جامعة محمد لمين دباغين -سطيف2
كلية الحقوق و العلوم السياسية
قسم العلوم السياسية
مقياس قضايا السياسة العالمية المعاصرة———— ماستر2 علاقات دولية

الأستاذة : د بركان إكرام email : paxikramika@hotmail.com
السنة الجامعية 2024 / 2023

ملاحظة: نظرا للتفصيل في دروس مقياس قضايا السياسة العالمية يرجى من الطلبة فهم الدروس واستكشاف أهم الرو ابط التي تجمع بين القضية والأخرى، والاستغناء عن الحفظ الحرفي

درس حول الهجمات والجر ائم الالكترونية و الأمن السيبر اني

يسعى هذا الدرس المتمركز حول الأمن السيبراني إلى تبيان طبيعة التهديدات الأمنية الناجمة عن التطورات في المجال التكنولوجي والمعلوماتي وأشكالها المختلفة، ومدى خطورة هذه التهديدات على أمن الفواعل الدولية مقارنة بالتهديدات التقليدية. وذلك إلى جانب تحديد كيف تغيرت طبيعة وسبل إدراة الصراع في العلاقات الدولية نتيجة للتطورات في تكنولوجيا المعلومات، وإمكانية أن تحل الحروب و الصراعات الالكترونية محل الحروب والصراعات التقليدية على الساحة الدولية.

نتيجة للاعتماد المتزايد من قبل الفواعل الدولية على أنظمة وشبكات المعلومات والبنى التحتية المعلوماتية ، أصبحت قضايا الأمن الالكتروني من أبرز قضايا العلاقات الدولية في العصرالحديث. إذ نجد أن عديد الدول- خاصة الدول الكبرى كالولايات المتحدة الأمريكية ، الصين وروسيا- قد قامت بتطوير سياسات أمنية تهدف إلى مواجهة التهديدات الأمنية ذات الطبيعة الالكترونية التي قد تتعرض لها. كما قام عدد كبير من المنظمات الدولية كالاتحاد الأوروبي وحلف الناتو، بإنشاء هياكل داخلية وتطوير سياسات تتولى مهمة تحقيق الأمن الالكتروني للدول الأعضاء.

ومن ثمة بات الأمن الاكتروني يمثل أحدث وأهم صور الأمن في العلاقات الدولية / مما أدى إلى تزايد اهتمام الباحثين في مجال العلاقات الدولية بدراسته، والبحث في القضايا المرتبطة به. ولعل أبرز هذه القضايا هي أنماط التفاعل ما بين الفواعل الدولية . فمن ناحية نجد هناك العديد من أشكال التفاعلات الصراعية التي لها آثار سلبية في العلاقات بين الفواعل الرسمية منها الهجوم السيبراني الروسي ضد استونيا وجورجيا في 2008، وغيرها بما بات يعرف بالصراعات الالكترونية Cyber conflict والتي لم تعد مقصورة فقط على الدول و إنما تتضمن فواعل أخرى كما حدث بين غوغل والصين في 2010.

الأمن السيبير اني:

أصبح ظهور التهديدات والجرائم السيبيرانية تحديا كبيرا للأمن القومي وكذلك الدولي ، لدرجة أن العديد من الباحثين اعتبر أن الفضاء السيبراني بمثابة المجال الخامس في الحروب بعد البر والبحر والجو والفضاء ، وهو ما استدعى ضرورة وجود ضمانات أمنية ضمن هذه البيئة الرقمية، تبلورت بشكل أساسي في ظهور الأمن السبيراني Cyber Security كبعد جديد ضمن أجندة حقل الدراسات الأمنية.

- **تعريف للفضاء السيبر اني:**

أكد دانيال كوهل على أن الفضاء السيبراني هو أكثر من مجرد أجهزة كملبوتر ومعلومات رقمية ، و هماك أربعة جوانب للفضاء السيبراني يجب أن بعكسها التعريف وهي :

- مساحة تشغيلية Qn operational space : يستخدم الأشخاص والمؤسسات الفضاء الالكتروني للعمل وإحداث التأثيرات ، إما في الفضاء الالكتروني فقط أو عبر المجالات الأخرى.
- مجال طبيعي A natural domain : الفضاء الالكتروني هو فضاء طبيعي، يتكون من نشاط كهرومغناطيسي ويتم إدخاله باستخدام التكنولوجيا الالكترونية.
- يستند إلى المعلومات Information based: يدخل الأشخاص إلى الفضاء الالكتروني لإنشاء المعلومات وتخزينها وتعديلها وتبادلها واستغلالها.
- مجموعة شبكات مترابطة Interconnected networks: وجود اتصالات تسمح للنشاط الكهرومغناطيسي بنقل المعلومات .

تعريف الأمن السيبر اني:

إن مصطلح الأمن السيبراني ظهر عالميا منذ 2013، وتعتبر مصطلح السيبرانية واحد من أكثر المصطلحات ترددا في معجم الأمن الدولي، ومعناها " الفضاء المعلوماتي"، ما يعني أن الأمن السيبراني " أمن الفضاء السيبراني". ويعرف كل من Neittaanmaki Pekka, Lehto Martti في كتابهما الموسوم بـ Cyber Security :Analytics, technology and automation حيث اعتبراه " عبارة عن مجموعة من الاجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكمبوتر وعواقبهما، و يتضمن تنفيذ التدابير المضادة المطلوبة.

