نشوء القوة السيبرانية وتأثيرها في انماط الصراع الدولي

م. حسين باسم عبد الأمير (*)

مقدمة

أدت التطورات والظهور السريع الذي لا يرحم لشبكة الويب العالمية والإنترنت إلى تغييرات مذهلة لا تمحى في المجتمعات الحديثة والاقتصاد العالمي وأيضا في إدارة السياسة والحرب. في الواقع، حدثت هذه التغييرات في مساحة زمنية صغيرة نسبيا وبهذا النطاق يتعين على المحللين والباحثين المتخصصين تمييز جميع الآثار المترتبة على نشوء وصعود مفهوم القوة السيبرانية. من الصعب تحديد الآثار المترتبة على الاستراتيجية، وذلك رغما عن أن الاتجاهات والقضايا العامة معروفة جيدا لدرجة أن الاستراتيجيين أصبحوا الآن قادرين على تحليل الاتجاهات. نظرا لأن القوة السيبرانية لها تأثير واسع وملموس على إدارة الحرب، فإنها تنتج تحديات كبيرة للدراسات الاستراتيجية. إذ قد تؤدي هذه التأثيرات الواسعة والملموسة، إلى جانب التحديات والفرص المصاحبة لها، إلى إحداث تغيير في طبيعة الحرب وأنماط الصراع. وهكذا يحاول هذا البحث مناقشة هذه الاتجاهات والقضايا وشرح ما يعنيه كل ذلك بالنسبة لمستقبل الإستراتيجية والصراع.

فرضية البحث:

ينطلق البحث من فرضية مفادها: بأن نشوء القوة السيبرانية ساهم في إعادة صياغة السياسة الدولية وأثر بشكل واضح في أنماط الصراع خلال القرن الحادي والعشرين. وسيحاول هذا البحث التحقق من هذه الفرضية.

أهداف البحث:

يسعى هذا البحث الى شرح ومعرفة مصطلح/مفهوم "القوة السيبرانية" عبر تحديد نطاق المفهوم وتقديم التعاريف التي فسرت هذا المفهوم. كما ويحاول البحث أيضا تعزيز وتمتين فهم واستيعاب مصطلح/مفهوم "القوة السيبرانية" من خلال عرض ومناقشة المصطلحات/المفاهيم الأخرى التي تدور

(*) مركز الدراسات الاستراتيجية / جامعة كربلاء
hussain.b@uokerbala.edu.iq

في نفس فُلك القوة السيبرانية مثل "الفضاء السيبراني" و "الهجوم السيبراني" و "السلاح السيبراني" وما شابه. إن الفهم الكافي للقوة السيبرانية يؤدي إلى معرفة دورها الجوهري في المساهمة الحيوية والفعالة في إعادة صياغة السياسة الدولية وانماط الصراع. وهكذا، سوف يحاول البحث الإجابة عن الأسئلة التالية:

١- ما المقصود بـ القوة السيبرانية؟

٢- ما المقصود بالفضاء السيبراني

٣- ما المقصود بـ الهجوم السيبرانية؟

٤- ما المقصود بـ السلاح السيبراني؟

٥- ما المقصود بـ الحرب السيبرانية؟

٦- هل يمثل الأمن السيبراني -أو الدفاع السيبراني- تحديا كبيرا للمسؤولين عن تحقيقه؟

٧- هل توجد مبادئ عامة ملزمة للقانون الدولي يجري تطبيقها على الحرب والصراع السيبراني؟

٨- ما هي الآثار المترتبة على الأهمية المتزايدة للقوة السيبرانية في السياسة الدولية واستخدام القوة العسكرية وانماط الصراع في القرن الحادي والعشرين؟

منهجية البحث:

لقد اعتمد هذا البحث على المنهج التحليلي، الذي يقوم على جمع المعلومات ثم تحليلها، فضلا عن استخدام المنهج المقارن كأحد مناهج البحث العلمي، كونه متعدد الاتجاهات، فهو شكل من اشكال القياس، وهو مرادف لمنطق التحليل العلمي. بالإضافة الى استناد البحث الى المنهج التاريخي لما له من أهمية في متابعة وتطور الواقع خلال الحقب التاريخية.

ولغرض الاحاطة بموضوع البحث، فقد تم تقسيم محتوياته إلى مبحثان، ركزنا في المبحث الاول على عرض المصطلحات والمفاهيم الأساسية مثل: (الفضاء السيبراني، القوة السيبرانية، والمجال المعلوماتي أو السيبراني). وكذلك يشتمل المبحث الثاني على ثلاث مطالب خصصنا المطلب الأول لمناقشة وشرح الدفاع ضد التهديدات الالكترونية وتحقيق الأمن السيبراني بينما يركز المطلب الثاني على عرض الصعوبات التي ترافق السعي الى تطبيق القانون الدولي على الفضاء السيبراني والقوة السيبرانية. في حين يركز المبحث الثالث على مناقشة مساهمة القوة السيبرانية والدور الذي تؤديه في إعادة صياغة السياسة الدولية وانماط الصراع.

المبحث الأول: عرض المصطلحات والمفاهيم الأساسية

تضع الدراسات الإستراتيجية أهمية خاصة للتعريفات على الرغم من أنها تقع في سياقها وثقافتها. على سبيل المثال، قد لا يتوافق التعريف الأمريكي للقوة الجوية بالضرورة مع التعريف الأوغندي، وذلك نظرا للاختلافات الشاسعة في التجارب التاريخية والعملياتية، فضلاً عن الاختلافات في القدرات وكيفية استخدام أداة القوة الجوية لتحقيق الأهداف السياسية المحددة من قبل الحكومات المعنية. ومع ذلك، في نهاية المطاف، فإن المناقشات التعريفية حول القوة الجوية، ومثلها القوة البرية والبحرية، تميل إلى أن تدور حول عدد محدود

من التعريفات المتنافسة. لكن الأمر ليس كذلك مع الفضاء السيبراني، وما يترتب عليه من قوة سيبرانية. هناك عدد كبير من التعريفات المتنافسة للفضاء السيبراني وعدد من التعريفات المتنافسة للقوة السيبرانية، وكذلك هو الحال مع الهجمات والحرب السيبرانية، يمكن تفسير كثرة التعريفات الفسيفسائية من خلال الانتباه الى أن الفضاء السيبراني والقوة السيبرانية كظواهر استراتيجية تعتبر جديدة نسبيا عند مقارنتها بالقوة البرية والبحرية والجوية وحتى الفضائية.

المطلب الأول: الفضاء السيبراني (Cyber Space)

ظهر مصطلح "الفضاء السيبراني" لأول مرة في احدى روايات الثمانينيات من القرن الماضي ضمن عمل مؤلف الخيال العلمي "ويليام جيبسون"، أولا في قصته القصيرة عام ١٩٨٢ "الكروم المحترق" ولاحقا في روايته "نيو رومانسر" عام ١٩٨٤. في السنوات القليلة التالية، أصبحت الكلمة مرتبطة بشكل بارز بشبكات الكمبيوتر عبر الإنترنت. ووصف الفضاء الإلكتروني/السيبراني بأنه "هلوسة توافقية".

الفضاء السيبراني هو مفهوم يصف تقنية رقمية مترابطة على نطاق واسع. "يعود التعبير إلى العقد الأول من انتشار الإنترنت. ويشير إلى عالم الإنترنت باعتباره عالما منفصلا متميزا عن الواقع اليومي الحقيقي. في الفضاء السيبراني يمكن للناس الاختباء خلف هويات مزيفة. دخل المصطلح الثقافة الشعبية من الخيال العلمي والفنون ولكنه يستخدم الآن من قبل الاستراتيجيين والتقنيين والمتخصصين في مجال الأمن والحكومة والقادة العسكريين والصناعيين ورجال الأعمال لوصف مجال بيئة التكنولوجيا الرقمية العالمية، والتي تُعرف عموما على أنها الوقوف على الشبكة العالمية للبنى التحتية لتكنولوجيا المعلومات المترابطة وشبكات الاتصالات وأنظمة معالجة الكمبيوتر.

كتجربة اجتماعية، يمكن للأفراد التفاعل وتبادل الأفكار وتبادل المعلومات وتقديم الدعم الاجتماعي وإجراء الأعمال التجارية وتوجيه الإجراءات وإنشاء وسائط فنية وممارسة الألعاب والمشاركة في النقاشات والشؤون السياسية وما إلى ذلك، باستخدام هذه الشبكة العالمية. أصبح مصطلح الفضاء السيبراني وسيلة تقليدية لوصف أي شيء مرتبط بالإنترنت وثقافة الإنترنت المتنوعة.

تعريف الفضاء السيبراني:

- وفقا لما ذكره "تشيب مورنينغستار" و "راندال فارمر" يتم تعريف الفضاء السيبراني من خلال التفاعلات الاجتماعية الضمنية بدلا من تطبيقه التقني. من وجهة نظرهم، فإن الوسيلة الحاسوبية في الفضاء السيبراني هي زيادة لقناة الاتصال بين أناس حقيقيين؛ السمة الأساسية للفضاء السيبراني هي أنه يوفر بيئة تتكون من العديد من المشاركين والفاعلين الذين لديهم القدرة على التأثر والتأثير في بعضهم البعض. إنهم يستمدون هذا المفهوم من ملاحظة أن الناس يبحثون عن الثراء والتعقيد والعمق داخل عالم افتراضي.

- في حين ذكرت "دوروثي دينينج" ان الفضاء السيبراني هو مساحة المعلومات التي تتكون من المجموع الكلي لجميع شبكات الكمبيوتر.

- وكذلك يصف "وين شفارتاو" الفضاء السيبراني بأنه: ذلك المكان غير الملموس بين أجهزة الكمبيوتر حيث توجد المعلومات مؤقتا في طريقها من أحد طرفي الشبكة العالمية إلى الطرف الآخر.

- وفي نفس الوقت ذكر الجنرال "جيمس إي. كارترايت" نائب رئيس هيئة الأركان المشتركة الامريكية بأن مجال الفضاء السيبراني يتميز باستخدام الإلكترونيات والطيف الكهرومغناطيسي لتخزين وتعديل وتبادل البيانات عبر أنظمة شبكية والبنى التحتية المادية المرتبطة بها.

- بينما وصف نائب وزير الدفاع الأمريكي الأسبق "جوردون إنجلاند" الفضاء السيبراني بأنه مجال عالمي داخل بيئة المعلومات يتكون من شبكة مترابطة من البنى التحتية لتكنولوجيا المعلومات، بما في ذلك الإنترنت وشبكات الاتصالات وأنظمة الكمبيوتر والمعالجات ووحدات التحكم المدمجة.

