رؤية استراتيجية

العمليات السيبرانية الأوروأطلسية ومهددات الجيوسيبرانية الروسية «رؤية في الاشتباك السيبراني الأورو ـ روسي»

علي زياد فتحي*
باحث من العراق

* طالب دكتوراه ـ كلية العلوم السياسية ـ جامعة النهرين

المقدمــة

قد ساهم التطور السريع لتكنولوجيا المعلومات والاتصالات خلال العقود الماضية إسهاما ملحوظا في زيادة القدرة التصارعية بين القوى المتضاربة في مضامير السياسية الدولية، حيث احدث الصراع والتنافر الاستراتيجي بين القوى الاورواسيوية من جهة وروسيا الاتحادية من جهة أخرى الى بلوج نوع جديد من الصراع والتصاعد الاستراتيجي بأبعاده جديدة من خلال بلجوج جيل جديد من أدوات الصراع والاشتباك والذي غير أن هذا التوصيل والاتكال المتزايدين قد أحدث أيضا طائفة واسعة من التحديات الجديدة، من هجمات الحرمان من الخدمة وسرقة الملكية الفكرية إلى الهجمات على الشبكات الحكومية والهياكل الأساسية الحيوية.

ظلت الصراعات التقليدية والقوة العسكرية تحددان لفترة طويلة طبيعة الصراعات الدولية بين روسيا ومنظومة الاوراطلسية، إلا أن اتساع تأثيرات العامل التكنولوجي في السياسات الدولية،

حيث اختصر الفضاء السيبراني حاجز الزمان والمكان، وخلق مساحات للتفاعلات الداخلية والدولية في الواقع الافتراضي

ان أي بحث او دراسة علمية ولتبلغ مبتغاها وهدفها، لا بد ان تركز على منهج علمي، ولطبيعة الموضوع، اعتمد الباحث على المنهج على (المنهج الوصفي) من خلال قراءة حيثيات الاستراتيجيات المتبعة في مضامير الصراع الروسي ـ الاوراطلسي، كما اعتمد الباحث على (المنهج التحليلي) من اجل الاستواقف على مكامن تركيبة الأدوات السيبرانية المتبعة فيد إدارة الصراع الافتراضي الروسية ـ الاوراطلسية.

المحور الأول:
الجيوسبرانية الروسية والانتقال من التنظير الى الاندفاع

تنطلق عقيد الجيوسيبرانية الروسية من تتبنى موقف اندفاع أكثر حزما على أساس ان لها الرغبة في استهداف أنظمة البنية التحتية الحيوية والسلوك وعمليات التجسس في الفضاء الحيوي الاورواطلسي، حيث تهدف العقيدة الروسية هذه مصالح دول حلف الشمال الأطلسي والذي يمثل بوابة من بوابات الحرب للمنظومة الغربية حيال روسيا، كما ان ارتبط تصاعد الصراع بين روسيا ودور الاورواطلسية بقيادة الولايات المتحدة الامريكية خلال السنوات الماضية باستدعاء متنام لحرب المعلومات كأحد المداخل الهامة للتأثير في مسارات الصراع، ففي خضم التنافس على قيادة النظام تشكل توجه استراتيجي مغاير لدى روسيا له امتداداته التاريخية في الحقبة السوفيتية، هذا التوجه مفاده ان الانتصار في الصراع مع الغرب لن يتحقق بالاعتماد القاصر على الأدوات العسكرية التقليدية، ولكن الامر يتطلب أدوات الحرب الحديثية وغيرها من الأدوات وهو ما يطلق عليه رئيس هيئة الأركان العامة الروسية (فاليري جيراسيموف) نهجاً مختلفا لتحقيق الأهداف السياسية والعسكرية الروسية من خلال الطرق غير المباشرة وغير المتماثلة.

أولاً: دلالات ومفهوم الجيوسيبرانية الروسية

تتبلور العقيد الجيوسيبرانية لروسية من وثيقة وزارة الدفاع الروسية المعنونة (مفهوم الأنشطة الفضائية المعلوماتية للقوات المسلحة الروسية) لتكشف عن الحيز الهام الذي تمثله المعلومات في الاطار الاستراتيجي الروسي، وتبنت الوثيقة تعريف فضاء المعلومات بأنه مجال النشاط المتصل بتشكيل المعلومات ونقلها واستخدامها، بالإضافة الى من ما يطلق عليه عقيدة (جيراسيموف)، وهذه العقيدة تنطوي على مجموعة من الأفكار بشأن الأدوات غير التقليدية في الحروب الراهنة، والتي تتضمن أدوات مختلفة من بينها المعلومات، سواء من خلال الفضاء الإعلامي او الفضاء الالكتروني، واستهداف نقاط الضعف للخصوم وتجنب المواجهة العلنية حتى المراحل النهائية للصراع.

