جامعة سيدي محمد بن عبد الله بفاس
الكلية متعددة التخصصات تازة
UNIVERSITÉ SIDI MOHAMED BEN ABDELLAH DE FES
FACULTÉ POLYDISCIPLINAIRE DE TAZA

رسالة مقدمة لاستكمال متطلبات نيل شهادة الماستر في القانون العام

ماستر: استراتيجية صنع القرار

بعنوان

# الدفاع السيبراني في شمال إفريقيا: المغرب والجزائر نموذجا

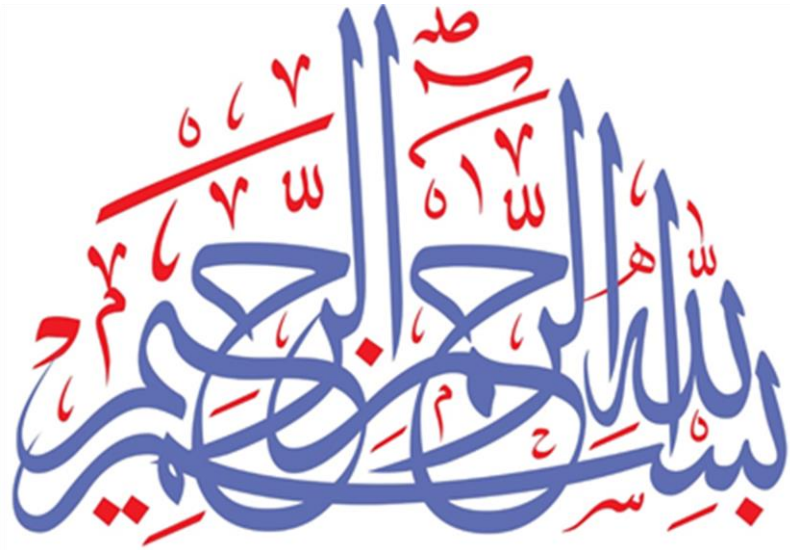
تحت إشراف الأستاذ: د.وديع الهامل

إعداد الطالب: إدريس عبادي

لجنة المناقشة:

| | | |
|---|---|---|
| د.وديع الهامل | أستاذ باحث بالكلية متعددة التخصصات تازة | رئيسا ومشرفا |
| د.عبد القادر لشقر | أستاذ باحث بالكلية متعددة التخصصات تازة | عضوا |
| د. عبد المجيد بوكير | أستاذ باحث بالكلية متعددة التخصصات تازة | عضوا |
| د.مصعب التجاني | أستاذ باحث بالكلية متعددة التخصصات تازة | عضوا |
| د. محمد الجلطي | أستاذ باحث بالكلية متعددة التخصصات الناظور | عضوا |

السنة الجامعية: 2022-2023


بسم الله الرحمن الرحيم


وقل رب زدني علما

# شكر وعرفان

أحمد الله و أشكره إذ أكرمني بفضله و عطائه و أمدني بالقوة و ألهمني نعمة الصبر لإنجاز هذا العمل المتواضع. فإن أصبت فمن الله و إن أخطأت فمن تقصيري، وما توفيقي إلا بالله العلي القدير، و أصلي و أسلم على سيدنا محمد معلم البشرية جمعاء وناصحها لما فيه صلاحها.

في البداية، أغتنم هذه الفرصة للاعتراف لذوي الفضل بفضلهم و تقديم خالص الشكر لهم، على توجيهاتهم القيمة لي طيلة مدة هذا البحث؛ أخص بالذكر أستاذي الفاضل "وديع الهامل"، لتفضله بالإشراف على هذه الرسالة، ولتوجيهاته الثمينة وكرم عنايته طيلة مدة بحثي في هذا الموضوع الأمني.

ومن المهم أن أتوجه بخالص تقديراتي واحتراماتي إلى كل أساتذتي في الكلية المتعددة التخصصات بمدينة تازة.

كما أشكر اللجنة المناقشة و كل من كان له الفضل في إتمام هذا العمل، و أتمنى أن يكون ذلك في ميزان حسناتهم. وأخص بالذكر الدكاترة الأجلاء:

| | |
|---|---|
| د.عبد القادر لشقر | أستاذ باحث بالكلية متعددة التخصصات تازة |
| د. عبد المجيد بوكير | أستاذ باحث بالكلية متعددة التخصصات تازة |
| د.مصعب التجاني | أستاذ باحث بالكلية متعددة التخصصات تازة |
| د. محمد الجلطي | أستاذ باحث بالكلية متعددة التخصصات الناظور |

فلكم مني أساتذتي فائق الثناء والتقدير، وكل الاحترام والتوقير.

لا تفوتني الفرصة كذلك، دون شكر من أغفل القلم عن إدراجهم، لكن لم يغفل القلب عن تفكرهم . فللجميع مني أصدق الشكر و أخلص التقدير.

# إهداء

إلى راعي العلم والعلماء في هذا البلد العظيم، إلى جلالة الملك القائد الأعلى ورئيس أركان الحرب العامة للقوات المسلحة الملكية، الذي ما فتئ يرخص لضباطه، ولوج المؤسسات العلمية داخل وخارج الوطن، لمواكبة التطور الفكري الوطني والانفتاح على التجارب العلمية الغربية.

إلى روحي والدي الطاهرتين، رحمة الله عليهما، اللذين سهرا على تربيتي وبرضاهما أكرمني العلي القدير كثيرا. أسأل الله ﷻ أن يغفر لهما ويرحمهما ويسكنهما فسيح جناته. إنه سميع مجيب الدعوات.

إلى أيقونة بيتي وأم أطفالي، التي لم تبخل بجهدها لمساعدتي في السراء والضراء. فاللهم شافها وعافها وألبسها لباس الصحة والعافية، هي وجميع مرضى المسلمين، إنك على كل شيء قدير.

إلى ابنتي مروة وإلى ابني علي، وفقهما الله في دينهما ودنياهما.

أهديكم جميعا ثمرة هذا العمل المتواضع، راجيا من العلي القدير، أن يتقبله مني وأن يكتبه لي في ميزان حسناتي.

# لائحة المختصرات
# Abréviations

بالعربية

| | |
|---|---|
| ص | الصفحة |
| ص ص | من الصفحة..... إلى الصفحة |
| ط | الطبعة |
| ط غ | طبعة غير متوفرة |

بالفرنسية

| | |
|---|---|
| ADN | Administration de la Défense Nationale du Royaume du Maroc(إدارة الدفاع الوطني بالمملكة المغربية ) |
| ANRT | Agence Nationale de Réglementation des Télécommunications (الوكالة الوطنية لتنظيم الاتصالات) |
| CGEM | Confédération Générale des Entreprises du Maroc (الاتحاد العام للمقاولات المغربية) |
| CMRPI | Centre Marocain de Recherches Polytechniques (المركز المغربي لأبحاث البوليتكنيك) |
| CNDP | Commission Nationale de Contrôle de la Protection des Données Personnelles (الهيئة الوطنية للرقابة على حماية البيانات الشخصية) |
| CoE | Conseil de l'Europe"مجلس أوروبا " |
| DGSSI | Direction Générale de la Sécurité des Systèmes d'Information(المديرية العامة لأمن نظم المعلومات) |
| Ed | Edition(طبعة) |
| MA-CERT | Centre Marocain d'Alerte et de Gestion des Incidents Informatiques (المركز المغربي للإنذار وإدارة حوادث الكمبيوتر) |
| OSCE | Organisation pour la Sécurité et la Coopération en Europe (منظمة الأمن والتعاون في أوروبا) |
| p | Page(صفحة) |
| pp | de la page…….jusqu'à la page……..ص ص |
| N° | Numéro |
| Vol | Volume |

بالإنجليزية

| | |
|---|---|
| AU | African Union(الاتحاد الافريقي) |
| CCP | Chinese Communist Party(الحزب الشيوعي الصيني) |
| CISA | Certified Information Systems Auditor<br>(مدقق نظم معلومات معتمد) |
| CSDP | Common Security and Defence Policy<br>(سياسة الأمن والدفاع المشتركة) |
| DCO | Digital Cooperation Organization<br>(منظمة التعاون الرقمية ) |
| DDoS | Distributed Denial of Service attack<br>(هجمات حجب الخدمة الموزعة) |
| D S R | Digital Silk Road(طريق الحرير الرقمي) |
| ECOWAS | Economic Community Of West African States<br>(الجماعة الاقتصادية لدول غرب أفريقيا) |
| ICT | Information and Communication Technologies<br>(تكنولوجيا المعلومات والاتصالات) |
| ICANN | Internet Corporation for Assigned Names and Numbers<br>(شركة الإنترنت للأسماء والأرقام المخصصة) |
| IETF | Internet Energing Task Force<br>فريق مهام هندسة الإنترنت |
| ISP | Internet Service Provider<br>(مزود خدمة الإنترنت أو موفر خدمة الاتصال بالإنترنت) |
| maCERT | Moroccan Computer Emergency Response Team<br>(فريق الاستجابة لطوارئ الحاسوب) |

## الملخص

تناولت هذه الدراسة الاستراتيجية موضوع الدفاع السيبراني في شمال أفريقيا، وبالضبط في المغرب والجزائر. خصصت الدراسة شقا نظريا، ركزت فيه على قراءة الفضاءين السيبرانيين المغربي والجزائري بناء على تقاطع توجهات ثلاث نظريات متباينة؛ الواقعية والليبرالية والنقدية. كما تطرقت الدراسة إلى التهديدات السيبرانية المؤرقة لمضجعي البلدين، تبين أن جل تلك التهديدات انحصرت في تبادل التهم بينهما؛ تهم لم ترق لحرب إلكترونية. وبناء على تلك التهديدات، يسعى البلدان، في الآونة الأخيرة، إلى تكتيف جهودهما في بلورة سياستيهما التنظيميتين في المجال السيبراني، وذلك عبرمراجعة بنيتيهما التحتيتين؛ وطنيا، إقليميا ودوليا، و تفعيل قوانينهما التنظيمية لمجاليهما السيبرانيين وفق المتغيرات الراهنة. لكن، مع كل تلك الاجتهادات، يشير المؤشر العالمي لقياس قدرات الأمن السيبراني إلى تأخر هذين البلدين، خصوصا الجارة الجزائر. تأخر زاد في شدته غياب تعاون إقليمي وحضور تعنت جزائري.



## Abstract

This strategic study dealt with the issue of cyber defense in North Africa, specifically in Morocco and Algeria. The study devoted a theoretical part, in which it focused on reading the Moroccan and Algerian cyberspaces, based on the intersection of the orientations of three different theories; Realism, liberalism and criticism. This study also touched on the cyber threats that haunt the two countries, it realized that the most of these threats were limited to the exchange of accusations between them, but these Charges did not amount to electronic warfare. Based on these threats, the two countries have recently sought to combine their efforts in formulating their regulatory policies in the cyber field by reviewing their infrastructures. Nationally, regionally and internationally, and activating their regulatory laws for their cyber domains in accordance with current changes. However, with all these jurisprudence, the global index for measuring cybersecurity capabilities indicates the lagging of these two countries, especially Algeria. The delay was exacerbated by the absence of regional cooperation and the presence of Algerian intransigence.

## مقدمة

في القرن التاسع عشر، كان السوسيولوجي الفرنسي "إيميل دوركايم" " David Émile Durkheim" لا يفتأ يردد أمام طلابه بجامعة السوربون الفرنسية، تلك العبارة: " إذا تكلم ضميرنا، كان المجتمع هو المتكلم فينا". وكان يلمح بذلك إلى أثر التنشئة الاجتماعية في الأفراد. ويعد هذا مفهوما في زمانه، يؤشر إلى حجم تأثير المدرسة والعائلة والمؤسسات الاجتماعية التقليدية في طرائق الأفراد. لم يكن يعلم أن دور الافتراضي سيتعاظم في مجتمع المعرفة والمعلومات، في بلدان العالم المختلفة، ولم يكن يدري أن الأنظمة الحاكمة سيتزايد تخوفها من تأثير الافتراضي وأثره في إنتاج القوة وإعادة توزيعها[1].

تعاظم تخوف تلك الأنظمة، إذن، إثر انتقال العالم من النزعة الصناعية إلى مجتمع ما بعد الصناعي المرتبط بالنظم المعلوماتية والمعرفية[2]. زادت درجة التخوف وامتدت إلى بعض الدول العظمى، وبالضبط إلى رؤسائها. فبعدما كان البعض يرى أن اختراق الكمبيوترات لا يمكن تحقيقه إلا في الأفلام، رأى الرئيس الأمريكي السابق "رولاند ريغن" عكس ذلك، وهو يشاهد فيلم " ألعاب الحرب""Wargames"[3]، فتساءل "لماذا لا يتحول هذا الخيال إلى حقيقة؟". غير هذا السؤال الذي وجهه ريغان إلى الجنرال فيسي المألوف ووَسَم للمرّة الأولى اهتمام رئيس أمريكي، أو توجيه من البيت الأبيض، إلى ما سيُصطلح على تسميته لاحقا " وسائل الحرب السيبرانية"[4].

---

[1]-جوهر الجموسي، الافتراضي والثورة مكانة الإنترنت في نشأة مجتمع مدني عربي، المركز العربي للأبحاث ودراسة السياسات، الدوحة، ط1، 2016، ص ص. 9-11.

[2]-دارن بارني، المجتمع الشبكي، ترجمة أنور الجمعاوي، سلسلة ترجمان، المركز العربي للأبحاث ودراسة السياسات، بيروت، ط1، 2015، ص ص،16-18.

[3]-مناورات (بالإنجليزية: WarGames): فيلم خيال علمي أمريكي صدر في 1983، من تأليف لورانس لاسكر ووالتر إف باركس وإخراج جون بادهام. الفيلم من بطولة ماثيو برودريك وآلي شيدي ودابيني كولمان وجون وود وباري كوربن.
قصة الفيلم ارتبطت بطالب المدرسة الثانوية ديفيد لايتمان (ماثيو برودريك)، الذي اخترق شركة ألعاب كمبيوتر وتمكن من لعب ألقابها التي لم يتم إصدارها. ولكن عندما يبدأ لعبة الحرب النووية الحرارية العالمية، لم يدرك أنه يلعبها على أرض الواقع. يجمع فيلم الحركة للمراهقين في الثمانينيات، ألعاب الحرب، هوس العصر بألعاب الفيديو بمخاوفه من حرب نووية. لكن الفيلم أيضًا على وشك أن يدور حول العصر الرقمي القادم، ويتنبأ بدقة بعلاقتنا مع أجهزة الكمبيوتر والذكاء الاصطناعي.
( The haughty culturist, wargames (1983): winning at death and destruction, 6.01.2021, link: http://bitly.ws/KLCu, seen on:23.05.2023.)

[4]-فرد كابلان، المنطقة المعتمة: التاريخ السري للحرب السيبرانية، ترجمة لؤي عبد المجيد، سلسلة عالم المعرفة، المجلس الوطني للثقافة والفنون والآداب، الكويت، عدد 470، 2019، ص ص،11-35.

أضحت الرقمية في العصر الحالي، عصر العولمة، تحتل مكانة حاسمة، والحقيقة أن الحضارة الحالية مبنية بشكل أساسي على الرقمية. يسود هذا الأمر في جميع عمليات تنفيذ الأنشطة والإجراءات والأفعال بين الأشخاص، المهنيين والدول. لا يمكن إنكار أن حياة الدول والشركات والمواطنين أضحت تغزوها تكنولوجيا المعلومات والاتصالات الجديدة. وأصبح العالم محوسبا ومترابطا بشكل متزايد، وغير معصوم من الأخطاء الرقمية[5].

خلقت تلك الهيمنة الرقمية المعاصرة أثرا عميقا ومباشرا، في تحطيم الحصون الجغرافية وبعثرة الثقافات المغلقة وإعادة بناء الجماعات والهويات الاجتماعية. فانبثقت عن ذلك أنماط محدثة من المبادلات الاقتصادية والثقافية، تطوقها بنية اتصالية ومعلوماتية تزداد تشابكا، مما خلق ما يسمى المجتمع الشبكي( Network Society)[6].

وفي وقت مبكر من عام 1997، في مقال بعنوان "الإنترنت يجعل العالم جيوسياسيًا"، أعلن كاتب المقال هيرودوت: " أن الإنترنت يبدو قد فشل في إبطاء الصراعات الجيوسياسية، بل على العكس من ذلك، قد ساعد على تكاثرها وتعقدها". فليس من المستغرب أن يصبح الفضاء الإلكتروني جبهة جديدة للهجوم، في ضوء السهولة والاستيعاب العالمي للاتصال السيبراني. هناك قلق عالمي حقيقي من أن طبيعة ونطاق الهجمات السيبرانية يمكن أن تسبب عواقب بعيدة المدى وجد مدمرة[7].

لقد ألغى الفضاء السيبراني الحدود الجغرافية التقليدية، وأضحت الأنشطة اليومية - في البنوك، أو تبادل التأملات ، أو "البريد الإلكتروني"[8]، أو أنظمة التحكم و البنية التحتية-

---

[5]-Abderrahman BELGOURCH et autres, Le cyberspace Diversité des menaces & difficultés de régulation, Imprimerie Pappeterie Elwatanya, Mohammedia, Ed1, 2020 ,p.221

[6]-محمد سويلمي، في الإسلام الرقمي كيف ارتحل المسلمون إلى الفضاء السيبراني، الدار التونسية للكتاب، تونس، ط 1، 2021، ص ص،133-134.

[7]-Frédérick Douzet, La géopolitique pour comprendre le cyberespace, revue de géographie et de géopolitique, Cairn.Info, France, n° 152-153, 2014, p. 3.

[8]-**البريد الإلكتروني** وسيلة اتصال سريعة كانت في بداية اختراعها مقتصرة على الشركات والمصالح الحكومية والجامعات أيضا، لحفظ المستندات وسهولة تداولها بين الموظفين، لتسهيل الاتصال وتسيير العمل وإنجازه. أما الآن فهي وسيلة اتصال متوفرة للعالم أجمع، ويستخدمها أيضا الأفراد العاديين، وطريقة استخدامه سهلة جدا، ويتوافر به الخيارات المتعددة.( (دحان حزام القريطي، الأمن السيبراني وحماية أمن المعلومات، دار الفكر الجامعي، الإسكندرية، ط1، 2021، ص.239. ).

تحدث من خلال الشبكات الرقمية بوثيرة جد متسارعة. لهذا السبب هناك قلق عالمي من أن يصبح الفضاء السيبراني وجهة للهجمات المستقبلية[9].

هذا القلق العالمي لم يكن وليد الصدفة، بل راحت تظهر معالمه مع نهاية التسعينيات، حين وقعت أولى الهجمات السيبرانية المهمة في سياق الصراع في يوغوسلافيا. قرر آنذاك حلفاء الناتو إجراء حملة قصف جوي في صربيا، سميت "عملية قوات الحلفاء". من جهتهم وردا على ذلك، قرر المتسللون الصرب مهاجمة مواقع التحالف وخوادم البريد. إذا ظلت عواقب هذه الهجمات الأولى طفيفة، فإن الأمر نفسه لا ينطبق على الهجمات التي استهدفت إستونيا وجورجيا، أو حتى على انتشار فيروس Stuxnet[10][11].

فالهجمات السيبرانية الحقيقية سجلت حضورها الفعلي في 26 و 27 أبريل من عام 2007، حين اندلعت احتجاجات واسعة النطاق في تالين "Tallinn"، عاصمة إستونيا، بعد

---

[9]-Miranda Grange, cyber warfare and the law of armed conflict, **Victoria University of Wellington**, 2014, link: http://bitly.ws/EkhW, seen on: 10.05.2023, p.4.

[10]- **Stuxnet**: أول برنامج ضار تسبب في تدمير مادي في العالم الحقيقي. تم تطوير هذا الفيروس من قبل المخابرات الإسرائيلية والولايات المتحدة من أجل هزيمة البرنامج النووي الإيراني. لا تقتصر الهجمات الإلكترونية والفيروسات دائمًا على المجال الرقمي، ويمكن أن يكون لها أيضًا تأثير في العالم الحقيقي. في عام 2010، تعلم خبراء الأمن السيبراني ذلك مع ظهور Stuxnet، فهوعبارة عن دودة كمبيوتر قوية صممتها أجهزة المخابرات في الولايات المتحدة وإسرائيل. تم نشره ضد مركب إيراني منعزل، لكنه انتشر بشكل غير متوقع إلى أنظمة الكمبيوتر الخارجية. يمكن أن نستنتج أن Stuxnet كان جزءًا من عملية تخريب كبيرة وعالية المستوى نفذتها الحكومات ضد خصومها.

الآن من المقبول عمومًا أن نؤكد أن Stuxnet تم إنشاؤه من قبل وكالة الأمن القومي ووكالة المخابرات المركزية وأجهزة المخابرات الإسرائيلية. تم التعرف على هذا البرنامج الضار لأول مرة من قبل مجتمع الأمن السيبراني في عام 2010، ولكن من المحتمل أن تكون بداية تطويره منذ عام 2005.صممت حكومتا الولايات المتحدة وإسرائيل Stuxnet كأداة لإحباط برنامج تطوير الأسلحة النووية الإيرانية، أو على الأقل تأخيره. كانت إدارة بوش ثم إدارة أوباما مقتنعة بأنه إذا طورت إيران أسلحة ذرية، فإن إسرائيل ستشن غارات جوية ضد منشآتها النووية وتثير حربًا في جميع أنحاء المنطقة. كان يُنظر إلى عملية "الألعاب الأولمبية" على أنها بديل غير عنيف. قرب نهاية ولاية بوش، تمت الدعوة لعقد اجتماع في غرفة العمليات بالبيت الأبيض. تم عرض أجزاء من جهاز طرد مركزي تم تدميره على طاولة المؤتمر، وقررت الولايات المتحدة أن الوقت قد حان لنشر البرنامج الضار.