- وكذلك وصف "غريغوري جيه راتراي" الفضاء السيبراني بأنه يتكون من أجهزة وشبكات وأنظمة تشغيل ومعايير إرسال تعمل بالطاقة الإلكترونية.

- كما وأشار تقرير المشروع المشترك بين معهد ماساتشوستس للتكنولوجيا وجامعة هارفارد بعنوان (استكشافات في العلاقات الدولية السيبرانية) الى ان السمة المميزة والتأسيسية للفضاء السيبراني هي أنه لا يوجد كيان مركزي يمارس السيطرة من قبله على جميع الشبكات التي تشكل هذا المجال الجديد. كما هو الحال في العالم الحقيقي، لا توجد حكومة عالمية، يفتقر الفضاء الإلكتروني إلى مركز هرمي مؤسسي محدد مسبقا. بالنسبة للفضاء السيبراني، وهو مجال بدون مبدأ مرتب هرميا، بالتالي، يمكننا توسيع تعريف السياسة الدولية التي صاغها كينيث والتز: على أنها "بلا نظام قانوني قابل للتنفيذ". هذا لا يعني أن بُعد القوة في الفضاء السيبراني غائب، ولا أن القوة مشتتة ومبعثرة في ألف تيار غير مرئي، ولا أنها منتشرة بالتساوي عبر عدد لا يحصى من الأشخاص والمنظمات، على العكس من ذلك، يتميز الفضاء السيبراني بهيكلة دقيقة لتراتبية القوة.

- وأيضا "يمكن اعتبار الفضاء السيبراني بأنه الخدمات التي تستخدم البنية التحتية للإنترنت لتقديم المعلومات للمستخدمين من خلال أجهزتهم، فهي موجودة بالكامل داخل مساحة الكمبيوتر والأجهزة الاخرى، وموزعة عبر شبكات معقدة ومتغيرة بشكل متزايد." بدأ مصطلح "الفضاء السيبراني" يصبح مرادفا فعليا للإنترنت، ولاحقا شبكة الويب العالمية، خلال التسعينيات، خاصة في الأوساط الأكاديمية والمجتمعات المتقدمة."

- وأخيرا ذكر "كويهل" واصفا الفضاء السيبراني بأنه مجال عالمي داخل بيئة المعلومات يتم تأطير شخصيته المميزة والفريدة من خلال استخدام الإلكترونيات والطيف الكهرومغناطيسي لإنشاء المعلومات وتخزينها وتعديلها وتبادلها واستغلالها عبر شبكات مترابطة ومتداخلة باستخدام تقنيات الاتصالات المعلوماتية .

في الواقع، على الرغم من أنه يمكن العثور على العديد من التعريفات للفضاء السيبراني في

كل من المؤلفات العلمية والمصادر الحكومية والرسمية، غير أنه لا يوجد تعريف رسمي متفق عليه بالمطلق حتى الآن.

من وجهة نظر الاستراتيجي، تحاول التعريفات منح مصطلح الفضاء السيبراني معنىً مشابها لتعريفات القوة البرية والبحرية والجوية والفضائية. بالنظر إلى العدد الكبير من التعريفات المتداولة اليوم، والتي يركز كل منها على جانب واحد ومعين أكثر من جوانب الفضاء السيبراني الأخرى، مما يجعل التمكن من تقديم تعريفا شاملا يمكن أن يشير إلى جميع الجوانب غير مرجح في المستقبل القريب.

تختلف جميع التعريفات المتداولة اليوم من حيث ما يشكل الفضاء السيبراني. نتيجة لذلك، تتضمن بعض التعريفات ميزات معينة يمكن العثور عليها في الفضاء السيبراني، بينما تتجاهل بعض التعريفات الاخرى نفس الميزات. يمكن أن تكون الحروب التعريفية بطبيعتها مملة لأولئك الذين لا يشتركون فيها بشكل مباشر، ولكن في حالة الفضاء السيبراني، فإن ما هو موجود وما لم يتم تضمينه في أي تعريف قد يكون له آثار خطيرة على تطبيقاته الاستراتيجية. وفي هذا الصدد يذكر "بيتز وستيفنز" قائلا:

إن مسألة تعريف الفضاء السيبراني ليست مسألة تافهة. إن ما نقرر تضمينه أو استبعاده من الفضاء السيبراني له آثار كبيرة على عمليات القوة، لأنه يحدد نطاق استراتيجيات الفضاء السيبراني وعمليات القوة السيبرانية.

خصائص وسمات الفضاء السيبراني:

وفي سبيل معرفة الفضاء السيبراني بتركيز أكبر يذكر في هذا الصدد الباحثين المختصين عددا من الخصائص المميزة للفضاء السيبراني، وهي كالتالي :

١- تكلفة دخول منخفضة. تعد الموارد والخبرة المطلوبة لدخول الفضاء الإلكتروني والتواجد فيه واستغلاله متواضعة للغاية مقارنة بالموارد والخبرة المطلوبة لاستغلال المجالات البرية والبحرية والجوية والفضائية. يمكن لأي شخص لديه إمكانية الوصول إلى تقنيات المعلومات والاتصالات الشبكية أن يستخدمها.

٢- جهات فاعلة متعددة. تعني التكلفة المنخفضة للدخول إلى الفضاء الإلكتروني أن عدد وأنواع الجهات الفاعلة القادرة على العمل في المجال والتي من المحتمل أن تحدث تأثيرا استراتيجيا غير محدودة تقريبا عند مقارنتها بالمجالات البرية والبحرية والجوية والفضائية. إذ يشارك الأفراد والجماعات والمنظمات والشركات والجهات الفاعلة غير الحكومية، وكذلك الدول في الفضاء الإلكتروني.

٣- يمكن تكرار الفضاء الإلكتروني باستمرار. يمكن أن يكون هناك العديد من الفضاءات الإلكترونية في وقت واحد بقدر ما يمكن للمرء أن يولده. مع الفضاء السيبراني، يمكن أن يكون هناك العديد من الأشياء الموجودة في وقت واحد -بعضها متنازع عليه والبعض الآخر لا. بالنسبة للجزء الأكبر، لا شيء نهائي في الفضاء السيبراني، مع القوة الجوية مثلا، يمكن تدمير طائرات العدو، وهنا تنتهي المسألة. في الفضاء الإلكتروني، على سبيل المثال، يمكن إغلاق موقع ويب لمجموعة ارهابية عن قصد، غير أنه يمكن لنفس المجموعة استحداث موقع ويب جديد في غضون ساعات على خادم

مختلف باستخدام اسم مجال مختلف. وبالمثل، يمكن إصلاح الشبكات وإعادة تشكيلها بسرعة بفضل الأجهزة غير المكلفة نسبيا والمتاحة بسهولة.

٤- الفضاء السيبراني قريب من المعلومات اللحظية التي تعبر الفضاء السيبراني بما يسمى السرعة الشبكية - السرعة التي يستطيع بها أي جزء من الشبكة في أي وقت نقل المعلومات. في كثير من الحالات، تقترب السرعة الصافية من سرعة الضوء؛ في حالات أخرى، لا يكون الأمر بهذه السرعة. ومع ذلك، فبالنسبة للمستخدم البشري، يمكن للشبكات الحديثة أن تبدو وكأنها تنقل المعلومات بشكل فوري تقريبا.

المطلب الثاني: الهجوم السيبراني (Cyberattack)

في أجهزة الكمبيوتر وشبكات الكمبيوتر، الهجوم هو أي محاولة لكشف أو تغيير أو تعطيل أو تدمير أو سرقة أو الحصول على معلومات من خلال الوصول غير المصرح به إلى أحد الأصول أو الاستخدام غير المصرح به. الهجوم السيبراني هو أي مناورة هجومية تستهدف أنظمة معلومات الكمبيوتر أو البنى التحتية أو شبكات الكمبيوتر أو أجهزة الكمبيوتر الشخصية. المهاجم هو شخص أو عملية تحاول الوصول إلى البيانات أو الوظائف أو المناطق المحظورة الأخرى في النظام وذلك من دون إذن وتصريح، ويحتمل أن يكون ذلك بقصد ضار. اعتمادا على السياق، يمكن أن تكون الهجمات السيبرانية جزءاً من الحرب السيبرانية أو الإرهاب السيبراني. يمكن استخدام الهجوم السيبراني من قبل دول ذات سيادة أو أفراد أو مجموعات أو منظمات، وقد ينشأ من مصدر مجهول.

قد يسرق الهجوم السيبراني أو يغير أو يدمر هدفا محددا عن طريق اختراق نظام حساس. يمكن أن تتراوح الهجمات الإلكترونية من تثبيت برامج التجسس على جهاز كمبيوتر شخصي إلى محاولة تدمير البنية التحتية لدول بأكملها. يسعى الخبراء القانونيون إلى قصر استخدام المصطلح على الحوادث التي تسبب ضررا ماديا، وتمييزه عن انتهاكات البيانات الروتينية وأنشطة القرصنة الأوسع نطاقا. وذلك بعد ان أصبحت الهجمات الإلكترونية معقدة وخطيرة بشكل متزايد.

تعريف الهجوم السيبراني:

ومثل الفضاء السيبراني، فقد جرى تعريف الهجوم السيبراني بعدة تعريفات منها ما يلي:

- وفقا لما ذكره " روبرت بوريس" يتم تعريف الهجوم السيبراني على انه عمليات برمجية حاسوبية ضارة أو أي فعل متعمد آخر مصمم لتغيير أو تعطيل أو إنكار من أو إتلاف المعلومات الموجودة في أجهزة الكمبيوتر وشبكات الكمبيوتر أو أجهزة الكمبيوتر والشبكات نفسها."

- وأيضا يستخدم "وليام أوينز" وزملائه استعارة لتعريف الهجوم السيبراني واصفا إياه بأنه "استخدام الإجراءات المتعمدة -ربما على مدى فترة زمنية طويلة- لتغيير أو تعطيل أو خداع أو تحطيم أو تدمير أنظمة أو شبكات الكمبيوتر المعادية أو المعلومات أو البرامج الموجودة في هذه الأنظمة أو الشبكات أو التي تعبرها. قد يكون لمثل هذه التأثيرات على

الأنظمة والشبكات المعادية أيضا تأثيرات غير مباشرة على الكيانات المقترنة بها أو التي تعتمد عليها

- في حين ذكر تقرير إدارة مخاطر الأمن الإلكتروني في مجال الكهرباء الصادر عن وزارة الطاقة الأمريكية بأن الهجوم السيبراني هو "الهجوم، عبر الفضاء السيبراني، يستهدف استخدام منصة للفضاء السيبراني بغرض تعطيل أو تخريب أو تدمير أو التحكم بشكل ضار في بنية تحتية حاسوبية، أو لتدمير سلامة البيانات أو سرقة المعلومات الخاضعة للرقابة.

