التهديدات والجرائم السيبرانية:

تأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها.

Cyber Threats and Crime:
Its impact on the national security of countries and strategies to combat it

د. لامية طالة

Talla lamia

كلية علوم الإعلام والاتصال، جامعة الجزائر 3 ، lamia.tll@gmail.com

تاريخ الاستلام: 2020/06/21 تاريخ القبول: 2020/08/24 تاريخ النشر: 2020/12/21

ملخص:

يعد الأمن السيبراني سلاحا استراتيجيا بيد الحكومات والأفراد، لاسيما أن الحرب السيبرانية أصبحت جزءا لا يتجزأ من التكتيكات الحديثة للحروب والهجمات بين الدول .."، ويشمل الأمن السيبراني أمن المعلومات على أجهزة وشبكات الحاسوب الآلي، بما في ذلك العمليات والآليات التي يتم من خلالها حماية معدات الحاسوب الآلي والمعلومات والخدمات من أي تدخل غير مقصود أو غير مصرح به أو تغيير أو إتلاف قد يحدث.

ويمكن اعتبار تحدي الأمن السيبراني أعلى تحديات الأمن القومي في القرن الواحد والعشرين، مع الإشارة إلى أن المفهوم الحديث للأمن لا يقتصر فقط على الجوانب العسكرية، بل يواكب كل التهديدات والتحديات التي يمكن أن تشكل عائقا أمام الاقتصاد الرقمي وتدفق المعرفة، فقد أسقطت تكنولوجيا المعلومات والاتصالات مفهوم الحدود الجغرافية، السياسية والثقافية بين الدول، ما يضع السيادة الوطنية على المحك، خاصة مع اختراق المواقع الحكومية الرسمية والتجسس المعلوماتي على الدول.

كلمات مفتاحية: الأمن السيبراني، الحروب السيبرانية، الجرائم السيبرانية.

Abstract:

Cybersecurity is a strategic weapon in the hands of governments and individuals, especially since cyberwar is now an integral part of modern tactics of war and attacks between nations. Automated information and services may be generated by any unintended or unauthorized interference, alteration or damage.

The cybersecurity challenge can be viewed as the greatest national security challenge of the 21st century. It should be noted that the modern concept of security is not limited to the military aspects, but that it has to deal with all the threats and challenges that can hamper the digital economy and the flow of knowledge. The geographic, political and cultural borders between countries jeopardize national sovereignty, in particular with the penetration of official government websites and information spying on states.

Keywords: cybersecurity, cyberwar, Cybercrimes.

المؤلف المرسل: لامية طالة ، **الإيميل** lamia.tll@gmail.com

مقدمة:

كانت ثورة المعلومات وظهور الانترنيت إيذانا ببزوغ العصر السيبري، وخلق بيئة جديدة هي **الفضاء السيبراني (Cyber space)** هذا الأخير الذي أصبح يؤثر في النظام الدولي، خاصة مع بروز شكل جديد من القوة هي **القوة السيبرانية (Cyberpower)**، التي توزعت وانتشرت بين عدد أكبر من الفاعلين على المستوى الدولي والمحلي، مما جعل الفضاء السيبراني مجالا جديدا للصراع بين الدول.

فقد أدى ظهور الفضاء الإلكتروني واستخداماته إلى تغيير شكل وطبيعة عمل النظام السياسي حيث لعب دور المؤسسات الوسيطة والتواصل ما بين عملية صنع القرار والرأي العام، كما ساعد على نقل النشاط السياسي الداخلي إلى ظاهرة عالمية حيث التواصل بين دول العالم المُختلفة والانفتاح على التطورات الديمقراطية في العالم وزيادة الوعي بحقوق الإنسان عالمياً جعل هناك حالة من حالات تدويل القضايا المحلية سواء بجذب اهتمام الرأي العام الدولي أو الضغط على المؤسسات السياسة الحاكمة من قبل المؤسسات الدولية، أو العمل على النيل من شرعية النظام وسمعته الدولية.

بالمقابل، تزداد المخاطر السيبرانية كلما ازدادت هيمنة تكنولوجيا المعلومات والاتصالات على النسق العام للحياة، فأصبحنا أمام جرائم حقيقية ومتكاملة الأركان، تتم عن طريق شبكة الإنترنت بأشكال مختلفة، كسرقة الأموال، النصب والاحتيال، التخطيط لعمليات إرهابية، ترويج الأخبار المضللة، وكذلك القرصنة باعتبارها الجريمة الأكثر شيوعاً في العالم الرقمي.

وفي هـذا السـياق، فـإن البحـث في قضـايا التهديـدات السـيبرانية والتحـديات الأمنيـة يقتضي الغوص في حيثيات العصر الرقمي الجديد، وتوصيف بيئة هذه التهديدات، حيث أن شبكة الإنترنت تتوفر على أكثر من مليار و 700 مليون موقع إلكتروني مع انتشار واسع لسنة 2018.

واتصالاً بموضوع التهديدات السيبرانية، تشير عدة تقارير وإحصائيات إلى أن 95% من الشـركات الكبرى متعـددة الجنسـيات تعترف بتعرضها للقرصـنة، حيث اتخـذت أكثر من 135 حكومة في العالم إجراءات حازمة تخص العالم الافتراضي والأمن الإلكتروني، خاصة مـع كثرة الاعتـداءات الإلكترونيـة بـين الـدول، ناهيـك عـن تزايـد عمليـات سـرقة الملكيـة الفكريـة وقرصـنة المنشـآت الاقتصـادية والتجاريـة، الجامعـات، المعاهـد البحثيـة، والمؤسسات الإعلامية، علاوة على انتشار شبكات الإرهاب السيبراني التي توفر نقاط التلاقي والتنسيق بين التنظيمات الإرهابية وتبادل المعلومات والخبرات.