حيث كانت هذه العقيد تعتبر ان تزايد استحضارها في روسيا خلال السنوات الماضية، مع سعي روسيا الحثيث لاستعادة ارثها التقليدي كقوة مؤثرة في النظام الدولي، وما يستلزمه ذلك من توظيف أدوات الحرب السيبرانية وفي هذا السياق، اعتمدت روسيا على عقيدة امن المعلومات في الاتحاد الروسي[1]، وأكدت الوثيقة

(1) سلام الوافي، الحرب الإلكترونية، مظهر من مظاهر عرض القوة، بين روسيا وأمريكا، مركز الوقت للتحليل والاخبار، 2017، مقالة منشورة على شبكة المعلومات الدولية الانترنيت على الرابط التالي
https://www.alwaght.com/ar/News/8293/

على البعد العسكري لمسالة المعلومات كأساس لأمن الدولة، وتحدد أسلحة المعلومات باعتبارها احدى الأدوات لتحقيق الأهداف السياسية، ويدور مضامين هذه العقيدة بالآتي:

1 ـ خلق بنية متسامحة:

ان حرب المعلومات تستهدف خلق بنية متسامحة تجاه المصالح والرؤية الروسية، ولا يتوقف إيجاد مثل هذه البنية على ادارج المعلومات التضليلية في سلسلة صنع السياسات على سبيل الحصر، ولكنه يمكن ان يجري عبر وسائل الاعلام الجماهيري والاجتماعية لأحداث تأثير في اراء وتوجهات الافراد العاديين، ومن ثم جعلهم اكثر تقبلاً وتسامحاً مع الرواية الروسية الرسمية، وبالتالي تخفيف حدة المقاومة لسياسة روسيا حيل منطقة الاورواطلسية[2].

(2) جون سائر، الحرب السيبرانية الجديدة بين روسيا والولايات المتحدة الامريكية، صحيفة الأيام ، 2017/6/5، العدد7686، ص14

2 ـ تقويض القدرة على المواجهة

فالكثير من عمليات حرب المعلومات الروسية وخاصة في ما يتعلق بالقرصنة الالكترونية تضعف من إمكانيات خصوم روسيا وقدرتهم على المواجهة وهو ما يتجلى بشكل كبير في الحرب الروسية الجورجية عام 2008، حيث ان الهجمات السيبرانية التي نفذت في جورجيا بالتزامن مع دخول القوات الروسية افضت الى تعطيل استجابة جورجيا للغزو الروسي، لا سيما مع ما أدت اليه عمليات القرصنة الروسية من اضعاف قنوات التواصل بين الحكومة والجمهور، وإيقاف المعاملات المالي، بالإضافة الى عرقلة انتقال المعلومات حول ما يحدث في مناطق الحرب الى العالم الخارجي.

3 ـ تشويه القوى المناهضة

ووفقاً لهذا الطرح وظفت روسيا المعلومات لتشكيل سرديات ورويات تشوه القوى المناهضة لها، وفي الوقت ذاته تشييد صور إيجابية لحلفائها، فقد ظلت روسيا لسنوات تروج لمقولات ان الثورات الملونة التي شهدتها جورجيا وأوكرانيا كانت نتاجاً لمجموعات من المحرضين المدعومين من الولايات المتحدة الامريكية كجزء من التدخل الخارجي المعتمد في كلا الدولتين من اجل اخراجهما من المدار الروسي، وقد استحضرت روسيا هذا النموذج اثناء الانتخابات التي شهدتها الدول الغربية في السنوات الأخيرة حينما وقفت بجانب تكتلات ومرشحين محسوبين على التيار اليمين المتطرف[3].

(3) وليد سالم، هل بإمكان الولايات المتحدة الإنتصار في حرب إلكترونية ضد روسيا، مركز كاتيون، 2017، مقالة منشورة على شبكة المعلومات الدولية الانترنيت على الرابط التالي
http://katehon.com/ar/article/hl_bmkn_lwlyt_lmthd_lntsr_fy_hrb_lktrwny_dd_rwsy

4 ـ اثارة المشكلات الداخلية

حيث تنطوي حرب المعلومات الروسية على التكريس لأوضاع داخلية مازومة في المجتمعات الغربية، فحينما اثار الاعلام الروسي قضية الفتاة الألمانية من اصل روسي عام 2016، التي ادعت انه تم الاعتداء عليها من قبل رجال لهم ملامح شرق أوسطية، كان يحاول الضغط على الحكومة الألمانية عبر استداء قضية اللاجئين بما تتضمنه من دلالات سلبية ضاغطة في الكثير من المجتمعات الغربية.

5 ـ مواجهة العقوبات الغربية:

فعقب تدخل روسيا في اوركرانيا عام 2014، وضم شبه جزيزرة القرم بعد استفتاء مارس 2014، تزايدات الغزلة الأوروبية المفروضة على روسيا واعتمدت الدول الأوروبية الية للعقوبات ضد روسيا في عام 2014، تتضمن عدداً من الإجراءات كحظر التأشيرات وتجميد الأصول وفرض قيود تجارية واقتصادية، منا تزايدت العقوبات الامريكية المفروضة على روسيا[4].

ثانياً: البنى التأثيرية في الجيوسيبرانية الروسية

تمثل روسية ثقل سيبراني عالمني نظراً لتفوقها في مجال الاتصال والاستخبار الالكترونية وردع الفيبروسات المضادة، حيث تتبوأ وكالة الاستشارات الأمنية زيكوريون الاستشارية في تحليل المعلومات والتي مقرها موسكو المرتبة الأولى في خدمات القرصنة كواحدة من أفضل خمس جيوش سيبرانية في العالم، روسيا زادت تمويل قدرات الإنترنت الدفاعية بعد سلسلة من الهجمات الإلكترونية الأمريكية والإسرائيلية على المواقع النووية الايرانية في عام 2010.

