المحاضرة السابعة–أثر التهديدات السيبرانية على الأمن القومي:

أولا– مفهوم الأمن القومي وأبعاده.

1– مفهوم الأمن القومي.

شاع مصطلح الأمن القومي بعد الحرب العالمية الثانية، إلا أن جذوره تعود إلى القرن السابع عشر، وبخاصة بعد معاهدة وستفاليا عام 1648التي أسست الدولة القومية أو الدولة – الأمة – Nation State وشكلت حقبة الحرب الباردة الإطار والمناخ اللذين تحركت فيهما محاولات صياغة مقاربات نظرية وأطر مؤسساتية وصولاً إلى استخدام تعبير"إستراتيجية الأمن القومي"، وسادت مصطلحات الحرب الباردة مثل الاحتواء والردع والتوازن والتعايش السلمي كعناوين بارزة في هذه المقاربات بهدف تحقيق الأمن والسلم وتجنب الحروب المدمرة التي شهدها النصف الأول من القرن العشرين.

لقد تطور مفهوم الأمن القومي تجاه التهديدات الجديدة غير التقليدية واتسع مجال الأمن ليمتد من الجانب العسكري لمجالات أخرى عديدة، وإذا كان الأمن القومي يعنى بالحماية وغياب التهديد لقيم المجتمع الأساسية، وغياب الخوف من خطر تعرض هذه القيم للهجوم، فإن الفضاء السيبراني قد فرض إعادة التفكير في مفهوم الأمن، وفي هذا المحور وقبل التطرق إلى مصطلح الأمن القومي سنحاول تفكيكه لمعالجة مفهوم الأمن ومن ثم القومية لنصل في محصلة المحور إلى مفهوم الأمن القومي وأبعاده.

أ– **مفهوم الأمن لغة واصطلاحا:**

- **الأمن لغة:**

الأمن في اللغة هو نقيض الخوف، والفعل الثلاثي أَمِن أي حقق الأمان، قال ابن منظور: "أمنت فأنا آمن، وأمنت غيري أي ضد أخفته، فالأمن ضد الخوف، والأمانة ضد الخيانة، والإيمان ضد الكفر، والإيمان بمعنى التصديق، وضده التكذيب، فيقال آمن به قوم وكذب به قوم".

وكلمة الأمن بهذا المعنى ترمي إلى معنيين رئيسيين هما سكون القلب، كما قال ابن فارس والرازي والثقة والطمأنينة كما قال الزمخشري .

وقد ورد المفهوم في القرآن الكريم بقوله تعالى: "فليعبدوا رب هذا البيت الذي أطعمهم من جوع وآمنهم من خوف."

ومن خلال ما تقدّم منكلام وأقوال أهل اللغة والبيان يتضح أ ّن للأمن في لغة العرب باطلاقات عدة فهو يعني: "الطمأنينة، وعدم الخوف، والثِقة، وعدم الخيانة.

- **الأمن اصطلاحا:** أما عن"الأمن" في الاصطلاح فيشير إلى شعور عام بالطمأنينة، وهذا الشعور ناجم عن اعتقاد بالقدرة على مواجهة كافة أنواع المخاطر أو التهديدات، والسيطرة على كافة الأدوات والآليات الكفيلة بمواجهة تلك المخاطر والتهديدات، أيا كان مصدرها، سواء بالاعتماد على الموارد والقدرات الذاتية، أو على موارد وقدرات الآخرين من الحلفاء والأصدقاء، وكل الراغبين في مد يد العون والمساعدة.

