مجلة مدارات سياسية
EISSN: 2710 - 8341 ISSN: 2588 - 1825
المجلد (08) / العـدد: (01)، (2024)، ص 362 - 378

الأمن السيبراني
Cyber Security

قاسم سعيد قاسم القدسي
جامعة الجزائر 3، (الجزائر)، alyamani2@live.fr

تاريخ الإستلام: 2024/05/10 تاريخ قبول النشر: 2024/ 06/26 تاريخ النشر: 2024/06/30

ملخص:

تهدف هذه الدراسة إلى تسليط الضوء على الحروب السيبرانية في عصرنا الحديث وتوضيح خطورتها الكبيرة وتأثيرها على الأمن القومي للدول واستقرار المجتمع الدولي. كما تسعى الدراسة إلى اقتراح سبل مكافحة هذه الظاهرة من خلال توفير جميع الوسائل الضرورية لحماية البيانات من التهديدات المتزايدة نتيجة للتقدم التكنولوجي السريع الذي أصبح صعب التنبؤ به والسيطرة عليه بشكل سابق له.

الكلمات مفتاحية: الأمن السيبراني؛ الحروب السيبرانية؛ أمن المعلومات.

Abstract:

This study aims to shed light on cyber wars in our modern era and clarify their great danger and impact on the national security of countries and the stability of the international community. The study also seeks to suggest ways to combat this phenomenon by providing all necessary means to protect data from increasing threats as a result of rapid technological progress that has become difficult to predict and control previously.

Keywords: Information Security; Cyber Warfare; Cyber Security.

1. مقدمة:

منذ ثمانينيات القرن العشرين بدأت ثورة تكنولوجية في مجال الإعلام والمعلومات والاتصالات، إذ انتشرت شبكة الإنترنت وأحدثت تحولًا في الاقتصادات والمجتمعات، حيث أصبحت المعلومات والمعرفة والتنظيم الأفقي أساسًا للتطور وتحولت الشبكة إلى بوابة مفتوحة للاستكشاف والتفاعل وتنوعت في أساليبها وأهدافها.

لا سيما في العصر الحديث شهدنا أنواعًا مختلفة من الحروب بدأت بالحروب التقليدية بين طرفين معروفين، ثم تطورت إلى الحروب الشاملة التي استخدمت فيها الدول كل مقدراتها العسكرية والاقتصادية والسياسية والإعلامية، وفي النهاية شهدنا الحرب الباردة بين الولايات المتحدة والاتحاد السوفيتي والتي تميزت بأنها حرب وكالة حيث تدخلت الدولتان في صراعات في مناطق مختلفة وتأثيراتها امتدت إلى جميع أنحاء العالم.

وتعتمد العديد من دول العالم الحديث على استخدام الشبكات الإنترنت وبروتوكولات الاتصال الحديثة لتبادل المعلومات بشكل سريع وآمن، مع الحفاظ على سرية العمل وعدم الكشف غير الشرعي عن المعلومات. تتوافق هذه الصفات مع متطلبات العصر التكنولوجي الحديث وتمثل القواعد الرقمية الحديثة (Cyber Space) فضاء يحتوي على بيانات ومعلومات رقمية حساسة تمثل الأمن والتنمية للدول، والدول التي تعتمد على التكنولوجيا الرقمية تصبح عرضة للصراعات الحديثة.

فمنذُ أصبح الفضاء السيبراني يحتل مكانة مهمة بين الدول بسبب التقدم التكنولوجي حيث يمكن لأي دولة استهداف أي هدف بسرعة وبتكلفة قليلة عبر وسائل الاتصال الإلكترونية، لذلك قامت الدول بتعزيز أمنها الالكتروني لحماية فضائها تم تقاسم التكنولوجيا الناشئة في الفضاء العالمي للمعلومات، وواجهت الدول صعوبات في تحديد حدودها بسبب طبيعة الإنترنت وتكنولوجيا المعلومات لذلك أصبح من الضروري على الدول تحديد حدودها وجمع المعلومات الرقمية في الفضاء المعلوماتي.

وتتميز الحروب السيبرانية بالصمت والظلام وتكاليف منخفضة ومرونة في الوقت وسرعة الأداء وقوة التأثير وصعوبة تحديد هوية المهاجم، حيث يتم التركيز على مفهوم الحروب الالكترونية وأهدافها في مختلف أقطاب العالم وآلية عملها والبيئة المناسبة لتنفيذها، وتحليل القطاعات المستهدفة وتأثيرها على التطور والبنية التحتية كما تم التطرق إلى أسلحة الحروب والأيديولوجية التي تحكمها، وعليه نحاول من خلال هده المقالة الإجابة على الإشكالية التالية:

*كيف يمكن التقليل أو تفادي الحروب السيبرانية بين الدول من خلال تحصين هذه الأخيرة لأنظمة أمنها المعلوماتية وبالتالي تحصين الأمن القومي لها؟

وحتى تسهل الإجابة على الإشكالية المحورية نقوم بتقسيمها إلى الأسئلة الفرعية التالية:

*ما المقصود بالحروب السيبرانية وكيف تهدد الأمن ألمعلوماتي عامة والأمن القومي خاصة؟

*ما المقصود بأمن المعلومات وما علاقته بالأمن القومي؟

2. ماهية الحروب في الفضاء السيبراني:

1.2 الفضاء السيبراني والحروب السيبرانية (المفهوم والفواعل):

يُتداول مصطلح "الفضاء السيبراني على أكثر من صعيد ذلك كونه أساسا فضاءً اجتماعيا للتواصل والتبادل، إلَا أنَه أضحى مجالا حيويا وجيواستراتيجيا تُخاض فيه العديد من الحروب والهجمات الرقمية.

وتم تعريف الإنترنت من قبل الوكالة الفرنسية لأمن أنظمة الإعلام (ANSSI)، وهي جهة حكومية مسؤولة عن الدفاع السيبراني في فرنسا: بأنه "المساحة الافتراضية التي تم إنشاؤها من خلال الاتصال العالمي بين أجهزة معالجة البيانات الرقمية." ونُلاحظ أن هذا التعريف يركز على الجانب التقني للفضاء السيبراني من خلال إدراج مفهوم الربط التقني، مما يجعله يقتصر على أصحاب الاختصاص من التقنيين فقط دون عامة الجمهور أو حتى الباحثين من تخصصات أخرى، كما أن هذا التعريف يُغفل العامل البشري والذي يُعد جزءا أساسيا في فهم الفضاء السيبراني[1].

وبناءً على المذكور أعلاه يمكن تعريف الفضاء السيبراني على أنه: مجال يتألف من عناصر مادية وغير مادية مثل أجهزة الكمبيوتر وأنظمة الشبكات والبرمجيات وحوسبة المعلومات ونقل وتخزين البيانات أضافة إلى مستخدمي هذه العناصر، ويجب أن نلاحظ أن تحديد هذا المفهوم يعتمد على فهم كل دولة لأمنها القومي حيث يعتبر البعض أن الفضاء السيبراني يشكل جزءًا أساسيًا من استراتيجية الدفاع الوطني.

