ASJP
Algerian Scientific Journal Platform

مجلة افاق للعلوم
Issn: 2507-7228 – Eissn: 2602-5345
https://www.asjp.cerist.dz/en/PresentationRevue/351



المجلد:09 العدد: 03(2024) ص 621-631

الفضاء السيبراني ، فواعل وتهديدات

Cyberspace, actors and threats

بلفرد لطفي لمين*
جامعة الجزائر 03 (الجزائر)
Altobes1234@gmail.com

د. امحند برقوق
جامعة الجزائر 03 (الجزائر)
berkouk1@ yahoo.com

معلومات المقال

تاريخ الارسال:
30 افريل 2024

تاريخ القبول:
08 جوان 2024

الكلمات المفتاحية:
- ✓ الفضاء السيبراني
- ✓ الفواعل السيبرانية
- ✓ التهديدات السيبرانية

الملخص:

غالبا ما أثارت مسألة الفضاء السيبراني نقاشا واسعا في أوساط المحللين والخبراء ومحترفي مجال الأمن السيبراني، الذين إستقروا إجماعا على بعده الأمني، بالنظر إلى طبيعته التي تضفي له صفة الفضائية (La spacialité) على غرار المجال البري والبحري والجوي والفضائي، مُشكلا بذلك مضمارا أفرزته تكنولوجيات الإعلام والاتصال والإلكترونيات الدقيقة والمعلوماتية من خلال الربط البيني لشبكات الحواسيب ومعدات مختلفة على غرار تجهيزات التوجيه والألياف البصرية بما أتاح تدفق المعلومات وتبادلها بسرعة فائقة بفضل دمج الهاتفية (Téléphonie) والإعلام الآلي وتقنيات السمعي البصري. ولعل البعد الأمني لهذا الفضاء وتعدد فواعله جعل من مسألة التهديدات السيبرانية، لاسيما الهجمات الإلكترونية، محورا أساسيا يتعيّن على الدول إدراجها ضمن أجنداتها الإستراتيجية لضمان حماية منشآتها الرقمية وبياناتها صونا للأمن الوطني.

Article info

Received
April 30;2024
Accepted
June 08; 2024

Keywords:
- ✓ *Cyberspace*
- ✓ *Cyber Actors*
- ✓ *Cyber Threats*

Abstract :

The issue of cyberspace has often given rise to a wide-ranging debate among analysts, experts and cybersecurity professionals, who have unanimously agreed on its security dimension, given its spatial nature, similar to the terrestrial, maritime, air and space domains, thus forming an arena created by the emergence of information and communication technologies, microelectronics and computing through the interconnection of computer networks and various equipment, such as routing equipment and optical fibers, enabling the circulation and exchange of information at high speed thanks to the integration of telephony and audiovisual technologies. The security dimension of this area and the multiplicity of actors involved have made the issue of cyberthreats, particularly cyberattacks, a key one that countries need to incorporate into their strategic agendas to ensure the protection of their digital infrastructures and data in order to safeguard national security

* المؤلف المرسل

Attribution - Pas d'Utilisation Commerciale - Pas de Modification 4.0 International (CC BY-NC-ND 4.0)

1. مقدمة

لقد برز الفضاء السيبراني كمجال للتفاعلات الدولية بما أتاح توظيفه في مجالات متعددة ذات طبيعة مدنية وأخرى عسكرية، ومسرح للنشاط الإجرامي وميدان للحروب تُشن فيها هجمات سبرانية وإنتهاكات تطال الرصيد الرقمي للدول، ولعل المتتبع للشأن الأمني في المشهد السيبراني الدولي يستخلص هيمنة الهجمات السيبرانية في سُلم التهديدات في الفضاء السيبراني، لاسيما من خلال رصد آخر حالة بتاريخ 28 أفريل 2024، إستهلت بسلسلة هجمات إستهدفت الشبكات في جميع أنحاء العالم[1] حيث سُجلت محاولات الوصل بدءا من تاريخ 18 مارس 2024 لإشباع الخوادم (Serveurs) وفق ما أدلت به شركة سيسكو (CISCO)[2] الأمريكية المختصة في الأمن السيبراني الموطنة في كاليفورنيا.

ولعل التحليل الإستدلالي الرجعي لمسار التهديدات السيبرانية يؤكد طابع خطورة "الهجمات الإلكترونية" على إختلاف أنواعها وصولا إلى درجة تأثيرها على البرنامج النووي للدول، على غرار السلاح الحاسوبي الأمريكي الموسوم "ستوكس نات" (Stuxnet) ضد برنامج إيران للأسلحة النووية والذي تم اكتشافه في جوان 2010، من قبل شركة بيلاروسية متخصصة في منتجات أمن تكنولوجيا المعلومات VirusBlokAda، إذ كشفت السلطات الإيرانية بعد ذلك أنها كانت ضحية هجوم على منشآتها النووية، التي تضررت جراء تدمير ألف جهاز طرد مركزي في موقع تخصيب اليورانيوم بمفاعلها النووي بمدينة ناتنز. ووفقًا لبعض المصادر، أدى هذا الهجوم إلى تأخير البرنامج النووي العسكري الإيراني من ستة أشهر إلى عامين، حيث وُصف الفيروس "ستوكس نات" بأنه "السلاح السيبراني الأكثر تطورًا على الإطلاق أو "سلاح دمار شامل إلكتروني"[3].

إنطلاقا مما سبق نطرح الإشكالية التالية: ما ماهية الفضاء السيبراني في ظل التهديدات التي يفرضها فواعل متعددي الخلفيات في ذات الفضاء؟

المحور الأول/ الفضاء السيبراني وفواعله

الفضاء السيبراني

الأصول التاريخية للفضاء السيبراني

يعتبر مصطلح "الفضاء السيبراني" حديث النشأة وهو ترجمة لنظيره الإنكليزي (Cyberspace) الذي يتكون من دمج بادئة Cyber المستمدة من كلمة Cybernétique التي وُظفت لأول مرة في سنة 1948 من طرف عالم الرياضيات نوربيرت فيينر (Norbert Wiener) و كلمة Space اللتين تعنيان تباعا "التحكم السيبراني" والفضاء.