وعلى هذا النحو، يمكن اعتبار تحدي الأمن السيبراني أعلى تحديات الأمن القومي في القرن الواحد والعشرين، مع الإشارة إلى أن المفهوم الحديث للأمن لا يقتصر فقط على الجوانب العسكرية، بل يواكب كل التهديدات والتحديات التي يمكن أن تشكل حجر عثرة أمام الاقتصاد الرقمي وتدفق المعرفة، فقد أسقطت تكنولوجيا المعلومات والاتصالات مفهوم الحدود الجغرافية، السياسية والثقافية بين الدول، ما يضع السيادة الوطنية على المحك، خاصة مع اختراق المواقع الحكومية الرسمية والتجسس المعلوماتي على الدول.

وهـو أسـاس مقالنـا الـذي يتمحـور حـول الاسـتخدام السـيئ لهـذا الفضـاء السـيبراني، وخلقه لبيئة مليئة بالمخاطر والتهديدات الخطيرة على الأمن القومي للدول، حيث تغيرت مفاهيم القوة والصراع والحرب، وارتبطت طبيعتها بالفضاء السيبراني.

I. تحولات القوة وظهور القوة السيبرانية:

شـهد العقـد الأخير تطـورات سـريعة في مجـالي الحوسـبة وتكنولوجيـا المعلومـات بمـا أفضى إلى تغييرات بعيدة المدى في كل مجالات الحياة تقريبا، سيما في المجالين العسكري والأمني اللـذين شـهدا تغيرات عديـدة تتعلق بطريقـة القتـال وأسـلوب بنـاء قـوة الجيـوش، ويعزى ذلك جزئيا إلى المستجدات التي طرأت على أنماط التفكير الاستراتيجي.

إن أشكال القوة تتغير بتغير التكنولوجيا، وقد أثر الفضاء الإلكتروني في الأشكال التقليدية القوة، وطرح مفهوما وشت جديدة في القوة الإلكترونية، وقد كان لهذا الشكل الجديد نور في بلورة مفهوم انتشار القوة، وتعدد الفاعلين الممارسين لها سواء من الدول أو من غير الدول، ما هدد الدور التقليدي للدول وقلل من سيادتها على إقليمها.

يعد مفهوم القوة أحد أهم المفاهيم في العلاقات الدولية والمفسر الأساسي الذي يمكن الاعتماد عليه في فهم التفاعلات الدولية والمواقف التي تتخذها الفواعل المختلفة، وتظهر أهميته تلك في فهم الصراعات الدولية وكيفية تجاوب الأطراف فيها بناء على قوتها المادية والمعنوية.

تطور مفهوم القوة وتعددت اتجاهاته على مر التاريخ فيما بين القوة العسكرية والقوة الاقتصادية والقوة على الإقناع والتأثير حتى العصر الحديث ونزوع التكنولوجيا الحديثة وتأثيرها في مفهوم القوة سواء كانت المادية أو المعنوية.

إن التغيير في العالم سمة رئيسية للدول في ظل الفوضى التي تعم النظام الدولي، وامتلاك هذه القوة السياسية، أو الاقتصادية، أو العسكرية ليس هو المقياس الفعلي لنجاح سياسات التأثير في الآخرين، بل إن فن إدارة هذه القوة يمثل العنصر الرئيسي الأخر لنجاح أي سياسة فعلية تأثيرية، وقوة ردع ضد الآخرين، فكما يقول ألفن توفلر Alvin Toffler " المعرفة هي القوة، وأن امتلاك المعرفة هو أساس لامتلاك الثروة والقوة العسكرية"[1].

ترتبط القوة السيبرانية بامتلاك المعرفة التكنولوجية والقدرة على استخدامها، وهي القدرة على استخدام الفضاء الالكتروني والمعلومات للتأثير في الأحداث على النحو الذي يحقق الأهداف المرجوة لاستخدام الوسائل والأدوات الالكترونية.

اعتبرها جوزيف ناي Joseph S. Nye أنها مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحواسيب والمعلومات والشبكات الالكترونية والبنية التحتية المعلوماتية والمهارات البشرية المترية للتعامل مع هذه الوسائل، حيث يرى أن القوة الالكترونية فرضت تحديات على الأطراف الدولية وخاصة الكبرى والتي كانت تحتكر مصادر القوة مثل

[1] ألفن توفلر: تحول السلطة، ترجمة لبني الريدي، الهيئة المصرية العامة للكتاب، مصر، 1995، ص 25.

الولايات المتحدة الأمريكية، وانتقال القوة وانتشارها بين أطراف متعددة سواء كانت دول أو عبر دول يؤدي إلى تهديد أمنها واستقرارها.

وقد حدد " ناي " ثلاثة أنواع من الفاعلين والذين يمتلكون القوة الالكترونية وهم:

✦ **الدولة**: وهي تمتلك القدرة على تنفيذ هجمات الكترونية، وتطوير البنية التحتية وممارسة السلطة ضمن حدودها، وحتى تتمكن الدولة من ممارسة النفوذ داخليا أو خارجيا عبر القوة السيبرانية يجب أن تتوفر على مجموعة عناصر أهمها:

- **وجود بنية تحتية سيبرانية**: تشمل أجهزة الكمبيوتر، وشبكات الاتصالات، والبرمجيات، وقواعد البيانات لمختلف الأنظمة والقطاعات.
- **بنية مؤسسية**: تتولى مهمة ممارسة القوة السيبرانية وتحقيق الأمن السيبراني للدولة.
- **بنية تشريعية**: تكون ضامنة ومحددة لاستعمال القوة السيبرانية.
- **إستراتيجية بأهداف واضحة**: تحدد طرق العمل والأهداف المرجوة.