حيث تقدر حجم القوى السيبرانية لروسية خصوصاً الموجهة نحو منطقة الاوروواطلسية ما بين 2000 إلى 1000 موظف، وتنفق وزارة الدفاع الروسية حوالي 500 مليون دولار سنويا على هذه الترتيبات الالكترونية، وبالتالي فان مجالات القوة والتفوق الروسي تندرج نحو التأثير الكبير للدعاية الالكترونية الروسية فضلاً عن عمق التأثير للحرب الالكترونية العسكرية لاعتبارات تتعلق بتفوق الروس في منظومات التشويش والتضليل العسكري، فضلا عن القوة الردعية الروسية في حلق الفيروسات ومنع الاختراقات المضادة، كذلك الإمكانات العالية في مجال الاستخبار والاختراق الالكتروني.

ويمكن تحديد الوسائل الارتكازية للتأثير في العقيد الجيوسيبرانية الروسية بالاتي[5]:

(4) خالد بن شريف، الفضاء السيبراني.. امتداد حرب باردة بين واشنطن وموسكو، مركز تصويت ، 2017، مقالة منشورة على شبكة المعلومات الدولية الانترنيت على الرابط التالي https://www.ultrasawt.com/5445/5463522626/65445/5463522626/6366/

(5) ANDY GREENBERG،How An Entire Nation Became Russia›s Test Lab for Cyberwa، center wired، 2017، Article published on the World Wide Web on the following link https://www.wired.com/story/russian_hackers_attack_ukraine

1 ـ التجسس والاستخبارات الإلكترونية

2 ـ الهجمات الإلكترونية، التي تسبب أذى البنية التحتية لدول الاورواطلسية

3 ـ حروب المعلوماتية في وسائل الإعلام والشبكات الاجتماعية

ثالثاً: البنى العقائدية لجيوسيبرانية الروسية

تختلف الرؤية الاستراتيجية الروسية عن نقيضتها الاورواطلسية في ما يخص العقيدة السيبرانية وسبل توجه أدوات هذه العقيدة نحو العمق التأثيري والموجه للمصالح الروسية، حيث ترى الحرب السيبرانية بشكل مختلف عن نظيراتها الاورواطلسية (المنظومة الغربية)، فروسيا لديها اكثر الطرق استراتيجية لتهجيد ولدمج منظومات الجيل الخامس والتي تشمل الحرب الدعائية الالكترونية ومنظومة الحرب الالكترونية بالإضافة الى منظومة الحرب السيبرانية، وبالتالي تمتلك من السطوة والتأثير من يأهلها من ممارسة السطوة الإلكترونية والتأثير الالكترونية في العمق الاستراتيجي الاورواطلسي من خلال تنظيم وسائل التدخل والتنفذ في عمق القارة الاوربية وفي داخل الحلفاء الاستراتيجيين للولايات المتحدة الامريكية.

اذ يمكن القول ان الاندفاع السيبراني الروسي هو مختلف تماما عن نقيضتها الغربية، حيث ينظر منظرو الفكر السيبراني على ان الندفاع والانغماس السيبراني ينبع من عقيدة الجيوسيبرانية لورسية والتي تتمثل في كيفية استخدام قدرات الاتصال للإنترنت وتنظيم الوسائل الالكتروني من اجل تهجدين الجهد الحربي الالكتروني من اجل تعضيد النهج الروسي للحرب السيبرانية، ومعالجتها سواء من حيث نظريته أو أسسه العملية[6].

1 ـ يعتقد الروس بان روسيا مقفلة جيواستراتيجياً ووجودية والنضال مع القوى الداخلية والخارجية التي تسعى إلى تحدي لها الأمن في مجال المعلومات. الإنترنت، والتدفق الحر لل المعلومات التي يولدها، على حد سواء تهديدا وفرصة في هذا يتعلق.

2 ـ لا يستخدم المنظرون العسكريون الروس عموما مصطلحات حروب الإنترنت أو الحرب الإلكترونية، بدلا من ذلك، فإنها يدركون العمليات السيبرانية في نطاق أوسع يتمثل في إطار حروب المعلومات، وهو مفهوم شامل يشمل امن الحواسيب وعمليات الشبكة، والحرب الإلكترونية، والعمليات النفسية، والاستخبارات الالكترونية[7].

(6) خافيير إسكاليرا، كيف استغلت الاستخبارات الروسية شركات التكنولوجيا لديها في الحرب السيبرانية؟، نون بوست، 2017، مقالة منشورة على شبكة المعلومات الدولية الانترنيت على الرابط التالي https://www.noonpost.org/content/20357

(7) David Batashvil، Russia›s cy_ ber war: past, present,. euobserv_ er center، 2017، Article published on the World Wide Web on the following link https://euobserver.com/opin_ion/136909

3 ـ تمشيا مع المفاهيم السوفياتية التقليدية من محاربة التهديدات المستمرة من في الخارج وفي الداخل، حيث تدرك روسيا ان الصراع داخل مساحة المعلومات أن تكون ثابتة نوعا ما ولا تنتهي، وهذا يشير إلى أن روسيا سوف يكون لديها شريط منخفض نسبيا لاستخدام الانترنت، وهو ما يعتقدوا منظروا الامن السيبراني الغربيون حيث ينظر إليها على أنها ذات طبيعة هجومية وتصاعدية.

4 ـ السيبرانية الهجومية تلعب دورا أكبر في الجيش الروسي التقليدي وربما تلعب دورا في المستقبل في استراتيجية روسيا إطار الردع، على الرغم من أن الجيش الروسي كان بطيئا في احتضان السيبرانية لأسباب هيكلية وعقائدية على حد سواء، حيث تؤكد الدراسات الغربية ان روسيا في صدد تعزيز تعتزم القدرات السيبرانية الهجومية وكذلك القدرات السيبرانية الدفاعية، من اجل تعضيد القوة التقليدية خصوصاً في الجناح الشرقي لاوروبا من اجل ممارسة التنفذ واسترجاع استراتيجية الذات الروسية المفتقدة.

