الصفحة الرئيسية للمجلة: www.asjp.cerist.dz/en/PresentationRevue/796 PISSN : 2477-9970 - EISSN : 2822-1540

الإستراتيجية الروسية في الحرب السيبرانية:
قراءة في نموذج الصراع السيبراني الروسي مع بعض الدول

Russian strategy in cyber warfare:
Read the model of Russian cyber conflict with some countries

ط.د. شريطي أسامة *
جامعة العربي التبسي، تبسة
(الجزائر)
oussama.cherite@univ-tebessa.dz

أ. بن عزوز حاتم
جامعة العربي التبسي، تبسة
(الجزائر)
hatem.benazouz@univ-tebessa.dz

ملخص:

تهدف هذه المداخلة إلى الوقوف على نماذج عالمية من الحروب السيبرانية بين الدول حيث تعد الحروب السيبرانية من الأساليب الحالية المعتمدة في مواجهة بين ا لدول لحماية أمنها القومي حيث أن تطور الدولة يتوقف على مدى امتلاكها للتطور التكنولوجي و استخدماها في مجال الدفاع عن نفسها فالنمط التقليدي للحروب أصبح من الاستراتيجيات القديمة في المجتمع الحالي فالدول المتقدمة ألغت كل التكتيكات العسكرية في مجال حماية أمنها القومي وذلك نظرا للخسائر المادية والبشرية التي تسببها الحملات العسكرية فوجدت البديل في ذلك ألا وهو استخدام البرامج و الحملات الالكترونية في حروبها ضد الدول وقد شهد العالم العديد من الحملات الالكترونية الحربية بين الدول وذلك من خلال الاطلاع على خصوصية البرامج الحكومية و اختراقها سواء كان ذلك في الجانب السياسي او الاقتصادي او الاجتماعي وقد تعددت النماذج العالمية في تلك الحروب و نذكر من بينها الحرب السيبرانية التي تبنتها روسيا ضد الدول و منه تتطرق هذه المداخلة الى التعرف على الإستراتيجية الروسية في الحرب السيبرانية و ذلك من خلال تقديم قراءة حول أهم الحروب التي خاذتها روسيا ضد هذه الدول

الكلمات المفتاحية: الحروب السيبرانية؛ الغزو الالكتروني؛ الأمن السيبراني؛ برامج الحماية.

***

* المؤلف المرسل: ط.د. شريطي أسامة

Abstract:

This intervention aims to identify global models of cyber wars between countries, where cyber wars are one of the current methods adopted in a confrontation between countries to protect their national security, as the development of the state depends on the extent to which it possesses technological development and used it in the field of self-defense. The traditional pattern of wars has become Among the old strategies in the current society, the developed countries abolished all military tactics in the field of protecting their national security, due to the material and human losses caused by military campaigns, and found the alternative in that, which is the use of electronic programs and campaigns in their wars against countries, and the world has witnessed many electronic warfare campaigns Between countries, by looking at the privacy of government programs and their penetration, whether in the political, economic or social aspect. There are many global models in those wars, and we mention among them the cyber war that Russia adopted against countries, and from this intervention deals with the identification of the strategy The Russian in the cyber war, by providing a reading about the most important wars that Russia took against these countries.

Keywords*: cyberwars; cyber-invasion; protection programs.*

المقدمة:

يشهد العالم اليوم تطورات كبيرة في مجال تكنولوجيات الإعلام الآلي وتم إدخال هذه التكنولوجيات في الأشغال العامة للدولة من خلال رقمنه كل المواقع الحكومية الهامة التي تعتبر كشريان حياة لهاته الدول و كتدعيم لهاته المواقع يتم استخدام برامج حماية خاصة بهاته المواقع بغية حماية خصوصيتها و خصوصية الدولة في المجال الاقتصادي و السياسي و غالبا ما يتم استهداف هاته المواقع من قبل الدول الأعداء حيث تصبح في هذه الحرب معادلة دولة مستهدفة ضد دولة مستقوية حيث إن هذا الاستهداف هدفه شل المواقع الحكومية بغية السيطرة على الوضع الاقتصادي و السياسي للبلد المستهدف حتى يسهل السيطرة عليه و هي بمثابة وسيلة ثانوية إلى جانب الحروب التقليدية. وفي الغالب إن هاته الحروب يقودها مختصين في هذا المجال يتميزون بالقدرة و الحنكة الكافية في تحكم في برامج و الالكترونيات التي تخدم هذا النوع من الحروب مستعينين في ذلك من الدعم الحكومي للدولة المستقوية. فالعالم مليء بالأمثلة على هاته الحروب المستحدثة حيث انه في عام (2015) اكتشفت" شركة LAST PASS نشاطا غير معتادا على شبكيتها حيث تبين أن مجموعة من المهاجمين قد سرقوا عناوين البريد الالكتروني للمستخدمين و رسائل التذكير الخاصة بكلمات المرور و في مثال أخر تعرض البيانات الشخصية الحساسة الخاصة ب 147 من عملاء شركة " EQUIFAX" الائتمانية في الولايات المتحدة الأمريكية للخطر من قبل مجرمي الانترنت[01].