وقدمت وزارة الدفاع الأمريكية " البنتاغون" تعريفا دقيقا لمصطلح الأمن السيبراني باعتباره" جميع الإجراءات التنظيمية اللازمة لحماية المعلومات بجميع أشكالهما المادية والالكترونية، من مختلف الجرائم : الهجمات، التخريب، التجسس والحوادث:. في حين اعتبر الاعلان الأوروبي الأمن السيبراني أنه" قدرة النظام المعلوماتي على مقاومة محاولات الاختراق التي تستهدف البيانات".

عموما يمكن القول أن الأمن السيبراني يشير الى مجموعة الأنشطة والتدابير التي تهدف إلى حماية الحواسيب ، وشبكات الحاسب الآلي، والأجهزة والبرامج وما تتضمنه أو تتبادله من معلومات وبيانات، وغيرها من عناصر الفضاء الالكتروني، ضد أي هجوم أو اعتداء أو اتلاف. كما تنطوي أيضا على الكشف عن التهديدات الأمنية المختلفة والتفاعل معها، والتخفيف من الآثار السلبية المترتبة عنها، و استعادة ما تم اتلافه من مكونات.

من هذا لمنطلق أصبح الباحثون في العلاقات الدولية وبقية الحقول الفرعية في الدراسات الأمنية والدراسات الاستراتيجية يركزون بشكل متزايد حول أثر التكنولوجيا على الأمن القومي والدولي وذلك لتأثيرها على مفاهيم مثل القوة، والسيادة ، والحوكمة العالمية والأمننة. أما على مستوى ممارسة الدول ، فقد ارتبط ظهور الأمن السيبراني بظهور الهجمات السيبرانية.

-القوة السيربانية: يعترب Jr ,Nye .S Joseph أستاذ العلاقات الدولية الأب الروحي لمصطلح القوة السيبرانية ومن أهم من تحدثوا عنه، باعتباره شكل من أشكال القوة، حيث عرفها بما يلي: "القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، أي أنها القدرة على استخدام الفضاء السيبراني لخلق مزايا، والتأثير في الأحداث المتعلقة بالبيئات الواقعية الأخرى، وذلك بواسطة أدوات إلكترونية ، ويعرفها "Kuehl.T Daniel بأنها القدرة على استخدام الإنترنت لخلق مزايا والتأثير على الأحداث في البيئات التشغيلية كافة من خلال أدوات القوة"

الإطار النظري للأمن السيبر اني :

يعتمد الأمن السيبراني في إطاره النظري الى مقولات دايفيد ليون وديدي بيغو، المنتميان إلى مدرسة باريس للدراسات الأمنية، حيث يشير دافيد ليون إلى ما أطلق عليه " المراقبة أو العين الالكترونية" ، التي تعني أن السلطة يجب أن تكون منظورة وغير ملموسة ، و لها أنشطة جديدة وتتخذ في مجتمعنا المعاصر أشكالا عديدة منها استخبارات الاتصالات، واستخبارات الرادار، و الاستحبارت الالكترونيات ، واستخبارات الصور، حيث تعمل جميعها تحت علامة الاستخبارات التقنية التي تشكل نظاما جديدا للقوة في العلاقات الدولية، و تعمل بمثابة مصدر تقني استراتيجي للحقيقة الأمنية، من خلال قدرتها الظاهرة على توفير المعلومات المنفصلة الخالية من القيمة حول الموضوع المراقبة معتمد على "الصورة لا تكذب" .

كما يعتمد على فرضية جوزيف ناي في مقالته حول القوة الناعمة حيث أشال إلى أن التغيرات التي شهدها العالم بعد الحرب الباردة وأهمها زيادة العولمة والتقدم التكتولوجي الاستثنائي الذي بمكن التعبير عنخ بالثورة المعلوماتية شبب في الجزء الأعظم من المشكلات والتهديدات التي تنتاب العالم اليوم. ويوضح ناي أن هذه المتغيرات، خاصة المتغير التكنولوجي أدت إلى تراجع التهديدات المرتبطة على القوة الصلبة لصالح ظهور تهديدات المرتبطة بالقوة الناعمة، والتي خلقت تهديدات الا تتمتع فيها الدولة بميزة مطلقة كونها تفع خارج سيطرة القوة العسكرية و البنى الأساسية الحكومية والسيطرة المؤسسية .

وبناء على ما سبق يمكن أن نستنتج خصائص التهديدات الجديدة :

- تتميز بعنصر المفاجأة والمرونة و التكتيكات غير التقليدية وصعوبة تحديد طرف الهجوم.
- توثر هذه التهديدات على الرأي العام الداخلي ، وعمل المؤسسات الرسمية ، و المجتمع الدولي.
- تستخدم وسائل غير تقليدية على رأسها الوسائل التكنولوجية لأحداث أثر على الطرف الآخر يتراوح بين التهديد، والتخريب، و الهجوم العنيف واحداث أضرار جسيمة.
- تزيد فعالية هذه التهديدات بتداخل أشكالها مع الأشكال التقليدية .

أهمية الأمن السيبراني وأهدافه:

يهدف الأمن السيبراني إلى:

- تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات.
- التصدي لهجمات وحوادث أمن المعلومات التي تستهدف الأجهزة.
- سد الثغرات في أنظمة أمن المعلومات.
- مقاومة البرمجيات الخبيثة ، وما تحدثه من أضرار بالغة للمستخدمين.
- الحد من التجسس والتخريب الالكتروني على مستوى الحكومات والأفراد.