5 ـ كما يمكن القول ان تجارب الحرب في جورجيا وأوكرانيا والتي اتاحت فرصة كبيرة لروسيا من اجل سقل وتعديل تكتيكاتها الالكترونية من اجل إعادة التموضع ووخفض مستوى الإخفاقات في مجال الحرب السيبرانية، وصولاً الى اثبات ذاتها وقدراتها على الساحة العالمية، ويمكن أن تكون هذه المظاهرات في وقت لاحق بمثابة أساس لإشارة أو ردع خصوم روسيا[8].

واخيراً يمكن القول ان حرب المعلومات مثلت احد مسارات الاستجابة الروسية لهذه العزلة لما يمكن ان تلحقه من خسائر بالمجتمعات الغربية، ولذا فان احد التفسيرات التي طرحت لعملية القرصنة التي تعرض لها الحزب الديمقراطي اثناء الانتخابات الرئاسية الامريكية عام 2016، كانت تصوير القرصنة على انها ثار من الحزب الذي وسع حزمة العقوبات الاقتصادية المفروضة على روسيا.

(8) Michael Connell & Sarah Vogler، Russia›s Approach to Cyber Warfare، realcleardefense، 2017، Article published on the World Wide Web on the following link https://www.realcleardefense.com/articles/2017/05/09/russias_approach_to_cyber_warfare_111338.html

المحور الثاني:
مضامين عقيدة التالين في الاستراتيجية الاوراطلسية

تبنى الناتو منذ نشأته استراتيجية الردع والاحتواء ذات المضمون العسكري حيال القضايا المحيطة به خصوصا في مواجهة الاتحاد السوفيتي سابقاُ، وبعد تفكك الاخير وما نجم من تغييرات استراتيجية عصفت بشكل دوائر السياسة الدولية، بالإضافة الى التحولات الكبرى التي شابت العلاقات الدولية نتيجة التطورات

التقنية والاعلامية، حيث تبنى حلف شمال الأطلسي الناتو استراتيجية بإسم " تالين»[9] مكونة من 282 صفحة، والتي تتضمن الرؤى والأساليب والتكتيكات التي يتبنها لموجهة الحروب الالكترونية وتنظيم قواعد الاشتباك عبر الإنترنت، ويُذكر أن مسؤولين عسكريين أمريكيين ذكروا قلقهم ومخاوفهم من هجمات الكترونية مستمرة تتعرض لها الولايات المتحدة ومنشئاتها الحساسة وإعلامها وبنيتها التحتية وخاصة من قبل الصين، حيث يؤكد حلف شمال الأطلسي أن الحرب الالكترونية أصبحت سلاحاً حاله كحال السلاح الحربي، كما تعطي استراتيجية " تالين" الحق للدولة التي تتعرض لهجوم الكتروني شن حرب هجومية الكترونية مضادة على الدولة الأخرى، كما تؤكد استراتيجية "تالين" أنه يمكن استخدام القوة العسكرية الحقيقة في حالة تم شن هجوم الكتروني على دولة وأدى هذا الهجوم لخسائر بالأرواح البشرية[10].

(9) مدينة تالينTallinn عاصمة جمهورية إستونيا ومركزها الإداري مقاطعة هاريو وأكبر مدن البلاد وهي أقدم عاصمة في شمال أوروبا، وتعرف أيضاً باسمها القديم رفال Reval من القرن الثالث عشر حتى عام 1917، تحتل مساحة المدينة 159.2 كم 2 ويبلغ عدد سكانها، ويقع على الساحل الشمالي من البلاد، على شاطئ خليج فنلندا وعلى بعد 80 كم إلى الجنوب من عاصمة فنلندا هلسنكي، شرق ستوكهولم وغرب سانت بطرسبرغ.

(10) Cyberwar ـ does it exist, nato.int. 2017 https://www.nato.int/docu/review/2013/Cyber/Cyberwar_does_it_exist/EN/index.htm

اولاً: دلالات الاستراتيجية الجديدة

كما اتجهت دول حلف الشمال الاطلسي الى تبني استراتيجية سيبرانية ذات بعد استخباراتي، فبعد أحداث أوسيتا الجنوبية وتبني روسيا استراتيجية دولية تهدف إلى كسر الأحادية الدولية والتفرد بالقرار الدولي، انطلقت شرارة الحرب الهجينة، خوصا من الجانب الغربي والذي بدء بتحشيد الامكانيات الاعلامية والرقمية المهجنة الكبيرة من أجل تحريك الرأي العام الدولي ضد السياسات الروسية العالمية وبالخصوص في منطقة شرق أوروبا ووسطها، حيث تحرك الناتو نحو تبني استراتيجية رقمية مهجنة يتم تنفيذها بواسطة مركز الاتصالات الاستراتيجي والذي تم إنشاؤه في بداية عام 2017، ويعمل المركز بتمويل من الناتو، وتم التوقيع عليه من قبل كلاً من استونيا وألمانيا وإيطاليا ولاتفيا وليتوانيا وبولندا وهولندا والمملكة المتحدة و فنلندا والسويد وفرنسا.

