الإرهاب الإليكتروني "الحروب السيبرانية Cyber warfare"
التكتيكات والأدوات والاستراتيجيات

أ.دينا عصمت والي*

أ.د.حسن عماد مكاوي**

ملخص الدراسة :

يطلق على هذا العصر الذي نعيشه عدة مسميات من بينها عصر تكنولوجيا الاتصال، وعصر الرقمنة، وعصر المعلوماتية، وعصر الوسائط المتعددة، والذكاء الاصطناعي، وغيرها من المسميات التي ترجع إلى ما يتسم به عصرنا الحالي من تقنيات مستحدثة، أدى استخدام هذة التقنيات بالضرورة إلى استغلالها في الحروب السيبرانية أي حروب الجيل الخامس.

حيث تطورت أشكال وأنواع الحروب عبر الزمن حتى الآن إلى 5 أنواع من الحروب، ومن المعروف بأن كل حرب تتشكل أدواتها بما يتسم به عصره، و يشكل أخطرها ما نعيشه في القرن الحادي والعشرين وهي الحرب السيبرانية التي قد لا تعرف الدولة أنها مستهدفة ومن أي جهة وما الهدف؟.

ويعرف إسماعيل صبري مقلد 2012 الثورة الرقمية بأنها "ذلك الكم الهائل من المعرفة التي أمكن السيطرة عليه بواسطة تكنولوجيا المعلومات وثورة الاتصال المتمثلة في تكنولوجيا الاتصال الحديثة، وقوامها الأقمار الصناعية والألياف البصرية وثورة الحواسيب الإليكترونية التي توغلت في جميع مناحي الحياة".

أما الحرب السيبرانية فهي حرب وساحتها هي الفضاء السيبراني، وتتسم بأنها حرب اللا عنف، هدفها هو إسقاط الأنظمة بلا سلاح مباشر عبر المظاهرات والاضطرابات والاعتصامات والعصيان المدني ومحاصرة مقرات الدولة واحتلالها سلميًا، أما عن الجانب العسكري فيها فقد يكون غير متواجد خاصة في مراحله الأولى، أو قد لا يوجد أصلا فيها، بل عبارة عن إشاعة الفوضى في البلد المستهدفعن بعد، كما حدث في ثورات الربيع العربي في عام 2011 في عدد كبير من الدول العربية؛ كتونس ومصر وسوريا وليبيا وغيرها، أو ما سمته أو أطلقت عليه الولايات المتحدة الأمريكية مصطلح "الفوضى الخلاقة".

ونجد أن دينامية عمل وسائل التواصل الاجتماعي التى تتسم بأنها وسيط رخيص وسريع وغني بأدواته المختلفة والمتطورة، والتي تجعل منها أداة جيدة في تحقيق أهداف الحروب السيبرانية وذلك لكونها أداة رخيصة وفعالة في تلك الحروب السبرانية.

الكلمات الدالة: الثورة الرقمية -حروب الجيل الخامس- الحرب السيبرانية- الحرب الإليكترونية- الهجمات الإليكترونية- الإرهاب الإليكتروني- الفضاء السيبراني- الحوسبة السحابية- وسائل التواصل الاجتماعي

---

*باحثة دكتوراه بكلية الإعلام جامعة القاهرة .

**الأستاذ بقسم الإذاعة والتليفزيون بكلية الإعلام – جامعة القاهرة .

Cyber Warfare and the Role of Social Media: Tactics, Tools, and Strategies

Ms. Dina Esmat Waly*

Prof.Hassan Emad Makawi**

Absttract:

This research explores the evolution of warfare from traditional, state-on-state conflicts to the complex domain of cyberwarfare. It analyzes the characteristics of different generations of warfare, highlighting the unique challenges posed by cyber threats. The study concludes that cyberwarfare has become a significant threat to national security, targeting critical infrastructure and information systems.

The study examines the historical progression of warfare, from conventional conflicts to the digital age of cyberwarfare. It highlights how technological advancements have transformed the nature of war, leading to new forms of conflict and asymmetric threats. The research underscores the importance of understanding cyber threats to develop effective defense strategies.

Research Problem: Despite the proliferation of definitions for cyberwarfare, existing definitions often rely on static factors like tools and timeframes. However, the dynamic nature of cyberwarfare, characterized by rapid technological advancements and constant innovation, renders these definitions inadequate. The advent of artificial intelligence exemplifies this evolution. This study aims to deepen our understanding of fifth-generation warfare, which targets critical information infrastructure and seeks to manipulate the cultural and ideological landscape of adversaries.

Keywords Digital Revolution -Fifth-Generation Warfare Cyberwarfare - Electronic Warfare -Cyber Attacks -Cyber Terrorism Cyberspace -Cloud Computing -Social Media.

* PhD Researcher at the Faculty of Mass Communication, Cairo University

** Professor in the Department of Radio and Television, Faculty of Mass Communication, Cairo University

مقدمة:

تعددت أشكال وأجيال الحروب بدءًا من الحرب التقليدية التي تمثلت في الجيل الأول من الحروب، حيث كان طرفاها واضحين معلومين، وتكون النتيجة بانتصار طرف على الأخر، وهنا يكون واضح فيها من الرابح ومن الخاسر ومن الذي يفرض قواعده وأحكامه على الآخر، كالذي حدث في الحرب العالمية الثانية، واستسلام الإمبراطورية اليابانية في الثاني من سبتمبر عام 1945 أمام الولايات المتحدة الأمريكية وبريطانيا (قوات الحلفاء)، ومن سمات هذه الحروب أن يكون لها بداية ونهاية ورابح وخاسر، أما عن الجيل الثاني من الحروب، حيث تتمثل في الحروب الشاملة ليس فيها مدني ولا عسكري؛ بل كل موارد الدولة السياسة والاقتصادية والديمغرافية والثقافية والدعائية مسخرة للمجهود الحربي، وهى إلى حدٍ بعيد تشبه الجيل الأول في وضوح الرابح والخاسر والبداية والنهاية، أما الجيل الثالث من الحروب؛ كالذي أعقب الحرب العالمية الثانية، وسميت بالحرب الباردة بين الاتحاد السوفيتي والولايات المتحدة الأمريكية، مسرحها كان العالم بأسره، وأهم ما يميزها هي حروب الوكالة (حرب كوريا 1950 - 1953)، وحروب الجوسسة الشاملة، والدعاية العقائدية الشاملة، والحرب الاقتصادية، والانقلابات العسكرية، والدوران في فلك إحدى الكتلتين، كما تميزها ظاهرة جديدة وهي حروب التحرير الشعبي من الاستعمار أو من الأنظمة المستبدة، حيث لها طابعًا خاصًا هو حروب العصابات الثورية كالتي حدثت في إفريقيا ما بين حروب عصابات، وتمرد سواء سلمي أو مسلح، ونزاعات مسلحة، وحروب أهلية، وثورات، والاستناد إلى حليف قوي (كحرب الحدود الجنوب أفريقيا والتي تسمى بحرب الاستقلال الناميبية من 1966 إلى 1990، وكحركة الشباب الإسلامية في الصومال)، وتعتمد على استنزاف العدو عسكريًا واقتصاديًا، وإنهاكه وتشويهه دعائيًا.

أما حروب الجيل الرابع والتي سادت منذ تسعينات القرن العشرين وسقوط الاتحاد السوفيتي وتمثلت في اختلال الموازين العسكرية حيث أنتجت حروب الصدمة والترويع التي تدمر كل شيء كما، في حرب أمريكا ضد العراق وأفغانستان وصربيا، بحيث تعتمد على أساليب خاصة كالاغتيالات والتفجيرات والاختطاف والسطو، إضافة إلى ظهور الحروب الأهلية كما في دول العالم الثالث.

