Conflict Management in Cyberspace An Analytical Study

https://www.doi.org/10.56830/ROLB3067

Ali Mosa Aldada
Assistant Professor& Head of Political Science Department, Applied Science University – Bahrain
Corresponding author: ali.aldada@asu.edu.bh

Abstract

With the information revolution, a new form of power emerged, which is cyber power, where some countries use the capabilities provided by cyberspace for several considerations, foremost of which are security and military power. Here, a new dimension has emerged in international conflicts, which is the management of cyberspace conflicts, where one party to the conflict can inflict heavy losses on the other party and cause paralysis of its information and communication infrastructure, which causes military and economic losses. For example, by cutting off communication systems between military units and each other, misleading their information, stealing confidential information about them, manipulating and falsifying economic and financial data, or even erasing them from computers. In light of this transformation in cyberspace, as a new field of international interactions, the case of its work in civil uses and others of a military nature emerged, and violent, hostile activities crystallized in the phenomenon of cyber conflicts, which was characterized by the multiplicity of its manifestations, characteristics and actors, and its emergence through two main directions: a trend related to the work of Soft power in managing conflict through cyberspace, and the other direction is related to employing hard power in managing this conflict.

Keywords: Conflict management, cyber, cyberspace.

World Research of Business Administration Journal
Vol. 2, No. 3, Nov November 2022

THE SCIENCE PUBLISHING HOUSE

إدارة الصراعات في الفضاء السيبراني
دراسة تحليلية

علي موسى الددا
أستاذ العلاقات الدولية المساعد، ورئيس قسم العلوم السياسية، جامعة العلوم التطبيقية – مملكة البحرين

ملخص:
مع ثورة المعلومات، ظهر شكل جديد من أشكال القوة، هو القوة السيبرانية (Cyber power)، حيث تستخدم بعض الدول، القدرات التى يوفرها الفضاء الإلكتروني لاعتبارات عدة، في مقدمتها الأمن والقوة العسكرية. وهنا بالضبط، ظهر بعد جديد في الصراعات الدولية، وهو إدارة صراعات الفضاء الإلكتروني أو السيبراني (Cyber space)، حيث يستطيع، أحد أطراف الصراع أن يوقع خسائر فادحة بالطرف الآخر، وأن يتسبب في شل البنية المعلوماتية والاتصالية الخاصة به، وهو ما يسبب خسائر عسكرية واقتصادية فادحة، وذلك مثلاً من خلال قطع أنظمة الاتصال بين الوحدات العسكرية وبعضها البعض، أو تضليل معلوماتها، أو سرقة معلومات سرية عنها، أو من خلال التلاعب في البيانات الاقتصادية والمالية وتزييفها، أو حتى مسحها من أجهزة الحواسيب. في ظل هذا التحول في الفضاء السيبراني، كمجال جديد للتفاعلات الدولية، برزت حالة توظيفه في الاستخدامات المدنية، والأخرى ذات الطبيعة العسكرية، وتبلورت الأنشطة العدائية العنيفة في ظاهرة الصراعات السيبرانية، التي اتسمت بتعدد مظاهرها وخصائصها والفاعلين فيها، وظهورها عبر اتجاهين أساسيين: اتجاه يتعلق بتوظيف القوة الناعمة في إدارة الصراع عبر الفضاء الإلكتروني، والاتجاه الآخر يتعلق بتوظيف القوة الصلبة في إدارة هذا الصراع.

كلمات مفتاحية: إدارة الصراع، السيبرانية، الفضاء السيبراني.

مقدمة:

أدى التطور التكنولوجي، كانتشار الإنترنت والأجهزة النقالة، وتوافر الحزمة العريضة للإنترنت عبر الأجهزة النقالة وتدني كلفتها، إلى ارتفاع أعداد مستخدمي الإنترنت، وتزايد الاعتماد على هذه التكنولوجيات في التنمية الاقتصادية والاجتماعية. إلا أن الانفتاح الذي يميّز شبكة الإنترنت، والفضاء السيبراني عموماً، جعلها عرضة للتعديات والأنشطة الإجرامية، وهو ما يعكس تنامي في القدرات والتهديدات، وتعاظم التاثير على أمن البنية التحتية الكونية للمعلومات. وقد ذكر خبراء المعهد الأوروبي لمكافحة الإرهاب، أن الصراعات السيبرانية قد تحتل مكان الصراعات التقليدية، وأنها ربما تمثل مفاتيح الانتصار في المستقبل القريب، ولذلك أصبح الأمن الإلكتروني من أهم الهواجس الأمنية للدول، بهدف ضمان أمن وسلامة منشآتها الإلكترونية.

وتشكل الهجمات السيبرانية والقرصنة الإلكترونية، اثنتين من الطرق الفعالة والمدمرة، التي يتم استغلالها لإلحاق الضرر بدولة أو بمؤسسة بدون عناء، مقارنة بالهجمات المسلحة التي تتطلب مجهودات ومعدات ووقت أكبر. ولذا، تطرح الدراسة إشكاليتها بالاستناد الى تتبع أثر سعي بعض الدول الى تحقيق مصالحها الخاصة، بتوظيفها للفضاء السيبراني بكل ما يتضمنه من أبعاد وأنماط، وذلك لتحقيق غاياتها وأهدافها. ومن هنا تركزت الإشكالية، في محاولة الدراسة الإجابة على السؤالين التاليين: هل يمكن لأعمال إدارة دارة الصراعات ضمن الفضاء السيبراني، أن تكون بديلاً للحروب التقليدية مستقبلاً؟ وهل الدول في العديد من الحالات، قادرة على تحقيق حماية أمنها الإلكتروني؟

Print ISSN 2771-1161
Online ISSN 2771-1153

ولأن هذه الدراسة، تعنى بالبحث في إدارة الصراع ضمن الفضاء السيبراني، ومدى انتشار أنواعه دولياً، وبيان مدى فاعلية دور التقنيات في ذلك الانتشار، والأسباب التي تدفع باتجاه ذلك، كان لزاماً علينا أيضاً توضيح أثر استخدام التقنيات والمعلومات، في إدارة الصراعات السيبرانية مستقبلاً، وذلك من خلال الانطلاق من فرضية قوامها، أن الصراعات السيبرانية، تحمل الكثير من الأسباب والدوافع نحو السيطرة على حروب المستقبل، وتحقيق أهداف وغايات سياسية واستراتيجية. وفي سبيل ذلك كله سيتم استخدام المنهج الوصفي التحليلي، والذي يساعد على وصف الظاهرة كما هي في الواقع، وصفاً دقيقاً تعبيرياً، وتحليلها واشتقاق الاستنتاجات، التي تعين في النهاية على الإجابة على الأسئلة واختبار الفرضية.