يتعرض حلف شمال الأطلسي لما يقارب 500 هجوم سيبراني شهريا، حيث تحدث المدير العام لوكالة الاتصالات و المعلومات التابعة للناتو (كيفن شيد) في مؤتمر وكالة الدفاع الأوروبية عام 2017 الذي عقد في العاصمة البلجيكية بروكسل حول نشاطات الحلف في مجال الدفاع السيبراني، و أكد على ان تقاسم المعلومات هي النقطة الأهم لتنمية قدرات الدول في الفضاء السيبراني، مشيرا الى تثمينهم للتعاون بين الناتو و الاتحاد الأوروبي في هذا المجال، شبه (كيفن شيد) الهجمات السيبرانية بالتسونامي، مؤكدا على الأهمية الكبرى لأنظمة الانذار المبكر في مجال

الحرب السيبرانية، حيث تتعرض شبكات حلف شمال الأطلسي لما يقارب 500 هجوم سيبراني شهريا دون للاشارة الى الجهة المهاجمة، ويعتبر الناتو الفضاء السيبراني بمثابة فضاء عسكري فضلا عن الجو والبر والبحر[11].

(11) Cyber Security, republic of Estonia ministry of foreign affairs, 2017 http://vm.ee/en/cyber_security&prev=search

يساهم مركز الاتصالات الاستراتيجي، الذي يوجد مقره في ريغا، لاتفيا، شرق اوروبا، بتحسين قدرات الاتصالات الاستراتيجية الاستخباراتية الهجينة داخل الناتو والدول المتحالفة معه، إذ يشكل الاتصال الاستراتيجي جزءا لا يتجزأ من الجهود الرامية إلى تحقيق الأهداف السياسية والعسكرية للناتو والتي في طليعتها صد النفوذ السيبراني لروسيا بكل أشكاله عن منطقة شرق ووسط أوروبا، وتتمحور أهداف المركز حول المساهمة في عمليات اتصالات الناتو من خلال توفير تحليلات الاستخبارات الشاملة، وتقديم المشورة في الدعم التكتيكي، فهو إذا قوة استخباراتية بنيت من قبل المشاركين متعددي الجنسيات عبر قطاعات مدنية وعسكرية وأكاديمية متجانسة في ما بينها من أجل تسخير التكنولوجيات الحديثة، والأدوات الافتراضية للتحليلات الاستخباراتية، الأدوات التكتيكلية والادور لعقيدة الدافاع المشترك التالين

ثانياً: الأسس وتكتيكات استراتيجية تالين

بالإضافة الى تكثيف جهود الاعضاء على مبدأ (الاتصالات الاستراتيجية) والذي يدور معناها التكتيكي حول[12]:

(12) NATO and Cyber Defence, natolibguides.info, 2017 http://www.natolibguides.info/cybersecurity

1 ـ تعزيز مبدأ الاتصالات الاستراتيجي للناتو: أولى اهتمامات مركز الاتصالات الاستراتيجي هو تقويم وترميم الاتصالات السياسية والاستخباراتية بين دول الحلف والتي باتت تعاني من ترهل وبرود في الاتصال نتيجة الاختلاف في المواقف السياسية وتباعد الروئ الاستراتيجية وهذا ما انعكس على البيئة الهيكيلة للحلف.

2 ـ موجهة الاعلام السيبراني الروسي: يعمل المركز على تتبع وصد وكالة سبوتنيك الروسية الناطقة بـواحد وثلاثون لغة حيث يتهم الناتو هذه الوكالة بأثارة الدعاية المضادة لدول الناتو، كذلك تفعيل دور الإعلامي السيبراني الغربي المضاد نحو الداخل الروسي من أجل إحداث تأثير على التوجهات الروسية الاقليمية منها والعالمية.

3 ـ تنظيم منصة استخباراتية ببعد سيبراني: تطور مفهوم الاستخبارات عن ما كان عليه في العقد السابق حيث اتجهت اليوم الى استخدام أساليب الرقمنه والاتصالات

النانوية، ومن خلال مركز الاتصالات الاستراتيجي الذي يقبع في لاتفيا في شرق اوروبا يتيح لدول الناتو تكثيف منظومات الاتصال والاستخبار على الجانب الروسي.

4 ـ فرض السيطرة السيبرانية على منطقة شرق اوروبا: يتجه مركز الاتصالات الاستراتيجية على فرض جدار الإكتروني ضد الفضاء السيبراني الروسي والذي بدأ يشكل تهديدا حقيقيا على المصالح السيبرانية لدور الناتو، وبالتالي اتجهت دول الناتو نحو تفعيل خدمات المركز من خلال الرصد السيبراني الاعلامي والاستخباراتي وتكثيف التعاون والتواصل الدعائي لدول الناتو[13].

(13) Tallinn Paper: The Law of Cyber Targeting, ccdcoe.org, 2017 https://ccdcoe.org/multimedia/tallinn_paper_law_cyber_targeting.html

5 ـ ادارة منظومة السيطرة الدعائية السيبرانية: من اولويات مركز الاتصالات الاستراتيجي هي تقوية منظومة الدعاية الموجهة والمضادة للوجود الروسي في شرق اوروبا خصوصا في دول حوض البلطيق والتي تعد بوابة الصراع المتقدم لأوروبا وروسيا خصوصاً أن هذه المنطقة باتت تتصاعد بها تيارات مناهضة لدور الناتو في القارة الاوروبية.