القوى الفاعلة في الأمن السيبراني:

يحدد جوزيف ناي أنواع من الفاعلين الذين يملكون القوة السيبرانية كما يلي :

1- **الدول :** والتي لديها قدرة كبيرة على تنفيذ هجمات سيبرانية وتطوير البنية التحتية وممارسة السلطات داخل حدودها.

وكثيرا ما يقال إن روسيا مسؤولة عن الهجمات السيبرانية على إستونيا في ،2007 وجورجيا في 2008. وأن الصين مسؤولة عن عدد من عمليات الاستغلال السيبراني الشهيرة في الكثير من البلدان. وأن الولايات المتحدة و/ أو إسرائيل مسؤولة عن الهجوم السيبراني على المنشآت النووية الإيرانية (الفيروس »ستوكسنت«. ولكن لم يقر أحد من هذه البلدان رسميا بالقيام بأي من هذه الأنشطة، ولم يُجر الإعلان عن دليل قاطع- إن وجد- على أن القيادة السياسية لأي بلد أمرت أو أشرفت على أي من هذه الأنشطة.

على الرغم من الطبيعة الفوضوية للنظام الدولي، ولكن الجماعة الدولية تسعى لمحاولة الاتفاق على قواعد منظمة لاستخدام الفضاء السيبراني، عبر طرح القضية في العديد من المحافل الدولية كمؤتمر دافوس الاقتصادي لعام 2021حيث احتلت القضية صدارة أجندة المؤتمر كذلك الحال بشان قمة ميونخ 2020 التي أكدت على أهمية الدور الذي تلعبه الحكومات في مجال الأمن السيبراني، وقمة العشرين التي عقدت في فبراير 2020 وتوصلت إلى الحاجة إلى وجود السياسات الملائمة لتخفيف أثر الهجمات السيبرانية.

2- **المنظمات الدولية:**

تهدف لتضافر الجهود الحكومية لمواجهة الهجمات والتهديدات السيبرانية، وتتنوع دورها ما بين تبادل الخبرات والمعلومات وتوفير الكوادر المدربة، والمساعدة في وضع الخطط والاستراتيجيات لمكافحة الجريمة السيبرانية، دعم الجهود الدولية للتصدي للهجمات السيبرانية. كالمنظمة الدولية للشرطة الجنائية "الإنتربول"، حيث تقدم ساحة من أجل التواصل بين أجهزة الشرطة وسائر الجهات المعنية في مجال مكافحة الجريمة السيبرية لتبادل الخبرات والمعلومات وأفضل الممارسات. قد أنشأ الاتحاد الأوروبي المجلس الأوروبي ضد الجريمة

السيبرانية، والذي نجح في التوصل لاتفاقية بودابست للجريمة السيبرانية وأسفر عنها تأسيس مكتب برنامج الجريمة السيبرانية للتصدي للتحديات.

3- **الفواعل غير الدولاتية :** والتي تتعدد بين

الشركات متعددة الجنسيات التي تمتلك بعض شركات التكنولوجيا موارد قوة تفوق قدرة بعض الدول، فشركات كجوجل ، فايسبوك، ومايكروسوفت تسمح لها بامتلاك قواعد بيانات عملاقة.

الجماعات الإرهابية : والتي تعتبر من أبرز الفواعل خاصة بعد 11 سبتمبر، حيث يشتغل الفضاء السيبراني في عمليات التجنيد والتعبئة و الدعاية و جمع الأموال والمتطوعين ،و جمع المعلومات حول الأهداف العسكرية.

أصغر في مقدراتها من الدول، لها أهدافا تخريبية، إلا أن قدرتهم على القيام بعمليات واسعة النطاق تعوزها مساعدة أجهزة استخبارات دولية، وان كان من اليسير عليها اختراق المواقع الإلكترونية واستهداف الأنظمة الفاعلة. قد تمارس الضغط لتفعيل تبادل المعلومات الأمنية الرقمية، أو اختراق نظم التأمين وأمن المعلومات فتستخدم الجماعات الإرهابية هذا الفضاء لسرقة المعلومات، وتسهيل كل ما هو غير مشروع من عينة تجارة البشر والسلاح مستغلى ما يسمى السوق السوداء على الشبكة العنكبوتية .

المنظمات الإجرامية : والتي تقوم بعمليات القرصنة السيبرانية، وسرقة المعلومات واختراق الحسابات البنكية، وتحويل الأموال.

4- **الأفراد :** وحتى الآن كان الفاعلون المعروفون الذين نفذوا أعمال استغلال سيبراني وهجمات سيبرانية هم أطراف دون المستوى الوطني، أفراد في معظمهم. وفي الغالب بقصد الربح. أصبح الفرد بفعل الفضاء السيبراني عنصرا فاعلا ومؤثرا في العلاقات الدولية، ومثال على ذلك وثائق ويكيليكس الذي نجح في نشر الملايين من الوثائق السرية للإدارة الأمريكية، ما خلق مشاكل دبلوماسية بين الولايات المتحدة الأمريكية وحلفائها.

من هنا يتضح، أن الأمن السيبراني والتقدم التكنولوجي قد أثر على تحديد ماهية الوحدات الدولية الفاعلة، بل أضحى نفسه فاعلا على الساحة الدولية، ويسر لفاعلين قائمين بالفعل على زيادة فاعليتهم لتحقيق أهدافهم بطرق مشروعة وغير مشروعة تؤثر بدورها على السياسة الدولية.