-**الإشكالية :** الحرب السيبرانية من نماذج الحروب الجديدة التي لاقت رواجا كبيرا في عصرنا الحالي حيث شغل هذا نوع من الحروب عقول الساسة و صناع القرار حول دول العالم نظرا للتأثير الهائل و الصامت لهذا النوع من الحروب بالإضافة إلى صعوبة الإثبات الجنائي لها ومنه يتمحور التساؤل الرئيسي لهذه الدراسة حول فيما تتمثل اهم النماذج

-**مخطط الدراسة :** حيث تم تقسيم الدراسة إلى محورين أساسيين حيث تمثل المحول الأول في عرض تعريف موجز لمفهوم الحرب السيبرانية بالإضافة إلى أهم الأدوات المستخدمة فيها و أخيرا مبادئ هذا النوع من الحروب أما المحور الثاني فتم عرض فيه نموذج الروسي في الحروب السيبرانية و ذلك من خلال التطرق إلى الإستراتيجية الروسية في الحروب السيبرانية بالإضافة إلى أهم المؤسسات التي من شانها خوذ هذه الحروب و أخيرا عرض نماذج حروب للدولة الروسية ضد دول العالم.

1.تعريف الحروب السيبرانية :

لم تعد الحروب تقتصر على استخدام الأسلحة الفتاكة التي تحملها الطائرات او المدرعات فهذه توشك أن تتوارى في المستقبل وراء ظل حروب ربما تكون أكثر فتكا و هي الحروب الالكترونية.

-مفهوم الحرب السيبرانية CAYBER WARFARE:حيث عرفت وزارة الدفاع الأمريكية الحرب السيبرانية بأنها توظيف القدرات السيبرانية حيث يكون الغرض الأساسي هو تحقيق الأهداف او الآثار العسكرية في الفضاء السبيراني او من خلاله و يضيف تقرير خدمة أبحاث الكونغرس لعام (2001) يمكن استخدام مصطلح الحرب السيبرانية لوصف الجوانب المختلفة للدفاع و مهاجمة شبكة المعلومات و الحواسيب في الفضاء السبيراني فضلا عن حرمان الخصم من القدرة على فعل الشيء نفسه.

ووفقا للقرار نفسه الصادر عن مجلس الأمن الدولي مؤخرا الحرب السيبرانية هي استخدام أجهزة الحاسوب او الوسائل الرقمية من قبل الحكومة او بمعرفة او موافقة صريحة من تلك الحكومة ضد دوال أخرى او ملكية خاصة داخل دولة أخرى بما في ذلك الوصول المتعمد او اعتراض البيانات او تدمير البنية التحتية الرقمية و إنتاج و توزيع الأجهزة التي يمكن استخدامها لتخريب النشاط المحلي[02].

2.مبادئ إدارة الحرب السيبرانية :

1.2. عدم وجود قيود جسدية : في الحرب يجب على القوات البحرية أن تسافر عبر المحيطات و يجب على القوات البرية التنقل عبر التضاريس وهذا لا ينطبق على الحرب السيبرانية حيث انه يمكن شن هجوم في أي مكان و بنفس التأثير و هذا الرأي له بعض الحجج المضادة ومع ذلك يمكن القول انه لا يزال هناك بعض الحدود الفيزيولوجية تماما كما يجب الجندي العادي فان الهجوم السبيراني ينتقل عبر الكابلات المادية.

2.2. التأثيرات الحركية : الهدف من الحرب السيبرانية هو إحداث تأثيرات حركية هذا يتضمن الضرر المادي و ببساطة التأثير على القرار.

3.2. الخلسة : يختلف التخفي في الحرب الالكترونية في التخفي عن الحرب العادية أثناء التمويه و الدروع المضادة و التسلل التقليدي و يركز التسلل الالكتروني بين حركة المرور المشروعة هذا المبدأ يمس مفهوم الغدر.

4.2. قابلية التغيير وعدم الاتساق : و يعكس هذا وجهة نظر "براكس" ودوجان" بأن مجال الانترنت لا يمكن التنبؤ به بينما الرصاص تطير في واقع معين قد لا يعمل المجال الالكتروني بنفس الطريقة نظرا لجميع عوامل البرامج و الأجهزة المعينة.