رسميًا، لم تعترف أي حكومة رسميًا بتطويرStuxnet. ومع ذلك، في مقطع فيديو تم إصداره في عام 2011 للاحتفال بتقاعد قائد الجيش الإسرائيلي، غابي أشكنازي "Gabi Ashkenazi"، تم تقديم هذا البرنامج الضار باعتباره أحد نجاحاته... لم يتم التعرف على المهندسين الذين يقفون وراء Stuxnet. ومع ذلك، فنحن نعلم أنهم كانوا كثيرين ومؤهلين تأهيلاً عالياً. وفقًا لخبراء Kaspersky Lab ، كان فريقًا من عشرة مبرمجين بحاجة إلى سنتين إلى ثلاث سنوات من العمل لإنشاء هذه الدودة. لم يتمكن الباحثون الأمنيون مطلقًا من الوصول إلى قاعدة رموز Stuxnet، لكنهم تمكنوا من الكشف عن أسرارها من خلال تحليلها. على وجه الخصوص، فهموا أنه مكتوب بعدة لغات، بما في ذلك C و ++ C والعديد من اللغات الموجهة للكائنات. هذا هو أحد البراهين على مدى تطور هذه البرامج الضارة. بعد ذلك، تم تحديد العديد من الديدان الأخرى التي لها نفس قدرات الإصابة مثل Stuxnet. ومن الأمثلة على ذلك Duqu و Flame. يشير هذا التشابه إلى أن هذه البرامج الضارة قد تم إنشاؤها بواسطة نفس الفريق، والذي سيستمر بالتالي في العمل سراً.

(Adriana. L, Stuxnet : zoom sur la « cyber-arme » et comment s'en protéger, **Cyberuniversity**, 21.11.2021, lien de l'article, http://bitly.ws/EtcL, date visite, 12.05.2023.

[11]-Camille Rabussier, l'application du droit international dans le cyberespace, Master Droit comparé, Université Paris II Panthéon Assas, Paris, France, Année Universitaire 2018-2019, pp. 15.

قرار الحكومة بإزالة نصب تذكاري للحقبة السوفيتية بعد الحرب العالمية الثانية. هذا النصب التذكاري تم تشييده في عام 1947، للاحتفال بانتصار الجيش السوفيتي على ألمانيا النازية. ستتحول هذه الاحتجاجات الجسدية إلى احتجاجات على الكمبيوتر، مع الموجة الأولى من الهجمات السيبرانية التي استهدفت صفحات الويب الخاصة بالمؤسسات الحكومية الإستونية ووسائل الإعلام الوطنية[12]. تسبب هذا الهجوم الذي نُسب إلى روسيا، في حدوث شلل مؤقت داخل هذه الدولة. غالبية المتسللين كانوا بالفعل من الروس واحتجوا على تفكيك النصب التذكاري لذكرى الجنود السوفييت الذين ماتوا في الحرب العالمية الثانية[13].

وبعد فترة وجيزة من الهجمات السيبرانية التي ضربت إستونيا، جاء دور جورجيا لتجربة الهجمات السيبرانية، وإن كان ذلك في سياق مختلف. ففي أغسطس 2008، اندلع صراع بين الاتحاد الروسي وجورجيا حول أوسيتيا الجنوبية (l'Ossétie du Sud)، وهي منطقة متنازع عليها بين الدولتين. تتمتع هذه المنطقة بحكم ذاتي بحكم الأمر الواقع منذ نزاع عام 1991 بين أوسيتيا وجورجيا، لكنها لا تزال بحكم القانون منطقة تابعة للأراضي الجورجية، ومعترف بها على هذا النحو من قبل المجتمع الدولي. على الرغم من وقف إطلاق النار والجهود العديدة لحل النزاع، إلا أنه لا يزال دون حل[14]. عانت جورجيا هجمات سيبرانية على مواقع وزارتي الخارجية والدفاع. تحولت الأوهام إذن إلى حقيقة، وأضحت اختراقات كمبيوترات الدول حقيقة لا حلما، أو مجرد فيلم من إبداعات الخيال الفكري. ونتيجة تلك الاختراقات بدأت تبرز استراتيجيات الدول في إعادة قراءة أمنها القومي وتبني خارطة طريق تتماشى والهجمات السيبرانية الجديدة[15]. أصبح مجال السيبرانية، إذن، يتصاعد ويتضخم في جميع أرجاء العالم[16].

حتى إفريقيا اهتمت هي الأخرى بظاهرة الهجمات السيبرانية؛ ففي عام2017، فاز بجائزة أفضل رواية أفريقية في الخيال العلمي،" تادي طومسون" عن كتابه "ماء الورد"،

---

[12]-Camille Rabussier, l'application du droit international dans le cyberespace, Op.cit, pp.15-16.

[13]-Pascal Boniface, la géopolitique 50 fiches pour comprendre l'actualité, Editions Eyrolles, Paris, Ed.09, 2023, p.61.

[14]-Camille Rabussier, Ibid, p. 18.

[15]-جوهر الجموسي، الافتراضي والثورة مكانة الإنترنت في نشأة مجتمع مدني عربي، مرجع سابق، ص ص،9-11.

[16]-فرد كابلان، المنطقة المعتمة: التاريخ السري للحرب السيبرانية، مرجع سابق، ص.15.

الذي تناول حكاية وكيل خدمة أمنية يكافح الاحتيال السيبراني في نيجيريا في عام 2066. لهذه الرواية من الخيال العلمي، إشارة قوية إلى أن إدخال قضايا الإنترنت في إفريقيا ليس من باب الصدفة، بل راجع إلى الاهتمام العالمي المتزايد بتلك الظاهرة الجديدة، الذي توسع مجالها مع بزوغ استخدام كلمة "الفضاء السيبراني"، المستوحاة من كلمة "علم التحكم الآلي"، في عام 1984، من قبل مؤلف روايات الخيال العلمي ويليام جيبسون[17]. هذا الأخير حاول توضيح "هلوسة توافقية يعاني منها يوميًا أطفال العالم، الذين يتعلمون المفاهيم الرياضية، " آنداك. تظهر المقارنة بين هاتين الروايتين أن إفريقيا قد اندمجت في حاضرها، وقبل كل شيء، في مستقبلها وفي تلك الثورة الصناعية الرابعة[18].

تم تنفيذ هذه الثورة الرقمية منذ نهاية القرن العشرين بناء على تطوير الإنترنت[19]. في نفس الوقت ومثل أي نشاط بشري، كان صعود المجال الرقمي مصحوبًا بمخاطر أدت إلى ظهور وتطوير تهديدات جديدة ذات ملامح وعواقب أكثر أو أقل دقة: الجرائم السيبرانية، الإرهاب السيبراني والصراع السيبراني، وطرح قضايا أمن نظم المعلومات بشكل حاد[20].

في هذه البيئة متعددة الأوجه، يوجد شمال أفريقيا بدوله المغاربية بصفة عامة، والمغرب والجزائر -المحور الرئيسي- لهذه الدراسة بصفة خاصة. تتوسع رقمنة هذه البقعة الإفريقية يوما بعد يوم وبشكل واضح، تحاول هي الأخرى الحصول على موطئ قدم في

---

[17]-**ويليام جيبسون** أمريكي الجنسية، من مواليد كونواي بجنوب كارولينا بتاريخ 1948/3/17. كاتب خيال علمي وأحد قادة حركة السايبربانك"cyberpunk ". كان يبلغ من العمر ست سنوات عندما توفي والده عن طريق الاختناق. في عام 1966 ، توفيت والدته أيضًا. يبلغ جيبسون 18 عامًا، وبالتالي يرى تجسيدًا لأحد أسوأ مخاوفه. ترك المدرسة دون حتى اجتياز شهادته، ونجا من خلال إعادة بيع أسواق السلع المستعملة لسكان المدن الذين ذهب للبحث عنهم في الريف. في عام 1968، هرب إلى كندا لتجنب إرساله إلى فيتنام واستقر عام1972 في فانكوفر. هناك استأنف دراسته ببطء وسافر كثيرًا وتزوج في عام 1977، عندما أوشكت دراسته على الانتهاء. بدأ جيبسون، مثل الآخرين، في كتابة قصص قصيرة تشد الانتباه. كتاباته الأولى عبارة عن قصص مستقبلية حول موضوعات مثل تأثير علم التحكم الآلي والواقع الافتراضي الناشئ آنذاك على الجنس البشري في المستقبل القريب. ركوب الأمواج على أساليب الشرير والقوطية في ذلك الوقت. وُلدت **Cyberpunk** مع رواية ويليام جيبسون الأولى في عام 1984 ("Neuromancer") "Neuromancer"، والتي حققت نجاحًا أدبيًا هائلاً. حاز على استحسان خاص (جائزة نيبولا وجائزة هوغو وجائزة فيليب ك. ديك)، تم وضع الخطوط الرئيسية لهذا النوع. أكملت الروايتان التاليتان ما ستكون أول ثلاثية له تسمى "ثلاثية الكونورب Comte" :("Sprawl Trilogy") " "Count Zero") "Zéro، (1986و(1988 "Mona Lisa" Overdrive") "Mona Lisa s'eclate" ،.
حصل ويليام جيبسون، مخترع مصطلح الفضاء السيبراني، على الدكتوراه الفخرية في العلوم الإنسانية، من جامعة كوستال كارولينا في كونواي. **(lien de l'article William Gipson : http://bitly.ws/F99T)**

[18]-Mourad El Manir, L'Afrique face aux défis protéiformes du cyberespace, **policy center for the new South**, 01.12.2023, lien de l'article: http://bitly.ws/DcHt, date visite: 19.04 .2023, p.5.

[19]-Pascal Boniface, la géopolitique 50 fiches pour comprendre l'actualité, Op.cit, p.61.

[20]-Ibid.

العالم السيبراني دون استعداد جيد، لا من حيث الموارد البشرية المدربة بحكمة، ولا في سجل البنى التحتية من المتطلبات المادية والكمبيوترية. القارة أيضا معاقة بسبب نقص الأدوات بصفة عامة، والأدوات اللازمة للتعامل مع التهديدات والمخاطر، بصفة خاصة، والتي تولدها التنمية المستمرة للفضاء السيبراني.

## أهمية الموضوع

بناء على ما سبق، ارتبط الاهتمام في هذه الدراسة، بتسليط الضوء على درجة استعداد شمال إفريقيا-المغرب والجزائر نموذجا- لمواجهة التحديات التي يفرضها الفضاء السيبراني، من خلال تقرير حول تطور الفضاء الرقمي في تلك المنطقة، واعتباره فضاء للصراع ومجالا لممارسة العلاقات الدولية[21]. يكتسي موضوع هذه الرسالة أهمية بالغة على مستويين اثنين:

### الأهمية العلمية

تتمثل أهمية هذه الدراسة، في تناولها لموضوع محوري على المستوى العلمي، حيث يندرج موضوع البحث ضمن الدراسات الأمنية والاستراتيجية، وتتجلى أهميته العلمية من خلال التعريف بالدفاع السيبراني في شمال إفريقيا، وبالضبط في المغرب والجزائر، بحكم جوارهما المبني على انعدام الثقة المتبادلة بين الطرفين. ودورهما في بناء سرح استراتيجي دفاعي.

### الأهمية العملية

يعتبر موضوع الدفاع السيبراني في شمال إفريقيا، وبالضبط في المغرب والجزائر، من المواضيع التي تعنى بأهمية كبيرة لدى النظامين، خاصة في الآونة الأخيرة، والمكانة التي حضي بها لدى البلدين. من هذا المنطلق تبرز أهمية الموضوع العملية، من خلال معرفة كيفية تعامل النظامين مع الفضاء السيبراني، ومدى قوتهما أو قدرتهما في مواجهة التهديدات الداخلية والخارجية المختلفة، والتحديات الصعبة.

[21]-Mourad El Manir, L'Afrique face aux défis protéiformes du cyberespace, Op.cit, p.5.

**الإطار المفاهيمي والنظري للبحث " الكلمات المفتاح":** اشتملت الدراسة على أربع كلمات مفتاح لابد من التدقيق في معانيها ومفاهيمها لغويا واصطلاحيا. تمثلت هذه الكلمات في؛ **الدفاع السيبراني، شمال أفريقيا، المغرب والجزائر.**

**الدفاع السيبراني:** ما الذي نعني ب"الدفاع السيبراني"؟

قبل البحث في معنى الدفاع السيبراني، يلزم التطرق إلى معنى السيبرانية في اللغة. فمصطلح السيبرانية من أكثر المصطلحات ترددا في معجم الأمن الدولي، وتشير المقاربة الإيتيمولوجية ل"Cyber" إلى أنها لفظة يونانية الأصل مشتقة من كلمة "Kybernetes"، بمعنى الشخص الذي يدير دفة السفينة، حيث تستخدم مجازا للمتحكم "governor"[22].

وبالعودة إلى معاجم اللغة، نجدها عرفت في معجم "المورد" بأنها "علم الضبط ومصدرها cybernetics"، وهو مصدر يتوافق مع مفهوم الهجمات السيبرانية، المرتبط بضبط الأشياء عن بعد والسيطرة عليها. أما معجم المصطلحات العسكرية الأمريكية، لم يرجع كلمة سايبر إلى مصدرها، بل أعاد كلمة سايبر إلى استخدامها الفعلي، أي العسكري وعرفها بأنها "أي فعل يستخدم عن طريق شبكات إلكترونية بهدف السيطرة أو التعطيل لبرامج إلكترونية أخرى". فيما عرفها معجم مصطلحات الأمن المعلوماتي بأنها: " هجوم عبر الفضاء السيبراني يهدف إلى السيطرة على مواقع إلكترونية، أو بنى تحتية محمية إلكترونيا لتعطيلها، أو تدميرها، أو الإضرار بها"[23].

أما في اللغة العربية، نسجل تحديا حقيقيا وصعوبة جمة في اختيار مصطلح مقارب لمصطلح (cyber)، و ما يوضح تلك الصعوبة على سبيل المثال؛ الترجمة العربية لعنوان اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية كانت ترجمة غير صائبة، إذ ترجم العنوان (Convention on Cybercrime) إلى (الاتفاقية المتعلقة بالجريمة السيبرانية) ويعود السبب في ذلك إلى عدم وجود مصطلح مناظر في اللغة العربية[24].

---

[22]-دحان حزام القريطي، الأمن السيبراني وحماية أمن المعلومات، مرجع سابق، ص.11.

[23]-أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، منشورات زين الحقوقية والأدبية، بيروت، ط غ، 2018، ص.11-12.

[24]-المرجع نفسه، ص.12.

أما سبب اختيارنا لمصطلح السيبرانية في هذه الرسالة، فيعود إلى المصطلح الذي استخدمه "نوربرت وينر" "Norbert Wiener"[25] في أواخر الأربعينيات[26]. فهو الأب الروحي المؤسس للسبرنيتيقية من خلال مؤلفه الشهير " cybernetics or control and communication in the animal and the machine"

وأشار في كتابه إلى أن السبرنيتيقية هي التحكم والتواصل عند الحيوان والآلة والإنسان، ليستبدل مصطلح الآلة بعد الحرب العالمية الثانية بالحاسوب[27]. وكذلك تم استخدام مصطلح السيبرانية في وثائق الأمم المتحدة الصادرة باللغة العربية[28].

يمكن تأريخ ظهور مصطلح السيبرانية، كتخصص علمي مع نشر كتاب نوربرت وينر، **"السيبرانية"** في عام 1948 والذي، على الرغم من كونه تقنيًا للغاية، فقد بيعت منه 30000 نسخة بمجرد نشره. دخلت السيبرانية إلى أوروبا من خلال كتاب نوربرت وينر:

---

[25]-**"نوربرت وينر" "Norbert Wiener"**: وُلد نوربرت وينر في كولومبيا بولاية ميسوري. كان والده، أستاذ اللغات السلافية في جامعة هارفارد، زميلًا لودفيك ليجزر زامنهوف في وارسو. طفل معجزة، كان نوربرت يستطيع القراءة في سن سنة ونصف وتلقى تعليمه في المنزل حتى سن السابعة. ثم أقام لفترة وجيزة في المدرسة قبل أن يكمل تعليمه الابتدائي في المنزل. في عام 1903، عاد إلى مدرسة آير الثانوية حتى تخرج منها عام 1906. في سبتمبر 1906، في سن 11، التحق بجامعة تافتس لدراسة الرياضيات. تخرج عام 1909 ثم التحق بجامعة هارفارد حيث درس علم الحيوان. ولكن في عام 1910، التحق بجامعة كورنيل ليبدأ درجة البكالوريوس في الرياضيات. في العام التالي عاد إلى هارفارد حيث بدأ أطروحة حول المنطق الرياضي. حصل على الدكتوراه عام 1912. كان عمره 18 عامًا فقط. بعد دفاعه عن أطروحته، غادر إلى أوروبا، وأقام أولاً في كامبريدج حيث عمل أستاذا في بيرتراند راسل وجودفري هارولد هاردي، ثم في غوتنغن حيث تابع دورات إدموند لانداو وديفيد هيلبرت. ثم عاد إلى كامبريدج، ثم إلى الولايات المتحدة. بين عامي 1915 و 1916، درس الفلسفة في جامعة هارفارد، قبل أن يعمل في شركة جنرال إلكتريك ثم في موسوعة أمريكانا. بتحريض من أوسكار فيبلين، أجرى بعد ذلك بحثًا عن المقذوفات في ساحة اختبار أبردين في ماريلاند. بقي هناك حتى نهاية الحرب، وبعد ذلك حصل على منصب أستاذ الرياضيات في معهد ماساتشوستس للتكنولوجيا (MIT). في عام 1926 تزوج من مارغريت إنجمان وعاد إلى أوروبا على منحة دراسية من مؤسسة غوغنهايم. أمضى معظم وقته في جوتنجن أو كامبريدج مع هاردي. عمل بشكل خاص على الحركة البراونية، وتحويل فوريه، ومشكلة ديريتشليت، والتحليل التوافقي ونظريات Tauberian. حصل على جائزة بوشر عام 1933. خلال الحرب العالمية الثانية، رفض المشاركة في مشروع مانهاتن (مشروع تطوير القنبلة النووية)، بينما كان يعمل بنشاط في البرنامج المضاد للطائرات، مما شجعه على تجميع أبحاثه المختلفة حول نظرية الاتصال. في عام 1943، مع مساعديه Julian Bigelow & Arturo Rosenblueth، اقترح نظام DCA جديد يمكن أن يتنبأ بمسار الطائرة المستهدفة من نموذج يحلل سلوك الطيار مع العلم أنه كان يطارد. من عام 1946 إلى عام 1950، شارك في الاجتماعات الشهيرة متعددة التخصصات المسماة مؤتمرات Macy وفي 1947-1948، قام بإضفاء الطابع الرسمي على المبدأ المركزي لهذه المؤتمرات تحت اسم علم التحكم الآلي. بعد الحرب، وفقًا لفيليب بريتون، الذي أصيب بصدمة من مشاركة العلماء في مآسي هيروشيما وأوشفيتز، أصبح رسولًا لدين علماني جديد: يوتوبيا التواصل: اقترح رؤية جديدة للعالم. كانت المعلومات والاتصالات العناصر الأساسية. توفي يوم18 مارس سنة 1964، عن سن (70 سنة) بمدينة ستوكهولم، السويد.

(Techno-Science.net, Norber Wienner, lien de l'article : http://bitly.ws/HHup, date visite : 08.06.2023).

[26]-أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، مرجع سابق، ص ص،12-13.

[27]-دحان حزام القريطي، الأمن السيبراني وحماية أمن المعلومات، مرجع سابق، ص ص،11-12.

[28]-أحمد عبيس نعمة الفتلاوي، المرجع نفسه، ص ص،12-13.

"السيبرانية"، الذي نُشر في باريس عام 1948. ويُعرَّف بأنه المجال الكامل لنظرية التحكم والاتصال، سواء في الآلات أو في الحيوانات. وما يقارب نصف الكتاب مخصص لسرد نظريات الفيزياء الرياضية، التي لم تكن تقريبًا معروفة في أوروبا، وللتطوير الذي ساهم فيه كل من وينر وطلابه بشكل كبير، والمرتبط أساسا بميكانيكا جيبس الإحصائية و نظرية السلاسل الزمنية، حيث تكون مساهمة وينر نفسه ذات أهمية خاصة ،في ما يسمى بـ "نظرية المعلومات" لشانون[29].

في الواقع كان هذا العمل عبارة عن توليفة من العمل المنجز منذ أربعينيات القرن الماضي من جانب الأنجلو أمريكي. وفكرة السيبرانية، أو باللاتينية (grec kubernêtikê, de kubernân, gouverner)، مصطلح له ارتباط بمصطلح "القيادة"، وبالضبط قيادة السفن[30] .