كما أن عملية تعزيز الجانب الدلالي لهذا الفضاء تستدعي تحليل البنية التركيبية له، إذ يُمكن اعتبارها بنية ذي ثلاث طبقات هي[2]:

أولا/ الطبقة المنطقية: تشمل جميع البرامج التي تحول المعلومات إلى تنسيق رقمي، حيث يتم تحويل اللغة البشرية إلى لغة الآلة باستخدام خوارزميات، ثم تحويلها إلى برامج مكتوبة بلغة البرمجة.

ثانيا/ الطبقة المادية: تشمل معدات الحواسيب والبرمجيات والمعدات الضرورية لعملية الربط البيني.

ثالثا/ الطبقة الإعلامية: تُعتبر هذه الطبقة إضافة اجتماعية للطبقتين السابقتين في العصر الرقمي ويُمكن لكل فرد أن يمتلك هويات رقمية متعددة مثل عنوان بريد إلكتروني ورقم هاتف محمول وصور رمزية على منصات التواصل الاجتماعي.

2.2 الفواعل في الفضاء السيبراني:

تتكون تركيبة الفواعل في الفضاء السيبراني من مستويين، الأول على المستوى الدولاتي، أمَا الثاني فهو على المستوى اللادولاتي[3]:

1/ الفواعل الدولاتية:

وهنا نُشير أساسا إلى الاحتكار القانوني والمنظم للدولة للفضاء الافتراضي، من خلال مختلف أجهزتها (وزارات، وحدات الأمن...)، حيث تعتبر الدولة فاعل محوري في تسيير الفضاء الافتراضي انطلاقا من إمكاناتها المادية والبنيوية والبشرية والقانونية.

ولذلك لابد للدولة من التحكم في مجال الفضاء السيبراني وهو الفضاء الذي يزاحمها فيه العديد من الفواعل الأخرى التي قد تصل حد تهديد مصالح الدولة نفسها.

2/ الفواعل اللادولاتية:

وهنا يأتي دور الأفراد والجماعات والمنظمات غير الحكومية والشركات التي أصبحت بإمكانهما التحكم في توجهات الدول وإدارتها وفق سياسات معينة من خلال الفضاء السيبراني، وسنتناول أهم هذه الفواعل كالتالي:

أ – أصبح الفرد فاعلاً مهماً في العالم الرقمي حيث يمتلك القدرة على إحداث تغيير جذري وأصبحت هذه التحولات مجال استخدام للدول أيضاً، كما في حالة ذلك ما قام به "مارك زوكربارغ" (Mark Zoukerberg) عام 2004، حين أسَس شبكة (فيسبوك) لتستقطب أكثر من ملياري مستخدم عبر العالم على أقل تقدير.

ب – تعتمد المنظمات غير الحكومية بشكل كبير على استخدام شبكة الإنترنت ووسائل التكنولوجيا الحديثة لنشر الوعي والضغط على الحكومات، تقوم هذه المنظمات بتنظيم حملات اجتماعية وتعبئة المجتمع المدني للضغط على الحكومات من أجل تغيير السياسات في مجالات معينة، على سبيل المثال تعمل اليوم العديد من منظمات البيئة العالمية على مواجهة قرار الرئيس الأمريكي (دونالد ترامب) بالانسحاب من اتفاقيات التغير المناخي.

ج – المجموعات الافتراضية (Virtual groups): وهنا يأتي دور القراصنة (Hackers)، وغالبا ما يسعون لتحقيق أهداف مختلفة (ربحية، سياسية، إيديولوجية...)، ومثال دلك نجد المجموعة الافتراضية المشهورة (Anonymous)، والتي تسعى لتسويق خطابات ومطالب سياسية في العالم.

3.2 تعريف الحروب السيبرانية:

تحوّلت الساحة العالمية للإنترنت إلى ساحة حروب حقيقية في عالم افتراضي تقني يعتمد على أحدث التكنولوجيا الرقمية ووسائل الاتصال الحديثة، وتتنوع أشكال هذه الحروب بين الفردية والجماعية والدولية والمؤسساتية والسياسية والاقتصادية والاجتماعية، وأيضاً تشمل هذه الحروب الاتهامات بالإرهاب والمقاومة ضد الاستبداد وغيرها من أشكال الصراعات في الفضاء السيبراني والتي تجري بعيدًا عن أنظار وأذني البشرية.

تعرف الحروب السيبرانية: بأنها صراعات تتم عبر الأنظمة الحاسوبية والشبكات الإلكترونية وتستهدف البيانات والمعلومات والأنظمة الحاسوبية للأعداء، وتتميز هذه الحروب بعدم تقييدها بالمكان والزمان، ويمكن أن تستمر بشكل دائم ومتواصل وهي تُعتبر الحروب السيبرانية تهديدًا كبيرًا للأمن القومي للدول، حيث يمكن للهجمات السيبرانية أن

تتسبب في تعطيل البنية التحتية الحيوية للدولة وتسريب المعلومات الحساسة منذ ابتكار الإنسان لأدوات التواصل الأولى حين بدأت تكنولوجيا الاتصالات تتطور بشكل سريع، فقد بدأت هذه التكنولوجيا القديمة والحديثة منذ ابتكار الإنسان لأدوات التواصل مثل الأصوات والتخابر والتلغراف والهواتف السلكية وأنظمة البرق الصوتية وأنظمة الترميز وآلات الطباعة وغيرها، وتم استخدام هذه التكنولوجيا في الحروب العالميتين الأولى والثانية وفي الحروب والثورات التي وقعت في عصر الثورة الفكرية والصناعية.

ومع التقدم التكنولوجي تطورت أدوات التواصل بشكل كبير وأصبحت جزءاً لا يتجزأ من حياتنا اليومية في العصر الحالي، وبزيادة هذه التطورات زادت أهمية الصراعات السيبرانية عبر الإنترنت حيث أصبحت الوسائل الرقمية أكثر فعالية وسرعة وتأثيراً.

يجمع البعض بين مفهوم الحروب السيبرانية في الفضاء التكنولوجي والفيروسات البيولوجية من حيث آلية العمل حيث تصيب الإنسان بالأمراض، وتُعرف هذه الحروب بأنها "حروب الوحدات المركزية المتقنة العمل" حيث تهدف إلى نشر الوباء السيبراني في جسم الضحية من خلال إرسال معلومات رقمية تستهدف التخريب أو التنصت والتجسس، وهذه الحروب تعتبر امتدادًا للأسلحة الجرثومية والبيولوجية التي تم ابتكارها مع انتشار الأسلحة النووية ولكن بشكل رقمي.