6 ـ رصد واستخبار القدرات العسكرية الروسية: إن من سلم اهتمامات المركز هي استحضار القدرات الاستخباراتية حيال روسيا خصوصاً الاستخبارات العسكرية من أجل رصد القدرات العسكرية المتصاعدة في مجال الصواريخ الاستراتيجية ومنظومة الدرع الصاروخ.

واخيراً يمكن القول إن الناتو قد استحدث منظومة جديدة من الوسائل الهجينة لمواجهة الوجود الروسي في القارة الاوروبية من خلال مركز الاتصالات الاستراتيجي والذي تتنوع وسائل عمله ما بين الوسائل الدبلوماسية والاعلامية والدعائية والسيبرانية والاستخباراتية، كل هذه الوسائل أنتجت جيل جديد من الموجة الشرقية والغربية نتيجة منعطفات التغيير الدولي ومنعكسات السياسية الدولية والتي القت بظلالها على طبيعة الصراع والتنافس في القارة الاوربية.

المحور الثالث:
مضامير الاشتباك والتناحر الرقمي الأورو ـ روسية

يمكن القول ان المنطقة المحصورة من الحدود الغربية لروسيا وصولاً الى ضفاف الأطلسي هي بمثابة مجال حيوي جيوسيبراني، ينشط فيه مضامير الصراع والحرب السيبرانية بين روسيا من جهة والقوى الغربية والولايات المتحدة من جهة أخرى المنضوية تحت منظومة الناتو، حيث تدفع روسيا باستخدام وسائل وتكتيكات رائدة في مجال حرب المعلومات والدعائية الافتراضية وهو ما أعطاها قدرة يمكن وصفها

بالتفوقية على الجانب الأخرى والذي بدا يغلب عليه عامل عدم الاتزان والارباك السيبراني.

وتشمل الحرب السيبرانية التي تقوم بها روسيا هجمات الحرمان من الخدمة، وهجمات القراصنة، ونشر المعلومات المضللة والدعاية، ومشاركة الفرق التي ترعاها الدولة في المدونات السياسية، ومراقبة الإنترنت باستخدام تقنية سورم، واضطهاد المعارضين السيبرانيين، وغير ذلك من التدابير السيبرانية، حيث يتم تنسيق جميع هذه الأنشطة من قبل أجهزة الاستخبارات الروسية التي هي جزء من قسم كب 16، كما وصف الصحافي الاميركي بيت ايرلي في مقابلاته مع ضابط الاستخبارات الروسي المنشق سيرغي تريتياكوف القدرات الاختراقية في مجال التجسس السيبراني لروسيا من خلال قدرة الاستخبارات الروسية الوصول إلى شبكات الانترنيت الإعلامي لدولة المستهدفة دون علم أجهزة الاستخبارات تلك الدولة، من خلال نشر الدعاية على مواقعها الوطنية وارسال رسائل إلكترونية ومنشورات إعلامية مضادة ومضللة، بالإضافة الى الدعاية المقنعة كتقارير تعليمية أو علمية، حيث تم اختراق المواقع الأكثر ملاءمة لتوزيع التضليل السيبراني، وانطلقاً من هذه الوسائل والقدرات يمكن التطرق الى اهم حلقات الاشتباك والصراع السيبراني بين روسيا والمنظومة الغربية وبالاتي:

اولاً: دوائر الصراع والحرب السيبرانية الروسية على جورجيا عام 2008

وفيما يتعلق بالهجمات الإلكترونية على جورجيا في عام 2008، ذكر تقرير مستقل أصدرته الولايات المتحدة في معهد أبحاث الولايات المتحدة الأمريكية بشأن العواقب السيبرانية، حيث أشار الى أن الهجمات كانت مشاركة مباشرة من قبل أجهزة الاستخبارات الروسية السيبرانية، كما اكد التقرير على ان عدة هجمات كان مصدرها من أجهزة حاسوبية تابعة لمستخدمين موجودين في روسيا وأوكرانيا ولاتفيا وكان هؤلاء العملاء السيبرانيين يشاركون في هذه الهجمات بضراوة من خلال ضرب منظومات المؤسسات المالية والإعلامية التابعة لجورجيا، خلال حرب أوسيتيا الجنوبية عام 2008 [14].

(14) رؤوف بوناب، هذه استراتيجيات بوتين الستة للتأثير على الانتخابات الألمانية، مركز العربي 24، 2017، مقالة منشورة على شبكة المعلومات الدولية الانترنيت على الرابط التالي https://arabi21.com/sto_/ry/1031745

ثانياً: اثر التهديدات السيبراني على نتائج الانتخابات الرئاسية الأوكرانية عام 2014

أطلق القراصنة الموالية لروسيا سلسلة من الهجمات الإلكترونية على مدى عدة أيام لتعطيل الانتخابات الرئاسية الأوكرانية في مايو 2014، كما عملوا على الإفراج عن

رسائل البريد الإلكتروني المخترقة، بالإضافة الى محاولة تغيير حصص التصويت، وتأخير النتيجة النهائية للانتخابات، كما اطلقت روسية برامج الخبيثة كانت ستعرض رسما بيانيا يعلن فيه المرشح اليميني المتطرف دميترو ياروش، تمت إزالة الفائز الانتخابي من لجنة الانتخابات المركزية في أوكرانيا قبل أقل من ساعة من إغلاق الاقتراع، على الرغم من ذلك، ذكرت القناة الأولى في روسيا ياروش قد فاز وبث الرسم المزيف، مستشهدا بموقع اللجنة الانتخابية، حيث ان هذه النتائج المزيفة موجهة إلى جمهور معين من أجل تغذية الرواية الروسية التي ادعت منذ البداية أن المتطرفين الوطنيين والنازيين كانوا وراء الثورة في أوكرانيا[15].