في القرن التاسع عشر، أشار أندريه ماري أمبير"André-Marie Ampère" (الفيزيائي ومؤسس ديناميك-الكهربائ 1775-1836) في تصنيف العلوم الذي اقترحها، وأشار إلى "السيبرانية"، أوعلم التحكم الآلي، ووصفها بأنها "علم حكومة الرجال"[31]. أما بالنسبة لعالم الرياضيات الأمريكي نوربرت، فقد بدأ في استخدام كلمة السيبرانية، أوعلم التحكم الآلي، لوصف أنظمة التحكم المحوسبة. وفقًا لـوينر "Wiener"، يتعامل علم السيبرانية مع العلوم التي تتعامل مع التحكم في الآلات والكائنات الحية، من خلال التواصل والتعليقات. وفقًا للنموذج السيبراني، تبادل المعلومات والتلاعب بها يتم عبر استخدامها في البيولوجية والفيزيائية وأنظمة كيميائية. ينطبق علم التحكم الآلي فقط على أنظمة شبيهة بالآلة، حيث الوظيفة- للنظام والنتيجة النهائية يمكن أن يكون تصميمها وتحديدها رياضيًا، أو على الأقل توقعها. النظام السيبراني هو نظام مغلق، غالبًا ما يتم عرض البادئة "cyber" جنبًا إلى جنب مع أجهزة الكمبيوتر والروبوتات. صاغ "وليام جيبسون"، وهو روائي خيال علمي، مصطلح الفضاء السيبراني في روايته Neuromancer(جيبسون 1984). يعتبر

[29]-Louis COUFFIGNAL, La cybernétique, presses universitaires de France, Paris, Ed.1, 1963, p.6.
[30]-Ivan LAVALLEE, Cyber Révolution et Révolution Sociale, les temps de Cerises, France, 2022, pp.205-206.
[31]- Ibid.

أدب الخيال العلمي وتصور أفلام الفضاء السيبراني جيبسونيان، أوالمصفوفة، كمعلومات عالمية محوسبة، شبكة يتم فيها ترميز البيانات في ثلاثي الأبعاد، شكل متعدد الألوان. يدخل المستخدمون عبر واجهة الكمبيوتر، حيث بعد ذلك يمكنهم "الطيران" عبر الفضاء لاستكشاف المناطق الحضرية عن طريق دخول بيانات المباني[32].

وثمة تعريفات أخرى للفضاء السيبراني، فالاتحاد الدولي للاتصالات ووكالة الأمم المتحدة المتخصصة في مجال تكنولوجيا المعلومات والاتصالات تعرفه بأنه الحيز المادي وغير المادي الذي ينشأ ،أو يتكون من جزء، أو من كل العناصر التالية: حواسيب ،أجهزة ممكنة، شبكات، معلومات محوسبة، برامج ، مضامين، معطيات مرور، رقابة ومستخدمون لكل ذلك)، والفضاء السيبراني هو مجال عالمي داخل بيئة المعلومات تم تشكيله من خلال استخدام الإلكترونيات ...واستغلال المعلومات عبر الشبكات المترابطة والمرتبطة باستخدام تكنولوجيا المعلومات والاتصالات. ويمكن تعريفه على أنه امتداد للوسائط الرقمية عبر خطوط نقل مختلفة، معدنية، وألياف بصرية ولا سلكية وقنواتها على شبكات الإنترنت، إذ يعد الفضاء السيبراني التعبير التكنولوجي الفائق السرعة للمعلومات. كما عرفته الوكالة الفرنسية لأمن أنظمة الأعلام ANSSI ( وهي وكالة حكومية مكلفة بالدفاع السيبراني الفرنسي )على أنه :فضاء التواصل المشّكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية). وهناك من يرى فيه واحداً من سبع مجالات إلى جانب الجو، الفضاء الخارجي، البحر، البر، الفضاءين الألكترو-مغناطيسي والإنساني، وأنه( ساحة الحرب الخامسة) بعد البر، البحر والجو[33].

## شمال إفريقيا

أشارت بعض الدراسات أن شمال إفريقيا يشمل كلا من مصر، ليبيا، تونس، الجزائر والمغرب[34]، وقسمت المنطقة إلى المشرق (مصر وليبيا) والمغرب العربي (تونس، الجزائر، المغرب). وإذا أردنا أن نكون أكثر دقة، يجب أن نأخذ في الاعتبار الحقيقة أن ليبيا

[32]-Martti Lehto, The Cyberspace Threats and Cyber Security Objectives in the Cyber Security Strategies, **ResearchGate**, 01.09.2015, link: http://bitly.ws/DkAm, seen on, 21.04.2023.

[33]-تغريد صفاء و لبنى خميس مهدي، أثر السيبرانية في تطور القوة، مجلة حمورابي، العراق، العدد 33-34، 2020، ص ص،149-150.

[34]-International federation of Red Cross and Red Crescent Societies, North Africa, 31.01.2010, link: http://bitly.ws/Dppi, seen on 23.04.2023.

جزء من كل من هذين الكيانين؛ فقد تم استخدام اسم ليبيا لأول مرة بواسطة "Homer"، حيث تم استخدامه على الأرجح من طرف المصريين الذين تعرضوا لضغوط من قبل ليبو – وبالتالي ليبيا، البربر الصحراويين الذين سعوا لاختراق وادي النيل طمعا في خيرات المنطقة. وخلال العصور القديمة، تم ترسيم الحدود بين المنطقتين من خلال "مذبحة Philenes"، التي بنيت في قاع خليج سيرتي العظيم؛ الخليج الفاصل بين برقة و طرابلس حيث تلتقي الطرق المتقاطعة والساحلية والمسارات العابرة للصحراء المؤدية إلى أحواض النيجر وتشاد عبر فزان[35].

في حين ربطت دراسات أخرى شمال إفريقيا بالمغرب الأقصى، الجزائر وتونس[36]. وعرفت القرون الوسطى والعصور الحديثة الدول البربرية أو بلاد البربرية. وفي القرن التاسع عشر وضع الجغرافيون عبارة إفريقيا الصغرى ليدلوا على وجود قارة صغيرة واقعة ضمن قارة كبيرة، وعبارة بلاد الأطلس لتأكيد أهمية تشكل الصخور"Tectonique"، وكثيرا ما تجري على الألسن لفظة إفريقيا الشمالية الفرنسية وذلك من الوجهة السياسية. وفي بعض الأحيان تستعمل لفظة شمال إفريقي، وفي هذا مزج جديد لا طائل تحته بين إفريقيا الشمالية والشمال الإفريقي[37].

واليوم لا يعرف عامة الناس أن المغرب الأقصى والجزائر وتونس آهلة بالبربر، ويعمدون إلى تسميتهم عربا. أما الأهالي فكثيرا ما كانوا يسمون أنفسهم أمازيغ( مؤنثه تمازيغت وجمعه أمازيغن)، ومعناه " الرجال الأحرار"، ثم " النبلاء ." وقد أطلق هذا الاسم على قبائل عديدة قبيل الاحتلال الروماني[38].

وإذا ماعرفنا شمال إفريقيا، فلن تستقيم هذه الدراسة دون التعريج على المحورين الرئيسيين، موضوع الدراسة، المغرب والجزائر.

---

[35]-Bernard Lugan, Histoire de l'Afrique du Nord (Égypte, Libye, Tunisie, Algérie, Maroc) Des origines à nos jours, Éditions du Rocher, Monaco, Groupe Artège, 2016, p.7.

[36]-شارل أندري جوليان، تاريخ إفريقيا الشمالية تونس، الجزائر، المغرب الأقصى، من البدئ إلى الفتح الإسلامي 647م، ترجمة محمد مزالي والبشير بن سلامة، مؤسسة تاوالت الثقافية، ليبيا، ط 2، 2011، ص.7.

[37]-المرجع نفسه.

[38]-المرجع نفسه.

## المغرب

مصطلح لغوي ذو دلالات جغرافية، قصد به الكتاب العرب الاتجاه الأصلي الذي يحدد مغرب الشمس، على عكس المنطقة الواقعة في شروق الشمس والتي تسمى بالمشرق، أما لفظ العربي فإنه امتداد لحيز الدول العربية، وهو مفهوم حضاري إيديولوجي، لكن إذا كانت تسمية المغرب العربي هي المتداولة في الأوساط الرسمية، فإن المنطقة عرفت عدة تسميات كالمغرب الكبير وهو مفهوم له قيمة مادية كمية وذو خلفية سياسية محضة ولا يرتبط بالقيم الإيديولوجية والحضارية، كما نجذ لفظة "شمال إفريقيا"، والتي تستعمل كثيرا في الأطروحات الأجنبية وهي تسمية عمودية ذو توجه جغرافي تاريخي، رغم أن أغلب الكتاب العرب لاسيما المغاربة منهم، يعتقدون أن توظيف هذا المصطلح ينم عن رغبة هؤلاء في سلخ الهوية العربية عن دول المغرب العربي، كما سميت باسم "بلاد البربر "نسبة إلى السكان الأوائل الذين استقروا بالمنطقة، وتطرح هذه التسمية إشكالا حول أصلها، إلا أنه ومهما يكن من أمرها، فإن أغلب المصادر ترجع هذا اللفظ إلى الحضارة الرومانية التي أطلقتها على الشعوب التي لا تتكلم اليونانية عموما، لأن البربر– كما تمت تسميتهم -كثيرا ما كانوا يسمون أنفسهم بالأمازيغ أي الرجال الأحرار. و إجمالا فان تسمية المغرب العربي تنم إضافة إلى ما سبق عن تميز هذا الفضاء، عربيا عن الغرب ومغربيا عن العربي[39].

يضم المغرب العربي كلا من ليبيا، موريطانيا، تونس، الجزائر والمغرب. وإذا ما ركزنا على المغرب، فهذا الأخير يعتبر أكبر بقليل من ولاية كاليفورنيا، ويحتل الركن الشمالي الغربي الاستراتيجي لإفريقيا، حيث يلتقي البحر الأبيض المتوسط بالمحيط الأطلسي. يطل المغرب على أضيق جزء من مضيق جبل طارق- القناة التي تربط البحر الأبيض المتوسط بالمحيط الأطلسي- على بعد 13 كم (8 ميل) فقط من إسبانيا. في حوزة المغرب خط ساحلي يبلغ 1110 كم (690 ميل) وحدود برية تمتد على طول 2046 كم (1270 ميل)[40].

---

[39]-سعيدي ياسين، التحديات الأمنية الجديدة في المغرب العربي، رسالة لنيل شهادة الماستر في العلوم السياسية والعلاقات الدولية، جامعة وهران محمد بن أحمد 2، كلية الحقوق والعلوم السياسية، الجزائر، السنة الجامعية، 2015-2016، ص.41.

[40]-Defense Langage Institute Foreign Language Center , **DLIFLC**, Cultural Orientation-Moroccan, link: http://bitly.ws/ExDL, seen on 15.05.2023, p.06.

فالمغرب جزء من المغرب العربي (أو المغرب، ويعني "الغرب" باللغة العربية)، مما يشير إلى الجزء الغربي من شمال إفريقيا. للمغرب حدود برية مع الجزائر من الشرق والجنوب الشرقي، إلى جانب الصحراء المغربية المتنازع عليها في الجنوب. يقع المحيط الأطلسي في غرب المغرب، والبحر الأبيض المتوسط في شماله. على الرغم من أن البر الرئيسي لإسبانيا يقع على بعد 13 كم (8 ميل) شمالًا عبر مضيق جبل طارق، يشترك المغرب في حدود برية مع الدولة الأوروبية في جيبين مستعمرين إسبانيين صغيرين على البحر الأبيض المتوسط: مدينتي سبتة ومليلية المغربيتين. تشترك موريتانيا في حدود برية مع الصحراء المغربية[41] .

## الجزائر

عموما تسمية الجزائر يقصد بها الإقليم الواقع غرب الخلافة الإسلامية باتجاه غروب الشمس، عكس البلاد الواقعة في اتجاه شروق الشمس وهي بلاد المشرق[42].

ويشير ابن خلدون الخبير بأوضاع المغرب الأوسط(الجزائر)، إلى أنه بلد زناتة الواقعة ما بين الزاب شرقا ونهر ملوية غربا، وهو الوادي المعروف قديما بملوشة، وهي حدود ثابتة تقريبا من الغرب لم تتغير إلا في بعض الأوقات والحالات. واعتبر المنطقة الممتدة من الجزائر إلى بجاية ودواخلها بلاد صنهاجة الشمال، وعاصمتها مدينة "أشير" بولاية المدية حاليا، وكذلك حيث كانت تستقر قبيلة زواوة وجعل المنطقة الممتدة من بجاية إلى ما وراء قسطنطينة، تقطنها قبائل كتامة، وعجيسة وجراوة. غير أن هذا التقسيم استند إلى توزيع قبلي صرف لمرحلة ما قبل القرن 11م. 5ه [43].

وحدد الجغرافي الإدريسي إقليم المغرب الأوسط(الجزائر)، في نهاية القرن 12م.6ه بقوله: "ومدينة بجاية في وقتنا، مدينة المغرب الأوسط، وعين بلاد بني حماد، ومدينة تلمسان قفل بلاد المغرب الأوسط". ولم يختلف معه الجغرافي "ابن سعيد المغربي(1287م-685ه)

---

[41]-Defense Langage Institute Foreign Language Center, Cultural Orientation- Moroccan, Op.cit, p.06.

[42]-عبد العزيز فيلالي، بحوث في تاريخ المغرب الأوسط في العصر الوسيط، دار الهدى- عين المليئة، الجزائر، ط غ، 2020، ص ص.11-12.

[43]-المرجع نفسه.

لاعتباره مدينة بجايا قاعدة المغرب الأوسط[44]. أما الحدود الشرقية، ففي أغلب الأحيان، امتدت إلى ما وراء بونة، كم أشار إلى ذلك المؤرخ عبد الواحد المراكشي(1249-647ه) بقوله" ومدينة بونة هي أول بلاد إفريقية". واتفق معه ابن سعيد المغربي، حيث جعل :"أول سلطة إفريقية على البحر مدينة بونة"، وضبط عبد الرحمان بن خلدون، الحدود الجنوبية للمغرب الأوسط إلى ورجلان والصحراء في عهد بني حماد[45].

## إشكالية البحث

من الواضح اليوم أن الغالبية العظمى من التغييرات في العالم الحقيقي أضحت تنعكس على الفضاء السيبراني. لهذا السبب وجب علينا أن ندرك تمام الإدراك، أن كل صراع، مهما كان سياسيا أو عسكريا، من المحتمل أن يتطور إلى صراع سيبراني خطير، بل قد تحل المواجهة السيبرانية في بعض الأحيان محل التصادم العسكري التقليدي[46].

وحتى مفهوم القوة الذي ارتبط أساسا و لعقود كثيرة بالشكل الصلب للقوة العسكرية، أضحى أمرا غير مقبول مع التطورات العلمية والتقنية، بل صار واجبا إحداث تغييرات على ذلك المفهوم، لكي يواكب متغيرات النظام الحديث، الذي خيم فيه ظهور الأنترنت وتأثيره على القيم السياسية وتوجهات الفاعلين من الدول ومن غير الدول. وبناء عليه، لم تبق القوة منحصرة على الفاعلين من الدول، بل سطعت إلى الوجود فواعل جديدة، استطاعت منح القوة بعدا آخر لا يقتصر على البعد المادي وإنما يتعداه للأبعاد المعنوية والسيبرانية[47]. ظهر إذن شكل جديد من القوة؛ هو القوة السيبرانية "Cyber power" التي لها تأثير كبير على المستوى الدولي والمحلي، وهو ما يعني تغيرات في علاقات القوى في السياسات الدولية[48].

عرفت هذه التغييرات طريقها إلى شمال إفريقيا بصفة عامة، وإلى المغرب والجزائر بصفة خاصة. وبات الدفاع السيبراني من المجالات السياسية الأمنية التي تزعج البلدين، وتؤرق مضجعي فاعليهما رسميين كانوا أو غير رسميين. من هنا برزت **إشكالية الرسالة، التي ارتبطت أساسا بالقيام بمقارنة التجربتين المغربية والجزائرية في مدى قدرة دفاعيهما**

---

[44]-عبد العزيز فيلالي، بحوث في تاريخ المغرب الأوسط في العصر الوسيط، مرجع سابق، ص ص،11-12.

[45]-المرجع نفسه.

[46]-Yoann ROBERT, Cyber défense : La prise de conscience étatique, **EGE école de guerre économique**, 01.09.2019, lien de l'article : http://bitly.ws/DwSE , date visite, 26.04.2023.

[47]-تغريد صفاء و لبنى خميس مهدي، أثر السيبرانية في تطور القوة، مجلة حمورابي، مرجع سابق، ص ص،145-146.

[48]-دحان حزام القريطي، الأمن السيبراني وحماية أمن المعلومات، مرجع سابق، ص.17.

**السيبرانيين في مواجهة التحديات الأمنية السيبرانية وكيفية تنظيمهما وطنيا، إقليميا ودوليا.**

## الأسئلة الفرعية

تفرعت عن هذه الإشكالية مجموعة من الأسئلة الفرعية التي حاولت الدراسة الإجابة عليها؛

-كيف يمكن تناول دراسة الدفاع السيبراني في المغرب والجزائر من منظور نظريات العلاقات الدولية الثلاث؛ الواقعية، الليبرالية والنقدية؟

-ماهي تداعيات التهديدات السيبرانية الداخلية والخارجية تجاه البلدين المغرب والجزائر؟

-كيف يبنيان هيكليهما التنظيميين لتحقيق الدفاع السيبراني بهما؟

-ماهي الاستراتيجيات الأمنية والقوانين المنظمة للفضاء السيبراني بكلا البلدين؟

-ماهي المؤسسات المحورية والتعاونات الإقليمية والدولية للبلدين في إطار مواجهة التحديات السيبرانية؟

## فرضيات الدراسة

-في وجود انتقادات موجهة إلى النظريات الفكرية الثلاث؛ الواقعية، الليبرالية والنقدية يبقى من الصعب الجزم بإمكانية الاعتماد على نظرية واحدة دون غيرها لدراسة واقع الدفاع السيبراني في شمال إفريقيا، وبالضبط في المغرب والجزائر. وبناء عليه، وحتى تكتمل الرؤية حول واقع الدفاع السيبراني في المغرب والجزائر، لابد من الاعتماد على تلك النظريات الثلاث. وهذا لا يمنع من الانفتاح على نظريات أخرى لاستكمال وتوضيح رؤية أكثر حول هذا الواقع؛

-في غياب تعامل أكاديمي محايد وهيمنة الجهاة الرسمية على المعطيات الواردة حول الواقع السيبراني الجزائري، يحتم على الباحث اللجوء إلى المؤشرات العالمية لدراسة الحالة السيبرانية في الجزائر؛

-ضبابية القانون الدولي في المجال السيبراني، يؤثر سلبا على تفعيل القوانين الداخلية المعتمدة من طرف البلدين، المغرب والجزائر، لتأطير الحقل السيبراني بهما؛

-رغم وجود مؤسسات فاعلة في المجال السيبراني في البلدين، فغياب تعاون إقليمي بينهما يفرمل عجلات النمو في شمال أفريقيا؛

-وجود اتفاقيات إقليمية ودولية في الميدان السيبراني تبقى من النقط الإيجابية، غير أنها غير كافية إذا لم تتوفر إرادة التعاون بين مختلف البلدان؛ المغرب والجزائر نموذجا.

**الفرضية الرئيسة للبحث:** تفترض هذه الرسالة جوابا على الإشكالية أعلاه، التي ارتبطت أساسا بالقيام بمقارنة التجربتين المغربية والجزائرية في مدى قدرة دفاعيهما السيبرانيين في مواجهة التحديات الأمنية وكيفية تنظيمهما وطنيا، إقليميا ودوليا. يتبين أنه لا يمكن دراسة الواقع السيبراني المغربي الجزائري دون استحضار بعض النظريات الفكرية، ودون الاعتماد على تقاطع توجهاتها. كون الاعتماد على نظرية واحدة لا يكفي للإحاطة بجميع جوانب الظاهرة الاجتماعية المدروسة.

ويتضح أن التجربتين المغربية والجزائرية تسعيان لإثبات ذاتهما في مجال الدفاع السيبراني باعتمادهما على مجموعة من الآليات الساعية لمواجهة التحديات السيبرانية، غير أن تلك المحاولات لا ترقى إلى المبتغى، خصوصا من جانب الجارة الجزائرية، في ظل التطور السريع للهجمات السيبرانية وتعاون مغاربي ضئيل مع غياب الانسجامية لمواجهة هذه المعضلة. ومما يزيد الأمر تعقيدا وسوءا، عداء الجزائر التقليدي تجاه المغرب، والذي تقمص حلة جديدة؛ حلة العداء السيبراني. فبدل تظافر الجهود بين دول شمال إفريقيا، المغرب والجزائر نموذجا، لمواجهة هذه الآفة الخطيرة، لا تفوت الجزائر أي فرصة لتوجيه اتهاماتها الواهية المرجع للمغرب بكونه(حسب معتقدات الفاعلين الرسميين الجزائريين) مصدر هجمات سيبرانية ضدها.

## حدود الدراسة

**المجال المكاني:** يتحدد المجال المكاني لهذه الدراسة انطلاقا من عنوانها. والعنوان ارتبط أساسا بالدفاع السيبراني في شمال إفريقيا، وبالضبط في المغرب والجزائر. وذلك بغرض قياس مدى قوة وجاهزية الدولتين في الدفاع السيبراني في حيزهما المكاني، والقيام بمقارنتهما مع بعضهما البعض.