وهناك من يربط مفهوم الحرب السيبرانية ببيئة الإنترنت فقط حيث ساعدت على انتشار المعلومات في مختلف أرجاء العالم بشكل كثيف، وسهلت الوصول إليها بشكل سريع وبناءً على ذلك يتم تعريف الحروب السيبرانية بأنها "الحرب التي تستهدف المعلومات"، وتعتبر اعتداءات تطال مواقع البيانات الموجودة على الإنترنيت وتحاول الاستيلاء على معطياتها بين أطرافٍ متناقضة الأهداف ومتعارضة المصالح، ومختلفة المواقف".

يتماشى المفهوم السابق مع الجوانب السياسية والعسكرية التي تستخدم الفضاء السيبراني كساحة لتحقيق أهدافها، حيث تعتمد تقنيات المعلومات لتحقيق التفوق المعلوماتي وحماية الخطط الاستراتيجية والابتعاد عن الهجمات السيبرانية.

وفي سياق عسكري مماثل تُعتبر المجالات العسكرية من بيئات الحروب السيبرانية التي تتميز بالتجانس والالتصاق، وتعرف الحروب السيبرانية في هذه المجالات بأنها "الحروب التي تتم بالتعاون مع الحروب العسكرية حيث تستهدف الأهداف السيبرانية والرقمية والمعلوماتية، مثل التجسس على الإشارات الصادرة من أجهزة الكمبيوتر التابعة للأهداف المستهدفة وتتبع الموجات الرقمية الصادرة من الهواتف المحمولة وغيرها"، وبالتالي تستهدف هذه الهجمات السيبرانية المصالح القومية والسياسية والعسكرية والأمنية للأهداف المحددة، وتتخذ شكل هجمات سيبرانية أو اختراقات سيبرانية تهدف إلى تعطيل البنية المعلوماتية لها.

ويعتبر بعض القانونيين أن ديناميكيات الحروب السيبرانية تشترك قانونيًا مع إشاعة الرعب والإرهاب، وبناءً على هذه النظرة القانونية يمكن تعريف الحروب السيبرانية على أنها "نظام يستند إلى إثارة الرعب في الشبكة العنكبوتية (الإنترنت)، بهدف تنفيذ أعمال مختلفة لترويع أمن الأفراد والجماعات والمؤسسات والدول وإرهاقهم اقتصاديًا، وتسبب في أزمات نفسية واجتماعية ناتجة عما يعرف بالإرهاب الصامت"[4].

تهدف الحروب السيبرانية إلى إلحاق الأضرار النفسية والمعنوية بالأفراد والدول وقد تشمل أيضًا الأضرار المادية، وتعتمد هذه الحروب بشكل كبير على الشبكات الرقمية وتستخدم أدوات تكنولوجية ووسائل إعلامية متنوعة، وتتميز بأنها غير عنيفة ولا تعتمد على الأسلحة التقليدية بل قد تستخدم الترسانات العسكرية الضخمة، وتعتبر الحروب السيبرانية امتدادًا للحروب التقليدية والمادية حيث يشارك فيها المدنيون والعسكريون معًا، وتستهدف بشكل أساسي تدمير البنية العلمية والمعلوماتية للهدف وتستهدف أيضًا الاتصالات العسكرية واللوجستية والمعلومات الاقتصادية والساسة والمحتوى التقني والرقمي وغيرها.

إن الدفاع عن البيئة الرقمية يتطلب تعاوناً دولياً وتبادل معلومات وخبرات بين الدول والمنظمات لمواجهة التهديدات السيبرانية بفعالية، وهناك أيضاً جانب أيديولوجي في استراتيجيات الحرب في الفضاء السيبراني حيث يمكن أن يكشف عن هوية الجاني أو يوضح دوافع هذه الحروب بشكل إيجابي أو سلبي.

3. ببيئة الحروب السيبرانية وكيفية تنفيذها:

تم فتح الباب الواسع أمام تدفق هائل من المعلومات على البشرية من خلال وسائل الاتصال السيبرانية وذلك بشكل سريع جدًا، وقد ساهمت هذه الوسائل في توفير الوقت والجهد والمال لرواد هذه المجتمعات، وأثرت في تحسين بيئات الملايين من المشتركين الذين استخدموها لتحقيق أهدافهم المعلوماتية وفقًا لاحتياجات أعمالهم وأغراضهم المختلفة في استخدام هذه الشبكات المجتمعية والمعلوماتية، بما في ذلك الجانب التنافسي.

أولا/ بيئة الحروب السيبرانية:

تعتمد بيئة العمل في مجال الحروب السيبرانية على التحولات الكبيرة التي شهدتها البشرية في العصر الحديث، فقد تم تبني مفاهيم المجتمعات المعلوماتية التي تعتمد على كميات هائلة من البيانات الرقمية والقومية الكبيرة وشبكات الاتصال الحديثة، وانتشار الإنترنت وخدمات نقل المعلومات عبر البروتوكولات ووسائل التواصل، والأعمال التجارية الالكترونية والوثائق المحوسبة وغيرها من الوسائل التي تعتمد على البيئات السيبرانية.

وفي سياق الثورة المعلوماتية المتنامية تكونت بيئات تقنية وسيبرانية تعتبر مفهوم التحكم والرقابة غير مقبول، وتدعو إلى المزيد من الابتكارات الرقمية والاتصالية والتي تعزز مفهوم الحداثة والانصهار الجغرافي بين شعوب العالم، وقد ساهمت هذه البيئات الرقمية بشكل كبير في تشكيل بيئات الحروب السيبرانية.

وتثير تحديات تحديد بيئة العمل في الحروب السيبرانية العديد من الجدليات بما في ذلك تفسير مفهوم الحروب السيبرانية، ويعتقد البعض أن انتشار الإنترنت واستخدام تكنولوجيا المعلومات قد ساهم في زيادة الجرائم السيبرانية (الجرائم الإلكترونية) التي تسبب أضرارا اقتصادية واجتماعية ونفسية وسلوكية وأخلاقية، حيث تُعرف هذه الجرائم على أنها "اعتداءات حديثة نسبيا" بسبب تطور التكنولوجيا وتتميز بكونها متجددة باستمرار وتحتوي على جوانب تكنولوجية متعددة ومرونة عالية في التشغيل، وقد أدت هذه الجرائم إلى ظهور فئة جديدة من المجرمين تعرف بمجرمي المعلوماتية (Cybercriminels)[5].

لا شك أن للتطور التكنولوجي والمعلوماتي الحديث تأثيرات سلبية على المجتمعات البشرية، ومع ذلك يبقى استخدام المهارات التقنية والاتصالية هو العامل المحدد لتوجيه هذا التطور في البيئات الرقمية، فمن غير الممكن أن نجمع بين أولئك الذين يستغلون هذا التطور لإلحاق الضرر بأفراد المجتمع، مثل سرقة الأموال واختراق الأمن الوطني والدولي لتحقيق أهدافهم الشخصية، وبين أولئك الذين يستخدمون هذه الوسائل والتطورات كوسيلة لمقاومة الاحتلال أو الدفاع عن وطنهم من الاستغلال التكنولوجي الذي يمارسه الدول الكبرى في العالم.