أبعاد الأمن السيبراني:

يرتبط الأمن السيبراني بعدة مجالات مختلفة اقتصادية، اجتماعية وسياسية وإنسانية وقانونية بهدف تحقيق منظومة أمن متكاملة وذلك كما يلي :

- **الأبعاد العسكرية :**

تتمثل الميزة الأساسية للأمن السيبراني في بعده العسكري عن طريق قدرة القوة السيبرانية على ربط الوحدات العسكرية ببعضها البعض عبر العالم الافتراضي، وهذا ما يسهل عملية تبادل المعلومات وسرعة إعطاء الأوامر العسكرية، الذي ينعكس ايجابا على تحقيق الأهداف العسكرية.

كما تنشأ أهمية هذا البعد من خطورة الهجمات السيبرانية والاختراقات التي تؤدي إلى نشأة الحروب والصراعات المسلحة، واختراقات أنظمة المنشأة النووية، وما قد يحدث عنها من تهديدات لأمن الدول والحكومات ويؤدي إلى الكوارث.

فبالنظر للنظام الدولي الحالي الذي تهيمن عليه الولايات المتحدة الأمريكية كقوى عظمى وحيدة في العالم، يمكن القول أنها لم تعد قادرة على القيادة داخل الفضاء السيبراني رغم ما تمتلكه من مقدرات عسكرية هائلة. فتتعرض الولايات المتحدة الأمريكية إلى هجمات سيبرانية متكررة تمثل تهديدا لأمنها القومي، ففي ظل اهتمام الإدارات الأمريكية المتلاحقة بالتسليح والاهتمام بالتفوق العسكري، كان الأمن السيبراني محل جدلا فيري آدامز أن "التفوق العسكري الساحق والميزة الرائدة في تكنولوجيا المعلومات، جعلت الولايات المتحدة الدولة الأكثر عرضة للهجمات الإلكترونية"، فمن غير المرجح أن تتفوق أية دولة على الولايات المتحدة في القوة العسكرية التقليدية في المستقبل القريب. لذا ستبدأ الدول المعادية في إنفاق الموارد لتطوير أسلحة إلكترونية تمنحها ميزة غير متكافئة، وربما تهزم الولايات المتحدة دون إطلاق طلقة واحدة، مما شكل صعوبة في الوقاية من هذه الهجمات. في 13 ديسمبر 2020 تعرضت ما لا يقل عن 6 وكالات حكومية أمريكية للاختراق بفعل برنامج خبيث أصاب آلاف الشركات فيما يبدو أنها واحدة من أكبر عمليات الاختراق التي تم الكشف عنها، حيث استطاع متسللين النفاذ إلى البريد الإلكتروني الخاص بوزارتي الخزانة، والتجارة الأمريكيتين مما سبب مشاكل كثيرة تخطت حدود الدولة الامريكية ذاتها.

- **الأبعاد السياسية :**

ثمة سبب محتمل آخر ذو طابع سياسي لمثل العمليات الهجومية السيبرانية، فقد يستخدم الجاني العملية السيبرانية في خدمة غرض سياسي معيَّن. فالهجوم السيبراني أو استغلال الفضاء السيبراني قد يُستخدم في إرسال رسالة سياسية إلى أمة، أو تجميع معلومات استخبارات لأغراض سياسية، أو لإقناع طرف آخر أو التأثير عليه ليتصرف على نحو معيَّن، أو لإثناء طرف آخر عن القيام بأفعال معيَّنة . ويطلق عليها بالقرصنة الوطنية patriotic hacking هذا النوع من القرصنة ظهر في العديد من الصراعات الدولية كالصراع الفلسطيني الإسرائيلي، والهندي الباكستاني.

تقوم الأبعاد السياسية للأمن السيبراني على أساس حماية نظام الدولة وكيانها، حيث يمكن أن تستخدم التقنيات في بث معلومات وبيانات قد يحدث من خلالها زعزعة لاستقرار أمن الدول والحكومات حيث تصل بسرعة فائقة إلى شريحة أكبر من المواطنين بغض النظر عن صحة البيانات والمعلومات التي يتم نشرها.

- **الأبعاد الاجتماعية :**

تسمح طبيعة الانترنت المفتوحة بالمواطنين بالتعبير عن تطلعاتهم السياسية وطموحاتهم الاجتماعية، غير أن ذلك يمكن أن يعرضهم إلى السقوط في خطر المواد الاباحية أو الإرهابية ، أو نشر الفكر المتطرف، ومحاولة تجنيد الشباب، كما يعرض الهويات إلى الاختراق خارجي ما يهدد السلم الاجتماعي للدولة، وعليه لابد من التوعية لهده المخاطر السيبرانية في بعدها الاجتماعي.

- **الأبعاد الاقتصادية :**

يرتبط الأمن السيبراني ارتباطا وثيقا بالاقتصاد، فالتلازم واضح بين اقتصاد المعرفة وتوسع استخدام تقنيات المعلومات والاتصالات التي تتيح تعزيز التنمية الاقتصادية لبلدان كثيرة. يضاف إلى ذلك دخول العالم عصر المال الالكتروني ضمن بيئة تقنية متحركة بعد إطلاق خدمات المحفظة الالكترونية، إذ تزداد استثمارات المصارف والمؤسسات المالية في مجال المال الرقمي.يشير تقرير صادر عن شركة Emarkaterإلى أن حجم التجارة الالكترونية بلغ 1.5 ترليون دولار عام 2014، ونظر لارتفاع معدل الجرائم السيبرانية ،فإن ذلك يمثل تهديدا صريحا لنمو الاقتصاد الرقمي مالم تقم الدول بتعظيم معايير الأمن السيبراني ضد هذه الجرائم.