أولاً: مفهوم الصراع في الفضاء السيبراني وضبط المفاهيم

قبل الولوج إلى عالم الحروب السيبرانية (cyber wars) ، فإنّ كلمة سايبر أو سيبراني، تفضي إلى معانٍ عدة، فهي تشير أولاً إلى شبكات الحاسوب حول العالم، وتشير ثانياً إلى شبكات الإنترنت، وكل الأنشطة المتعلقة بها والتي يتم تنفيذها من خلالها. بمعنى أنّها تعني كل ما يتعلق بثقافة الحاسوب والإنترنت، أي المعلومات والبيانات التي تخزنها الحواسيب حول العالم، وكذلك تلك التي تستقبلها أو تنتجها. والمقصود بالصراعات السيبرانية، أنّ هذه الصراعات قد تستهدف بنى تحتية أساسية للدول، لكنها ليست البنى المادية بالضرورة، بل البنى التحتية للمعلوماتية، مثل قطاعات عسكرية وخدمية وحكومية واقتصادية وبنكية وغيرها. وبذلك فإنّ صراعات الفضاء الإلكتروني غير محددة المجال، وغامضة الأهداف، كونها تتحرك عبر شبكات المعلومات والاتصالات العابرة للحدود الدولية، إضافة إلى اعتمادها على أسلحة إلكترونية جديدة تلائم طبيعة السياق التكنولوجي لعصر المعلومات، حيث يتم توجيهها ضد المنشآت الحيوية.

إذاً، تبدو هذه الصراعات فعالةً جداً، بل ومدمرةً على مستوياتٍ عديدة، ربما تفوق مستويات الدول ذاتها، ذلك أنّ تزايد ارتباط العالم بالفضاء الإلكتروني، اتسع معه خطر تعرض البنية التحتية الكونية للمعلومات لهجمات إلكترونية، خصوصاً مع تراجع دور الدولة في ظل العولمة وانسحابها من بعض القطاعات الإستراتيجية لمصلحة القطاع الخاص، وفي الوقت عينه، تصاعدت أدوار الشركات متعددة الجنسيات، خاصة العاملة في مجال التكنولوجيا.

لم تكن تلك الصراعات هجوميةً فقط، بل تتقصد متابعة نشاط الآخرين السيبراني، ومحاولة منع اعتداءاتهم، فالإنترنت فتح حقلاً جديداً للمخاوف في العالم فعلاً، فشركاتٌ عالمية كبرى، اقتصادية أو تعمل في مجالات التقنية، أخذت تخاف من السرقة المتطورة لتقنياتها وأسرارها وخطط عملها، وهو ما يذكر "كابلان" مثالاً واضحاً عليه في كتابه "حول تجهيز الصين لفريق متخصص من أجل الولوج إلى قواعد بيانات شركات أمريكية مثلاً." لقد كشف تطور الإنترنت، للكثير من المؤسسات الكبرى خاصةً كانت أم حكومية، أنه لم يعد ممكناً لها إخفاء أسرارها بطريقةٍ حقيقية، فهي على الأقل، يجب أن تكشف أوراقها وبياناتها لطرفٍ أمنيٍ تقنيٍ ما، حتى يتكفل بحمايتها من طرفٍ آخر يود تدميرها وتدمير بياناتها. فعلى الأقل، الكثير من الأشياء التي تحدث يومياً بغزارة يتم التحكم بها عن طريق الإنترنت (الخالدي، ٢٠١٩) . وبفضل الثورة المعلوماتية، ظهر لدينا بيئة جديدة وهى الفضاء الإلكتروني (Cyber space) ، وهي تختلف عن البيئات الأخرى (الاقليم البري، البحري، الجوي، الفضاء الخارجي) (معراوي،، ٢٠٢١)، كونها من صنع الإنسان، ولكنها تشترك فى بعض من السمات والخصائص مع البيئات الأخرى، بحيث أضحى الفضاء الإلكتروني عنصراً مؤثراً فى النظام الدولي، نظراً لما يحمله من أدوات تكنولوجية متطورة، تلعب دوراً مهماً فى عمليات الحشد والتعبئة في العالم برمته، فضلاً عن التأثير في القيم السياسية، والتأثير على أنماط "القوة – الحرب – الأمن"(Nigel Inkster, 2017) .

الفضاء السيبراني(Aleksandar KLAIC, 2015) **:** عرفته الوكالة الفرنسية لأمن أنظمة الإعلام- وهي وكالة حكومية مكلفة بالدفاع السيبراني الفرنسي- بأنه: فضاء التواصل المشكّل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية. فهو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، مكوّن من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو مستعملين. كما أن هناك مَن عرّف الفضاء السيبراني، بوصفه الذراع الرابعة للجيوش الحديثة (الجراش، ٢٠٢٢).

الهجمات السيبرانية: يمكن تعريفها بكونها: فعلاً يقوّض من قدرات ووظائف شبكة الكمبيوتر، لغرض قومي أو سياسي، من خلال استغلال نقطة ضعف معينة، تُمكّن المهاجم من التلاعب بالنظام. (البهي، ٢٠١٧)

الجريمة السيبرانية: مجموعة الأفعال والأعمال غير القانونية، التي تتم عبر معدات أو أجهزة إلكترونية أو شبكة الإنترنت أو تبث عبرها محتوياتها. وهي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها، فهي الجريمة المتصلة باستخدام الكمبيوتر، أي عبارة عن تصرف غير قانوني، يرتكب باستخدام تقنيات المعلومات والاتصالات (قرة، ٢٠١٩).

القوة السيبرانية (لبنى، ٢٠٢٠)**:** يعد "جوزيف.س ناي" Joseph. S Nye، من أبرز المهتمين بالقوة السيبرانية، حيث يعرّفها بأنها "القدرة على الحصول على النتائج المرجوة، من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، أي أنها القدرة على استخدام الفضاء السيبراني لإيجاد مزايا للدولة (Jelle, 2016)، والتأثير على الأحداث المتعلقة بالبيئات التشغيلية الأخرى، وذلك عبر أدوات سيبرانية (Joseph & Nye, 2010)".