وتعتمد بيئات الحروب السيبرانية على درجة استخدام الابتكارات التقنية والرقمية فيها مع إيلاء اهتمام للجانب الأخلاقي، والذي قد يتم تجاهله في تلك البيئات وتنقسم بيئة الحروب الرقمية إلى ثلاثة أقسام وفقًا لذلك وهي[6]:

1 – بيئة حرب المعلومات الشخصية: تتميز بطابعها الشخصي وتهدف إلى الإضرار والاستيلاء.

2 – بيئة حرب المعلومات بين الشركات تتسم بالطابع التنافسي بينها.

3 – بيئة حرب المعلومات العالمية تنشأ عندما تندلع صراعات بين دول مختلفة أو بين عدة أطراف.

وبسبب التطورات المتسارعة في قطاع تكنولوجيا المعلومات في عصرنا الحالي يصعب تحديد ملامح أو حدود لبيئة الحروب السيبرانية، ويشهد هذا القطاع إقبالًا بشريًا كبيرًا حيث يوجد من يشيد به ومن يشكك فيه، لذلك يختلف الباحثون في تحديد ملامح هذه البيئات، وهناك من يبالغ في تصوير المخاطر التي تنشأ عن البيئات مستندين إلى مؤشرات حاسمة تنشأ عن البيئات الرقمية وتؤثر على البشرية بشكل عام، وهناك من يستهزئ بهذه البيئات ويعتمدون على قدرة الإنسان على فرض رقابته وسيطرته عليها ويؤكدون أن هناك من يبالغ في تضخيم سلبية هذه البيئات لتحقيق أهدافه الشخصية.

يمكن القول هنُا، أن الفضاء السيبراني بشكلٍ عام ومع ما يحتويه من بيئاتٍ رقميةٍ وتكنولوجيةٍ، تُشكل بتداخلها معاً، ساحات الحروب المعلوماتية، وبيئات الصراعات الناشئة عبر الفضاء السيبراني العالمي والتي يتمثل أهمها بما يلي:

1 – الإنترنيت: والذي يعد من أكثر البيئات الرقمية ملائمةً للحروب الالكترونية.

2 – الموجات والترددات الرقمية: كتلك المنبعثة من وسائل الاتصالات الرقمية المحمولة وغير المحمولة كشبكات الهواتف من الأجيال الحديثة الثالثة والرابعة والخامسة،3G/ 4G /5G .

3 – البني المعلوماتية المحوسبة: لاسيما البني التحتية المعلوماتية العسكرية والمصرفية والحكومية والاقتصادية والاجتماعية والسياسية، والمتبادلة رقمياً بوسائل الإنترنيت وأجهزة الاتصال الحديثة.

4 – المنصات الإعلامية، ووسائل الترويج، وساحات الإعلان الحديثة.

5 – بيئة تكنولوجيا الحروب والعسكرية.

6 – تؤدي الأقمار الصناعية ومراكز الاتصال والقيادة والسيطرة الرقمية دوراً بارزاً في التكنولوجيا الحديثة وغيرها من الوسائل المتعددة.

ثانيا/ آلية عمل الحروب السيبرانية: (الهجوم والدفاع):

في عصرنا الحالي يشهد العالم ظهور لوحة الحرب السيبرانية كتحدي مهم وبالتالي تسعى العديد من حكومات الدول إلى اتخاذ سياسات تقنية ورقمية، وتهدف إلى إنشاء إدارات خاصة تعنى بهذا النوع الحديث من الحروب، ومن بين هذه السياسات إنشاء مراكز متخصصة في إدارة شبكات الإنترنت ومعالجة القضايا التكنولوجية، والتي تتطلب استعداد الدول لتنفيذ خطط للحد من الهجمات السيبرانية وتوجيه ردع سيبراني وحتى محاولة السيطرة على منافذ توزيع الإنترنت داخل حدودها الوطنية.

وتعتمد آلية عمل الحرب السيبرانية بشكل أساسي على وجود عنصرين أساسيين في أي صراع سيبراني قد يحدث في الفضاء الرقمي، ويُعتبر توفر المعلومات أحد هذين العنصرين الهامين حيث تعتمد الحروب التكنولوجية بشكل كبير على هذا العنصر، بالتالي يمكن القول أن توفر المعلومات هو الأساس الأول لآلية عمل الحروب السيبرانية، أما العنصر الثاني فهو القدرات العقلية والذهنية والتي تلعب دورًا حاسمًا في تخطيط وتوجيه الهجمات السيبرانية في عالم رقمي معقد ومليء بالمعلومات[7].

ربما يعتبر البعض أن توفير العنصرين الأساسيين ضرورة لأي نوع من الحروب في العالم سواء كانت تقليدية أو ردعية أو سيبرانية، ومع ذلك يعتمد نجاح وسائل الاتصال الحديثة وأدوات تكنولوجيا المعلومات المتطورة التي تشكل جنود الحروب السيبرانية، وتعمل على تزويدها ببنية معلوماتية صحيحة تنبع من عقل بشري يدرك أهدافه بشكل صحيح، ولكي تكون قادرة على استهداف أهدافها الرقمية بدقة بدون هذه الثنائية الضرورية، لن تتمكن أي حرب سيبرانية من تحقيق أهدافها بشكل رقمي دقيق ولن تكون قادرة على أداء مهامها بكفاءة وفعالية تامة.

وتعتمد العمليات الحربية السيبرانية على توافر العنصرين التكنولوجي والبشري وتعتمد هذه العمليات على إجراءات تقنية وفنية تنفذ خطوات وآليات الحرب السيبرانية في العالم الرقمي وتنقسم إلى الآتي:

***عمليات الهجوم السيبراني:** تنطلق من قاعدة معلوماتية تعتبر مركزاً لمعظم عمليات الحروب السيبرانية في العالم، وتهدف هذه العمليات المعلوماتية إلى السيطرة على معلومات الخصم بهدف منعه من القيام بأي عمليات مسبقة ويتم التركيز في هذه العمليات على ضرب معلومات الخصم السياسية والاقتصادية والعسكرية، وذلك بهدف إلحاق الأضرار المادية والمعنوية النفسية به وتعرض العالم لعدة "هجمات إلكترونية" بالفعل، حيث كانت تلك العمليات موجودة منذ سنوات على أرض الواقع، ومن بين أبرز 7 أمثلة حية على "الهجمات السيبرانية" عالمياً نجد ما يلي:

1/ في عام 2007، تعرضت دولة استونيا لأول هجوم سيبراني استهدف خدمات الاتصالات وتكنولوجيا المعلومات لمدة تقارب 10 أيام.

2/ في نفس السنة، تعرضت شركة "TJX" لهجمات قراصنة، حيث تمكن القراصنة من سرقة بيانات البطاقات الائتمانية وحسابات البنوك وعناوين أكثر من 45 مليون شخص.