وتتفق معظم الأدبيات التي قامت بتعريف مفهوم الأمن على أن المفهوم يشير عموماً إلى تحقيق حالة من انعدام الشعور بالخوف، وإحلال شعور الأمان ببعديه النفسي والجسدي محل الشعور بالخوف، والشعور بالأمان قيمة إنسانية كونية مرغوبة لا تقتصر على فئة اجتماعية معينة أو مرتبطة بمستوى الدخل، فالفقير مثل الغني يحتاج إلى الشعور بالأمان ويسعى إلى تحقيقه وإن اختلفت درجات المتمتع به، ونظراً لصعوبة تحقيق الأمان الكامل، فقد أصبح يُنظر للأمن على أنه مسألة نسبية مرهونة بالسعي لتعزيز أفضل الشروط لتوافره.

والحديث عن الأمن، يستدعي تعريف الخطر،أي التهديد الذي يتعرض له النظام إضافة إلى نقاط الضعف،أو الثغرات التي تعتريه، ومن ثم الإجراءات المفروض اتخاذها، لدفع الخطر. فالتهديد هو نوع الأعمال العدائية، التييمكن أن تمارس ضد النظام، بينما نقاط الضعف هي مستوى الانكشاف على هذا التهديد، في سياق معين. والإجراءات التي يفترض اتخاذها، لا يمكن أن تقتصر في أي حال من الأحوال على التقنية، بل أنها تتناول بناء القدرات، والتوعية، والتدريب، ونقل الخبرات، عدا عن مجموعة من القواعد المحددة والواضحة، التي يفترض إتباعها.

ب- **مفهوم القومية لغة واصطلاحا:**

- **القومية لغة:**

الجذر اللغوي لكلمة القومية هو (ق.و.م،) والقوم يعني الرجال دون النساء، وهو لفظ جمعي لا واحد له،وربما يدخل النساء فيه على سبيل التبع، وجمع القوم أقوام. أما الفعل الثلاثي منها قام، والرباعي أقام، ومنها يأتي معني الارتباط بالمكان.

- **اصطلاحا:**

والقوم هم الجماعة التي ترتبط بمكان ما وتقيم فيه، وعندما يوجد قوم من الناس في أرض واحدة ويمارس

أفراده الحياة بثقافة واحدة توجد بينهم علاقات أخرى قوية تدور حول المصلحة المشتركة والتضامن والنسب، وعلاقات اجتماعية تجعلهم يداً واحدة، وتلك الروابط هي التي توجد ما يُسمى بالقومية.

والقومية هي صلة اجتماعية عاطفية تنشأ من الاشتراك في الوطن والجنس واللغة والمنافع وقد تْنتهي بالتضامن

والتعاون إلى الوحدة، وتعد مبدأ سياسيا اجتماعيا يُفضل معه صاحبه كل ما يتعلق بأمته على سواه مما يتعلق بغيرها، أو هي الاعتقاُد السائد لدى الشعب في أنه يشكل جماعة متميزة ذات سمات خاصة تميزه عن الآخرين، مع توفر الرغبة في حماية هذا التميز والارتقاء به ضمن حكومة ذاتية . ومفهوم "القومي" في الاصطلاح يعرف على أنه الشعور بالانتماء إلى مجموعة بشرية معينة ترتبط فيما بينها

بروابط مشتركة، قد تكون ناجمة عن وحدة الأصل العرقي، أو اللغة والثقافة، أو التاريخ والمصالح المشتركة، وبالتالي تشعر بأن لهاُ هوية خاصة تميزها عن "أقوام" أخرى مختلفة عنها فيُ كل ـ أو بعض ـ هذه السمات. 2

ت-- **مفهوم الأمن القومي:**

يعرف تريجر وكرننبرج الأمن القومي بأنه "ذلك الجزء من سياسة الحكومة الذي يستهدف خلق الظروف المواتية لحماية القيم الحيوية، ويعرفه هنري كيسنجر بأنه يعني "أية تصرفات يسعى المجتمع – عن طريقها – إلى حفظ حقه في البقاء، أما **روبرت ماكنمارا** فيرى أن "الأمن هو التنمية، وبدون تنمية لا يمكن أن يوجد أمن، والدول التي لا تنمو في الواقع، لا يمكن ببساطة أن تظل آمنة. وتعرف الأمانة العامة لجامعة الدول العربية، الأمن القومي بأنه قدرة الأمة على الدفاع عن أمنها، وحقوقها، وصياغة استقلالها، وسيادتها على أراضيها، وتنمية القدرات والإمكانات العربية، في مختلف المجالات، مستندة إلى القدرة العسكرية والدبلوماسية، آخذة في الاعتبار الاحتياجات الأمنية الوطنية لكل دولة، والإمكانات المتاحة، والمتغيرات الداخلية والإقليمية والدولية، التي تؤثر على الأمن القومي العربي.