وحتى تكتمل عناصر القوة السيبرانية لابد للدولة من القيام بتطوير أسلحة في مجال الحرب السيبرانية لاستعمالها سواء في العمليات الهجومية أو من أجل الردع.

✦ **الفاعلون من غير الدول**: وهم قادرون على أحداث اختراقات المواقع الكترونية، واستهداف أنظمة الاتصالات الدفاعية وتنفيذ أعمال إرهابية. وهم لا يمتلكون مقومات الدولة نفسها في الهجومات الافتراضية، ولكنهم يشكلون خطرا كبيرا على البيئة الدولية لقيامهم بالأعمال التخريبية، حيث يمكننا التفصيل أكثر بخصوص الفاعلين من غير الدول كالتالي:

✦ **الشركات متعددة الجنسيات**: تمتلك بعض شركات التكنولوجيا موارد للقوة تفوق قدرة بعض الدول، ولا تنقصها سوى شرعية ممارسة القوة التي مازالت حكرا على الدول، فخوادم شركات مثل: جوجل Google وميكروسوفت Microsoft وفيسبوك Facebook تسمح لها بامتلاك قواعد البيانات العملاقة التي من خلالها تستكشف وتستغل الأسواق، وتؤثر في اقتصاديات الدول وفي ثقافة المجتمعات وتوجهاتها.

✦ **المنظمات الإجرامية**: تقوم هذه المنظمات الإجرامية بعمليات القرصنة السيبرانية، وسرقة المعلومات واختراق الحسابات البنكية وتحويل الأموال، كما توجد

سوق سوداء على الانترنيت المظلم Dark internet لتجارة المخدرات والأسلحة والبشر، حيث تكلف هذه الجرائم السيبرانية مليارات الدولارات سنويا.

✦ **الجماعات الإرهابية**: تعد من أبرز الفواعل الدولية، خاصة بعد أحداث 11 سبتمبر، حيث تستغل الفضاء السيبراني في عمليات التجنيد والتعبئة والدعاية وجمع الأموال والمتطوعين، كما تحاول جمع المعلومات حول الأهداف العسكرية، وكيفية التعامل مع الأسلحة وتدريب المجندين الجدد عن بعد، رغم أنها لم تصل بعد إلى مرحلة القيام بهجوم سيبراني حقيقي على منشآت البنية التحتية للدول.

✦ **الأفراد " القراصنة"**: وهم الذين يملكون معرفة الكترونية ويستطيعون توضيفها، ولكن تصعب ملاحقتهم والكشف عن هويتهم، حيث أصبح الفرد بفضل الفضاء السيبراني فاعلا مؤثرا في العلاقات الدولية، ومن أبرز النماذج ظاهرة الويكيليكس Wikileaks " الذي نجح في نشر ملايين الوثائق السرية للإدارة الأمريكية وقنصلياتها، مما خلق مشاكل دبلوماسية بين الولايات المتحدة الأمريكية وحلفائها[1].

II. علاقة الفضاء السيبراني بالتغييرات في العلاقات الدولية: " الصراع السيبراني أو الحروب السيبرانية":

كشف استخدام الفضاء السيبراني عن حال التعارض الحقيقي أو المتخيل للاحتياجات والقيم والمصالح بين العديد من الجهات سواء كانوا دولا أو أفرادا أو جماعات أو شركات، مما ساعد على بلورة أساليب للصراع الدولي ذات الطابع التقني والتجاري والاقتصادي والعسكري، إلى جانب ظهور طرائق بديلة عن الحرب المباشرة بين الدول أو بين الخصوم عبر شبكات الاتصال والمعلومات.

وبالتالي أصبح الفضاء السيبراني ساحة جديدة للصراع بشكله التقليدي ولكنه ذو طابع سيبراني يعكس النزاعات التي تخوضها الدول أو الفاعلين من غير الدول على خلفيات دينية أو عرقية أو أيديولوجية أو اقتصادية أو سياسية، ويتمدد الصراع السيبراني بداخل شبكات الاتصال والمعلومات متجاوزا الحدود التقليدية وسيادة الدول[2].

---

[11] جوزيف ناي: **مستقبل القوة**، مرجع سابق، ص 57-59 بتصرف.

[2] منى الأشقر جبور: **السيبرانية هاجس العصر**، المركز العربي للبحوث القانونية والقضائية، بيروت، 2017، ص 41.

مفهوم الحرب السيبرانية:

لا يوجد إجماع على تعريف محدد ودقيق لمفهوم الحرب السيبرانية، فيعرفها كل من "ريتشارد كلارك" Richard Clarke و"روبرت كنايك" Robert Knake على أنها: " **أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها** ".

ويعرفها "باولو شاكريان Paulo Shakarian بأنها :" **امتداد للسياسة من خلال الإجراءات المتخذة في الفضاء السيبراني من قبل دول أو فاعلين غير دوليين، حيث تشكل تهديدا خطيرا للأمن القومي** "[1].

يقترح باحثون آخرون أن يتم التركيز- بدلا من ذلك - على أنواع وأشكال النزاع التي تحصل في الفضاء السيبراني، ويحددون مستوياتها كالتالي:

★ **القرصنة السيبرانية**: وتقع في المستوى **الأول**، ومن أمثلته القيام بعمليات قرصنة المواقع من خلال إغراقها بالبيانات الإلكترونية أو بتعطيل الحواسيب الخادمة.

★ **الجريمة السيبرانية والتجسس السيبراني:** ويقعان في المستوى **الثاني والثالث** وغالبا ما يستهدفان الشركات والمؤسسات وفي حالات نادرة بعض المؤسسات الحكومية.