3/ تم اختراق قاعدة بيانات تصميمات الطائرة المقاتلة f35i في عام 2009، وتمت سرقة بيانات تصل إلى "تيرابايت"، مما قد يؤثر في المستقبل على أمان الطائرة.

4/ تم اكتشاف فيروس "ستاكس نت" الذي أدى إلى اختراق وتعطيل منظومة التحكم في المفاعلات النووية الإيرانية خلال عام 2010.

5/ تم الإعلان في عام 2013 عن اختراق فيروس لمفاعل نووي روسي يستخدم لتوليد الطاقة الكهربائية.

6/ تعرضت شركة "سوني" للاختراقات التي تسببت في سرقة بيانات تقدر بحوالي 100 تيرا بايت خلال عام 2014.

7/ تم اختراق إحدى شركات إدارة المستشفيات الأمريكية خلال عام 2014، مما سمح للهاكرز بالوصول إلى أنظمة المستشفيات وسرقة بيانات أكثر من 4.5 مليون مريض.

***عمليات الدفاع السيبراني** :وتشمل الإجراءات والوسائل الوقائية وذلك للحد من ردة فعل الخصم المهاجم. تتلخص هذه العمليات الدفاعية بالمنع والوقاية، والتي تهدف إلى حماية النظم وتزويد الجهة الهجومية بالمعلومات الضرورية وتنبيهها وتحذيرها والكشف عن أي اختراقات رقمية في حال حدوثها، ووضع الخطط الاستباقية لمنع حدوث أي اختراقات معلوماتية.

يجب على مسيري المجتمعات المعلوماتية توجيه آليات عمل أدواتهم الرقمية نحو مسارين مختلفين في البيئات الرقمية والتكنولوجية وهما:

1 – يمكن استغلال التقنيات الحديثة لنشر الثقافة الأمنية التي تهدف إلى حماية المعلومات القومية، ويمكن أن تصل هذه الرسالة إلى المجتمعات الخارجية بأن هذه الشعوب تشارك في العمل السيبراني الجماعي، ولا تعتمد فقط على الجهود الحكومية لضمان أمن المعلومات السيبرانية والقومية.

2 – عدم السيطرة على التكنولوجيا الحديثة يعني الاعتماد الكامل عليها والبقاء في دائرة الاستهلاك، مما يؤدي إلى استنزاف الموارد الوطنية كما يحدث في العديد من الدول النامية[8].

4. خصائص الحروب الإلكترونية:

رغم أن الحرب السيبرانية تشبه الحرب التقليدية في بعض الجوانب إلا أن الفضاء السيبراني يتمتع بسمات فريدة تخلق أبعادا جديدة وغير متوقعة، فالأنظمة في هذا الفضاء مرتبطة بالحواسيب وشبكات الاتصال مما يجعل الاضطراب الناتج عن هجمات تقنية يتجاوز حدود الدول ويؤثر على عدة بلدان، وقد تتعرض خدمات الإنترنت التي تعتمد على خوادم في بلد معين للاختراق من قبل مهاجمين يتواجدون في بلد آخر مما يسبب أضرارا مالية كبيرة للشركات التجارية الرقمية، ولا تقتصر الهجمات على الشبكات المدنية فقط بل تمتد أيضا إلى الاتصالات العسكرية، حيث يمكن للمهاجمين استخدام تقنيات الاتصال المجهولة والتشفير لإخفاء هويتهم وتنفيذ الهجمات دون الحاجة إلى التواجد في الموقع الذي يتأثر به النظام.

بالإضافة إلى ذلك يتم استخدام الأدوات البرمجية المتاحة على نطاق واسع عبر الإنترنت لتنفيذ هجمات آلية يمكن للمهاجم باستخدام هذه الأدوات والهجمات المبرمجة مسبقًا مهاجمة آلاف الأنظمة الحاسوبية في يوم واحد باستخدام جهاز واحد، وخاصة إذا كان لدى المهاجم إمكانية الوصول إلى أكثر من جهاز، مثل الوصول عبر برنامج تسلل روبوتي فيمكنه زيادة حجم الهجوم بشكل أكبر فعلى سبيل المثال تشير التحليلات إلى أن الهجمات التي شنت ضد المواقع الحكومية في استونيا، وتمت من خلال آلاف الأجهزة داخل "برنامج تسلل روبوتي" أو مجموعة من الأجهزة المشبوهة لتشغيل برامج تحت سيطرة خارجية، وهي ما تجعل برامج التسلل الروبوتية من الصعب تتبع المهاجم الأصلي لأن الأدلة تشير فقط إلى الأفراد الآخرين في برنامج التسلل، ويشير التحليل الحالي إلى أن حوالي ربع جميع الأجهزة المتصلة بالإنترنت يمكن أن تصاب ببرامج تسلل تجعلها جزءًا من برنامج تسلل روبوتي.

وتسهم الأدوات البرمجية في تبسيط الهجمات السيبرانية وتمكين المستخدمين ذوي الخبرة المحدودة في مجال الحاسوب أو المجموعات العسكرية ذات التقدم الضعيف من تنفيذ هذه الهجمات، بالإضافة إلى ذلك فإن الهجمات التي تعتمد على تكنولوجيا المعلومات والاتصالات عمومًا تكون أرخص من العمليات العسكرية التقليدية، مما يسمح للدول الصغيرة بتنفيذها. وبهذا يمكن لدولة ذات قدرات عسكرية ضعيفة أن توجه ضربة قاصمة للبنية التحتية الحرجة من خلال هجمات سيبرانية، وهذا الاختلال المحتمل في التوازن يجعل الحرب السيبرانية جذابة كاستراتيجية لتحقيق المساواة في الفرص وفي سيناريوهات تكون فيها القوة العسكرية غالبة على القوة الضعيفة، وزيادة الخوف من الحرب الالكترونية نتيجة لوقوع هجمات سيبرانية فعلية (حتى وإن كانت محدودة) وتقوض ثقة الجمهور في تكنولوجيا المعلومات والاتصالات، وبالتالي فإن التذبذبات النفسية المحتملة للنزاع السيبراني يمكن أن تؤدي إلى آثار واسعة الانتشار تعطل استخدام التكنولوجيات الجديدة وتعرقل التقدم في العديد من القطاعات[9].

5 . المبادئ والأسس التي تحكم الحروب الإلكترونية:

تشبه الحروب السيبرانية الحروب التقليدية في أنها تحمل جوانب كبيرة من الأيديولوجيا التي تدعمها الأطراف المتنازعة افتراضياً، وقد تكون هذه العقيدة واضحة في الهجمات السيبرانية التي تشنها الجهات المتنازعة، أو قد تكون مخفية بين طيات هذه الهجمات، مثل التسميات والأشكال التي تحملها الصراعات السيبرانية. على سبيل المثال، تسعى الولايات المتحدة إلى نشر قيمها الرأسمالية في العالم من خلال استخدام التكنولوجيا والثقافة، ويعتقد بعض الاقتصاديين اليابانيين أن العولمة الاتصالية والسيبرانية الأمريكية يمكن تحديدها من خلال الإنترنت والدولار واللغة الإنجليزية، التي تشكل معًا عقيدة أمريكية تهدف إلى نشر الثقافة الأمريكية في جميع أنحاء العالم. ومن الأمثلة الأخرى على هذا الصراع الأيديولوجي الرقمي، قامت الصين مؤخرًا بتبديل محرك البحث غوغل بمحرك بحث صيني، داعمًا للقومية الصينية، في محاولة للتخلص من الهيمنة الغربية والأمريكية في العالم السيبراني.