مشكلة الدراسة:

تعددت التعريفات الخاصة بالحروب السيبرانية، لكنها مازالت تقف عند محددات الأدوات والزمان وهما عنصران يتنافيان مع طبيعة هذه الحروب، من حيث التغيير والتطوير اللحظي للأدوات واستخدامها، كذلك عنصر الوقت الذي لا يسمح له بتحديد قدرات هذا النوع من الحروب، ولعلنا نجد في دخول عصر الذكاء الاصطناعي أبرز مثال لذلك، حيث تنبع مشكلة الدراسة من محاولة لفهم أكبر لحروب الجيل الخامس الذي يستهدف البني التحتية المعلوماتية للقطاعات العسكرية والحكومية والاقتصادية، كما تستهدف تغيير البيئة الثقافية والفكرية للخصوم فهي سلاح استراتيجي للحكومات والأفراد، وأداة هامة في الحروب الحديثة بين الدول.

أهمية الدراسة:

♦**أولاً الأهمية العلمية:** يعتبر مجالاً جديدًا للعلم وبما أن الحروب السيبرانية تخصص علمي جديد يضاف إلى علوم الإعلام خاصة في الوطن العربي ومصر ويمكن أن تشكل هذه الدراسة إضافة معرفية وتطبيقية في هذا المجال.

♦**ثانيًا أهمية مجتمعية:** زيادة الوعي بحروب الجيل الخامس ووسائلها وحجم تأثيرها.

الدراسات السابقة:

يسمى هذا العصر بعصر تكنولوجيا الاتصال، وعصر الرقمنة، وعصر المعلوماتية، وعصر الوسائط المتعددة، والذكاء الاصطناعي، وغيرها من المسميات التي ترجع إلى ما يتسم به العصر من تقنيات مستحدثة، أدت بالضرورة إلى الحروب السيبرانية أي حروب الجيل الخامس، ففي ظل تطور أشكال وأنواع الحروب عبر الزمن إلى 5 أنواع من الحروب كل حرب تتشكل بما يتسم به عصره، حيث يشكل أخطرها ما نعيشه في القرن الحادي والعشرين وهو الحرب السيبرانية التي قد لا تعرف الدولة أنها مستهدفة ومن أي جهة وما الهدف؟.

ويعرف إسماعيل صبري مقلد 2012 الثورة الرقمية بأنها "ذلك الكم الهائل من المعرفة التي أمكن السيطرة عليه بواسطة تكنولوجيا المعلومات وثورة الاتصال المتمثلة في تكنولوجيا الاتصال الحديثة، وقوامها الأقمار الصناعية والألياف البصرية وثورة الحواسيب الإليكترونية التي توغلت في جميع مناحي الحياة"[1].

لذلك فهي حرب اللا عنف، حيث تهدف لإسقاط الأنظمة بلا سلاح مباشر عبر المظاهرات والاضطرابات والاعتصامات والعصيان المدني ومحاصرة مقرات الدولة واحتلالها سلميًا، أما عن الجانب العسكري فيها فقد يكون غير متواجد خاصة في مراحلها الأولى، أو قد لا يوجد أصلا فيها، بل عبارة عن إشاعة الفوضى في البلد المستهدف، كما حدث في ثورات الربيع العربي في عام 2011 في عدد كبير من الدول العربية؛ كتونس ومصر وسوريا وليبيا وغيرها، أو ما سمته أو أطلقت عليه الولايات المتحدة الأمريكية مصطلح "الفوضى الخلاقة" .

دراسات تناولت علاقة الحروب السيبرانية بالتطور التكنولوجي والثورة الرقمية:

الثورة الرقمية في الشؤون العسكرية فهي مصطلح نشأ في السبعينيات والثمانينيات من القرن القرن الماضي لكنه سرعان ما تطور إلى مصطلح أكثر شمولية إلى الثورة في الشؤون العسكرية RMA.

ويعرفها معظم المحللين بأنها الزيادة في القدرة العسكرية وفاعليتها الناشئة عن التغير الدائم والمتبادل في تكنولوجيا الأنظمة وأساليب التشغيل والمنظمات العسكرية.

ويعرفها معيزي، ليندة، الدهقاني 2022 بأنها: "تغيير رئيسي في طبيعة الحرب نتيجة للتقدم المبتكر في التكنولوجيا العسكرية إلى جانب التغييرات الدراماتيكية في العقيدة العسكرية والمفاهيم المعلوماتية والتنظيمية، بشكل يغير من سلوك العمليات العسكرية وسيرها"[2].

وهناك علاقة وثيقة بين الثورة الرقمية والتطور الميداني العسكري، حيث ساهم التطور الهائل في تدفق المعلومات والذى صاحبه تطور في أنظمة الحاسوب وأنظمة الشبكات والذى تم الاعتماد عليه في الأنظمة العسكرية المعلوماتية بشكل كلي من خلال الربط الشبكي للمعلومات التشغيلية وجعل انتقالها متاح لكل مقاتل وبذلك يتضح أن للتطور التكنولوجي دور حاسم في الحرب الحديثة.

كما أن الذكاء الصناعي Artificial Inteligence اليوم واستخدامه ليكون أداة حرب وبما يتضمنه من أسلحة ذكية تفيد بتحقيق الوعي بساحة المعركة حيث يضم مجموعة من الأسلحة الموجهة والدقيقة والتى تتمثل في تطبيق القوة الذكية بإطلاق ذخائر دقيقة التوجيه ما أدى إلى زيادة القوة التدميرية ودقتها بشكل كبير جدًا عن سابقيه، وهنا يتضح أن للتطور التكنولوجي دور حاسم في الحروب الحديثة.

ثانيًا: الحروب السيبرانية أو السيبيرية التعريف :

أ- دراسات ركزت على نشأة المصطلح وتطوره:

لفظ Cyber هي كلمة يونانية مشتقة من كلمة Kybernets وتعني الشخص الذى يدير دفة السفينة، حيث يرجع البعض هذه التسمية إلى منتصف القرن العشرين، مع عالم الرياضيات الأمريكي Narbert Wieners الذى استخدمها للتعبير عن التحكم الآلى.

كما يشير مفهوم الفضاء السيبراني Cyber Space إلى شبكات الاتصال الإليكتروني والواقع الافتراضي وشبكات الإنترنت وعدد هائل من البيانات.

ويقصد بالحرب السيبرانية أيضًا بأنها: "عمليات في الفضاء الإلكتروني، حيث تستخدم وسائل وأساليب قتال ترقى إلى مستوى النزاع المسلح أو تُجرى في سياقه، ضمن المعني المقصود في القانون الدولي الإنساني".

وقد تطور هذا المصطلح من التحكم الألى إلى الفضاء السيبراني، وهنا نجد أن تعريف مصطلح الفضاء السيبراني أكثر شمولاً في التعريف التي قدمته إدارة السلامة العامة الكندية[3] "أنه العالم الإليكتروني الذى تم إنشاؤه بواسطة شبكة تكنولوجيا المعلومات المترابطة، وتكون المعلومات متاحة على هذه الشبكات ويتم مشاركتها على نطاق واسع، والفضاء الإليكتروني ليس ثابتًا بل هو نظام بيئي ديناميكي متطور ومتعدد المستويات في بنيته التحتية المادية والبرمجية واللوائح والأفكار والابتكارات التي يتأثر بها المساهمين الذين يمثلون المجموعة المتنوعة من المقاصد البشرية".

وقد ظهرت الحرب السيبرانية كأداة من أدوات الجيل الخامس للحروب كما يطلق على الفضاء السيبراني بالذراع الرابع للجيوش[4]، وكان أبرز التعريفات التي وضعت للحروب السيبرانية منذ 2001 والى الآن جاءت كالآتي:

أنها أحد أنماط الحروب الإلكترونية، وهي إجراء عسكري يتضمن استخدام الطاقة الكهرومغناطيسية للتحكم في المجال الذي يتميز باستخدام الإلكترونيات والطيف الكهرومغناطيسي لاستخدام البيانات.