- في حين ذكر "ديفد كلارك" وزملاؤه ان الهجوم السيبراني هو "إجراء يهدف إلى التسبب في إيقاف الخدمة أو إتلاف أو تدمير المعلومات المخزنة أو العابرة من خلال نظام أو شبكة تكنولوجيا المعلومات.

- وفي نفس الوقت ذكر التقرير المشترك الصادر عن "بنك التسويات الدولية" و"المنظمة الدولية لهيئات الأوراق المالية" بأن الهجوم السيبراني هو "استغلال نقاط الضعف من قبل الخصم للاستفادة بقصد تحقيق تأثير سلبي على بيئة تكنولوجيا المعلومات والاتصالات.

- وكذلك وصف تقرير "فريق العمل المعني بالردع السيبراني التابع لمجلس علوم الدفاع الأمريكي" الهجوم السيبراني بأنه "أي إجراء متعمد يؤثر على التوافر المرغوب أو سلامة البيانات أو نظم المعلومات التي تعتبر جزءاً لا يتجزأ من النتائج التشغيلية لمنظمة معينة. ليست كل الاختراقات السيبرانية تشكل هجمات؛ في الواقع الغالبية العظمى ليست كذلك. قد يكون للهجمات السيبرانية آثار مؤقتة أو دائمة؛ قد تكون مدمرة للمعدات أو تؤدي فقط إلى تعطيل الخدمات؛ ويمكن إجراؤها عن بعد أو عن طريق الوصول القريب.

في الواقع، جرى تصميم الهجمات الإلكترونية بشكل متزايد لسرقة المعلومات بصمت دون ترك أي ضرر قد يلاحظه المستخدم. تحاول هذه الأنواع من الهجمات الهروب من الاكتشاف من أجل البقاء على الأنظمة المضيفة لفترات أطول من الوقت.

يمكن أن يكون للهجمات السيبرانية على شبكات المعلومات الوطنية عواقب وخيمة، مثل تعطيل العمليات الحساسة، أو التسبب في خسارة الإيرادات والملكية الفكرية، أو فقدان الأرواح. تميل الفروق بين الجريمة والإرهاب والحرب إلى التعتيم عند محاولة وصف هجوم على شبكة الكمبيوتر بطرق موازية للعالم المادي. على سبيل المثال، إذا قامت دولة قومية برعاية جهات فاعلة غير حكومية سراً، والتي تبدأ عملية لدعم الأنشطة الإرهابية أو لإحداث اضطراب اقتصادي، يصبح التمييز بين الجرائم السيبرانية والحرب السيبرانية أقل وضوحا. نظرا لأنه من الصعب معرفة مصدر الهجوم السيبراني، فقد يوجه المهاجم شكوكه تجاه طرف أخر بريء. وبالمثل، قد تؤدي التفاعلات بين الإرهابيين والمجرمين الذين يستخدمون تكنولوجيا الكمبيوتر في بعض الأحيان إلى طمس التمييز بين جرائم الإنترنت والإرهاب السيبراني. قد يكون الأمر كذلك أن الأفراد الذين يقدمون خبرة الكمبيوتر لمجرم أو إرهابي قد لا يكونون على دراية بنوايا الفرد الذي طلب الدعم. حتى الآن، ما يزال من الصعب تحديد المصادر المسؤولة عن معظم

الهجمات المزعجة والمعقدة بشكل متزايد التي ابتلي بها الإنترنت. نظرا لصعوبة تحديد مصدر الاختراقات أو الهجمات السيبرانية، يجادل البعض بأنه على عكس الرد على الأعمال الإجرامية التقليدية، يجب أن يكون التركيز على الفعل بدلاً من الجاني، كما ينبغي خفض عتبة شن الإجراءات الدفاعية والهجومية.

تتطلب مواجهة مثل هذه الهجمات تطوير قدرات قوية لتقليل نقاط الضعف وردع أولئك الذين لديهم قدرات ونية لإلحاق الضرر بالبنى التحتية الحيوية للدولة.

خصائص وسمات الهجمات السيبرانية

وفي سبيل معرفة الفضاء السيبراني بتركيز أكبر يذكر في هذا الصدد الباحثين المختصين عددا من الخصائص المميزة للهجمات السيبرانية، وهي كالتالي :

- لا يحتاج المهاجمون إلى أن يكونوا قريبين ماديا من أهدافهم لارتكاب هجوم سيبراني.

- تسمح التكنولوجيا للإجراءات بعبور حدود الدولة الوطنية المتعددة بسهولة.

- يمكن تنفيذ الهجمات تلقائيا وبسرعة عالية ومن خلال مهاجمة عدد كبير من الضحايا في نفس الوقت.

- يمكن للمهاجمين أن يظلوا مجهولي الهوية بسهولة أكبر.

المطلب الثالث: السلاح السيبراني (Cyber Weapon)

السلاح السيبراني هو وكيل برمجيات ضارة يُستخدم لأهداف عسكرية أو شبه عسكرية أو استخبارية كجزء من هجوم سيبراني.

الأسلحة السيبرانية هي ذخائر خفية، مكتوبة بالأصفار والآحاد، مثل كل أكواد الكمبيوتر. يمكنهم اختراق شبكات كاملة أو إصابة أجهزة كمبيوتر فردية. لديها الاستطاعة في إرباك قدرات العدو، وإيقاف الهجمات العسكرية قبل حدوثها، وإعاقة أنظمة الاتصال، كل ذلك بدون وميض أسلحة الحرب التقليدية. إنها كأسلحة تعتمد على نقاط الضعف في البرامج، وسوء الترتيب الإلكتروني، والأشخاص الذين يفتحون عن غير قصد مرفقات مصابة ببرامج ضارة.

الجهة الراعية

يتمثل جزء من التمييز عن البرامج الضارة الأخرى في أن الوكيل تتم رعايته -أي، تم انشاؤه أو تطويره أو استخدامه- ليس من قِبل متسلل يمارس القرصنة أو جماعة إجرامية منظمة، وانما بدلا لذلك من قبل دولة أو جهة فاعلة غير حكومية، يحتمل أن تتضمن الأخيرة الجماعات الإرهابية والجهات الفاعلة الأخرى المدرجة في مذاهب حروب الجيل الخامس GW.

في سبتمبر العام ٢٠١٨، أصدرت وزارة الدفاع الأمريكية خطة إستراتيجية لم تؤكد خلالها فقط وجود وامتلاك أسلحة سيبرانية ولكنها أعلنت التزامها باستخدامها "لتعزيز المصالح الأمريكية" والدفاع عنها. كان الهجوم السيبراني على إيران في حزيران/ يونيو ٢٠١٩ دليلا على هذا النهج الجديد الأكثر عدوانية."

في العام ٢٠١٨، أعطى البنتاغون للقيادة السيبرانية مكانة مساوية للأوامر القتالية

الأخرى، والتي تشمل القيادة المركزية وقيادة العمليات الخاصة، وهو مؤشر على الأهمية المتزايدة للإنترنت كمجال استراتيجي وأصل عسكري.

في الماضي، كان التهديد بالدمار المتبادل المؤكد هو الطريقة التي تبقي بها القوى النووية قدرات بعضها البعض الفتاكة تحت السيطرة. قد تقدم الأسلحة السيبرانية بعض الضمانات نفسها، ولكن فقط إلى حد ما. فعلى عكس الأسلحة النووية، باهظة الثمن والمملوكة من قبل عدد قليل من الدول، فإن الأسلحة السيبرانية رخيصة ومتاحة على نطاق واسع، ليس فقط للدول القومية ولكن للمجرمين والجهات الفاعلة الشريرة. وعلى عكس الأسلحة التقليدية، التي يمكن تتبع مسارها بسهولة، فإن الأسلحة السيبرانية، التي تتحرك عبر كابلات الألياف الضوئية التي تنتشر عبر وحول العالم، تسمح لمستخدمها بالإنكار المعقول. ومن ثم، كيف تفرض تهديدا عندما لا يكون واضحا من أين يأتي الهجوم أو من المسؤول عنه؟ يمكن أن يكون تأثير الهجوم السيبراني بعيد المنال في الواقع، جعلت إدارة ترامب السابقة، وعلى رأسها بولتون، العمليات السيبرانية الهجومية ذراعا لا يتجزأ من فن الحكم. وهكذا، يبقى السؤال مفتوحا حيال الأسلحة السيبرانية ما إذا كانت ستصبح أيضا أسلحة فتاكة في الحرب.

المطلب الرابع: القوة السيبرانية (Cyber Power)

إذا كان الفضاء السيبراني هو المجال الذي يمكن فيه إنشاء المعلومات وتخزينها ونقلها ومعالجتها بشكل عام، فإن القوة السيبرانية هي عملية تحويل المعلومات إلى تأثير استراتيجي. يتجلى هذا التأثير الاستراتيجي في نهاية المطاف في العمليات المعرفية البشرية، ولكن يمكن أيضا أن يتجلى بشكل غير مباشر في المجالات الاستراتيجية للبر والبحر والجو والفضاء، وكذلك الفضاء السيبراني نفسه.

إن أهمية الفضاء السيبراني منتشرة في كل مكان في عصرنا الحالي: من دوره في الاقتصادات الوطنية وفي التجارة والنقاش السياسي إلى استخدامه كأداة للإكراه والتجسس، ومركزيته المتصورة كأحد محددات النجاح في الحرب. وهكذا، مع تزايد استفادة الجهات الفاعلة الحكومية وغير الحكومية من القدرات السيبرانية لتحقيق أهدافها الاستراتيجية، تزداد المنافسة في الفضاء السيبراني على القواعد التي تحكمه.

تعريف القوة السيبرانية:

بالمقارنة مع الفضاء السيبراني، هناك تعريفات أقل نسبيا للقوة السيبرانية. تؤكد تعريفات القوة السيبرانية على كيفية استخدام الفضاء السيبراني لتحقيق أهداف استراتيجية. تؤكد إحدى فئات التعريفات على أداة القوة السيبرانية دون مناقشة العملية الجدلية لممارسة تلك القوة في مواجهة الخصم. تقر الفئة الأخرى من التعريفات باستخدام القوة السيبرانية ضد خصم متعمد وذكي من المحتمل أن يحاول أيضا استخدام القوة السيبرانية لتحقيق غاياته الخاصة. وتتراوح بعض هذه التعريفات بما يلي:

- وفقا لما ذكره " دانيال كويهل" يتم تعريف القوة السيبرانية على انها القدرة على استخدام الفضاء السيبراني لخلق مزايا والتأثير على

الأحداث في جميع البيئات الوظيفية وعبر أدوات القوة.