وفي المقابل نجد أن الهجمات السيبرانية في الجرائم الإلكترونية، تؤثر سلبا على المصالح الاقتصادية عبر الممارسات الاحتيالية الالكترونية، وجرائم الاستغلال والسطو، والتخريب الاقتصادي والقرصنة الإلكترونية، وسرقة الأصول الفكرية، وغسل الأموال والجرائم المالية عبر الأنترنت. وفقا للتقرير السنوي الرسمي لجرائم الإنترنت لعام 2019 الصادر عنVentures Cybersecurity، فإن الجرائم الإلكترونية هي أكبر تهديدا لكل شركة وفاعل دولي في العالم، وواحدة من أكبر المشكلات التي تواجه البشرية. فتتوقع مشاريع الأمن السيبراني أن تكلف الجريمة الإلكترونية 6 تريليونات دولار سنوى مع نهاية عام 2021 مقارنة بـ3 تريليونات دولار في عام 2015 العالم.

ناهيلك عن استخدام العملات المشفرة وما تحمله من مخاطر اقتصادية كامنة للدول التي لا تمتلك نظما متقدمة تكنولوجية وأيضا خروج ودخول الأموال دون رقابة البنوك المركزية للدول وغيرها من الأثار السلبية التي قد تظهر جراء التعامل وتداول هذه العملات الرقمية.

- **الأبعاد القانونية :**

إن التطورات التكنولوجية المتسارعة، تفرض مواكبة التشريعات القانونية لها، من خلال وضع أطر وتشريعات للأعمال القانونية وغير القانونية في الفضاء السيبراني، فالملاحظ أن الجريمة السيبرانية تفتقد في معظم البلدان إلى الأطر القانونية الصارمة للتعامل معها، إضافة إلى ضرورة تفعيل التعاون الدولي لمكافحتها.

في الأخير يمكن القول أن الأمن السيبراني هو بعد جديد ضمن أبعاد الأمن القومي ، أحدث تغيرات جوهرية في مفاهيم العلاقات الدولية كالصراع والقوة والتهديد . حيث حتم على فواعل المجتمع الدولي الانتقال من العالم المادي إلى العالم الافتراضي المتشابك والمعقد. وبالتالي أصبح الأمن السيبراني ضرورة حتمية في عالم اليوم، خاصة في ظل ارتباط كافة التفاعلات الدولية بالجانب الرقمي والتكنولوجي، الأمر الذي يستدعي على الدول إيجاد ميكانيزمات ووسائل فعالة لمواجهة المخاطر والتهديدات السيبرانية التي تتميز بالسرعة والغموض والدقة، ومن ثمة تحقيق الأمن السيبراني والحفاظ على مكاسب الدولة وأمنها القومي.

أهم الآليات (الأسلحة) الالكترونية:

تشير الأسلحة الالكترونية إلى تلك الأدوات التي يتم استخدامها للتهديد أو إحداث الضرر المادي أو الوظيفي للأجهزة أو النظم والهياكل الالكترونية ومنها :

1- **الحرمان من الخدمة Denial of Service :** هو ذلك الهجوم الذي يهدف إلى إيقاف قدرة الهدف على تقديم الخدمات المعتادة أو المفترض تقديمها ، وذلك عن طريق إغراق جهاز الحاسب الآلي المقدم للخدمة بكم كبير من الأوامر تؤدي إلى عرقلته أو توقفه عن العمل.

لقد شهدت الساحة الدولية أكبر موجة من هجمات الحرمان من الخدمة عام 2000 والتي نتج عنها ايقاف عدد من المواقع ومنها Yahoo,eBay,CNN,Amazon، دون الإعلان عن مصدر التهديدات أو الأهداف الكامنة وراءها. وفقا لتقرير صادر من مركز التنسيق الخاص بفرق الاستجابة لطوارئ الحاسب الآلي في الولايات المتحدة على أن 2001 شهد أكثر من 13 ألف هجوم من هجمات الحرمان من الخدمة الموزعة على أكثر من 5000 موقع الكتروني مختلف تنتمي لأكثر من 3000 منظمة في مدة لا تتجاوز ثلاثة أسابيع، مما يدل على تصاعد وتيرة هذه الهجمات وحدتها واتساع نطاق تأثيرها. اضافة إلى استخدام هذه الهجمات من روسيا ضد كل استونيا 2007، جورجيا2008 وأوكرانيا 2008 بعد طلب الانضمام إلى حلف شمال الأطلنطي والتي استهدفت الوزارات والمواقع الاخبارية.