ويعرف عبدالغفار الدويك إنه يمكن التمييز بين ثلاث صور رئيسة لعمليات الحرب السيبرانية[5]: **أولاً**: مهاجمة شبكات الحاسب الآلي عن طريق اختراق الشبكات أو من خلال نشر الفيروسات بهدف تعطيل الشبكة وتغذيتها بمعلومات محرفة لإرباك مستخدمي الشبكات. **ثانيًا**: الدفاع عن شبكات الحاسب الآلي من أي اختراق خارجي، عبر تأمينها من خلال إجراءات معينة، يقوم بها "حراس الشبكات" من خلال برامج وتطبيقات تقوم بأعمال المراقبة للزائرين غير المرغوبين (الهاكرز) و"استيقافهم" للتعرف على هويتهم أمام بوابات افتراضية للشبكات، بجانب المسح الشامل للشبكات بحثًا عن الفيروسات والألغام السيبرانية، والكشف عنها وتأمينها. **ثالثًا**: استطلاع شبكات الحاسب الآلي وتعني القدرة على الدخول غير المشروع والتجسس على شبكات الخصم، بهدف الحصول على البيانات دون تدميرها والتي قد تشتمل على أسرار عسكرية ومعلومات استخباراتية، وفي بعض الحالات قد يُسمح للزائر المجهول بالدخول على الشبكة، وتتبعه بهدف التعرف على أساليب الخصم والقيام بعمليات ردع سيبراني مضاد.

ومن أبرز التعريفات للحرب السيبرية أو السيبرانية Cyber warfare بأنها تُرجمت كلمة «سايبر Cyber» الإنكليزية بمعنى أنها «تخيلي» أو «افتراضي» والسايبر هو كلمة يجري استخدامها لوصف الفضاء الذي يضم الشبكات العنكبوتية المحوسبة، ومنظومات الاتصال والمعلومات وأنظمة التحكم عن بعد.

وتختلف استخدامات السايبر وأشكاله من دولة إلى أخرى تبعًا لأولويات هذه الدول، فمنها الأمني والسياسي والاستخباراتي والمدني والمهني والمعلوماتي البحت.

ويتشكل كيان السايبر في الدول كلّها بشكلٍ عام من وجود ثلاثة عناصر أساسية تضم الأجهزة الصلبة (Hardware)، والبرمجيات الرقمية الناعمة (Software)، والعامل البشري من مبرمجين ومستخدمين.

وقد عرف «قاموس أوكسفورد الإنكليزي» الحرب السيبرية بأنّها: «استخدام لتقنيات الحاسوب بهدف تخريب نشاطات دولة أو منظمة أو أفراد، وبخاصة الهجومات المحضّرة على منظومات المعلومات الخاصة، وذلك لغايات استراتيجية أو عسكرية».

أمّا خبيرة التكنولوجيا Margaret Rose كتبت على موقع Techopedia المنصة التعليمية المتخصصة في تعليم التكنولوجيا ولدية أكثر من 100 باحث وكاتب ومحرر في مجال التكنولوجيا كما لدية ما يزيد عن 3 مليون زائر شهريًا فقد عرّفها بأنّها: «كل هجوم افتراضي يجري بدوافع سياسية على أجهزة العدو الإلكترونية وشبكات الإنترنت وأنظمة المعلومات الخاصة به، لتعطيل منظوماته المالية وأنظمته الإدارية، وذلك من خلال سرقة قواعد معلوماته السرّية أو تعديلها لتقويض الشبكات العنكبوتية والمواقع ونظام الخدمات»[6].

ب- دراسات ركزت على أنماط الحروب السيبرانية:

وتتسم الحرب السيبرية أو السيرانية بأنها تهدف إلى عمليات تخريب أوتجسس:

- **التخريب Sabotage:** قد تتعرض حواسيب الأنظمة العسكرية والمالية لخطر التخريب بهدف تعطيل عملياتها الطبيعية وتجهيزاتها.
- **التجسس Espionnage:** تستخدم طرق غير شرعية لتعطيل عمل الشبكات العنكبوتية وحواسيبها، وأنظمتها بهدف سرقة معلومات سرّية من مؤسسات الخصم أو الأفراد ونقلها إلى الصديق السياسي، أو العسكري أو المالي.

كما يرى بعض المراقبين أنّ الحروب الإلكترونية أو الحروب السيبرانية، هي حرب بكل ما للكلمة من معنى، حيث عرّفها الدكتور Paul Rosenzweig2012 أستاذ القانون في جامعة جورج واشنطن، في بحث له عن قانونية هذه الحرب بأنّها: «حربٌ ذكية أقوى من أي هجوم بري أو جوي، وأكثر ذكاءً وأقل تكلفة، فهي لا تحتاج إلى معدات حربية ولا جنود، ولكنّها تحتاج إلى قدرات علمية عالية».

وهو يعتبر أنّ "حرب السايبر هي تطوّر طبيعي في مفهوم الحروب، نقلتها إلى جيل جديد يعتمد على التحكّم والسيطرة عن بُعد"(7).

كما أشار باول روزينزفيج إلى أنّ لحرب السايبر تأثيرًا عالميًا مدمرًا".

ويرى البعض الآخر أنّ مضمون الحرب الإلكترونية يتعلق بالتطبيقات العسكرية للفضاء السيبراني، حيث تعني - في أحد تعريفاتها - قيام دولة أو فواعل من غير الدول بشنّ هجوم إلكتروني في إطار متبادل، أو من قبل طرف واحد.

ثالثًا: دراسات تناولت الفروق بين الحرب الإليكترونية والحروب السيبرانية:

على الرغم من انتشار اسم «الحرب الإلكترونية» إعلاميًا، فإنّه يُعتبر مصطلحًا قديمًا كان بالأساس مقتصرًا على رصد حالات التشويش على أنظمة الاتصال، والرادار، وأجهزة الإنذار، بينما يكشف الواقع الراهن في الفضاء الإلكتروني عن دخول شبكات الاتصال والمعلومات إلى بنية الاستخدامات الحربية ومجالاتها.

الأمن السيبراني من أهم مجالات الأمن في القرن الحادي والعشرين، ومن المعروف أن الهيمنة السيبرانية ترسم ملامح الحروب في القرن القادم، مما يستلزم تغيير الإستراتيجية في اتجاه التصعيد مع قوى أخرى معادية نشطة في ساحة الحرب السيبرانية التي تحارب عليها..

3- أنواع الهجمات السيبرانية:

-وتعتبر من أكثر الهجمات السيبرانية شيوعا هي ما تعرف بهجوم حجب الخدمة أو Distributed Denial of Service أو هجمات الحرمان من الخدمات وهي هجمات تتم عن طريق إغراق المواقع بسيل من البيانات غير المهمة، يتم إرسالها على المواقع

المستهدفة بشكل كثيف مما يسبب بطء الخدمات أو زحامًا مروريًا بهذه المواقع، ينتج عنه صعوبة وصول المستخدمين لها بسبب هذا "الاكتظاظ المعلوماتي".

شخص في المنتصف "Man In The Middle"- كما يعتبر هجوم تعدٍ عملية يقوم بها المهاجم لاعتراض محادثة جارية بين طرفين، وتبدو وكأنها تجري بين الطرفين مباشرة، لكن يتم التحكم بها من قبل الشخص المهاجم، فيقوم بعرض وإضافة وإزالة وتعديل واستبدال الرسائل التي يتم تبادلها في هذه المحادثة.

التصيد الاحتيالي بهدف Phishing Attacks- كما تعد عملية الحصول على معلومات خاصة ومهمة مثل أسماء المستخدمين وكلمات المرور وتفاصيل بطاقة الائتمان، من أجل استخدامها الضار ضد أصحابها، ويتم ذلك من خلال تطبيق يبدو جدير بالثقة أثناء الاتصال الإليكتروني أسلوب شائع وفعال لتحقيق الاختراق.