**المجال الزماني:** إذا كانت جل الدراسات العلمية يسهل حصرها من حيث المكان، فالأمر يختلف معها من حيث الزمان، وهذا راجع إلى حركية واستمرارية تفاعلات الظواهر الإنسانية والاجتماعية وترابطها المعقد، فغالبا ما يجد الباحث نفسه أمام ظواهر قديمة بتفاعلات جديدة. والظاهرة السيبرانية لم تسلم هي الأخرى من هذه الخاصية، وإن ارتبطت أساسا بالطفرة التقنية التي حصلت في مضمار المعلوميات، ومع ذلك فجدورها امتدت إلى حقبة أبعد من القفزة العلمية العالمية.

منهج الدراسة: اعتمدت الدراسة على المناهج التالية: **المنهج النسقي**؛ يعتمد المنهج النسقي على فكرة مركزية، مرتبطة ببناء نموذج من التفكير، يتسم بالشمولية وقادر على دراسة التفاعلات الدينامية. وليس السببية وإدراك الأنساق باعتبارها مجموعات ساكنة بل مجموعات متحولة[49].استفاد هذا التوجه في التحليل من علم البيولوجيا وعلم التوجيه ونظريات الاتصال، قبل أن يطور نظرياته التي انبثقت من رواده الثلاثة: "بارسونز" ونظريته حول " الفعل الاجتماعي"، وديفيد إستون و "فكرة النظام"، ثم "غبرييل إلموند" ونظريته "المتعلقة بالوظيفة".

اعتمدت دراسة إشكالية الموضوع، المتمثلة في الدفاع السيبراني في شمال إفريقيا المغرب والجزائر نموذجا، على المنهج المذكور أعلاه، وذلك من خلال إيجاد مدخلاتها المتمثلة في كيفية تعامل البلدين في مجال دفاعهما السيبراني، و إبراز مخرجاتها المتضمنة في مدى قوة استراتيجيتي البلدين في مضمار السيبرانية، وتجلية تغذيتها الراجعة التي أسفرت عن بعض التوصيات الضرورية لنجاح الدفاع السيبراني في البلدين .

-أما **المنهج المقارن**، هو نوع من الأساليب التي تحلل الظواهر ثم تجمعها معًا للعثور على نقاط التمايز والتشابه. ينصب تركيز البحث المقارن على أوجه التشابه والاختلاف بين الظواهر والحالات. ويعني التحليل المقارن وصف وشرح أوجه التشابه والاختلاف في المواقف، أو العواقب بين نطاق واسع من الوحدات الاجتماعية مثل المناطق والأمم والمجتمعات والثقافات. يعكس هذا التعريف مقارنات مثل المقارنة عبر الثقافات في الأنثروبولوجيا، والمقارنة عبر المجتمع في علم الاجتماع، والمقارنة عبر المستوى الوطني

[49]-إبراهيم أبراش، المنهج العلمي وتطبيقاته في العلوم الاجتماعية، دار الشروق للنشر والتوزيع، عمان الأردن، ط1، 2009، ص. 126.

في العلوم السياسية. البحث أو التحليل أو المنهج المقارن هو مصطلح واسع يشمل المقارنة الكمية والنوعية. قد تستند الكيانات الاجتماعية إلى خطوط عديدة، مثل الخطوط الجغرافية أو السياسية في شكل مقارنات عبر المستوى الوطني أو الإقليمي[50]. لهذا السبب، اعتمدت الدراسة على المنهج المقارن، حتى يتسنى لنا مقارنة الدفاعين السيبرانيين للبلدين؛ المغرب والجزائر، والوقوف على مدى جدية كل واحد منهما.

كذلك اعتمدت الدراسة على **المنهج المؤسسي القانوني**. شكل هذا المنهج، رغم تعرضه لانتقادات حادة من بعض المدارس الحديثة، أحد أهم المناهج التي استعملت قديما لدراسة الأنظمة السياسية، بل هناك من يرى استمرار الحاجة إلى إعماله من أجل إحاطة شاملة ببعض الظواهر السياسية. ينظر المنهج المؤسسي القانوني إلى النظام السياسي كمرادف لنظام الحكم وبذلك ينصرف لدراسة مؤسساته[51]، ويعتقد أنصاره الذين يعتبرون الدولة وحدة التحليل أن جوهر التقدم السياسي يكمن في بناء المؤسسات السياسية[52]. وبناء على ما سبق، وبما أن الرسالة ارتبطت بالدولتين؛ المغرب والجزائر، ودور مؤسساتهما في تحقيق دفاع سيبراني بهما، استوجب البحث استحضار المنهج المؤسسي القانوني.

خطة الدراسة: ارتأت الدراسة تناول الموضوع من خلال فصلين:

**الفصل الأول:** الدفاع السيبراني في المغرب والجزائر وتداعيات التهديدات السيبرانية عليهما؛

**الفصل الثاني:** الهيكل التنظيمي للدفاع السيبراني في المغرب والجزائر.

---

[50]-محمد تيسير، المنهج المقارن في البحث العلمي، **مؤسسة المجلة العربية للعلوم ونشر الأبحاث**، 24.11.2022، رابط المقال:https://rb.gy/upppw، تاريخ الدخول: 25.04.2023.

[51]-علي الدين هلال ونيفين مسعد، النظم السياسية العربية قضايا الاستمرار والتغيير، **مجلة الكتب العربية**، رابط الكتاب: http://bitly.ws/KFiT، تاريخ الدخول: 06.07.2023، ص 87.

[52]-كمال المنوفي، مقدمة في مناهج وطرق البحث في علم السياسة، جامعة القاهرة، ط غ، 2006، ص.28.

## الفصل الأول: الدفاع السيبراني في المغرب والجزائر وتداعيات التهديدات السيبرانية عليهما

يقتضي البحث في الجانب النظري للدراسات الأمنية استحضار نظريات العلاقات الدولية، العلوم الإنسانية والاجتماعية بشكل عام. فلا يمكن لأحد أن يدعي تمكنه من فرع من فروع المعرفة دون إلمامه بالنظريات المؤطرة لتلك المعرفة. قد يظن هذا الشخص أن بمقدوره التقدم بشكل أكبر في بحثه عبر الركون إلى التجارب والخبرات السابقة، ودون الاعتماد على أي نظرية، أو مبادئ معينة عامة، لكن الواقع أثبت عكس ذلك، وأوضح حتمية الاعتماد على النظريات لتعبيد مسلك الباحث[53].

وإذا ما حاولنا الرجوع إلى الماضي القريب، نجد أن عالم نظريات العلاقات الدولية كان بسيطا نسبيا إلى غاية منتصف الثمانينات؛ مرحلة سيطرة الواقعية والليبرالية الجديدتين على النقاش داخل الولايات المتحدة الامريكية. غير أن نهاية الحرب الباردة شكلت نقطة تحول نظري مميزة في طبيعة النقاش حول نظرية العلاقات الدولية. فنهاية الحرب الباردة أوضحت حدود المنظار المهيمن على التفسير وقدرته على التنبؤ. كما أن تأثير ظاهرة العولمة فتح الباب على مصراعيه أمام دارسي العلاقات الدولية للذهاب أبعد من المسائل التقليدية التي تمس أسباب الحروب والتعاون. وأعادت العولمة بعث النقاشات المرتبطة بدور وقدرة الدولة، مفهوم السيادة والفواعل الجديدة على الساحة الدولية. كما أنها لم تغيب أهمية المقاربات الاقتصادية في العلاقات الدولية. ومن هذا المنطلق باتت الوظيفة الرئيسية لنظرية العلاقات الدولية تتمثل في تمكيننا من تحسين معرفتنا بالواقع الدولي سواء في فهمه فقط أو لتغييره. إنها تساعدنا على تنظيم معلوماتنا السابقة و اكتشاف معلومات جديدة أكثر دقة[54].

ومن المعلومات الجديدة التي صارت تؤرق مضجع الباحثين، نسجل تواجدا ملموسا للاتصالات والحوسبة الحديثة في حياتنا اليومية. هذا التواجد والاعتماد المتزايد على شبكات

---

[53]-قسوم سليم، الاتجاهات الجديدة في الدراسات الأمنية دراسة في تطور مفهوم الأمن عبر منظارات العلاقات الدولية، رسالة لنيل شهادة ماستر في العلوم السياسية والعلاقات الدولية، جامعة الجزائر، كلية العلوم والإعلام قسم العلوم السياسية والعلاقات الدولية، الجزائر، السنة الجامعية، 2009-2010، ص ص، 36-38.

[54]-المرجع نفسه.

التواصل يوفر فرصًا للوكلاء الراغبين في استغلال نقاط ضعف الأنظمة. يتراوح هؤلاء العملاء من الدول القومية إلى الجهات الفاعلة غير الحكومية[55].

ولفهم هذا التواجد الجديد المؤثر في حقل العلاقات الدولية، لا بد من معرفة الأدبيات أو النظريات الفكرية المتعارف عليها، لكن ما يعاب على تلك النظريات المؤطرة للعلاقات الدولية، أن تيارها السائد له ارتباط وطيد بالتاريخ الغربي المتداخل مع النظرية السياسية الغربية. فالواقعية، مثلا، هي فكرة تجريدية تتأتى من ميزان القوة الأوروبية للقرن الثامن عشر، من السلوك المقترن بالقرنين السادس عشر والسابع عشر، وبالطبع، من النظرية السياسية اليونانية القديمة. أما الليبرالية، فهي فكرة تجريدية تتأتى من المنظمات الحكومية الدولية للقرنين التاسع عشر والعشرين، ومن نظريات الاقتصاد السياسي. وفي حين أن الماركسية تعد تجريدا من فرع آخر ينبثق من نظريات القرنين التاسع عشر والعشرين الأوروبية، المتعلقة بالاقتصاد السياسي وعلم الاجتماع التاريخي، فإن المدرسة الإنجليزية عبارة عن تجريد ينبثق من السلوك الديبلوماسي الأوروبي في القرن التاسع عشر ومن تقليد أوروبي طويل للنظرية القانونية القائمة على افتراض أن كل قانون؛ بما في ذلك القانون الدولي، يستلزم وجود مجتمع. ومن الواضح أن البنائية ليست تجريدا منبثقا من الممارسة الغربية، ولكنها نظرية مستمدة من فلسفة المعرفة الغربية. لقد بني حقل العلاقات الدولية، إلى حد بعيد، على افتراض أن التاريخ الغربي والنظرية السياسية الغربية هما تاريخ العالم ونظريته السياسية أيضا[56].

إنه من السهولة بمكان الكشف عن مغالطة هذا الافتراض، وذلك من خلال التساؤل عن الشكل الذي كانت ستبدو عليه نظريات العلاقات الدولية لو طور هذا التخصص المعرفي في مكان آخر بدلا من العالم الغربي[57]. لكن، وفي ظل غياب تواجد مكان آخر لنظريات العلاقات الدولية من غير الحقل الغربي، ارتأت الدراسة الاعتماد على النظريات الثلاث

---

[55]-Col PEC Martin, Cyber warfare schools of thought: bridging the epistemological ontological divide, Master of defense studies, Canadien Forces College , Canada, 2015, page.05.

[56]-أميتاف أشاريا و باري بوزان، تشكيل العلاقات الدولية العالمية أصول حقل العلاقات الدولية وتطوره في ذكراه المئوية، ترجمة عمار بوعشة، سلسلة عالم المعرفة، المجلس الوطني للثقافة والفنون والآداب، الكويت، عدد 502، 2023، ص ص،21-22.

[57]-المرجع نفسه، ص.22.

المهيمنة في حقل العلاقات الدولية؛ النظريات الواقعية، الليبرالية والنقدية(المبحث الأول)، وحاولت إسقاط تلك النظريات على الدفاع السيبراني المغربي و الجزائري ، وقراءتهما من منظور تلك النظريات الثلاث فقط(المبحث الثاني).

## المبحث الأول: الدفاع السيبراني في المغرب والجزائر من منظور نظريات العلاقات الدولية

لابد لكل حقل معرفي من نظرية، أو نظريات، وذلك حسب طبيعة الحقل المعرفي موضع الدراسة، والتساؤلات التي تحيط بالحقل، ومساحة الحركة المتاحة أمام الباحثين للتعاطي مع الموضوع المدروس وإثرائها بالأجوبة والأطروحات النظرية، وتأثيرات البيئة المحيطة على مجريات البحث، ومدى تقبل الموضوع للجهد النظري. فتطور النظرية وعمق التنظير يشكلان العنصر المفتاحي للوصول إلى العلم، لأن النظرية تزودنا بطرق لترتيب الحقائق (facts) وتحويلها إلى معلومات وبيانات (data). وتقوم النظرية بعد ذلك باصطفاء المعلومة المهمة والمفيدة من بين تلك المعلومات المتاحة، وتستفيد منها في عمليات الوصف والتصنيف والتحليل والتفسير والتنبؤ[58]. تركز دراسة مجموعة واسعة من نظريات العلاقات الدولية في جعل السياسة الدولية أكثر وضوحًا – وفي فهم أفضل للجهات الفاعلة والهياكل والمؤسسات والعمليات وحلقات معينة بشكل رئيسي. في بعض الأحيان تكون تلك النظريات مجبرة في اختبار الفرضيات، وفي اقتراح تفسيرات سببية بهدف تحديد الاتجاهات والأنماط الرئيسية في العلاقات الدولية - ومن هنا جاء الادعاء بأنها نظريات تفسيرية[59].

وقد تعددت تلك النظريات؛ فهناك الواقعية الكلاسيكية، النيوكلاسيكية، الليبرالية، المدرسة الإنجليزية، الماركسية، النظرية النقدية، ما بعد الحداثة، البنائية، النسوية، وهناك السياسة الخضراء[60].

---

[58]-أنور محمد فرج، نظرية الواقعية في العلاقات الدولية دراسة نقدية مقارنة في ضوء النظريات المعاصرة، مركز كردستان للدراسات الاستراتيجية، السليمانية، كردستان-العراق، ط غ، 2007، ص.87.

[59]-Scott Burchill and others, Theories of International Relations, Palgrave Macmillan, Houndmills, Basingstoke, New York, Ed3, 2005, p6 and 27.

[60]-Ibid, pp, 29-235.

وفي سبعينيات القرن العشرين –كما هو معروف ومتداول بين باحثي ومفكري الحقل – انتهى النقاش بين النظريات (الواقعية والليبرالية والماركسية) إلى تشكيل خارطة تنظير جديدة، أقصيت منها الماركسية ممثلة في نسخة التبعية، واقتصرت على بقاء كل من الواقعيين الجدد والليبراليين الجدد الذين شكلوا ما يسمى بـ "التحالف نيو- نيو". حفز هذا التحالف النظري الماركسيين كي يجدوا لهم مكانا في خارطة التنظير الجديدة، والتي يقول لسان حالها: إذ لم تستطع أن تكون لك قدرة الإبداع والمنافسة أمام الواقعية الجديدة فما عليك إلا اختيار أحد الطريقين، إما التسليم بما تقول به الواقعية الجديدة والعمل في ظل مسلماتها ومقولاتها (كما فعلت الليبرالية الجديدة رغم ادعائها بالوصول إلى نتائج مختلفة من المسلمات نفسها)، أو الاندثار والرجوع إلى أماكن الظل. إلا أن الماركسيين (تحت مسمى النقديين أو النظرية النقدية) اختاروا هذه المرة طريق المواجهة وتصعيدها إلى أقصى مداها، بحيث أعادوا في البداية تنظيم صفوفهم من خلال إعادة مراجعة شاملة لأفكارهم وأطروحاتهم وتطويرها كي تكون قادرة على البقاء والمنافسة النظرية، وفي مرحلة ثانية دخلوا في عملية تقويض شاملة لكل ما يطرحه العقلانيون فلسفيا وأنطولوجيا وأبستمولوجيا ومنهجيا وحتى قيميا. لقي هذا المشروع التقويضي احتفاء ومساندة العديد من المقاربات والتيارات النظرية الأخرى (ممثلة في ما بعد الحداثة والنسوية والبنائية) التي تعاني مع النقدية التهميش والإقصاء من طرف العقلانيين من جهة، ومن جهة أخرى تشارِكها في مشروعها الرامي إلى تقديم البديل عما تطرحه العقلانية[61].

ونظرا لأهمية تلك النظريات الثلاث؛ الواقعية، الليبرالية والنقدية، في حقل العلاقات الدولية، اكتفت الدراسة بإسقاطها على الواقع السيبراني المغربي ونظيره الجزائري، عبر مطلبين. تناولت في المطلب الأول(الدفاع السيبراني في المغرب والجزائر والمدرسة الواقعية)، وفي المطلب الثاني(الدفاع السيبراني في المغرب والجزائر من منظور النظريتين الليبرالية والنقدية).

[61]-محمد الطاهر عديلة، تطور الحقل النظري للعلاقات الدولية: دراسة في المنطلقات والأسس، أطروحة لنيل شهادة دكتوراه العلوم في العلوم السياسية والعلاقات الدولية، فـرع العلاقات الدولية، جامعة الحاج لخضر- باتنة، كلية الحقوق والعلوم السياسية قسم العلوم السياسية، الجزائر، السنة الجامعية، 2014-2015، ص.288 .

## المطلب الأول: الدفاع السيبراني في المغرب والجزائر في ضوء المدرسة الواقعية

لا تستقيم دراسة الدفاع السيبراني في المغرب والجزائر بدون استحضار النظريات الفكرية المؤطرة للعلاقات الدولية، وحتى تتضح الرؤية أكثر حول المجال السيبراني المغربي-الجزائري يبقى أجدرا الانطلاق من المدرسة الواقعية، وتسليط الضوء حول مكانتها في الفكر السياسي المغربي-الجزائري (الفرع الأول)، ثم القيام بقراءة واقعية للدفاع السيبراني في المغرب والجزائر(الفرع الثاني).

### الفرع الأول: مكانة المدرسة الواقعية في الفكر السياسي المغربي-الجزائري

يستخدم مصطلح "الواقعية" بعدة طرق وبتخصصات مختلفة؛ في الفلسفة مثلا، إنها نظرية وجودية تعارض المثالية والاسمية. الواقعية العلمية هي فلسفة علم معارضة بشكل مختلف للتجريبية، الذرائعية، التحقق والوضعية. تعارض "الواقعية" في الأدب والسينما الرومانسية، أما في العلاقات الدولية، فالواقعية السياسية هي تقليد التحليل الذي يؤكد على الضرورات التي تواجهها الدول لمتابعة سياسة القوة للمصلحة الوطنية. هذا هو المعنى الوحيد للواقعية التي سنتناولها هنا، بخلاف الإشارة إلى أن هذه الحواس المختلفة، على الرغم من أوجه التشابه العائلية الواضحة، فإنها لا توجد صلات ضرورية[62].

العديد من الواقعيين السياسيين، على سبيل المثال، هم فلسفيون اسميون وتجريبيون. يستبعد الواقعيون "الراديكاليون" كل شيء تقريبًا باستثناء القوة والاهتمام الذاتي من السياسة (الدولية). يؤكد الواقعيون "الأقوياء" على هيمنة القوة والمصلحة الذاتية والصراع مع السماح بمساحة متواضعة للقوى والمخاوف "غير الواقعية" البارزة سياسياً[63].

يقودنا هذا التقديم حول الواقعية إلى الاعتماد عليه للقيام بقراءة طبيعة العلاقة المغربية الجزائرية من زاوية المدرسة الواقعية عبر محطتين؛ محطة لتعريف النظرية الواقعية(الفقرة الأولى)، ومحطة ثانية لدراسة مكانتها في العلاقة المغربية الجزائرية(الفقرة الثانية).

#### الفقرة الأولى: ماهية المدرسة الواقعية

سجل البروز الفعلي للتيار الواقعي إبان الحرب العالمية الثانية، حيث اعتبرت الواقعية المدرسة الفكرية الأكثر هيمنة، ولا تزال حاضرة دائمًا في سياسة القرن الحادي

[62]-Scott Burchill and others, Theories of International Relations, Op.cit, pp.29-52.
[63]-Ibid.

والعشرين، بخطوطها الخمس الأساسية المرتكزة على كون؛ السياسة الدولية فوضوية، وأن الدول ذات السيادة هي الجهات الفاعلة الرئيسية في السياسة الدولية، وكذلك الدول هي جهات فاعلة، وحدوية وعقلانية تعمل وفقًا لمصالحها الوطنية الخاصة، أما الأهداف الأساسية للدولة فهي أمنها القومي وبقاؤها. و في الأخير القوة والقدرات الوطنية هي اختبار أساسي للعلاقات بين الدول[64].

كانت الواقعية هي التقليد النظري السائد طوال الحرب الباردة. افترضت أن الشؤون الدولية عبارة عن صراع من أجل القوة بين الدول. هذه الأخيرة تسعى لتعزيز مصالحها بشكل منفرد، وهي متشائمة بشكل عام بشأن احتمالات القضاء على الصراع والحرب. سادت الواقعية في سنوات الحرب الباردة، لأنها وفرت تفسيرات بسيطة ولكنها قوية للحرب والتحالفات والإمبريالية والعقبات التي تعترض التعاون والظواهر الدولية الأخرى، ولأن التركيز كان آنذاك منصبا على المنافسة، متسقًا مع السمات المركزية للتنافس الأمريكي السوفيتي[65].