ومن الأمور المتعارف عليها في العلاقات الدولية، أن مصادر قوة الدولة وأشكالها تتغير، فإلى جانب القوة الصلبة، ممثلة في القدرات العسكرية والاقتصادية، تزايد الاهتمام بالأبعاد غير المادية للقوة، ومن ثم بروز القوة الناعمة التي تعتمد على جاذبية النموذج والإقناع. ومع ثورة المعلومات ظهر شكل جديد من أشكال القوة، (صبرينة، ٢٠٢٠) هو القوة السيبرانية (Cyber power) التي لها تأثير كبير على المستوى الدولي والمحلي، فمن ناحية أدت إلى توزيع وانتشار القوة بين عدد أكبر من الفاعلين، ما جعل قدرة الدولة على السيطرة موضع شك، ومن ناحية أخرى، منحت الفاعلين الأصغر، قدرةً أكبر على ممارسة كل من القوة الصلبة والقوة الناعمة عبر الفضاء السيبراني، وهو ما يعني تغيرات في علاقات القوى في السياسة الدولية. من هذا المنطلق، أصبح الباحثين في حقل العلاقات الدولية وبقية الحقول الفرعية في الدراسات الأمنية والدراسات الاستراتيجية، يركزون بشكل متزايد حول أثر التكنولوجيا على الأمن القومي والدولي، ويشمل ذلك تأثيرها على المفاهيم ذات الصلة كالقوة والسيادة.

ثانياً: أسباب ظهور وتنامي الصراعات السيبرانية

إن ازدياد نطاق المعرفة في مجال العلوم والتكنولوجيا بشكل كبير، أدى الى أن تكون هناك حاجة ماسة للعقول المبتكرة والمبدعة، لاستكشاف مجالات غير معروفة وغير مكشوفة في مختلف المجالات، ولمواكبة العالم الحديث وعصر التكنولوجيا الذي تحركه المعرفة (غزال، ٢٠٢٢م). ولعله من أول الأسباب التي أدت الى ظهور الصراعات السيبرانية، استحداث أجهزة الكمبيوتر في منتصف الخمسينيات من القرن الماضي، كأداة لمعالجة وحفظ المعلومات رقمياً (Digital)، رافقه تضافر جهود عدد من الشركات الخاصة والعامة، توج بتطوير وحدة المعالجة المركزية (CPU)، وذلك لتسهيل المهام الموكلة له، وقد تطور ذلك بصورة جذرية في العقود اللاحقة، حتى أصبح جهاز الكمبيوتر أساساً في عمل الكثير من المؤسسات الخاصة والعامة، فضلاً عن الحياة اليومية.

أما السبب الثاني في ظهور الصراعات السيبرانية، فيعزى الى ظهور الشبكة العنكبوتية (الإنترنت)، وهو الذي أحدث انقلاباً مثيراً في حياة البشرية، من خلال التواصل ونقل المعلومات بسرعة فائقة. وقد سارعت الدول في وتيرة استخدام الكمبيوتر لتحقيق قفزات نوعية في المجال الأمني والعسكري في مطلع التسعينيات من القرن الماضي، حتى أطلق البعض عليها مصطلح الحرب السيبرانية الباردة Cyber Cold War أو سباق التسلح السيبراني Cyber arms race (الصادق، ٢٠١٧).

لقد ساهم تزايد ارتباط العالم بالفضاء السيبراني في جميع مرافق الحياة، وفي كل المجالات مثل (قطاعات الطاقة والاتصالات والنقل والصحة والمياه والخدمات الحكومية والمالية والتجارة الإلكترونية، وغيرها)، في اتساع خطر تعرض البنى التحتية المعلوماتية لهجمات إلكترونية من دول معادية أو أفراد أو جماعات أو شركات، لتنال من الأمن الوطني للدول. وأيضا تراجع دور الدول في ظل الخصخصة وانسحابها من بعض القطاعات

Print ISSN 2771-1161
Online ISSN 2771-1153

الإستراتيجية لمصلحة القطاع الخاص، و تصاعد أدوار الشركات متعددة الجنسيات، والتي تملك قدرات تقنية تفوق الحكومات، خاصة العاملة في مجال التكنولوجيا، كفاعل مؤثر في إدارة صراعات الفضاء السيبراني.

كما ساهم تزايد اعتماد الدول على الأنظمة الإلكترونية في جميع منشآتها الحيوية، بأن جعلها عرضة للتهديد السيبراني، لما له من سمات مدنية وعسكرية متداخلة، خاصة أن الثورة التكنولوجية الحديثة تمخضت عنها ثورات أخرى لتطوير التقنيات العسكرية، إلى جانب قلة تكلفة الحروب السيبرانية، مقارنة بنظيراتها التقليدية، فقد يتم شن هجوم إلكتروني، بما يعادل تكلفة طائرة بدون طيار من خلال أسلحة إلكترونية متطورة، ومهارات بشرية عالية، وإمكانية تنفيذ الهجوم في أي وقت، وبدون أن يتطلب القيام به وقتاً طويلاً.

ومن الجدير الإشارة، الى أن هناك عدم قدرة لدى المجتمع الدولي، في التدخل لاحتواء أسلحة الصراعات السيبرانية، ولا يوجد إمكانية لتفعيل التفتيش مثل ما هو عليه الحال في الأسلحة التقليدية، خاصة مع اتساع نطاق مخاطر الأنشطة العدائية للهجمات السيبرانية، سواء من الدول أو من جماعات أو أفراد، وذلك مع وجود مؤشرات على احتمال تطوير الجماعات الإرهابية لقدراتها السيبرانية، بالرغم من محدوديتها لديها حالياً. ولكن مع تطور القدرات البشرية على إنتاج تقنيات جديدة تهدد البنى التحتية المعلوماتية، وتراجع سيادة بعض الدول على الشركات التكنولوجية العابرة للحدود، وشبكات الجريمة، والقرصنة الإلكترونية، والجماعات الإرهابية وغيرها، أصبح التفوق في القدرة على إدارة الصراعات في الفضاء السيبراني أو الإلكتروني، سلاحاً حيوياً في تنفيذ عمليات ذات فاعلية في الأرض والبحر والجو، واعتماد القدرة القتالية في هذا الفضاء على نظم التحكم والسيطرة التكنولوجية (العصيمي،، ٢٠١٧).