حيث قامت مجموعة من الشباب العربي والإسلامي بإطلاق موقع للتواصل الاجتماعي يحمل اسم "سلام وورلد"، والذي يهدف إلى تحقيق السلام العالمي ويعتبر هذا الموقع نسخة إلكترونية محدثة تشبه موقع التواصل الاجتماعي الشهير فيسبوك ولكن بطابع إسلامي، يسعى الموقع إلى جذب أكبر عدد ممكن من المستخدمين المسلمين على مستوى العالم وتوحيدهم في منصة اجتماعية تعتمد على المبادئ الإسلامية، يهدف الموقع أيضًا إلى نشر القيم الإسلامية عبر الإنترنت وتقديم منصة مشتركة للتواصل بين المسلمين دون عوائق لغوية أو جغرافية أو إيديولوجية.

وتعمل الشبكة العنكبوتية ووسائل الاتصال الرقمية الحديثة على نشر الأيديولوجيات التي يرغب صناعها في فرضها على العالم، بهدف الحفاظ على سيطرتهم ونفوذهم في المجتمع. تقوم الولايات المتحدة والدول الغربية بتوجيه أيديولوجيتها عبر الوسائل السيبرانية للتأثير على العالم، وتليها إسرائيل في سعيها لنشر قيمها وسيطرتها على العالم الرقمي وتهدف هذه الدول إلى الفوز في الحرب السيبرانية وتحقيق الانتصارات باستخدام التكنولوجيا والتقنيات الحديثة، وفي هذا السياق يعتبر الباحث "يحيى اليحياوي" أنه كلما وجد اتصال بين الأشخاص فإن هناك بالضرورة وجود إيديولوجيا، وإذا لم تكن هذه الإيديولوجيا واضحة وجلية فإنها موجودة بشكل ضمني ومبطن، والإيديولوجيا التي يشير إليها هنا ليست مقتصرة فقط على الاتصال نفسه، بل هي أيضًا متجذرة في المضمون (أي الرسالة التي تنقلها العلاقة بين المرسل والمتلقي) وتكمن أيضًا في الجانب "الأدواتي" للعلاقة نفسها وتشكل أساسها الأساسي[10].

6. أسلحة الحروب السيبرانية:

عزز الفضاء السيبراني التفاعل وتبادل المعلومات والأفكار في جميع أنحاء العالم وأصبحت تكنولوجيا المعلومات والاتصالات هي العمود الفقري للنمو الاقتصادي، والعديد من الأعمال تعتمد على توافر الإنترنت بشكل مستمر، ومع ذلك تتعرض أنظمة المعلومات لسرقة البيانات وزيادة التجسس والحروب السيبرانية وتتميز هذه الحروب بسرعتها

الفائقة، حيث يتم نقل البيانات بسرعة عالية عبر الألياف الضوئية، كما أنها عالمية الطابع وتؤثر في مجالات متعددة وتتم في ساحات غير مرئية وبوسائل خفية تركز هذه الحروب بشكل رئيسي على شبكات الإنترنت، حيث تهدف إلى إلحاق الضرر بأنظمة ووسائل الخصم الإلكترونية.

ويتطلب العمل اليومي على شبكات الإنترنت وجود خطط للتفاعل السيبراني تعتمد على نظم وتطبيقات وبرامج دفاعية يجب أن تكون هذه الخطط قادرة على أداء المهام وتنفيذ العمليات تحت مظلة من البرامج الحمائية، ويجب وجود خبراء مسلحين ببرامج تحقق لهم الدفاع النشط سيبرانيا على مدار الساعة وهذا يجعل التعامل مع الأزمات السيبرانية أكثر إيجابية وفعالية تُبنى خطط الدفاع النشط على الخبرات السابقة وعلى منهجية علمية تفاعلية مع الهجمات، من خلال بناء غرف قيادة العمليات المجهزة إلكترونياً. يجب أن تكون هذه الغرف تحت قيادة مجلس الأمن الوطني السيبراني للدولة وتكون قادرة على التحول من حالة الدفاع إلى الردع وحتى الهجوم السيبراني المضاد، في مقال نشرته جريدة الشرق الأوسط في 22 جويلية 2018، أكد "جيمس ستافريدس وولف دينيستين" أنه من غير المرجح أن يختار بوتين عبور حدود دول الناتو بالدبابات والمدرعات والطائرات، بل سيستخدم ساحة قتال عبر الفضاء الإلكتروني كوسيلة للتأثير والتهديد كما فعل في جورجيا وأوكرانيا[11].

لقد برز دور الفضاء السيبراني بوضوح كمجال جديد في العمليات العدائية من خلال سلسلة من الصراعات بدءًا من الصراع بين استونيا وروسيا في عام 2007، والحرب بين روسيا وجورجيا في عام 2008 وصولاً إلى الصراع بين كوريا الجنوبية والولايات المتحدة الأمريكية في عام 2009، حيث شهدت هجمات إلكترونية كورية على شبكات البيت الأبيض ومن ثم جاء الهجوم الإلكتروني بفيروس "ستاكسنت" على برنامج إيران النووي عام 2010، ممثلاً نقلة مهمة في تطور واستخدام الأسلحة الإلكترونية ولعبت شبكات التواصل الاجتماعي دورًا سياسيًا في إدارة الفوضى في عدد من الدول العربية خلال عامي 2011 و2012، بينما شهدنا هجومًا على آلاف من أجهزة الكمبيوتر في شركة النفط السعودية "أرامكو" في عام 2016، بالإضافة إلى هجمات القراصنة ضد قطاعات الطاقة والصناعة والنقل وشركات الطيران المدني في بعض دول الخليج.

وهكذا أصبحت الحروب اليوم حروبا هجينة وتلعب السيبرانية فيها دورا رئيسيا وأصبحت "الحرب السيبرانية" تتسم بدرجة كبيرة من التطور السريع، وبسبب المنافسة الشديدة القائمة بين شركات البرمجيات الكبرى والتعاون بين هذه الشركات وشركات تصنيع السلاح، وفرص التكامل الكبيرة بين الجانبين ويمكن في هذا الإطار التمييز بين ثلاثة صور رئيسية لعمليات الحرب السيبرانية Cyber War opérations [12]:

الأولى مهاجمة شبكات الحاسب الآلي عن طريق اختراق الشبكات وتغذيتها بمعلومات محرفة لإرباك مستخدمي الشبكات، أو من خلال نشر الفيروسات بهدف تعطيل الشبكة.