ولم يعد تعريف الأمن القومي مرتبطا بالتهديدات القديمة فقط، بل هناك نوع آخر من التهديدات حددت تعريفه مثل التعريف الذي قدمه "محمد جمال مظلوم " حيث اعتبر أن هناك تهديدات غير تقليدية وظواهر جديدة تهدد الأمن هي " تهديدات ذات طابع عالمي لا تقتصر على دولة بذاتها، وهي متداخلة بحيث يمكن أن تؤدي أحد التهديدات الى تهديد آخر ، أو يفاقم من نتائجه السلبية، ولا يمكن التعامل معها بشكل نهائي وفقا لنظريات الأمن في صياغته التقليدية، إذ يُعتبر الأمن السيبراني أحد عناصر الأمن القومي غير التقليدي، وذلك لأن أحد مستخدمي الفضاء الالكتروني بإمكانه أن يوقع خسائر فادحة بالطرف الأخر .

ولأسباب تتعلق بالأمن القومي والرفاه الاقتصادي، تحتاج الحكومات إلى المساعدة في عملية حماية

البنية التحتية لمعلوماتها الحيوية، وتعزيز هذه الحماية وضمانها لا يمكن الوصول إليه إلا من خلال وجود استراتيجية وطنية تعنى بالأمن السيبراني، وإن استراتيجية الأمن الوطني السيبراني بشكل عام هي :"كافة التدابير المتعلقة بسرية المعلومات والبيانات التي يتم معالجتها وتخزينها وإبلاغها عن طريق وسائل إلكترونية أو مشابهة، وحمايتها والنظم المرتبطة بها من التهديدات الخارجية أو الداخلية،" وتهدف هذه الاستراتيجية إلى تطوير وتنفيذ قدرات الأمن السيبراني .

وما يجدر الإشارة إليه أن مفهوم الأمن القومي في تبلور واضح مع التغيرات الحاصلة في موازين القوى، إضافة إلى تطور مفهوم دور الدولة، الذي لم يعد تقليديا قائما على حقها في اللجوء إلى استخدام القوة، في الداخل، أو للدفاع عن أراضيها، ضد التهديدات الخارجية، فمع الاعتماد على الأنظمة المعلوماتية، والأجهزة المتصلة بالشبكة العالمية للمعلومات، والعملية المعقدة لطبيعة هذه الأجهزة، من هواتف ذكية، وأجهزة كمبيوتر، وارتفاع نسبة مستخدمي الفضاء السيبراني، تزداد نسبة توقع الاعتداءات و الخروقات والجرائم المعلوماتية، وهذا ما أشار إليه تقرير صادر عن **مركز ماكينزي**، الذي توقع زيادة المعلومات الرقمية، بمعدل ، 44%خلال الأعوام المتدة من 2009 إلى 2020.

إن نسبة التقارير التي تؤكد على ارتفاع نسب اختراق الأنظمة وسرقة البيانات وتسربها، كاختراق أنظمة معلومات بعض الشركات العالمية، الذي تسبب في كشف بيانات عدد كبير من المستخدمين، كذلك الأمر عند اختراق بيانات وزارات هامة في الدولة وتدمير أنظمة معلوماتها، فهذه كارثة أمنية حقيقية تمس بأمن الدولة القومي، ما استدعى الأمر بالدول إلى ضرورة الاهتمام بهذا المجال ووضع خطط ودراسات استراتيجية لمواجهة هذه الأخطار .