ثالثاً: الفاعلون القادرون على امتلاك القوة السيبرانية

حسب "جوزيف ناي"، أبرز المهتمين بالقوة السيبرانية، فإن الذين قد يمتلكون مثل هذه القوة، ينقسمون الى ثلاثة أنواع، هي:

١- الدول : والتي لديها قدرة كبيرة على تنفيذ هجمات سيبرانية وإدارة الصراعات المتعلقة بها، وتطوير البنية التحتية وممارسة السلطات داخل حدودها. فالدولة هي الفاعل المحوري بامتياز في هذا العالم الافتراضي لما لها من مكانة على أساس التفوق التكنولوجي والمؤهلات التي ترشحها للحصول على هذه المكانة.

٢- الفواعل من غير الدول: ويستخدم هؤلاء الفاعلون القوة السيبرانية، لأغراض هجومية بالأساس، إلا أن قدرتهم على تنفيذ أي هجوم سيبراني مؤثر، تتطلب مشاركة ومساعدة متطورة، ولكن يمكنهم اختراق المواقع الإلكترونية واستهداف الأنظمة الدفاعية (Joseph & Nye, 2010) . وتشمل هذه الفواعل ما يلي (خليفة، ٢٠١٤):

-الشركات متعددة الجنسيات: حيث تمتلك بعض شركات التكنولوجيا، موارد للقوة تفوق قدرة بعض الدول، ولا تنقصها سوى شرعية ممارسة القوة، التي ما زالت حكراً على الدول، فخوادم شركات مثل: جوجل Google وفيسبوك Facebook ومايكروسوفت Microsoft، تسمح لها بامتلاك قواعد البيانات العملاقة، التي من خلالها تستكشف وتستغل الأسواق، وتؤثر في اقتصاديات الدول وفي ثقافة المجتمعات وتوجهاتها.

-المنظمات الإجرامية: تقوم هذه المنظمات الإجرامية بعمليات القرصنة السيبرانية، وسرقة المعلومات واختراق الحسابات البنكية وتحويل الأموال، كما توجد سوق سوداء على الإنترنت المظلم Dark internet لتجارة المخدرات والأسلحة والبشر (زروقة، ٢٠١٨).

-الجماعات الإرهابية: تعد من أبرز الفواعل الدولية، خاصة بعد أحداث 11سبتمبر ٢٠٠١م، حيث تستغل الفضاء السيبراني في عمليات التجنيد والتعبئة والدعاية وجمع الأموال والمتطوعين، كما تحاول جمع

المعلومات حول الأهداف العسكرية، وكيفية التعامل مع الأسلحة وتدريب المجندين الجُدد عن بعد، رغم أنها لم تصل بعد إلى مرحلة القيام بهجوم سيبراني حقيقي على منشآت البنية التحتية للدول (حكيم، ٢٠١٨).

٣- الأفراد: أصبح الفرد بفضل الفضاء السيبراني، فاعلاً مؤثراً في العلاقات الدولية، ومن أبرز النماذج ظاهرة الويكيليكس "Wikileaks"، الذي نجح في نشر ملايين الوثائق السرية، ما خلق مشاكل دبلوماسية بين العديد من الدول.

رابعاً: أبعاد الصراعات السيبرانية

تطال أبعاد الصراعات السيبرانية، جميع المسائل الاقتصادية والسياسية والعسكرية والاجتماعية والانسانية (قرة، ٢٠١٩).

١- **الأبعاد العسكرية:** تتمثل الميزة النسبية للأمن السيبراني في بعده العسكري، عن طريق قدرة القوة السيبرانية على ربط الوحدات العسكرية ببعضها البعض عبر العالم الافتراضي، وهذا ما يسهل عملية تبادل المعلومات الذي ينعكس إيجاباً على تحقيق الأهداف العسكرية(Elliott, 2010) .

٢- **الأبعاد الاجتماعية:** تسمح طبيعة الإنترنت المفتوحة عبر المدونات والشبكات الاجتماعية بشكل خاص، لكل مواطن بأن يعبر عن تطلعاته السياسية وطموحاته الاجتماعية، حيث تمثل مشاركة جميع شرائح المجتمع فرصة للاطلاع على الأفكار والمعلومات المختلفة، بما تتضمنه من حاجة لدى المجتمع في الحفاظ على استقرار الفضاء السيبراني والمجتمع الذي يرتكز إليه. لكن في المقابل يعرِّض أخلاقيات المجتمع للخطر، نظراً لصعوبة مراقبة محتوى الإنترنت، كما يعرِّض الهويات لعمليات اختراق خارجي، ما قد يتسبب في تهديد السلم الاجتماعي للدولة، وعليه فلابد من العمل على توعية المواطن بهذه المخاطر لتحقيق الأمن السيبراني في بعده الاجتماعي (العنزي، ٢٠١٣).

٣- **الأبعاد السياسية:** هناك أمثلة كثيرة تدفع نحو الاهتمام بالبعد السياسي للأمن السيبراني، كالتسريبات المختلفة للوثائق الحساسة التي تؤدي إلى مشكلات متفاقمة جداً على المستوى الخارجي والدولي، كما أنه لا أحد يُنكر الدور المتعاظم لشبكات التواصل الاجتماعي على المستوى السياسي (حملات انتخابية، تظاهرات افتراضية، حركات احتجاجية إلكترونية...الخ) (طالة).

٤- **الأبعاد الاقتصادية:** يرتبط الأمن السيبراني ارتباطاً وثيقاً بالاقتصاد، فالتلازم واضح بين اقتصاد المعرفة وتوسع استخدام تقنيات المعلومات والاتصالات، والتي تتيح تعزيز التنمية الاقتصادية لبلدان كثيرة عبر إفادتها من فرص الاستخدام التي تقدمها الشركات الدولية والشركات الكبرى التي تبحث عن إدارة كلفة إنتاجها بأفضل الشروط، إلا أن هذا الواقع المشرق يطرح مسائل مختلفة، سواء ما تعلق منها بحماية مقدم الخدمة والعمل أو ما تعلق بحماية المستهلك عبر الإنترنت .أضف إلى ذلك دخول العالم عصر المال الإلكتروني، ضمن بيئة تقنية متحركة بعد إطلاق خدمات المحفظة الإلكترونية، إذ تتزايد استثمارات المصارف والمؤسسات المالية في مجال المال الرقمي. وكمثال على ذلك، يشير تقرير صادر عن شركة "emarkater"، إلى أن حجم التجارة الإلكترونية بلغ 1.5 تريليون دولار عام 2014م، مقارنة بعام 2013م، الذي بلغت فيه 1.2 تريليون دولار، ونظراً لارتفاع معدل الجرائم السيبرانية المنظمة والخطيرة، فإن ذلك يمثل تهديداً صريحاً لنمو الاقتصاد الرقمي، ما لم تقم الدول بتعظيم معايير الأمن السبراني، بما يضمن الحد من هذه الجرائم (حسين، ٢٠٢١).