والواقعية ليست نظرية واحدة بالطبع. فالواقعيون "الكلاسيكيون" مثل هانز مورغنثاو "Hans Morgenthau " ورينولد نيبور"Reinhold Niebuhr" يعتقدون أن الدول، مثل البشر، لديها رغبة فطرية في السيطرة على الآخرين، مما دفعها إلى خوض الحروب. شدد "مورغنثاو" أيضًا على مزايا نظام توازن القوى الكلاسيكي متعدد الأقطاب، وشهد التنافس ثنائي القطب بين الولايات المتحدة والاتحاد السوفياتي خطورة كبيرة[66].

على النقيض من ذلك ، تجاهلت نظرية "الواقعية الجديدة" (النظرية النيوواقعية): التي قدمها كينيث والتز"Kenneth Waltz" الطبيعة البشرية وركزت على تأثيرات النظام الدولي. بالنسبة لوالتز، يتألف النظام الدولي من عدة قوى عظمى، كل منها يسعى للبقاء على قيد الحياة. وعلى عكس مورغنثاو" Morgenthau "، ادعى أن القطبية الثنائية أكثر استقرارًا من تعدد الأقطاب. كان التنقيح المهم للواقعية هو إضافة "نظرية الدفاع الهجومي"،

[64]-ND International Security Center, An Introduction to Realism in International Relations, **UNIVERSITY OF NOTRE DAME**, July 21, 2022, link: http://bitly.ws/DYIa, seen on: 04.05.2023.
[65]-Stephen M Walt, One world many theories**,** 1998, link: http://bitly.ws/yQ5p, seen on, 11.01.2023.
[66]-Ibid.

على النحو الذي وضعه روبرت جيرفيس " Robert Jervis"، وجورج كويستر" George Quester"، وستيفن فان إيفرا"Stephen Van Evera ".

جادل هؤلاء العلماء بأن احتمالية الحرب تكون أكثر عندما يمكن للدول أن تغزو بعضها البعض بسهولة. عندما كان الدفاع أسهل من الهجوم، كان الأمن أكثر وفرة، وانخفضت حوافز التوسع، ويمكن أن يزدهر التعاون. وإذا كان للدفاع ميزة، يمكن للدول أن تميز بين الأسلحة الهجومية والدفاعية، عندها يمكن للدول أن تكتسب الوسائل للدفاع عن نفسها دون تهديد الآخرين، وبالتالي تخميد آثار الفوضى[67].

غير أن النتيجة غير المقصودة والمؤسفة للجدل حول الواقعية الجديدة هو ذاك الجزء الكبير من نقدها، والذي جعل نظرية السياسة الدولية يكاد يتعذر الوصول إليها من قبل شخص عادي. ففي حين أن نظرية الواقعية الكلاسيكية كانت تهدف إلى دعم الممارسة الدبلوماسية وتوفير دليل يتبعه أولئك الذين يسعون إلى فهم والتعامل مع التهديدات المحتملة، فنظرية الواقعية الجديدة، المهتمة بمختلف الصور والمشاريع الكبرى غير مناسبة لأداء هذه المهمة. ربما السبب الرئيسي وراء ذلك هو الاهتمام المتجدد بالواقعية الكلاسيكية، وخاصة في أفكار "مورغنثاو"؛ بدلاً من أن يُنظر إليه على أنه شكل عفا عليه الزمن من الفكر الواقعي ما قبل العلمي، حلت محله نظرية الواقعية الجديدة، يعتبر تفكيره الآن أكثر أهمية مما تم التعرف عليه سابقًا[68].

وإذا كانت الواقعية أجندة بحثية مزدهرة في كل من العلاقات الدولية والنظرية السياسية، إلا أنه من المهم التعرف على الاختلافات المهمة بين الواقعيين؛ فهم يقدمون إجابات متضاربة للعديد من الأسئلة المنهجية والسياسية والأخلاقية. في حين أن الواقعية الوضعية الجديدة قد تساعد المنظرين السياسيين في مسائل الجدوى والمشكلات (والفرص)الخاصة بسن الإصلاح في النظام الدولي، الواقعيون الآخرون يرفضون إطارهم المنهجي[69].

---

[67]-Stephen M Walt, One world many theories, Op,cit.

[68]-Arvind Adityaraj, Political Realism in International Relations, **College of Commerce Arts and Science**, Patna, india, link: http://bitly.ws/yQgk, seen on, 12.01.2023, pp.18-19.

[69]-Duncan Bell, Political Realism and International Relations, **CORE**, http://bitly.ws/yQgI, seen on, 12.01.2023, p.10.

لا يمكن النظر إلى النظريات السياسية على أنها واقعية ما لم تشمل المؤسسات الدولية، الممارسات والقواعد. على الرغم من وجود علامات مشجعة على وجود هذه المشكلة، أمام الواقعيين الليبراليين والراديكاليين الكثير من العمل للقيام بها[70].

### الفقرة الثانية: مكانتها في المغرب والجزائر

لقراءة العلاقة المغربية الجزائرية من منظور النظرية الواقعية، لابد من تصفح تاريخ نزاعاتهما والتمعن في فتراته، متى تواجد العنف بقوته الصلبة، ومتى تواجدت الصراعات المقلقة لمضجعي الدولتين ولكن بدون حضور أسلحة. فإذا استثنينا "حرب الرمال" والتي يمكن قراءتها بمنظور الواقعية الكلاسيكية التي تبني النظرية على الحرب بين الدول، فباقي الصراعات المغربية الجزائرية يمكن مناقشتها برؤية واقعية نيوكلاسيكية.

"حرب الرمال" وليدة لأزمة الحدود غير واضحة المعالم بين الجزائر والمغرب تلك الحدود التي تركها الاستعمار الفرنسي مبهمة المعالم، فكانت بمثابة الشرارة الأولى لمشاكل البلدين خلال فترة ما بعد الاستقلال. اندلعت الحرب في منطقة تندوف، التي كانت منطقة حدودية يطالب المغرب بضمها. فالمغرب الكبير، الذي تصوره في الأصل الزعيم القومي علال الفاسي، يمثل امتدادًا واسعًا للأراضي التي تشمل الصحراء "المغربية"، موريتانيا، الجزء الشمالي الغربي من مالي والمناطق الجنوبية الغربية من الجزائر[71].

بعد فترة وجيزة من حصول الجزائر على استقلالها، خلال صيف وخريف عام 1962، نشأت التوترات محليًا عندما قاومت العناصر القبلية الموالية للمغرب في منطقة تندوف إقامة الجزائريين مما تسبب في حوادث عنف بين قوات الأمن والسلطات المدنية، في هذا الجو المتوتر احتلت القوات الجزائرية النقاط الحدودية ل"حاسي بيدا" و"تندجوب" جنوب نهر درعة، في 8 أكتوبر 1963، على ما يبدو ردًا على تحرك المغرب السابق للسيطرة عليهما في أواخر شتنبر. أثار مثل هذا الإجراء اجتماعات لممثلي حكومات كلا الجانبين في محاولة للتفاوض على تسوية بشأن قضية الحدود، لكن مواقفهما الرسمية تم التأكد على عدم إمكانية التوفيق بينها. يشرح في مذكراته "عبد الهادي بوطالب"، وزير

[70]-Duncan Bell, Political Realism and International Relations, Op.cit, p.10.
[71]-Ana Torres-Garcia, US diplomacy and the North African ‘War of the Sands’ (1963), **The Journal of North African Studies**, 01.03.2013, link: http://bitly.ws/yWkg, seen on: 15.01.2023.

الإعلام المغربي في ذاك الوقت بعد مناقشته مع الرئيس بن بلة، تعنت الجزائر العاصمة، واستحالة فض النزاع بالتفاوض، حينها قرر الملك الراحل الحسن الثاني أن السبيل الوحيد للخروج من الوضع هو استعادة المواقع الحدودية بالقوة، وبالتالي إطلاق حرب الرمال. هذه المرحلة الأولى من الصراع كانت غامضة. ألقى كلا الطرفين باللوم على بعضهما البعض في اندلاع الأعمال العدائية ولم تتوفر أي معلومات مستقلة. تطورت الاشتباكات على الحدود إلى مواجهة عسكرية مفتوحة تفاقمت خلال أيام قليلة في وقت لاحق، عندما لم يتمكن الجزائريون من استعادة كلا المركزين، توسعوا شمالاً وهاجموا في مناطق مغربية. هذا الهجوم، إلى جانب حقيقة أن المساعدة العسكرية لكوبا والجمهورية العربية المتحدة لنظام بن بيلا، أصبحت معروفة للجمهور بحلول 20 أكتوبر1963، ومثلت نقطة تحول في الحرب. كان هذا واضحا عندما بدأت الحكومات الغربية في إيلاء اهتمام أكبر لهذا النزاع الحدودي. كما أشارت المعلومات الاستخبارية التي تم جمعها إلى تصميم ناصر على دعم الجزائر بالسلاح وحتى القوات الغربية. بدأت الدبلوماسية في ممارسة الضغط على جميع الأطراف المعنية. سعت الولايات المتحدة، إلى جانب فرنسا وإسبانيا، إلى وقف القتال قبل أن يعجل بتدخل خارجي غير مرغوب فيه في شمال أفريقيا، والذي يمكن أن يؤدي إلى تدخل سوفياتي في نهاية المطاف[72].

استنادا لما سبق، تبقى حرب الرمال بين المغرب والجزائر، هي الحدث الوحيد، المجسد للنظرية الواقعية الكلاسيكية. في هذا الحدث حضرت القوة الصلبة وكان نزاع مسلح مباشر وحقيقي بين البلدين.

فيما تبقى من النزاعات بين البلدين، يمكن قراءتها بعين الواقعية النيوكلاسيكية. فالروايات والتصريحات الرسمية للدولتين؛ المغرب والجزائر، تحافظ على التنافس بينهما، دون اللجوء إلى استخدام القوة الصلبة. في بعض الأحيان يتم التقليل من أهمية الخطب، لكنها تساعد على فهم كيف يمكن أن يتفاقم التوتر السياسي. يحمل كل من المجتمعين المغربي والجزائري رواية مهيمنة تميز هويتهما الوطنية والسياسية التي تؤثر على صنع القرار. تساهم هذه الرواية، التي يتم بناؤها أحيانًا في مواجهة أخرى، في تعزيز التنافس مع دولة

[72]-Ana Torres-Garcia, US diplomacy and the North African ‘War of the Sands’ (1963), Op.cit, p.8.

أخرى ويتم حشدها باستمرار خلال الأزمات السياسية الدبلوماسية. تمارس القوى المغربية والجزائرية في بعض الأحيان نفوذًا غير متناسب، من خلال السيطرة على جزء كبير من مصادر المعلومات، ويمكنها استخدام بعض وسائل الإعلام وبعض الشخصيات العامة الوطنية لجعلهم متحدثين باسمهم وبالتالي التحكم في نشر السرد. تؤثر هذه الروايات الرسمية أيضًا، وفي كثير من الأحيان، على الجغرافيا السياسية للدولتين المغربية والجزائرية، ويعتبر أحد مصادر تنافسهما السعي وراء القيادة الإقليمية ولكن أيضًا سباق التسلح[73].

ومع ذلك، هناك حقيقة واحدة يصعب قياسها في مجتمعات البلدين: تأثير ومصداقية الخطاب في الرأي العام. هناك تحركات انطلقت على الشبكات الاجتماعية، والتي تتنوع بين الرغبة في المصالحة بين الشعبين وتمجيد الرومانسية الوطنية، ولكن من دون أن يكون من الممكن تحديد عينة تمثيلية فعلية داخل السكان. من المهم أيضًا التأكيد على أنه بشكل عام، تتطور المجتمعات بشكل أسرع بكثير من الطبقات الحاكمة التي ظلت ثابتة على نمط التنافس في شمال إفريقيا وفي القارة الأفريقية، فيما يتعلق بالمسائل الجيوسياسية وطريقة شن الحرب. وفقًا للأكاديمية خديجة محسن فينان، تم التعبير عن مطالب المواطنين في المغرب العربي (من أجل الحريات والكرامة) منذ العقد الأول من القرن الحادي والعشرين من خلال "النشر الإلكتروني" (إنشاء حسابات ناشطين على الشبكات الاجتماعية التي تنظم التجمعات من جميع الأنواع). تركز المطالب الشعبية بشكل أساسي على السياسة الداخلية، وبالتالي لا يعتبر المواطنون التنافس بين الدول أولوية، ولا يهتمون كثيرًا بتخصيص ميزانيات غير متناسبة للدفاع عندما كان من الممكن استخدام هذه المبالغ في الخدمات العامة الأساسية مثل الصحة أو التعليم. في حالة الجزائر، فإن المعارضة مع المغرب هي وسيلة لإضفاء الشرعية على السلطة من خلال إعطاء الشعور بالتهديد الخارجي. لا يمكننا قياس التأثير على الرأي الجزائري بدقة، على الرغم من أنه يمكننا أن نلاحظ على الشبكات الاجتماعية رغبة بعض المواطنين الجزائريين في إعادة تأكيد أخوتهم مع جيرانهم المغاربة. ما قد يكون محاولة من

[73]-Tilila Sara Bakrim, Rivalité Maroc-Algérie : la guerre des récits Introduction, **Fondation pour la recherche stratégique**, 07.04.2022, lien de l'article : http://bitly.ws/yW9k, date visite, 14.01.2023, pp.10-11.

قبل النظام لإعادة تنشيط القومية التي عفا عليها الزمن إلى حد ما قد يصبح دعاية في نظر المجتمع. نحن ، بحسب خديجة محسن فينان، في حرب اتصالات[74].

لكن المجتمعات المدنية، على الرغم من رغبتها، لا تصنع سياسة إقليمية. توجد بالفعل حوارات بين الباحثين والنشطاء وغيرهم، لا سيما في الشتات. وفي الوقت نفسه، يؤثر نمط التنافس على فرص التكامل المغاربي والتبادلات الاقتصادية والفكرية وحتى الثقافية. على أي حال، فإن رفض النظام الجزائري لأي محاولة حوار بدأها المغرب يقطع آفاق التعاون وأي تكامل اقتصادي بين هذين البلدين في الوقت الذي يواجهان فيهما تحديات اقتصادية وأمنية هائلة بسبب عدم الاستقرار في المنطقة[75].

## الفرع الثاني: واقع الدفاع السيبراني في المغرب والجزائر

الغرض من هذا الفرع هو تقييم الأهمية الحالية وصلاحية الواقعية كأداة تفسيرية في العلاقات الدولية المعاصرة، على سبيل المثال الدفاع السيبراني المغربي والجزائري. تم تحريك جميع فقرات الفرع بجهد نظري لتحديد الجوانب المفاهيمية للواقعية ومحاولة تحديد ما إذا كان التقليد لا يزال يوفر الأدوات المفاهيمية اللازمة لعلماء العلاقات الدولية. تُظهر الدراسة، بشكل عام، أنه على الرغم من العديد من أوجه القصور فيها، لا تزال الواقعية تقدم فهمًا متعدد الأوجه للسياسة العالمية وتنير التحديات المتزايدة لها. وللتوسع أكثر والوقوف على هذه الحقيقة، تناولت الدراسة في هذا الفرع العلاقة بين النظرية الواقعية والدفاع السيبراني(الفقرة الأولى)، ثم مكانتها في واقع الدفاعين السيبرانيين؛ المغربي والجزائري(الفقرة الثانية).

### الفقرة الأولى: النظرية الواقعية والدفاع السيبراني

مع انتشار تكنولوجيا المعلومات والاتصالات (ICT)، أصبح الأمن السيبراني مصدر قلق رئيسي لواضعي السياسات، ويحظى باهتمام كبير من علماء العلاقات الدولية. حيث يشكل الأمن السيبراني تحديا كبيرا للأمن الاقتصادي والوطني للبلدان. فالفضاء السيبراني يعتبر الآن المجال الخامس للحرب بعد الأرض، البحر، الجو والفضاء، **والنظرية الواقعية**

[74]-Tilila Sara Bakrim, Rivalité Maroc-Algérie: la guerre des récits Introduction, Op.cit, pp.10-11.
[75]-Ibid.

**يمكن أن تساعدنا في فهم هذا الشكل الجديد نسبيًا من الصراع**. فلطالما كانت الواقعية نموذجًا مهيمنًا في مجال العلاقات الدولية، وتستند إلى مجموعة عامة من الافتراضات حول السياسة الدولية، وتركز على كون الدولة هي أهم الجهات الفاعلة التي تعمل كوحدات مستقلة. لكن وضمن نظام دولي يفتقر إلى سلطة مركزية وعقلانية، يُظهر مجال الأمن السيبراني الناشئ تجددًا للواقعية المتأثرة، ووجهات نظر مع التركيز على الأمن والمنافسة وتوزيع القوة وميزة الهجوم على الدفاع وفوائد ردع الاستراتيجيات، وبالتالي توفير فرصة لتقييم دور الواقعية في المجال السيبراني[76].

يعتبر البعض الواقعية إطار عمل مفيد لفهم الفضاء السيبراني. كما كتب ريردون وشوكري (2012): " يمكن استخدام نظريات الواقعية للردع وإدارة الأزمات والصراع في فهم ما إذا كان الفضاء السيبراني يعمل على تحقيق الاستقرار أو عدم الاستقرار، سواء كانت التقنيات السيبرانية مصدرًا جديدًا للنزاع أو السلام، وما إذا كانت الدول ستنخرط في سباق التسلح السيبراني"[77].

ينبني الافتراض الأساسي للواقعية على أن الدول هي أقوى الجهات الفاعلة وبالتالي أهمها في السياسة الدولية. لكن ثورة المعلومات تتحدى أسبقية الدولة، على أي حال، بسبب زيادة مشاركة الجهات الفاعلة غير الحكومية التي تهدد ديناميكيات السلطة التقليدية. تزداد أهمية الجهات الفاعلة غير الحكومية في العلاقات الدولية، كما تجادل نظرية "ناي" حول انتشار السلطة، وهذا صحيح بشكل خاص في المجال السيبراني حيث يمكن للمجرمين الأفراد والمنظمات والجماعات الإرهابية الاستفادة من إمكانية الوصول إلى الإنترنت لتهديد هيمنة الدولة، وحيث تلعب الشركات الخاصة دورًا، كمزود للأمن وكمصادر للضعف. لكن لا ينبغي أن نبالغ في هذه القضية لأن الدول لا تزال هي الجهات الفاعلة الأكثر هيمنة عندما يتعلق الأمر بالصراع السيبراني. تلعب الجهات الفاعلة غير الحكومية والإرهابيون دورًا، لكن تكتيكاتهم كانت عمومًا غير فعالة، أو استخدمت كغطاء للدول القومية التي تسعى لإخفاء أفعالها. يبدو أن الدول تظل في نهاية المطاف في وضع أفضل للاستفادة من أدوات الحرب

[76]-ANTHONY J.S. CRAIG & BRANDON VALERIANO, Realism and Cyber Conflict: Security in the Digital Age, Bristol, England2018, seen on : 29.03.2023, link: http://bitly.ws/CgVT, pp,85-96.
[77]-Ibid.

الإلكترونية، بموارد للاستثمار في القوى العاملة والبحث والتطوير والتعليم التي من غير المرجح أن تنافسها الجهات الفاعلة غير الحكومية[78].

تبدو الواقعية وكأنها منظور العلاقات الدولية الغريزي لفهم الصراع السيبراني. يشير تحليلنا إلى أن الواقعية تظل إطارًا مناسبًا لتحديد القضايا المهمة المتعلقة بالأمن في المجال السيبراني، ويمكن أن توفر في بعض الأحيان رؤى مفيدة حول بعض الخصائص الدائمة للعلاقات الدولية. فمن نواح كثيرة، يشبه المجال السيبراني عالمًا واقعيًا بطبيعته الفوضوية والافتقار إلى الحوكمة المؤسسية، حيث تخشى الدول بعضها البعض وتطور قدراتها في الاستجابة. تثير الواقعية الاهتمام أيضًا بأسئلة حول القوة السيبرانية، حول من يمتلكها، ومدى ارتباطها بالاستقرار الدولي. من حيث ما إذا كانت القوة السيبرانية ستحول ديناميات السلطة التقليدية[79].

بالنظر إلى القضايا المثارة هنا، نشجع على تطوير نظريات جديدة على أساس الملاحظة التجريبية، أو المنطق الاستنتاجي للمجال السيبراني بدلاً من التراجع تلقائيًا عن النظريات الواقعية التي تم تطويرها لشرح الأشكال الحركية للحرب. مع مزيد من البحوث التجريبية، يمكننا ذلك من اكتساب فهم أكثر دقة للقضايا الرئيسية؛ مثل تأثير الإنترنت، سباقات التسلح على العلاقات بين الدول، توزيع القدرات السيبرانية بين الفاعلين الحكوميين وغير الحكوميين، أسباب ضبط النفس رغم شدة المنافسة الأمنية وتصورات الميزة الهجومية. يمكن أن تساعدنا الإجابات على هذه الأسئلة بشكل دقيق في صياغة إرشادات سياسية أفضل للحكومات[80].