2- **البرامج الضارة (الخبيثة) Malware:**

هي تلك البرامج الخبيثة التي تستخدم لإلحاق الضرر بأجهزة الحاسب الآلي ونظم المعلومات المستهدفة من الهجوم الالكتروني، وهناك أنواع عديدة للبرامج الخبيثة ، منها ما هو معلوم، وأخرى غير معلوم للمستخدم منها :

- الفيروسات Viruses : هي برامج حاسوبية خبيثة مضرة بالحواسيب ، وهناك أنواع منها ما يبدأ عمله بوقت أو حادثة معينة، ومنها ما يكون مكونا من أجزاء متعددة، ومنها ما تتغير صفاته بشكل دوري ومنها ما يكون متخفيا عن برامج مكافحة الفيروسات.
- الديدان Warme: تمتاز الديدان عن الفيروسات باعتماديتها على نفسها لتتاكثر وبسرعة الانتقال وصغر الحجم. وهو ما يؤثر على فعالية الحاسوب وشبكة المعلومات.
- الخداع أو البلاغ الكذابHowx : هو بلاغ عن ظهور فيروس يربك به الناس ويضيع به أوقاتهم، وقد يؤثر على الحاسوب.
- روبوت أوبوت Bot: يصيب الحاسب الروبوت غالبا عند زيارة مواقع الويب أو فتح مرفقات البريد الالكتروني أو فتح ملفات وسائط مصابة.
- برامج طلب فدية Ransom ware: عبارة عن نوع من البرامج الضارة التي تمنعك من الخروج من جهازك أو تشفير الملفات الخاصة بك باستخدام مفتاح غير معروف للمستخدم، ثم تفرض عليك فدية لاستعادتها.
- برنامج استغلال الخوف Scare ware: هو برنامج مصمم لارسال رسائل مزورة تفيد بأن النظام في خطر أو يحتاج إلى تنفيذ برنامج معين للعودة إلى التشغيل العادي.
- رسائل اصطياد الخادعة Phishing Scam: هي رسائل الكترونية تبدو وكأنها مرسلة من هيئة حقيقية غالبا ما تكون بنك، لتحديث المعلومات والبيانات الخاصة ليتم استغلالها.

- الأحصنة الطروادة Trojan Horses: هذا النوع من الفيروسات لا يتكاثر كثل الفيروسات و الديدان، ولكن يمكن في النظام بشكل خفي، يحاول استغلال حاسوب لشن هجمات على حواسيب أخرى، أو التجسس عن طريق لوحة المفاتيح والتي يمكن أن تحتوي على بطاقة الائتمان أو كلمة المرور.
- البرامج التجسسية Spyware : هي برامج تراقب سلوكك على جهازك سواء مراقبة كتاباتك أو المواقع التي تزورها بغرض التجسس الخبيث لاستسقاء معلومات سرية ككلمات المرور، أو أرقام الحسابات البنكية، أو لأغراض تجارية مثل معرفة أنماط المستخدم الاستهلاكية، أو المواقع التجارية الأكثر تسوقا.

3- **المر اقبة Monitoring** :تقوم هذه البرامج بمراقبة الهدف وإرسال معلومات عنه وعن الموقع الالكتروني التي يدخل عليها وغيرها من البيانات إلى المهاجم.

4- **سرقة كلمة السر:** والتي يقوم من خلالها سرقة المعلومات من مواقع حساسة كالمواقع البنكية. أو المواقع التجارية.

أشكال التهديدات الالكترونية:

على الرغم من تعدد صور وأشكال الهجمات الالكترونية أو السيبرانية ، غير أنه يمكن تقسيمها إلى أربع مجموعات :

أ- التجسس الالكتروني Cyber espionage: هو القيام باختراق شبكة أو جهاز إلكتروني بهدف سرقة المعلومات الموجودة عليه.ولأن هذه الهجمات تستطيع إحداث خسائر كبيرة في وقت محدود، أصبحت عديد الدول تلجأ إليها، إما من خلال النزاعات السياسية والتوتر السياسي مع الدول الأخرى، وإما وقت الحروب بالتزامن مع العمليات العسكرية التقليدية. من أبرز أمثلة التجسس إدعاءات بأن الصين قامت بالتسلل إلى مؤسسات حكومية في كل من الو م أ و المملكة المتحدة بما في دلك وزارتي الدفاع التابعة لهما، وقد أطلق على هذه الاعتداءات هجمات الأمطار العملاقة التي بدأت في 2002إلى 2007.

ب- الجرائم الاكترونية[1] Cyber crime : وهي الجريمة التي يتم فيها استخدام الآليات والأسلحة الالكترونية السابق عرضها للقيام بهجوم الكتروني بهدف تحقيق مكاسب مالية بالأساس. وتتعدد أشكالها بين سرقة الهوية بغرض الاحتيال، أو الاحتيال عبر الانترنت، أو هجمات الاختراق.....

ت- الارهاب الالكتروني Cyber terrorism : يشير إلى الاعتداءات و التهديدات الموجهة إلى أجهزة الحاسب الآلي والشبكات الإلكترونية والمعلومات الموجودة عليها بهدف إجبار الحكومات و المجتمعات على أفعال معينة لأغراض سياسية أو اجتماعية.

ث- الحرب الالكترونية Cyber war : وهي الحرب التي تتم إدارتها في مجال الفضاء الالكتروني والتي تكون الفواعل الرئيسية فيها هي الدول.وقد تكون هده الحرب جزءا من حرب شاملة في البر والبحر و الجو.