- يستخدم "جوزيف ناي" استعارة لتعريف القوة السيبرانية واصفا إياها من حيث مجموعة من الموارد التي تتعلق بإنشاء والتحكم والاتصال في البنية التحتية للمعلومات الإلكترونية والحاسوبية والشبكات ومهارات البرمجيات البشرية. وهذا لا يشمل فقط إنترنت أجهزة الكمبيوتر المتصلة بالشبكة. ولكن أيضا الشبكات الداخلية والتقنيات الخلوية والاتصالات الفضائية، قائلا: القوة السيبرانية هي القدرة في الحصول على النتائج المفضلة من خلال استخدام موارد المعلومات المترابطة إلكترونياً في المجال السيبراني.

- في حين ذكر " كريس ديمشاك " ان القوة السيبرانية هي القدرة الوطنية على تعطيل الفاعل السيئ المحجوب في مكان ما في العالم الرقمي سواء كان دولة أو غير حكومي، بما يتناسب مع دوافعها/قدراتها للهجوم بآثار عنيفة ومع ذلك تكون مرنة ضد المفاجآت السيئة المفروضة أو المحسّنة عبر جميع جوانب الاستدامة الوطنية الحاسمة الأنظمة.

- وفي نفس الوقت ذكر " ديفيد بيتز" و"تيم ستيفنز" بأن القوة السيبرانية يمكن فهمها على أنها مجموعة متنوعة من القوى التي تنتشر في الفضاء السيبراني والتي تشكل تجارب أولئك الذين يتصرفون في الفضاء السيبراني ومن خلاله ... وبالتالي فإن القوة السيبرانية هي مظهر من مظاهر القوة في الفضاء السيبراني وليست جديدة أو مختلفة شكل من أشكال القوة.

القوة السيبرانية هي قدرة منظمة للمجتمع على الاستفادة من التكنولوجيا الرقمية للمراقبة والاستغلال والتخريب والإكراه في النزاعات الدولية. يمكن للمجتمع الذي يتمتع بقوة سيبرانية كبيرة أن يشارك في عدد كبير من الإجراءات: يمكنه استغلال الدول الأخرى أو تقويضها اقتصاديا؛ جمع المعلومات الاستخبارية السياسية والعسكرية بشكل أكثر كفاءة من التجسس الرقمي السابق؛ التدخل في الخطاب السياسي الأجنبي عبر الإنترنت؛ تحطيم القدرات القتالية للعدو؛ تخريب البنية التحتية الحيوية والإنتاج الصناعي الضخم، وحتى التسبب في خسائر بشرية كبيرة. كل هذا يمكن أن يتم من خلال التطبيق الذكي للتكنولوجيا الرقمية وبدون ضرورة نشر قوات عسكرية أو جواسيس بشريين.

بالنظر إلى تذكرة الدخول الرخيصة إلى نادي القوة السيبرانية، فمن المنطقي ألا تسرع القوى العظمى فحسب، بل الدول الصغيرة بشكل خاص، في تطوير قوات إلكترونية عسكرية. اعتبارا من اليوم، من المفترض لأكثر من ١٠٠ دولة أن تنشئ وتحافظ على جيوش سيبرانية، وهذا لا يشمل التجسس الرقمي، وانما لتكون أداة تستخدم بشكل روتيني في فروع الدفاع التقليدية.

خصائص وسمات القوة السيبرانية:

وبالمثل، يمكن استنتاج وتحديد خصائص معينة للقوة السيبرانية:

١- القوة السيبرانية منتشرة. إن القوة البرية والبحرية والجوية والفضائية قادرة على إحداث تأثير استراتيجي على كل مجال من المجالات الأخرى، ولكن لا شيء يولد تأثيرا استراتيجيا

في جميع المجالات بشكل مطلق ومتزامن مثل القوة السيبرانية. تعتبر الاثار السيبرانية أمرا واقعيا في الجيش والاقتصاد والمجتمع في عدد متزايد من البلدان، وهي تُمكّن بشكل حاسم القوة البرية والبحرية والجوية والفضائية- بالإضافة إلى أدوات القوة الأخرى، مثل الدبلوماسية والإعلام، والتجارة.

٢- القوة السيبرانية مكملة. على عكس القوة البرية والبحرية والجوية، ولكن من نواح كثيرة نسبيا مثل القوة الفضائية، فإن القوة السيبرانية هي إلى حد كبير أداة تكميلية. إنها غير مباشرة لأن القدرة القسرية للقوة السيبرانية محدودة ومن المرجح أن تظل محدودة. إن إغلاق شبكة الطاقة عبر القوة السيبرانية، على سبيل المثال، سيكون له بلا شك عواقب وخيمة، ولكن بدلا من إجبار ضحيته على التنازل لصالح مطالب المهاجم، قد يؤدي في الواقع إلى استجابة أكثر كارثية.

٣- يمكن أن تكون القوة السيبرانية متخفية. أحد عوامل الجذب للقوة السيبرانية للعديد من المستخدمين هو القدرة على استخدامها خلسة على نطاق عالمي دون أن تُنسب إلى الجاني الفعلي. يمكن زرع البرامج الضارة في شبكات العدو دون علم حتى يتم تنشيط السلاح السيبراني ويسبب الضرر المقصود به. يمكن مداهمة قواعد البيانات للحصول على معلومات سرية أو خاضعة للملكية، وقد لا يكون مالكو هذه المعلومات أكثر حكمة حيث يتم سرقة تيرابايت من البيانات. وبالمثل، يمكن للمواطنين العاديين ممارسة حياتهم اليومية فقط ليكتشفوا أن مجرمي الإنترنت قد استخدموا بطاقات الائتمان الخاصة بهم أو الحقوا الضرر بتصنيفهم الائتماني عبر سرقة هويتهم. هذه القدرة على استخدام القوة السيبرانية خلسة، مدعومة بالصعوبات الكامنة في تحديد هوية ودوافع معظم المهاجمين، تجعلها أداة جذابة للغاية لأولئك الذين يرغبون في القيام بأنشطة سرية مشينة.

المطلب الخامس: الحرب السيبرانية (Cyber Warfare)

في أوائل عام ٢٠١٠، أكد مدير المخابرات الامريكية السابق الأدميرال مايك ماكونيل قائلا: "الولايات المتحدة تخوض حربا سيبرانية اليوم، ونحن نخسر. الأمر بهذه البساطة" (ماكونيل ٢٠١٠). ماكونيل من بين العديد من المختصين والمؤلفين الذين يستخدمون مصطلح الحرب السيبرانية أو الصراع السيبراني لوصف مجموعة من الأنشطة المشينة التي تحدث في الفضاء السيبراني كل يوم. تتراوح الغالبية العظمى من هذه الأنشطة من صغار القراصنة المتسللين الذين يستعرضون مهاراتهم إلى الاحتجاج السياسي والمعارضة عبر الإنترنت، إلى النشاط الإجرامي والتجسس؛ ولكن عدد قليل جدا من الهجمات السيبرانية يمكن وصفها بأنها هجمات سيبرانية فعلية قد تسبب ضررا خطيرا للأمن القومي للدولة. هذا لا يعني إنكار أن مقالب القراصنة وعمليات التسلل هي مزعجة، بل وخطيرة، أو أن الجريمة والتجسس التي تتم بوسائل إلكترونية ليست قضايا مهمة تحتاج إلى سياسة متماسكة واستجابة صلبة. ومع ذلك، هناك سؤال حول ما إذا كانت هذه الأنشطة تشكل معا حربا سيبرانية؟؟ ومن ثم، فهي تسترعي نوع الاستجابة التي قد تحتاجها الحرب.

مع ذلك، يجـادل بعض المختصين، بأن ظهور الفضاء السيبراني قد غيّر طبيعة الحرب بشكل كبيـر، مما جعـل أي حادثة إلكترونية شـريرة تُرتكـب ضد دولة أو مجتمعها أو اقتصادها يعد بمثابـة نمطا جديدا من أنماط الصراع. غالبا ما يُنظر إلى الفاعلين الذين لديهم شـكل من أشكال العداء تجاه هدفهم بأنهم يخلقون حادثة إلكترونية لإكراه هذا الهدف في الإذعان لهدفهم السياسـي على أنهـم منخرطون في الحرب السـيبرانية. وفي هذا السـياق يصف "كريس ديمشاك" هذا الوضع الناشـئ بأنـه تغيير في نمـط الصراع قائلا:

تنتقل طبيعة الحرب من الصدامات العنيفة التي تهدد المجتمع لمرة واحدة بين الجيران القريبين إلـى نسـخة عالمية من حـالات انعـدام الأمن المزمنـة والخطيرة بشـكل عرضـي وكارثي والتـي تشـمل المجتمـع بأسـره. "كريـس ديمشـاك" الحـرب السـيبرانية هي اسـتخدام الهجمـات الرقمية لمهاجمة دولة، مما يتسـبب في ضرر مماثل للحرب الفعلية وتعطيل أنظمة الكمبيوتر الحيوية. هناك جدل كبير بين الخبراء فيما يتعلق بتعريف الحرب السـيبرانية، وحتى إذا كانـت موجـودة بالفعل. أحـد الآراء هو أن مصطلح "الحرب السـيبرانية " تسمية خاطئة، حيـث لا يمكـن وصـف أي أعمـال إلكترونية هجومية حتى الآن على أنها "حرب".

بينمـا هناك جدل حول كيفيـة تعريف "الحرب السـيبرانية" واستخدامها كمصطلح، فإن العديد مـن البلـدان بما فـي ذلـك الولايـات المتحدة والمملكة المتحدة وروسـيا والصين وإسـرائيل وكوريا الشمالية وإيران لديهم قدرات سيبرانية نشطة للعمليات الهجومية والدفاعية.

تعريف الحرب السيبرانية:

هناك جدل مسـتمر حول كيفية تعريف الحرب السـيبرانية ولا يوجـد تعريـف مطلـق متفـق عليه بشـكل واسـع. في حين أن غالبية العلماء والمؤسسات العسكرية والحكومات يستخدمون تعريفات تشـير إلـى الدولة والجهـات الفاعلة التي ترعاها الدولة، ولكن وفي الوقت نفسـه قد تشـمل التعريفات الأخرى الجهات الفاعلة غير الحكومية، مثل الجماعات الإرهابية أو الشركات أو المتطرفيـن السياسـيين أو الأيديولوجييـن. وكذلك نشطاء القرصنة والمنظمات الإجرامية عبر الوطنية اعتمادا على سياق العمل.