### الفقرة الثانية: النظرية الواقعية وتفسيرها للدفاع السيبراني في المغرب و الجزائر

لاتتوفر النظريات الواقعية على القدرة لتفسير مراحل أقل حدَّة من الصراع الدولي: فالنظريات الواقعية بمختلف فروعها معنيَّة بحالة الحرب وحالة البقاء، وقد تصلح النظريات الواقعية في تفسير الحالات التي تسعى فيها الدولة نحو تدمير خصمها نهائيًّا للتخلص من "المعضلة الأمنية"، لكن يبقى التساؤل عن قدرة النظريات الواقعية على تفسير حالات أقل

[78]-ANTHONY J.S. CRAIG & BRANDON VALERIANO, Realism and Cyber Conflict: Security in the Digital Age, Op.cit, pp.85-96.
[79]-Ibid.
[80]-Ibid.

حدَّة من الصراع غير حالة الحرب والتي تنطبق على حالات الصراع السيبراني، الذي لا يمكن فيه سحق الخصم أو تدميره نهائيًّا، ويبقى جليًّا أنه حتى الآن لم يشهد العالم حالة حرب سيبرانية كاملة أو واضحة يمكن قياسها، بل مستويات أقل من الصراع السيبراني مثل شنّ هجمات سيبرانية على الأفراد و البنوك و الشركات[81].

وما يحصل بين المغرب والجزائر في المجال السيبراني، لم يخرج عن هذا الإطار، فهو لم يتطور إلى صراع دولي بين الجارين الغريمين. هناك اتهامات في ما بينهما، لا تعتمد على معطيات صريحة وصحيحة، ولم ترق إلى صراع سيبراني بينهما.

على سبيل المثال، اتهمت وكالة الأنباء الجزائرية، المغرب بالوقوف وراء أحدث الهجمات السيبرانية على موقعها على الإنترنت، ووجه النظام الجزائري عدة اتهامات مماثلة للمغرب، مشيرًا إلى أن حلًا لإنهاء الجمود السياسي بين البلدين بعيد المنال عن الحدوث في أي وقت قريب[82].

مع تكثيف النظام الجزائري لحملاته العدائية ضد المغرب منذ تعليق جميع العلاقات الدبلوماسية مع المملكة في أغسطس 2021، أضحت مثل هذه الاتهامات من الجزائر سمة مشتركة للعلاقات المتوترة بين الجارتين[83]، لكن كما أشرنا سابقا لا ترقى إلى مصاف الهجمات السيبرانية[84] الصريحة، وعليه لا يمكن قراءتها من منظور واقعي.

---

[81]-إيهاب خليفة، الحالة السيبرانية في نظريات العلاقات الدولية: الحاجة إلى مراجعة جديدة، مركز المعلومات واتخاذ القرار- رئاسة مجلس الوزراء، مصر، 02.12.2021، رابط المقال: http://bitly.ws/CibV، تاريخ الدخول: 30.03.2023، ص ص، 08-11.

[82]-Safaa Kasraoui, Algeria's News Agency Accuses Morocco of Being Behind Latest Cyberattacks, **Morocco World News**, 13.02.2023, link: http://bitly.ws/Ci9q, seen on, 30.03.2023.

[83]-Ibid.

[84]-**الهجمات السيبرانية**: تختلف أنواع الهجمات السيبرانية بحسب نوع الأسلحة المستخدمة في تنفيذها، وكذلك بحسب طبيعة الأهداف المراد تعطيلها. وتتنوع أنواع الهجمات السيبرانية إلى هجمات رفض الخدمة (DOS)، الهجمات الطمسية (Defacement attacks)، فتنفذ على مرحلتين: المرحلة الأولى تبدأ بقيام القراصنة الإلكترونيين والمتسللين بإرسال برامج لاكتشاف نقاط الضعف في البرامج(ماسحات الضعف)، ثم في المرحلة الثانية يتم استبدال صفحة الويب المستخدمة بصفحة أخرى تحت سيطرة الجهة المهاجمة، كما حصل في اختراق قناة وكالة الأنباء القطرية عام 2017من قبل قراصنة. هناك هجمات سرقة كلمات المرور للتسلل إلى النظم، أو الاختراقات غير المصرح بها. ونوع آخر من الهجمات يتمثل في **نشر البرامج الضارة** ويعتبر هذا النوع من الهجمات النوع الأول من الهجمات واسعة الانتشار، ويشمل الفيروسات والبرامج الضارة، وتعمل على تخريب أنظمة التحكم أو حجب الخدمة أو رفضها.
(-محمد السامرائي، دور القانون الدولي في مكافحة الهجمات السيبرانية، الذاكرة للنشر والتوزيع، بغداد، ط1، 2023، ص.51-54).

بالإضافة إلى ما سبق، كان هناك تقرير أجرته منظمة العفو الدولية و "مختبر المواطن" Citizen Lab"، هذا التقرير يتعمق في المنهجيات العلمية والبيانات والأحداث المحيطة بالعديد من حالات التجسس الرقمية المزعومة التي يعتقد أن الحكومة المغربية ارتكبتها[85]. لكن أثيرت شكوك فيما يتعلق بسمعتهما في معلومات المجتمعات الأمنية والعلمية. على وجه التحديد، لقد ظهر أن ملف استخدام نتائج الطب الشرعي المحمول لدعم مزاعم وجود برنامج تجسس بيغاسوس على عمرراضي، كلود مانجين، وهواتف أخرى، تم العبث بها وتزييفها عن طريق العديد من النتائج الإيجابية الخاطئة التي لم تكن كذلك وكشف عنها الباحثون[86].

وما يزيد في دحض المزاعم الجزائرية و تفنيد مزاعم تلك اللجنتين المذكورتين أعلاه، التقرير الذي صدر عن لجنة التحقيق بالبرلمان الأوروبي حول قضية "بيغاسوس"، بتاريخ 18.06.2023، والذي خلص إلى أنه "لا يوجد دليل يدين المغرب باستخدام برنامج التجسس الإسرائيلي ضد أي دولة"[87].فتقدير قوة الدولة السيبرانية يعتبر أمرًا صعب القياس؛ لأنها غير ملموسة أو مرصودة، ولا تعلن الدول عن قدراتها السيبرانية الهجومية، فمثلا لم

[85]-Jonathan Boyd Scott, "Exonerating Morocco disproving the spyware", 18.02.2023, link: http://bitly.ws/Cib3, seen on 30.03.2023.
[86]-Ibid.
[87]-An European commission of inquiry acquits Morocco of using the spyware “Pegasus”, **Breaking latest News**, 18.06.2023, link: http://bitly.ws/IQpn, seen on: 18.06.2023.

يتم الإعلان رسميًّا حتى الآن عن المسؤول عن بناء برمجية" ستاكس نت[88]" التي ضربت البرنامج النووي الإيراني بين عامي2010 - 2009 [89].

فصعوبة معرفة الجهة المهاجمة هو ما يحصل بين المغرب والجزائر. قد تتكاثر الاتهامات بينهما بدون مرجعية تقنية دقيقة. لكن وبالتوازي مع التوترات السياسية بين الجزائر والمغرب، هناك مواجهة أخرى تدور رحاها في الفضاء السيبراني، أطلق عليها بعض الخبراء **حرب الظل**. نشر قراصنة الحساب الرسمي لوزارة العدل على تويتر عدة تغريدات تدعم العملية الروسية في أوكرانيا، متهمين الرئيس الأوكراني فولوديمير زيلينسكي بـ "النازية وقتل مواطنيه". في 12 مارس 2022، أطلق مجلس القضاء الجزائري تحقيقا قضائيا في القرصنة، قائلا في بيانه "سيتم إبلاغ الجمهور بنتائج التحقيقات في الوقت المناسب"[90].

جدير بالذكر أن هذه الهجمات السيبرانية ليست الأولى من نوعها. في نوفمبر 2021، تم اختراق موقع الاتحاد العام للمقاولات المغربية (CGEM)، بينما هاجمت مجموعة القرصنة المغربية، فريق المغرب هاك، موقع وزارة المالية الجزائرية. في 17 ديسمبر 2020، قام قراصنة بتعطيل الموقع الإلكتروني للوكالة الوطنية المغربية لتقييم الموارد الهيدروكربونية. وقالت وزارة الطاقة في بيان في اليوم التالي إن موقع الوكالة تعرض لهجوم من قراصنة، وطالبت المستخدمين بعدم الدخول إلى الموقع حتى يتم وقف الهجوم.

---

[88]-**ستاكسنت"Stuxnet"**: برنامج ضار مصنف على أنه دودة، والذي تسبب في أضرار جسيمة منذ ظهوره في عام 2010. وقد تم استخدامه بشكل خاص لاستهداف المنشآت النووية في إيران. لهذا السبب، يعتبر Stuxnet أكثر البرامج الضارة تدميراً في فئته. فهو أول برنامج ضار تسبب في أضرار تتجاوز المجال الرقمي، حيث تسبب في التدهور المادي للبنى التحتية المستهدفة. على الرغم من عدم إعلان أي دولة مسؤوليتها عن إنشائها، يبدو أن أجهزة المخابرات في الولايات المتحدة وإسرائيل طورت بشكل مشترك هذا البرنامج الضار بهدف إلحاق الضرر بالبرنامج النووي الإيراني. جعل الهجوم الذي استهدف محطات الطاقة الإيرانية دودة Stuxnet مشهورة باستغلال ثغرة في الصناعة وكونها أول برنامج ضار يتسبب في أضرار مادية للمعدات. أكسبه هذا الهجوم الإلكتروني غير المسبوق لقب الباحثين باعتباره "أول سلاح رقمي في العالم". غالبًا ما يُشار إلى Stuxnet على أنه فيروس، لكنه في الواقع فيروس متنقل على الكمبيوتر. على الرغم من أن كلا النوعين من البرامج قادران على إتلاف الملفات الموجودة على الجهاز المستهدف، إلا أن الدودة تعمل بشكل مستقل أكثر من الفيروسات. لا يتطلب تفعيل أي تفاعل بشري، ويمكن أن ينتشر تلقائيًا بعد اختراق نظام الكمبيوتر. يمكن للفيروس المتنقل أيضًا تنفيذ إجراءات أخرى: على سبيل المثال، استخدام النطاق الترددي أو فتح الأبواب الخلفية أو إدخال برامج ضارة أخرى، مثل برامج التجسس أو برامج الفدية"spywares ou des ransomwares ".
(Delphine Lacour, Qu’est-ce que le ver Stuxnet?, 14.09.2022, lien de l’article : http://bitly.ws/Fq6F, date visite : 25.05.2023).

[89]-إيهاب خليفة، الحالة السيبرانية في نظريات العلاقات الدولية: الحاجة إلى مراجعة جديدة، مرجع سابق، ص ص، 08-11.

[90]-Hamdy Bashir, A Cyber Shadow- War between Algeria and Morocco, **Arab Wall**, 22.03.2022, link: http://bitly.ws/zsLS, seen on: 30.03.2023

وبحسب مراقبين، تصاعدت موجة الهجمات واستهدفت بشكل كبير المواقع الحكومية وبعض المؤسسات الإعلامية[91].

كما أكدنا صعوبة معرفة الجهة التي تسببت في هجوم سيبراني، فالجزائر اتهمت المغرب بدون مرجعية تقنية وعلمية. لهذا السبب، نفى المغرب الاتهامات الجزائرية بشأن الهجمات الأخيرة، وطالب وزير الخارجية المغربي الجزائر بتقديم أدلة ملموسة، موضحا أن المغرب سيتخذ إجراءات قانونية في التعامل مع هذه الادعاءات. وأشار إلى أن "هذه الاتهامات جاءت على أساس تكهنات بحتة"، وأن ما أسماه "الحملة الخبيثة والمضللة" تقودها مجموعة من المنصات الدولية التي تخدم أجندات معروفة بأنها معادية للمغرب. هذه المزاعم، على حد قوله، تروج لها دوائر "منزعجة من النجاحات "التي تراكمت في المغرب في السنوات الأخيرة[92]. هذا ما جاء على لسان الوزير المغربي، لكن كما يصعب معرفة الجهة التي تبنت الهجوم السيبراني، يصعب كذلك تأكيد، أو نفي صحة ما صرح به الوزير.

## المطلب الثاني: الدفاع السيبراني في المغرب والجزائر من منظور النظريتين الليبرالية والنقدية

من نواح كثيرة، كانت مدرسة الفكر المادية الليبرالية هي الأقل وضوحًا في الانقسامات الرئيسية للتفكير حول موضوع السيبرانية. نشر الليبراليون القليل من البيانات حول الحقل السيبراني، فعمومًا لم يجذب مستويات مماثلة من الاهتمام، لأن مدرسة الفكر هذه هي الأكثر توسعية من بين المدارس الأخرى، من حيث أنها تكرس نفسها لسؤال حول كيفية تشكيل تكنولوجيا المعلومات لمجتمعنا، بدلاً من التقييد الصارم لنفسها لمسألة الحرب بصفة عامة، والحرب السيبرانية بصفة خاصة. على هذا النحو، فإن المدرسة الليبرالية مخفية داخل نطاق أوسع لدراسات إدارة الإنترنت والخصوصية واستكشاف التأثير الاجتماعي لحوسبة التقنيات. ومع ذلك، في هذه المجالات، غالبًا ما يكون هناك اعتبار محدد للحرب السيبرانية موجود ضمن هذه الدراسات نظرًا لتداخل مجالات القضايا[93]. وهذا الاعتبار المحدد هو الذي بحثت عليه الدراسة في تعامل المغرب والجزائر مع الدفاع السيبراني في الفرع الأول(قراءة

[91]- Hamdy Bashir, A Cyber Shadow- War between Algeria and Morocco, Op.cit.
[92]-Ibid
[93]-Col PEC Martin, Cyber warfare schools of thought: bridging the epistemological ontological divide, Op.cit, p. 57.

ليبرالية للدفاع السيبراني في المغرب والجزائر). أما في الفرع الثاني، فحاولت الدراسة الوقوف على المدرسة النقدية، من خلال تعريفها ومحاولة إسقاطها على النموذج الدفاعي السيبراني –المغربي الجزائري(قراءة نقدية للدفاع السيبراني في المغرب والجزائر).

## الفرع الأول: قراءة ليبرالية للدفاع السيبراني في المغرب والجزائر

الليبرالية هي سمة مميزة للديمقراطية الحديثة، يتضح من انتشار مصطلح "الديمقراطية الليبرالية" كطريقة لوصف البلدان ذات الانتخابات الحرة والنزيهة، وسيادة القانون والحريات المدنية المحمية. ومع ذلك، فإن الليبرالية - عند مناقشتها في نطاق نظرية العلاقات الدولية- تطورت إلى كيان متميز خاص بها. تحتوي الليبرالية على مجموعة متنوعة من المفاهيم والحجج حول كيفية احتواء المؤسسات، السلوكيات، الصلات الاقتصادية والتخفيف من حدة القوة العنيفة للدول. عند مقارنتها بالواقعية، فإنها تضيف المزيد من العوامل في مجال رؤيتها -لا سيما مراعاة المواطنين والمنظمات الدولية. وعلى وجه الخصوص، كانت الليبرالية هي الرقاقة التقليدية للواقعية في نظرية العلاقات الدولية؛ لأنها تقدم وجهة نظر أكثر تفاؤلاً للعالم، ترتكز على قراءة مختلفة للتاريخ عن تلك الموجودة في الدراسات الواقعية[94].

بناء على ما تقدم ، تمت قراءة الدفاع السيبراني في المغرب والجزائر قراءة ليبرالية، عبر التطرق لماهية المدرسة الليبرالية(الفقرة الأولى)، ومكانة تلك المدرسة في المغرب والجزائر(الفقرة الثانية).

### الفقرة الأولى: ماهية المدرسة الليبرالية

تعتبر المفاهيم المؤسسة لليبرالية مفاهيم شديدة الاختلاف لدرجة أنه يمكننا الحديث عن ليبراليات" بعضهم يفضل مصطلح التعددية"، لذا لسنا بصدد تناول بناء نظري موحد ومتماسك إزاء هذه النظرية، وإن اشتركت مرتكزاتها الفكرية، وسياقاتها التاريخية، ومنطلقاتها الإيديولوجية. فالليبرالية تعد من المنظورات التي تمتلك تصورا أمنيا مخالفا للواقعية. هذا الاتجاه يعتبر الأمن القومي والتحالفات نتاجا لتطبيق المنظور الواقعي، لكن الليبراليين يمتلكون تصورا بديلا يتمثل في الأمن الجماعي والسلام الديمقراطي، عبر إنشاء

[94]-Jeffrey W.Meiser, Introducing Liberalism in International Relations Theory, **E-international relations**, 18.02.2018, link: http://bitly.ws/ESXc, seen on: 18.05.2023, p.1.

منظمات ومؤسسات دولية وإقليمية تعمل على ضمان وتحقيق الأمن والسلام بطريقة تعاونية وتبادلية بين الدول، ما يعني وجود فاعلين غير الدولة[95].

تعتبر النظرية الليبرالية من أهم نظريات العلاقات الدولية، وهي نظرية متشعبة و متعددة الروافد. وللنظرية الليبرالية مفهوم أساس يتمثل في القوة ولكن في صورتها الاقتصادية. وتعترف النظرية الليبرالية بالفاعلين من غير الدول كالمنظمات الدولية والشركات متعددة الجنسيات، كما تحلل أدوارها في العلاقات الدولية. وتتفق الليبرالية مع النظرية الواقعية في بعض المظاهر وتختلف عنها في مظاهر أخرى. هذا من ناحية، ومن ناحية أخرى تنقسم الليبرالية إلى ليبرالية كلاسيكية وأخرى جديدة مؤسسية، وتتمتع كل منهما بالمفكرين والعلماء الذين أثروا الفكر الليبرالي وساهموا فيه أيما مساهمة، من أمثال "إيمانويل كانط"،"بنثام"، "دويل"، "فوكوياما"، "كوهين" و"ناي". ومن أهم إسهامات النظرية الليبرالية؛ نظرية المنفعة، نظرية السلام الديمقراطي، فكرة نهاية التاريخ، دور القانون الدولي ونظرية الاعتماد المتبادل. وعلى الرغم من كل ما قدمته النظرية الليبرالية من إسهامات في حقل العلاقات الدولية، إلا أنها لم تسلم من بعض الانتقادات التي طالت فروضها الأساسية، ولكن ذلك لا يقلل من شأن النظرية الليبرالية كأحد النظريات الوضعية في مجال العالقات الدولية[96].

فهي ليست مجرد أداة أيديولوجية لمزيد من واقعية وصرامة النظريات، كما يدعي نقادها، ولا مجموعة انتقائية من الفرضيات المرتبطة فقط بـالتاريخ الفكري المشترك والالتزام المعياري، حيث يضطر مؤيدوها حاليًا إلى التنازل، بل هي نظرية متماسكة منطقيًا، متميزة من الناحية النظرية، علمية اجتماعية قابلة للتعميم تجريبياً - نظرية تتبع افتراضات صريحة وتولد مجموعة غنية من الادعاءات ذات صلة بالسياسة العالمية، للوصول إلى ما هو أبعد من حالات التعاون بين أقلية من الدول الليبرالية[97].

---

[95]-سعيدي ياسين، التحديات الأمنية الجديدة في المغرب العربي، مرجع سابق، ص.22.

[96]-مروة خليل محمد مصطفى، القدرة التفسيرية للنظرية الليبرالية في عامل متغير "دراسة تقويمية"، 2021، رابط المقال: http://bitly.ws/zdco، تاريخ الدخول: 21.01.2023.

[97]-Andrew Moravcsik, Taking Preferences Seriously: A Liberal Theory of International Politics, **Princeton.edu,** 1997, link: http://bitly.ws/zdpH, seen on: 21.01.2023, p.35.

تحكم النظرية الليبرالية ثلاث فرضيات رئيسية: طبيعة الفاعلين المجتمعيين، الدولة والنظام الدولي[98].

**الافتراض الأول يرتبط بأولوية الفاعلين المجتمعيين؛** فالفاعلون الأساسيون في السياسة الدولية هم الأفراد والجماعات الخاصة، الذين هم في المتوسط عقلانيون ويكرهون المخاطرة والذين ينظمون التبادل والعمل الجماعي لتعزيز المصالح المتباينة في ظل القيود التي تفرضها الندرة المادية، القيم المتضاربة، والاختلافات في التأثير المجتمعي[99].

تستند النظرية الليبرالية على وجهة نظر "من أسفل إلى أعلى" للسياسة، حيث يتم التعامل مع مطالب الأفراد والجماعات المجتمعية على أنها تحليلية قبل أن تكون سياسية. فالعمل السياسي متضمن في المجتمع المدني المحلي وعبر الوطني، ويُفهم على أنه تجميع الأفراد العقلانيين المحددين ذوي الأذواق المتباينة والالتزامات الاجتماعية، والموارد المتاحة. يحدد الأفراد المتميزون اجتماعيا المصالح المادية والفكرية بمعزل عن السياسة، ومن تم النهوض بالمصالح من خلال التبادل السياسي والعمل الجماعي. يفترض أن الأفراد والجماعات يتصرفون بعقلانية في السعي وراء الرفاهية المادية والمثالية[100].