وبالرجوع إلى المصادر العلمية فإنّ هذا العالم الرياضي، وظف مصطلح Cybernétique خلال دراسته لموضوع القيادة و الإتصال في عالم الحيوانات، وبخصوص أصل بادئة سايبر Cyber فإنّ معاجم اللغة تفيد بأنّ أصلها يوناني، ترجع إلى مصطلح (kybernetes) الذي ورد بداية في مؤلفات الخيال العلمي وتعني القيادة أو التحكم عن بعد[4]، كما أنّ قاموس "المورد" يرى أنّ السايبر من السيبرانية التي يعرفها بأنها علم الضبط من المصدر اليوناني Cybernetics [5]، وهو مصدر يتماشى وسياق مفهوم الهجمات السيبرانية، أي ضبط والتحكم في الأشياء عن بعد و السيطرة عليها، كما أكده معجم الأمن المعلوماتي، إذ يعتبر السيطرة على المواقع الإلكترونية لأهداف سلبية عن بعد تحاكي بروتوكول تفعيل الهجمة السيبرانية [6].

التعريف (التعريفات) :

إن تعدد دلالات "الفضاء السيبراني" (Polysémie) أدى إلى ظهور عدة محاولات لتعريفه، حيث يرى الخبير الفرنسي Bertrand Boyer بأنّه " فضاء اتصالات يتكون من الترابط العالمي لمعدات المعالجة الآلية للبيانات الرقمية"[7].

ووفقًا للمفهوم الفرنسي للدفاع السيبراني، فإن الفضاء

Attribution - Pas d'Utilisation Commerciale - Pas de Modification 4.0 International (CC BY-NC-ND 4.0)

السيبراني هو "مجال عالمي يتكون من شبكة مترابطة من البنى التحتية لتكنولوجيا المعلومات، بما في ذلك الإنترنت وشبكات الاتصالات السلكية واللاسلكية وأنظمة الحاسوب والعمليات وآليات التحكم المتكاملة. ويشمل المعلومات الرقمية المنقولة، وكذلك أنظمة توفير الخدمات عبر الإنترنت"[8].

وحسب المفهوم الأمريكي فإنّ الفضاء السيبراني هو: "مجال عالمي ضمن بيئة المعلومات، ويتألف من شبكات مترابطة من البنى التحتية المترابطة وتكنولوجيات المعلومات، بما في ذلك الإنترنت، وشبكات الاتصالات السلكية واللاسلكية، وأنظمة الحاسوب، والعمليات المدمجة، وأجهزة التحكم".

وبعيداً عن الطابع التقني الغالب في هذه التعريفات، يمكننا تصور تعريف للفضاء السيبراني على أنّه "شبكة عالمية تربط فعلياً بين الأنشطة البشرية من خلال الترابط بين الحواسيب وتتيح تداول المعلومات وتبادلها بسرعة.

ولقد عرفت الوكالة الفرنسية لأمن أنظمة المعلومات ANSSI (Agence Nationale de Sécurité des Systèmes d'Information) الفضاء السيبراني على أنّه "فضاء التواصل الناتج عن الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات المرقمنة" [9].

ولا يجب الخلط بين الأنترنت والفضاء السيبراني، فالأنترنت يعبر عن نظام عالمي من شبكات الحواسيب، يتألف من مجموعة من الشبكات الوطنية والإقليمية والخاصة، أي أنه شبكة من الشبكات، ويشكل جزءاً فقط من الفضاء السيبراني.

أ-3. تكوين الفضاء السيبراني :

الفضاء السيبراني هو فضاء معقد، يدمج بين مكونات مادية ملموسة وعناصر لامادية، تتفاعل في ترابط تام؛ فهو مكون من ثلاث طبقات متميزة وهي الأجهزة والبرمجيات والطبقات البشرية. والمكونات المادية هي الحواسيب وأجهزتها الطرفية ولواحقها المرتبطة ببعضها البعض بواسطة أنظمة اتصالات مختلفة (الألياف البصرية والكابلات والأقمار الصناعية.....إلخ)، ويتم التحكم فيها وإدارتها بواسطة برامج حاسوبية مناسبة (برمجيات) مصممة من قبل الموارد البشرية المختصة. ولعل الإستقراء المتقاطع لمختلف تعريفات الفضاء السيبراني يؤدي بنا إلى إستنتاج أيلولتها إلى تحديد بنيوي موضوعي للفضاء السيبراني، بتركيبة تتشكل من ثلاث طبقات أساسية، وهي:

الطبقة المادية: وتتمثل في البنية التحتية لشبكات الحاسوب، بما في ذلك الأنترنت (الخوادم، والألياف البصرية، والكابلات البحرية، وأقمار البث والإرسال، وأجهزة المودم، وأجهزة التوجيه، وغيرها).

الطبقة المنطقية: وتشمل أنظمة تشغيل الكمبيوترات، وبروتوكولات الاتصال بالشبكة بروتوكولات الاتصالات، وحزم البرمجيات المختلفة اللازمة لإدارة الشبكات، .....إلخ.

الطبقة الدلالية أو الإعلامية: تتكون من جميع البيانات والمعلومات والمحتوى المتداول داخل الشبكة أو المخزنة على وسائط/ذاكرة الحاسوب.

ب/ الفواعل في الفضاء السيبراني

ينظر إلى الفضاء السيبراني على أنّه مسرح للتفاعل بين مختلف الفواعل. وهناك عدة طرق لتصنيف الفواعل أو ما يسمى ب "اللاعبين" في الفضاء السيبراني.

تصنف المقاربة الكرونولوجية الفواعل حسب درجة استحواذهم على الفضاء السيبراني. هذا النهج يجعل من الممكن التمييز بين ثلاث فئات من أصحاب المصلحة:

- اللاعبون الكلاسيكيون: وهم اللاعبون التاريخيون في تحليل العلاقات الدولية. هؤلاء اللاعبون يُفعّلون العنف المشروع وينظمون الأقاليم وينتجون المعايير. وفي الواقع، هؤلاء اللاعبون الكلاسيكيون هم المنظمات الدولية وفوق الوطنية وكذلك الدول نفسها. وينظر إلى الفضاء السيبراني على أنه مصدر "مخاطر" و "تهديدات".
- اللاعبون المتحولون: وهم اللاعبون التقليديون الذين تغيرت طبيعتهم نتيجة الثورة الرقمية. ويمكنهم التفاعل في هذا الفضاء الجديد. وتشمل هذه الفئة "المجموعات

AFAK for Sciences Journal مجلة آفاق للعلوم EISSN: 2602-5345 ISSN: 2507-7228

Attribution - Pas d'Utilisation Commerciale - Pas de Modification 4.0 International (CC BY-NC-ND 4.0)

الصناعية الكبرى"، والعصابات الإجرامية، والمجموعات الصحفية الرئيسية، وما إلى ذلك، وجميعهم يتقنون أدوات الاتصال الجديدة، ويعتبرون الفضاء السيبراني مكسبا بالنسبة للاعبين المتحولين.