(15) ليوبوف ستيبوشوفا، روسيا تؤثر على مصير انتخابات 24 بلدًا في العالم، مركز نون بوست، 2017، مقال منشورة على شبكة المعلومات الدولية الانترنيت على الرابط التالي http://www.noonpost.org/content/16194

ثالثاً: الحرب السيبرانية الروسية على المانيا

بادرات روسيا بتنظيم هجمات إلكترونية ضد أحزاب ومؤسسات سياسية ألمانية، بغية إضعافها قبيل الانتخابات، من خلال تسريب وثائق سرية، مثل تلك التي تمت سرقتها من البرلمان في عملية قرصنة كبرى تعرض لها في سنة 2015، ويعتقد أن فريقا من القراصنة يدعى «سوفاسي» يقف وراء تلك العملية، ومن المرجح أنهم ينتمون إلى المخابرات الروسية.

أن المانيا أصبحت في حالة من الإرباك إزاء حملات الداعاية الالكترونية التي قامت بها روسيا وفي هذا الإطار، كما اكدت الحكومية ألمانية على أن الحكومة الروسية تشن حملات إعلامية عبر قناتها الرسمية «روسيا اليوم» وموقع «سبوتنيك» الإخباري، فضلا عن توظيف أساليب ساخرة في مواقع التواصل الاجتماعي، لنشر دعايتها فيما يتعلق بالانتخابات الألمانية.[16]

(16) حسام عدنان، المخابرات الألمانية تحذّر من تزايد نفوذ روسيا في أوروبا، صجيفة الخليج اون لاين، 2017، مقالة منشورة على شبكة المعلومات الدولية الانترنيت على الرابط التالي https://www.noonpost.org/content/15624

وكان الهدف من هذه الحملات الدعائية موجهة بدرجة أولى إلى الناخبين الألمان الذين يتكلمون الروسية، والذين يبلغ عددهم حوالي 3 ملايين، فضلا عن ذلك، تستهدف هذه الحملة الناخبين القوميين والمحافظين، على غرار أنصار حزب «البديل من أجل ألمانيا» اليميني المتطرف.[17]

(17) حميد شكري، تأثير موسكو على الانتخابات الألمانية: حقيقة أم لعبة انتخابية، صحيفة الخرب اليومية، 2017، مقالة منشورة على شبكة المعلومات الدولية الانترنيت على الرابط التالي https://www.alarab.co.uk/article/morenews/117721

خيرا الأمثلة على هذه الحملات الدعائية وعمليات التلاعب بالرأي العام، وتتمثل هذه الحادثة في قضية الفتاة ليزا، التي جدت في عام 2016، حيث تواترت قصة مفادها أن فتاة روسية عمرها 13 سنة تعرضت للاختطاف والاغتصاب على يد مجموعة من اللاجئين في ألمانيا.[18]

(18) حسام عدنان، مصدر شبق ذكره، الانترنيت

آنذاك، اتهمت وسائل الإعلام الروسية ألمانيا بإخفاء القصة، والتستر على جنسية الضحية، من جانبه، أدلى وزير الخارجية الروسي سيرغي لافروف بدلوه في القضية،

وطالب الجانب الألماني بتقديم توضيحات، كما خرجت مظاهرات احتجاجية في ألمانيا، على الرغم من أن الأبحاث أظهرت في النهاية أن القصة برمتها تم اختلاقها، ودفع ذلك الحكومة الألمانية للاحتجاج لدى نظيرتها الروسية، ومطالبتها بالتوقف عن بث الدعايات السياسية.[19]

(19) حميد شكري، مصدر شبق ذكره، الانترنيت

كما أن حزب «البديل من أجل ألمانيا» قد يكون إحدى الوسائل التي قد تلجأ لها روسيا، بهدف التأثير على السياسات الألمانية، حيث تشبه أفكار أنصار هذا الحزب من القوميين المتطرفين والمحافظين إلى حد كبير توجهات أنصار الرئيس بوتين في روسيا.

وتظهر العلاقة بين الطرفين من خلال البرنامج الانتخابي الذي يتبناه حزب «البديل من أجل ألمانيا»، فقد أعرب هذا الحزب عن رفضه للعقوبات الاقتصادية المسلطة على روسيا، في حين يعتبر أن ما تقوم به روسيا من خلال ضم شبه جزيرة القرم يعد أمرا قانونيا، بعلّة أن هذه المنطقة في نظرهم كانت دائما تابعة لروسيا.

كما تتجه روسيا نحو ورقة أخرى للتأثير على الأجواء السياسية في ألمانيا، ألا وهي المناورات العسكرية التي يعتزم تنفيذها في هذا الشهر، تحت اسم «زاباد 2017»، والتي تمثل أكبر مناورات مشتركة بين روسيا وبيلاروسيا منذ نهاية الحرب الباردة، وعموما، ستدور هذه المناورات التي سيشارك فيها حوالي 100 ألف جندي روسي بين 14 و20، ومن المثير للاهتمام أن هذه المناورات أثارت حفيظة حلف الناتو، على خلفية اتساع مداها، وغموض النوايا الحقيقة من ورائها، في ظل مخاوف من أن يتجاوز الأمر مجرد القيام بمناورات عسكرية، ويتحول إلى تحرك حقيقي، أو استعداد لأمر ما.[20]

(20) ليوبوف ستيبوشوفا، مصدر شبق ذكره، الانترنيت

وفي هذا الصدد، وصف قائد القوات الأمريكية في أوروبا، فريديريك هودجس، الأمر بأنه شبيه «بحصان طروادة»، وذلك بهدف إدخال تغييرات تكتيكية على تمركز واستعدادات القوات الروسي، وفي الختام، ان مثل هذه التحركات العسكرية قبل أيام قليلة من الانتخابات الألمانية قد سببت احراج سياسي في أوروبا، خصوصاً لبعض المرشحين، على غرار أنجيلا ميركل.