وفي تقرير المخاطر العالمية 2022 لمنتدى الاقتصادي العالمي [8] أكد أن الاعتماد المتزايد على الأنظمة الرقمية - الذي اشتد بسبب جائحة كوفيد 19 أدى إلى تغيير المجتمعات، حيث خضعت الصناعات للرقمنة السريعة، وتحول الموظفين إلى العمل عن بعد حيثما أمكن ذلك، وانتشرت المنصات والأجهزة التي تسهل هذا التغيير، وفي الوقت نفسه، تتزايد تهديدات الأمن السيبراني - في عام 2020، حيث زادت هجمات البرمجيات الخبيثة وبرامج الفدية بنسبة 358٪ و 435٪ على التوالي وتتجاوز قدرة المجتمعات على منعها أو الاستجابة لها بشكل فعال.

كما وضح أن انخفاض الحواجز التي تحول دون دخول الجهات الفاعلة في مجال التهديدات السيبرانية، وأساليب الهجوم الأكثر عدوانية، وندرة المتخصصين في الأمن السيبراني وآليات الحوكمة المرقعة كلها تؤدي إلى تفاقم المخاطر، كما أن الهجمات على الأنظمة الكبيرة والاستراتيجية تحمل عواقب مادية متتالية عبر المجتمعات، في حين أن الوقاية سيترتب عليها حتما تكاليف أعلى، كما ستؤثر المخاطر غير الملموسة - مثل المعلومات المضللة والاحتيال والافتقار إلى السلامة الرقمية داخل الأنظمة الرقمية - على ثقة الجمهور في وسائل الإعلام بشكل عام.

كما أن التهديدات السيبرانية الأكبر ستعيق التعاون بين الدول إذا استمرت الحكومات في اتباع مسارات أحادية الجانب للسيطرة على المخاطر.

وكما ذكرنا في السابق لاتقتصر الحروب السيبرانية على دول تجاه دول بل تمتد لتشمل دول ومنظمات وتنظيمات إرهابية وشركات محلية ودولية وأفراد "هكرز" تجاه دول أو مؤسسات أو أفراد، ويكون الهدف إما عسكري أو سياسي أو اقتصادي.

رابعًا: دراسات تناولت ظهور وتطور مصطلح الإرهاب الإليكتروني:

أصبح مصطلح الإرهاب الإليكتروني الأكثر تداولًا في الآونة الأخيرة، ولمعرفة مفهوم المصطلح بشئ من التفصيل نجد أن مصطلحٌ الإرهاب كما عرفته وزارة "Politt 1998" أن وزارة الخارجية الأمريكية بأنه "عنف متعمد ذو دوافع سياسية ضد أهداف غير مقاتلة

من قبل جماعات غير وطنية أو عملاء سريين"، وقام بدمج هذا المصطلح مع مصطلح الإنترنت ليحصل على تعريف جيد لمصطلح الإرهاب الإليكتروني أو الإرهاب السيبراني " هجوم متعمد ذو دوافع سياسية ضد المعلومات وأنظمة وبرامج الكمبيوتر والبيانات يؤدي إلى العنف ضد أهداف غير مقاتلة من قبل جماعات غير وطنية أو عملاء سريين"[9].

بيد أن البعض يشير إلى أن أي استخدام للتكنولوجيا الرقمية من قبل المنظمات الإرهابية بوصفه إرهابا سيبرانيًا، في حين أن البعض الآخر أكثر شمولية، حيث يصف أي استخدام للشبكات الرقمية من شأنه أن يلحق الضرر بالبنية التحتية الحيوية بأنه إرهاب سيبراني.

جدير بالذكر أنه يميل معظم المتخصصين أكثر إلى استخدام مصطلحات الحرب السيبرانية والإرهاب السيبراني، والجريمة السيبرانية.

وفي كل الأحوال يذهب كثيرون إلى استخدام ذلك التعريف البسيط للغاية: الإرهاب الإلكتروني هو استخدام الإنترنت لارتكاب الإرهاب، كما يشير عدد من الباحثين إلى أن الإرهاب الإلكتروني يمتلك جاذبية خاصة عن الإرهاب التقليدي ذلك لأنّه: رخيص، وسّري، ومدمّر.

ربط بعض الباحثين مفهوم الإرهاب الإليكتروني بأحداث 11 سبتمبر على الرغم من أن بعض الباحثين يعودون بتاريخ استخدام المصطلح إلى عام 1980، حيث "أنه إلتقاء الإرهاب والفضاء السيبراني [10]، وهو يفهم بشكل Denning 2000 وقد عرفه على أنه "هجمات غير مشروعة وتهديدات بشن هجمات ضد أجهزة الكمبيوتر والشبكات والمعلومات المخزنة عليهم بهدف ترهيب أو إكراه حكومة ما أو شعبها لتعزيز أهداف سياسية أو اجتماعية". ولوصف الهجوم بأنه إرهاب سيبراني، لابد أن يسفر عن عنف ضد الأشخاص أو الممتلكات أو على الأقل لإحداث ضرر يكفي لإثارة الخوف، ويمكن أن تؤدي هذه الهجمات إلى الموت أو الإصابات الجسدية، أو الانفجارات، أو حوادث الطائرات، أو تلوث المياه، أو الخسائر الاقتصادية الفادحة وقد تُعد الهجمات الخطرة على البنى التحتية الحيوية إرهابًا سيبرانيًا اعتمادًا على تأثيرها، أما الهجمات التي تؤدي إلى تعطيل خدمات غير حيوية أو التي هي بالأساس مصدر إزعاج مكلف لا تعد إرهابًا سيبرانيًا"[11].

ونذكر بأن الإرهاب الإليكتروني في مفهومه المبسط هو استخدام الشبكة العنكبوتية لارتكاب إرهاب أو تخريب ما في مؤسسة حيوية، وهذا المفهوم يختلف كليًا عن مفهوم الجريمة الإليكترونية التي سنتناولها بالتفصيل لاحقًا.

وقد يكون الإرهاب الإليكتروني مكون من هجمة سيبرانية واحدة أو عدة هجمات سيبرانية، وقد يكون على منشأة واحدة مستهدفة أو عدة منشآت.

وقد عرفه Raghavan 2003 [12] على أنه "الاستخدام المتعمد للأنشطة التخريبية، أو التهديد بها، في الفضاء الإلكتروني، بقصد تعزيز أهداف اجتماعية أو أيديولوجية أو دينية أو سياسية أو أهداف مماثلة، أو لتخويف أي شخص في تعزيز هذه الأهداف.

وعادة ما يمكن أن تتخذ هذه الهجمات أشكالاً مختلفة: يمكن للإرهابي أن يقتحم شبكة الكمبيوتر الخاصة بالشركة مما يتسبب في الخراب أو تخريب خطوط الغاز في بلد ما أو

إحداث فوضى في النظام المالي الدولي. وقد تتسبب هذه الهجمات الإرهابية ضد البنية التحتية للمعلومات وأنظمة الكمبيوتر وبرامج الكمبيوتر والبيانات في حدوث إصابات وخسائر في الأرواح وتدمير الممتلكات. الهدف من مثل هذه الهجمات غير القانونية هو تخويف أو إقناع الحكومة أو شعبها بتعزيز هدف سياسي أو اجتماعي".

خامسًا: أهداف الحروب السيبرانية / الإرهاب الإليكتروني كما تناولتها الدراسات السابقة:

وتستهدف الهجمات السيبرانية كما حددها "سمير بارة 2017" في أربع أنواع لتعطيل الخدمة، أو إتلاف المعلومات أو تعديلها، أو التجسس على الشبكات، أو تدمير الأصول والمعلومات(13).

كذلك فإن من أبرز وأهم أهداف الإرهاب الإليكتروني أو الحرب السيبرانية هي البنية التحتية للمعلوماتية للقطاعات العسكرية والحكومية والاقتصادية، كما أن استهداف البيئة الثقافية والفكرية للحكومات والأفراد للخصوم وتغييرها يعتبر سلاح استراتيجي، وأداة هامة في الحروب الحديثة بين الدول المتحاربة.