□ اللاعبون البارزون: هم الكيانات التي تتمتع حاليًا بثقل كبير على الساحة الدولية، والتي تهز المعايير السياسية والنماذج الاقتصادية. فعلى سبيل المثال، لدى "أمازون" و"جوجل" نماذج ضريبية لا تتكيف مع المعايير الضريبية التقليدية، وتعتبر هذه الفئة الفضاء السيبراني "مجال حيوي" بالنسبة لها.

وفي التحليل التقليدي، يتم تصنيف المجموعات البشرية وفقًا للدولة أو الدين أو الوضع الإجتماعي. ومن خلال تنظيمها بهذه الطريقة، تقدم الجهات الفاعلة في الجغرافيا السياسية للفضاء السيبراني تحليلاً جديداً للتغيرات المعقدة في التوليفات البينية. وفي هذا السياق، يرى الخبير Olivier KEMPF أنّه يمكن تصنيف الفواعل السيبرانيين على النحو التالي:

❖ **الفواعل الأفراد**

يعتبر الفرد عنصرًا محوريًا في الفضاء السيبراني، بما يجعله فاعلا استراتيجيًا. وهكذا يتبنى الفرد عدة مواقف متزامنة ومتعددة، يرد وصفها أدناه:

- **مستخدم الأنترنت:** من الواضح أن أول مظهر وظيفي للفرد في الفضاء السيبراني هو أنه مستخدم للأنترنت، وبالتالي فهو مستخدم لشبكات الحاسوب، سواء كانت مرتبطة بالإنترنت أو منفصلة عنها، مثل شبكة مصرفية[10].
- **المواطن:** كما في المقاربة الكلاسيكية، يعتبر كل فرد "مواطناً" في دولته، ويمكنه المساهمة في النقاش العام و عليه فيحق لكل مستعمل أنترنت المساهمة بشكل متماثل، في الفضاء السيبراني، إذ يعتبر هذا الأخير فضاء متاح للتعبير الديمقراطي، حيث يمكن للمواطن، على عكس طبيعته الغالبة كـ "مستقبِل"، أن يتدخل بانتظام في النقاش العام.
- **المحتال:** يمكن لمستخدم الإنترنت أن يكون نصابا أو محتالاً. فالنصب هو فعل متعمد وغير مشروع يرتكب بإستخدام الحواسيب والاتصالات السلكية واللاسلكية للحصول على مزايا غير مستحقة، عادة ما تكون مالية.
- **المستهلك:** أدت التطورات التي طرأت على وسائل الإعلام والاتصال إلى زيادة كبيرة في عدد نقاط الاتصال مع المستهلك، مما سهّل في المعاملات التجارية وأدى إلى تغيير عادات المستهلك التقليدية.
- المتبني غير المؤهل (Script Kiddie): وهو شخص غير مؤهل يستخدم نصوصًا أو برامج أو برمجيات طورها مصممون آخرون لمهاجمة أنظمة وشبكات الحاسوب وتقويض المواقع الإلكترونية.

❖ **الفواعل الجماعية:** هي مجموعات تضم عدد من الأفراد، بهدف الحصول على منافع مشتركة.

✓ **الشركات:** إنّ كثافة الاتصالات عبر الشبكات المختلفة التي تشكل الفضاء السيبراني، والتي تمثل الأنترنت الجزء الرئيسي منها وتحدياً حقيقياً للشركات التجارية. ومع ذلك، فإن الفضاء السيبراني هو مجال جديد يتعيّن إدراجه ضمن ورقة طريق الشركات في إعداد إستراتيجياتها لاسيما وأنه مصدرا للفرص ومكمنا للتهديدات.

✓ **وسائل الإعلام:** منذ ظهور الفضاء السيبراني، شهدت وسائل الإعلام تغيراً جذرياً. وهناك الآن تقاطع واسع بين تكنولوجيا المعلومات والاتصالات ووسائل الإعلام. فقد أصبحت وسائل الإعلام القديمة مثل الصحافة المكتوبة (الصحف الورقية) والملصقات وغيرها والتلفزيون مدعومة الآن بشكل متزايد ببرمجيات تتيح رقمنتها ومعالجتها وتوزيعها بشكل فوري تقريباً على جمهور واسع (مثل النشر على الإنترنت).

✓ **الجماعات الإجرامية:** أتاحت الرقمنة فرصا ذهبية للجماعات الإجرامية ومكنتها من تطوير أدواتها على نحو أكثر، حيث حوّل المجرمون نشاطهم إلى الفضاء السيبراني وطوروا خططهم التكتيكية لاسيما بفضل الأنترنت المظلم

Attribution - Pas d'Utilisation Commerciale - Pas de Modification 4.0 International (CC BY-NC-ND 4.0)

الذي يضمن لهم التكتم الهوياتي لمستعمليه وتطور العملة الرقمية التي قوضت نسق تقفي الحركات المالية.

✓ **الإرهابيون:** لقد طور الإرهابيون العديد من الطرق لإستخدام الفضاء السيبراني لأغراض غير مشروعة، ولكن هذا الإتجاه يوفر أيضاً فرصاً لجمع المعلومات الإستخباراتية وغيرها من الأنشطة لمنع ومكافحة الأعمال الإرهابية. فالإرهابيون لا يستخدمون الفضاء السيبراني للتخطيط لأعمالهم وتمويلها فحسب بل يستخدمونه أيضاً لتجنيد وتدريب أعضاء جدد، والتواصل، والبحث عن أهداف محتملة أو تحديدها، ونشر الدعاية وتحريض الآخرين على ارتكاب أعمال إرهابية[11] .