★ **الإرهاب السيبراني**: ويقع في المستوى **الرابع**، ويعبر عن الهجمات غير الشرعية التي ينفذها فاعلون غير حكوميون ضد أجهزة الكمبيوتر والشبكات والمعلومات المخزّنة.

★ **الحرب السيبرانية**: وهي المستوى **الأخطر** للنزاع في الفضاء السيبراني، وتهدف إلى التأثير على الإرادة السياسية للطرف المستهدف وقدرته في عملية صنع القرار، وكذلك التأثير فيما يتعلق بالقيادة العسكرية و/أو توجهات المدنيين في مسرح العمليات الإلكتروني

[1] محمد محارب: حرب في الفضاء الإلكتروني: اتجاهات وتأثيرات على إسرائيل، كلية النجاح، نابلس، 2013، ص 86.

تداعيات الحروب السيبرانية على الأمن القومي:

سببت الحروب السيبرانية جملة من المخاطر والتداعيات على تفاعلات السياسة الدولية، يمكن طرح أبرزها على النحو الآتي:

✦ **تصاعد المخاطر السيبرانية**: خاصة مع قابلية المنشآت الحيوية (مدنية وعسكرية) في الدول للهجوم، الأمر الذي يؤثر في وظائف تلك المنشآت، وبالتالي فإن التحكم في تنفيذ هذا الهجوم يعد أداة سيطرة إستراتيجية.

✦ **تعزيز القوة وانتشارها**: عمل الفضاء السيبراني على إعادة تشكيل قدرة الأطراف المؤثرة، وأدى إلى عملية انتشار القوة بين فاعلين متعددين.

✦ **عسكرة الفضاء السيبراني**: حيث برز في هذا الإطار عدة اتجاهات، مثل التطور في مجال سياسات الدفاع والأمن السيبراني، وتصاعد القدرات في سباق التسلح السيبراني، وتبني سياسات دفاعية سيبرانية لدي الأجهزة المعنية بالدفاع والأمن في الدول، وتزايد الاستثمار في مجال تطوير أدوات الحرب السيبرانية داخل الجيوش الحديثة.

✦ **إدماج الفضاء السيبراني ضمن الأمن القومي للدول**: وذلك عبر تحديث الجيوش، وتشكيل وحدات متخصصة في الحروب السيبرانية، وإقامة هيئات وطنية للأمن والدفاع السيبراني، والقيام بالتدريب، وإجراء المناورات لتعزيز الدفاعات السيبرانية.

✦ **الاستعداد لحروب المستقبل**: حيث تتبنى العديد من الدول إستراتيجية حرب المعلومات باعتبارها حربا للمستقبل، وترى الدول الكبرى أن من يحدد مصير تلك المعركة المستقبلية ليس من يملك القوة فقط، وإنما القادر على شل القوة، والتشويش على المعلومة[1].

مفهوم الأمن القومي قد طرأ عليه الكثير من التعديل والتغيير، على مستوى التهديدات، الفاعلين، والقطاعات، حيث خلق فضاء جديدا للتفاعل، هو الفضاء السيبراني، وبدا واضحا أن الدول تتجه نحو عسكرة الفضاء السيبراني، مما نتج عنه

[1] عادل عبد الصادق: **الحروب السيبرانية : تصاعد القدرات والتحديات للأمن العالمي**، مرجع سابق.

ظهور تهديدات جديدة تتزايد في الحجم والشدة، وتشكل تهديدا خطيرا للأمن القومي، فكلما زاد التشابك، زادت التهديدات السيبرانية، وأثر ذلك على الأمن القومي.

III. مفهوم الأمن السيبراني:

إن اعتماد عالم اليوم على المعلومة حقيقة ثابتة، وهي تفرض اعتمادا أكثر على الأنظمة الالكترونية التي تعالجها، والحديث عن الأمن يستدعي تعريف الخطر، أي التهديد الذي يتعرض له النظام، إضافة إلى نقاط الضعف والثغرات، ومن ثم الإجراءات المفروض اتخاذها، لدفع الخطر، ونتيجة زيادة التهديدات والمخاطر في الفضاء السيبراني التي تواجه الدول ظهر مفهوم الأمن السيبراني.

يعرف الأمن السيبراني بأنه: " **أمن الشبكات والأنظمة المعلوماتية، والبيانات، والمعلومات، والأجهزة المتصلة بالانترنيت، وعليه فهو المجال الذي يتعلق بإجراءات، ومقاييس، ومعايير الحماية المفروض اتخاذها، أو الالتزام بها، لمواجهة التهديدات، ومنع التعديات، أو على الأقل الحد من آثارها** "[1].

يعرف ريتشارد كمرر Richard A.Kemmerer الأمن السيبراني بأنه :" **عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة**".

بينما عرفه إدوارد أمورسو Edward Amorso على أنه: " **وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل والأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها**،.. "[2].

كما يمكن تعريف الأمن السيبراني، انطلاقا من أهدافه، بأنه النشاط الذي يؤمن حماية الموارد البشرية، والمالية، المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار، التي تترتب في حال تحقق المخاطر والتهديدات، علها يتيح إعادة التوسع إلى ما كان عليه، بأسرع وقت ممكن، بحيث لا تتوقف عجلة الإنتاج، وبحيث لا تتحول الأضرار إلى خسائر دائمة.

---

[1] منى الأشقر جبور: **السيبرانية هاجس العصر**، مرجع سابق، ص 25.

[2] ج. رضوان: **الأمن السيبراني: أولوية في استراتيجيات الدفاع**، مجلة الجيش، مؤسسة المنشورات العسكرية، العدد 630، الجزائر، جانفي 2016، ص 40.

