مجلة البحوث المالية والتجارية
المجلد (25) – العدد الثاني – إبريل 2024

رؤية تحليلية للثورة السيبرانية

An Analytical Vision of Cyber Revolution

الباحث / أحمد محمود صفى الدين عبد العزيز ماضي

باحث دكتوراه– كلية التجارة

جامعة بورسعيد – قسم العلوم السياسية والادارة العامة

إشراف

أ.د / محمود السعيد محمود
نائب رئيس جامعة القاهرة
للدراسات العليا والبحوث

أ.د / وئام السيد عثمان
أستاذ ورئيس قسم العلوم السياسية
كلية التجارة – جامعة بورسعيد

	تاريخ الإرسال	2024-02-05
	تاريخ القبول	2024-02-08
	رابط المجلة:	https://jsst.journals.ekb.eg/

الملخص:

سعت الدراسة للإجابة عن الإشكالية الرئيسة التي تمثلت في ماهي أساليب الدفاع والردع الإلكتروني لتحقيق الأمن السيبراني؟ من خلال عدة محاور تناولت عدة مفاهيم كالقوة السيبرانية ، الفضاء السيبراني ، الارهاب السيبراني ، والأمن السيبراني واستخدمت الدراسة المنهج النظري بطريقته الاستنباطية، والمنهج العلمي بطريقته الاستقرائية حيث إنهما أساس طرق البحث في المعرفة السياسية ، فقد أتبعت الدراسة إطارا منهجيا متكاملًا ، وهو ما تَوصى به الدراسات الحديثة فقد أهتمت الدراسة بظاهرة السيبرانية من حيث قوتها ومجال استخدامها والتهديدات والتحديات التي تجابها الدول في هذا المجال ، فأمكن الاستفادة من المنهج الوصفي الذى يهتم بدراسة الظواهر الطبيعية ، والاجتماعية، والدراسات الوصفية والسياسية، كما أمكن أيضًا الاستفادة من منهج التحليل النسقي ، والمنهج الاستقرائي .

توصلت الدراسة الى مجموعة من النتائج أهمها انه أصبح الفضاء السيبراني ساحة جديدة للصراع بشكله التقليدي ولكنه ذو طابع سيبراني وكشف استخدام الفضاء السيبراني عن حالة التعارضِ الحقيقي للاحتياجات والقيم والمصالح بين العديد من الفاعلين ، وساعد ذلك على ظهور أساليبِ جديدة للصراع الدولي ، تباينت بين الطابع التقني و التجاري و الاقتصادي والسياسي العسكري ،إلى جانب ظهور طرق بديلة عن الحرب المباشرة بين الدول عبر شبكات الاتصال والمعلومات.

وجاءت من أهم التوصيات السعي لتطويرآليات التعاون الدولي مع الدول الصديقة والمنظمات الدولية والهيئات الاقتصادية والسياسية في مجال تبادل الخبرات ومجالات التعاون في موضوعات الأمن المعلوماتي والسيبان ومكافحة الحروب السيبرانية والجريمة السيبرانية مع السعي إلى نشر ثقافة الأمن السيبراني بين فئات المجتمع وتطوير برامج التوعية لفئات المجتمع من مستخدمي الإنترنت وكذا في الشركات والجهات الحكومية.

الكلمات الافتتاحية :

القوة السيبرانية ، الفضاء السيبراني ، الإرهاب السيبراني ، الأمن السيبراني والدفاع والردع الإلكتروني.

Abstract:

The monograph aimed to address the main problem, which revolved around identifying the methods of electronic defense and deterrence to achieve cybersecurity. It covered several dimensions, exploring various concepts such as cyber power, cyberspace, cyberterrorism, and cybersecurity. The monograph employed a theoretical approach using deductive methods and a scientific approach using inductive methods, as they form the foundation for research in political knowledge. The monograph followed an integrated methodological framework, recommended by contemporary research. It focused on the phenomenon of cyber power, examining its strength, scope of application, and the threats and challenges faced by nations in this domain. The descriptive method, which investigates natural and social phenomena, as well as descriptive studies in politics, were utilized. Additionally, the monograph benefited from the systematic analysis approach and the inductive approach as well.

The monograph yielded a set of findings, the most significant of which is that cyberspace has become a new arena for conflict, with a cyber-nature, diverging from traditional forms. The utilization of cyberspace unveiled a genuine clash of needs, values, and interests among numerous actors. This facilitated the emergence of novel methods for international conflict, encompassing technological, commercial, economic, political, and military dimensions. Additionally, alternative approaches to direct interstate warfare have surfaced, utilizing communication networks and information systems.

One of the key recommendations involves seeking the enhancement of mechanisms for international cooperation with friendly nations, international organizations, and economic and political entities in the exchange of expertise and collaboration in the fields of information security, cybersecurity, combating cyberwarfare, and cybercrime. This includes efforts to promote a culture of cybersecurity among various segments of society and develop awareness programs for internet users, as well as within companies and government entities.

Key Keywords:

Cyber power, cyberspace, cyberterrorism, cybersecurity, electronic defense and deterrence.

أولاً : المقدمة :

يعتبر تعريف مصطلح الفضاء السيبراني من المصطلحات التي مازالت تخضع للتطورات العلمية والسياسات العالمية واستمراريتها وموقفها من السيطرة والتحكُّم في فاعليات ومجريات الحياة بمستوياتها المتعددة والمتنوعة والمتباينة والمركَّبة ومن خلال مجالات و ميادين العمليات الرقمية والإلكترونية والتكنولوجية العلمية المتعددة والمتداخلة والمركَّبة والتي تستهدف إنشاء وتخزين وحفظ وتعديل واستغلال المعلومات والسيطرة عليها من خلال ابتكارات نظم وهندسة وفاعليات المعلومات المترابطة ومعلومات شبكة الإنترنت العنكبوتية والبنية التحتية .

يعد وليام جيبسون Gibson William أول من استخدم كلمة cyber مقترنة بكلمة space لتظهر في مصطلح الفضاء السيبرانى١٩٨٤م. وقد جاء استخدام الفضاء السيبراني كنمط من استخدام القوة عن طريق التأثير على عمل مصادر المعلومات وأنظمة الاتصالات عن طريق الهجوم السيبراني بما يؤدى ذلك إلى إرباك عمل البنية التحتية الحيوية في كتابة الكلاسيكي عام ١٩٨٤م (١)cyber space أثناء دراسته لموضوع القيادة والسيطرة والاتصال في عالم الحيوان، فضلًا عن الهندسة الميكانيكية .

كما عرف الاتحاد الدولي للاتصالات ووكالة الأمم المتحدة المتخصصة في مجال تكنولوجيا المعلومات والاتصالات الفضاء السيبراني بأنه الحيز المادي وغير المادي الذى ينشأ أو يتكَّون من جزء أو من كل العناصر التالية : حواسيب أجهزة ممكنة وشبكات ومعلومات محوسبة وبرامج ومضامين ومعطيات مرور ورقابة والذين يستخدمون كل ذلك [٢] ، والفضاء السيبراني هو مجال عالمي داخل بيئة المعلومات تم تشكيله من خلال استخدام الإلكترونيات، واستغلال المعلومات عبر الشبكات المترابطة والمرتبطة باستخدام تكنولوجيا المعلومات والاتصالات. ويمكن تعريفه على أنه امتداد للوسائط الرقمية عبر خطوط نقل مختلفة معدنية وألياف بصرية ولاسلكية وقنواتها على شبكات الإنترنت، إذ يعد الفضاء السيبراني التعبير التكنولوجي الفائق السرعة للمعلومات.

كما عرَّفته الوكالة الفرنسية لأمن أنظمة الإعلام ANSSI وهى وكالة حكومية مكلفة بالدفاع السيبراني الفرنسي على أنه فضاء التواصل المشّكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية (٣). وهناك من يرى فيه واحداً من سبع مجالات إلى جانب الجو والفضاء الخارجي والبحر والبر والفضاءين الإلكترومغناطيسى والإنساني وأنه ساحةُ الحرب الخامسة بعد البر والبحر والجو والفضاء.

ومما سبق يمكن تعريف مصطلح الفضاء السيبراني على أنه التعامل مع العالم من خلال شبكة الكترونية لها استقلاليتها من الداخل وتقوم بنيتها الأساسية على التقنيات الحديثة وهو أيضاَ أنظمة التعامل مع الحاسب وهو المجال المجازي لأنظمة الحاسب والشبكات الإلكترونية حيث تخزن المعلومات إلكترونياً وتتم الاتصالات المباشرة على الشبكة لذا فهو عالم مادى يشمل مواضيع مثل المعلومات الشخصية والمعاملات الإلكترونية والملكية الفكرية وغيرها من المواضيع ذات الصلة .

ويرتبط الفضاء السيبراني ارتباطا وثيقاً وعملياً وتفاعلياً بما يعرف بالمجتمع الافتراضي كأحد أكثر مجالات وميادين وتطبيقات وتأثيرات الفضاء السيبراني والمجتمع الافتراضي ويعنى جماعة من البشر تربطهم اهتمامات مشتركة ولا تربطهم بالضرورة حدود جغرافية أو أواصر عرقية أو قبلية أو سياسية أو دينية يتفاعلون عبر وسائل الاتصال ومواقع التواصل الاجتماعي الحديثة ويطورِون فيما بينهم شروط الانتساب إلى جماعة وقواعد الدخول والخروج وآليات التعامل والقواعد والأخلاقيات التي ينبغي مراعاتها.