✓ **النشطاء القراصنة:** الناشطون في مجال القرصنة هم الأشخاص الذين يدافعون عن إلتزام أيديولوجي يؤيد ويفضل العمل المباشر عبر الإنترنت. ويمكن تعريف ناشطية القرصنة على أنها استخدام مكثف ومستمر للفضاء السيبراني، بشكل قانوني أو غير قانوني، كوسيلة للإحتجاج العام أو للترويج لأيدولوجية معبر عنها أو أجندة سياسية.

✓ **القراصنة:** القراصنة هم أشخاص لديهم معرفة وفهم عميقين لتكنولوجيا الكمبيوتر وكيفية تفاعل الأجهزة والبرمجيات والشبكات. والجدير بالذكر إختلاف القراصنة حسب النوايا التي تحدوهم، فالبعض يتيحون إمكانياتهم لهدف نبيل، كما أنّ نبل أهدافهم لا يعني حتما قانونية أساليبهم، إذ نجد ثلاثة أنواع من القراصنة:

o **القراصنة أصحاب القبعة البيضاء:** لا يغامرون في الأعمال غير القانونية. يناقشون تقنيات اختراق الحاسوب والبرمجة والقرصنة. يعتبرون أنفسهم متحمسين لأمن الكمبيوتر ويريدون مشاركة معرفتهم مع معارفهم. إذا اكتشف ثغرة ما، فإنه لن يكشف عنها علناً، لكنه سيشاركها، غالباً دون مقابل، مع المتخصصين في هذا المجال الذين سيتمكنون من سدها.

o **القراصنة أصحاب القبعة الرمادية:** يناقشون ويختبرون الأساليب الإجرامية. دون تدمير أي شيء، يكتفون بمجرد الولوج إلى أنظمة الكمبيوتر على نحو غير شرعي. وفي حالة إكتشافهم لثغرة أو إستحوذوا على برنامج خبيث أو تمكنوا من "اختراق" برنامج ما، فإنهم سيجعلون اكتشافهم متاحاً للجميع دون الإكتراث بشأن سوء الإستخدام أو تحويل الأمر إلى مناورات خبيثة من طرف جهات إجرامية ناهيك عن المقتضيات القانونية التي قد تحكم هذه الممارسة بما ينجر عنها من تداعيات. كما أن هؤلاء القراصنة لا يكترثون لأدبياتهم والأخلاقيات بقدر ما يهمهم بيع "إكتشافاتهم" و ""كفاءاتهم" "لمن يدفع أكثر".

o **القراصنة أصحاب القبعة السوداء:** تخترق هذه الفئة دوما القانون وتستخدم مهاراتها لإلحاق الضرر وتشكل تهديداً حقيقياً. فهؤلاء يخترقون أنظمة الكمبيوتر في محاولة للإضرار بمالكيها والمساس بسلامة بياناتها أو سرقتها.

□ الجهات الفاعلة التابعة للدولة:

تبقى الدولة هي الثابت الرئيسي في التسلسل الهرمي للفواعل المتدخلة في الفضاء السيبراني، ويتمثل دورها في هذا الفضاء الجديد في تنظيم وتقنين وتأمين وإدارة المنشآت الحساسة التي تتيح الوصول إلى الفضاء السيبراني. وإذا إعتبرنا أيضًا الخصائص المكونة للدولة ذات السيادة وفقًا للمبادئ المعترف بها في اتفاقية مونتي فيديو المؤرخة في 26 ديسمبر 1933، وهي وجود إقليم محدد ومعروف، وجود سكان مقيمين به، وجود حد أدنى من أشكال الحكم بالإضافة إلى القدرة على إبرام علاقات مع دول أخرى، نلاحظ أن المفهوم الكلاسيكي للدولة يشهد تحولاً مع تطور الفضاء السيبراني، وفي الواقع فإن هذا التحول يقوم على المبادئ التالية:

o **اندثار الجانب الجغرافي المحدود:** إن اعتبار الدولة كمساحة جغرافية تخضع لمسألة الحدود أصبح ضربا من الخيال، بعد إنصهار الحدود البرية بين الدول في هذا الفضاء السيبراني.

o **تقويض سلطة الدولة وسيادتها:** إن مبدأ بسط سيادة الدولة وتكريس سلطتها قد يكون محل تقويض في الفضاء

AFAK for Sciences Journal مجلة آفاق للعلوم EISSN: 2602-5345 ISSN: 2507-7228

Attribution - Pas d'Utilisation Commerciale - Pas de Modification 4.0 International (CC BY-NC-ND 4.0)

السيبراني، حيث تجد الدولة نفسها أحيانا تتنازل على سلطتها بفعل فقدان السيطرة على الفضاء السيبراني وإشكالية عدم ضبطه، وهذا ما يتجلى من خلال أمثلة كثيرة، على ذكر المنصات الرقمية لها والتي تأويها دول أخرى بإستعمال الحوسبة السحابية، مما يجعل القانون الواجب التطبيق يُحدّد بعنصر إسناد إلى الدولة صاحبة إقليم تواجد الحوسبة السحابية على حساب القواعد القانونية الواجبة التطبيق على رعايا الدولة المستخدمين للمنصات.

o **فقدان احتكار العنف المشروع:** إنّ خاصية إحتكار الدولة للعنف المشروع، يشوبها غموض في المجال الرقمي بقدر سيادتها، إذ لم تعد السيطرة على الأراضي والحفاظ على السيادة السياسية أمرًا سهل الإتاحة مع ظهور التقنيات الرقمية.

المحور الثاني: تحليل الهشاشات والتهديدات المرتبطة بالفضاء السيبراني.

سيخصص هذا الجزء لوصف عوامل الضعف في الفضاء السيبراني والتهديدات ذات الصلة بالأمن الوطني.

عوامل الضعف:

لقد تحول الفضاء السيبراني من مجال دون رقابة إلى فضاء الأكثر رقابة في العالم، بفعل الإستخدام الناجع للتقنيات الحديثة المتاحة والتي يسهل إقتناؤها لأغراض سياسية أو إجرامية، وبالخصوص الإرهابية والتخريبية حيث شكّل ذلك تهديداً حقيقياً وتحدياً كبيراً للدول والحكومات.