2 - **أبعاد الأمن القومي.**

هناك العديد من الأبعاد التي انطوت تحت مظلة الأمن وتعددت هذه الأبعاد التي يجب على الدولة حمايتها إلى خمسة أبعاد كالتالي:

أ- **البُعد السياسي:** ويتمثل في الحفاظ على الكيان السياسي للدولة وهو ذو شقين داخلي وخارجي، ويتعلق البعد الداخلي بتماسك الجبهة الداخلية والسلام الاجتماعي والوحدة الوطنية، بينما يتمثل البعد الخارجي في أطماع الدول الأخرى في مقدرات الدولة ومواردها ومدى تطابق تلك الدول مع الدولة المقصودة سياسياً واقتصاديا واجتماعيا وتحكمه مجموعة من المبادئ الاستراتيجية التيُ تحدد أولويات المصالح الأمنية وأسبقياتها .

ب-**البُعد الاقتصادي:** يهدف هذا البُعد إلى توفير المناخ المناسب للوفاء باحتياجات الشعب وتوفيرُ سبل التقدم والرفاهية للشعب; فمجال الأمن القومي هو الاستراتيجية العليا الوطنية التي

تهتم بتنمية واستخدام كافة موارد الدولة المتاحة لتحقيق أهدافها السياسية بل أن النمو الاقتصادي والتطور التكنولوجي هما الوسيلتان الرئيسيتان لتحقيق المصالح الأمنية للدولة وبناء قوة الردع الاستراتيجية وتنمية التبادل التجاري وتصدير العمالة إلى غير ذلك من المؤشرات المهمة التي تدل على اندماج الجانب الاقتصادي بالأمن القومي .

ت-**البُعد الاجتماعي:** يهدف الأمن الاجتماعي إلى تحقيق الأمن و الاستقرار و الاطمئنان للمجتمع سواء أفرادا أو مجموعات وتنمية الشعور بالانتماء والولاء، كما يستلزم الأمن الاجتماعي تأمين الخدمات الأساسية للإنسان، فلا يشعر بالعوز والفقر والمرض و يشمل الخدمات المدرسية و الثقافية و الرعاية الإنسانية و التأمينات الاجتماعية و على مواجهة الظروف الطارئة . حتى لا يتعرض الأمن القومي للخطر فبتحقيق العدالة يكون هناك تعزيز للوحدة الوطنية والتفاف الشعب حول القيادة السياسية وعلى العكس يؤدي الظلم الاجتماعي لطبقات معينة أو تزايد نسبة المواطنين تحت خط الفقر إلى تهديد داخلي حقيقي للأمن القومي يصعب السيطرة عليه وخاصة في ظل تفاقم مشاكل البطالة والصحة والتعليم.

ث-**البُعد العسكري:** تتحقق مطالب الأمن والدفاع من خلال بناء قوة عسكرية تكون قادرة على تلبية احتياجات التوازن الاستراتيجي العسكري والردع الدفاعي على المستوى الإقليمي لحماية الدولة من العدوان الخارجي وذلك من خلال الاحتفاظ بالقوة العسكرية في حالة استعداد قتالي دائم وكفاءة قتالية عالية للدفاع عن حدود الدولة وعمقها والقوة العسكرية هي الأداة الرئيسية في تأييد السياسة الخارجية للدولة وصياغة دورها القيادي على المستوى الإقليمي والدولي.

ج- البُعد الثقافي: يُحافظ البعد الثقافي على الأمن القومي من خلال حماية الفكر والمعتقدات والعادات والتقاليد والقيم وهو الذي يعزز انطلاق مصادر القوة الوطنية في كافة الميادين في مواجهة التهديدات الخارجية والتحديات الداخلية، فالدور الثقافي بالغ الأهمية في تحصين الوطن من الأطروحات الثقافية للعولمة وصراع الحضارات إذا أخذناه بمفهومه الشامل متضمناً الفكر والثقافة والتعليم والإعلام والفنون والأدب; إذاً فالأمن القومي يعني " تمكين الشعب من ممارسة منظومة القيم الخاصة به على أرضه المستقلة.