الثانية 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 بحثاً عن الفيروسات وتأمينها.

الثالثة، 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، تتسلح الحروب السيبرانية بالعديد من الأدوات والوسائل التّقنية والرقمية، والتي يتم توظيفها في الصراعات الافتراضية الدائرة عبر الفضاء السيبراني في صورةٍ مشابهةٍ للحروب التقليدية التي تندلع على أرض الواقع، وتتنوع أسلحة الحرب السيبرانية باختلاف تأثيراتها ومقدار قوتها ومدى الآثار التي تُخلفها، فمنها ما هو بسيط التأثير ومنها ما هو أعلى من ذلك بكثير وتبعا لكل ما سبق يمكن إجمالي أهم أسلحة الحروب السيبرانية، والتي يتم استخدامها عبر الفضاء السيبراني كوسائل للحرب السيبرانية إلى ما يلي:

أولا: القرصنة والاختراق السيبراني:

1/ القرصنة السيبرانية:

الهاكرز هم الأشخاص المؤهلين للعمل الحاسوبي والسيبراني في عالم البرمجيات والرقميات ويعتبرون جزءًا أساسيًا من القرصنة التي تُعتبر من أضخم وأشمل الأسلحة السيبرانية المستخدمة عبر الفضاء الرقمي، ويتميز هؤلاء الأشخاص بخبرة ودراية عالية جدًا في التعامل مع الحاسوب مما يمكنهم من اختراق مختلف الوسائل الاتصالية والنظم التكنولوجية، بدءًا من الحواسيب والهواتف وصولًا إلى الموجات والألياف الضوئية وغيرها، وتعتمد آلية عمل الهاكرز على تجنيد العديد من الأشخاص المؤهلين لهذا النوع من العمل، وهم قادرون على استخدام مهاراتهم بشكل فعال لاختراق الأنظمة والتسلل إليها.

2/ الاختراق السيبراني:

تتمثل فكرة هذا النظام أو البرنامج السيبراني في استغلال معلومات الخصم وتدميرها بالإضافة إلى تخريب نظامه الحاسوبي والآلي بهدف تحقيق تقدم أمني وعسكري واقتصادي وسياسي، ويمكن أن تتم هذه المواجهة على مستوى فردي أو مؤسساتي أو حتى دولي ويتنوع أشكال الاختراق السيبراني، ولكن جميعها تهدف إلى الدخول إلى قلب معلومات الخصم واستخراجها وذلك باستخدام نظام محو يستهدف البنية المعلوماتية للهدف المحدد[13].

ثانيا: الرسائل الصامتة وزرع الفيروسات والخداع السيبراني[14]:

1/ الرسائل الصامتة:

تقنية برمجية مخصصة للهواتف الذكية من الجيل الثالث وما فوق، تتمثل في إرسال رسائل دون إدراك صاحب الهاتف لوصولها، تساعد هذه الرسائل على تحديد موقع الشخص بدقة من خلال حساب قوة إشارة الموجات الرقمية التي تنبعث من الهاتف وتصل إلى ثلاث مراكز استقبال قريبة، وتسببت هذه التقنية في العديد من الأزمات في المجتمعات الغربية بسبب انتهاكها للخصوصية مما أثر على مبيعاتها عالمياً، على الرغم من قبولها وانتشارها بين رجال الأمن في بعض الدول.

2/ زرع الفيروسات التقنية في البيئات المعلوماتية:

وهي تلك البرامج الإلكترونية المدمرة تعمل ضمن آلية محددة تحددها مطوروها وتأتي بأشكال وأنواع متعددة، تهدف هذه الفيروسات السيبرانية إلى خلق فوضى في نظام تشغيل الضحية المستهدفة وتلويث بيئتها الرقمية، بهدف تعطيل الوصول إلى المعلومات وفقدان جزء كبير من بياناتها الرقمية وقد يصل الأمر إلى تعطيل الأجزاء الفعلية من أنظمة التشغيل الخاصة بها.

3/ الخداع السيبراني:

وتعد وسائل تأمين الصراعات السيبرانية من أهم الأدوات المستخدمة في هذا المجال، حيث تساهم في تحقيق المفاجأة في المعارك السيبرانية ويتضمن هذا السلاح الرقمي عدة وسائل مهمة، مثل التقليد الصوتي والتشويش السيبراني والتضليل المعلوماتي ونشر الشائعات والتنصل الافتراضي والابتزاز السيبراني بالإضافة إلى طرق أخرى للخداع الرقمي.

ثالثا: تأثير شبكات التواصل الاجتماعي في انتشار الأفكار عبر الوسائط المفتوحة[15]:

1/ شبكات التواصل الاجتماعي:

وهي تركيبات اجتماعية تقنية ذات محتوى رقمي تقوم بربط الحلقات الاجتماعية ببعضها ببعض مثل العمل والدين وغيرها، وتضم في طياتها مختلف الفئات العمرية وجميع المستويات الاجتماعية والاقتصادية وكافة الدرجات الثقافية والتعليمية، واستخدم هتلر البث التلفزيوني خلال الحرب العالمية الثانية لنشر خطاباته وتحميس جنوده وجماهيره، وهذه الطريقة استخدمها الخميني أيضًا خلال الثورة الإسلامية في إيران باستخدام ما عرف بـ "الشريط الإسلامي"، لقد اعتمد كل من هتلر والخميني على البث التلفزيوني في ذلك الوقت لأنهما كانا يدركان فائدة هذه الوسيلة الجديدة من وسائل الإعلام الاجتماعي في نقل أهدافهما إلى الجمهور، وهذا المشهد نفسه يلقي بظلاله اليوم على الصراع التقني الناشب عبر الفضاء السيبراني العالمي.

ومع ظهور سلاح جديد وهو شبكات التواصل الاجتماعي، تغيرت ديناميكية الحروب السيبرانية وتضم هذه الشبكات مواقع ذات تأثير كبير على مستوى العالم مثل الفيس بوك وتوتير واليوتيوب والبريد الإلكتروني والماسنجر أضافة إلى غوغل بلس والمدونات السيبرانية وغيرها. وتعتبر هذه المواقع بيئة مثالية للحروب السيبرانية حيث توفر سهولة الوصول والاستخدام وتفاعلية عالية وشعبية كبيرة، وتطور سريع على الرغم من أنها قد تستخدم لأغراض اصطياديه إلا أنها تعتبر منبراً هاماً للتغيير السياسي.