ثانياً : أهداف الدراسة :

تتمثل الأهداف الرئيسة للدراسة في عرض أبرز الإسهامات والنظريات المعنية بالثورة السيبرانية وتأثيراتها في مجال العلاقات الدولية، وكذا أساليب تحقيق الدفاع والردع الإلكتروني لتحقيق الأمن السيبراني في ظل هذه النظريات.

ثالثاً : أهمية الموضوع :

تعود أهمية الدراسة إلى اعتبارين : (موضوعي، وشخصي) :

الاعتبار الأول : الناحية الموضوعية : وتتمثل في (الأهمية العلمية، والأهمية العملية) كما يلى :

أ – الأهمية العلمية تتمثل في :

(١) أنها استكمال للدراسات التي أجريت في مجال الثورة السيبرانية .

(٢) تقديم زاوية جديدة في تحليل مدى تأثير الثورة السيبرانية على الدولة المصرية والنظام الدولي .

ب– الأهمية العملية تتمثل في :

(١) التوصُّل إلى حلول للتحديات والتهديدات الناجمة عن الثورة السيبرانية على الدول .

(٢) تنصرف الأهمية العملية إلى نتائج الدراسة وتوصياتها التي تسهم في وضع آليات للحد من مخاطر الثورة السيبرانية .

(٣) هذه الدراسة تمثل تجربة يمكن للدول الأخرى التي تتشابه ظروفها مع مصر أن تستفيد منها .

الاعتبار الشخصي ويتمثل في :

محاولة الباحث استكمال البحث في مجال العلاقات الدولية باعتباره جزءاً لا يتجزأ من العلوم السياسية ، بما يحدثه ذلك من التراكم العلمي الإيجابي لدى الباحث .

رابعاً : تساؤلات الدراسة :

التساؤلات الرئيسة : تتركز تساؤلات الدراسة في السؤال الرئيس وهو :
ما مدى تأثير الثورة السيبرانية على النظام الدولي ؟

وفى إطار هذا التساؤل الرئيس ، يمكن الإجابة على التساؤلات الفرعية التالية :

أ – ماهية القوة السيبرانية ؟

ب– ما هو الفضاء السيبراني ؟

ج – ما هو مفهوم ومشتملات الإرهاب السيبراني ؟

د – كيف يمكن تحقيق الأمن السيبراني ؟

هـ – ماهي أساليب تحقيق الدفاع والردع الإلكتروني لتحقيق الأمن السيبراني ؟

خامساً : حدود الدراسة (المجال الموضوعي – المجال الزمنى) :

المجال الموضوعي :

تناولت الدراسة موضوع الثورة السيبرانية وتأثيرها على النظام الدولي وتكمن أهمية الدراسة في كون القوة السيبرانية لها تأثيرها على النظام الدولي بوجه عام والدولة المصرية بوجه خاص حيث تمثل الثورة في مجال المعلومات والاتصالات إحدى آليات القوة الناعمة التي كان لها أثرها على النظام الدولي ، وعلى الدولة المصرية على المستوى القومي والإقليمي والدولي .

المجال الزمنى :

أ – تم التناول القوة السيبرانية المصرية في الفترة (٢٠٠٠ – ٢٠٢٠) مع التركيز على التأثيرات الناتجة عن فترة ما يطلق عليه ثورات الربيع العربي والتي رسَّخت استخدام الثورة السيبرانية كآلية للقوة الناعمة على المستوى الداخلي لهذه الدول بوجه عام والدولة المصرية بوجه خاص.

ب–كما شهدت هذه الفترة العديد من التطورات في العلاقات المصرية على المستوى الدولي والإقليمي والإفريقي والعربي واحتلال مصر لمكانة متقدمة في مجال التأمين السيبراني وزيادة تأثيرها الدولي .

سادساً : الدراسات السابقة :

الدراسات السابقة التي قام الباحث بمراجعتها لم تتناول تأثير الثورة السيبرانية على الأمن القومي المصري، ولم تتناول جهود الدولة المصرية في تعزيز أمنها السيبراني ، كما أنها لم تتناول النظرة المستقبلية للدولة المصرية لتأمين مرافقها الحيوية الاستراتيجية من المخاطر

والتهديدات الواردة عبر الفضاء السيبراني والسماوات المفتوحة ، ولم تشمل الدراسات السابقة النظرة المستقبلية لدعم الأمن السيبراني المصري باستغلال قوتها الناعمة.

سابعاً : الإطار المنهجي للدراسة :

تعددَّت طرق البحث في علم السياسة ما بين المناهج والاقترابات والأدوات المنهجية إلا أنه مازال كلاً من المنهج النظري بطريقته الاستنباطية، والمنهج العلمي بطريقته الاستقرائية هما أساس طرق البحث في المعرفة السياسية ، فالمعرفة السياسية كمعرفة واقعية تبدأ من الواقع الاجتماعي لتحليله وتعتمد في ذلك على الملاحظة وهى أداة المنهج العلمي الاستقرائي ، ثم يتم الاختيار من بين أحداث الواقع المراد تحليله ما يعبِر منها عن الطابع السياسي للإنسان لنظمها في نسق كلى أي في صورة كلية وذهنية تتمثل بها الظاهرة السياسية وفى هذا يرتبط منهج المعرفة السياسية بالأسلوب النظري [٤] ، ومن أجل تحقيق التكامل المنهجي ، وتوخّى المزيد من الدقّة، والموضوعية وصولاً للنتائج، تستخدم الدراسة تطبيق منهج بحثى طبقاً للهدفَ الأساسي الذى تسعى إليه الدراسة. فقد أتبعت الدراسة إطاراً منهجيا متكاملاً، وهوما توَصى به الدراسات الحديثة ، فاستخدمت أكثر من منهج ويتحدد منهج البحث على ضوء طبيعة البحث وهدفه ، ويركز أنصار هذا المنهج في دراسة العلاقات الدولية على كل ما يتعلق بالمصلحة الوطنية ، كما أمكن الاستفادة من المنهج الوصفي الذى يهتم بدراسة الظواهر الطبيعية ، والاجتماعية ، والدراسات الوصفية والسياسية ، ودراسة كيفية توضيح خصائص الظاهرة ومدى ارتباطها بالظواهر الأخرى ، كما أمكن أيضًا الاستفادة من منهج التحليل النسقي[٥] ، والمنهج الاستقرائي لاستخدامه في تقديم تصور متكامل لتحقيق الدفاع والردع الإلكتروني لتحقيق الأمن السيبراني .

وفى ضوء ما سبق ولتوضيح أبعاد الثورة السيبرانية يتم تناولها من المحاور التالية :

المحور الاول : الفضاء والقوة السيبراني :

- أهم سمات الفضاء السيبراني هي:[٦]

أ - مجال عملياتي حيث يعد الميدان الخامس للحروب المدنية .

ب- تعد البنية التحتية لأنظمة الاتصالات وتقنية المعلومات جزءاً أساسيا من الفضاء السيبراني .

ج- الفضاء السيبراني لا يقتصر على شبكة الإنترنت فقط وإنما شبكات عالمية أخرى مثل /GPS / ACARS/ SWIFT .

مكونات الفضاء الإلكتروني :

بعد أن أصبح الفضاء الإلكتروني بما يحمله من أدوات تكنولوجية تلعب دورا هاما في التعبئة والحشد في العالم فضلًا عن التأثير في القيم السياسية ، كان لابد من معرفة أهم المكونات الأساسية التي تلعب الدور الهام في مفهوم الفضاء الإلكتروني، إذ يتكون الفضاء الإلكتروني من ثلاث طبقات وهى :

١- الطبقة المادية : أو المكون المادي أو الطبيعي وهى تشمل البنية التحتية المعلوماتية من معدات الحواسيب ، البرمجيات ، والمعدات الضرورية لعملية الربط بين الفاعليين الدوليين واستخدام تكنولوجيا المعلومات مثل الأسلاك والمحولات .

٢- الطبقة المنطقية أو المحتوى : وهى تعكس شكل المعلومات في الفضاء الإلكتروني ، حيث تشمل مجموع البرامج المترجَّمة للمعلومة على شكل معطيات رقمية ، حيث يتم الانتقال من لغة الإنسان والعمليات التقليدية إلى لغة الآلة في شكل خوارزميات واستخدام العمليات الحديثة في التفاعل باستخدام برامج مطورة بلغة البرمجة .

٣- الطبقة الإعلامية وعملية الاتصال : وتتمثل في البعد الاجتماعي للشخص وهى مكملة للمكونين السابقين ، حيث أن الفضاء الإلكتروني يمكن أن يكون لكل إنسان عدة هوِيات رقمية سواء العنوان ، البريد الإلكتروني، رقم الهاتف أو صورة على مواقع التواصل الاجتماعي ، تتمثل في عملية الاتصال بين المعلومات والبشر[٧]. الثلاث طبقات مكملين لبعضهم البعض وكل مكوِن أو طبقة يخدم على الآخر وتنتقل عملية التأثير والتأثر من وإلى الفضاء السيبراني عبر مسارات القوة أو اتجاهات سيطرت على المجال العام الدولي [٨].