5.2.الهوية و الامتيازات : الهدف الأساسي للمهاجم الالكتروني هو انتحال الهوية لشخص لديه الحق في الوصول للمطلوب لإحداث الضرر حيث تهدف عملية الاكتشاف السابقة إلى الوصول إلى الجذر و الهندسة الاجتماعية و هي مصممة لجمع كلمات المرور للمستخدمين المتميزين.

6.2. الاستخدام الثنائي: جميع أدوات الحرب السيبرانية ذات استخدام مزدوج حيث تشتمل على كل من الحرب و الاستخدامات السلمية هذا على عكس الحرب الحركية حيث الأدوات بشكل عام تستخدم مرة واحدة.

7.2. مراقبة البنية التحتية: جزء كبير من الحروب السيبرانية هو التحكم في البنية التحتية مجموعتان في حالة حرب في الفضاء السبيراني سوف تسيطر فقط على عدد محدود حيث أن الحصول على السيطرة المباشرة على البنية التحتية سيجلب مزايا [(03)].

3.أدوات الحرب السيبرانية:

هي رموز الحاسوب مصممة لاستخدامها بهدف تهديد او إلحاق الضرر جسدي او وظيفي او تقني بالهياكل او الأنظمة او حتى الأشخاص و الأسلحة و هذا ما ذهب إليه ريد بقوله هي أدوات لإلحاق الضرر و تعتمد الحرب السيبرانية بصفة عامة على الأجهزة و البرامج.

-الأجهزة: و هي الأدوات الميكانيكية و المغناطيسية و الالكترونية و الكهربائية التي تشتمل على نظام الحاسوب مثل وحدة المعالجة المركزية او محرك الأقراص او لوحة المفاتيح او الشاشة كما تعتبر الكابلات و الأقمار الصناعية و أجهزة التوجيه و شرائح الحاسوب و ما شابه ذلك جزءا من هذه الأجهزة

-البرامج: و هي السلاح الرئيسي في الحرب السيبرانية تتكون من البرامج المستخدمة لتوجيه عمليات الحاسوب و استخداماته و البرامج الضارة هي الأدوات التي تملكها الدول و التي يمكنها أن تلحق الضرر بخصمها . (04)

4.الإستراتجية الروسية في الحرب السيبرانية:

1.4.أنواع هجمات الحروب السيبرانية الروسية :

1. التجسس و يشير إلى مراقبة الدول الأخرى لسرقة الأسرار في الحرب الالكترونية و يمكن أن يشمل ذلك استخدام هجمات التصيد الاحتيالي لخرق أنظمة الكمبيوتر الحساسة.

2. التخريب يجب على المنظمات الحكومية تحديد المعلومات الحساسة و المخاطر إذا تم اختراقها قد ت سرق الحكومات المعادية او الإرهابيون المعلومات او يدمرونها او يستفيدون من التهديدات الداخلية مثل الموظفين غير المبالين.

3. هجمات رفض الخدمة DOS تمنع هجمات رفض الخدمة الوصول إلى موقع الويب عن طريق إغرائه بطلبات مزيفة و إجبار الموقع على التعامل مع هذه الطلبات يمكن استخدام هذا النوع

من الهجمات لتعطيل العمليات و الأنظمة الهامة و منع الوصول إلى المواقع الحساسة من قبل المدنيين او العسكريين و أفراد الأمن او الهيئات البحثية

4. هجمات شبكة الطاقة الكهربائية تسمح مهاجمة شبكة الطاقة للمهاجمين بتعطيل الأنظمة الحيوية و تعطيل البنية التحتية حيث يمكن أن تؤدي إلى تعطيل شبكة الاتصال و جعل الخدمة مثل الرسائل النصية و الاتصالات غير قابلة للاستخدام

5. هجمات الدعاية و ذلك من خلال محاولات السيطرة على عقول و أفكار الأشخاص الذين يعيشون في البلد المستهدف و يمكن استخدامها في فضح الحقائق المحرجة و نشر الأكاذيب لجعل الناس يفقدون الثقة في بلدهم او يقفون إلى جانب أعدائهم

6.هجمات الاضطراب الاقتصادي تعمل معظم الأنظمة الاقتصادية الحديثة باستخدام أجهزة الكمبيوتر يمكن للمهاجمين لاستهداف شبكة الكمبيوتر للمؤسسات الاقتصادية مثل أسواق المالية و أنظمة الدفع و البنوك لسرقة الأموال او منع الناس من الوصول إلى الأموال التي يحتاجونه[(05)]ا.