فهو النشاط أو العملية، والقدرة، أو نظم المعلومات واتصالات الدولة، حيث تكون المعلومات الواردة فيه محمية من أي دافع من التلف، والاستخدام غير المسرح به أو التعليل، أو الاستغلال.

ومن الناحية العملية الإجرائية يمكن تلخيص الأمن السيبراني على أنه لا يتعدى المفاهيم التالية:

- يتعاون الأمن السيبراني إلى حل كبير من وسائل دفاعية تستخدم لكشف وإحباط المتسللين.
- الأمن السيبراني ينطوي على حماية شبكات الكمبيوتر والمعلومات التي تحتويها من الاختراق ومن الضرر الخبيث أو التعطيل.
- الأمن السيبراني ينطوي على الحل من هجوم المخاطر الخبيثة على البرمجيات وأجهزة الكمبيوتر والشبكات، وهذا يشمل الأدوات المستخدمة للكشف عن اقتحام ووقف الفيروسات، ومنع وصولها، وفرض التوثيق، وتمكين الاتصالات المشفرة.
- الأمن السيبراني هو مجموعة من الأدوات والسياسات والمفاهيم والضمانات الأمنية، والمبادئ التوجيهية، من المخاطر المحدقة بالمعلومات ومعالجتها، والإجراءات، والتدريب، وأفضل الممارسات، وضمان التقنيات التي يمكن استخلاصها لحماية البيئة الإلكترونية وتنظيم أصول الاستخدام[1].

من خلال ما ورد من تعريفات يمكن القول بالأمن السيبراني هو عبارة عن مجموع الوسائل التقنية والتنظيمية والإدارية التي يته استخدامها لمنع الاستخدام غير المصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرار عمل نظم المعلومات وتعزيز حماية سرية البيانات الشخصية وخصوصيتها واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني.

أبعاد الأمن السيبراني:

[1] بارة سمير: **الأمن السيبراني (Cyber Security) في الجزائر: السياسات والمؤسسات**، المجلة الجزائرية للأمن الإنساني، العدد الرابع، جويلية 2017، ص 257-258.

يطـال الأمـن السـيبراني جميـع المسـائل العسـكرية، الاقتصـادية، والاجتماعيـة، والسياسـية، والإنسـانية، بهـدف تحقيـق منظومـة أمـن متكاملـة تعمـل على الحفـاظ على الأمـن القـومي للدولـة من كل التهديـدات السـيبرانية، وعليـه لابـد من توضيح أبعـاد الأمـن السيبراني، التي نوردها كالآتي:

1. **البعد العسكري**: كانت بدايات الانترنت في بيئة عسكرية، بشكل أساسي، لتنتقل فيما بعد إلى الأوساط العلمية والأكاديمية، تمثلت في أبحاث تخدم القدرات العسكرية وتطورها، والانجازات العلمية، التي تسهم في تفوق بلد على آخر، حيث كان التنافس على أشده بين الاتحاد السوفيتي، والولايات المتحدة الأميركية في مجال الوصول إلى الفضاء الخارجي، وتطوير الأسلحة النووية[1].

وتكمن الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء الإلكتروني، بها يسمح بسهولة تبادل المعلومات وتدفقها، وسرعة اتخاذ القرارات العسكرية، ومن ثمة تحقيق الأهداف عن بعد، ومن دون شك فإن عدم استغلال هذه التقنية والتسلح بها، أو تأمينها بشكل جيد عن أي اختراق خارجي، سيؤدي بالضرورة إلى شن هجمات إلكترونية مضادة على شبكات القوات العسكرية، ومن ثم تدمير قواعد البيانات، وما يلحقه من مخاطر.

حيث أنها يمكن أن تشكل كذلك نقطة ضعف، خاصة إذا لم تكن مؤمنة جيدا من الاختراق، الذي قد يؤدي إلى تدمير قواعد البيانات العسكرية، أو قطع الاتصال بين القيادة والوحدات العسكرية، فضلا عن إمكانية التحكم في بعض الأسلحة وخروجها عن السيطرة: طائرات بدون طيار، صواريخ موجهة، أقمار صناعية وغيرها.

2. **البعد الاقتصادي**: لقد أصبح الفضاء الإلكتروني جاذبا لقطاعات المجتمع كافة، وباتت المعرفة محرك الإنتاج والنمو الاقتصادي، كما أيقن الجميع أن مبدأ التركيز على المعلومات والتكنولوجيا يعد عاملا من العوامل الأساسية للنهوض بالاقتصاد، وهو ما دفع بالدول في الآونة الأخيرة إلى زيادة استثماراتها في المعرفة، وأصبحت عصرنة الاقتصاد

[1] منى الأشقر جبور: **الأمن السيبري: التحديات ومستلزمات المواجهة**، اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، القاهرة، 2012، ص 15.

مرتبطة بالتحكم بالاقتصاد الرقمي من طرف مختلف الفاعلين الاقتصاديين والاجتماعيين[1].

كما أن استخدام الكمبيوتر وشبكة الانترنت في تسيير وتطوير الصناعات وتحريك الاقتصاد، ومعالجة كل المعاملات الاقتصادية والمالية وأصبح الكل مترابطا عبر شبكات الكمبيوتر، مما يستدعي الحديث عن أهمية تحقيق الأمن السيبراني في المجال الاقتصادي.

3. **البعد الاجتماعي**: من الضروري تعميم المفهوم الصحيح والسليم للأمن إلى كل المشتركين في الشبكة الدولية للمعلومات، إذ تعتبر من الخطوات الأساسية التي تقوي مستوى الأمن إذا ما صيغت بطريقة واضحة ونفذت بذكاء، ولذلك يعتبر تنظيم الحملات الإعلامية والتثقيف المدني لأجل مجتمع معلومات مسئول من الضرورة بمكان، بحيث تغطي التحديات والمخاطر، وتدابير الأمن والوقائية والرادعة لأجل تثقيف جميع الأفراد السيبرانيين للتعاطي مع عملية الأمن.