أ – المسـار الأول: يتعلق بعملية الانتقال للأحداث من أرض الواقع إلى الفضاء السيبراني

ب – المسار الثاني: يتعلق بانتقال وتحديد الفضاء السيبراني لعناصر تهديد إلى أرض الواقع عن طريق الاستجابة .

جـ – المسار الثالث: يتعلق بدور الفضاء السيبراني كوسيلة إعلام يتم استخدامها كنشاط موازٍ للحوادث على الأرض .

د – المسار الرابع : ويتعلق بما يتم نشره عبر الفضاء السيبراني مثل إطلاق الفيروسات أو القرصنة أو سرقة المعلومات أو التجسس .

٤- واقترن الفضاء السيبراني بمفاهيم مختلفة منها انعدام الجغرافية وظهور جغرافيا الإبحار المعلوماتي في اتجاهات شتى، وهذا ما جعل ظاهرة الفضاء السيبراني أهم خصائص عصر المعلومات إذ تجمع تكنولوجيا المعلومات والاتصال ما بين تكنولوجيا المعلومات أو المعلوماتية ، والتي هي مجموعة من الوسائل المستخدمة لإنتاج واستغلال وتوزيع المعلومات بكل أشكالها مكتوبة، مسموعة ومرئية وتكنولوجيا الاتصال وهى البنية التحتية التي تمكن التواصل الاجتماعي وتؤمن انتقال الرسالة من مرسل إلى متلقى[٩] ويمكن توضيح مكونات تكنولوجيا المعلومات والاتصال كما يأتي :

أ – الأجهزة : وتعرف على إنها الجزء المادي لتكنولوجيا المعلومة المتمثل بالحواسيب والأجهزة الملحقة بها لتنفيذ المهام المطلوبة[١٠].

ب– الإنترنت : ويعرف على أنه الترابط الهائل لشبكات الحاسب ذات النطاق العالمي التي تمكن الاتصال بين البرامج التكنولوجية المتباينة ، أو إنه نظام الحواسب الذى يربط معاً (تشابك) في النظام ليسمح بتبادل المعلومات والمصادر، وإن استخدام الحواسب المرتبطة بواسطة وسائل الاتصالات مثل التليفونات يجعل سهولة تواصُّل كل الأفراد عبر العالم .[١١]

جـ – البرمجيات : وتتألف برمجيات الحاسب من تعليمات مبرمجة ومفصلة بهدف السيطرة والتنسيق على مكونات الأجهزة المادية في نظام المعلومات والبرمجيات وهى برامج الحاسب التي تحكم عمل المكونات المادية وتتولى مهام تطبيقات مختلفة .

د – الشبكات : وهى عبارة عن مجموعة من الحواسب تنظم معا وترتبط بخطوط أتصال بحيث يمكن لمستخدمها المشاركة في الموارد المتاحة ونقل تبادُّل المعلومات فيما بينها ، تستخدم هذه الشبكات لتحقيق مجموعة من الأغراض مثل توفير الاتصال بين الأشخاص ، والوصول للمعلومات عن بعد ، والتجارة الإلكترونية وتخفيض الوقت والمصروفات ، وهناك عدة أنواع من الشبكات منها المحلية والمنطقة والواسعة .

ومما سبق يرى الباحث أن السيبرانية مجال آخر لاستعراض القوى ، وممارسة النفوذ وتحقيق التفوق والتنافس الدولي ، فلم تعد ترسانات الأسلحة التقليدية وأسلحة الدمار الشامل هي المعيار الأساس لقياس القوة بعد الثورة المعلوماتية ، إذ وفرت تكنولوجيا المعلومات والاتصال أسلحة من نوع جديد .

٣– القوة السيبرانية :

أفرزت الثورة المعلوماتية شكلاً جديداً من أشكال القوة هي القوة السيبرانية ، وذلك نتيجة للتقدم التكنولوجي السريع في أجهزة الكومبيوتر والاتصالات والبرمجيات بحلول القرن الحادي والعشرين .

مفهوم القوة السيبرانية cyber power :

ظل مفهوم القوة السيبرانية موضع جدل للكثير، فإحدى المحاولات لتعريف القوة السيبرانية تنص على إنها القدرة على استخدام الفضاء السيبراني لخلق مزايا وتأثير الأحداث في جميع البيئات وعبر أدوات القوة ، ويبقى مبدأ «القوة» الأكثر قابلية للتطبيق للدول الباحثة عن تفاعل استباقي في المجال الدولي بمعنى « إنشاء الفرص الاستراتيجية عبر الفضاء السيبراني » .

وقد حدد «جوزيف ناي» مصطلح القوة السيبرانية لفهم الدور الذى يؤديه الإنترنت في تشكيل قدرة الأطراف الدولية ، والتي يعد من أبرزها الأطراف الدولية والدول الناشئة لتحقيق أهدافها. إن العصر الإلكتروني قد قلل من الصعوبات، لكنهَّ في الوقت نفسه فرض تحديات كبرى على هؤلاء الأطراف خاصةً الولايات المتحدة المحتكرة لمصادر القوة منذ نهاية الحرب الباردة (١٢).

ويمكن تعريف القوة السيبرانية أيضًا من حيث مجموعة الموارد التي تتعلق بالتحكم والاتصال بالمعلومات الإلكترونية والمعلومات المستندة إلى الكومبيوتر والبنية التحتية والشبكات والبرمجيات والمهارات البشرية، أو هي القدرة على الحصول على النتائج المرجوة من خلال استخدام موارد المعلومات المترابطة إلكترونياً في الفضاء السيبراني[١٣]، لإيجاد مزايا الدولة والتأثير على الأحداث المتعلقة بالبيئات التشغيلية الأخرى، وذلك عبر أدوات إلكترونية وإنها مجموعة من الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الإلكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدَّربة [١٤] للتعامل مع هذه الوسائل

المحور الثاني : الإرهاب السيبراني :

كانت بداية استخدام مصطلح الإرهاب الإلكتروني في ثمانينيات القرن الماضي والتي خلص فيها إلى صعوبة تعريفٍ شامل للإرهاب التكنولوجي ، ولكنه تبنَّى تعريفاً للإرهاب الإلكتروني مقتضاه أنه هجمة إلكترونية غُرضُها تهديد الحكومات أو العدوان عليها سعيا لتحقيق أهداف سياسيةٍ أو دينيةٍ أو أيدولوجية ، وأن الهجمة يجب أن تكونَ ذات أثرٍ مدمر تخريبي مكافئ للأفعال المادية للإرهاب، ومن خصائص الإرهاب السيبراني غياب جهة السيطرة والرقابة على الشبكة المعلوماتية ، إذ لا توجد جهة مركزية موحدة تتحكم فيما يعرض على الشبكة وتتحكم في مدخلاتها ومن ثَمَّ مخرجاتها .

تغيرت خُطط الإرهاب وأدواته المستخدَمة بمرور الوقت ظهر الإرهاب السيبراني الذى يستهدف فيه الإرهابيون البنيه التحتية للدول وأنظمة معلوماتها وقواعدها العسكرية وذلك بسبب ضعف منظومات الحماية وعدم وجود أطر تشريعية واضحة لتنظيم الفضاء السيبراني بالإضافة للانتشار الهائل لتكنولوجيا الاتصال والمعلومات وزيادة الاعتماد عليها مما أدى إلى إمكانية ارتكاب جرائم سيبرانية يصعب على الأجهزة الأمنية المتخصصة تتبعها أو الوصول إلى مرتكبيها

تعريف الإرهاب السيبراني :

١- الإرهاب بصفة عامة هو كل فعل (مادى أو معنوي) يهدف إلى خلق حالة من الترويع أو الترهيب أو إشاعة الذعر بين الناس أو الإخلال بسلامة المواطنين أو إلحاق الضرر بالبنى التحتية للدول (المنشآت الحيوية – أجهزة الدولة – ...) ويرتكب مادياً باستخدام كلًا من (الأسلحة

والذخائر – والمتفجرات) ومعنوياً باستخدام أي أداة أخرى تؤدى الغرض ذاته (الشائعات – التأثير على الروح المعنوية) .

٢-الإرهاب السيبراني أصبح شائعاً في السنوات الأخيرة وبات خطرا كبيراً على الصعيد الدولي ولا سيَّما مع التطور السريع لتقنيَّات الاتصال والاعتماد المتزايد للبشر على (الإنترنت) ووسائل التواصل الاجتماعي إلا أنه ليس هناك تعريف عالمي متفق عليه للإرهاب السيبراني .٣-يعرف مكتب التحقيقات الفيدرالي الأميركي الإرهاب السيبراني بأنه : (هجوما متعمداً ضد نظام كمبيوتر وبياناته وبرامجه وتطبيقاته ومعلومات أخرى بهدف التسُّبب في الضرر والدمار) .

٤-عرَّفت وزارة الدفاع الأميركية الإرهاب السيبراني بأنه : (عمل إجرامي يتم الإعداد له باستخدام الحاسبات ووسائل الاتصالات ينتج عنها عنف وتدمير أو بث الخوف وذلك بهدف التأثير على الحكومة أو السكان لكى تمتثل لأجندة سياسية أو اجتماعية أو فكرية معينة) .