2.4.الإستراتيجية السيبرانية الروسية للأمن السيبراني:

يعد الهدف الأسمى للأمن السيبراني هو القدرة على مقاومة التهديدات المتعمدة وغير المتعمدة والاستجابة والتعافي، وبالتالي التحرر من الخطر أو الأضرار الناجمة عن تعطيل أو إتلاف تكنولوجيا المعلومات والاتصالات أو بسبب إساءة استخدام تكنولوجيا المعلومات والاتصالات ويتطلب حماية الشبكات وأجهزة كمبيوتر، والبرامج والبيانات من الهجوم أو الضرر أو الوصول غير المصرح به.

و تبلور الاهتمام الروسي بقضايا الأمن الإلكتروني في (عام 2000)، فعندما قامت روسيا بتطوير استراتيجية أمنية تبنى على أساس الإيمان الكامل بالدور الذي يلعبه الأمن الإلكتروني في تحقيق المصالح القومية وتعزيز الاستقرار الاجتماعي والسياسي.

وق أعلنت روسيا أيضاً في(عام 2010) عن العقيدة العسكرية الخاصة بها، و التي أشارت إلى أن الصراعات العسكرية الحديثة تتضمن الاستخدام المتكامل للقدرات العسكرية وغير العسكرية، مع الاهتمام بإبراز دور أكبر لحرب المعلومات. وقد تم تشكيل قيادة مستقلة للأمن السيبراني، هذا علاوة على الإدارة السيبرانية داخل الجيش الروسي لتعزيز جاهزية القوات المسلحة الروسية للدفاع ضد الهجمات السيبرانية، واتخاذ الإجراءات الاحترازية ضد الهجمات السيبرانية من خلال الشبكات. وقامت روسيا بشراء آلات كتابه لاستخدامها في المكتبات الحيوية حتى لا تتعرض المكتبات السرية للاختراق، وبلغ الإنفاق العسكري الروسي على حرب الفضاء الالكتروني 127 مليون دولار من إجمالي إنفاق عسكري بلغ 40 بليون دولار في روسيا، التي تحتل المركز الرابع عالمياً في مجال تطوير قدرات

الأسلحة الالكترونية. وفى عام (2013)، توافقت كل من الولايات المتحدة الأمريكية وروسيا على إنشاء "الخط الساخن السيبرانى" للمساعدة في نزع فتيل أي أزمات تتعلق بالانترنت في المستقبل. (06)

ومن ناحية أخرى اعتزمت روسيا من خلال منظمة "البريكس" تأسيس فضاء إلكتروني خاص بها مستقل عن شبكة الانترنت الحالية بهدف التخلص من الهيمنة وعمليات التجسس الالكترونية الأمريكية، واتخذت خطوات فعلية لذلك، حيث تقوم البرازيل ببناء منظومة كابلات التي يمكن أن تربطها بروسيا والصين وجنوب إفريقيا، بكابل طوله 34 ألف كيلو متر، وهو يربط بين مدينة "فلاديفوستوك" فى شرق روسيا و"فورتاليزا" فى البرازيل، مروراً بشانتو الصينية و"تشيناى" الهندية و"كيب تاون" فى جنوب إفريقيا، ليس هذا فحسب، بل من المتوقع أن يوفر المشروع خدمات الإنترنت في 21 دولة افريقية، وبذلك يتم إنشاء شبكة انترنت جديدة موازية لشبكة الانترنت الحالية، وتكون منافساً قوياً للولايات المتحدة، وتعتزم دول "البريكس" أيضاً إصدار تشريعات تجبر القوى الرئيسية في الانترنت مثل "جوجل" و"فيسبوك" و"ياهو" على تخزين المعلومات التي يتم جمعها داخل دول المجموعة محلياً، كي لا تتمكن وكالة الأمن القومي الأمريكية من الوصول إليها.

وفى السنوات الأخيرة، قامت الحكومة الروسية بعمليات تقييم لمخاطر التهديدات الإلكترونية ، إلا أن نتائجها وما أسفرت عنه من سياسات لم يتم الإعلان عنه للعامة. ولكن بشكل عام يمكن القول بأن روسيا تضع المخاطر الإلكترونية في المرتبة الخاصة بالتطرف والمخاطر البيئية والجريمة المنظمة العابرة للحدود، وتأتى الهجمات الإلكترونية ضمن قائمة أكثر عشرة مخاطر تهدد البنية التحتية، وذلك وفقاً لاستراتيجية الأمن القومي الروسية. وتأتى في المرتبة الثانية، ضرورة تطوير القدرات التكنولوجية للقوات المسلحة حتى يتحقق الردع الإلكتروني.