ترفض النظرية الليبرالية الفكرة الطوباوية القائلة بوجود انسجام تلقائي للمصالح بين الأفراد والجماعات في المجتمع، لكنها تؤكد أن بعض الأفراد في أي مجتمع متقبلين للمخاطر أو العمل غير العقلاني. تشير النظرية الليبرالية إلى أن صراع المطالب المجتمعية والاستعداد لاستخدام الإكراه في السعي لتحقيقها مرتبطة بعدة عوامل، أهمها: المعتقدات الأساسية المتباينة، والصراع على السلع المادية النادرة، وعدم المساواة في السلطة السياسية. تلك العوامل الثلاث ماهي إلا اختلافات عميقة لا يمكن التوفيق بينها، فكلما كانت التفاوتات المجتمعية كبيرة، كلما كان الصراع هو الأكثر احتمالا[101].

**الافتراض الثاني: تمثيل وتفضيلات الدولة.** في المفهوم الليبرالي للسياسة الداخلية، الدولة ليست فاعلاً بل مؤسسة ممثلة تخضع باستمرار للقبض والاستيلاء، والبناء وإعادة

---

[98]-Andrew Moravcsik, Taking Preferences Seriously: A Liberal Theory of International Politics, Op.cit, p.4.
[99]-Ibid, pp.4-5.
[100]-Ibid.
[101]-Ibid.

الإعمار من قبل ائتلافات الفاعلين الاجتماعيين. أما التمثيل، من وجهة النظر الليبرالية، فليس مجرد سمة رسمية لمؤسسات الدولة ولكنه يتضمن خصائص مستقرة أخرى للعملية السياسية، رسمية أو غير رسمية، والتي تمنح امتيازًا لمصالح مجتمعية معينة. فالأنظمة الاستبدادية الزبائنية مثلا، قد تميز أولئك الذين لديهم روابط عائلية، أو بيروقراطية، أو اقتصادية، عن أولئك الذين ليس لديهم نفوذ. حتى عندما تكون المؤسسات الحكومية عادلة رسميا، قد تولد بعض الاحتكارات الاجتماعية أو الاقتصادية سياسات توزيع غير متكافئة نسبيًا للممتلكات أو المعلومات أو التنظيم[102].

**الافتراض الثالث: الترابط والنظام الدولي**: بالنسبة لليبراليين، يعكس سلوك الدولة أنماطًا مختلفة من تفضيلاتها، وتدرك أولوياتها المميزة في ظل قيود متفاوتة تفرضها تفضيلات دول أخرى. ولخلق ترابط ونظام دولي، لا بد من تبادل تنازلات سياسية من خلال التنسيق، أو الالتزام المسبق بين تلك الدول. هاتان الآليتان يمكن أن تحسن رفاهية الدول. هذه الافتراضات الليبرالية الثلاث، ولا سيما الثالثة- في جوهرها، "ما تريده الدول و قد يبدو المحدد الأساسي لما يفعلونه "- منطقيًا. ومع ذلك، فقد رفضت نظرية العلاقات الدولية السائدة بشكل موحد مثل هذه الادعاءات في الماضي[103].

## الفقرة الثانية: مكانتها في المغرب والجزائر

ترى النظرية الليبرالية أن الدولة ليست هي الفاعل الوحيد في العلاقات الدولية، بل إن هناك فواعل أخرى غير الدول تؤدي دورًا مهمًّا في العلاقات الدولية، مثل الجماعات الإرهابية ،الشركات متعددة الجنسيات والمنظمات غير الحكومية، مع الاعتراف بأن الدولة هي الأكثر تأثيرًا في مجمل العلاقات. وتؤكد الليبرالية أهمية الأمن الجماعي، باعتباره وسيلة لتعزيز الأمن الدولي، من خلال إقامة مؤسسات للأمن الجماعي توفر آلية أكثر فاعلية[104].

ويمكن الاستفادة من النظريات الليبرالية في تحليل بعض المتغيرات الخاصة بطبيعة الفضاء الإلكتروني وطبيعة الصراع السيبراني، في الاهتمام مثلًا بالأبعاد غير

---

[102]-Andrew Moravcsik, Taking Preferences Seriously: A Liberal Theory of International Politics, Op.cit, pp.6-8.

[103]-Ibid, pp.8-9.

[104]-إيهاب خليفة، الحالة السيبرانية في نظريات العلاقات الدولية: الحاجة إلى مراجعة جديدة، مرجع سابق، ص ص،12-14.

العسكرية للقوة، غير أن هناك بعض الإشكاليات التي ما زالت تعترض تلك النظرية، والتي منها[105]:

-عدم قدرة المنظمات الدولية على التخلص من حالة الفوضى في الفضاء السيبراني: تُعوِّل النظريات الليبرالية على دور المؤسسات الدولية في التخلص من حالة الفوضى في العلاقات الدولية، لكن الواقع يشير إلى عكس ذلك، وبصورة خاصة حالة الفوضى في الفضاء السيبراني؛ فالمنظمات الدولية المعنية بإدارة الإنترنت مثل منظمة الأيكان "ICANN"[106] الخاصة بإدارة عناوين ونطاقات الإنترنت وكذلك الاتحاد الدولي للاتصالات، لا تستطيع التغلب على حالة الفوضى في الفضاء السيبراني[107].

-صعوبة تفسير حالة الأمن الجماعي في الصراعات السيبرانية: لم توفر الليبرالية إطارًا يمكن من خلاله فهم الأمن الجماعي السيبراني في ظل الإشكاليات التي يثيرها من صعوبة فنية في معرفة الطرف المعتدي من الأساس، ولم توضح أيضًا آلية يمكن من خلالها تحقيق الأمن الجماعي لمواجهة الصراعات السيبرانية، في ظل وجود حالة من التكتم على الأسرار التقنية بين الدول؛ للحفاظ على قوتها النسبية في مواجهة غيرها. و الأسلحة السيبرانية يمكن تطويرها واستخدامها من قبل فاعلين من غير الدول، ويعتبر النموذج الأبرز على ذلك دودة" ستاكس نت " التي اعتبرها البعض نموذجًا حقيقيًّا للحرب السيبرانية؛ حيث

---

[105]-إيهاب خليفة، الحالة السيبرانية في نظريات العلاقات الدولية: الحاجة إلى مراجعة جديدة، مرجع سابق، ص ص،12-14.

[106]- **ICANN**: (شركة الإنترنت للأسماء والأرقام المخصصة)، هي شركة خاصة وغير حكومية وغير ربحية، مسؤولة عن تخصيص مساحة عنوان بروتوكول الإنترنت (IP) وتعيين معلمات البروتوكول وإدارة نظام اسم المجال (DNS) ووظائف إدارة نظام خادم الجذر. سبق لهيئة أرقام الإنترنت المخصصة (IANA) أداء هذه الخدمات.

ما هو هدف ICANN ولماذا هو مهم؟

ICANN هي شراكة بين القطاعين العام والخاص مسؤولة عن الوظائف التالية المتعلقة بأسماء وأرقام الإنترنت: تخصيص مساحة عنوان IP،إدارة نظام اسم المجال من المستوى الأعلى، تعيين معرف البروتوكول، إدارة مجال المستوى الأعلى، إدارة جذر خادم نظام اسم المجال.

هذه الوظائف مهمة للحفاظ على استقرار الإنترنت العالمي ودعم الاتصال العالمي غير المنقطع. يجب على ICANN أن توازن بين المخاوف المحلية والوطنية والإقليمية والدولية أثناء إدارة DNS بطريقة مقبولة لغالبية مستخدمي الإنترنت في العالم.

تحكم مذكرة التفاهم (MoU) لعام 1998 بين ICANN ووزارة التجارة الأمريكية كيفية تعامل ICANN مع الوظائف المسؤولة عنها كمنظمة مستقلة ودولية.

(Peter Loshin, DEFINITION: ICANN (Internet Corporation for Assigned Names and Numbers), **TechTarget**, link: http://bitly.ws/Fvtm, seen on: 25.05.2023).

[107]- إيهاب خليفة، المرجع نفسه، ص ص،12-14.

استطاعت تدمير آلاف من أجهزة الطرد المركزية الإيرانية، مع ذلك لم يتم اكتشاف مصدره، أو تصريح دولة ما رسميًّا بأنها خلف هذا الهجوم[108].

أما بالنسبة لحالة المغرب والجزائر، نجد كثرة الاتهامات بينهما، دون قدرة أي طرف للوصول إلى مصدر الهجوم الحقيقي. وهذا دليل صارخ على صعوبة تطبيق النظرية الليبرالية في دراسة الحالة السيبرانية المغربية-الجزائرية.

نذكر في هذا الصدد، الهجوم الذي تعرض له الموقع الإلكتروني لاتحاد الشركات المغربي، بتاريخ 22 نونبر 2021، من طرف هاكر جزائري، حيث فوجئ الأشخاص الذين حاولوا زيارة موقع الويب بالعثور على صورة غير لائقة على الصفحة الأولى للموقع. وعرض الموقع العلم الجزائري برسالة تقول: "لا سلام بين الأنظمة". هذا الهاكر المهاجم لو لم يترك توقيعه مع العلم الجزائري على موقع CGEM المغربي، لما أشارت أصابع الاتهام إلى الجزائر[109]. وحتى إذا أشارت أصابع الاتهام إلى الجزائر، فمن الصعب الجزم بأن أجهزة الدولة هي الفاعل الرئيس في مثل تلك الهجومات.

وقد تزامن هذا الهجوم مع تصاعد التوتر بين المغرب والجزائر، حيث قطعت الجزائر العلاقات مع المغرب في أغسطس 2022، واتخذ النظام الجزائري منذ ذلك الحين العديد من الخطوات لاتهام المغرب بمجموعة واسعة من المؤامرات التي لم يتم إثباتها بعد والتي من الواضح أنها مفبركة من طرف الجزائر[110].

يضاف إلى ضعف النظرية الليبرالية في قراءة القضايا السيبرانية، العلاقة الجدلية بين الأمن والخصوصية الفردية. فالليبرالية لم تحسم هل يحق للدولة التجسس على الأفراد بداخلها ؟ وهل يحق للشركات التكنولوجية الكبرى العابرة للحدود أن تجمع المعلومات الشخصية عن الأفراد من مختلف دول العالم ؟[111]. لكن ما يجب معرفته، أن الدول المتقدمة في المجال الرقمي، أصبحت تتفاعل مع معطيات الأنترنت، وتركز عليها كثيرا، قصد القيام بدراسات استشرافية جد دقيقة، هذا من جهة، ومن جهة أخرى تحسبا لأي طارئ لا أمني.

---

[108]-إيهاب خليفة، الحالة السيبرانية في نظريات العلاقات الدولية: الحاجة إلى مراجعة جديدة، مرجع سابق، ص ص،12-14.

[109]-Safaa Kasraoui, Algeria's News Agency Accuses Morocco of Being Behind Latest Cyberattacks, Op.cit.

[110]-Ibid.

[111]-إيهاب خليفة، المرجع نفسه.

فتقنيات المعلومات الجديدة مقلقة بقدر ما هي مبهرة. كون الأدبيات تصر أكثر على قدرة الإنترنت على تحرير الفرد، لكنها بطريقة غير مباشرة تتحكم فيه عن طريق تلك الخوارزميات، على سبيل المثال (مايكروسوفت، فيسبوك، جوجل، آبل، أمزون والتي يعبر عنها اختصارا ب"GAFAM"[112]). ثم يأتي العمل على المعلومات بامتداد GAFAM إلى عالم السياسة، كما أظهرت اكتشافات " إدوارد سنودن[113]" بشكل كافٍ على ممارسات وكالة الأمن القومي[114].

فأشكال المراقبة الرقمية الحالية تتشابك فيها السياسة والتجارة والأمن في إدارة موحدة لآثار الأفراد، وتخضع-أي المراقبة- للصراع بين المنصات والدول والمواطنين. وهنا تبرر كلمات "تريستان هاريس" "Tristan Harris"، مبتكر المنظمة غير الحكومية "Time Well Spent"، والذي وفقًا له "قد يؤثر عدد قليل من الأشخاص على رأي مليار شخص من الناس في العصر الرقمي الحالي[115].

---

[112]-**GAFAM**: هو اختصار لخمسة أسهم تكنولوجية شهيرة في الولايات المتحدة: Google، Apple، Amazon، Facebook و Microsoft. إن GAFAM قريبة جدًا من اختصار FAANG الأكثر شيوعًا، ولكنها مع ذلك مختلفة عنها، والتي تشير مجتمعة إلى أسهم التكنولوجيا الأمريكية: Facebook و Apple و Amazon و Netflix و Google. في الأخير، يحل Netflix محل Microsoft. وعلى الرغم من وجود الكثير من مؤشرات السوق لتتبع بشكل جماعي تطورات القطاع ، إلا أن هناك عددًا قليلاً من الشركات التي تقود المجموعة من حيث تأثير القطاع. FAANG و GAFAM و BATX هي اختصارات للشركات المؤثرة التي لها تأثير كبير على قطاعاتها والسوق ككل.

تتكون GAFAM من (GOOGLE) و(AAPL) و(Facebook) (META) Meta سابقًا) و (AMZON) و( Microsoft). جميع الشركات الخمس مدرجة في بورصة ناسداك.

(Cory Mitchell, GAFAM Stocks, **Investopedia**, 15.09.2022, link: http://bitly.ws/FwIH, seen on: 25.05.2023).

[113]-**إدوارد سنودن**، بالكامل إدوارد جوزيف سنودن "Edward Snowden, in full Edward Joseph Snowden" (من مواليد 21 يونيو 1983، إليزابيث سيتي، نورث كارولينا، الولايات المتحدة)، مقاول المخابرات الأمريكية والمبلغ عن المخالفات الذي كشف في عام 2013 عن وجود برامج سرية واسعة النطاق لجمع المعلومات أجراها الأمن القومي وكالة (NSA). سلطت القضية الضوء على مجموعة من القضايا، بما في ذلك الاستخدام السري لسلطة الحكومة، والخصوصية في العصر الرقمي، وأخلاقيات الإبلاغ عن المخالفات، والدور الذي يمكن أن تلعبه الإنترنت والمتصفحات المجهولة على شبكة الإنترنت المظلمة مثل **Tor** في تسهيل مثل هذا الإبلاغ عن المخالفات.

في أغسطس 2014، مع انتهاء صلاحية منح سنودن للجوء المؤقت، منحته الحكومة الروسية تصريح إقامة لمدة ثلاث سنوات (اعتبارًا من 1 أغسطس)، والذي سيسمح له بمغادرة البلاد لمدة تصل إلى ثلاثة أشهر. تم تمديد التصريح في عام 2017، وتم منح سنودن الإقامة الدائمة في عام 2020. في سبتمبر 2022، منح الرئيس الروسيفلاديمير بوتين سنودن الجنسية الروسية.

(Michael Ray, Edward Snowden American intelligence contractor, **Britannica**, 22.05.2023, link: http://bitly.ws/GTjv, seen on: 03.06.2023).

[114]-Christophe Bezes et Maria mercanti-guérin, Stratégies d'acquisition des GAFAM: derrière le contrôle des technologies, celui des corps. Une analyse inspirée par Michel Foucault, 01.10.2021, lien de l'article: http://bitly.ws/CK3W, date visite : 09.04.2023, pp, 24-33.

[115]-Ibid.

وفي مقالهما "ثورة المعلومات والأمن والعلاقات الدولية"، أكد "إريكسون" و "جيوكوميلو" على أهمية التعاون للتخفيف من تهديد الهجمات السيبرانية. وهما يؤكدان أن "الحكومة وحدها لا تستطيع تأمين الفضاء السيبراني" . لكنهما لا يقترحان بديلاً حقيقياً. من **وجهة نظر نيوليبرالية** ، يمكن حل هذه المعضلة الأمنية من خلال إنشاء مؤسسات دولية[116]. وهذه المعضلة هي التي تعيشها شمال إفريقيا بصفة عامة، **والمغرب والجزائر** بصفة خاصة. فبدل خلق تكتل دفاعي سيبراني، يرصد مكامن الهجومات السيبرانية ويقضي عليها، نسجل اتهامات متبادلة بين المغرب والجزائر.

## الفرع الثاني: قراءة نقدية للدفاع السيبراني في المغرب والجزائر

النظرية النقدية لها معنى ضيق وواسع، في نفس الوقت، في الفلسفة وفي تاريخ العلوم الاجتماعية. تشير "النظرية النقدية" بالمعنى الضيق إلى عدة أجيال من الفلاسفة والمنظرين الاجتماعيين الألمان في التقليد الماركسي الأوروبي الغربي المعروف باسم مدرسة فرانكفورت. وفقًا لهؤلاء المنظرين، يمكن التمييز بين النظرية "النقدية" والنظرية "التقليدية" وفقًا لغرض عملي محدد: تعتبر النظرية بالغة الأهمية إلى الحد الذي تسعى فيه إلى "تحرر الإنسان من العبودية"، وتعمل بمثابة "تحرير ... تأثير "، وتعمل على" خلق عالم يلبي احتياجات وقوى البشر". نظرًا لأن مثل هذه النظريات تهدف إلى شرح وتحويل جميع الظروف التي تستعبد البشر، فقد تم تطوير العديد من "النظريات النقدية" بالمعنى الأوسع. لقد ظهرت بالارتباط مع العديد من الحركات الاجتماعية التي تحدد أبعادًا متنوعة لهيمنة البشر في المجتمعات الحديثة. ومع ذلك، في كل من المعنى الواسع والضيق، توفر النظرية النقدية الأسس الوصفية والمعيارية للبحث الاجتماعي الذي يهدف إلى تقليل الهيمنة وزيادة الحرية في جميع أشكالها[117].

---

[116]-Constantine J.Petallides, Cyber Terrorism and IR Theory: Realism, Liberalism, and Constructivism in the New Security Threat, **inquiries journal**, VOL. 4 NO. 03, 2012, link: http://bitly.ws/CH4T, seen on: 08.04.2023.

[117]-Ohman and others, Critical Theory, **The Stanford Encyclopedia of Philosophy (Spring 2021 Edition)**, link: http://bitly.ws/ETfJ, seen on: 19.05.2023.

من هذا المنطلق سعت الدراسة في هذا الفرع إلى قراءة الدفاع السيبراني في المغرب والجزائر قراءة نقدية، عرفت فيه المدرسة النقدية (الفقرة الأولى)، ثم مكانتها في المغرب والجزائر (الفقرة الثانية).

### الفقرة الأولى: ماهية المدرسة النقدية

تعد معرفة السياق التاريخي لظهور هذه النظرية أمرا مهما يساعد الباحث على قدر كبير في فهم التوجهات العامة لهذه النظرية والمواقف التي تتبناها منهجيا وعمليا. ظهرت النظرية النقدية في إنتاجات بعض المدارس الفكرية وإسهامات بعض المفكرين كاتجاه فكري في مجالات الفلسفة، علم الاجتماع والأنثروبولوجيا، إلا أن اسمها ارتبط بمدرسة فرانكفورت للبحث الاجتماعي سنة 1923، التي تتبنى في أبحاث مفكريها نظرة نقدية للمجتمع تركز على الجانب الاجتماعي العملي في السلوك وتسعى جاهدة للبحث عن الطاقات الكامنة في الحرية والعدالة والسعادة ، حين تمارس تحت ظروف وشروط تاريخية محددة وتهدف إلى بناء نظام اجتماعي أفضل يحقق تلك الطاقات والظروف[118].

تشغل النقدية حيزا مهما ضمن أهم النظريات "التأملية" التي برزت في ثمانينيات القرن العشرين، كرد فعل على هيمنة وإقصائية التيار العقلاني الممثل في التوليفة "نيو- نيو" (الواقعية الجديدة مع الليبرالية الجديدة)، وكمحاولة لتنقيح الإرث الماركسي وإعادة إحيائه وبعثه من جديد، ليصبح قادرا على المنافسة النظرية، وكمشروع فكري وعملي للعلاقات الدولية يتجاوز راهنها النظري (هيمنة النظريات العقلانية) وواقعها العملي (عالم رأسمالي) نحو آفاق جديدة من العدالة والمساواة بين الأفراد والمجتمعات والدول[119].

فنظرية العلاقات الدولية النقدية هي مجموعة متنوعة من المدارس الفكرية في العلاقات الدولية التي انتقدت الوضع النظري و/ أو الفوقي النظري و/أو السياسي الراهن، سواء في نظرية العلاقات الدولية وفي السياسة الدولية على نطاق أوسع - من المواقف الوضعية وما بعدها. تشمل الانتقادات الوضعية المقاربات الماركسية والماركسية الجديدة وبعض الخيوط ("التقليدية") البنائية الاجتماعية. تشمل انتقادات ما بعد البنيوية، ما بعد الاستعمار، النظرية "النقدية" البنائية والنقدية (بالمعنى الدقيق للكلمة المستخدمة من قبل

---

[118]- سعيدي ياسين، التحديات الأمنية الجديدة في المغرب العربي، مرجع سابق، ص.31.

[119]-محمد الطاهر عديلة، تطور الحقل النظري للعلاقات الدولية: دراسة في المنطلقات والأسس، مرجع سابق، ص.305 .

مدرسة فرانكفورت)، النيو جرامشي معظمهم النسوية، وبعض مناهج المدرسة الإنجليزية، وكذلك علم الاجتماع التاريخي غير الفيبري،"علم الاجتماع السياسي الدولي" و "الجغرافيا السياسية النقدية" وما يسمى بـ "المادية الجديدة" (مستوحاة جزئيًا من نظرية الممثل والشبكة). كل هذه الأساليب الأخيرة تختلف عن الواقعية والليبرالية في مقدماتها المعرفية والأنطولوجية[120].