٥- مما سبق يمكن تعريف الإرهاب السيبراني على أنه (كل فعل يتم باستخدام الوسائل والأساليب المعلوماتية أو الإلكترونية وبغرض ارتكاب أعمال عنف أو ترويع الآخرين وإلحاق الضرر بهم أو تهديدهم بغرض سيأسى أو أيدولوجية لفرض إرادة سياسية أو عقائدية محددة على متخذ القرار أو التأثير على توجهات الرأي العام ويمكن أن يتم الإرهاب السيبراني من قبل أفراد أو منظمات وقد تنشأ هذه الهجمات من قبل دول أو جهات مجهولة المصدر)

خصائص الإرهاب السيبراني :

يتسم الإرهاب السيبراني بالعديد من الخصائص التي تميِّزه عن الإرهاب في صورته التقليدية وذلك على النحو الاتي :

١- الإرهاب السيبراني هو إرهاب عابر للقارات والحدود ولذا لا يخضع لأى نطاق جغرافي معين ويندرج تحت مظلة الجريمة السيبرانية والتي تحدث بطبيعة الحال في بيئة رقمية يحتاج مرتكبها لاستخدام الحاسب الآلي حيث يتسم مرتكبي جرائم الإرهاب السيبراني بالخبرة في استخدام تكنولوجيا المعلومات وبالتالي تكون أهدافهم ليست صعبة المنال .

٢-صعوبة تتبع أثر الجاني في جرائم الإرهاب السيبراني حيث يوجد العديد من الصعوبات التي تقف حائلًا دون الوصول لدليل مادى يربط الجاني بالواقعة نظرا لاعتماد المنظمات الإرهابية التي ترتكبه على كوادر محترفة ونقص خبرات الأجهزة الأمنية في التعامل معه بالإضافة إلى عدم وجود تشريعات تَجِّرمه ببعض الدول ويعد أحد أخطر أنواع الإرهاب حيث يؤثر بالسلب على الأمن القومي للدول المستهدفة.

٣-لا يحتاج في ارتكابه إلى العنف والقوة بل يتطلب وجود حاسب آلي متصل بالشبكة المعلوماتية ومزود ببعض البرامج اللازمة ، يتعاون فيه عدة أشخاص قد يكونوا من مختلفي الجنسيات وتشترك في استخدامه عدة منظمات مع اختلاف الوسائل والأساليب.

٤-يحتاج إلى خبرات معينة للتَحُّفظ على الأدلة الرقمية بسبب سهولة إتلافها وتدميرها.

فواعل الفضاء الإلكتروني :

فتح الفضاء السيبراني الباب على مصراعيه لفواعل جديدة غير الدولة ، إذ أسهمت في مجمل العمليات السيبرانية ويمكن تقسيم هذه الفواعل في الفضاء السيبراني إلى ما يلى :

أ - الدول : وتمثل الخطُ الأكبر والفاعل والأكثر قوة في مجال الفضاء السيبراني[١٥]، مما قد يدفع الفواعل من الدول وغير الدول للتنافس من أجل التفوق السيبراني واعتبرت الدولة لزمنٍ طويل الفاعل الرئيسي والأول في السياسة الدولية ، والمؤثرة بصفة كبيرة في مسارات وتوجهات السياسة الدولية على الرغم من التفاوت الحاصل بين الدول وهى تشكل لاعبا محورياً ، وقد أصبح العالم حسب منظور المدرسة الواقعية في حركة التفاعل الدولي الرقمي هو عنوان للوحدات الدولية الفاعلة، إذ يرى «زيغني برجسك» أنه يبدو أن دور الدولة يتراجع كوحدةً أساسيةً في المجتمع الدولي وفى حياة الفرد ويعود هذا الانحسار إلى نهاية الحرب الباردة .

ب- فواعل من غير الدول : يعرِّف بريان هوكين Brain Hocking ومايكل سميث Michael Smith الفاعلين من غير الدول Non state actors بأنهم جماعةٌ أو منظمة تتمتع بالاستقلال ، أي بمقدار من الحرية عن السعي لتحقيق أهدافها و تمثيل

أتباعها ومؤيديها ، والنفوذ أي القدرة على إحداث فرق تجاه قضية ما في سباق معين مقارنة بتأثير فاعل آخر في القضية ذاتها [١٦] ويمكن تقسيمهم إلى ما يأتي :

(١) المنظمات الدولية : وهى ظاهرة حديثة نسبيا فأول هذه الظاهرة كان سنة ١٨١٥م وهى "اللجنة المركزية لتنظيم الملاحة في الراين"، إلا أن عدد هذه المنظمات تزايد بسرعة كبيرة وذلك لتلبية ضروريات الحياة في الجماعة الدولية ، وتشير بعض التقديرات إلى أنه يوجد في عالم اليوم حوالى ٣٦٠ منظمةً دوليةً. والمنظمة عبارة عن هيئة أنشأتها مجموعة من الدول بإرادتها للإشراف على شأن من شئونها المشتركة وتمنحها اختصاصات ذاتية تباشرها هذه الهيئة، وتكون هذه في المجتمع الدولي وفى مواجهة الدول الأعضاء نفسها كهيئة الأمم المتحدة. وهناك منظمات دولية غير حكومية وهى عبارة عن بنية تعاونية في مجال محدد وتجمع مؤسسات غير دولية مثل منظمة أطباء بلا حدود ومنظمة العفو الدولية وغيرها وعلى المستويين من المنظمات والاتحادات والنقابات بمختلف أشكالها [١٧] الدولي والإقليمي .

(٢) الشركات المتعددة الجنسيات : وهى شركات ذات بعد اقتصادي إذ تحتكر المال والأسواق وتحظى بامتيازات من قبل الدول طمعا في الاستثمار، وتضغط على الدول من أجل إنقا ص قيمة الضرائب والجمارك، وتدعى أحياناً شركات عابرة للقوميات، وهى عبارة عن لاعبين نافذين يقومون بنشاطات تجارية لقاء الربح في أكثر من بلد.[١٨]

(٣) الأفراد: ساعدت تكنولوجيا المعلومات والاتصالات والإنترنت الفاعلين من غير الدول على امتلاك القوة السيبرانية وتشكيل شركات عالمية بعيدة عن سيطرة الدولة، إذ وفر الفضاء السيبراني بيئة مناسبة لتواصل الأفراد، ويمكن تقسيمهم إلى أربع فئات رئيسية كما يلى :

(أ) المبتدئون: وهم فئة تمتلك قدرات ومهارات باستخدام لغة برمجية في جهاز الحاسوب ، وعاد ة ما يكون أعمار هذه الفئة سن المراهقة ويكون هدفهم الرئيسي هو تحقيق المغامرة والإثارة في الفضاء السيبراني فضلًا عن رغبتهم بأن يصبحوا قراصنة .

(ب) القراصنة : وهم أشخاص لهم القدرة على التعامل مع أنظمة الحاسب الآلي والشبكات وتخطى أي إجراءات أو أنظمة حماية اُتخذت لحماية تلك الحاسبات أو الشبكات، وتعود بداية القرصنة إلى ستينيات القرن الماضي، إلا أن أول عملية قرصنة قد سجِلت عام 1878م بإحدى شركات الهاتف المحلية الأمريكية، ولعل أشهر القراصنة الأمريكي «كيفن متينيك» الذى يعد أشهر هاكرز في التاريخ ، وقد أطلق على نفسه The mentor، وقد قام بنشر دراسة شهيرة تعرف باسم «بيان الهاكر» وهو بيان رسمي لأهداف ووجهات نظر القرصان، نُشرت الدراسة في المجلة الإلكترونية Prick، ومن ثم تم اعتقاله، وتَعد الدراسة أشهر ما كُتب عن قرصنة الحاسوب.

وتكلف القرصنة اقتصاد العالم نحو ٥٧٥ بليون دولار أمريكي سنويا، وإن أشهر حروب الإنترنت هي «حرب الهاكرز العظمى» التي دارت رحاها بين عامي ١٩٩١م- ١٩٩٤م بين فريقين من الهاكرز المحترفين، وشهد عام ٢٠٠٢م حرباً سيبرانية دولية بين الهاكرز العرب المسلمين ضد اليهود، وشهدت الهند مصيراً مماثلًا من قبل هاكرز باكستانيين، وكذا الحرب الأمريكية – الصينية عام ٢٠٠١م بسبب أزمة طائرة التجسس الأمريكية بالصين .

كما تشمل عمليات القرصنة على القرصنة السياسية، وتكون الدوافع الرئيسية من وراء قيام القراصنة السياسيين hacktivism هي دوافع سياسية بالأساس ، ومن أبرز الأمثلة على الجماعات التي تقوم بالقرصنة السياسية هي الجماعة التي أطلقت على نفسها أنين موس anonymous أو المجهولين، وهى تَعد أشهر مجموعات القرصنة، وتضم عدداً كبيراً من القراصنة المنتشرين حول العالم، ويعتمد بعض القراصنة على مهاراتهم للوصول بطريقة غير قانونية وغير مرخص بها إلى معلومات تختزنها ذاكرة الحاسوب، وحين يحصلون عليها يسعون إلى تسريبها بغية جعلها متاحة للناس وخصوصا الصحفيين ورسائلهم الإخبارية ، ويشبه دورهم إلى حد كبير بالمبلغين الذين يحاولون الانتفاع من المعلومات السريَّة whistleblowers، لأنهم يعتقدون أن بقاء هذه المعلومات طي الكتمان جزء من الفساد المؤسسي.