وفيما يلـي أمثلة على التعاريـف التي اقترحها المختصين في هذا المجال:

- وفقـا لما ذكـره الدكتور "كيث سـكوت" في بحثه "صراع مسـتمر ومتواصل: نحو نموذج سيبراني للحرب" يتم تعريف الحرب السيبرانية بأنها: تُسـتخدم "الحرب السـيبرانية" في سياق واسع للإشـارة إلى الاستخدام المشـترك للقوة التكنولوجية داخل شـبكات الكمبيوتر حيث يتم تخزيـن المعلومات أو مشـاركتها أو نقلها عبر الإنترنت.

-ركـز باركس ودوغـان على تحليـل الحرب السيبرانية من حيث شبكات الكمبيوتر وأشاروا إلى أن "الحرب السـيبرانية عبـارة عن مزيج من هجوم شبكات الكمبيوتر والدفاع والعمليات التقنية الخاصة."

- قـدم باولـو شـاكاريان وزمـلاؤه التعريـف التالي مسـتمدا من تعريف كلاوزفيتز للحرب: "الحرب هي استمرار للسياسة بوسائل أخرى:

"الحرب السيبرانية هي امتداد للسياسة من خلال

الإجراءات المتخذة في الفضاء الإلكتروني من قبل جهات فاعلة حكومية (أو من قبل جهات فاعلة غير حكومية لديها توجيه أو دعم مهم من الدولة) والتي تشكل تهديدا خطيرا لأمن دولة أخرى، أو إجراء من نفس الطبيعة يتم اتخاذه ردا على تهديدا محتملا لأمن الدولة نفسها ".

- بينما قدمت البروفيسور تادو التعريف التالي:

"ترتكز الحرب السيبرانية على استخدامات معينة لتكنولوجيا المعلومات والاتصالات في إطار استراتيجية عسكرية هجومية أو دفاعية أقرتها الدولة وتهدف إلى تعطيل موارد العدو أو السيطرة عليها فورا، والتي تشن في بيئة المعلومات، مع وكلاء وأهداف تتراوح بين المجالات المادية وغير المادية والتي قد يختلف مستوى العنف فيها حسب الظروف ".

- في حين أقترح روبنسون وزملاؤه أن نية المهاجم تحدد ما إذا كان الهجوم حربا أم لا، ومن ثم، عرّف الحرب السيبرانية على أنها "استخدام الهجمات الإلكترونية بقصد شبيه بالحرب."

- يُعرِّف المنسق القومي الأمريكي السابق للأمن وحماية البنية التحتية ومكافحة الإرهاب، ريتشارد كلارك، الحرب السيبرانية على أنها "إجراءات من قبل دولة قومية لاختراق أجهزة الكمبيوتر أو الشبكات الخاصة بدولة أخرى بغرض إحداث ضرر أو تعطيل." قد يتم تسليح البنية التحتية المادية الإلكترونية الخاصة بها واستخدامها من قبل الخصم في حالة حدوث نزاع إلكتروني، وبالتالي تحويل هذه البنية التحتية إلى أسلحة تكتيكية.

الجدل حول المصطلح

هناك جدل حول مدى دقة مصطلح "الحرب السيبرانية". ويخلص "يوجين كاسبيرسكي" -مؤسس شركة كاسبرسكي لاب- إلى أن "الإرهاب السيبراني " مصطلح أكثر دقة من "الحرب السيبرانية". ويذكر أنه "مع هجمات اليوم، فأنت جاهل بشأن من قام بذلك أو متى سيضرب مرة أخرى. إنها ليست حربا سيبرانية، بل إرهابا سيبرانيا". وفي ذات السياق ذكر "هوارد شميت" منسق الأمن السيبراني السابق في إدارة أوباما قائلا: "لا توجد حرب سيبرانية... أعتقد أن هذه استعارة مروعة وأعتقد أن هذا مفهوم مروع. إذ لا يوجد فائزون في تلك البيئة."

الدوافع

هناك عدد من الأسباب التي تدفع الدول إلى القيام بعمليات إلكترونية هجومية. دعا خبير الأمن السيبراني ومستشار الناتو "ساندرو جايكن" الدول إلى التعامل مع الحرب السيبرانية على محمل الجد حيث ينظر إليها على أنها نشاط جذاب من قبل العديد من الدول، في أوقات الحرب والسلام. تقدم العمليات السيبرانية الهجومية مجموعة كبيرة ومتنوعة من الخيارات الرخيصة والخالية من المخاطر لإضعاف البلدان الأخرى وتقوية مواقع الدول المهاجمة. بالنظر إلى منظور جيوستراتيجي طويل الأجل، يمكن للعمليات الهجومية السيبرانية أن تشل الاقتصادات بأكملها، وتغير وجهات النظر السياسية، وتثير الصراعات داخل الدول أو فيما بينها، وتقليل كفاءتها العسكرية، وتعادل قدرات الدول ذات الاقتصاد والقدرات العسكرية العالية مع قدرات الدول

منخفضة الاقتصاد والقدرات العسكرية الفعلية، ويستخدمون الوصول إلى البنى التحتية الحيوية لابتزازهم.

عسكريا:

مع ظهور الإنترنت كتهديد كبير للأمن القومي والعالمي، أصبحت الحرب السيبرانية والهجمات السيبرانية أيضا مجال اهتمام وتركيز للجيش والقوات العسكرية.

في الولايات المتحدة، يعتبر استحداث القيادة السيبرانية باعتبارها أحدث مقاتل عالمي ومهمتها الوحيدة هي الفضاء السيبراني، خارج ساحات القتال التقليدية البرية والبحرية والجوية والفضائية". وستحاول القيادة السيبرانية إيجاد، وعند الضرورة، تحييد الهجمات الإلكترونية والدفاع عن شبكات الكمبيوتر العسكرية.

نظرا لأن الجيش والقوات المسلحة أصبحت أكثر فأكثر متورطة في التهديد الوطني والعالمي الذي يقترحه استخدام المجال السيبراني، فقد ظهر ببطء مجال بحثي جديد في مجال العلوم العسكرية. في الأساس، ينصب تركيزهُ على وصف وفهم وشرح ماهية العمليات العسكرية السيبرانية وما يمكن القيام به ومعالجتها. في كتيب العلوم العسكرية، يعرّف "آرون برانتلي" و"ماكس سميتس" العمليات العسكرية السيبرانية على أنها "العمليات السيبرانية التي يخطط لها وينفذها كيان عسكري تابع لدولة قومية لتحقيق مكاسب إستراتيجية أو عملياتية أو تكتيكية". أكثر من ذلك، يجادلون بأن هذه الأنواع من العمليات العسكرية تنقسم عادة إلى ثلاثة أنواع من العمليات وهي العمليات السيبرانية الدفاعية وعمليات التجسس السيبراني والعمليات السيبرانية الهجومية.

شكوك حول وجود مفهوم الحرب السيبرانية

في أكتوبر ٢٠١١، نشرت مجلة الدراسات الاستراتيجية، وهي مجلة رائدة في هذا المجال، مقالًا بقلم "توماس ريد" بعنوان "الحرب السيبرانية لن تحدث" والذي جادل فيه بأن جميع الهجمات السيبرانية ذات الدوافع السياسية هي مجرد نسخ متطورة من التخريب أو التجسس أو التدمير، وأنه من غير المحتمل أن تحدث حرب سيبرانية في المستقبل. وأضاف أنه من المضلل استخدام هذا المصطلح واقترح بدلا عنه استخدام "القوة السيبرانية في الحرب، أو الحرب بالوسائل السيبرانية"

وهكذا يمكننا ان نخلص إلى الافتراض بأن تعريفات كل من الفضاء السيبراني والهجوم السيبراني والسلاح السيبراني والقوة السيبرانية والحرب السيبرانية هي في مرحلة جنينية من الناحية المفاهيمية، مما يترك الاستراتيجيين مشغولين في فرز ما هو صحيح وما هو خطأ وما هو قابل للنقاش بشكل بارز. قد تدفع هذه الحالة البعض إلى القول بأن الفضاء السيبراني كمجال استراتيجي ليس غير ناضج فحسب، بل ربما لا يستحق النظر فيه ضمن التيار الرئيسي للدراسات الاستراتيجية. كلا الافتراضين سيكون خطأ. كمجال استراتيجي، فإن الفضاء السيبراني نشطا بطرق متنوعة منذ سنوات عديدة حتى الآن. نظرا لانتشار الفضاء السيبراني في كل جانب من جوانب الحياة الحديثة، فإن أعماله وديناميكياته هي الأكثر أهمية للدراسات الاستراتيجية ولأي استراتيجي ممارس. وكذلك، كان البشر يقاتلون في البر والبحر لعدة قرون قبل أن يأتي المنظرون

الاستراتيجيون لتحديد تلك الأنشطة وجعلها ذات مغزى للخطاب السياسي. لماذا يجب أن يكون الفضاء السيبراني مختلفا؟

المبحث الثاني: بُعد جديد للصراع

مع وجود ما يقرب من ثلاث مليارات مستخدم جنبا إلى جنب مع الانتشار المتزايد للفضاء السيبراني في المجتمعات، فليس من المستغرب أن يصبح الفضاء السيبراني مكانا للصراع المستمر، مما يؤدي إلى الاضطراب والخداع والسرقة. في حين أن الصراع هو سمة دائمة الوجود للفضاء السيبراني، فليس كل النزاعات هناك تعادل ما قد يعتبره الكثيرون حربا بالمعنى الكلاسيكي الذي قدمه كلاوسفتز والقاضي بأن الحرب هي عمل من اعمال القوة لتحقيق هدف السياسة. في الواقع، فان الخلافات في الفضاء السيبراني تنطوي على ثأر شخصي، وتنافسات تنظيمية، ومواطنين مدفوعين بدافع الهوية وما شابه.

نظرا لأن الفضاء السيبراني تُهيمن عليه الجريمة في الوقت الحالي، يمكن القول بإن الميزة التفضيلية في الصراع السيبراني لصالح المهاجم. نتيجة لذلك، قد يبدو أن الفضاء السيبراني هو بيئة غنية بالأهداف لأي مهاجم محتمل، على الرغم من أنه يجب ملاحظة أن الهجوم السيبراني لا يخلو من مشاكله وتحدياته. يعتقد بعض العلماء أن سهولة الهجوم السيبراني على أهداف حيوية للأداء اليومي للمجتمعات الحديثة يبشر بعصر من الاضطراب الدائم، والذي لا يمكن التخفيف من آثاره إلا من خلال التركيز على المرونة في شبكات البنى التحتية الحيوية والتخزين ونقل المعلومات الحساسة.