فالفضاء السيبراني يوفر للجهات المعادية فرصاً للاتصالات والمعلومات والتدريب والتمويل والتخريب وما إلى ذلك، وهو فضاء للتعبير عن مختلف الأيديولوجيات الإرهابية والعنصرية والفاشية وغيرها من تلك التي تنبذها المجتمعات. وترى المنظمات الإرهابية والتحريضية في الفضاء السيبراني مسرحًا لناشطيتها ومنبرا للدعاية المغرضة وأداة للتجنيد والتدريب، ووسيلة لإقامة اتصال دائم بين مؤيديها وأنصارها والناشطين على نطاق عالمي.

ومع ذلك، فإن الفضاء السيبراني ليس المجال المفضل للمجرمين فحسب، بل يشكل حقلا لنشاط الدول وفواعل آخرون، التي تتمظهر هشاشتها بدلالة عدة عوامل، نذكرها:

هشاشة مقترنة بالتصميم :

في مجال المعلوماتية، ولا سيما في مجال أمن الحاسوب، تعتبر الثغرة الأمنية عيب في برنامج أو نظام حاسوبي يمكن إستغلاله للوصول إلى النظام المعني وتقويض سلامته، أو لتنفيذ برامج أو أوامر بهدف الوصول إلى البيانات أو سرقتها أو تعديلها.

إن الثغرات المتعلقة بالتصميم هي نتيجة لعيوب أو أوجه قصور في تصميم المخطط الخوارزمي العام للبرمجيات أو المعدات وكذلك نتيجة للأبواب الخلفية التي تركها المصممون أو المطورون عمداً.

بشكل عام، تحتوي الإصدارات الأولى من البرمجيات على "أخطاء" تتسبب في تعطل البرنامج. يقوم ناشرو البرمجيات بتصحيح منتجاتهم بشكل دوري وتقديم تحديثات مجانية لعملائهم.

وقد أصبح الكشف عن العيوب في البرمجيات وأنظمة الكمبيوتر تخصصاً للشركات التي تسوق منتجات الأمن السيبراني، وكذلك لمطوِري برامج التسلل والتجسس.

هشاشة مرتبطة بالإستخدام :

يمكن تصور نقاط ضعف ترتبط بإستخدام التقنيات والتسهيلات التي يوفرها الفضاء السيبراني لأغراض خبيثة بمجرد إنشاء اتصال بالإنترنت، إذ بمجرد توصيل جهاز كمبيوتر أو أي جهاز آخر يتيح الربط بالأنترنت، يتم تحديده تلقائيًا من خلال عنوان بروتوكول "IP" مفرد له من قبل مزود خدمة الأنترنت الخاص به.

بالنسبة لعموم الجمهور، تكون عناوين بروتوكول "IP" متغيرة بما يجعلها ديناميكية. هذا يعني أنّه من أجل التمكن من تحديد هوية مستعمل الأنترنت، يتعيّن الحصول في آن واحد على بروتوكول عنوانه "IP" وساعة وصله بالشبكة.

AFAK for Sciences Journal مجلة آفاق للعلوم EISSN: 2602-5345 ISSN: 2507-7228

Attribution - Pas d'Utilisation Commerciale - Pas de Modification 4.0 International (CC BY-NC-ND 4.0)

وهذا ما يجعل الإرهابيين والقراصنة يستعملون تقنيات مختلفة لإخفاء هويتهم من أجل تقويض نسق تحديد موقعهم والتعرف عليهم. كما يستخدم القراصنة تقنيات مختلفة لإخفاء أو تشويش عناوين IP الخاصة بهم مثل إستخدام تقنيات وأدوات VPN "الشبكة الخاصة الإفتراضية" وخدمات الولوج عن بعد للحصول على عناوين IP أخرى، موطنة في دول أخرى ولا يمكن تحديد مصدرها الحقيقي.

كما أنّ إنتحال الهوية أو إستعمال هويات مزيفة هي أيضاً ممارسة شائعة بين مستخدمي الإنترنت، حيث عند شراء أسماء النطاقات أو البرمجيات أو منتجات الأجهزة، أو عند إنشاء حسابات بريد إلكتروني أو صفحة فيسبوك أو حساب تويتر، يستخدم هؤلاء عادةً هويات ليست بهوياتهم.

التهديدات على الأمن الوطني المرتبطة بالفضاء السيبراني:

من الضروري وضع تصنيف للتهديدات التي يتعرض لها الأمن الوطني والمرتبطة بشكل مباشر أو غير مباشر بالفضاء السيبراني والتي هي من عمل الفواعل في ذات الفضاء.

وفي هذا السياق، قمنا بتصنيف هذه التهديدات إلى فئتين: التهديدات المباشرة والتهديدات غير المباشرة على الأمن الوطني.

التهديدات المباشرة :

وهي التهديدات في الفضاء السيبراني التي لها تأثير مباشر على الأمن الوطني، وهي:

الإرهاب السيبراني :

الإرهاب السيبراني ترجمة لنظيره بالفرنسية Cyberterrorisme هو مصطلح عام مكون من البادئة "سايبر" التي تشير إلى الفضاء السيبراني وكلمة إرهاب. وهو شكل جديد من أشكال التهديد على السلم والأمن الوطنيين.

ويعتبر الإرهاب السيبراني تجليا لإستغلال الهشاشات التي أوجدتها تكنولوجيات الإعلام والاتصال. وقد استغل الإرهابيون هذه الوسائل المتطورة في الوقت المناسب لتنفيذ أعمالهم الإرهابية، مغتنمين الخدمات والوظائف التي يوفرها الفضاء السيبراني في مساعيهم الإرهابية بسهولة واقتصاد في الوسائل.

وفي هذا السياق، تجدر الإشارة إلى إحتمال استخدام الإرهابيين للطائرات بدون طيار والطائرات المدنية، وهو أمر يجب أن يؤخذ على محمل الجد، لا سيما بالنظر إلى انتشار الإستخدام المدني لهذه الطائرات، لاسيما وأنّ هذه التكنولوجيا إستقطبت إهتمام المنظمات الإجرامية. فهناك في السوق طائرات بدون طيار موجهة للإستعمال المدني، يتم التحكم فيها عن بعد بواسطة الأجهزة اللوحية أو الهواتف الذكية، والتي يمكن تعديلها بسهولة لحمل الأسلحة والمتفجرات أو حتى الصواريخ من أجل تنفيذ هجمات عن بعد أو إنطلاقا من قارة أخرى عبر الأنترنت.