وفيما بعد ظهرت نظرية جديدة لها مجموعة من المبادئ تمكّن من التفسير والاختبار، ومن ثَمَّ توقع المسارات، وهى نظرية الهاكتولوجيا histology وتعرف هذه النظرية بأنها النظرية التي تدرس أي محاولة مقصودة ومتعَّمدة للحصول وجمع وبث معلومات غير متاحة ضمن الفضاء العام وسياقه دون الحصول على موافقة المصدر ومن ثَمَّ نشرها من خلال الإعلام، وتدرس هذه النظرية كل الجوانب والأساليب المتعلقة بالهجمات السيبرانية وقرصنة وتسريب المعلومات ونشر الأخبار المفبركة أحيانا. ويقدم المثربون والمؤسسات والمواقع ما تملكه من محتوى إلى الصحف والقنوات الإخبارية سواء كان مجانى أو بدعم مادى.

(٤) جماعات الإرهاب الإلكتروني : وعادة تسمى هذه الجماعات الفاعلون العنيفون من غير الدول وهم الجماعات أو التنظيمات التي تلجأ إلى استخدام أدوات العنف المادي والنفسي بطريقة جماعية ، من أجل تحقيق غايات معينة ، ولا تنتمى لأجهزة الدولة الرسمية، مثل الحركات الراديكالية والجماعات الأصولية ، إذ تعمل الأخيرة بمتلازمة "البؤر" في تنفيذ مخططاتها أينما وجدت مرفأ أو بؤرة تؤيدّ أفكارها ، فهي تبحث عن المؤيدين والمناصرين لها في العالم .

أساليب الإرهاب السيبراني:

يشتمل الإرهاب السيبراني على العديد من التقنيات التي تستخدم للتخطيط والتحريض والتجنيد وزيادة التطرف والتمويل والتنفيذ والتي تستهدف (النظم العسكرية – البنية التحتية – نظم الاتصالات – نظم المواصلات) ويمكن بلورة أساليب استخدام الجماعات الإرهابية للفضاء السيبراني كالآتي :

إنشاء واستخدام المواقع الإلكترونية :

١- تقوم العناصر الإرهابية بتصميم وإنشاء مواقع على شبكة المعلومات الدولية منها مواقع معلنة وأخرى سرية لبثّ أفكارهم وأيدولوجياتهم وإبراز قوتهم ويطلَق عليها المواقع الجهادية حيث يتم استخدامها في الآتي :

أ – التعبئة الفكرية وتجنيد الإرهابيين الجدد .

ب- إصدار التعليمات والتلقين الإلكتروني .

جـ - التدريب الإلكتروني وتعليم الطرق والوسائل والتكتيكات التي تساعد على القيام بشن الهجمات الإرهابية مع شرح [كيفية صناعة القنابل - المتفجرات - الأسلحة الكيميائية - طرق اختراق (البريد الإلكتروني - المواقع الإلكترونية) وتدميرها - الدخول إلى المواقع المحجوبة التي تحتاج إلى أساليب خاصة للدخول اليها] .

د - تمرير التمويلات من خارج الدول بهدف شراء وتدبير الأسلحة والمعدات .

٢- أمثلة على المواقع الجهادية على شبكة المعلومات الدولية :

أ - "موقع النداء": الموقع الرسمي لتنظيم القاعدة بعد أحداث الحادي عشر من سبتم برعام ٢٠٠١م وكانت من خلاله تصدر البيانات الإعلامية للقاعدة .

ب - "ذروة السنام": صحيفة إلكترونية دورية للقسم الإعلامي لتنظيم القاعدة .

جـ - معسكر البتار : مجلة عسكرية إلكترونية متخصصة تصدر عن تنظيم القاعدة وتختص بالمعلومات العسكرية والميدانية والتجنيد .

د - "شموخ الإسلام" : الموقع الرسمي لجماعة "أنصار بيت المقدس" "وتنظيم داعس" "وجبهة النصرة" بسوريا ومعظم التنظيمات الإرهابية المتطرفة .

المحور الثالث : الأمن السيبراني :

مفهوم الأمن السيبراني :

أ - اصطلاحيا : هناك العديد من التعاريف التي قُدمت لمفهوم الأمن السيبراني، حيث يعرف بأنه مجموعة من الإجراءات المتخذة في مجال الدفاع ضد الهجمات السيبرانية ونتائجها التي تشمل تنفيذ التدابير المضادة المطلوبة .

وهذا ما ذهب إليه الكاتبان Neittaanmäki Pekka,Lehto Martti في كتابهما باسمCyber Security: Analytics, Technology and Automation، حيث أعتبر أن الأمن السيبراني هو "عبارة عن مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكمبيوتر وعواقبها، ويتضمن تنفيذ التدابير المضادة المطلوبة".

ب- بينما عرفَه إدوارد أمورسو Amoroso Edward بأنه " وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها، وتوفير الاتصالات المشفرة " .

وفى التقرير الصادر عن الاتحاد الدولي للاتصالات حول اتجاهات الإصلاح في الاتصالات لعام ٢٠١٠م – ٢٠١١م عرِف الأمن السيبراني بأنه " مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية ومقاربات لإدارة المخاطر، وتدريبات وممارسات وتقنيات يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين " .

وقدمت وزارة الدفاع الأمريكية "البنتاغون" تعريفاً دقيقًا لمصطلح الأمن السيبراني ، فاعتبرته "جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية، من مختلف الجرائم" الهجمات، التخريب، التجسس والحوادث".

في حين اُعتبر الإعلان الأوروبي الأمن السيبراني أنه يعنى" قدرة النظام المعلوماتي على مقاومة محاولات الاختراق التي تستهدف البيانات." وهنا تجدر الإشارة إلى أن الأمن السيبراني مفهوم أوسع من أمن المعلومات ، فالأمن السيبراني يهتم بأمن كل ما هو موجود على السايبر من غير أمن المعلومات ، بينما أمن المعلومات لا يهتم بذلك ، كما أن أمن المعلومات يهتم بأمن المعلومات الفيزيائية" الورقية"، بينما لا يهتم الأمن السيبراني بذلك .

إجرائياً : يمكن القول إن الأمن السيبراني هو مجموعة الآليات والإجراءات والوسائل والأطر التي تهدف إلى حماية (البرمجيات وأجهزة الكمبيوتر) الفضاء السيبراني بصفةٍ عامةٍ من مختلف (الهجمات والاختراقات) التهديدات السيبرانية (التي قد تهدد الأمن القومي للدول).

٤- أهمية الأمن السيبراني وخصائصه :

يعد الهدف الأسمى للأمن السيبراني هو القدرة على مقاومة التهديدات المتعمَّدة وغير المتعمَّدة 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 الكمبيوتر، والبرامج والبيانات من الهجوم أو الضرر أو الوصول غير المصرح به، ونتيجة لأهمية الأمن السيبراني في واقع مجتمعات اليوم فقد جعلته العديد من الدول على رأس أولوياتها، خاصة بعد الحروب الإلكترونية التي بدأت تظهر تجلياتها بين بعض الدول الكبرى في إشارةٍ صريحةٍ إلى نهاية الحروب التقليدية التي كانت تستخدم فيها الأسلحة الثقيلة، والإعلان عن بداية حروب جديدةٍ هي الحروب الإلكترونية ويتميز الأمن السيبراني بمجموعة من الخصائص منها :

أ - طابع متعدد التخصصات الاجتماعية والتقنية .

ب- كونه شبكة خيالية الحجم والقدرات يمكن أن تكون مماثلة على نطاق واسع .

جـ - درجة عالية من التغيير والترابط وسرعة التفاعل .

٥- أبعاد الأمن السيبراني :

أما بالنسبة لأبعاد الأمن السيبراني فإنهَ يطَال جميع المسائل الاقتصادية والسياسية والعسكرية

والاجتماعية والقانونية وفيما يلى توضيح ذلك :

أ - الأبعاد الاقتصادية : أرتبط الأمن السيبراني ارتباطا 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 تُقدّمها الشركاتَ الدولية والشركات الكبرى التي تبحث عن إدارة كَلَفةَ إنتاجها بأفضل الشروط، إلا أن هذا الواقع المشرق يطرح مسائل مختلفة سواء ما تعلق بحماية مقدّم الخدمة والعمل أو بحماية المستهلك عبر الإنترنت، بالإضافة إلى دخول العالم عصر المال الإلكتروني ضمن بيئة تقنية متحركة بعد إطلاق خدمات المحفظة الإلكترونية، إذ تتزايد استثمارات المصارف والمؤسسات المالية في مجال المال الرقمي.

ونظرا لارتفاع معدل الجرائم السيبرانية المنظمة والخطيرة ، فإن ذلك يمثل تهديداً صريحاً لنمو الاقتصاد الرقمي ما لم تقم الدول بتعظيم معايير الأمن السيبراني بما يضمن الحد من هذه الجرائم.