ثانيا-التهديدات السيبرانية للأمن القومي:

تعددت مصادر تهديد الأمن القومي، فهناك تهديدات مباشرة ذات تأثير عال واحتمالية حدوث عالية، ومنها "الهجمات السيبرانيةCyber Attacks " التي قد تأخذ عدة أشكال أكثر تطورا من مجرد هجمات، وذلك مثل الحروب السيبرانية ، Cyber warfareالتي تأتي أيضا في إطار عدم الاستقرار السياسي، والإرهاب السيبراني، حيث تمثل هذه المجموعة مصادر للتهديد المباشر للأمن

القومي للدول.

1- الهجمات السيبرانية:

تتمثل التهديدات التي يواجهها الأمن السيبراني في ثلاثة جوانب:

أ- تشمل الجرائم الإلكترونية جهات فاعلة فردية أو مجموعات تستهدف الأنظمة لتحقيق مكاسب مالية أو التسبب في تعطيلها.

ب-غالبًا ما تتضمن الهجمات الإلكترونية جمع معلومات ذات دوافع سياسية.

ت-يهدف الإرهاب السيبراني إلى تقويض الأنظمة الإلكترونية لإثارة الذعر أو الخوف.

إذًا، كيف يمكن للجهات الخبيثة السيطرة على أنظمة الكمبيوتر؟ فيما يلي بعض الأساليب الشائعة المستخدمة لتهديد الأمن السيبراني.

ث-لبرامج الضارة: تعد البرامج الضارة أحد أكثر التهديدات السيبرانية شيوعًا، وهي برامج أنشأها مجرم إلكتروني أو متسلل لتعطيل جهاز الكمبيوتر الخاص بالمستخدم الشرعي أو إتلافه. غالبًا ما تنتشر البرامج الضارة عبر مرفق بريد إلكتروني غير مرغوب فيه أو تنزيل يبدو شرعيًا، ويمكن أن يستخدمها مجرمو الإنترنت لكسب المال أو في هجمات إلكترونية ذات دوافع سياسية.

ج-الفيروس: برنامج ذاتي النسخ يلتصق بملف نظيف وينتشر في جميع أنحاء نظام الكمبيوتر، مما يؤدي إلى إصابة الملفات برموز ضارة.

ح-أحصنة طروادة: نوع من البرامج الضارة المتخفية في هيئة برامج شرعية. يخدع مجرمو الإنترنت المستخدمين لتحميل أحصنة طروادة على أجهزة الكمبيوتر الخاصة بهم حيث تتسبب في تلف البيانات أو جمعها.

خ-برامج التجسس: برنامج يسجل سرًا ما يفعله المستخدم، حتى يتمكن مجرمي الإنترنت من الاستفادة من هذه المعلومات. على سبيل المثال، يمكن لبرامج التجسس التقاط تفاصيل بطاقة الائتمان.

د- برامج الفدية: برامج ضارة تعمل على تأمين ملفات المستخدم وبياناته، مع التهديد بمسحها ما لم يتم دفع فدية.

ذ- برامج الإعلانات المتسللة: برامج إعلانية يمكن استخدامها لنشر البرامج الضارة.

ر- شبكات الروبوت: شبكات من أجهزة الكمبيوتر المصابة بالبرامج الضارة والتي يستخدمها مجرمو الإنترنت لأداء المهام عبر الإنترنت دون إذن المستخدم.