وعرفت اللجنة الدولية للصليب الأحمر على صفحتها الرسمية بتاريخ 28-6-2013 الحروب السيبرانية بأن تعبير "الحرب السيبرانية"، يُستخدم من قبل فئات عديدة من الناس للإشارة إلى أشياء مختلفة(14).

ويُستخدَم المصطلح للإشارة إلى وسائل وأساليب القتال التي تتألف الفضاء الإلكتروني ترقى إلى مستوى النزاع المسلح أو تُجرى في سياقه، ضمن المعني المقصود في القانون الدولي الإنساني.

حيث يقدم دليل تالين حول القانون الدولي الخاص بالحرب السيبرانية وهو من إعداد اللجنة الدولية للخبراء بدعوة من مركز التميز للدفاع السيبراني التعاوني التابع لحلف شمال الأطلسي (الناتو)، مطابع جامعة كمبريدج 2013، تعريفاً "للهجوم السيبراني" بموجب القانون الدولي الإنساني بوصفه "عملية إلكترونية سواء هجومية أو دفاعية يتوقع أن تتسبب في إصابة أو قتل أشخاص أو الإضرار بأعيان أو تدميرها".

ويكمن صلب الموضوع في حجم التفاصيل، أي ما ينبغى أن يفهم على أنه "ضرر" في العالم الإلكتروني، حيث اتفق أغلب الخبراء على أنه علاوة على الضرر المادي فإن توقف أحد الأعيان عن العمل قد يشكل ضرراً أيضًا.

وتتمثل وجهة نظر اللجنة الدولية في أنه إذا تعطل أحد الأعيان (أجهزة الكمبيوتر)، فليس من المهم كيفية حدوث ذلك سواء بوسائل حركية أو عملية إلكترونية، وهذه القضية مهمة للغاية في الممارسة العملية.

كما أشارت إلى أن أي عملية إلكترونية تستهدف تعطيل شبكة مدنية خلاف ذلك، لن يشملها الحظر الذي يفرضه القانون الدولي الإنساني على الاستهداف المباشر للأشخاص المدنيين والأعيان المدنية.

ولقد ساهمت اللجنة الدولية بصفة مراقب في مناقشات الخبراء الذين صاغوا دليل "تالين" لضمان انعكاس القانون الدولي الإنساني القائم في الدليل بأقصى قدر ممكن، وتعزيز الحماية التي يوفرها هذا الفرع من القانون لضحايا النزاعات المسلحة.

ويساور اللجنة الدولية قلق بشأن الحرب السيبرانية بسبب ضعف الشبكات الإلكترونية والتكلفة الإنسانية المحتملة من جراء الهجمات السيبرانية، فعندما تتعرض الحواسيب أو الشبكات التابعة لدولة ما لهجوم أو اختراق أو إعاقة، قد يجعل هذا الأمر المدنيين عرضة لخطر الحرمان من الاحتياجات الأساسية مثل مياه الشرب والرعاية الطبية والكهرباء، وإذا تعطلت أنظمة تحديد المواقع GPS عن العمل، قد تحدث إصابات في صفوف المدنيين من خلال تعطيل عمليات إقلاع مروحيات الإنقاذ على سبيل المثال، كما يمكن أن تتعرض السدود أو المحطات النووية أو أنظمة التحكم في الطائرات لهجمات سيبرانية نظرًا لاعتمادها على الحواسيب.

وبما أن أنظمة الشبكات مترابطة إلى حد يجعل من الصعب الحد من آثار هجوم سيبراني ضد جزء من المنظومة دون الإضرار بأجزاء أخرى وبالتالي تعطيل المنظومة بأكملها، كما يمكن أن تتضرر مصالح مئات الآلاف من الناس، وصحتهم وحتى حياتهم. وتذكر اللجنة الدولية جميع أطراف النزاع بتوخي الحرص بشكل مستمر من أجل حقن دماء المدنيين، وهو أحد أهم الأدوار التي تقوم بها، فالحروب لها قواعد وحدود تنطبق على اللجوء إلى الحرب السيبرانية بنفس القدر الذي تنطبق به على استخدام البنادق والمدفعية والصواريخ.

الحرب السيبرانية من حيث Arquilla, John, Ronfeldt, David 1993، وقد عرف كلا من حيث الأهداف بأنها "تنفيذ العمليات العسكرية، والاستعداد لتنفيذها، وفقا للمبادئ المعلوماتية، من خلال تعطيل أو تدمير النظم المعلومات والاتصالات على أوسع نطاق، وتشمل أيضا تدمير العقيدة العسكرية للعدو التي يعتمد عليها لتحديد هويته، وخططه، وتصرفاته، وأهدافه، والتحديات التي يواجهها، وذلك عبر معرفة كل شئ عن العدو، ومنعه في الوقت نفسه من معرفة أي شيء عن الطرف الآخر، وتحويل ميزان المعرفة ليكون في مصلحة هذا الطرف"[15].

وتشير الحرب السيبرانية إلى أساليب وأنماط الحرب ووسائلها التي تعتمد على تكنولوجيا المعلومات وتُستخدم في سياق نزاع مسلح ضمن المعنى الوارد في القانون الدولي الإنساني، بخلاف العمليات العسكرية الحركية التقليدية.

وتعتبر المصطلحات "الهجمات السيبرانية" أو "العمليات السيبرانية" أو "الهجمات على شبكات الحواسيب"، والتي تُستخدم في سياقات مختلفة والتي لا تقتصر دائماً على النزاعات المسلحة.

أما عن العبارة الأكثر شمولاً فهي "العمليات السيبرانية" للإشارة إلى عمليات ضدّ أو بواسطة حاسوب أو نظام حاسوب من خلال تدفق البيانات.

وقد تهدف هذه العمليات إلى القيام بأمور مختلفة، مثل التسلل إلى نظام حاسوب وجمع بيانات أو تصديرها أو إتلافها أو تغييرها أو تشفيرها، أو مثل إطلاق عمليات يسيطر عليها النظام المُتَسلل إليه أو تبديلها أو التلاعب بها، وفي بعض الظروف لا يقتصر أثرها على بيانات نظام الحاسوب أو الحاسوب المستهدف بل ترمي في الواقع عادةً إلى إحداث أثر في "العالم الحقيقي".

ويستطيع المرء من خلال التلاعب بنظم الحواسيب الداعمة على سبيل المثال أن يستخدم نظم العدو لمراقبة الحركة الجوية أو نظمه لتدفق خطوط أنابيب النفط أو محطاته النووية، ونتيجة لذلك، يكون الأثر الإنساني المحتمل لبعض العمليات السيبرانية هائلاً.

وليس بالضرورة أن تتم تنفيذ عمليات سيبرانية تؤدي إلى عواقب خطيرة على السكان المدنيين، ولكن من الممكن تقنياً التدخل في نظم مراقبة المطارات أو غيرها من شبكات النقل أو السدود أو محطات الطاقة النووية من خلال الفضاء السيبراني، ولا يمكن صرف النظر عن سيناريوهات كارثية محتملة، من قبيل تصادم طائرات أو تسرب سموم من مصانع كيماوية أو تعطيل بنية تحتية أو خدمات حيوية مثل شبكات الكهرباء أو المياه، ومن الأرجح أن يكون أهم ضحايا هذه العمليات من المدنيين.

لا ينطبق القانون الدولي الإنساني إلا إذا ارتكبت العمليات السيبرانية في سياق نزاع مسلح، أكان بين دول، أو بين دول وجماعات مسلحة منظمة، أو بين جماعات مسلحة منظمة.

وبالنتيجة، نحتاج إلى التمييز بين المسألة العامة للأمن السيبراني وبين المسألة الخاصة بالعمليات السيبرانية في النزاع المسلح.