ب- الأبعاد السياسية : هناك أمثلة كثيرة تدفع نحو الاهتمام بالبعد السياسي للأمن السيبراني ، كالتسريبات المختلفة للوثائق الحساسة التي تؤدى إلى مشكلاتٍ جسيمةٍ جداً على المستوى الإقليمي والدولي ، كما أنه لا أحد ينكر الدور المتعاظم لشبكاتٍ التواصل الاجتماعي على المستوى السياسي (حملات انتخابية، تظاهرات افتراضية، حركات احتجاجية إلكترونية ...) كما يتم استغلال هذه المواقع من طرف العديد من الحكومات لتمريرها.

جـ- الأبعاد العسكرية : لقد تجلّت البداياتَ الأولى للإنترنت في بيئة عسكرية بشكل مضاعف، وذلك لكى تنتقل في سياق لاحقٍ إلى الأوساط الأكاديمية والعلمية وأبحاث تستخدم القدرات العسكرية وتتمثل الميزة النسبية للأمن السيبراني في بعده العسكري عن طرق قدرة القوة السيبرانية على ربط الوحدات العسكرية ببعضها البعض عبر العالم الافتراضي، وهذا ما يسهل عملية تبادل المعلومات ونقل الصورة، الذى ينعكس إيجابا على تحقيق الأهداف العسكرية.

د- 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 وبما تكونه من حاجة لدى المجتمع في الحفاظ على استقرار الفضاء السيبراني والمجتمع الذى يرتكز إليه، لكن في المقابل يعرض أخلاقيات المجتمع للخطر، نظرا لصعوبة مراقبة محتوى الإنترنت، كما يعرض الهوِيات لعمليات اختراق خارجي ما قد يتسبَّب في تهديد السلم الاجتماعي للدولة، وعليه فلابد من العمل على توعية المواطن بهذه المخاطر لتحقيق الأمن السيبراني في بعده الاجتماعي .

هـ- 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، إضافةً 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 ، وأيضًا توسعت بعض المفاهيم لتشمل أساليب الممارسة الجديدة باستخدام تقنيات المعلومات والاتصالات ، كالحق في إنشاء المدونات الإلكترونية ، والحق في إنشاء التجمعات على الإنترنت، وأيضًا الحق في حماية ملكية البرامج المعلوماتية. ومما سبق يرى الباحث أن الأمن السيبراني هو بعد جديد ضمن أبعاد الأمن القومي، أحدث تغييرات جوهرية في مفاهيم العلاقات الدولية كالصراع والقوة والتهديد، حيث حتّمِ على فواعل المجتمع الدولي الانتقال من عالم مادى إلى عالم افتراضي في غاية التعقيد والتشابك، وبالتالي أصبح مفهوم الأمن السيبراني ضرورة حتمية في عالم اليوم، خاصة في ظل ارتباط كافة التفاعلات الدولية بالجانب الرقمي والتكنولوجي، الأمر الذى يستدعى على الدول ضرورة إيجاد مكانيات ووسائل فعالة لمواجهة المخاطر والتهديدات السيبرانية التي تتميز بالسرعة والغموض والدقة، ومن ثَمَّة تحقيق الأمن السيبراني والحفاظ على مكاسب الدولة وأمنها القومي.

المحور الرابع : الدفاع والردع الإلكتروني لتحقيق الأمن السيبراني للدول في ظل التحديات الراهنة :

أهداف الدفاع في الفضاء السيبراني :

يهدف الدفاع الإلكتروني إلى الحفاظ على قدرات الأمن الوطني التكنولوجي للدول ، من خطوط اتصالات وشبكات كمبيوتر وبنية تحتية سواء مدنية أو عسكرية ، فضلًا عن تأمين البيانات الحيوية بما يساهم في تحقيق الأمن السيبراني للدول، وفيما يلى يمكن تحديد بعض أهداف الدفاع الإلكتروني[١٩].

١- حماية الأهداف العسكرية : والتي تشمل تأمين نظم الإدارة والمراقبة ونظم التحكم والقيادة والسيطرة ونظم توجيه الأسلحة وقطاع الاتصالات الحربية والأسلحة الآلية القيادة، مثل

الطائرات من دون طيار، فضلًا عن حماية المنشآت العسكرية والحيوية مثل محطات الطاقة النووية من أي اختراق إلكتروني.

٢- حماية البيانات العسكرية : والتي تشمل معلومات حول أفراد القوات المسلحة كالأسماء والرتب والمرتبات والوظائف داخل الجيش وأماكن الإقامة الشخصية ، فضلًا عن خطوط التسليح وتصميمات الأسلحة وخرائط انتشار القوات وتوزيع الأسلحة .

٣- حماية البنية التحتية الحرجة : مثل قطاع الاتصالات والمواصلات ومحطات الطاقة ، وقواعد البيانات الحكومية وخدمات الحكومات الذاتية والبنوك والمؤسسات المالية والقطاع الصحي .

٤- دعم وحدات الحرب الإلكترونية : وهى تلك الوحدات الخاصة بإدارة الحروب السيبرانية للدول ، حيث تكون مهمة الدفاع الإلكتروني هي تأمين الخطوط خلف هذه الوحدات، بما يحمى أهداف الدول الاستراتيجية في حالة شن هجوم إلكتروني مضاد عليها ، وتوفير غطاء إلكتروني للوحدات المقاتلة بهدف التمويه والخداع وصعوبة تعقُّب مصدر الهجمة .

٥- تحقيق الردع الإلكتروني : وذلك من خلال رفع تكلفة الهجوم الإلكتروني للدولة المعتدية، عبر إنشاء نظم دفاع إلكترونية صعبة الاختراق التي تحتاج إلى وقت وجهد كبيرين لاختراقها ، مع تطوير قدرات تتبع الهجمات الإلكترونية واكتشاف مصدرها بما يؤدى في النهاية إلى التأثير على قرارات الخصم وردعه عن شن هجمات إلكترونية على الدولة.

الردع الإلكتروني لتحقيق الأمن السيبراني:

يهدف الردع إلى خلق مجموعة من المحفّزات المانعة لقيام أحد أطراف الصراع من القيام باعتداء أو هجوم مستقبلًا، وإذا كان ذلك هَو هدف الردع في التفاعلات الدولية على أرض الواقع ، فإنه مختلف جزئيا عن حالة الردع الإلكتروني، لأن أحد الفواعل غير قادر على إزالة تدمير الطرف الآخر كليا كما في حالة الردع النووي مثلًا، كما أنه ليس من السهل تحقيق الردع الإلكتروني بسبب خاصية التخفي، والتي تمنع مستخدم القوة الإلكترونية من التعرف على خصمه أو التوقع من أين سوف تأتيه الضربة، وفى ظل نظام دولي يتميز بتعدد القطبية ما يزيد من حالات الصراع، فضلًا عن تعدُّد الفاعلين من الدول وغير الدول الذين يستخدمون فضاء القوة السيبرانية في التفاعلات الدولية، الإضافة إلى خاصية التخفي فإن احمالات الصراع الدولي تزداد مع التقدم التقني.(٢٠)

إنه في ظل تنامى التوتر والصراعات في العلاقات بين الدول على المستويين الإقليمي أو الدولي يتوقع أن تلجأ الدول إلى توظيف الحروب الإلكترونية كأدوات إضافية في إدارة صراعها مع خصومها، خاصة مع تنامى أدوار الفواعل المسلحة من غير الدول ، وهو ما يؤشر

إلى زيادة التهديدات النابعة من الفضاء السيبراني مستقبلاً، مما يتطلب من الدول كافة اتخاذ إجراءات لضبط سلوكها في الفضاء السيبراني، فضلاً عن تطوير القدرات الدفاعية لتأمين نفسها في مواجهة تلك التهديدات [٢١] ، وفى هذا الصدد فإنه يمكن الإشارة إلى أن الدفاع السيبراني الوقائي يتحقق من خلال ثلاثة أساليب رئيسة وهى :

١- الكشف المبكر عن الهجمات في وقتها الحقيقي : وهو ما يتم من خلال استخدام حساسات الشبكات والبرامج والتطبيقات (Sensors)، بالإضافة إلى توظيف المعلومات الاستخباراتية لرصد أي نشاط غير طبيعي قد يصنف على أنه هجمات سيبرانية، وبداية مواجهتها واحتواءها قبل أن تبدأ نشاطها في الشبكة أوعلى النظم المستهدفة .

٢- الهجوم السيبراني الاستباق:

وذلك من خلال استخدام ونشر "الديدان البيضاء" (White Worms) وهى برامج قادرة على اكتشاف التطبيقات الضارة وتدميرها قبل توظيفها في إطلاق هجمات سيبرانية محتملة ، كما تقوم أيضًا بتدمير أدوات وبرمجيات القراصنة، وهو ما يساعد في إحباط مخطط الهجمات نفسها ، وتحديد هوِيَّة ومصدر الهجمة، بما يمكّن من إطلاق هجمة إلكترونية مضادة فيما تعرف بالاختراق العكسي (Hack-back).