المطلب الأول: مشكلة الأمن السيبراني

في الفضاء السيبراني، تتمتع الهجمات بميزة على الدفاع، وبالتالي فإن التحدي الذي يواجه المهتمين بالأمن السيبراني هو أن يكونوا ناجحين في الحفاظ على دفاعاتهم طوال الوقت وهو توقع مستحيل الوفاء به إلى أجل غير مسمى. بالنسبة لأي مهاجم إلكتروني محتمل، يكون التحدي أسهل بكثير من نواحٍ عديدة، يجب أن ينجح مرة واحدة فقط في مهاجمة نظام أو شبكة مستهدفة.

يعاني الأمن السيبراني أيضا من مشكلة الإسناد. غالبا ما يُشار إلى غموض هوية وموقع الجهات الفاعلة باسم "مشكلة الإسناد". يمكن إخفاء الهجمات السيبرانية وتوجيهها عبر بلدان مختلفة، وحتى تصميمها لإعطاء مظهر من مكان آخر غير نقطة الإطلاق الأصلية. بالنسبة لأي ضحية لهجوم سيبراني، فإن هذا يجعل من الصعب عزو الهجوم السيبراني إلى مرتكبه الحقيقي، مما يحد من فرص توجيه اللوم أو صياغة رد قد يشمل هجوما إلكترونيا انتقاميا أو حتى استخدام القوة العسكرية. إن توجيه اللوم وصياغة استجابة مناسبة للهجوم السيبراني يمثل مشكلة لأن الإسناد قد يكون صعبا للغاية.

الإسناد هو أكثر من مجرد تحديد الموقع الجغرافي للهجوم الإلكتروني. كما أنه يتعلق بإسناد هوية المهاجم ودوافعه للهجوم. لمجرد أن الهجوم الإلكتروني قد يُنسب إلى أنه قد نشأ من بلد معين، فهذا لا يعني بالضرورة أن أولئك الذين نفذوا الهجوم فعلوا ذلك بعلم وتفويض من حكومة ذلك البلد، أو أن الهجوم المعني كان يقصد بالفعل أن يكون عملا من أعمال الحرب. من الصعب للغاية التحقق بشكل موثوق من

تحديد هوية المهاجم ودوافعه، وهو ما يعيق مرة أخرى إسناد المسؤولية عن هجوم إلكتروني، فضلاً عن صياغة الرد المناسب. على سبيل المثال، يمكن أن يُعزى الهجوم السيبراني إلى أنه قد نشأ من بلد معين، لكن أدوات وأساليب التحليل الجنائي السيبراني غير قادرة على التأكد بشكل موثوق مما إذا كان الهجوم المعني قد تم تنفيذه بواسطة عصابة لأغراض إجرامية أو بواسطة عملاء من حكومة ذلك البلد لأغراض التجسس مدفوعة بغايات سياسية.

نظرا للتحديات الكبيرة التي ينطوي عليها الأمن السيبراني، إلى جانب الميزة الهجومية التي تتمتع بها الهجمات السيبرانية، فقد روج عدد من العلماء لفكرة الردع السيبراني كوسيلة لمنع الهجمات السيبرانية الكارثية. لا يوجد سوى الردع. ومع ذلك، ما تزال الفكرة القائلة بإمكانية ردع الهجمات السيبرانية لها ما يُعيقها، اعتمادا على استراتيجية الردع المستخدمة. يركز جزء كبير من الأدبيات المتعلقة بالفضاء السيبراني والردع على استراتيجيات العقاب، حيث يعاقب الهجوم السيبراني بهجوم سيبراني انتقامي أو أي رد عسكري أو دبلوماسي أو اقتصادي آخر. تكمن مشكلة استراتيجية الردع بالعقوبة في أنها تفترض ليس فقط أن الضحية للهجوم الإلكتروني سيكون قادرا على تحديد موقع مصدر الهجوم، ولكن أيضا تفترض هويات المهاجمين ودوافعهم. بالنظر إلى أن الإسناد ما يزال يمثل تحديا كبيرا، فإن استراتيجية الردع بالعقاب في الفضاء السيبراني لا يمكن الاعتماد عليها وتنطوي على درجة عالية من المخاطر ليس فقط في رد الفعل المفرط على أي هجوم، ولكن حتى سوء التقدير الكامل الذي قد يؤدي إلى معاقبة أطراف أخرى بريئة.

وهكذا يمكن ان نخلص الى القول بأن الأمن السيبراني -أو الدفاع السيبراني- يمثل تحديا استثنائيا بسبب الميزة الهجومية التي يتمتع بها المهاجمون السيبرانيون. كما ان تحديد هوية المهاجم ودوافعه يمثل تحديا خاصا ويمكن أن يعيق الاستجابة الفعالة.

المطلب الثاني: تطبيق القانون الدولي

لا توجد طريقة للتأكد من كيفية تطبيق المجتمع الدولي لمبادئ القانون الدولي على هجمات شبكات الكمبيوتر. كما هو الحال مع التطورات الأخرى في القانون الدولي، سيعتمد الكثير على كيفية استجابة الدول والمؤسسات الدولية للظروف الخاصة التي تُثار فيها هذه القضايا لأول مرة.

إذا اقتصرنا على لغة المادة ٥١ من ميثاق الأمم المتحدة، فإن السؤال الواضح سيكون، "هل تشُن شبكة الكمبيوتر" هجوما مسلحا "يبرر استخدام القوة في الدفاع عن النفس؟"

إذا ركز المرء على الوسائل المستخدمة، فقد نستنتج أن الأعمال الإلكترونية غير المحسوسة بالنسبة للحواس البشرية لا تشبه القنابل أو الرصاص أو القوات. من ناحية أخرى، يبدو من المرجح أن المجتمع الدولي سيكون مهتما بعواقب الهجوم على شبكة الكمبيوتر أكثر من اهتمامه بآليته. قد يكون من الصعب الترويج لفكرة أن الاقتحام غير المصرح به لنظام معلومات سري، يشكل هجوما مسلحا. لكن، من ناحية أخرى، إذا أدى هجوم منسق على شبكة الكمبيوتر إلى إغلاق نظام مراقبة الحركة الجوية لدولة ما إلى جانب أنظمتها المصرفية والمالية والمرافق العامة، وفتح بوابات العديد

من السـدود مما يـؤدي إلى حـدوث فيضانات عامة تتسـبب في مقتل مدنيين على نطاق واسع وإلحـاق أضرار بالممتلكات، قـد لا يطعن أحد بـأن الدولة الضحيـة باعتبارهـا كانت ضحية لهجوم مسلح، أو لعمل مماثل لهجوم مسلح.

حتى لـو كانت الأنظمـة التي تمـت مهاجمتها عبارة عن أنظمة لوجستية عسكرية غير سرية، فـإن الهجـوم على مثل هـذه الأنظمة قـد يهدد بشكل خطير أمن الدولة. إذ أن عواقب العمليات السيبرانية أكثر أهمية من الوسائل المستخدمة.

وهكـذا، أدى ظهـور الإنترنـت كمجال حربي إلى بذل جهـود لتحديد كيفية اسـتخدام الفضاء الإلكتروني لتعزيز السـلام. على سبيل المثال، تديـر لجنـة الحقـوق المدنيـة الألمانيـة حملة مـن أجل السـلام الإلكتروني - للسـيطرة على الأسلحة السـيبرانية وتكنولوجيا المراقبة وضد عسـكرة الفضاء السـيبراني وتطوير وتخزين المآثـر الهجوميـة والبرامـج الضارة. تشـمل تدابير السـلام السـيبراني صانعي السياسـات الذين يطـورون قواعد ومعايير جديدة للحرب، ويقـوم الأفراد والمنظمات ببنـاء أدوات جديدة وبنـى تحتية آمنة، وتعزيز المصادر المفتوحة، وإنشـاء مراكز الأمـن السـيبراني، ومراجعة الأمـن السـيبراني للبنيـة التحتيـة الحيويـة، والالتزامـات بالكشـف عـن نقـاط الضعـف، ونزع السـلاح، واسـتراتيجيات الأمن الدفاعية واللامركزية والتعليم والتطبيق الواسع للأدوات والبنى التحتية ذات الصلة والتشفير والدفاعات الإلكترونية الأخرى.

وفي سبيل إيجاد منظور قانوني حاولت أطراف مختلفة التوصل إلى أطر قانونية دولية لتوضيح ما هـو مقبول وما هو غير مقبـول، لكن لم يتم قبول أي منها على نطاق واسع حتى الآن.

المطلب الثالث: القوة السيبرانية تعيد صياغة السياسة الدولية وانماط الصراع.

يؤثر انتشـار الفضاء السـيبراني وانتشار القوة السـيبرانية في كل مكان على العلاقات الدولية والدور المتميز للدولة في السياسة الدولية.

ساعد صعود القوة السيبرانية الدول النامية على تسـريع تنميتها الاقتصادية، مـع تمكين أدواتها العسكرية والدبلوماسية والثقافية لقوتها الوطنية. سمحت القوة السـيبرانية لعدد من الدول النامية بالتمتع بنمو اقتصادي كبير وزيادة متناسبة في فاعلية أدوات قوتهـا الوطنية. وبالتالي تمكينهم من اللحـاق بالـدول المتقدمة. وتعتبـر الصين والهنـد أفضـل تجلي لهـذه الظاهـرة، أعادت صياغـة توزيـع القوة داخـل السياسـة الدولية مما أدى إلى مكاسـب صافيـة للقوى الصاعدة، وخسائر نسبية للقوى التقليدية والمتقدمة.

أدى صعـود القوة السـيبرانية أيضا إلى تمكين الأفـراد والمنظمـات والجهـات الفاعلـة غير الحكومية، مما سـمح لهـم بالوصول إلى نطاق عالمي، وشـكل من أشـكال التأثير العالمي، لم يكـن متاحا لهم قبل عقود قليلة ماضية لأنه كان مكلفا للغاية أو يتجاوز قدراتهم التقنية.

يمكن للفضاء السـيبراني أيضـا تمكين الأفراد والجماعـات ذوي النوايا الحربية من اسـتخدام القدرات السيبرانية بشكل عدواني ضد الأهداف فـي جميع أنحـاء العالم، كما أوضح متسـللون مـن تنظيم داعـش الإرهابـي عندمـا اخترقوا واختطفوا بشكل مؤقت قدرات وسائل التواصل الاجتماعـي للقيـادة المركزيـة الأمريكيـة في كانون الثاني/يناير ٢٠١٥، وقد أدى هذا التمكين للأفـراد والجماعـات إلـى إعادة توزيـع القوة داخل السياسـة الدولية مما يقوض بشـكل أكبر

احتكار القوة الـذي تتمتع به الدول تقليديا. ومع ذلك، فإن هذا التمكين من خلال القوة السيبرانية لا يصـل إلى حد بعيد. إذ مـا تزال الدول تتمتع بقـدرات وإمكانيات للتوظيف وإبراز القوة التي هي خارج متنـاول الأفـراد والجماعات. على الرغم مـن أن العديد من الخبـراء يعتقدون أن القوة السـيبرانية تقوض بشكل كبير قوة الدولة مـن خلال إضعاف سـيادة الدولة، إلا أن الدول تجـد أيضا طرقـا مختلفـة لتأكيد سـيادتها في الفضاء السيبراني.

