائرة ضيقة من الدول المتقدمة في ميدان الفضاء السيبراني على غرار الولايات المتحدة الأمريكية روسيا والصين، ولكن مع جميع دول الأمم المتحدة، وذلك من أجل إبرام معاهدة شاملة تمنع أي نشاط إلكتروني ضار ضد البنى التحتية الحيوية لكل دولة عضو في الأمم المتحدة خاصة أن القانون الدولي القائم بما في ذلك ميثاق الأمم المتحدة بأكمله والقانون الدولي لحقوق الإنسان ينطبق على الفضاء الإلكتروني.

في الأخير يرى الخبير في الأمن السيبراني الدكتور" ادوين لي أرميستيد" (Armistead Lee Edwin)الذي ألف كتاب "عملية المعلومات: الحرب والواقع الصعب للقوة الناعمة" أن: عصر الحرب الباردة ثنائية الأقطاب قد انتهت ونحن نعيش الآن في عصر حيث السرعة هي أهم عنصر من عناصر القوة، لذلك فإن ما يخبئه المستقبل للقوات العسكرية، ومؤسسات الأمن القومي غير واضح ولا يمكن التنبؤ به".

8. الهوامش:

1حازم محمد خليل، استغلال الفضاء السيبراني في الحروب غير التقليدية: دراسة في الوكالة السيبرانية والإرهاب السيبراني، **المجلة العلمية لكلية الدراسات الاقتصادية والعلوم السياسية** جامعة الإسكندرية المجلد الثامن العدد 15 (يناير 2023) ص، 270.

2 أيمن سلامة، السيبرانية جديد الحرب الباردة بين روسيا وأميركا، على الرابط: https://www.skynewsarabia.com/blog/1401823 تاريخ التصفح يوم: 07 مارس 2023.

3 الحروب السيبرانية، وجهٌ جديد للعنف الدولي، على الرابط: https://elakademiapost.com تاريخ التصفح يوم: 20 سبتمبر 2022.

4 Military cyber capabilities، the military balance، London 2O21, pp. 503,506.

5 استراتيجية أميركية جديدة أكثر صرامة للأمن السيبراني، على الرابط:

https://www.alaraby.co.uk/entertainment_media/، تاريخ التصفح يوم: 14 فيفري 2023.

6 الحروب السيبرانية. نتائج ملموسة لمعارك غير مرئية، على الرابط:

https://www.aljundi.ae، تاريخ التصفح يوم: 2023/01/12.

7 Eugene Rumer, The Primakov (Not Gerasimov) Doctrine in Action, Carnegie Endowment for International Peace, Washigton DC, 2019, p12.

8 J. Betz et Tim Stevens ،Le cyberespace et l'État: vers une stratégie pour le cyber pouvoir; Routledge ، London, 2011. P. 157.

9 رغدة البهي، الردع السيبراني المفهوم والإشكاليات والمتطلبات، مجلة الدراسات الإعلامية المركز الديمقراطي العربي العدد الأول جانفي 2018، ألمانيا، ص، 220.

10 Kévin Limonier, La Russie dans le cyberespace : représentations et enjeux, Hérodote (n° 152-153), Éditions La Découverte, Paris ,2014, p 141.

11 Jean-Sun Luigi, Cyberguerre, nouveau visage de la guerre, Revue Stratégique (N° 112), Institut de Stratégie Comparée, Paris, 2016, p. 98.

12 Boyer. B, Cyber tactique, Conduire la guerre numérique, édition Nuvis, Paris 2014. P. 72.

9. قائمة المراجع:

– باللغة العربية

1) استراتيجية أميركية جديدة أكثر صرامة للأمن السيبراني، في: http://bitly.ws/FV42، (04/ 03/ 2023).

2) أيمن سلامة، السيبرانية جديد الحرب الباردة بين روسيا وأميركا في: http://bitly.ws/FPkU، (2020/12/19).

3)الحروب السيبرانية. نتائج ملموسة لمعارك غير مرئية، في:http://bitly.ws/JcpC ، (2021/04/01).

4) حازم محمد خليل، استغلال الفضاء السيبراني في الحروب غير التقليدية: دراسة في الوكالة السيبرانية والإرهاب السيبراني، **المجلة العلمية لكلية الدراسات الاقتصادية والعلوم السياسية** جامعة الإسكندرية المجلد الثامن العدد 15 (يناير 2023) ص، 270.

5) رغدة البهي، الردع السيبراني المفهوم والإشكاليات والمتطلبات، **مجلة الدراسات الإعلامية المركز الديمقراطي العربي**، العدد الأول (جانفي 2018).

– باللغة الأجنبية

1)Boyer. B, Cyber tactique, Conduire la guerre numérique, édition Nuvis, Paris 2014.

2) Eugene Rumer, the Primakov (Not Gerasimov) Doctrine in Action, Carnegie Endowment for International Peace, Washington DC, 2019.

3) J. Betz et Tim Stevens ،Le cyberespace et l'État: vers une stratégie pour le cyber pouvoir; Routledge ، London, 2011.

4) Jean-Sun Luigi, Cyberguerre, nouveau visage de la guerre, **Revue Stratégique** (N° 112), Institut de Stratégie Comparée, Paris, 2016.

5) Kévin Limonier, La Russie dans le cyberespace : représentations et enjeux, **Hérodote** (n° 152-153), Éditions La Découverte, Paris ,2014.