وقد تستحضر عبارات مثل "هجمات سيبرانية" أو حتى "الإرهاب السيبراني" وسائل الحرب، غير أن العمليات التي تشير إليها لا تجري بالضرورة خلال نزاع مسلح، ويمكن استخدام العمليات السيبرانية في جرائم تُرتكب في حالات يومية لا علاقة لها بحالات الحرب.

وفي الواقع، نسبة كبيرة من العمليات المعروفة عموماً بعبارة "هجمات سيبرانية" هي هجمات لاستغلال الشبكات تُنفذ لأغراض جمع معلومات غير مشروعة وتحصل خارج نطاق النزاعات المسلحة.

غير أنه في حالات النزاعات المسلحة، ينطبق القانون الدولي الإنساني عندما تلجأ الأطراف إلى أساليب الحرب ووسائلها التي تعتمد على عمليات سيبرانية.

أما عن مبدأ التمييز فإن تميز أطراف النزاعات دوماً بين المدنيين والمقاتلين، وبين الأهداف المدنية والأهداف العسكرية مهم للغاية وقد تكون الهجمات موجهة ضدّ المقاتلين أو الأهداف العسكرية فحسب.

وتُحظر الهجمات العشوائية التي تُوجه أو لا يمكن توجيهها ضدّ هدف عسكري محدد أو لا يمكن الحد من آثارها، حسبما يقتضي القانون الدولي الإنساني، وتُحظر الهجمات ضدّ الأهداف العسكرية أو المقاتلين بالمثل إذا كان يُتوقع أن تتسبب في إصابات أو أضرار مدنية

عرضية، الأمر الذي سيكون مفرطاً مقارنة بالمكاسب العسكرية المتوقعة الملموسة المباشرة (المعروفة بالهجمات غير المتناسبة).

وهذا يعني أن الأهداف المسموحة بموجب القانون الدولي الإنساني في تخطيط العمليات السيبرانية وتنفيذها هي فقط الأهداف العسكرية، من قبيل الحواسيب أو نظم الحواسيب المُستخدمة لدعم البنية التحتية العسكرية أو البنية التحتية المستخدمة على وجه خاص لأغراض عسكرية.

ومن هنا ظهر مفهوم ومصطلح جديد وهو "الأمن السيبراني" أو Cyber Security، والذي سنتناوله بمزيد من التفصيل من خلال الدراسات التي ركزت على تعريفه.

سادسًا: دراسات تناولت تعريف مصطلح الأمن السيبراني :

1-نشأة مصطلح الأمن السيبراني:

يعد الأمن السيبراني أحد أهم القضايا النظامية التي تواجه العالم اليوم، حيث تحول الأمن السيبراني من مجال تقني في المقام الأول يركز على تأمين الشبكات والتكنولوجيا إلى موضوع استراتيجي رئيسي ذي أهمية عالمية.

وحيث أن الأمن السيبراني هو ركيزة لمجتمع مرن رقميا، فإنه ضروري لضمان سلامة العمليات التجارية والاجتماعية المترابطة التي تقع على قمة النظم الإيكولوجية الرقمية المعقدة للمجتمعات الحديثة.

حيث تم تتبع أهميتها المتزايدة كقضية من خلال تقرير المخاطر العالمية للمنتدى الاقتصادي العالمي تحت عنوان "تبادل المعلومات السيبرانية: بناء الأمن الجماعي" أكتوبر 2020، حيث تم تصنيف التأثير المحتمل للهجمات الإلكترونية باستمرار كواحد من أكبر المخاطر التي تواجه الاقتصاد العالمي اليوم، ومنذ ظهوره الحديث نسبيا فقد واجه النظام البيئي للأمن السيبراني العديد من التحديات حيث عمل على إنضاج أنشطة الأمن السيبراني المعزولة للجهات الفاعلة في جميع أنحاء المجتمع إلى نظام بيئي متماسك، والذي يسمح لنفسه بأن يكون مسؤولا أمام جميع أجزاء المجتمع، وكان عليها أن تتغلب على هذه التحديات المشتركة في بيئة تتسم بالمرونة.

أدت جائحة COVID-19 إلى تحول رقمي سريع في العديد من القوى العاملة والقطاعات، مما زاد من اعتماد اقتصادنا العالمي على البنية التحتية الرقمية. وكانت النتيجة هى تفاقم تحديات الأمن السيبراني التي كانت موجودة من قبل، ولكنه أظهر أيضا لجميع أصحاب المصلحة الحاجة والحافز لمواجهة بعض أهم تحدياتنا بشكل مشترك.

وأصبحت هناك حاجة ملحة للتعاون من أجل وضع حلول لهذه التحديات المشتركة، وعلى رأس هذه الحلول هو تبادل المعلومات السيبرانية، حيث لا توجد منظمة واحدة لديها رؤية واضحة على مساحة المشكلة بأكملها، مما يجعل التعاون ومشاركة المعلومات أمرا ضروريا وربما يكون حتميا لمواجهة التحديات والمخاطر السيبرانية.

وحيث أن حجم تحدي الأمن السيبراني الذي يواجه المؤسسات العالمية يتطلب تحولا عقليا عن النماذج التقليدية لإدارة مخاطر الأعمال والأمن، فلم يعد من الممكن الاعتماد على قدرات المرء الخاصة، بدلا من ذلك، سيكون التغيير التدريجي ضروريا لمستقبل مرونة الأعمال.

كما يساعد تبادل المعلومات والقدرة على استخدامها على بناء القدرة على الصمود ودفع العمل الجماعي، فهي واحدة من أهم الأدوات الأساسية التي يتعين على المؤسسة حماية نفسها، ومع ذلك فإنه يجب مشاركة المعلومات لحل المشكلات المعقدة، فإن القدرة على تبادل الأفكار الصحيحة في الوقت المناسب بطريقة منهجية مع أصحاب المصلحة المناسبين ستسمح بالحماية الفعالة للأصول والملكية الفكرية والعمليات التجارية.

إن مشاركة المعلومات السيبرانية كمنصة للمرونة الجماعية يعد أحد أهم وأبرز الحلول الفعالة لمواجهة الهجمات السيبرانية أو الإرهاب الإليكتروني وهجماته، كما تؤكد مشاركة المعلومات السيبرانية قدرة النظام البيئي على أن يكون قادرًا على مشاركة الذكاء التقني على نطاق واسع مع العديد من أصحاب المصلحة المختلفين لتوليد المستوى المناسب من الوعي الظرفي للمؤسسات للدفاع عن نفسها، ويتم ذلك من خلال القيام بعمليات تبادل ومشاركة المعلومات، ما يمكن النظام البيئي الرقمي على الإجابة على ما كان من هجمات، وما يمكن فعله بشأن النشاط الضار، بحيث يجب أن تكون المؤسسات قادرة على القيام بذلك مجتمعه في ثلاثة مجالات رئيسية:

1) **استراتيجي:** المعلومات التي يمكن أن تساعد الشركات على فهم نوع التهديد الذي تدافع عنه، ودوافع التهديد وقدرته والعواقب والمخاطر المحتملة للهجمات.
2) **التشغيلية:** المعلومات التي يمكن أن تساعد في صنع القرار في المؤسسات وتخصيص الموارد وتحديد أولويات المهام، ويتضمن تحليلا للاتجاهات يوضح الاتجاه الفني للجهات الفاعلة في التهديد وفهما للتكتيكات والتقنيات والإجراءات الخبيثة.
3) **التقنية:** المعلومات من البيانات الفنية والمصادر والأنظمة التي توفر رؤى يمكن أن تؤثر على القرارات التكتيكية.

عادة ما يتم اشتقاق هذه البيانات من المراقبة في الوقت الفعلي تقريبا ومشاركة معلومات الشبكة المطلوبة لضبط أمان المؤسسة.