---

[1]- هناك العديد من الجرائم السيبرانية منها:
- جرائم التعدي على البيانات المعلوماتية، جرائم التعدي على الأنظمة المعلوماتية، إساءة استعمال الأجهزة أو البرامج المعلوماتية، الجرائم الالكترونية الواقعة على الأموال،جرائم الاستغلال الجنسي للقاصرات، جرائم التعدي على الملكية الفكرية للأعمال الرقمية، جرائم البطاقات المصرفية والنقود الالكترونية، الجرائم التي تمس المعلومات الشخصية، جرائم العنصرية والجرائم ضد الانسانية بوسائل معلوماتية، جرائم المقامرة الترويج للمواد المخدرة بوسائل معلوماتية عبر الانترنت، الجرائم المعلوماتية ضد الدولة والسلامة العامة، جرائم تشفير المعلومات .

وعلى الرغم من تعدد الصراعات الالكترونية في العصر الحديث ، إلا أن حربا إلكترونية حقيقة لم تحدث بعد.

الكورونا وزيادة معدلات الهجمات السيبر انية

ساهم انتشار فيروس كورونا عالميا في زيادة سرعة تحديث كثير من المجتمعات تكنولوجيا، وزيادة الاعتمادية علي التكنولوجيا في هذا الصدد، ولكن مع زيادة الاعتمادية زادات معها الهجمات السيبرانية. ففي إطار زيادة عدد الأجهزة المرتبطة بشبكة الأنترنت ، مع زيادة المحفزات السياسية والاقتصادية لاستغلال شبكة المعلومات الدولية، خاصة وقت الجائحة تزداد مخاطر الأمن السيبراني والتهديدات المتضمنة بزيادة معدلات الاختراق.

الشكل رقم ٣: إحصائيات عن بعض الهجمات السيبرانية بالعالم خلال جائحة الكورونا

المصدر: Fintech News, The 2020 Cybersecurity stats you need to know, August 20, 2020,

تمثل الولايات المتحدة والصين القوى الرائدة في العالم، حيث حدد التقرير اكثر القوى السيبرانية شمولا على مستوى العالم في عشرة دول، ورغم أنها تخلو من الدول العربية كما هو موضح في الجدول رقم ١ ولكن تحتل كل من السعودية ومصر ايران ، مكانة ضمن القوى السيبرانية المؤثرة في العالم وفقا لمقدرات القوى الوطنية للأمن السيبراني وفقا لعام2020.

الجدول رقم ١: ترتيب القوى السبرانيه العالميه العشرة خلال اعوام ٢٠٢٠ و٢٠١٨ و٢٠١١ وفقا للمؤشر العالمي للقوى السيبرانية القومية

م	القوى السيبرانية العالمية وفقا لمؤشر عام ٢٠٢٠	القوى السيرانية العالمية وفقا لمؤشر لعام ٢٠١٨	القوى السيبرانية العالمية وفقا لمؤشر عام ٢٠١١
١	الولايات المتحدة	المملكة المتحدة	المملكة المتحدة
٢	الصين	الولايات المتحدة	الولايات المتحدة
٣	المملكة المتحدة	فرنسا	استراليا
٤	روسيا	لتوانيا	المانيا
٥	هولندا	استونيا	كندا
٦	فرنسا	سنغافورة	فرنسا
٧	المانيا	اسبانيا	كوريا الجنوبية
٨	كندا	ماليزيا	اليابان
٩	اليابان	كندا	ايطاليا
١٠	استراليا	النرويج	البرازيل

المصدر: Julia Voo, Op.cit (& others)

أسباب الجرائم السيبرانية:

1- الرغبة في جمع المعلومات وتعلمها.
2- الاستيلاء على المعلومات والاتجار فيها.
3- قهر النظام وإثبات التفوق على تطور وسائل التقنية.
4- إلحاق الأذى بأشخاص أو جهات.
5- تحقيق أرباح ومكاسب مادية.
6- تهديد الأمن القومي والعسكري.

الجهود الدولية للتصدي للهجمات السيبرانية

على الرغم من غياب سلطة عليا تنظم التفاعلات بالفضاء السيبراني كما سبق الذكر، ولكن هناك جهود دولية تمت وتتم تستهدف ضبط التفاعلات وسلوك الوحدات الدولية الفاعلة في الفضاء السيبراني في إطار التنظيمات الدولية القائمة ويمكن طرح أبرزها فيما يلي :

- المستوى الأممي: قامت الأمم المتحدة بعدد من الجهود لمأسسة وتنظيم والتصدي للهجمات والجرئم السيبرانية تنوعت بين وضع قواعد موضوعية وإجرائية ومؤتمرات وقمم دولية وجهود لبعض الهيئات والاجهزة التابعة لها، ويمكن طرح ابرز تلك الجهود : وضعت الأمم المتحدة مجموعة من القواعد الموضوعية و إجرائية لمواجهة الجرائم السيبرانية ، ومؤتمرات وقمم دولية كمؤتمرها الثامن المنعقد بهافانا 1990 حول منع الجريمة إلى اصدار قانون خاص بالجرائم المتعلقة بالحاسوب. قامت لجنة الأمم

المتحدة لمنع الجريمة والعدالة الجنائية في أبريل 2010 في دورتها الثانية عشرة بصياغة مجموعة من الإعلانات تضمنت إنشاء فريق خبراء حكومي دولي لبحث مشكلة الجريمة السيبرانية والاستجابات الدولية لها.