ومما لا جدال فيه أن هجمات 11 سبتمبر 2001، مكنت المجتمع الدولي من إدراك الإمكانات المدمرة للإرهاب وبعده العابر للحدود الوطنية وطبيعته الضارة بالسلم والأمن الدوليين، حيث شهد العالم منذ حينها حملة دولية غير مسبوقة ضد جميع أشكال الإرهاب. ومع ذلك، وعلى الرغم من الجهود المتعددة الأبعاد (السياسية والقانونية والأمنية) التي يبذلها المجتمع الدولي في مكافحة الإرهاب ووجهه السيبراني، لا يزال الإرهاب السيبراني مصدر إزعاج يتعيّن على الدول إعتباره بكل يقظة.

إن نوايا المهاجمين وهوياتهم ودوافعهم هي العناصر اللازمة لتوصيف الهجوم. "يجب أن يكون الفعل مع سبق الإصرار والترصد، وأن يكون مدفوعًا بمصالح أيديولوجية، ومرتبطًا باعتبارات تتعلق بالأقليات القومية أو العرقية أو العملاء السريين، ومن المحتمل أن يولد حالة من الذعر، بهدف التأثير على الحكومات وإضعاف الدولة[12] .

وتُعرّف وزارة الأمن الداخلي الأمريكية الإرهاب السيبراني بأنّه "عمل إجرامي يُرتكب من خلال أجهزة الحاسوب ويؤدي إلى العنف أو الموت أو الدمار ويخلق حالة من الرعب بهدف التأثير على سياسة الحكومة".

Attribution - Pas d'Utilisation Commerciale - Pas de Modification 4.0 International (CC BY-NC-ND 4.0)

كما يوجد تعريف تقني للإرهاب السيبراني بأنّه "أي عمل متعمد لتدمير أو إضعاف أو تعديل البيانات أو تدفق المعلومات أو أنظمة الحاسوب الحيوية للدول أو الشركات ذات الأهمية الحيوية لحسن سير العمل في بلد ما، بهدف إحداث ضرر و/أو إحداث أكبر قدر من التأثير من أجل بث الرعب، لأسباب سياسية أو دينية أو أيديولوجية".

وبالإضافة إلى ذلك، فإن التهديد الإرهابي يلزم السلطات على الإهتمام بنقاط الضعف في أمن المنشآت القاعدية والبنى التحتية لتكنولوجيا المعلومات مثل محطات وشبكات الطاقة، أو أنظمة تكنولوجيا المعلومات والاتصالات في الإدارات الحكومية والشركات الكبرى.

الإستخبارات السيبرانية:

الإستخبارات السيبرانية هي إستخدام الفضاء السيبراني لأغراض استخباراتية، إذ يعتبر هذا الأخير المصدر الرئيسي للمعلومات المتاحة أو المحمية، كما أنه وسيلة للتجسس والتلاعب والتجنيد والتغطية الإعلامية في سياق حرب المعلومات وما إلى ذلك.

التهديدات غير المباشرة :

وهي التهديدات ذات الإنعكاسات غير المباشرة على الأمن الوطني، على ذكر الجريمة السيبرانية التي لها تأثير مباشر على الإقتصاد الوطني، أو ظاهرة التسريب السيبراني التي لها انعكاسات مباشرة ذات طابع سياسي من المحتمل أن يكون لها تأثير على الأمن الوطني.

الجريمة السيبرانية

الجريمة السيبرانية هي أحدى أشكال الجريمة والجنوح المرتبطة بالفضاء السيبراني، ومن ثم فهي تختلف عن الأشكال التقليدية للأفعال الإجرامية. وهي تشمل جميع الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، والتي يُمكن أن تُرتكب على أو بواسطة نظام حاسوبي موصول بالأنترنت.

التسريب السيبراني:

يعتبر تسريب المعلومات ظاهرة شائعة وجد قديمة، ومن بين حالات التسريبات الكبرى لمعلومات سرية ومكتومة التي كانت لها تداعيات خطيرة أحيانا ذات بعد إستراتيجي، على المؤسسات و/أو الشخصيات المعنية بهذه التسريبات، على ذكر قضية ويكيليكس.

وتندرج هذه القضية في سياق مفهوم "الويكي" الذي إخترعه عالم الكمبيوتر الأمريكي وارد كننغهام. وتمثلت الفكرة في وضع صفحات ويب على الأنترنت بمحتوى يمكن تعديله من قبل متفحصيه. كان الهدف من تطوير هذا المفهوم، الذي يمكن قراءته أيضًا على أنه "ما أعرفه هو"، هو زيادة الإنتاجية المعلوماتية على الشبكة في سياق متعدد المستخدمين من خلال تسريع المشاركة عبر الأنترنت. كما أدى ذلك إلى تطوير مشروع موسوعة ويكيبيديا متعددة اللغات، والتي تعتبر منذ سنوات من بين العشر مواقع الويب الأكثر تصفحا في العالم.

بالإضافة إلى ذلك، فإن ظهور أشكال جديدة من التهديد على الأمن الوطني مرتبطة بالفضاء السيبراني والوعي برهاناته الأمنية، تدعو الدول إلى ضرورة إعادة تكييف آليات الصد من أجل مواجهة هذه التحديات الجديدة وحماية المصالح الوطنية في الفضاء السيبراني.

الهجمات السيبرانية :

الهجمات السيبرانية هي استخدام موارد الحاسوب على غرار البرمجيات والأجهزة لتنفيذ عمليات محددة في الفضاء السيبراني، تهدف إلى تقويض التشغيل السليم لأنظمة الحاسوب، أو الولوج إليه للإطلاع على البيانات والمعلومات مع إمكانية تغيير المحتوى (إضافة وقراءة وكتابة وحذف) أو طمس الخدمات التي تقدمها هذه الأنظمة.