رابعاً: اثر التهديدات السيبراني على نتائج استفتاء المملكة المتحدة «خروج بريطانيا من الاتحاد الأوروبي»

في الفترة التي سبقت الاستفتاء على المملكة المتحدة الخروج من الاتحاد الأوروبي، اقترح رئيس الوزراء ديفيد كاميرون أن روسيا «قد تكون سعيدة» مع

تصويت إيجابي على خروج بريطانيا من الاتحاد الأوروبـي، في حين اتهمت الحملة المتبقية الكرملين بدعم سرا تصويت إيجابي بخروج بريطانيا من الاتحاد الأوروبي في عام 2016، ادعى نائب البرلمان بن برادشو في البرلمان أن روسيا تدخلت في حملة الاستفتاء على خروج بريطانيا من الاتحاد الأوروبي، وفي عام 2017، أصدرت لجنة الإدارة العامة والشؤون الدستورية التابعة لمجلس العموم تقريرا يشير إلى انهيار موقع تسجيل الناخبين الحكومي في يونيو / حزيران 2016 قبل أقل من ساعتين من الموعد النهائي للتسجيل المقرر أصلا (والذي كان ثم مددت)، يشير الى دور الاستخبارات السيبرانية الروسية في هذا الفعل، كما كشف التقرير دور الاستخبارات الروسية في انشاء وتمويل حركة الدعائية الالكتروني التي تحث الناخبين للتصويت بنعم للخروج من الاتحاد الأوربي.

خامساً: اثر التهديدات السيبرانية على نتائج الانتخابات الامريكية

تشير الكثير من التقارير والدراسة على ان للروس دور كبير ومؤثر في نتائج الانتخابات الامريكية، فعلى سبيل المثل كان الدور الروسي واضح من خلال الإفصاح عن المراسلات الالكترونية السرية لمشرح حزب الديموقراطي هيلري كلنتون والذي اثرت بشكل كبير على نتائج الانتخابات الامريكية آنذاك.

حيث اكدت شركة فيسبوك، أن بعض الإعلانات التي اشتراها الروس على فيسبوك في العام الماضي روجت لمناسبات مختلفة خلال حملة الانتخابات الرئاسة الأمريكية مما يشير إلى أن التدخل المزعوم قبل الانتخابات، وأعلنت وسائل الإعلام الأمريكية، في وقت سابق، أن وفقاً لبيانات شركة فيسبوك، قامت «بوتات انترنت» روسية أثناء السباق الرئاسي الأمريكي بشراء ساحات إعلان في هذه الشبكة الاجتماعية بهدف التأثير على نتائج الانتخابات.

بينما أكد الشركة الأمريكية المتخصصة في مجال الإعلان المرتبط بخدمات البحث على الإنترنت «غوغل» الأسبوع الماضي، أنه ليس لديها أي دليل على منصاتها الإعلانية يفيد بوجود حملة دعائية روسية على عكس ما تقول مؤسسة فيسبوك إن حملات إعلامية روسية ظهرت على شبكتها قبل وبعد انتخابات الرئاسة الأمريكية العام الماضي[21]، وصرح المتحدث الصحفي باسم الرئيس الروسي، دميتري بيسكوف، الخميس في الـ6 من الشهر الجاري، بأن الكرملين ليس على بمزاعم قيام برامج حاسوبية من روسيا بشراء ساحات الإعلان في «فيسبوك» من أجل التأثير على الانتخابات الأمريكية.

(21) حسام ياسر، فيسبوك: إعلانات روسية أثرت على نتائج الانتخابات الأمريكية، وكالة سبوتنيك الروسية، 2017، مقال منشورة على شبكة المعلومات الدولية الانترنيت على الرابط التالي
https://arabic.sputniknews.com/world/201709131026157443

الخاتمــة

لذلك، تطرقنا في هذا المضمار صيغة ارتــدادات الحرب السيبرانية الروسية على مجريات الاحداث في المنطقة الاوراطلسية والتي تمدد من حدود أوروبا الشرقية الى ضفاف الولايات المتحدة نحو الأطلسي، لكافة اشكال هذه الحرب والتي اتخذت من الداعية الالكترونية محوراً لها في بعض الأحيان كما اتخذت من سرقت المعلومات وتضليل العدو تكتيك أخرى للتأثير السيبراني فضلاً عن التاثير الالكتروني على مجريات الواقع السياسي الداخلي لبعض الدول مثل التدخل الروسي في الانتخابات الأوكرانية والمانية وصولاً الى التدخل الروسي في الانتخابات الامريكية والتي تمثل ضربة قاضية لمنظومة الامن والسيطرة الأطلسية، وبالتالي رسمت هذه التدخلات ومنحنيات الحروب الإلكترونية شكل جديدة لدوائر التفاعل والصراع في وسط القارة الاوربية.