2/ الغزو الفكري عبر الوسائط المفتوحة:

تعتبر المصادر المفتوحة هي تلك المصادر التي تكون متاحة للجميع، وتشمل العديد من الموارد مثل المجلات والنشرات والتقارير والكتب الرقمية والمدونات الرقمية والألعاب الرقمية، يستخدم القائمون على الحروب السيبرانية هذه المصادر بطرق مختلفة بما في ذلك استخدام استخبارات المصادر المفتوحة، والتي تقوم بجمع وتصنيف المعلومات وإرسالها للتحليل الذي يستخدمها ضد الهدف المراد، على الرغم من أن هذه المصادر تحتوي على جانب من الاختراق الخصوصي إلا أنها تعتبر قانونية ومتاحة للجميع، ولذلك فهي تستخدم الجهات الأمنية والاستخباراتية هذه المصادر للحصول على المعلومات بسهولة، ولكن يجب الانتباه للأجندة المعلوماتية التي تهدف لزرع التجسس السيبراني بدون رقابة قانونية.

رابعا: الأقمار الصناعية والتجسس ألمعلوماتي[16]:

1/ الأقمار الصناعية (Satellites) :

تعتبر الأقمار الاصطناعية أسلحة استحواذيه تهدف إلى السيطرة على أكبر قدر ممكن من المعلومات، حيث تقوم بالتقاط ملايين الصور للأهداف وإرسالها إلى قاعدة بيانات على الأرض، وتعد الأقمار الاصطناعية من أكثر الوسائل التقنية فعالية وتعقيدًا في حسم المعارك حيث يمكنها توجيه الصواريخ والقاذفات النارية نحو أهدافها على الأرض، وقد بلغت أهميتها وذروتها خلال الحرب الباردة حيث كانت تهدد العالم باندلاع حرب عالمية ثالثة، وفي الوقت الحاضر تستخدم الأقمار الاصطناعية في التشويش على المحطات الفضائية ومنعها من البث وذلك بأجندة وأهداف سياسية، وتعد هذه الاستخدامات تعبيرًا جديدًا عن الحرب السيبرانية التي تدور في العالم الافتراضي مثل التشويش الذي تعرضت له بعض القنوات الفضائية العربية مثل قناتي العربية والجزيرة خلال الثورات العربية.

2/ التجسس المعلوماتي (Spyware Information):

تعتبر وسائل التجسس التقني والمعلومات من أقدم وأشهر أساليب الحروب السيبرانية. فقد تم استخدام هذا السلاح منذ بداية استخدام الإنسان لوسائل الاتصال والتواصل. تتنوع وسائل التجسس المعلوماتي بين التنصت على المعلومات الصادرة من أجهزة الحواسيب والمحطات الطرفية، واعتراض المراسلات السيبرانية من الأقمار الصناعية والهواتف المحمولة. تتنوع هذه الوسائل بين القديمة والحديثة.

7. الخاتمة:

لم يتمكن العالم السيبراني من الهروب من قضية الحرب على عكس العالم المادي العادي فحيثما يوجد الإنسان يظهر التنافس والصراع وتنشأ الحروب، دون أن ينسى جانب السلام والتعاون والوئام فالخير والشر والأبيض والأسود وما بينهما أمور مألوفة عبر الزمان وفي كل مكان ونظرًا لأن العالم السيبراني هو امتداد للعالم المادي، ولكن بوسائل رقمية فإن الحرب السيبرانية تختلف عن الحرب المادية في أنها تقتصر على هذه الوسائل، ومع ذلك يجب أن نذكر هنا أن هذه الوسائل أصبحت لها تأثير في جوانب الحياة المختلفة وفي مجالات العمل المتنوعة، بما في ذلك تأثيرها على البنية التحتية الحيوية للدول والسيطرة عليها والنتيجة هنا هي أن الحرب السيبرانية هي حرب محصورة من حيث الوسائل، ولكنها تؤثر بشكل واسع في جوانب الحياة المختلفة. وكما هو الحال في الحروب في العالم الواقعي تكون الحروب في العالم السيبراني غالباً ليست شاملة بل تكون متقطعة، حيث يحدث هجمات واختراقات هنا وهناك وعلى الرغم من ذلك فإن الدول تستعد لمواجهة حروب سيبرانية شاملة من خلال تطوير قدرات الدفاع السيبراني التي تكشف الهجمات وتصد هجمات العدو وتهدف إلى ردع أي تحديات محتملة. وبسبب ارتباط الحرب السيبرانية بالتكنولوجيا الرقمية فإن الأسلحة المستخدمة فيها تختلف تمامًا عن الدبابات والطائرات والسفن والقنابل والمدافع والصواريخ، بل هي برامج ذكية تستهدف البنية الحاسوبية لتسبب الضرر فيها وفي كل ما يتصل بها، وبالتالي في حالة عدم توازن في الهجمات الالكترونية وقد تضطر الدول القوية إلى تحويل هذه الحرب إلى صراع حقيقي على الأرض.

8. الهوامش:

1. محمد الزعبي وآخرون، الحاسوب والبرمجيات الجاهزة، ط1، دار وائل للنشر، عمان 2002، ص5.
2. هدى حامد قشوش، جرائم الحاسب الالكتروني في التشريع المقارن، (دار النهضة العربية، القاهرة 1992)، ص6.
3. لطفي لمين بلفرد، "الفضاء السيبراني: هندسة وفواعل"، المجلة الجزائرية للدراسات السياسية، ENSSP، العدد الخامس، الجزائر،2016، ص ـ ص، 148-150.
4. نفس المرجع، ص 153.
5. مكاوي، حسن، تكنولوجيا الاتصال الحديثة في عصر المعلومات، ط 1، القاهرة: الدار المصرية اللُبنانية، 1993م، ص35.
6. المومني، نهلا، الجرائم المعلوماتية، ط1، عمان: دار الثقافة للنشر والتوزيع، 2008م، ص38.
7. نهلا المومني، الجرائم المعلوماتية، مرجع سابق، ص ص45 -47.
8. منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، بيروت 2017، ص ـ ص، 103-104.
9. منى الأشقر جبور، السيبرانية جس العصر، مرجع سابق، ص، ص 103-104.

10. شيخاني، سميرة، " الإعلام الجديد في عصر المعلومات "، في: مجلة جامعة دمشق: (ع 2،1، 26، 2010م) ص435، ص480، ص445.

11. محمد مختار، "الأمن السيبراني" مفاهيم المستقبل، اتجاهات الأحداث، العدد 6، 2015، ص 6.

12. الرشيدي علي بن ضبيان. العدوان على البيئة المعلوماتية: خطورته ومواجهته، مجلة كلية الملك خالد العسكرية، العدد 81، الرياض.2000، ص12.

13. الرشيدي علي بن ضبيان. العدوان على البيئة المعلوماتية: خطورته ومواجهته، مرجع سابق، ص12.

14. حسن بن أحمد الشهري، "الإرهاب الالكتروني – حرب الشبكات"، المجلة العربية الدولية للمعلوماتية،2015، ص19.

15. جاسم جعفر، حرب المعلومات بين إرث الماضي وديناميكية المستقبل، ط 1، عمان: دار البداية للنشر والتوزيع، 2010م، ص 65.

16. سلامة صفات، أسلحة حروب المستقبل بين الخيال والواقع، ط 1، أبو ظبي: مركز الإمارات للدراسات والبحوث الإستراتيجية،2005 ص38.