القـوة السـيبرانية هـي أداة اسـتراتيجية مفيدة حيث يمكن اسـتخدامها عالميا بدرجة معينة من عدم الكشـف عن هويتها في السـلام والأزمات والحرب. القوة السـيبرانية تتيـح الوصول الى العالميـة، وخلق القدرة علـى مهاجمة الأنظمة الحيويـة مثل البنيـة التحتية الوطنيـة عن بعد، وخداع الأفراد لإفشـاء المعلومات الحساسـة، وتعطيل الخدمات. مـن المحتمل أن تؤدي مثل هذه الهجمات وعمليات الخداع والاضطرابات التي تقوم بها القوة السيبرانية إلى تشويش التمييز بين السـلام والحرب. إن الإرهاب، واسـتخدام الإرهابييـن كـوكلاء مـن قبل الـدول، يطمس بالفعل هذا التمييز، لكن القوة السيبرانية تضيف إلى مـا قد يكـون غموضا خطيرا بين السـلام والحـرب. قد تدرك الـدول المعرضة لهجمات سـيبرانية لا حصـر لها تؤدي إلـى اضطراب مجتمعي كبيـر، أو تعاني من فقدان المعلومات الحساسـة المتعلقة بالدفاع الوطني، أنها ضحايا لأعمال تشكل مقدمة للحرب أو تستحق رد فعل عسكري. سوء الفهم وسوء التقدير من المخاطر الرئيسية في مثل هذه الظروف. بالنسبة لبعض المراقبين، تشـير هذه الاتجاهات إلى أننا ندخل عصرا من الاضطراب الدائم.

تخلـق القـوة السـيبرانية كفـاءات كبيـرة فـي كيفية تنظيم الأشـخاص للأنشـطة. تعمل القوة السـيبرانية أيضـا علـى تضخيم قـدرة الأفراد علـى التحكم فـي العمليات ونقـل كميات غير محدودة تقريبا من البيانـات عبر الكوكب دون أي تكلفـة تقريبـا، مما خلق فـرص لم يكن من الممكـن تصورها قبل عقـود قليلة فقط. بفضل القوة السـيبرانية وتأثيراتها يجري زيادة كفاءة الجيـوش الحديثـة أيضا، مما يؤدي إلى إنشـاء هياكل قوة أقل رشـاقة وقـدرات آلية أكثر، مما يعطي أولويـة لتجنيد المزيد مـن الأفراد ذوي المهـارات العالية. هناك بالفعـل اعتماد متزايد على القدرات والأنظمـة الآلية، مثل المركبات الموجهـة عن بعد، كمـا أن تكلفة التدريب حتى أقـل أفراد الخدمة رتبة تزداد بسـبب المهارات التقنيـة المعقدة المطلوبة فـي الجيوش الحديثة. الآثار المترتبة على اتجاهات القوة الإلكترونية هـذه داخـل الجيوش قابلـة للنقـاش، ولا يمكن فصلهـا عن سـياق كيف ومتـى ولأي غرض ستُسـتخدم القوة العسـكرية في القـرن الحادي والعشـرين. ومع ذلك، فمن المعقول أن نقترح أنه مع تغير التنظيم والبنية العسـكريين بسـبب انتشـار القوة السـيبرانية، قد يتغيـر أيضا متى وكيف سـيتم استخدام القوة العسـكرية. قد تبلغ هذه التغييـرات ذروتها في ثورة القرن الحادي والعشـرين في الشؤون العسـكرية إذا أدت إلى مذاهب عسكرية جديدة، وبُنى للقوة، وتغييرات في إدارة الحرب.

وهكـذا يمكن ان نخلـص الى القول بـأن القوة السيبرانية تعيد صياغة السياسة الدولية وانماط الصـراع. مرة مـن خلال المسـاعدة في إعادة توزيع القوة حيث سـاعدت القوة السيبرانية في تمكين الدول النامية من اللحاق بالدول المتقدمة

سـريعا، وكذلك سـاعدت القوة السـيبرانية في تمكيـن الأفـراد والمنظمات والجهـات الفاعلة غيـر الحكوميـة، ممـا سـمح لهـم بمزيـد من المشـاركة والتأثير في السياسـة الدولية. ومرة أخـرى، لا تؤثـر القوة السـيبرانية علـى بُنية القوة العسـكرية فحسـب، بل تؤثـر أيضا على كيفية اسـتخدامها وفي ظل أي ظروف. قد ينتج عنـه ثورة في الشـؤون العسـكرية فـي القرن الحادي والعشـرين. ومن ثـم، يعتقد البعض أن صعود القوة السـيبرانية يبشر بقدوم عصر من الاضطراب الدائم وتحول في أنماط الصراع.

الخاتمة:

يسـتمر الفضاء السـيبراني في الانتشار بشكل أعمق فـي كل وظيفة من وظائـف المجتمعات الحديثة في جميع أنحاء العالم. التفاعلات المعقدة واثارها التي تظهر في الفضاء السـيبراني تفيد المجتمعات بسـبب الاتصالات منخفضة التكلفة التي تسـهلها وبسبب الكفاءات وأتمتة الوظائف المملة التـي تخلقها وتمكنهـا. تخلق هذه الاثار والتفاعـلات المعقـدة أيضا مجموعـة من نقاط الضعـف فـي جميع أنحـاء المجتمـع الحديث. يمكن اسـتغلال هـذه الثغرات الأمنيـة من قبل أولئك الذين يعتزمون شن الهجمات السيبرانية.

نظـرا لأن المزيـد والمزيـد مـن وظائـف الحكومـة، بمـا فـي ذلك القـدرات العسـكرية والقيادة والسـيطرة، تعتمد بشـكل متزايد على الفضاء السـيبراني، يجب على الاسـتراتيجيين الاهتمـام بنقاط الضعف والفـرص التي يخلقها الفضـاء السـيبراني. يكمـن التحدي فـي إيجاد التوازن الصحيح بين الأمن السـيبراني المطلق وبين استخدام الفضاء الإلكتروني بشكل يجري خلاله تقييد الهجوم السيبراني الذي يخلق خطرا حقيقيا بشكل متزايد.

تقريبا كل جانب من جوانب الإسـتراتيجية في العالم المعاصر يتأثر ويتشكل بالقوة السيبرانية. الآثـار المترتبة علـى ذلك حتـى الآن لم تحدد بشكل كامل، ولهذا السبب فإن الفضاء السيبراني والقوة السـيبرانية لهمـا أهمية ومصلحة حيوية للاستراتيجيين والدراسات الاستراتيجية.

(References):

Reports:

Department of Defense Science Board:

1- Defense Science Board Task Force on Cyber Deterrence. WASHINGTON, DC. February 2017. P.2. https://tinyurl.com/mxbzj9m8

U.S. Department of Energy:

2- U.S. Department of Energy. "ELECTRICITY SUBSECTOR CYBERSECURITY RISK MANAGEMENT PROCESS." May 2012. https://tinyurl.com/4htdzhhh

United States Government Accountability Office:

3- Government Accountability Office (GAO). "CYBERSECURITY: Continued Attention Is Needed to Protect Federal Information Systems from Evolving Threats." 2010. https://tinyurl.com/3kp392hy

Bank for International Settlements

Defense in Information Warfare Operations." National Self-Defense. 2007. P.17. https://tinyurl.com/nah7zcfn

9- John Baylis, James Wirtz, and Colin S. Gray. "Strategy in the Contemporary World". Oxford University press, 5th Edition, 2016.

10- John Andrews. "The World in Conflict: Understanding the world›s trouble spots." 2015. https://tinyurl.com/4hftyafx

Conference Paper:

Cyberspace and International Politics Conference:

11- Marco Mayer. "International Politics in the Digital Age: Power Diffusion or Power Concentration?" University of Florence. September 2013.. https://tinyurl.com/4xdp8yns

Journals:

Journal of International Relations and Sustainable Development:

12- Ralph Langner. "Cyber Power - An Emerging Factor in National and International Security." Center for International Relations and Sustainable Development. https://tinyurl.com/t6k6ha2b

and International Organization of Securities Commissions:

4- Bank for International Settlements and International Organization of Securities Commissions. "Guidance on Cyber Resilience for Financial Market Infrastructures." June 2016. https://tinyurl.com/4y5sjrp3

National Academy of Sciences:

5- David Clark, Thomas Berson, and Herbert Lin. "At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues." National Academy of Sciences. https://tinyurl.com/2emb5hxk

CRS Report for Congress

6- John Rollins. Clay Wilson. "Terrorist Capabilities for Cyberattack: Overview and Policy Issues." Congressional Research Service. 2007. P.2. https://tinyurl.com/vdwkv2wr

Books:

7- A. Kiyuna and L. Conyers. "CYBERWARFARE SOURCEBOOK." April 2015. P.8. https://tinyurl.com/3y9xabnz

8- Demetrius Delibasis Fokas. "The Right of States to National Self-

The New Yorker:

18- Sue Halpern. “How Cyber Weapons Are Changing the Landscape of Modern Warfare.” Newyorker. July, 2019. https://tinyurl.com/4srmzkmw

Projects and Researchers:

19- Aaron Brantly and Max Smeets. “Military Operations in Cyberspace.” Springer. August 2020. PP.3-4. https://tinyurl.com/pzzyz6v3

20- Michael Robinson, Kevin Jones, Janicke Helge and Leandros Maglaras. “An Introduction to Cyber Peacekeeping.” April, 2018. P.1. https://tinyurl.com/5e68jjeu

21- Michael Robinson; Kevin Jones; Janicke Helge. “Cyber Warfare Issues and Challenges.” Journal of Computers and Security. P.15. https://tinyurl.com/3ppptyer

22- Robert Burris. “FUTURE OPERATING CONCEPT – JOINT COMPUTER NETWORK OPERATIONS.” AIR UNIVERSITY. 17 February 2010. https://tinyurl.com/wa92d4w

Articles:

Journal National Research Council:

13- William A. Owens, Kenneth W. Dam & Herbert S. Lin eds. “Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities.” National Research Council, Committee on Offensive Information Warfare, 2009. https://tinyurl.com/35fex423

The WIRED Journal:

14- Andy Greenberg. “The WIRED Guide to Cyberwar.” August 2019. https://tinyurl.com/465v9hnw

15- Ryan Singel. “White House Cyber Czar: ‹There Is No Cyberwar›.” Wired›s Epicenter blog. 2010. https://tinyurl.com/5rf8w6at

16- Scott Thil. “William Gibson, Father of Cyberspace.” 2011. https://tinyurl.com/btn47uc6

E-International Relations:

17- Clara Assumpção. “The Problem of Cyber Attribution Between States.” Charles University. May 2020. P.1. https://tinyurl.com/49seuewu

Colin S. Gray. “Strategy in the Contemporary World”. Oxford University press, 5th Edition, 2016. P.283

- Ibid.