٣- التضليل والإخفاء والخداع : وهو ما يتحقق عن طريق إخفاء هوية الأهداف الاستراتيجية للدولة على الإنترنت وتضليل الخصم أثناء محاولة الوصول إليها أو اختراقها ، من خلال أدوات التمويه والخداع وتغيير ملامح الأهداف الاستراتيجية للدولة، بما يساعد على تضليل الخصم وتشتيت الانتباه عن الهدف الرئيسي.[٢٢]

وعلى إثر ذلك قامت كل من روسيا، الصين،" إسرائيل"، بريطانيا، فرنسا، الولايات المتحدة الأمريكية، إيران، كوريا الشمالية بتطوير عقيدتها الأمنية، وأصبحت تعتبر الفضاء السيبراني مسرحا للعمليات العسكرية، كما أوجدت قيادات خاصة ومستقلة لقيادة العمليات السيبرانية [٢٣] ، والتي لديها وحدات قتالية خاصة بالحرب السيبرانية ، حيث تتميز بقدراتها الهجومية والدفاعية المتقدمة ولعل من أبرز تلك الوحدات القتالية الآتي :

أ – "القيادة السيبرانية الأمريكية" (US Cyber Command) والتي استحدثها البنتاغون في شهر يونيو ٢٠٠٩م ، ومهمتها الرد على هجمات قراصنة المعلومات وتنفيذ عمليات في الفضاء السيبراني .

ب– "الوحدة ٦١٣٩٨" في الصين والتي تتسم بأنشطتها السرية داخل جيش التحرير الشعبي الصيني حيث تقوم بعمليات التجسس الإلكتروني وقرصنة المعلومات والبيانات ، وقد بدأت في شن أول هجماتها منذ عام ٢٠١٦م .

جـ– "قراصنة الظل التابعين" للحكومة الروسية وهم من الطلبة المتميزين في استخدام الحاسب الآلي والذين أدمجتهم وزارة الدفاع الروسية في وحدات علمية خاصة، وتجدر الإشارة إلى أن روسيا تمتلك عدد كبير من القراصنة سواء المتطوعين أو الذين تم توظيفهم لخدمة أغراض عسكرية ،وقد كلفّتهم روسيا عام ٢٠٠٧م بشن هجمات سيبرانية سريعة ومدروسة شاملة على إستونيا أدت إلى دمار لوجستي كبير .

د – "الوحدة ٨٢٠٠" في إسرائيل والمسئولة عن قيادة الحرب السيبرانية في الجيش الإسرائيلي وتشكل تحالفاً مع وكالة الأمن القومي الأمريكية والقيادة السيبرانية الأمريكية، وتعتبر أهم وأكبر قاعدة تجسس إلكترونية إسرائيلية في منطقة" النقب "للتنصت على البث الإذاعي والمكالمات الهاتفية، الفاكس، البريد الإلكتروني في قارات آسيا وإفريقيا وأوروبا، ثم أضيفت إليها مهام الحرب السيبرانية في وقت لاحق، وقد أدت هذه الوحدة دورا رئيسياً في ضرب البرنامج النووي الإيراني من خلال تصميم فيروس "ستاكسنت"، مما جعل إسرائيل ثاني أكبر دولة في مجال التجسس والتنصت في العالم بعد الولايات المتحدة الأمريكية ولذلك تلجأ الدول المتمكنة من القوة السيبرانية إلى اعتماد الدفاع والردع السيبراني في آنٍ واحدٍ، حيث تتمحور أهداف الدفاع والردع السيبراني في الحفاظ على قدرات الأمن القومي التكنولوجي للدولة، من خطوط اتصالات وشبكة كمبيوتر وبنية تحتية سواء مدنية أو عسكرية، فضلاً عن تأمين البيانات الحيوية بما يساهم في النهاية في تحقيق الأمن الإلكتروني للدولة .

تبنت الولايات المتحدة الأمريكية" الاستراتيجية الدولية للفضاء الإلكتروني" وهى أول وثيقة سياسية من هذا النوع تبين الرؤية الشاملة لمستقبل التعاون الدولي المتعلق بالفضاء السيبراني، ومن ثمة فإنه من الأهمية ربط الأمن الشامل في الفضاء السيبراني ببذل الجهود الدولية العاجلة والمتكافئة لحل الصراعات بين الدول على أرض الواقع لمنع انتقالها إليه، إذ تبرز أيضًا أهمية العمل على توفيق القوانين المتعلقة بالصراع والحرب في الفضاء السيبراني مع القانون الدولي ،وأهمية المبادرات الدولية لحماية هذا الفضاء، فضلًا عن البحث والتطوير في مجال الدفاعات ضد الأخطار الإلكترونية والذى يتم على كافة المستويات وهى تختلف طبقًا لمعايير محددة مثل :

١- الثقافة الاستراتيجية : التي تعتمد بشكل خاص على المعتقدات المشتركة والتصورات والتاريخ والهويَّة الجماعية والعلاقة مع الدول الأخرى، ومدى قبول المعايير الدولية ، وبالنسبة إلى الدول الصغيرة ، تعد الحرب غير المتماثلة جزءا من التاريخ العسكري لذلك لا يمكن للدول الكبرى اعتماد استراتيجيات غير متماثلة في الفضاء السيبراني .

٢- توصيف التهديدات والتحديات والأولويات.

٣- طبيعة الدولة : دولة كبيرة أو صغيرة وهل لدى الدول الصغيرة الأهداف نفسها مثل الدول الكبيرة؟ وهل تستطيع الدول الصغيرة المطالبة باستغلال الفضاء السيبراني لمواجهة التحديات نفسها التي تواجهها الدول الكبيرة ؟

٤- تأثير الدول المسيطرة :هل صيغت العديد من الاستراتيجيات الوطنية في السنوات الأخيرة على غرار النماذج التي فرضتها الدول المهيمنة ؟ وهل يوجد تأثير وانتشار لقواعد ومبادئ تفرضها هذه الدول المهيمنة ؟ إن التحليل المقارن للاستراتيجية الوطنية يجب أن يحدد ويحلل ويشرح أوجه الاختلافات والتشابهات القوية ، ومن المحتمل أن تتضح من خلال الاستراتيجيات السيبرانية مجموعة العلاقات الدولية وحقائق المشهد الدولي وكذا القيود التقنية .

٥- يعتمد تطوير المعايير الدولية : للأمن السيبراني اعتمادًا كبيراً على الاستراتيجيات الوطنية الكبرى وانطلاقا من النقطة الأخيرة فقد حولت الدول بعض موارد الميزانية إلى مبادرات

الفضاء السيبراني، حيث وضعت مبالغ كبيرة خصصتها للبحث وتطوير قدرات الحرب السيبرانية ، كما أعلنت حكومات عديدة عن خطط وطنية متكاملة وبدأت تنفيذها للتصدي للتهديدات السيبرانية الجديدة، وتعبئة قطاعات متعددة وتحويل الموارد والاستراتيجية تحويلًا تاماً ،ويمكن أن يشمل هذا النوع من التحويل على الآتي :

أ – تدريب العسكريين أو إعادة تدريبهم .

ب– تحديث خدمات الاستخبارات للتركيز على جمع المعلومات العلمية والتكنولوجية ذات الصلة.

ج – إجراء عمليات محاكاة للحرب السيبرانية ، والمناورات العسكرية مع إيلاء اهتمام خاص لتطبيقات تكنولوجيا المعلومات والاتصالات .

د – بادرت دول عديدة إلى إجراء مسابقات وطنية لتحديد أفضل الأذهان (العقول) السيبرانية من بين سكانها المدنيين وتعيينهم .

هـ– تشجيع الاقتصاديات المحلية على تطوير قدرات تكنولوجية معززة لدعم الاستراتيجية العسكرية الجديدة .

و– تعكف بعض الحكومات أيضًا على إقامة مجموعة من القراصنة المدنيين من القطاع الخاص الذين يمكن اللجوء إليهم عند الحاجة، ويمكن أن تكون هذه الجهات الناشطة في مجال القرصنة، أفرادًا متخصصين في مجال التكنولوجيا أو حتى قراصنة سابقين غير شرعيين تم تعيينهم وتدريبهم لاستخدام مهاراتهم لأغراض الأمن الوطني .

ز – تلجأ بعض الدول إلى الاستعانة بوكلاء وقراصنة ومتخصصين من دول أخرى يعملون بالإنابة عنها، وتبين هذه التغيرات كلها التحول عن استراتيجيات رد الفعل إزاء التهديدات السيبرانية وإعادة توجيه نحو تطوير مناهج استباقية لحرب المعلومات للعمل بفعالية في ظروف التكنولوجيا العالية .

وفى ضوء حقائق العصر المعلوماتي، فإن حروب المستقبل ستعتمد على الذكاء الصناعي في ميدان التسلح العسكري ومنظومات الأسلحة التقليدية ، البرية و البحرية و الجوية و الفضائية ، لتجعل ميدان المعركة حقيقة صورية وقوة حاسوبية تحدد الأهداف وطريقة معالجتها نظم عرض العمليات ونتائجها ، والتقنيات المتعلقة بها .

ويرى "جيرى هاريسون "المدير السابق لمختبرات البحوث والإنماء في الجيش الأمريكي "أن البرمجة وحدها ستسمح بتحديد النتائج الباهرة في حروب المستقبل"، ومن ثمة برز الدور المؤثر للثورة المعلوماتية وثورة الاتصالات في النظرية العسكرية، وذلك بفعل عاملين ، الأول تمثل بربط نظم السلاح إلكترونيا، سواء عن طريق الربط المباشر اعتمادا على نظم آلية التحكم في أدائها، أو غير مباشر وذلك باستخدام وسائل الاتصال الحديثة لتمكين مراكز القيادة من القيام بهذا التحكم عن بعد ، أما العامل الثاني فقد تمثل في تقليص عامل البعد الجغرافي والفارق الزمنى الفاصل بين عمليات الوحدات العسكرية نتيجة زيادة مدى نظم السلاح ومعدلات سرعتها ودقه إصابتها للأهداف.