وبالتالي فإن مصطلح "الأمن السيبراني Cyber Security" مصطلح يهدف إلى "ممارسة الدفاع عن أجهزة الكمبيوتر، وأجهزة المحمول، والأنظمة الإليكترونية، والشبكات، والبيانات من الهجمات الخبيثة أو الهجمات السيبرانية، كما يرد بأنه يعني أمن الشبكات والأنظمة المعلوماتية، والبيانات والمعلومات والأجهزة المتصلة بالإنترنت، وبالتالي وعلية فهو يعنى الإجراءات ومعايير الحماية الواجب اتخاذها أو الالتزام بها لمواجهة التهديدات ومنع الهجمات أو الحد من آثارها[16].

ويختلف كل مجتمع أمني عن الآخر، بحيث يجب أن يحدد الرؤى الأساسية المطلوبة لحماية نفسه، سواء كانت هذه المعلومات معلومات تقنية أو رؤى حول السلوكيات أو الاتجاهات الاستراتيجية التي تم اتباعها.

بينما أدرج الإعلان الأوربي الأمن السيبراني على أنه "قدرة النظام المعلوماتي على مقاومة معلومات الاختراق والحوادث غير المتوقعة التي تستهدف البيانات"[17].

بينما عرفت وزارة الدفاع الأمريكية البنتاجون الأمن السيبراني Cyber Security بأنه "كافة الإجراءات التنظيمية التي تؤمن الحماية الكافية للمعلومات بجميع أنواعها وأشكالها، سواء كانت إليكترونية أو مادية، من المخاطر والهجمات والجرائم و وأفعال التخريب والجرائم والحوادث"[18].

وحاليا تبحث الأنظمة والحكومات عن نظام بيئي سيبراني مبتكر ومتكيف، حيث أصبح الابتكار الرقمي محركاً للنمو الاقتصادي، بل أن الأمان السيبراني ليس ضرورياً فقط لحماية حيث أصبح الأمن السيبراني جزءًا أساسيًا من اقتصاد الدول بسبب عدة عوامل رئيسية أبرزها:

1) **حماية المعلومات**: مع تزايد الاعتماد على التكنولوجيا، أصبحت البيانات الحساسة عرضة
2) **زيادة الثقة:** توفر أنظمة أمان قوية يعزز ثقة المستهلكين والمستثمرين، مما يؤدي إلى زيادة الاستثمارات والنمو الاقتصادي في هذا المجال الجديد.
3) **خلق فرص العمل:** يتطلب الأمن السيبراني مهارات خاصة، مما يساهم في خلق وظائف جديدة.
4) **الامتثال للقوانين:** تفرض العديد من الدول قوانين صارمة لحماية البيانات الخاصة بها، مما يدفع الشركات للاستثمار في حلول الأمن السيبراني..
5) **تعزيز الابتكار:** التركيز على الأمن السيبراني يؤدي إلى تطوير تقنيات جديدة، مما يعزز النمو في الاقتصاد الرقمي بشكل عام.
6) **التعاون الدولي:** يتطلب الأمن السيبراني تعاونًا بين الدول لمواجهة التهديدات الإلكترونية، مما يعزز العلاقات الاقتصادية.

وبشكل عام، يعتبر الأمن السيبراني استثمارًا حيويًا لدعم الاقتصاد الرقمي والتنمية المستدامة.

وعرفت إدارة السلامة العامة الكندية الأمن السيبراني Cyber Security بأنه "أمن السيبرانية حماية المعلومات الرقمية، بالإضافة إلى سلامة البنية التحتية التي تضمن وتنقل المعلومات الرقمية. وبشكل أكثر تحديداً، يتضمن أمن السيبرانية مجموعة من التقنيات والعمليات والممارسات وتدابير الاستجابة والتخفيف المصممة لحماية الشبكات والحواسب

والبرامج والبيانات من الهجمات، والضرر، أو الوصول غير المصرح به وذلك لضمان السرية والنزاهة والتوفر"[19].

كما عرف"Edward Amors 2007 "الأمن السيبراني بأنه الوسائل التي من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات ومنها الوسائل المستخدمة في مواجهة القرصنة وكشف الفيروسات[20].

وقد أرجع "بن برغوث، ليلي 2023" عدم كفاءة حماية البيانات وتحقيق الأمن السيبراني إلى قوانين حماية الخصوصية التي تمنع حروب الفضاء السيبراني، حيث فصل "خليفة 2018" ظروف تطور العقيدة العسكرية الذى فرضت على الدول البحث عن استراتيجيات لمواجهتها، من قبيل تطوير وسائل تقنية دفاعية، كتطوير أنظمة إنذار مبكر ضد الهجمات، وتطير برامج الحماية والتصدي، وتأسيس جيوش ووحدات عسكرية سيبرانية خاصة بهدف تعزيز قدرتها الدفاعية في الفضاء السيبراني، وتزويدها بالكوادر المدربة، وتدعيم قدرتها بأحدث تقنيات المواجهة في الفضاء السيبراني، حيث عمد البعض إلى تجنيد محترفي القرصنة والبرمجة في وحدات قتالية خاصة ضمن صفوف القوات المسلحة، مثال القيادة السيبرانية الأمريكية، والوحدة 61398 الصينية، وقراصنة الظل التابعة للحكومة الروسية، والوحدة 8200 في إسرائيل"[21].

وقد خلصت هذه الدراسة إلى عدد من النتائج أهمها أن هناك دورًا بارزا للفاعلين من غير الدول في هذه الحروب، يكون في بعض الأحيان مساويا لدور الدول، بما في ذلك الحركات الإرهابية والأفراد العاديين، وأن هناك فرص اندلاع هذه الحروب مع انتشار التكنولوجيا[22].

كما أن الحروب السيبرانية تؤثر بشكل كبير على تطوير العقيدة العسكرية للدول، وذلك من خلال عدة جوانب:

- **استراتيجيات جديدة:** تفرض الحروب السيبرانية على الجيوش إعادة تقييم استراتيجياتها العسكرية، حيث أصبحت العمليات السيبرانية جزءًا لا يتجزأ من التخطيط العسكري.
- **التكنولوجيا المتقدمة:** تزايد الاعتماد على التكنولوجيا المتقدمة في الحروب السيبرانية يدفع الدول لتطوير قدراتها في مجال الذكاء الاصطناعي، والتعلم الآلي، وأمن الشبكات.
- **الاستجابة السريعة:** تتطلب الحروب السيبرانية قدرة على الاستجابة السريعة للهجمات، مما يعزز من أهمية التدريب والتأهيل المستمر للقوات.
- **التعاون بين الوكالات:** تبرز الحاجة إلى التعاون بين الوكالات العسكرية والمدنية لمواجهة التهديدات السيبرانية، مما يعزز من التنسيق بين مختلف القطاعات.
- **حماية البنية التحتية:** تركز العقيدة العسكرية الحديثة على حماية البنية التحتية الحيوية من الهجمات السيبرانية، مما يضمن استمرارية العمليات العسكرية.
- **الأخلاقيات والقوانين:** تثير الحروب السيبرانية تساؤلات حول الأخلاقيات والقوانين الدولية، مما يستدعي تطوير أطر قانونية جديدة تنظم استخدام القوة السيبرانية.

- **الحرب النفسية:** تستخدم الحروب السيبرانية كوسيلة للحرب النفسية، حيث يمكن نشر المعلومات المضللة للتأثير على الرأي العام وزعزعة الاستقرار.

بالتالي فإن الحروب السيبرانية تعيد تشكيل العقيدة العسكرية، مما يجعلها أكثر تعقيدًا وتنوعًا في مواجهة التهديدات الحديثة.