- Ibid.

- Ibid.

- Ibid.

- Marco Mayer. “International Politics in the Digital Age: Power Diffusion or Power Concentration?” University of Florence. September 2013. P.9. https://tinyurl.com/4xdp8yns

- Sue Halpern. “How Cyber Weapons Are Changing the Landscape of Modern Warfare.” Newyorker. July, 2019. https://tinyurl.com/4srmzkmw

- John Baylis, James Wirtz, and Colin S. Gray. Op Cite. P.285.

- Ibid. P.285.

- Ibid. P.285.

- John Rollins. Clay Wilson. “Terrorist Capabilities for Cyberattack: Overview and Policy Issues.” Congressional Research Service. 2007. P.2. https://tinyurl.com/vdwkv2wr

- ibid.

- Robert Burris. “FUTURE OP-

23- John B. Sheldon. “Cyberwar.” Britannica. https://tinyurl.com/ap3r5y6e

24- Keith Breene. “Who are the cyberwar superpowers?” The World Economic Forum. https://tinyurl.com/3mxuttyb

25- Keith Scott. “Connected, Continual Conflict: Towards a Cybernetic Model of Warfare.” De Montfort University, UK. P.1. https://tinyurl.com/258hcybt

26- Raymond C. Parks and David P. Duggan. “Principles of Cyberwarfare.” IEEE Security & Privacy, vol. 9. pp.30-35. 2011. P.30. https://tinyurl.com/6y3aryd3

27- Veena Kumari. “CYBER LAW -I.” University of Lucknow, Faculty of Law. https://tinyurl.com/4ujvux2r

- Scott Thil. “William Gibson, Father of Cyberspace.” 2011. https://tinyurl.com/btn47uc6

- Veena Kumari. “CYBER LAW -I.” University of Lucknow, Faculty of Law. P.8. https://tinyurl.com/4ujvux2r

- Ibid. P.9.

- Ibid. P.3.

- John Baylis, James Wirtz, and

Infrastructures. June 2016. P.23. https://tinyurl.com/4y5sjrp3

Defense Science Board Task Force on Cyber Deterrence. WASHINGTON, DC. February 2017. P.2. https://tinyurl.com/mxbzj9m8

- John Rollins. Clay Wilson. Op Cite. P.17.

- Ibid. P.2.

- Ibid. P.23.

- Government Accountability Office (GAO). "CYBERSECURITY: Continued Attention Is Needed to Protect Federal Information Systems from Evolving Threats." 2010. P.3. https://tinyurl.com/3kp392hy

- John B. Sheldon. "Cyberwar." Britannica. https://tinyurl.com/ap3r5y6e

- Sue Halpern. Op Cite.

- Ibid.

- Sue Halpern. Op Cite.

- Ibid.

- Ibid.

- John Baylis, James Wirtz, and Colin S. Gray. Op Cite. P.285.

- Sue Halpern. Op Cite.

- John Baylis, James Wirtz, and Colin S. Gray. Op Cite. P.286.

ERATING CONCEPT – JOINT COMPUTER NETWORK OPERATIONS." AIR UNIVERSITY, AIR WAR COLLEGE. 17 February 2010. p.14. https://tinyurl.com/wa92d4w

William A. Owens, Kenneth W. Dam & Herbert S. Lin eds. "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities." National Research Council, Committee on Offensive Information Warfare, 2009. p.1 https://tinyurl.com/35fex423

- U.S. Department of Energy. "ELECTRICITY SUBSECTOR CYBERSECURITY RISK MANAGEMENT PROCESS." May 2012. P.65. https://tinyurl.com/4htdzhhh

- David Clark, Thomas Berson, and Herbert Lin. "At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues." National Academy of Sciences. P.32. https://tinyurl.com/2emb5hxk

- "Bank for International Settlements and International Organization of Securities Commissions." Guidance on Cyber Resilience for Financial Market

https://tinyurl.com/258hcybt

- Raymond C. Parks and David P. Duggan. "Principles of Cyberwarfare." IEEE Security & Privacy, vol. 9. pp.30-35. 2011. P.30. https://tinyurl.com/6y3aryd3

- Keith Scott. Op Cite. P.1.

- Ibid. P.1.

- Michael Robinson; Kevin Jones; Janicke Helge. "Cyber Warfare Issues and Challenges." Journal of Computers and Security. P.15. https://tinyurl.com/3ppptyer

- Keith Scott. Op Cite. P.1.

- John Andrews. "The World in Conflict: Understanding the world›s trouble spots." 2015. https://tinyurl.com/4hftyafx

- Ryan Singel. "White House Cyber Czar: ‹There Is No Cyberwar›." Wired›s Epicenter blog. 2010. https://tinyurl.com/5rf8w6at

- A. Kiyuna and L. Conyers. "CYBERWARFARE SOURCEBOOK." April 2015. P.8. https://tinyurl.com/3y9xabnz

- Ibid. P.2.

- Aaron Brantly and Max Smeets. "Military Operations in Cyberspace." Springer. August 2020. PP.3-4. https://tinyurl.com/pzzyz6v3

- Ibid. P.286.

- Ibid. P.286.

- Ibid. P.286.

- Ralph Langner. "Cyber Power - An Emerging Factor in National and International Security." Center for International Relations and Sustainable Development. https://tinyurl.com/t6k6ha2b

Ibid.

- John Baylis, James Wirtz, and Colin S. Gray. Op Cite. P.289.

- Ibid. PP. 285-286.

- Ibid. P.286.

- Andy Greenberg. "The WIRED Guide to Cyberwar." August 2019. https://tinyurl.com/465v9hnw

- Keith Breene. "Who are the cyberwar superpowers?" The World Economic Forum. https://tinyurl.com/3mxuttyb

- Michael Robinson, Kevin Jones, Helge Janicke and Leandros Maglaras. "An Introduction to Cyber Peacekeeping." April, 2018. P.1. https://tinyurl.com/5e68jjeu

- Keith Scott. "Connected, Continual Conflict: Towards a Cybernetic Model of Warfare." De Montfort University, UK. P.1.

- Ibid. P.3.

- John Baylis, James Wirtz, and Colin S. Gray. Op Cite. P.287.

- Ibid. P.290.

- Ibid. P.290.

- Ibid. P.290.

- Clara Assumpção. "The Problem of Cyber Attribution Between States." Charles University. May 2020. P.1.

https://tinyurl.com/49seuewu

- Michael Robinson, Kevin Jones, Helge Janicke and Leandros Maglaras. 2018. Op Cite. P.6.

- Ibid.

- Clara Assumpção. Op Cite. P.2

- Demetrius Delibasis Fokas. "The Right of States to National Self-Defense in Information Warfare Operations." National Self-Defense. 2007. P.17. https://tinyurl.com/nah7zcfn

- Ibid. P.17.

- Ibid. P.17.

- Ibid. P.46.

- John Baylis, James Wirtz, and Colin S. Gray. Op Cite. P.294.

- Ibid. P.194.

- Ibid. P.194.

- Ibid. P.195.

- Ibid. P.196.

الملخص

شهدت السنوات الأخيرة انتشارا سريعا لتقنيات اتصالات المعلومات في جميع أنحاء العالم، مما أدى إلى إنشاء مجال متصل عالميا يسمى الفضاء السيبراني، كل جانب من جوانب المجتمع الحديث من كيفية التواصل إلى كيفية شن الحرب يمكن القول الآن أنه يعتمد على الإنترنت او سوف يعتمد عليه بالضرورة، تقريبا كل وظيفة من الوظائف الحديثة يتم تمكين المجتمع منها عبر الفضاء السيبراني. يمكن القول الآن أن كل جانب من جوانب المجتمع الحديث من كيفية إجراء التواصل إلى كيفية شن الحرب يعتمد على الإنترنت، وتقريبا يتم تسيير مختلف الوظائف في المجتمع الحديث عن طريق الفضاء الإلكتروني. هذه ميزة ونقطة ضعف خطيرة في نفس الوقت، تعمل مجموعة متنوعة من الجهات الفاعلة -بدءًا من الأفراد والمجموعات الصغيرة إلى الجهات الفاعلة غير الحكومية بل وحتى الحكومات- على تطوير قدرات الهجوم السيبراني التي يمكن أن تعطل بل وتدمر العناصر الأساسية للمجتمع الحديث، والدفاع ضد هذه التهديدات يمثل تحديا لأن الجريمة في الفضاء السيبراني هي الشكل السائد للحرب. لكن على الرغم من هذه الميزة، فإن الهجوم السيبراني ينطوي على مخاطر. إن انتشار الفضاء السيبراني، والأهمية المتزايدة للقوة السيرانية، لهما تأثير ملموس على السياسة الدولية واستخدام القوة العسكرية وانماط الصراع في القرن الحادي والعشرين. ما هي انعكاسات هذه الاتجاهات، ولماذا يجب أن يهتم الاستراتيجيون بها؟ هذا ما سوف نتعرض له خلال هذا البحث.

الكلمات المفتاحية: القوة السيبرانية ، الفضاء

السـيبراني ، الهجـوم السـيبرانية ، السـلاح السـيبراني ، الصـراع والحرب السـيبرانية ، الأمن السيبراني ، القانون الدولي السيبراني.

Abstract

The fast expansion of information communication technology across the globe in recent years has resulted in the creation of a global realm of interconnected information has emerged known as cyberspace. Virtually every function of contemporary civilization is facilitated by cyberspace, from how we communicate to how we conduct war. This is both a benefit and a significant weakness, as a wide range of entities -from individuals and small organizations to non-state actors and governments- are developing cyber-attack capabilities that can disrupt and even destroy essential components of modern civilization. Because the offence is the dominating mode of combat in cyberspace, defending against these threats is difficult. Cyberspace›s pervasiveness, as well as the increasing significance of cyberpower, are having a real effect on international politics and the use of military force in the twenty-first century. What do these patterns mean for strategists, and why should they be concerned? This is what we will be exposed to during this research.

Key Words : Cyber Power, Cyber Space, Cyberattack, Cyber Weapon, cyber war, Cyber Security, International Cyber Law.