٥- **الأبعاد القانونية:** إن التطورات التكنولوجية المتسارعة، تفرض مواكبة التشريعات القانونية لها، من خلال وضع أطر وتشريعات للأعمال القانونية وغير القانونية في الفضاء السيبراني، فالملاحظ أن الجريمة السيبرانية تفتقد في معظم البلدان إلى الأطر القانونية الصارمة للتعامل معها، إضافة إلى ضرورة تفعيل التعاون الدولي المشترك لمكافحتها. ولعل من أبرز الممارسات القانونية في مجال الأمن السيبراني هو ضمان بعض الحقوق في هذا المجال، كحق النفاذ إلى الشبكة العالمية للمعلومات، وأيضاً توسعت بعض

Print ISSN 2771-1161
Online ISSN 2771-1153

المفاهيم لتشمل أساليب الممارسة الجديدة باستخدام تقنيات المعلومات والاتصالات، كالحق في إنشاء المدونات الإلكترونية، والحق في إنشاء التجمعات على الإنترنت، وأيضاً الحق في حماية ملكية البرامج المعلوماتية (حسين، ٢٠٢١)

خامساً: مستقبل الصراعات السيبرانية

كلما كانت الدول متقدمة وتعتمد على الإنترنت، والخدمات الإلكترونية في مؤسساتها العظمى، كلما ازدادت مخاوفها من الدخول في صراعات الفضاء السيبراني، فمع التصاعد المستمر وتطور أدوات البرمجيات والتكنولوجيا الحديثة، تصاعدت خطورة انتشار الهجوم السيبراني بشكل أسرع وأقوى وأكثر تدميراً. وبالاستناد الى تقرير أعدته لجنة الدفاع والأمن القومي في البرلمان البريطاني مثلاً: عن مخاوف الهجوم السيبراني، أنه "أكثر دماراً من التفجير الذري..باستطاعته تدمير أنظمة الإلكترونيات، ومحطّات ضخ المياه، والهواتف، ومحطات الإذاعة والتلفزة، وتوقّيف الاتصالات، وانهيار الأنظمة المالية".

وتؤكد معظم الترجيحات، أن الصراعات السيبرانية، باتت تطيح بالحروب العسكرية التقليدية، حيث من المتوقع أن تندلع أكثر فأكثر بين الدول، رغم أن الهجمات الإلكترونية ليست دموية لكن مساحة المتضررين منها في المستقبل، ستكون أكثر من المتضررين من المعارك التي خاضتها بعض الدول. إذاً، والحالة هذه، فإن الصراعات الإلكترونية تعتبر مواجهات غير معلنة، تديرها الدول ضد بعضها البعض، من خلال مجموعات ممولة، تقوم بهجمات وحروب سيبرانية صامتة. وأهم ما يميزها أنها تتعامل مع عدو مجهول رغم أن دولاً تتهم دولاً أخرى صراحة، بافتعال هجوم رقمي معين(Kramer, Starr, & Wentz, 2009) .

بلغت الهجمات السيبرانية ذروتها في السنوات الأخيرة، على نحو جعل المسؤولين الحكوميين ورجال الأعمال في جميع أنحاء العالم، أكثر وعياً الآن بالتهديدات السيبرانية وإدارة مواجهتها، من أي وقت مضى، وهو ما دفعهم لاتخاذ تدابير لتعزيز الأمن الإلكتروني. وحسب "دينس زنج" Denise E. Zheng، أصبح الأمن السيبراني واحداً من أسرع القطاعات نمواً في صناعة التكنولوجيا العالمية، فضلاً عن مئات الشركات الجديدة المتخصصة فيه. وعلى مدار العقد الماضي فقط، سنت الولايات المتحدة وحدها ٣٤ قانوناً جديداً و٥ أوامر تنفيذية، لتحسين الأمن السيبراني، بما في ذلك تعزيز معايير البنية التحتية، وتبادل المعلومات المتعلقة بالتهديدات السيبرانية، ووضع عقوبات لمعاقبة وردع العناصر المهاجمة.

لقد تغيرت الحروب التقليدية، وأصبحت الجيوش العسكرية فى كافة أنحاء العالم، تهتم بحرب المعلومات ودورها فى حروب المستقبل، والتي يتوقع الكثيرين حدوثها فى الفضاء الإلكتروني (حمدوش، ٢٠٢١)، وأصبحت هناك مناورات يتم إجراؤها للتدريب على هذا النوع الجديد من الصراع، وكيف يمكن إدارته ومواجهته والاستعداد له. إن طبيعة الحروب وإن كانت لا تتغير، فإن سماتها تتغير مع تطور أدواتها، مثل ظهور الطائرات من دون طيار، كما أن صراعات الفضاء السيبراني قد تأخذ شكل حرب من دون نار أو دخان أو قصف، مع تمثل جانب العنف فيها، في الاختراقات والقرصنة ونشر الفيروسات وغيرها من الأساليب.

وبالرغم من فداحة الخسائر في الصراعات السيبرانية، فإن الأسلحة بسيطة، مثل فيروسات إلكترونية تخترق شبكة الحاسب الآلي، وتنتشر بسرعة بين الأجهزة، وتبدأ عملها في سرية تامة وبكفاءة عالية، وهي في ذلك لا تفرق بين المقاتل والمدني، وبين العام والخاص، وبين السري والمعلوم. ولقد بات من الصعب أن نتخيل صراعاً عسكرياً اليوم، بدون أن يكون لهذا الصراع العسكري أبعاداً إلكترونية، وأصبحت إدارة الصراعات السيبرانية في صلب اهتمامات الأنظمة الدفاعية لأي صراع يمكن أن يحدث في المستقبل.