ز- حقن :SQL يعد حقن) SQL استعلام اللغة المنظمة) نوعًا من الهجمات الإلكترونية المستخدمة للتحكم في البيانات وسرقتها من قاعدة البيانات. يستغل مجرمو الإنترنت نقاط الضعف في التطبيقات المستندة إلى البيانات لإدراج تعليمات برمجية ضارة في قاعدة بيانات عبر عبارة SQL ضارة. وهذا يتيح لهم الوصول إلى المعلومات الحساسة الموجودة في قاعدة البيانات.

س- التصيد: يحدث التصيد الإحتيالي عندما يستهدف مجرمو الإنترنت الضحايا برسائل بريد إلكتروني تبدو وكأنها من شركة شرعية تطلب معلومات حساسة. غالبًا ما تُستخدم هجمات التصيد الاحتيالي لخداع الأشخاص لتسليم بيانات بطاقة الائتمان والمعلومات الشخصية الأخرى.

ش- هجوم قطع الخدمة (هجوم رفض الخدمة): حيث يقوم مجرمو الإنترنت بمنع نظام الكمبيوتر من تلبية الطلبات المشروعة عن طريق إغراق الشبكات والخوادم بحركة المرور. وهذا يجعل النظام غير قابل للاستخدام، مما يمنع المنظمة من القيام بوظائف حيوية.

تركز بروتوكولات الأمان الإلكترونية أيضًا على أكتشاف البرامج الضارة في الوقت الفعلي، ويستخدم الكثيرون التحليل الإرشادي والسلوكي لمراقبة سلوك البرنامج ورمزه للدفاع ضد الفيروسات أو أحصنة طروادة التي تغير شكلها مع كل عملية تنفيذ (البرامج الضارة متعددة الأشكال والمتحولة). يمكن لبرامج الأمان أن تحصر البرامج الضارة المحتملة في فقاعة أفتراضية منفصلة عن شبكة المستخدم لتحليل سلوكها ومعرفة كيفية أكتشاف الإصابات الجديدة بشكل أفضل.

وتستمر برامج الأمان في تطوير دفاعات جديدة حيث يحدد متخصصي الأمن السيبراني التهديدات الجديدة وطرقًا جديدة لمكافحتها. لتحقيق أقصى أستفادة من برامج أمان المستخدم النهائي، ويحتاج الموظفون إلى التثقيف حول كيفية أستخدامها. والأهم من ذلك، أن استمرار تشغيله وتحديثه بشكل متكرر يضمن قدرته على حماية المستخدمين من أحدث التهديدات السيبرانية.

2- الإرهاب السيبراني:

يعتبر الإرهاب السيبراني تهديدا واضحا للأمن القومي للدول والذي يتضح من خطورة توظيف التقنيات الذكية في تنفيذ هجمات إرهابية سيبرانية، سواء عبر الفضاء السيبراني أو استخدام الربوتات وطائرات دون طيار في شن تلك الهجمات أو استخدام الطابعات ثلاثية الأبعاد في تصنيع الأسلحة.

وكان " **باري كولين** Barry Collin"من أوائل الذين استخدموا مصطلح الإرهاب السيبراني Cyber terrorism( )في ثمانينات القرن الماضي والتي خلص فيها إلى صعوبة وضع تعريف شامل للإرهاب التكنولوجي، ولكنه تبنى تعريفاً للإرهاب السيبراني بأنه : " هجمة إلكترونية غرضها تهديد الحكومات أو العدوان سعيا عليها لتحقيق أهداف سياسية أو دينية أو أيديولوجية، وأن الهجمة يجب أن تكون ذات أثر مدمر وتخريبي مكافئ للأفعال المادية للإرهاب."

فقد أضحت الأسلحة السيبرانية من أهم أدوات حروب الجيلين الرابع والخامس، وهي ليست حكرا على الدول فقط، إذ تقوم التنظيمات المتطرفة باستخدام بعض آلياتها، فهي مجرد فيروسات وبرمجيات خبيثة يتم تصميمها عبر برامج كمبيوتر، لشن هجمات إلكترونية على أهداف عسكرية أو مدنية، تؤدي إلى تدمير النظم والبرمجيات أو مكوناتها المادية أو إلحاق خلل وظيفي أو فني بها، بما قد يؤدي في النهاية إلى تدمير البنية التحتية للدول أو اختراق الأنظمة العسكرية والتجسس على الأفراد والمعلومات وأنظمة الاتصالات، وغيرها من الأعمال التخريبية التي تهدد أمن الدول.