وينبغي التشديد على واجب الأمن، والمسؤولية الفردية والتدابير الرادعة وكذلك التداعيات المحتملة في إطار القانون الجنائي التي تترتب على عدم احترام الالتزامات التي يوجبها الأمن، وبصورة أكثر عمومية، فإن من الضروري توفير التثقيف والتدريب على تكنولوجيات المعلومات والاتصال، وليس فقط على الأمن والتدابير الرادعة، إذ يجب للثقافة الأمنية أن تغرس داخل ثقافة تكنولوجيا المعلومات[2].

فحسب آخر إحصائيات يفوق مستخدمي الانترنيت 4 مليارات شخص في العالم، منهم أكثر من 2,6 مليار يستخدمون مواقع التواصل الاجتماعي، مما يجعلها أكبر تجمع للتفاعل البشري، ويفتح الباب واسعا لتبادل الأفكار والخبرات الجيدة، لكن في المقابل يعرض أخلاقيات المجتمع للخطر، نظرا لصعوبة مراقبة محتوى الانترنيت، كما يعرض الهويات لعمليات اختراق خارجي قد تتسبب في تهديد السلم الاجتماعي للدولة، وعليه

[1] محمد مختار: **هل يمكن للدول أن تتجنب مخاطر الهجمات الالكترونية؟**، مجلة اتجاهات الأحداث، العدد 6، مركز المستقبل للأبحاث والتطوير، أبو ظبي، 2015، ص 6.

[2] الاتحاد الأوروبي للاتصالات: **دليل الأمن السيبراني للبلدان النامية**، جنيف، 2009، ص 16-17.

فلابد من العمل على توعية المواطن بهذه المخاطر لتحقيق الأمن السيبراني في بعده الاجتماعي[1].

4. **البعد القانوني:** يترتب على النشاط الفردي والمؤسساتي والحكومي في الفضاء السيبراني، نتائج قانونية، وموجبات تسترعي اهتماما خاصا، لحل النزاعات اللي يمكن أن تنشا عنها، وهو ما يستدعي مواكبة التحولات التي رافقت ظهور مجتمع المعلومات، فظهرت حقوق أخرى، حق النفاذ إلى الشبكة العالمية للمعلومات، وتوسعت بعض المفاهيم، لتشمل أساليب الممارسة الجديدة باستخدام تقنيات المعلومات والاتصالات، كالحق في إنشاء المدونات الالكترونية، والحق في إنشاء التجمعات على الانترنت، والحق في حماية ملكية البرامج المعلوماتية، كما ظهرت موجبات جديدة ذات انعكاسات اقتصادية مثل: موجب الاحتفاظ ببيانات الاتصالات، وموجب الإبلاغ عن مخالفات وجرائم خاصة بالمحتوى، كل هذه التغيرات والتحولات تستوجب وجود ترسانة قانونية تنسجم مع التطورات الحاصلة، إن على مستوى الحقوق، أو على مستوى البيئات والعمليات[2].

ذلك أن 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 الحالات والبلدان أطرا قانونية صارمة للتعامل معها، إضافة إلى ضرورة تفعيل التعاون الدولي المشترك لمكافحتها.

5. **البعد السياسي:** هناك أمثلة كثيرة تدفع نحو الاهتمام بالبعل السياسي للأمن السيبراني، كالتسريبات المختلفة للوثائق الحساسة، التي تؤدي إلى مشكلات عويصة جدا، على المستوى الخارجي والدولي، علما أنه لا ينكر أحد الدور المعالم الشبكات التواصل الاجتماعي على المستوى السياسي: حملات انتخابية، تظاهرات افتراضية، حركات احتجاجية إلكترونية، ... كما يتم استغلال هذه المواقع من طرف العديد من الحكومات لتمرير سياساتها.

[1] محمد مختار: **هل يمكن للدول أن تتجنب مخاطر الهجمات الالكترونية؟**، مرجع سابق، ص 6-7.

[2] منى الأشقر جبور: **الأمن السيبري: التحديات ومستلزمات المواجهة**، مرجع سابق، ص 17.

وفي سياق آخر يجب أن لا نغفل عن استخدام هذه المواقع من طرف الحركات الإرهابية لتجنيد أفرادها وجمع التمويل لعملياتها، وآلية للاتصال بينها كأفراد وكجماعات، وهو ما استوجب على الدول العمل على حماية أمنها من التهديدات والمخاطر التي قد تتعرض لها من خلال شبكة الانترنت[1].

هذا إضافة إلى التسريبات للوثائق الحساسة والاختراقات التي غالبا ما تؤدي إلى أزمات دبلوماسية بين الدول، كما أن الفضاء السيبراني أصبح بيئة خصبة للحملات الانتخابية والدعاية لمختلف الفاعلين الدوليين.

IV. جهود الدول لمواجهة التهديدات السيبرانية:

من خلال التطرق إلى مختلف الجهود الوطنية والدولية من أجل مواجهة التهديدات السيبرانية، سواء في الجانب التقني أو الجانب القانوني.

أولا: الجهود الوطنية لتأمين الفضاء السيبراني:

1. بناء الجيوش السيبرانية: كان للتطور السريع للتكنولوجيا، خاصة الحرب السيبرانية تحديا لمفاهيم الأمن القومي، حيث أصبحت قضية الدفاع عن البنية القومية للمعلومات ذات أهمية قصوى، وعليه سعت معظم الدول إلى تشكيل جيوش سيبرانية ورصدت ميزانيات ضخمة للتطوير في مجال الهجوم والدفاع والحماية[2].