ولعلنا نجد في الهجمات السيبرانية الأخيرة التي قامت بها إسرائيل في لبنان بتاريخ 18/17 سبتمبر 2024، بعض المستجدات على ساحة الحروب السيبرانية وتطوير الأدوات حيث تمثل هذه الهجمات تحولا كبيرًا في شكل ومستوى الصراع العربي الإسرائيلي، في ضوء تفجيرات الأجهزة اللاسلكية نوع البيجر ونوع أيكوم، التي يستخدمها أعضاء حزب الله في لبنان، والذي تم من خلال تفجير أجهزة عن بعد، للقضاء على خصومها، حيث قُتل 37 شخصاً وأصيب أكثر من 3250 بينهم 300 بحالة حرجة، جراء موجة انفجارات ضربت أجهزة اتصالات لاسلكية من نوعَي بيجر وأيكوم في عدة مناطق في لبنان، في إطار خطة ممنهجة، لتوسيع نطاق الصراع جغرافيا، وتمديده زمنيا، والذي يعد انتهاكًا صريحًا للأعراف الدولية، المتبعة من قبل أفراد القانون الدولي، وإنما أيضا في الإطار النوعي، لتضيف إليه بعدًا سيبرانيًا، يمثل تهديدا صريحا للسلم والأمن الدوليين.

بالإضافة إلى الكشف عن الدور المتنامي للوحدة 8200 الإسرائيلية المتخصصة في الحرب الإلكترونية، وهي وحدة عسكرية إسرائيلية متخصصة في جمع المعلومات الاستخباراتية وتطوير التكنولوجيا العسكرية، والتي كانت أحد الأذرع الرئيسية في التخطيط والتنفيذ لهذه العملية، حيث نجد أن عامل الوقت في التحضير لمثل هذه العمليات ربما يستغرق عشرات السنين وعشرات الشركات الوهمية للإعداد لها[23].

بخلاف العديد من العمليات السيبرانية التي نفذتها حيث يقال أن الوحدة 8200 كانت ضالعة في هجوم "ستاكس نت" الفيروسي بين عامي 2005 و2010 الذى عطل أجهزة الطرد المركزي النووي الإيراني وغيرها من الهجمات.

وتجد الباحثة أن تعريف "الحرب السيبرانية Cyber War" كمصطح يمكن حصره في الآتي هي: "الحرب السيبرانية هي التي تستهدف إختراق نظم معلومات واتصالات بهدف تعطيل، أو إحداث خلل ما، أو تدمير لنظم المعلومات والاتصالات في الدولة المستهدفة، وذلك من خلال بث فيروسات أو برامج تخريبية أو مدمرة للأنظمة والشبكات الحاسوبية، أو إختراق حسابات لأفراد، أو حسابات لمؤسسات في الدولة المستهدفة، للوصول إلى معلومات خاصة أو سرية وتسريبها أو الاستفادة منها لأغراض عسكرية أو أمنية أو عدائية، ويمكن أن تستهدف الضربات الإليكترونية أهدافا عسكرية أو مدنية أو قطاعات خدمية أو إنتاجية، وتتميز بأنها الحرب الأكثر ذكاء والأقل تكلفة، ومن أهم خصائصها التطور السريع والتغير الدائم، كما أنها تتسم بأنها عمليات طويلة ومتوسطة المدى، كما تتسم بخاصية صعوبة تحديد هوية مصدر الهجوم، وتعتبر ساحة بديلة عن الساحة العسكرية التقليدية"

قائمة المراجع

أولاً: المراجع العربية:

1) "بعد تفجيرات «البيجر»... ما الوحدة «8200» الإسرائيلية السرية المختصة بالحرب الإلكترونية؟"، جريدة الشرق الأوسط 18 سبتمبر 2024، https://search.app/Meg8U8xHgc6XrJfD6
2) الأزمات والحروب السيبرانية.. تهديدات تتجاوز الفضاء الإليكتروني، عبد الغفار عفيفي الدويك 2019، مركز الأهرام، https://acpss.ahram.org.eg/News/16843.aspx مركز الأهرام للدراسات السياسية والاستراتيجية
3) اسماعيل صبري مقلد، مخاطر تسببها الفجوة الرقمية: ثورة المعلومات وحروب المستقبل المحتملة، مجلة استراتجيا آفاق المستقبل، العدد 15، يوليو/أغسطس/سبتمبر2012.
4) بارة سمير 2017، الحرب السيبرانية، السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني(2، 2017) الجزائر.
5) بن برغوث،ليلي (2023)، الأمن السيبراني وحماية خصوصية البيانات الرقمية في الجزائر في عصر التحول الرقمي والذكاء الاصطناعي: التهديدات، التقنيات، التحديات، وآليات التصدي، المجلة الدولية للاتصال الاجتماعي، مج 10، ع1.
6) جبور الأشقر 2017, السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، بيروت.
7) خليفة إيهاب 2028، الحرب السيبرانية، مراجعة العقيدة العسكرية استعدادا للمعركة القادمة، مجلة السياسة الدولية، العدد 211، المجلد 53، ص 17-22، مصر، القاهرة، مركز الاهرام للدراسات الاستراتيجية.
8) الشمري، صلاح الدين.م. الأمن السيبراني كمرتكز جديد في الاستراتيجية العراقية، قضايا سياسية، السنة الثانية عشر2020.
9) عباس بدران2010، الحروب الليكترونية: الاشتباك في عالم متغير، بيروت مركز دراسات الحكومة الاليكترونية.
10) معيزي، لينده، الدهقاني، أيوب 2022، الثورة الرقمية في المجال العسكري وتداعيتها على الحروب الحديثة: الحرب السيبرانية نموذجا، المجلة الجزائرية للحقوق والعلوم السياسية، مج7، ع1(2022)، 554-558.

ثانيًا: المراجع الأجنبية:

1) Amorso, E.G. Cyber Security. (S. Press, E'd.2007).
2) Arquilla, John, Ronfeldt, David, 1993, Cyberwar is Coming! Rand Corporation. Atwww.rand.org. Accessed on: 15/4/2020, New York Times, 17/6/2019. New York Times: US ramping up cyber attacks on Russia. At: https://www.nytimes.com/. Accessed on: 25/10/2020.
3) Computers at Risk: Safe Computing in The Information Age (1991), National Academies Sciences Engineering Medicine, https://nap.nationalacademies.org/catalog/1581/computers-at-risk-safe-computing-in-the-information-age
4) Consulting on Canada's Approach to Cyber Security, Public Safety Canada, Government of Canada, https://www.publicsafety.gc.ca/cnt/cnslttns/cnsltng-cnd-pprch-cbr-scrt/index-en.aspx.
5) Dorothy Denning, "Cyberterrorism," Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, 23 May 2000.
6) International Committee of the Red Cross,ICRC,International humanitarian law and cyber operations during armed conflicts,Report,

https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts, 28Novemebr2019.

7) Margaret Rose, What Does Cyberwarfare Mean, Techopedia 2023, https://www.techopedia.com/definition/13600/cyberwarfare.
8) Paul Rosenzweig " Making Good Cybersecurity Law and Policy: How Can We Get Tasty Sauage?".Paper submitted to 8 ISJLP 388 (2012-2013),Heinonline.
9) Pollitt 1998, Is Cyber Terrorism Real or is it Paranoia? South African Journal of Information management -Vol.5 (1),

https://sajim.co.za/index.php/sajim/article/download/208/204.

10) Raghavan 2003, Journal of Law, Technology and Policy p.297, https://heinonline.org/HOL/LandingPage?handle=hein.journals/jltp2003&div=3&id=&page
11) T. X. Hammes, « Technologies Converge and Power Diffuses ...The Evolution of Small, Smart, and Cheap Weapons, policyanaysis, no.786, ,27 January 2016. p.p3-5. 2carlo al bertocuoco,"the revolution in military affairs: theoretical utility and historical evidence», researchpaper, no.142.april 2010p.p16.17. 3Elinorc.sloan ,"the revolution in military affairs implication for canada and nato", Canadian Military Journal, autum,2000.
12) The classified Department of Defense Cyber Strategy 2023, https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF
13) The Global Risks Report 2022, 17th Edition, is published by the World Economic Forum, https://www.weforum.org/publications/global-risks-report-2022/.