وبما أن الفضاء السيبراني يرتبط بالجغرافية فإنه حسب رؤية الباحثة " ابتسام عبد الزهرة العقبى " وفقا لدراسة قدمتها عام ٢٠١٨م عنوانها " الصراع الجيوستراتيجي الأمريكي – الروسي في الفضاء الإلكتروني"، فإن الصراع سيكون حسب التطور التكنولوجي، من خلال علاقته بالمجالات الجغرافية التي يغطيها وهى (الأرض – الجو – البحر – الفضاء)، وعليه فإن نتيجة التوجه التكنولوجي تتجه نحو عولمة العالم اقتصاديا وثقافياً وسياسياً وخلق مركز القلب له ، ليكون نقطة التحكم والتوجيه في المستقبل، حيث سيدفع إلى وضع نظرية أخرى ستكون قيد التطبيق مستقبلاً

وهى تقوم على :

١- أن من يسيطر على المعرفة ويمتلكها ويتحكم بها، سيسيطر على الفضاء السيبراني ويتحكم في المجالات الجغرافية الأربعة (الأرض – الجو – البحر – الفضاء) .

٢- ومن يسيطر على المجالات الجغرافية الأربعة، سيسيطر على العالم، (والمقصود هنا كل من آسيا وإفريقيا والامريكيتين) وفى إطار التأكيد على أهمية فضاء القوة السيبرانية والذى تعتبر البعد الخامس من أبعاد القوة الاستراتيجية، من خلال كتابه الصادر عام ٢٠١١م مستقبل القوة (The Future of Power) يؤكد جوزيف ناي (Josef S.Nye)، على أن القوى الكبرى في العالم ستتعرض لضغوط شديدة لممارسة سيطرتها على المجال السيبراني في الطريقة التي اكتسبت بها التفوق على الجو والبحر والبر .

قائمة المراجع

مراجع باللغة العربية

الكتب :

الهيئة العامة للاستعلامات : مصر والأمن السيبراني ، يونيو ٢٠١٣ .

خالد وليد محمود: الهجمات عبر الإنترنت :ساحة الصراع الإلكتروني الجديدة، سلسلة دراسات ودراسة السياسات، المركز العربي لأبحاث ، قطر،2013 .

صالح بن علي بن عبد الرحمن، الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت: رؤية2030 ، هيئة الاتصالات وتقنية المعلومات، السعودية ، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، المانيا،2019

على زياد العلى : الصراع والأمن الجيو سيبراني في الساحة الدولية : دراسة في استراتيجيات الاشتباك الرقمي،(عمان :دار أمجد للنشر والتوزيع،٢٠٢٠) .

قادري إسماعيل ، إدارة الحروب النفسية في الفضاء الإليكتروني : الاستراتيجية الأمريكية الجديدة في الشرق الأوسط ، الندوة الدولية :عولمة الأعلام السياسي وتحديات الأمن القومي للدول النامية ، قسم العلوم السياسية كلية الحقوق والعلوم السياسية ، جامعة قاصدي مرباح ، الجزائر، (٧ مارس 2007) المجلس الأعلى للأمن السيبراني : الاستراتيجية الوطنية للأمن السيبراني (٢٠٠٧-٢٠٢١).

الدوريات :

أميرة عبدالعظيم محمد عبدالجواد :" المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام"، مجلة الشريعة والقانون، ج،3 ، ع٣٥ .

إيهاب خليفة :" تنامى التهديدات السيبرانية للمؤسسات العسكرية، مجلة اتجاهات الأحداث، ع 22 ، يوليو2017 .

إيهاب خليفة : الحرب السيبرانية، مراجعة العقيدة العسكرية استعدادا للمعركة القادمة، ملحق مجلة السياسية الدولية ، مركز الدراسات الاستراتيجي، الأهرام، العدد ٢١١، القاهرة، ٢٠١٨م .

حسين باسم عبد الأمير:" تحديات الأمن السيبراني 17 "ماي2018 ، مركز الدراسات الاستراتيجية، كربلاء، العراق.

حياة حسين ، الفضاء الإلكتروني وتحديات الأمن العالمي ، مجلة العلوم القانونية والسياسية، المجلد ١ ، العدد ١ ، الجزائر، أبريل ٢٠٢١.

خلود عاصم ومحمد إبراهيم ، دور تكنولوجيا المعلومات والاتصالات في تحسين جودة المعلومات وانعكاساته على التنمية الاقتصادية الجامعة ، مجلة كلية بغداد للعلوم الاقتصادية الجامعة ، العدد الخاص بمؤتمر الكلية ، ٢٠١٣م .

روان بنت عطية الله الصحفي : الجرائم السيبرانية – مجلة الإلكترونية متعددة التخصصات – العدد الرابع مايو٢٠٢٠م.

زينب شنوف : الحرب السيبرانية في العصر الرقمي : حروب ما بعد كلاوزفيتش – ورقة بحثية منشورة – المجلة الجزائرية للأمن والتنمية – المجلد ٩– العدد٢– يوليو٢٠٢٠م .

سارة عبدالعزيز سالم : خيارات الحد الأدنى – روسيا والحفاظ على المكانة في الفضاء ، ملحق تحولات استراتيجية، السياسة الدولية ، الأهرام ، القاهرة ، عدد ٢١١ ، إبريل ٢٠١٩م .

سهيلة هادى : الحروب التكنولوجية في ظل عصر المعلومات – مجلة رؤى استراتيجية – المجلد الرابع – عدد١٤، ٢٠١٧م .

الرسائل العلمية :

شعيب قاسمي – فؤاد بالغيث: الاستراتيجية الدولية في مكافحة الجريمة السيبرانية – دراسة حالة الجزائر– رسالة ماجستير – جامعة العربي التبس – تبسة: كلية الحقوق والعلوم السياسة ٢٠٢٠.

صلاح حيدر عبدالواحد : حروب الفضاء الإلكتروني؛ دراسة في مفهومها وخصائصها وسبل مواجهتها – رسالة ماجستير – جامعة الشرق الأوسط–٢٠٢١.

عبدلاي شرقي : التهديدات السيبرانية وإشكالية السيادة: إعادة قراءة لسيادة وستفاليا – رسالة ماجستير – جامعة احمد بوقرة بومرداس– (الجزائر) – ٢٠٢٣.

منال محمود : أثر الثورة المعلوماتية وثورة الاتصالات على التحور السياسية والأمنية في المنطقة العربية (٢٠١٠– ٢٠١٧) – رسالة ماجستير – كلية الآداب والعلوم –٢٠١٨.

وليد غسان : دور الحرب الالكترونية في الصراع العربي الإسرائيلي – رسالة ماجستير –جامعة النجاح الوطنية – كلية الدراسات العليا – فلسطين– ٢٠١٣

مواقع على الإنترنت

المركز الإعلامي لمجلس الوزراء (تقرير مؤسسة براند فاينانس عن القوة الناعمة لعام ٢٠٢٢)https://www.sis.gov.eg/Story

الهيئة العامة للاستعلامات :مصر وقارة أفريقيا مقال منشور ٢٢يونيو ٢٠٢٢– /https://www.sis.gov.eg/Story:

مراجع باللغة الاجنبية

Books

Anthony Craig And Brandon Valerian, Realism and Cyber Conflict: Security in the Digital Age, E-international Relations, FEB- 3-2018.

Anthony Craig And Brandon Valerian: Realism and Cyber Conflict: Security in the Digital Age, E-international Relations, FEB 3 2018

Arsenio T. Galahad, Cyber Troops and Net War: The Profession of Arms in

Constantine. Petal ides: Cyber Terrorism and IR Theory: Realism, Liberalism, and Constructivism in the New Security Threat, inquiries journal,VOL. 4 NO. 03, 2012,

joseph Nye ;The power to lead – New York – Oxford University press – 2008.

joseph Nye :Get smart –Combining Hard and soft –Foreign Affairs- July-august ,2009.

Joseph S. Nye, Cyber Power, (Cambridge: Harvard Kennedy School, Belfer center for Science and International affairs, May 2010.

Periodicals:

Steven Lukes :Power A radical View, (British sociological association ,1974.

The soft Power of Mohamed Salah-Published Article-Al Arabia News-20May 2020

War College Series: The Information Age, , United States, 2015

USNATO Military Terminology Group (2010). JP 1 (02) "Dictionary of Military and Associated Terms", 2001 (As amended through 31 July 2010) .

Internet sites:

James Adams: "Virtual Defense" Foreign Affairs Vol. 80, No. 3 (May – Jun., 2001), https://www.foreignaffairs.com/articles/200101-05-virtual-defense

Conferences

de la Chapelle, B: Towards Multi-Stakeholder Governance: The Internet Governance Forum as Laboratory. In W. Kleinwachter (ed.), The Power of Ideas: Internet Governance in a Global Multi-Stakeholder Environment (Berlin: Land of Ideas), (2007)