- المستوى الإقليمي: أنشأت منظمة حلف شمال الأطلسي (الناتو) هيئة معنية بإدارة الدفاع السيبراني، وفريقا للاستجابة للحوادث الحاسوبية يكفل إرسال فرق الدعم السريع إلى فرادى البلدان الأعضاء، ومركزا للتميز من أجل الدفاع السيبراني التعاوني ويضم هذا المركز الذي يوجد مقره في إستونيا خبراء يضطلعون بالبحث والتدريب في مجال الأمن السيبراني. وتضم إستونيا ولاتفيا وليتوانيا وألمانيا واسبانيا. ايطاليا والجمهورية السلوفاكية

المجلس الأوروبي – اتفاقية بودابست بشأن الجرائم السيبرانية من خلال توفير أحكام قانونية نموذجية يمكن أن تعتمدها البلدان وتكيفها مع احتياجاتها الخاصة.

- المستوى الثنائي :

سعت بعض الدول بشكل ثنائي مع مثيلتها من الدول الأخرى التعاون في مجل الأمن السيبراني كصندوق الصين إسرائيل بين شنغهاي وهونج كونج وتل أبيبGEOC ، تم تأسيسه عام 2013 للاستثمار في شركات التكنولوجيا الثقيلة، في مجالات علوم الحياة والطابعات ثلاثية الأبعاد، الأمن السيبراني، والذكاء الاصطناعي وأنترنت الأشياء.

وانطلاقا مما سبق، على الرغم من الجهود الدولية المبذولة في هذا الشأن لكن على الجماعة الدولية بذل مزيد من الجهد لوضع القواعد والإجراءات الرسمية التي تضبط سلوك الفاعليين الدوليين بالنسق الدولي.

يأتي الاهتمام بالأمن السيبراني مع زيادة الخسائر الناتجه عن الهجمات الإلكترونية وما يعنيه ذلك من تهديدات على الأمن القومي للدول، وبالتبعية على السلم والأمن الدوليين. فمن المتوقع أن تصل الأضرار الناجمة عن جرائم الإنترنت إلى ما يقدر بنحو 10.5 تريليون دولار بحلول عام 2025 وفقا لتقديرEdSurge .

اشكالات التي يثيرها الفضاء السيبر اني

- **اشكالية سيادة الدولة في الفضاء السيبر اني:**

اختلف علماء السياسة حول تأثير الأمن السيبراني على سيادة الدولة، فيرى دانيال لامباش أن الفضاء السيبراني ساهم في تعزيز سيادة الدولة عبر دعم "السيادة الإلكترونية"، أو "السيادة على البيانات"، أو ما يسمى بـ"السيادة الرقمية": أي فرض السيادة الوطنية بالفضاء السيبراني، بمعني تشكيل مناطق ذات سيادة وطنية في الفضاء السيبراني استنادا إلى نظرية الممارسة والمفاهيم المزدوجة لإعادة التوطين، وهو ما يُعرف بـ"الأنطولوجيا الإقليمية"،

عبر طرق ووسائل تمارس من خلالها الجهات الفاعلة (الدول أو غير ذلك) السيطرة على الفضاء السيبراني، كقيام الحكومات بقطع الإنترنت في أوقات الأزمات السياسية، أو التحكم في التعليمات البرمجية والخوارزميات بتقنيات الذكاء الاصطناعي، أو فرض الرقابة الصارمة على المحتوى، وهو ما تفعله تركيا وتايلاند. إضافة إلى اللجوء

للقرصنة الوطنية أو فرض قوانين "توطين البيانات" التي تحظر نقل البيانات عبر الحدود كالحالة الروسية والحالة الصينية، الأمر الذي يدعم إظهار قوة الدولة بشكل منتظم. فهناك العديد من الأدوات المتاحة للدول التي تسعى لإعادة إنشاء أراضيها الوطنية في الفضاء السيبراني، كحجب بروتوكول الإنترنت IP " Protocol "))Internet، والبحث عن الكلمات الرئيسية لمراقبة المناقشات حول الموضوعات الحساسة، ومنع الوصول إلى مواقع الويب التي تعتبر تخريبية. وهو ما تم تطبيقه في العديد من الدول، كالجدار الناري العظيم في الصين، ونظم الرقابة الحكومية الصارمة على الإنترنت في كوريا الشمالية.

- **إشكالية التفوق السيبراني للدول مقابل تهديدها للسلم والأمن الدوليين:**

في إطار ضبابية الفضاء الافتراضي وصعوبة الوقوف على حقائق الإدانة، تدور حول الدول اتهامات بارتكاب أفعال لاختراق السلم والأمن الدوليين بحجة التفوق السيبراني أو الردع الافتراضي، لتحقيق السيادة والنفوذ والأغراض السياسية المحددة والمطروحة. ويمكن رصد السمات السياسية لبعض الهجمات السيبرانية حيث تدور الشبهات حول دول بعينها كاختراق مكتب إدارة شؤون الموظفين في الولايات المتحدة عام 2014 وتم توجيه الاتهامات من قبل الحكومة الأمريكية إلى الصين، والهجوم السيبراني على أوكرانيا عام 2015 وأسفر عن قطع الكهرباء على ربع مليون أوكراني الذي اتهمت خلاله روسيا .فعلى الرغم من سرية وعدم القدرة على إثبات تورط الدول المذكورة في تلك الاعتداءات والجرائم، ولكنها تعكس لجوء الدول للساحة السيبرانية لاستكمال صراعاتها، وبسط نفوذها سواء بالتورط في الهجوم أو حتى بالزعم بتورط الدولة المعادية لها سواء صح الزعم من عدمه.