وتعتمد الاستراتيجية الروسية الخاصة بالحروب الإلكترونية مثل الصين على استخدام الأسلحة الإلكترونية الهجومية باعتبار أنها قوة مضاعفة "Fore Multiplier" في الحروب، بمعنى أنها تزيد من القدرات القتالية للدولة إذا ما تم استخدامها إلى جانب قدرات عسكرية أخرى. كما تعتمد الاستراتيجية الروسية على محاولة تعطيل البنية التحتية المعلوماتية للخصم، والاتصالات المدنية و العسكرية له قبل البدء في العمليات العسكرية التقليدية. فوفقاً للعقيدة العسكرية الروسية، لابد وأن يسبق الهجوم العسكري الناجح عمليات أخرى تهدف إلى منع الخصم من الحصول على معلومات من مصادر خارجية، وتعطيل عمليات التداول المالية والائتمانية، ومحاولة التأثير في الرأي العام في الدولة الخصم عن طريق المعلومات الخاطئة والدعاية التي تخدم المصالح الروسية. ومن ثم يساعد التخطيط في مرحلة ما قبل الهجوم للقيام بعملية الاختراق السري لأنظمة الخصم في تحقيق هذه

الأهداف. وأبرز مثال على تلك الهجمات التي اتهمت روسيا بشنها (سنة 2008)ضد جورجيا قبل توجيه ضربة عسكرية ضدها[07].

5.المؤسسات الروسية المتخصصة في حروب المعلومات :

1.5.دائرة الحماية الاتحادية "fso": هي هيئة تنفيذية اتحادية تؤدي وظائف تطوير سياسة الدولة و التنظيم القانوني التنظيمي و الرقابة و الإشراف في مجال حماية الدولة و الرئاسية و الحكومية و أنواع أخرى من الاتصالات و المعلومات الخاصة المقدمة إلى سلطات الدولة الفيدرالية و سلطات الدولة المكونة للهيئات الحكومية الأخرى حيث وقع "فلاديمير بوتين" مرسوما بشان تعديل اللائحة الخاصة بجهاز الأمن الفدرالي و تم استكمال قائمة الصلاحيات و ذلك بمنع و إزالة عواقب الهجمات الكمبيوتر على موارد روسيا و كذا مشاركة في سياسة الدولة بشان امن المعلومات الدولي .

2.5.جهاز الأمن الاتحادي "fsb": يعمل هذا الجهاز في العديد من المجالات منها حماية حدود الدولة الروسية و الدفاع عنها و ضمان امن المعلومات روسيا و ممارسة الوظائف الأساسية لأجهزة الأمن الفدرالية المحددة في التشريع الروسي و كذلك تنسيق الجهود و مكافحة التجسس للسلطة التنفيذية الفدرالية.

3.5.جهاز الاستخبارات الخارجية "svr": يتكون من عدة وكالات حكومية خاصة هيئات استخبارات أجنبية تابعة للاتحاد الروسي يهدف إلى حماية الفرد و المجتمع و الدولة من التهديدات الخارجية المعلوماتية.

4.5.جهاز الاستخبارات العسكرية "gru": يصفها الكونغرس الأمريكي بأنها منظمة كبيرة وواسعة وقوية فتقول الوزارة إنها مكلفة بضمان الظروف المواتية للتنفيذ الناجح لسياسة امن الدولة و تزويد المسئولين بالمعلومات الاستخباراتية التي يحتاجون إليها لاتخاذ قرارات في مجالات سياسية [08].

6.نماذج عن الحروب السيبرانية الروسية :

1.6الحرب السيبرانية الروسية على استونيا 2007 :

تعتبر "استونيا" إحدى دول البلطيق التي استقلت عن الاتحاد السوفييتي حيث بدأت مجموعة من الإصلاحات الاقتصادية و السياسية و الاجتماعية و انضمت إلى الاتحاد الأوروبي و حلف الناتو و ذلك لتعزيز أمنها و التخلص من القيود الروسية و كان أهم التحديات التي واجهتها استونيا وجود أقلية روسية تمثل 26 بالمائة من الشعب الاستوني. [09]

حيث تم تسريع الهجمات الالكترونية في (عام 2007) على استونيا بقرار الحكومة الاستونية بنقل نصب تذكاري للحرب مخصص للقوات السوفيتية أثناء تحرير استونيا من الألمان