لقد غيرعصر المعلومات الكثير من الأشياء، وبذلك تغير شكل الحروب، من الحروب التقليدية، التي تعتمد على جيوش عسكرية وأسلحة قتالية، لتصبح على شكل صراعات تدار في الفضاء السيبراني، ولتتميز هذه الحروب بالسرعة والدقة فى تنفيذ العمليات العسكرية، ولتأخذ لها مكاناً بين ما يعرف بأدوات الحرب الشاملة، ولتمتد هذه الحروب الآن- بعد أن كانت تستهدف أجهزة الإنترنت والحواسيب- لتستهدف قطاعات وصناعات محددة.

سادساً: أشكال الصراع السيبراني

يتضمن الصراع السيبراني، العديد من الاشكال، مثل (شلوش،، ٢٠١٨): سرقة كلمات المرور للمستخدمين، وذلك بالتسلل عبر النظام، مثل التخمين والخداع والبرمجيات الخبيثة والنفاذ إلى ملف تخزين كلمة المرور والسطو على كلمات المرور السرية والتجسس على المستخدمين. وكذلك هجمات رفض أداء الخدمة "إنكار الخدمة" حيث تستخدم لزيادة التحميل على الإنترنت والبنية التحتية للشبكات والخدمات، الأمر الذي يزعج الشركات والمنظمات، وهو على العكس من التقنيات التي يستخدمها مجرمو الإنترنت، لأن ذلك يمنع المستخدمين الشرعيين من الوصول إلى المنتجات والخدمات، كما يمكن أن يرتكبها فرد أو جماعة.

ومن أمثلة أشكال الصراع في الفضاء السيبراني أيضاً، ما يسمى بهجمات البنية التحتية، والتي تستهدف شبكات الكهرباء والاتصالات والأغذية والصرافة والمالية والمهام الحكومية. ونشير هنا الى شكل آخر، هو قرصنة المعلومات: ويتمثل ذلك في الهاكرز وهم المبرمجين القادرين على التعامل مع الكمبيوتر ومشاكله بدراية واحتراف، ويقدمون حلولاً لمشاكل البرمجة بشكل تطوعي، وهما نوعان، المحترفون الذين يستخدمون برامج او تقنيات فى محاولات لاختراق الأنظمة والأجهزة للحصول على معلومات سرية أو ربما للتخريب. والمبتدئون الذين يتسللون عبر الشبكات الهاتفية، اعتمادا على جهودهم الشخصية، وهم من أخطر أنواع الهاكرز (محمود، ٢٠١٣).

ومن ضمن أهم أسلحة الصراعات في الفضاء السيبراني، الفيروسات والبرمجيات الخبيثة، والتي تستخدمها بعض الشركات أحياناً، وهي برامج خبيثة تقوم بنسخ نفسها على أجهزة المستخدمين من غير معرفتهم، وتسعى إلى إحداث خلل أو تدمير فى ملفات أو جهاز المستخدم. وبقي القول أنه يندرج ضمن أشكال الهجمات أيضاً، برامج التجسس: وهي برامج خبيثة تعمل بشكل سري على أجهزة المستخدمين، وتهدف إلى جمع المعلومات الشخصية عن المستخدم. ويأخذ التجسس الإلكتروني عدة أشكال، وهي كلها أعمال غير شرعية، مثل: التنصت، المعلومات المضللة، الاختراق بدون اتصال (دريسي، ٢٠٢٢).

سابعاً: أنماط إدارة الصراع في الفضاء السيبراني

تأتي إدارة الصراع السيبراني على ثلاثة أنماط، وذلك باستخدام معيار الشدة، وبالاستناد أيضاً الى طبيعة النمط ومدى تقاربه أو تباعده عن استخدام القوة التقليدية.

١ـ نمط الصراع البارد والصراع الإلكتروني منخفض الشدة

يتم استخدام الفضاء الإلكتروني كساحة للصراع منخفض الشدة، ويأتي هذا النمط ليعبر عن صراع ذو طبيعة ممتدة ومستمرة ودائمة النشاط العدائي أو غير السلمي، ويعبر هذا النمط عن صراعات أخرى أعمق وممتدة ذات نواحي ثقافية أو اقتصادية أو اجتماعية، مع استخدام نمط "القوة الناعمة". ويتميز هذا النمط بدرجة كبيرة من التعقيد والتداخل في معركة لا نهاية لها، ما بقيت الأبعاد الأخرى للصراع، ولا يتطور هذا النوع من الصراعات بالضرورة، إلى حالة استخدام القوة المسلحة بشكلها التقليدي أو من خلال شن حرب إلكترونية واسعة النطاق. وتتم "الحرب الباردة الإلكترونية" من خلال شن الحرب النفسية والاختراقات المتعددة والتجسس وسرقة المعلومات (زروقة، ٢٠١٨)، وشن حرب الأفكار، ولا ترقى لعمل عسكري عنيف، أو يمكن أن تتم حتى من خلال انعكاس التنافس العالمي بين الشركات التكنولوجية والنفوذ ما بين الدول. والى جانب ذلك، تنشط جماعات دولية للقرصنة، للتعبير عن مواقف سياسية أو حقوقية مثل جماعة "ويكيليكس" و"أنونيموس". كما يمكن أن تتم الحرب الإلكترونية التي أشرنا إليها، في حالات الأزمات الدولية، مثل حالة التوتر بين إستونيا وروسيا في عام ٢٠٠٧م، والاختراقات المتبادلة بين الصين والولايات المتحدة وروسيا، أو تلك التي ما بين كوريا الجنوبية وكوريا الشمالية، وكذلك اتهام روسيا بالقرصنة الالكترونية في الانتخابات الأمريكية للتأثير في العملية الديمقراطية وضرب البنية المعلوماتية لدعم مرشح الرئاسة الامريكية "دونالد ترامب"، في مواجهة "هيلاري كلينتون "وهو ما تبعه من تعرض روسيا الى هجمات إلكترونية أخرى، واتهام روسيا كذلك بشن هجمات على النرويج والتشيك وبريطانيا، وهو ما دفع الأخيرة الى إعلان الرد في حال تعرضها لهجمات روسية (عبدالصادق، ٢٠١٦).

Print ISSN 2771-1161
Online ISSN 2771-1153

والخلاصة لهذا النمط من أنماط إدارة الصراعات السيبرانية، أنه يتضمن حروباً إلكترونية، لا تتضمن عملاً عسكرياً.