2. تشكيل هيئات وطنية للأمن السيبراني: بما أن التهديدات السيبرانية لا تفرق بين مدني وعسكري، سعت الدول إلى تشكيل هيئات متخصصة في الأمن السيبراني، تكون مهمتها:

- ✦ إعداد الإستراتيجية الوطنية للأمن السيبراني، والإشراف على تنفيذها.
- ✦ وضع السياسات وآليات الحوكمة والإرشادات المتعلقة بالأمن السيبراني وتعميمه.
- ✦ وضع أطر إدارة المخاطر المتعلقة بالأمن السيبراني.
- ✦ وضع أطر الاستجابة للحوادث والاختراقات.
- ✦ وضع السياسات والمعايير الوطنية للتشفير.

---

[1] محمد مختار: هل يمكن للدول أن تتجنب مخاطر الهجمات الالكترونية؟، مرجع سابق، ص 7.

[2] دعاء الجهيني: طريق محتمل لمواجهة تهديدات الفضاء الالكتروني؟، مفاهيم المستقبل، ملحق شهري يصدر مع دورية اتجاهات الأحداث، العدد 6، مركز المستقبل للأبحاث الدراسات المتقدمة، أبو ظبي، 2015، ص 21.

✦ رفع مستوى الوعي بالأمن السيبراني.

كما يحدد الإتحاد الدولي للاتصالات ITU خمسة معايير لتصنيف مستوى الأمن السيبراني للدول وهي كالتالي: معايير تشريعية، تقنية، تنظيمية، بناء القدرات، ومعيار التعاون[1].

3. التشريعات الوطنية للأمن السيبراني:

سنت العديد من دول العالم قوانين لمواجهة التهديدات السيبرانية، بعد أن ظهر جليا مدى سرعة انتشارها وفداحة الخسائر الناتجة عنها، وأجمع أغلب هذه القوانين أن هذه التهديدات ما هي إلا تعدي على الآخرين وعلى الممتلكات العامة والأنظمة بواسطة استخدام التقنية، وخصص جزء كبير من هذه القوانين عقوبات رادعة، وتعتبر المبادرات التشريعية الأمريكية، حول الأمن السيبراني، من أهم المبادرات في العالم التي تعالج مشكلة التهديدات، ذلك أنها ارتبطت مباشرة بمحاربة الإرهاب[2].

هذا إضافة إلى أن معظم الدول الأوروبية والأسيوية، والعربية، وغيرها من دول العالم التي أضافت إلى قانونها الجزائي ملحقا خاصا لمكافحة الجريمة السيبرانية مثل الجزائر.

ثانيا: الجهود الدولية من أجل فضاء سيبراني سلمي:

1. الحد من سباق التسلح السيبراني: يلعب التسليح أهمية إستراتيجية في توازن القوى على المستوى العالمي، في ظل بيئة يسودها الشك وعدم اليقين وقابلية تدمير المصالح الإستراتيجية بسرعة الضوء، وهو ما يحمل خطورة عسكرة الفضاء السيبراني، وبتبني عديد الدول إستراتيجية الحرب السيبرانية كحرب للمستقبل، واعتبار أن النصر في المعركة حليف من يقدر على شل القوة والتشويش على المعلومة.

واتجهت الدول لتعزيز قدراتها السيبرانية سواء في مجال الدفاع والردع أو الهجوم، بالإضافة إلى حماية بنيتها القومية للمعلومات، وذلك من خلال السعي إلى امتلاك التكنولوجيا وأنظمة الحماية، والعمل على تحقيق التفوق التقني[3].

---

[1] الاتحاد الأوروبي للاتصالات: **مؤشر الأمن السيبراني العالمي**، جنيف، 2017، ص 17.

[2] حسن بن أحمد الشهري: **الإرهاب الالكتروني - حرب الشبكات-**، المجلة العربية الدولية للمعلوماتية، 2015، ص 19.

[3] عادل عبد الصادق: **أسلحة الفضاء الالكتروني في ضوء القانون الدولي**، سلسلة أوراق، العدد 23، مكتبة الإسكندرية، 2016، ص 64.

2. **قانون تالين**: نظرا لصعوبة الحد من سباق التسلح السيبراني، من جهة، وقصور القانون الدولي في هذا المجال، نتيجة عدم وجود أي أساس قانوني ينظم اللجوء إلى الحروب السيبرانية، من جهة أخرى، تم إبرام صك قانوني عام 2013 يدعى **دليل تالين Tallinn manual**، الذي أعده مجموعة من خبراء القانون الدولي بدعوة من حلف شمال الأطلسي" **الناتو NATO**"، قصد دراسة مدى إمكانية تطبيق قواعد القانون الدولي الإنساني على الحروب السيبرانية[1].

ويجيب دليل تالين" على أهم النقاط الحساسة ذات الصلة بالحروب والهجمات السيبرانية التي تنفذها الدول، أو تلك التي تقوم بها جهات فاعلة من دون الدول، كمفهوم النزاع المسلح في إطار الحرب السيبرانية، وكذا مفهوم الجيوش السيبرانية، وكيفية إدارة الحرب السيبرانية من خلال قواعد الاشتباك السيبراني، وصفة المقاتل السيبراني، إضافة إلى إمكانية مراعاة القانون الدولي الإنساني المعروفة كمبدأ التمييز، ومدى شرعية استهداف المقاتل السيبراني بالوسائل العسكرية المادية كالطائرات العسكرية بدون طيار[2].