خلال الحرب العالمية الثانية حيث تم نقل التمثال من موقع "باريز" في تالين أثار هذا الإجراء رد فعل غاضب من الحكومة الروسية و سرعان ما تلاها هجمات (DDOS) ضد نظام الحكم و النظام المالي في استونيا بالإضافة إلى هجمات سيبرانية أخرى تنصلت موسكو من أي علم بها او رعايتها للهجمات ومع ذلك فان المدونات الروسية تحتوي على تعليمات حول كيفية الانضمام إلى (DDOS) علاوة على ذلك تتبع الطب الشرعي بعض هجمات حيث تم إيجاد عنوانين هاته الهجمات داخل روسيا و أشار المتحدث عن الحكومة الروسية في دفاع عن الاتهامات أن عناوين (IP) تم تزويرها حيث خلص احد المسئولين الاستونيين إلى أن هذه الهجمات تمثل شكلا جديد من أشكا ل القطاعين العام و الخاص أي أن الهجمات نفذت من قبل منظمة الجريمة المنظمة و لكن من إخراج الكريملين كما قال رئيس وكالة الأمن القومي الأمريكية "الجنرال كيث الكسندر" فجأة ذهبنا من الجريمة الالكترونية إلى الحرب الالكترونية في حيث يعتقد بعض الخبراء أن هجوم استونيا وفر وسيلة لموسكو لاختبار الأسلحة السيبرانية [10].

بالإضافة إلى هجمات « BOOT NET » و إلى « MAILBOMBING » حيث تعمل الأولى على محاولة التحكم في اكبر مجموعة ممكنة من شبكات الكمبيوتر بينما تعنى الثانية إغراق المستخدمين بالعديد من الرسائل التي تجعل البريد الالكتروني يتوقف عن العمل و كان الأثر المباشر هو فقدان الخدمات الحكومية و الخدمات المصرفية و من بين المواقع التي تأثرت بالهجمات موقع البرلمان الاستوني ووزير الدفاع فضلا عن الموقع الالكتروني لحزب رئيس الوزراء و عدد من الجامعات الكبرى و الصحف الوطنية و اضطر البنك إلى التوقف مؤقتا » HANSABANK » و كذلك استخدموا طرق أخرى تسمى « war dailing »المرتبطة بخطوط الهاتف و التي كان لها تأثير في الحصار على جميع مكاتب الحكومة و البرلمان و حجب الاتصالات عنها.[11]

2.6.الحرب السيبرانية الروسية على جورجيا 2008

بعد ذلك في (أوت 2008) تلاشت القوات الروسية في جورجيا بعد إطلاق تلك الدولة هجوم عسكري ضد "اوسيتيا" الجنوبية لاستعادة الأراضي من حكومتها المدعومة من روسيا الهجوم جاء عقب مزاعم جورجية بان كانت قوات حفظ السلام التابعة لها في "اوسيتيا" الجنوبية تتعرض للهجوم و أن روسيا كانت تنشر وحدات القتال في ذلك البلد و ردت روسيا بشن هجوم مضاد في "اوسيتيا الجنوبية" و ضد جورجيا نفسها حيث تلقت القوات الروسية الدعم من القوات الانفصالية في "اوسيتيا الجنوبية" و "أبخاريا "و رافقت هذه الهجمات هجمات الكترونية أدت إلى إغلاق مواقع رسمية في جورجيا بالإضافة إلى مواقع إخبارية محلية.[12]

فإضافة إلى القصف الصاروخي و الغزو العسكري زامنت روسيا بين الحرب التقليدية و الحرب السيبرانية في جورجيا حيث شنت هجوما سيبرانيا حيث قامت باختراق مواقعهم وشنت هجمات الحرمان من الخدمة ddos ضد القطاع الخاص و العام ووزعت البرامج الضارة على المتعاطفين الروس الذين يعيشون في جورجيا و ذلك بغرض نشر الفيروسات في جميع أنحاء شبكات البلاد و ذلك إلى أن تأثير الحرب السيبرانية في جورجيا لم يكن بالتأثير الكبير حيث كانت جورجيا تعتمد على الحد الأدنى من الاتصال بالأنترنت او من نتائج هذا الهجوم تعطل عمليات ألاف من المواقع الالكترونية التي تديرها الحكومة الجورجية و القطاع الخاص بالإضافة إلى تعطل محطتين تليفزيونيتين على الأقل مما اثر بشكل مباشر على السكان الجورجيين و قد تم اكتشاف برامج للتجسس بعد ذلك بعدة سنوات ففي مارس 2011 اكتشفت السلطات الجورجية برنامج يقوم بجمع المعلومات المتعلقة بالأمن القومي في الشبكات الدولية الجورجية و المنظمات المالية و حتى القطاع الخاص[13].