٢-نمط الصراع الإلكتروني متوسط الشدة

يتحول الصراع عبر الفضاء الإلكتروني، في هذا النمط، إلى ساحة موازية لحرب تقليدية دائرة، وبحيث يمكن دمجه مع حرب تقليدية، وذلك بالاعتماد على الشبكات الذكية، وغيرها من أنظمة المراقبة والرصد عن طريق الإنترنت (Mohan B. Gazula, 2017)، ويكون بذلك تعبيرًا عن حدَّة الصراع القائم بين الأطراف، وقد يكون مقدمة لعمل عسكري. ويدار الصراع عبر الفضاء الإلكتروني في هذا النمط، عن طريق اختراق المواقع وقصفها، وشنِّ حرب نفسية وغيرها من الطرق. ويستمد ذلك الصراع سخونته من قوة أطرافه وارتباطه بعمل عسكري تقليدي، وبخاصة مع وجود تكلفة ٤% فقط من تكلفة الآلة العسكرية، وبما يمكِّن من تمويل حملة حربية كاملة عبر الإنترنت بتكلفة دبابة. كما أنَّه لا يستغرق إلا وقتًا بسيطًا. وهنا يتم استخدام الفضاء الإلكتروني في الصراع بطريقة موازية للحرب التقليدية (عبدالصادق، ٢٠١٦). والخلاصة لهذا النمط، أنه يوصف بصراع إلكتروني يدار بشكل مصاحب أو كمقدمة لأعمال عسكرية لاحقة.

٣- : نمط الصراع الساخن والصراع الإلكتروني مرتفع الشدة

يتميز هذا النمط من الصراع، بسيطرة البعد التكنولوجي على إدارة العمليات الحربية، حيث يتم استخدام الأسلحة الإلكترونية فقط ضد منشآت العدو، ويتم استخدام الروبوتات الآلية في الحروب، والتي تتم إدارتها عن بعد، كاستخدام الطائرات بدون طيار مثلاً. وهنا يتم تطوير القدرات في مجال الدفاع والهجوم الإلكتروني والاستحواذ على القوة الإلكترونية، كما يتم استخدام الفضاء الإلكتروني في الاستعداد لحرب المستقبل والقيام بتدريبات على توجيه ضربة أولى لحواسيب العدو، واختراق العمليات العسكرية عالية التقنية، أو حتى باستهداف الحياة المدنية والبنية التحتية المعلوماتية. ولعل الهدف من وراء ذلك، تحقيق "الهيمنة الإلكترونية الواسعة" بشكل أسرع في حالة نشوب صراع (عبدالصادق، ٢٠١٦). ويتم التقدم في مجال استخدام كافة أنواع الأسلحة الإلكترونية عالية القدرة، كما قد يتم توجيه هجمات إلكترونية باستخدام عدد من الفيروسات. والخلاصة لهذا النمط، أنه يتضمن حروباً، تدار بالاعتماد على الأسلحة الإلكترونية بشكل كامل، (تدار إلكترونياً).

خاتمة:

لقد أصبح العصر الذي نعيش فيه، عصراً رقمياً، تتحكم فيه المعرفة والمعلومات ووسائل الاتصالات ، فمن يملك المعرفة يتحكم فى كل شيء، وأصبح الفضاء السيبرانى واقعاً والحروب السيبرانية حقيقة لا مفر منها، والتي يمكن اعتبارها بمثابة الجيل الخامس من الحروب. ولذلك يتوجب على الدول والأفراد الحذر والحيطة عند استخدام البيانات والمعلومات في المجال الافتراضي، لتجنب الوقوع في مخاطر التصيد الشبكي والهاكرز والجماعات الإرهابية.

وقد تبين لنا مما سبق، صحة الفرضية التي انطلقت منها الدراسة، من حيث أن الصراع عبر الفضاء الإلكتروني، يحمل الكثير من الأسباب والدوافع نحو السيطرة على حروب المستقبل، وتحقيق أهداف وغايات سياسية واستراتيجية.

كما أننا من خلال حيثيات الدراسة، أجبنا على التساؤلات التي تم طرحها في مشكلة الدراسة، حيث:

- أصبح الفضاء السيبراني مجالاً للصراعات المختلفة، بين الدول أو غير الدول، لتحقيق أكبر قدر من النفوذ والتأثير فيه، وبدأت تتبلور وتتمايز أنماط إدارة الصراعات السيبرانية عن نظيراتها التقليدية، من حيث المفهوم والتخطيط والتنفيذ وحدود ميدان التأثير.
- تعتبر الصراعات السيبرانية غامضة الأهداف مجهولة المصدر، تتحرك عبر شبكات المعلومات والاتصالات عالمياً، وتستخدم أسلحة إلكترونية تستهدف تقنية المعلومات، حيث يتم توجيهها ضد المنشآت

الحيوية، والطرف الذي يتمتع بقوة هجومية ويبادر بعنصر المباغتة، سيكون له الغلبة بغض النظر عن حجم قدراته العسكرية التقليدية، الأمر الذي يناقض نظريات الردع الإستراتيجي.

- من خصائص الصراعات في الفضاء السيبراني، عدم القدرة على التمييز بين استهداف المنشآت المدنية أو العسكرية في هجمات الحرب السيبرانية، ومن شبه المستحيل فرض حماية دولية عليها. وأيضاً عدم وجود توحيد لمسمى الحرب السيبرانية بين الدول، فقد يعتمد ذلك على استخدامها السياسي وتوظيفه دعائياً، وقد يطلق عليها مصطلح الحرب أو الغزو الإلكتروني أو الإرهاب أو الإرهاب الإلكتروني.
- فى المستقبل ستعتمد إدارة الصراعات السيبرانية على المعرفة، والتي تلعب الدور الحاسم فى الصراع على السلطة على الصعيد الدولي. والهجوم السيبراني سيغدو بديلاً عن السلاح النووي، حيث لا حاجة إلى حدود جغرافية معينة. كما أنه من الصعب في نظام الإنترنت حالياً، وجود نظام رادار كما في الحروب العسكرية التقليدية، لاكتشاف مصدر الهجوم، خاصة وأن البيانات على شبكة الإنترنت ليست محمية بدرجة عالية من الكفاءة، الأمر الذي يتسبب في اختراقها والتلاعب بالبيانات والمعلومات المتواجدة عليها .
- على مديري الصراعات في الفضاء السيبراني، أن يكونوا مدركين الى أن أسلحة الفضاء السيبراني، تتسم بقدرات غير محدودة على إلحاق الأذى، بدون أن تكون معلومة المصدر، كما أن عنصر المفاجأة متواجد، وتكلفة هذه الحرب هي أقل نسبياً من حروب الدمار الشامل، كما أن عبء الدفاع سيكون مهمته أكثر صعوبة من الجهد الذي يبذله المهاجمين .