3. **الاتفاقيات الإقليمية والدولية لأمن الفضاء السيبراني:** تعتبر اتفاقية بودابست 2001 (الاتفاقية الأوروبية لمكافحة الجريمة السيبرانية)، خطوة رائدة على مستوى التعاون بين الدول، وهي الوحيدة من حيث المدى وحجم الدول المنضمة إليها، دخلت حيز التنفيذ عام 2004، وتعتبر أداة إقليمية ملزمة لمكافحة الجريمة السيبرانية، عبر تحقيق الانسجام بين القوانين الوطنية، وقد شددت على ضرورة تحسين تقنيات التحقيق والبحث، وزيادة التعاون بين الدول.

أما على المستوى الدولي، فقد لعبت هيئة الأمم المتحدة عبر القرارات الصادرة عنها التي تدعم الأمن والسلامة في الفضاء السيبراني، وتوعية الوعي العالمي بالأمن السيبراني دورا في جذب انتباه الدول الأعضاء إلى أهمية التحديات السيبرانية، كما بذلت جهود عدة، من

[1] سعيد درويش: **ماهية الحرب الالكترونية في ضوء قواعد القانون الدولي**، حوليات جامعة الجزائر 1، العدد 29، الجزء الثاني، ص 119.

[2] سعيد درويش: **ماهية الحرب الالكترونية في ضوء قواعد القانون الدول**، مرجع سابق، ص 131.

قبل مجموعات عمل متخصصة، بدعم من الاتحاد الدولي للاتصالات، لإقرار مجموعة من المعايير والقواعد، التي تضمن الاستخدام السلمي المجال السيبراني[1].

لكن تبقى هذه الجهود، والمقررات والتوصيات، بالرغم من قيمتها على المستوى الدولي، غير كافية ولا فاعلة، نظرا لعدم الزاميتها القانونية، ولعدم إتاحتها إمكانية العقاب، هذا عدا عن الهوة الرقمية بين الدول، التي تزرع الشك بدل الثقة، خاصة مع سيطرة الولايات المتحدة الأمريكية على الانترنيت.

في الأخير نخلص إلى أن الأمن السيبراني أصبح قضية بالغة الأهمية من قضايا الأمن القومي، حيث قامت معظم الدول بتطوير عقيدتها الأمنية لتتلاءم مع المتغير الجديد، وهذا في محاولة لمواجهة التهديدات السيبرانية التي تزداد وتتطور بسرعة رهيبة.

خاتمة:

مع تطور المجتمعات والثورة التكنولوجية الهائلة في المعلومات والاتصال، والتوجه نحو مجتمع المعلومات والمعرفة، تشكل فضاء جديد هو الفضاء السيبراني، هذا الفضاء الذي يستعمله الأفراد كما الدول، أحدث تغييرات جذرية في مفاهيم العلاقات الدولية كمفهوم القوة والصراع والحرب، حيث تغيرت القوة وانتشرت بين الفاعلين، وتحول الصراع إلى صراع سيبراني، وعليه دعت الحاجة إلى تطوير مفهوم الأمن لمواجهة التهديدات الجديدة، حيث جاء مفهوم الأمن السيبراني كرد فعل على هذه التهديدات، التي مست جميع مجالات الحياة، خاصة مع اتجاه الدول لإنشاء قواعد البيانات القومية، وتطوير شبكات الاتصال، والاعتماد على شبكة الانترنت كبيئة أساسية للعمل، ما يعني أن التعرض للمخاطر السيبرانية يعني تعريض الأمن القومي لمخاطر كبيرة قد تهدد استقرار الدولة وتماسكها.

في كل يوم، المزيد من المستخدمين يتشاركون المزيد من البيانات على المزيد من الأجهزة، هذا الترابط والتفاعل في الفضاء السيبراني يتزايد يوما بعد يوم، وتتزايد معه المخاطر والتهديدات، هذه التهديدات التي تنوعت في الأشكال، والخطورة، بدأت بجرائم سيبرانية يقوم بها أفراد ومنظمات إجرامية كالاختراق والتجسس وسرقة الأموال، وتطورت إلى تخويف وابتزاز المجتمعات وإرهابهم عن طريق الانترنيت، لتصل إلى أخطر أنواع الصراع

[1] منى الأشقر جبور: **السيبرانية هاجس العصر**، مرجع سابق، ص 104.

بين الدول وتهديد أمنها القومي، حيث ظهر جليا عسكرة الفضاء السيبراني، واستعمال الأسلحة السيبرانية عالية التأثير في شن حروب سيبرانية مدمرة.

وحيث أن الفضاء السيبراني أصبح ساحة هامة للتفاعلات الدولية المختلفة، في ظل زيادة الهجمات السيبرانية بين الدول، بما يؤثر على أمنها القومي، سعت الدول فرادى ومجتمعة إلى بذل الجهد من أجل تطوير قدراتها، واتخاذ الإجراءات الوقائية الكافية لحمايتها من أي هجمات سيبرانية محتملة، فقامت بتشكيل وحدات الاستجابة لطوارئ الانترنيت، والهيئات الوطنية للأمن السيبراني، كما شكلت جيوشا سيبرانية لتقوم بمهمات الدفاع والهجوم والحماية، هذا في الجانب التقني، أما في الجانب القانوني، فطورت من منظومتها القانونية لتتلاءم مع التهديدات الجديدة، وبما أن الفضاء السيبراني، لا يعترف بالزمان والجغرافيا، بذلت الدول مساعي إقليميا ودوليا، لوضع أطر قانونية واتفاقيات دولية للفضاء السيبراني، وجعله أكثر أمنا.

وفي الأخير بما أنه لم يتحقق الأمن المثالي في العالم المادي، فلن يتحقق أمن مثالي في الفضاء السيبراني، لذلك فالهدف المرجو هو تقليل المخاطر إلى مستوى مقبول، يمكن معه الاستمرار في النمو والتقدم.