3.6.روسا و قيرغيزستان :

بعد خمسة شهور فقط من الصراع بين روسيا و جورجيا جاءت سلسلة ثالثة من الهجمات الالكترونية الكبرى ضد الحكومة و البنية التحتية لجمهورية سوفيتية سابقة في (يناير 2009) حيث أن اثنان من خوادم الانترنت الرئيسية في قرغيزستان تعرضت لهجمات DDOS كانت الهجمات قوية بما يكفي لإغلاق مواقع الويب و البريد الالكتروني داخل الدولة فتم إرجاع حركة مرور إلى خوادم روسية معروفة بنشاط جرائم الانترنت حيث حدث الهجوم في نفس الوقت الذي كانت فيه الحكومة الروسية تضغط على قرغيزستان لإنهاء وصول الولايات المتحدة إلى القاعدة الجوية في "ماناس" و هي مركز لوجيستي رئيسي يدعم العمليات العسكرية الأمريكية في أفغانستان. [14]

4.6.روسيا و اكرانيا :

يمكن القول إن الصراع السيبراني الروسي مع اكرانيا قد بدا في وقت مبكر من عام 2009 كجزء من حملة حرب معلومات أوسع ضد دول الناتو و الاتحاد الأوروبي لكن في سنة 2014 بدأت في الحرب فعليا ففي ذلك العام وقع الرئيس فلاديمير بوتين قرار يقضي باستعادة شبه جزيرة القرم و ضمها إلى روسيا من اوكرانيا و جمعت القوات الروسية على طول الحدود الوطنية لأوكرانيا و بدأت الحرب الروسية الاكرانية حيث تم كذلك شن العديد من هجمات حجب الخدمة و اختراق شبكة الاتصال كما تجسست روسيا من خلال العديد من البرامج .[15]

فأطلق قراصنة الموالية لروسيا سلسلة من الهجمات الالكترونية على مدى عدة أيام لتعطيل الانتخابات الرئاسية الاكرانية في مايو 2014 كما عملوا على الإفراج عن رسائل البريد الالكتروني المخترقة بالإضافة إلى محاولة تغيير حصص التصويت و تأخير النتيجة النهائية للانتخابات

كما أطلقت روسيا برامج خبيثة كانت ستعرض رسميا بيانيا يعلن فيه المتر شح اليميني المتطرف "ديميترو ياروش" تمت إزالة الفائز الانتخابي من لجنة الانتخابات المركزية في اكرانيا قبل اقل من ساعة من الإغلاق على الرغم من ذلك ذكرت القناة الأولى في روسيا ياروش قد فاز و بث الرسم المزيف مستشهدا بموقع اللجنة الانتخابية حيث أن هذه النتائج مزيفة موجهة إلى جمهور معين من اجل تغذية الرواية الروسية التي ادعت منذ البداية أن المتطرفين الوطنيين و النازيين كانوا وراء الثورة في اكرانيا [16].

4.6.روسيا و التنظيمات الإرهابية:

أطلقت "روسيا" في (30 سبتمبر 2015) حملتها العسكرية ضد التنظيمات التكفيرية الإرهابية في سوريا، و التي تمثلت أهدافها الرسمية المعلنة في حماية الجيش السوري من الانهيار حتى لا تسقط مؤسسات الدولة حسب الرواية الروسية ، فضلاً عن القضاء على تنظيمي "داعش"، وجبهة النصرة التابعين لتنظيم القاعدة وغيرها من التنظيمات الإرهابية الأقل نفوذاً وانتشاراً. وفى مواجهة هذا التدخل الروسي، تصاعد الجدل الداخلي بشأن جدواه ومدى انعكاسه على الداخل الروسي، واختلفت اتجاهات الرأي العام تجاه هذه الخطوة، خاصة في ضوء الذكرى السلبية للتدخل السوفيتي في أفغانستان.

هذا وقد نجحت الحكومة الروسية في تهدئة مخاوف الرأي العام من التدخل العسكري في سوريا، ونجحت في تعبئة الرأي العام لصالح تأييد هذا القرار، وذلك من خلال الخطوات التالية:

- سعى وزارة الدفاع الروسية لإصدار بيانات صحفية عن العلميات العسكرية في سوريا، ونشرها من خلال موقع الفاسبوك يومياً، فضلاً عن كتابة تغريدات على موقع توتير عن العمليات العسكرية الروسية في سوريا، وذلك بهدف تقديم معلومات مفصلة عن الضربات الجوية، كما يتم عرض مقاطع فيديو للعمليات العسكرية وللظروف المعيشية على اليوتيوب التي يعيش في ظلها أفراد الجيش الروسي في سوريا. وتهدف هذه الخطوة إلى زيادة الشفافية وتقديم انطباع بأن المناطق التي توجد فيها القوات المسلحة الروسية آمنة ومحمية.

- التأكيد على استخدام الجيش الروسي أسلحة ومعدات عسكرية متقدمة تقنياً، مما يقلل إلى حد كبير من خطر الإصابات والخسائر في صفوف الجيش الروسي في سوريا، فضلاً عن استبعاد القيادة الروسية إمكانية إرسال قوات برية إلى سوريا.

- توظيف الكرملين حادث استهداف الطائرة المدنية الروسية في سيناء بعمل إرهابي، للتأكيد على ضرورة توجيه ضربات انتقامية ضد "داعش"، وهو ما يتسق مع توجهات الرأي العام في هذا الإطار.