قائمة المراجع:

أولاً: المراجع العربية:

اسماعيل زروقة. (٢٠١٨). ، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، . *مجلة العلوم القانونية والسياسية*، المجلد ١٠، العدد ١، .

إيهاب خليفة. (٢٠١٤). ، القوة الإلكترونية وأبعاد التحول في خصائص القوة. ، *مكتبة الاسكندرية، مصر*، .

باسل معراوي،. (٢٠٢١). الحروب السيبرانية وتحديات الأمن العالمي، ٠٥-٠٦-٢٠٢١م -https://altareek media.com/ar/opinion/21.

حنان دريسي. (٢٠٢٢). ، الحروب السيبرانية: تحول في أساليب القتال وثبات المبادىء والأهداف، . *مجلة الفكر القانوني والسياسي*، ، المجلد ٦، العدد ١، .

حنين جميل أبو حسين. (٢٠٢١). ، الإطار القانوني لخدمات الأمن السيبراني، . *رسالة ماجستير مقدمة في جامعة الشرق الأوسط، الأردن*، .

خالد وليد محمود. (٢٠١٣). ، الهجمات عبر الانترنت ساحة الصراع الإلكترونى الجديدة، ،. *المركز العربى للأبحاث ودراسة السياسات*.

رغدة البهي. (٢٠١٧). ، الردع السيبراني: المفهوم والإشكاليات والمتطلبات، مجلة العلوم السياسية والقانون، *المركز الديمقراطي العربي*، العدد ١، .

سارة "محمد روحي" فتحي غزال. (٢٠٢٢م). ، الأمن السيبراني ودرجة وعي المؤسسات بأهميته، *المجلة العربية للنشر العلمي*، ، العدد ٤٧، .

Print ISSN 2771-1161
Online ISSN 2771-1153

سليمان العنزي. (٢٠١٣). وسائل التحقيق في جرائم نظم المعلومات، . *رسالة ماجستير، جامعة نايف العربية للعلوم ألمنية، الرياض،* .

شرقي صبرينة. (٢٠٢٠). ، الإرهاب الإلكتروني والتحول في مفهوم القوة، *مجلة الباحث للدراسات الأكاديمية*، ، المجلد ٧، العدد ٢،.

عادل عبد الصادق. (٢٠١٧). ، الحروب السيبرانية : تصاعد القدرات والتحديات للأمن العالمي، دوريات قضايا استراتيجية، . *المركز العربي لأبحاث الفضاء الإلكتروني،* .

عادل عبدالصادق. (٢٠١٦). أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني. *المركز العربي لأبحاث الفضاء الإلكتروني، القاهرة*، ط. ٢.

عاصف الخالدي. (٢٠١٩). الحروب السيبرانية المقبلة: وداعاً للسلاح التقليدي، ٢٢-٠٦-٢٠١٩م https://hafryat.com/ar/blog.

عبد الله محمد العصيمي،. (٢٠١٧). السيبرانية واشكال الحروب في المستقبل، ٢٠-١٢-٢٠١٧م. https://www.al-jazirah.com/2017/20171220/ar6.htm.

غريب حكيم. (٢٠١٨). ، الإرهاب السيبراني والأمن الدولي: التهديدات العالمية الجديدة وأساليب مواجهته. ، *المجلة الجزائرية للدراسات السياسية*، ، المجلد ٥، العدد ٢،.

فاتح حارك ، رياض حمدوش. (٢٠٢١). ، الدولة بين الهيمنة وتحقيق الأمن في الفضاء السيبراني، المجلة الجزائرية للأمن الإنساني، . المجلد ٧، العدد ١،.

فارس قرة. (٢٠١٩). ، الموسوعة السياسية، ٢٨-٠٨-٢٠١٩م https://political-encyclopedia.org/dictionary.

لامية طالة. (بلا تاريخ). ، التهديدات والجرائم السيبرانية: تأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها، *مجلة معالم للدراسات القانونية والسياسية*، ، المجلد ٤، العدد ٢.

لبنى خميس مهدي، و تغريد صفاء،. (٢٠٢٠). أثر السيبرانية في تطور القوة، مجلة حمورابي، العدد ٣٣-٣٤، ٢٠٢٠م.

لينا صالح الجراش. (٢٠٢٢). ، أثر استخدام الأمن السيبراني في تنمية مهارات الوعي، قسم تكنولوجيا التعليم والمعلومات، . *تمهيدي ماجستير، جامعة إب، الجمهورية اليمنية،* .

نورة شلوش،. (٢٠١٨). القرصنة الإلكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدول، . *مجلة مركز بابل للدراسات الانسانية*، ، المجلد ٨، العدد ٢، .

هبة عبد الفتاح. (بلا تاريخ). ، الحروب السيبرانية: الأكثر دماراً والأقل دموية. https://m.akhbarelyom.com/news/newdetails/2912272/1.

ثانيا: المراجع الأجنبية:

Aleksandar KLAIC .(2015) .A Method for the Development of Cyber Security Strategies . ‹*Information & Security: An International Journal* ‹‹I& S Volume 34.‹

Elliott, S. (2010). ,"Analysis on Defense and Cyberwarfare," . *Infosec Island, 8 July*.

Joseph, S., & Nye, J. (2010). , Cyber Power, Harvard Kennedy School,.

Kramer, F. D., Starr, S. H., & Wentz, L. K. (2009). Cyber power and National Security, ,. *National Defense University Press*.

Mohan B. Gazula. (2017). Cyber Warfare Conflict Analysis and Case Studies, M.S., . *Computer Science, Boston University, June* .

Nigel Inkster .(2017) .Measuring Military Cyber Power . ‹*Global Politics and, Strategy* ‹Volume 59,Issue 4.-

van Haaster Jelle .(2016) .Assessing Cyber Power, 8th International Conference on Cyber Conflict Cyber Power, NATO CCD COE Publications.

Print ISSN 2771-1161
Online ISSN 2771-1153