يمكن تنفيذ الهجمات السيبرانية بسهولة نسبية وبتكلفة منخفضة، على مسافة قصيرة وبمخاطر منخفضة جداً على المهاجم (المهاجمين). كما يمكن تنفيذها من قبل فاعل واحد أو أكثر، بإستخدام حاسوب أو أكثر من الحواسيب المتشابكة وفق هندسة تضفي لها شكل منصة إطلاق أو عبور بإستخدام أسلحة يشار إليها بإسم "الأسلحة السيبرانية" أو "الأسلحة المعلوماتية"،

Attribution - Pas d'Utilisation Commerciale - Pas de Modification 4.0 International (CC BY-NC-ND 4.0)

والتي تعتبر أسلحة الفضاء السيبراني المصممة بإستخدام الحاسوب و/أو التقنيات التكنولوجية لحرب المعلومات[13]، وهي:

- شبكات الروبوتات (Botnets):

وهي شبكة من الحواسيب (Zombies) التي يتم التحكم فيها عن بعد من قبل مستخدم خارجي لتنفيذ هجمات موزعة، ويمكن أن يصل حجم شبكة البوت نت إلى عدة آلاف من الآلات المنتشرة في عشرات البلدان.

- حصان طروادة (Cheval de Troie)

وهو برنامج خبيث، عادةً ما يكون مخفياً في ملف آخر، يعمل دون علم المستخدم ويقوم بتثبيت نفسه في نظام تشغيل الحاسوب، ثم يقوم بتنفيذ عمليات محددة، مثل فتح الوصول عن بعد إلى أجزاء محمية من نظام تشغيل الحاسوب وجمع البيانات الحساسة مثل عناوين البريد الإلكتروني وكلمات المرور والملفات التي تم الاطلاع عليها أو حفظها ومعلومات حول إصدار نظام التشغيل وموقع الحاسوب وما إلى ذلك.

وينقل حصان طروادة هذه البيانات إلى موقع في الفضاء السيبراني، سواء كان موقعاً إلكترونياً أو بريداً إلكترونياً أو دليلاً على الأنترنت أو عن طريق الرسائل النصية القصيرة.

- الفيروسات (Virus):

هي برامج كمبيوتر خبيثة، لديها بالإضافة إلى الإجراءات المبرمجة مسبقاً للقيام بها، القدرة على التكاثر عن طريق عدوة بإصابة برامج أو ملفات أخرى غير خبيثة.

- الديدان:

هي فيروسات كمبيوتر مستقلة وتتكاثر ذاتيا لتنتشر عبر الشبكة دون أن تصيب بالضرورة ملفات أخرى.

- الثغرات

هي تقنيات تُمكن من إكتشاف وإستغلال هشاشات وثغرات في البرمجيات وأنظمة التشغيل للحواسيب والهواتف الذكية، من أجل اختبار فعالية نظام المعلومات (مضاد الفيروسات، جدار الحماية الناري، كشف التسلل ...إلخ).

وتعتبر الثغرات أو العيوب في البرمجيات أو أنظمة التشغيل، نتيجة لأخطاء في التصميم أو التنفيذ والتي يتم توثيقها وتصحيحها علناً بمجرد إكتشافها.

الحرب السيبرانية :

إنّ مصطلح "الحرب السيبرانية" يمكن أن يُستعمل كذريعة للتوظيف، فالحرب التي يحكمها قانون تعبر عن نشاط عنيف علني، يؤدي إلى قتل البشر ويُدار في إقليم من طرف مجموعات منظمة عن قصد. و بإفتراض أنّ الأطراف المشاركة في النزاع هي كيانات دولاتية، يمكن تعريف الحرب السيبرانية على أنّها "المواجهة بين دولتين أو أكثر في الفضاء السيبراني من أجل الإضرار بأنظمة المعلومات ونسقاتها الإجرائية ومواردها وغيرها من الهياكل الحساسة، وإضعاف الأنظمة السياسية والاقتصادية والاجتماعية؛ العمل النفسي المكثف تجاه الساكنة لزعزعة استقرار المجتمع والدولة، وكذلك التأثير لإجبار الدولة المستهدفة على اتخاذ تدابير لصالح الطرف الخصم"[14] .

فالعدو يسعى دوما لإلحاق أكبر قدر من الإضرار بالبنى الحساسة مما يجعل المنشآت المدنية للإتصالات في صلب قائمة الأهداف الكامنة. فـ "الحرب السيبرانية هي عبارة عن صراع سبراني متقدم بين الدول، تُوجه فيه الهجمات السيبرانية من قبل فواعل دولاتية ضد المنشآت في إطار خطة لحملة عسكرية" [15].

أخطر الهجمات السيبرانية هي تلك التي تستهدف أنظمة التحكم الصناعي، وهي أنظمة آلية تنظم بعض المنشآت لاسيما في قطاعات المياه والإنتاج والنقل والصناعة والمالية.

في عام 2012، تعرضت شركة النفط والغاز السعودية أرامكو لهجوم سبراني إستهدف نظام SCADA[16] الخاص بها. ألحق هذا الهجوم الإلكتروني الضرر بحوالي 30,000 محطة عمل، أي ما يعادل 75% من حواسيب أرامكو، واستغرق نسق إستعادة نظام تشغيلها أكثر من أسبوعين.

ومن بين الأسلحة السيبرانية نجد فيروس ستوكس نت (Stuxnet)، وهو عبارة عن دودة حاسوبية شديدة التعقيد

Attribution - Pas d'Utilisation Commerciale - Pas de Modification 4.0 International (CC BY-NC-ND 4.0)

مصممة لتخريب نوع معين من أنظمة التحكم الصناعي (ICS) التي تنتجها شركة سيمنز (Siemens) وتستخدم في محطات الطاقة النووية في إيران.

وقد أظهرت التحليلات التقنية أن هذا الفيروس يتكون من عدد من الوحدات النمطية بما في ذلك الوحدة 315 التي تستهدف على وجه التحديد أجهزة الطرد المركزي IR-1، والوحدة 417 التي من شأنها أن تهاجم على وجه التحديد وحدة التوربينات البخارية المستخدمة في المحطة المركزية لإنتاج الكهرباء ببوشهر بإيران.

ويتطلب تصميم فيروس ستوكس نت (Stuxnet) مستوى عالٍ من الخبرة التقنية، ومعلومات إستخباراتية معمقة قبل البرمجة من أجل معرفة خصائص الأهداف المقصودة، والقدرة على اختبار الدودة قبل تلقيحها من أجل ضمان عملها بشكل فعال، وهو ما يفوق بكثير قدرات مؤسسة تجارية أو مجموعة من القراصنة.