ومما سبق، يتضح أن طريقة إدارة الكرملين التغطية الإعلامية الالكترونية للحرب الروسية في سوريا حتى الآن، نجحت في إيجاد مواقف إيجابية وداعمة من جانب أغلب فئات الشعب الروسي، خاصة أنه ليس من المتوقع أن تواجه القوات الجوية الروسية خسائر بشرية تذكر نتيجة عملياتها العسكرية في سوريا، وقد انعكس هذا النجاح في التغطية الإعلامية للحرب على نتائج استطلاعات الرأي العام التي قامت بها بعض مؤسسات قياس الرأي العام الروسية.[17]

خاتمة :

إن الحرب قد اتخذت شكلا جديدا في العصر الحالي ألا وهي حرب المعلوماتية حيث تم إيجاد شكل جديد من أشكال الحروب ألا وهو الحروب الهجينة للدلالة على الحروب التي تستعمل في الحرب الالكترونية إلى جانب الحرب التقليدية فالحرب السيبرانية بمثابة مكمل للحرب التقليدية فتتعدد أغراض هذه الحروب منها التجسس و نشر الدعاية بالإضافة إلى إحداث خلل في البنية التحتية وقد يصل مداها إلى التأثير الجسدي و إحداث الفوضى وذلك حتى يسهل احتلال هذا البلد بالقوة التقليدية وهذا يدل على أن كما زادت رقمنه القطاعات العامة زاد خطر هذه الحروب فانه من الواجب اخذ احتياطات الدول في هذا المجال وذلك من خلال أنظمة الحماية ومن التوصيات التي يمكن الخروج بها :

1 تطوير قطاعات تكوينية وطنية في مجال أنظمة الحماية و تكنولوجيات الإعلام الآلي وذلك من خلال تبني خبرات وطنية في هذا المجال.

2 تبني سياسات عالمية رائدة في هذا المجال.

3 العمل على إنشاء منظمات وطنية وإقليمية وعالمية والتي من شانها سن قوانين دولية لإدانة هذه الحروب كون أن تأثيرها كبير جدا.

4 عقد ملتقيات علمية هادفة تحت هذا المجال.

الهوامش:

[01] **محمد سعد محمود ، الحرب السيبرانية أدواتها وقودها خسائرها ، صفحة 7.**

[02] زينب شنوف ، الحرب السيبرانية في العصر الرقمي حروب ما بعد كلاوزفيتش ، المجلة الجزائرية للامن و التنمية، المجلد 9 ،العدد2 ، جويلية 2020 ، صفحة 91.

[03] Michael Robinson, cyber warfare issues and challenges, computer and security , 70/94, 2015 page

[04] زينب شنوف، مرجع سابق ، صفحة 98

[05] مقال منشور على الموقع التالي https://www.imperva.com/learn/application-security/cyber-warfare تم الاطلاع بتاريخ 2022/11/01

[06] اماني عصام ، استخدام روسيا للقوة السيبرانية في ادارة تفاعلاتها الدولية ، مجلة كلية الاقتصاد و العلوم السياسية ، جامعة القاهرة ، المجلد 22 ،العدد 4 ،اكتوبر 2022 على الموقع https://jpsa.journals.ekb.eg/article

07 اماني عصام ، نفس المرجع.

[08] عن موقع الرسمي للحكومة الروسية http://government.ru/en/department/113/ تم الاطلاع بتاريخ 2022/11/02

[09] قاضي هشام ، الامن السيبراني في الالفية الثالثة التهديدات التحديات سبل المواجهة ، الملتقى الافتراضي السيبراني الدولي الاول ، دار قاضي للنشر و الترجمة ، صفحة 15.

[10] ANDREW F. KREPINEVICH , CYBER WARFARE A NUCLEAR OPTION , CENTER FOR STRATEGIC AND BUGETARY ASSESSMENTS , 2012 PAGE 51/52

[11] قاضي هشام ،مرجع سابق ، صفحة 16

[12] ANDREW F. KREPINEVICH , Op.Cit , PADE 54

[13] قاضي هشام ، مرجع سابق ، صفحة 17

[14] ANDREW F. KREPINEVICH , Op.Cit ,PAGE 56

[15] قاضي هشام ، مرجع سابق ، صفحة 18

[16] على زياد فتحي ، رؤية استراتيجية العمليات السيبرانية الاوروميتوسطية و ممهدات الجيوسيبرانية الروسية رؤية في الاشتباك السيبراني الاورو روسي ، مجلة حمورابي ، العدد 30 ،السنة السابعة ، ربيع 2019 ، صفحة 13.

[17] اماني عصام ، مرجع سابق.