ووفقاً لوزارة الدفاع الأمريكية "البنتاغون" فإنها تعرف الإرهاب الالكتروني بأنه :" عمل إجرامي يتم الإعداد له باستخدام الحاسبات ووسائل الاتصالات ينتج عنها عنف وتدمير أو بث الخوف تجاه تلقي الخدمات بما يسبب الارتباك وعدم اليقين وذلك بهدف التأثير على الحكومة أو أو السكان لكي تمتثل لأجندة سياسية أو اجتماعية أو فكرية معينة "، وتتعدد استخدامات التنظيمات الإرهابية للتكنولوجيا ومخرجاتها، سواء لأغراض التجنيد والدعاية الدينية المتطرفة، أو للتمويل من مصادر خفية يصعب تعقبها، أو في صناعة الأسلحة وتنفيذ العمليات الإرهابية.

3- **الحروب السيبرانية.**

عرفت على أنها توظيف القدرات السيبرانية وذلك بهدف تحقيق غرض أساسي، يتمثل في تحقيق الأهداف أو الآثار العسكرية في الفضاء الإلكتروني أو من خلاله، وبالتاليُ يمكن تلخيص مفهوم الحروب السيبرانية في معناها الإجرائي بأنها: هي الهجمات التي تشنها بعض الدول ويكون مسرحها هو الفضاء الإلكتروني بغرض إلحاق الضرر بالمنشآت والبنى التحتية والأهداف العسكرية للدولة التي تعرضت للهجوم، وتتميز حروب الفضاء الإلكتروني بأنها يمكن أن تكون من فاعلين غير الدول فيكون هناك صعوبة في تحديد العدو والجهة والمهاجمة.

وعند تعريف حروب الفضاء الإلكتروني لابد من الإشارة إلى الجهود الفكرية لعدد من المعنيين بدراسة الحروب الإلكترونية مثل" **جون أركويلا** "و"**ديفيد رون** "اللذان عرفا حروب الفضاء الإلكتروني بأنها " إجراء أو استعداد لإجراء عمليات عسكرية بالاعتماد على المبادئ والآليات المعلوماتية، ما يعني تعطيل أو تدمير نظم المعلومات والاتصالات في دولة العدو المستهدفة،

وُيمكن تعريف الحروب الإلكترونية من النظرة القانونية بأنها نظام نتشر في الشبكة العنكبوتية تهدف إلى لم قائم على الرعب ا تنفيذ العديد من الأعمال لترويع أمن الأفراد والجماعات والمؤسسات والدول وإرهاقهم اقتصاديا وإدخالهم في أزمات نفسية واجتماعية ناتجة عما يعرف بالإرهاب الصامت، وينطلق هذا المفهوم من الواقع الغربي، وهي حرب ناعمة صامتة تأخذ أشكالاً عدة كشكل الاتصالات بين الجيوش وقاداتها وإضعاف شبكات النقل والإمدادات اللوجستية وضرب المعلومات الاقتصادية وإحراج الساسة والعبث بالمحتوى الفني والتقني.

والدولة هي الفاعل الرئيسي في الحروب السيبرانية بالأساس، حيث بدأت بعض الدول الاستعداد لهذا النوع من الحروب، سواء من خال إنشاء جيوش سيبرانية داخل صفوف القوات المسلحة للدول، أو من خال إبرام الاتفاقات السياسية والعسكرية، بعدم شن أي هجمة سيبرانية، مثل الاتفاقية المبرمة بين الولايات المتحدة الأمريكية والصين في عام 2015.