كانت أولى الهجمات الإلكترونية الإستراتيجية ضد دولة ما، هي تلك التي إستهدفت إستونيا في عام 2007. ففي أعقاب التوترات السياسية مع روسيا، تم شن موجات من الهجمات الإلكترونية في وقت واحد ضد أنظمة المعلومات في إستونيا، مما أدى إلى تعطيل العديد من البنوك والعديد من المواقع الإلكترونية الرسمية بما في ذلك مواقع البرلمان والوزارات والصحف اليومية ومحطات التلفزيون.

مما سبق، يتضح جليا أنّه لا يمكن الخوض في الحرب السيبرانية دون الحديث عن الأمن السيبراني، إذ أنّ الحيلولة وقايةً دون منع الحرب السيبرانية من النشوب هو أحد أهداف الأمن السيبراني. وقد تم تقديم هذا المفهوم لأول مرة في عام 2011 من قبل الأمين العام للاتحاد الدولي للاتصالات، حمدو توريه، في تقرير نشره، أعرب فيه عن مخاوف مبررة بشأن احتمالات الدمار في حال نشوب حرب سبرانية.

الخلاصة :

بعد دراستنا لموضوع الفضاء السيبراني وأهم التهديدات الناجمة عن تنوع فواعله وتعدد أبعاده يمكن أن نستنتج أنّ الجزائر على غرار الدول المهتمة بالشأن السيبراني، تواجه تحديات بأشكال جديدة يتعيّن عليها إدراج محور الأمن السيبراني في أجندتها السياسية والإستراتيجية الأمنية، حتى يتسنى للجزائر تحيين منظومتها الدفاعية والأمنية في ظل التطور السريع الذي شهدته التكنولوجيا، بما يمكن الدولة من صد الإعتداءات الرقمية وحماية مصالحها في الفضاء السيبراني.

المراجع باللغة العربية

- الدكتور أحمد عبيس نعمة الفتلوبي، الهجمات السيبرانية: مفهومها و المسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق المحلي، جامعة الكوفة، العراق ،2016/2015، ص5.

- الدكتور منير البعلبكي،" المورد : قاموس انكليزي –عربي"، دار العلم للملايين، بيروت، 2004 ،ص24.

المراجع باللغة الإنكليزية

- “Israeli Test on Worm Called Crucial in Iran Nuclear Delay” par William J. Broad, John Markoff et David E. Sanger, publié dans le journal “The New York Times”, 15 janvier 2011.

- Richard Kissel,"Glassory of Key Information Security Terms", National Institute of Standards and technology, U.S Department of Commerce ", Revision, 2, May, 2013, P57.

المراجع باللغة الفرنسية

-Bertrand Boyer, Cybertactique : conduire la guerre numérique, Paris, NUVIS, 2014, Page25.

-Bertrand Boyer, Cyberstratégie : l’art de la guerre numérique, Paris,NUVIS,2012, Page54.

-Olivier Kempf, Introduction à la cyberstratégie, Paris : Economica, 2012, p9

- Centre d'Etudes Scientifiques de Défense — CESD, Cyberterrorisme, Mythe ou réalité ? Cedric Thevenet, Université de Marne-La-Vallée 2005, p.7.

- Yannick HARELL, La Cyberstartégie russe, Paris, Nuvis, 2013, p 129

- Yannick HARREL, op.citp.129

المراجع الويبوغرافية

https://www.01net.com/actualites/, consulté le 28/04/2024 à 10h19 min

http://www.egeablog.net. L'individu, acteur stratégique du cyberespace, consulté le 29/04/2024 à 00h16.

Attribution - Pas d'Utilisation Commerciale - Pas de Modification 4.0 International (CC BY-NC-ND 4.0)

Russia — US bilateral on cybersecrutity, Critical terminology foundation, lien www.rus-cybersec-us.org consulté le 28/04/2024 à 23h25.

[1] https://www.01net.com/actualites/, 28 Avril 2024 à 10 h 19 min

[2] Cisco Systems هي شركة أمريكية لتكنولوجيا المعلومات تخصصت في الأصل في أجهزة الشبكات، ومنذ عام 2009 في الخوادم (Serveurs). وقد تنوعت منذ ذلك الحين في مجال البرمجيات، وعلى وجه الخصوص الأمن السيبراني.

[3] *"Israeli Test on Worm Called Crucial in Iran Nuclear Delay" par William J. Broad, John Markoff et David E. Sanger, publié dans le journal "The New York Times", 15 janvier 2011.*

[4] - الدكتور أحمد عبيس نعمة الفتلوي، الهجمات السبرانية: مفهومها و المسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق المحلي، جامعة الكوفة، العراق، 2016/2015، ص5.

[5] - الدكتور منير البعلبكي،" المورد : قاموس انكليزي – عربي"، دار العلم للملايين، بيروت، 2004 ،ص24.

[6] - Richard Kissel,"Glassory of Key Information Security Terms", National Institute of Standards and technology, U.S Department of Commerce ", Revision, 2, May, 2013, P57.

https://www.unodc.org/documents/terrorism/Publications, consulté le 29/04/2024 à 00h22.

قائمة الهوامش

[7]-Bertrand Boyer, Cybertactique : conduire la guerre numérique, Paris, NUVIS, 2014, Page25.

[8] -Bertrand Boyer, Cyberstratégie : l'art de la guerre numérique, Paris,NUVIS,2012, Page54.

[9] Olivier Kempf, Introduction à la cyberstratégie, Paris : Economica, 2012, p9

[10] - http://www.egeablog.net. L'individu, acteur stratégique du cyberespace, consulté le 29/04/2024 à 00h16

[11] - https://www.unodc.org/documents/terrorism/Publications, consulté le 29/04/2024 à 00h22.

[12] - Centre d'Etudes Scientifiques de Défense — CESD, Cyberterrorisme, Mythe ou réalité ? Cedric Thevenet, Université de Marne-La-Vallée 2005, p.7.

[13] - Yannick HARELL, La Cyberstartégie russe, Paris, Nuvis, 2013, p 129

[14] - Yannick HARREL, op.citp.129

[15] - Russia — US bilateral on cybersecrutity, Critical terminology foundation, accessible suivant le lien www.rus-cybersec-us.org consulté le 28/04/2024 à 23h25.

Attribution - Pas d'Utilisation Commerciale - Pas de Modification 4.0 International (CC BY-NC-ND 4.0)