يقصد بالنظرية النقدية تلك النظرية التي كان ينطلق منها رواد مدرسة فرانكفورت في انتقادهم للواقعية الساذجة المباشرة، فالنظرية النقدية تعني نقد النظام الهيجلي[121]، ونقد الاقتصاد السياسي، والنقد الجدلي. وتهدف هذه النظرية إلى إقامة نظرية اجتماعية متعددة المصادر والمنطلقات، كالاستعانة بالماركسية، والتحليل النفسي، والاعتماد على البحوث التجريبية. وبتعبير آخر، فالنظرية النقدية هي تجاوز" للنظرية الكانطية"[122]، والمثالية الهيجيلية، والجدلية الماركسية، فهي نقض للواقع، ونقد للمجتمع بطريقة سلبية إيجابية[123].

---

[120]-Francis Lokherd, Ortega Keith, International Relations Critical Theory, **Researchgate**, 01.07.2021, link: http://bitly.ws/yY8b, seen on: 16.01.2023.

[121]-**النظام الهيجلي**: نسبة إلى هيجل. ولِد جورج فيلهلم فريدريش هيجل في مدينة شتوتجارت عام 1770، وكان والده موظفًا صغيرا في بلاط دوقية فوتمبرج. وكان لديه أقارب يعملون مدرسين أو قساوسة في الكنيسة اللوثرية. في حقيقة الأمر، لا يوجد أي شيء استثنائي بوجه خاص فيما يتعلق بحياته، إلا أن العصر الذي عاش فيه كان شديد الأهمية على المستوى السياسي والثقافي والفلسفي. في عام 1789، تواترت عبر أوروبا أخبار سقوط سجن الباستيل، وهذه هي اللحظة التي كتب فيها الشاعر وردزوورث قولته الشهيرة:" أن تكون على قيد الحياة في فجر تلك الأحداث، فتلك نعمة، أما أن تكون شابا فقد أدركت الفردوس بعينه! كان هيجل حينها قد أوشك على إتمام عامه التاسع عشر، وقد أطلق هو أيضا على الثورة الفرنسية فيما بعدَ اسم «الفجر المجيد»، مضيفًا أن: «كل الناس شاركوا في الاحتفال بهذا العهد.» وقد شارك فيها بنفسه في صباح يوم أحد في فصل الربيع حين ذهب مع مجموعة من زملائه الطلاب لغرس شجرة حرية كرمز لبذور الآمال التي نثرتْها الثورة.( **بيتر سينجر، هيجل مقدمة قصيرة جدا ، ترجمة: محمد إبراهيم السيد، مؤسسة هنداوي للتعليم والثقافة، مصر، ط1، 2015**، ص.14.

[122]-**النظرية الكانطية**: قامت فلسفة كانط الترانسندنتالية transcendentale النقدية على نقد ودحض المذهب العقلي (ديكارت) والمذهب التجريبي- الحسي (لوك وهيوم) . باعتبار أن المعرفة المنبثقة عن الاتجاه العقلي لا تقوم على محتويات تجريبية – حسية، بل تنتج عن تفكير منطقي استنباطي. ذلك أن العقليين في عصر التنوير اعتبروا أن العالم منظم حسب قوانين، ويمكن معرفة هذا العالم عبر العقل والاستدلال المنطقي انطلاقا من مقدمات صحيحة ودون اللجوء إلى المعطيات الحسية (ديكارت)، وهذا ما يرفضه كانط.(المختار شعالي، نظرية المعرفة عند كانط، **هسبريس**،01.04.2017، رابط المقال:http://bitly.ws/nmQa ، تاريخ الدخول 19.05.2023).

فاستقلال العقل، هو المبدأ العام للفلسفة في **عصر كانط**، حرص فيه على شرح: قدرة العقل من الناحية النظرية الفكرية، أو الناحية العملية الأخلاقية. و ما يستطيع الإنسان معرفته، وما يجب عمله؟ ويأمل بلوغه. في كتاب(نقد العقل الخالص). بين كانط للتجريبيين والعقليين أخطاءهم في طرق الوصول إلى المعرفة وإمكانها، ومدى تحققها في الوجود الخارجي. وبين للحسيين والتجريبيين ضعف نظريتهم في المعرفة المستمدة من الحواس. و انتقد اكتفاء العقليين بفطرة العقل للحصول على المعرفة، دون الرجوع إلى الحواس والعالم الخارجي.( عايدة عبد الحميد عبد الرحمن، نظرية المعرفة عند كانط، **بنك المعرفة المصري**، 2017، رابط المقال: http://bitly.ws/EUvt، تاريخ الدخول 19.05,2023، ص:8)

[123]- حيدر فالح زايد، النظرية النقدية، رابط المقال:http://bitly.ws/zcco، تاريخ الدخول: 20.01.2023، ص.2.

تبدأ النظرية النقدية باعتقاد راسخ أن العمليات المعرفية ذاتها تتأثر بالمصالح السياسية، وأن نظريات العلاقات الدولية ليست استثناء مما سبق، فهي تصاغ من خلال التأثيرات الاجتماعية، الثقافية والإيديولوجية، وبالتالي فإن مهام النظرية النقدية هو الكشف عن أثر هذه المحددات، فأولى بوادر ظهور النظرية النقدية كمقاربة جديدة لدراسة العلاقات الدولية بدأت معالمها منذ 1976، عندما كتب روبرت كوكس "Robert Cox " في مؤلفه الشهير " التفكير حول مستقبل النظام العالمي" The Thinking about The futur of the world order"، والذي أظهر من خلاله غياب الخاصية النقدية لإسهامات النظريات الوضعية في العلاقات الدولية[124].

وتهدف النظرية النقدية حسب هوركايمر إلى تحقيق مهام ثلاث[125]:

أولها، الكشف في كل نظرية عن المصلحة الاجتماعية التي ولدتها وحددتها، وهنا يتوجه هوركايمر، كما فعل ماركس، إلى تحقيق الانفصال عن المثالية الألمانية، ومناقشتها في ضوء المصالح الاجتماعية التي أنتجتها.

والمهمة الثانية للنظرية النقدية عنده، هي أن تظل هذه النظرية على وعي بكونها لا تمثل مذهبا خارج التطور الاجتماعي التاريخي .فهي لا تطرح نفسها باعتبارها مبدأ إطلاقيا، أو أنها تعكس أي مبدأ إطلاقي خارج صيرورة الواقع. والمقياس الوحيد الذي تلتزم به هو كونها تعكس مصلحة الأغلبية الاجتماعية في تنظيم علاقات الإنتاج بما يحقق تطابق العقل مع الواقع، وتطابق مصلحة الفرد مع مصلحة الجماعة.

أما المهمة الثالثة، فهي التصدي لمختلف الأشكال اللامعقولة التي حاولت المصالح الطبقية السائدة أن تلبسها للعقل، وأن تؤسس اليقين بها على اعتبار أنها هي التي تجسد العقل، في حين أن هذه الأشكال من العقلانية المزيفة ليست سوى أدوات لاستخدام العقل في تدعيم النظم الاجتماعية القائمة، وهو ما دعاه "هوركايمر" بالعقل الأذاتي."

وقد أغفلت النظريات التقليدية الإلمام بجميع أبعاد الأمن السيبراني؛ وذلك لأنها تجاهلت البعد القيمي المعياري، غير أن النظريات النقدية خصصت حيزا مهما للأبعاد المعيارية، يظهر هذا الحيز في تزايد ارتباط العالم بثورة المعلومات، وتغيُّر منظومة القيم في

[124]-سعيدي ياسين، التحديات الأمنية الجديدة في المغرب العربي، مرجع سابق، ص.32.
[125]-حيدر فالح زايد، النظرية النقدية، مرجع سابق، ص ص، 2-3.

المجتمعات، كما حذرت النظرية النقدية من مخاطر الخصوصية غير المقيدة والروابط الحصرية التي تقود إلى غربة بين المجتمعات وإلى احتمال نشوب حرب أو إقصاء اجتماعي. وهي ترى أن سلوك الدول وتفاعلاتها في العلاقات الدولية تتبع الطريقة التي تفكر بها، وأن بنية النظام الدولي ليست بنية تراتبية مادية لوحدات هذا النظام، وإنما هي نتاج للتفاعلات الاجتماعية بين وحداته. وضمن هذا البناء الاجتماعي للنظرية النقدية، تكون التوزيعات المادية محددة بشكل كبير لسلوكيات الدول، لكنها ليست وحدها فهناك عنصر المعرفة بين الدول وخبرة التعاطي مع حالات التفاعل وعملية الإدراك المشترك، وهي كلها عوامل تفيد في تشكيل بنية النظام الدولي ومساراته التفاعلية[126].

## الفقرة الثانية: الواقع السيبراني المغربي-الجزائري من منظور النظرية النقدية

إن تركز جميع المعلومات والبيانات الضخمة لدى المؤسسات الحكومية، قد يصبح أحد أدوات تهديد حرية الأفراد داخل الدولة، أو حتى تهديد مسار العملية الديمقراطية داخل الدولة من خلال مؤسسات الدولة الداخلية نفسها. فقد تستغل الحكومات البيانات الضخمة الصادرة من الأفراد في تدعيم موقفها الانتخابي، وبالتالي الاستحواذ على مراكز القرار وعلى السلطة لسنوات عديدة، ومن ثمَّ تأتي هنا أهمية المدارس النقدية التي تولي اهتماما لدور الفرد في مواجهة الدولة، مثل مدرسة أبريستويث[127]، ومدرسة باريس، كما لا يمكن أن

---

[126]-إيهاب خليفة، الحالة السيبرانية في نظريات العلاقات الدولية: الحاجة إلى مراجعة جديدة، مرجع سابق.

[127]-**مدرسة أبريستويث**: أبريستويث بلدة صغيرة تقع على الساحل الغربي من ويلز، وتعتبر معقل أول قسم للسياسة الدولية في العالم "كرسي ويدرو ويلسون الذي تأسس عام"1919، والتي أصبحت مع بداية التسعينيات معقل المقاربة النقدية للأمن بقيادة علماء مثل "كين بوث" و"ريتشارد واين جونز"، أما كحركة فكرية وكتيار تنظيري تعود الجذور الأولى للمدرسة الإنجليزية إلى بداية الخمسينيات من القرن الماضي، وذلك عبر ما يسمى اللجنة البريطانية لنظرية السياسات الدولية، ويعتبر "روي جونس "أول من أشار إلى المدرسة في مقال نشره في مجلة الدراسات الدولية سنة 1981. ومن بين مؤسسي هذه المدرسة نجد: "شارلز مانينج" و"مارتن وايت" حيث مرت هذه المدرسة بأربعة مراحل أساسية يمكن تلخيصها فيما يلي؛-**المرحلة الأولى :** امتدت من سنة 1959 من خلال إنشاء اللجنة البريطانية إلى سنة 1966مع نشر كتاب" التحقيقات الدبلوماسية" لكل من "باترفلد" و "وايت"؛ -**المرحلة الثانية :**امتدت من 1966 إلى سنة 1977 حيث تميزت بإسهامات كل من "وايت" في عمله "أنظمة الدول" و"هيدلي بول" في "المجتمع الفوضوي" وكذلك "فانسون" في عمله "عدم التدخل"؛ - **المرحلة الثالثة**: امتدت من سنة 1977 إلى غاية ،1992 التي تميزت بإسهامات كل من "بول واطسن "في عمله" توسع المجتمع الدولي،" وكذلك " فانسون" في عمله "السياسة الخارجية وحقوق الانسان"؛ -**المرحلة الرابعة :**تبدأ من سنة 1992 إلى غاية اليوم، ويتعلق الأمر بوصول جيل جديد من المفكرين والخبراء لا يرتبطون باللجنة البريطانية، بحيث سايرت مقارباتهم مختلف السياقات والتطورات الحاصلة في نظرية العلاقات الدولية من خلال " الدراسات الدولية البريطانية" و"جمعية الدراسات الدولية"، حيث أن هاتين المؤسستين تهدفان إلى إعادة تنظيم المدرسة الإنجليزية من خلال مجموعة من المفكرين أمثال " جاكسن بيس"، و "ريتشارد ليتل"، و"نيكولاس رينج"، وغيرهم.. ليشكلوا ما يعرف بالمدرسة الانجليزية الجديدة.(صباح بالة، مدرسة ويلز (أبريستويث) للدراسات الأمنية، **الموسوعة السياسية الجزائرية**، 09.12.2022، رابط المقال:http://bitly.ws/EUF8 ، تاريخ الدخول 19.05.2023)

نغفل مدرسة كوبنهاجن[128]. فالنظريات النقدية سواء الوضعية مثل الليبراليين الجدد والتعددين "Pluralists " والتضامنيين"solidarists"، أو ما بعد الوضعية مثل ما بعد الحداثة والمحافظين"constructivist"، ترى أن" الفرد "في حد ذاته قد يصبح هو مستوى التحليل، وليس الدولة كما في حالة الواقعية، أو النظام الدولي كما في حالة الليبرالية. والنماذج التي توضح ذلك عديدة، منها نموذج "جوليان أسانج"، ونموذج "إدوارد سنودن"؛ حيث استطاع كلٌّ منهما أن يؤثر ليس فقط في الأمن القومي للولايات المتحدة الأمريكية من خلال نشر العديد من الوثائق السرية الحكومية، أو من خلال تسريب برامج التجسس السرية التي تقوم بها أجهزة الأمن القومي الأمريكي، بل استطاع أيضًا أن يؤثر في النظام الدولي كله، وتسبَّب ذلك في توتُّر العلاقات بين الولايات المتحدة وأشد حلفائها مثل ألمانيا وفرنسا. ومع ذلك لا يمكن القول إن النظريات النقدية هي الأقدر على تفسير حالة التهديدات السيبرانية؛ حيث تواجه قصورًا منهجيًّا على عدة مستويات، وهي[129]:

-الفاعل قد يكون غير معروف من الأساس: وذلك بسبب طبيعة التهديدات المعقَّدة الناجمة عن التهديدات السيبرانية، فمثلًا قد يكون التهديد الخارجي للدولة قادمًا من مجموعة من القراصنة الهواة الخارجين عن سيطرة الدولة الأخرى، وقد يكونون مستأجرين من دولة داخل إقليم دولة أخرى، وقد يكونون تابعين لدولة ومجندين في جيوشها النظامية ولكن الدولة لا تعلن ذلك صراحة، وقد يكونون متفرقين بين أكثر من دولة، وهذه هي الحالة الطبيعية في الحروب السيبرانية، حيث يتم شنُّ الهجمات على الدولة المستهدفة من أجهزة كمبيوتر منتشرة حول العالم، بما فيها الدولة محل الهجوم، وليس من إقليم دولة واحدة؛

---

[128]-**نشأة مدرسة كوبنهاغن للدراسات الأمنية**: تحيل تسمية "مدرسة كوبنهاغن" إلى الأجندة البحثية لمجموعة من الباحثين الأكاديميين في "معهد كوبنهاغن لأبحاث السلام" في الدانمارك، الذي تم إنشاؤه عام 1985وكان أول من أطلق عليها هذه التسمية هو"بيل ماك سويني " عام، 1996 في إشارة منه إلى الإسهامات النظرية لكل من "باري بوزان" و " أول وايفر" وآخرون ممن شاركهما برنامج البحث، فمنذ صدور الطبعة الأولى من كتاب "الناس، الدول والخوف: مشكلة الأمن القومي في العلاقات الدولية" عام 1983 أصبح عمل "بوزان "مرجعا لا غنى عنه لدارسي الأمن، ولقد حفزت الطبعة الثانية المنقحة من نفس المؤلف الصادرة عام، 1991 مجموعة من الباحثين إلى مواصلة التعمق في استكشاف المشكلة الأمنية إلى جانب "بوزان"، بحيث يشكل هذا الأخير منبرا نظريا هاما لدراسة الشؤون الأمنية ولقد تم إغلاقه سنة 2014م ، لكن وعلى مدى 13سنة نجح المشروع في تحقيق درجة كافية من التماسك والاستمرارية لتبرير استخدام مصطلح مدرسة من خلال ضمان مشاركة الحد الأدنى من العلماء والباحثين المنخرطين فيه.
(صباح بالة، مدرسة كوبنهاغن في تفسير الدراسات الأمنية، مرجع سابق).

[129]-إيهاب خليفة، الحالة السـيبرانية في نظريات العلاقات الدوليـة: الحاجة إلى مراجعة جديدة، مرجع سابق.

-غير قادرة على تفسير حالة الفوضى وعدم اليقين التي تسيطر على الفضاء الإلكتروني: حيث تقوم الدول بالتجسس على بعضها البعض بما فيها الدول الحلفاء، مثل ما كشف عنه "إدوارد سنودن "من تجسُّس الولايات المتحدة على حلفائها في أوروبا (مثل ألمانيا وفرنسا)، فجميع الدول تسعى نحو تحقيق مصالحها والحفاظ على أمنها القومي بأي طريقة كانت؛

-التحيُّز في التعبير عن مصالح الأقليات والمهمشين والمرأة: فعادة ما تنادي النظرية النقدية بالأخذ في الاعتبار المنظورات غير السائدة في دراسة العلاقات الدولية مثل أصوات الأقليات والمرأة والمصالح غير الغربية، في الوقت الذي يصعب فيه إعادة هيكلة الفضاء السيبراني للتعبير عن هذه الأصوات. ففي الدول الديمقراطية والتي تكفل فيها القوانين إعطاء مساحات لهذه الفئات لممارسة التأثير، فإن الطبيعة المركبة للفضاء الإلكتروني قد لا تسمح في بعض الأحيان بالتأثير عبر الفضاء السيبراني، فعلى سبيل المثال شهدت الانتخابات الأمريكية عام 2016، فضيحة "كامبريدج أناليتكا"[130]، حيث أسهم موقع "الفيس بوك" بطريقة غير مباشرة في تغيير توجُّهات الناخبين وطريقة تصويتهم في الانتخابات. ثم تكرَّر الأمر بصورة مشابهة عام 2021، حينما أعلنت موظفة منشقة عن "الفيس بوك " أن الخوارزميات التي تستخدمها الشركة تعلي معايير النمو والانتشار والتوسع على معايير الأمان والسلامة، وهي في ذلك تعطي الأولوية للمنشورات التي تحصل على أكبر قدر من الانتشار والمشاركات بغض النظر عما إذا كانت هذه المنشورات تعمِّق الانقسامات وحالات الاستقطاب أم لا، بما يعني في النهاية أن الفكر النقدي ذاته قد لا يصلح للفضاء الإلكتروني الذي هو – على المستوى النظري- جاء ليدعمه ويؤكده.

---

[130]- **فضيحة "كامبريدج أناليتكا**:"Cambridge Analytica scandal": كشف موقع Facebook عن بيانات تصل إلى 87 مليون مستخدم على Facebook لباحث عمل في Cambridge Analytica ، والتي عملت في حملة ترامب.
تم إنشاء"Cambridge Analytica " عندما اقترب"Steve Bannon " من المحافظين العملاقين"Rebekah " و " Robert Mercer"لتمويل شركة استشارات سياسية. أصبح بانون نائبًا لرئيس"Cambridge Analytica "، وخلال انتخابات عام 2016، تواصل مع حملة ترامب للتعريف بالطرفين. وبطبيعة الحال، أصبح بانون في نهاية المطاف مستشارًا كبيرًا لترامب قبل إقالته في أغسطس 2017.
كتب "مارك زوكربيرج" "Mark Zuckerberg"، المؤسس والرئيس التنفيذي لشركة Facebook، ردًا على هذه الفضيحة، "لقد كنت أعمل على فهم ما حدث بالضبط وكيفية التأكد من عدم حدوث ذلك مرة أخرى. النبأ السار هو أن أهم الإجراءات لمنع حدوث ذلك مرة أخرى اليوم اتخذناها بالفعل منذ سنوات. لكننا ارتكبنا أخطاء أيضًا، وهناك المزيد لنفعله، ونحن بحاجة إلى تصعيد الأمور والقيام بذلك ".
(Alvin Chang, The Facebook and Cambridge Analytica scandal, explained with a simple diagram, **Vox**, 02.05.2018, link: http://bitly.ws/HGgT, seen on: 08.06.2023).

أما ما يتعلق بمنطقة شمال إفريقيا-المغرب والجزائر نموذجا-، لو أردنا قراءتها من واقع - التحيُّز في التعبير عن مصالح الأقليات والمهمشين والمرأة، نسجل في هذا الباب، محاولة الجزائر تقمص هذا الدور، **من خلال تحيزها لأقلية مرتزقة-البوليساريو-**، تخلق مشكلة متجدرة في خصر المملكة المغربية، رغم كونها مشكلة ارتبطت بمخلفات الاستعمار وطريقة ترسيمه للحدود المغربية. وهذا ما أشار إليه المفكر الروسي دوغين. فهناك حقيقة تاريخية وجغرافية يؤكدها دوغين في كتابه، "أسس الجيوبولتيكا: مستقبل روسيا الجيوبولتيكي"، يحتل المغرب بالضمنية، في هذا الكتاب، موقع "الصديق بالطبيعة للإمبراطورية الروسية". في ذلك يقول دوغين: "لا يتبقى إلا العالم الإسلامي الممتد من الفيليبين والباكستان حتى بلدان "المغرب" أي إفريقيا الغربية. وعلى العموم فإن المنطقة الإسلامية واقع جيوبولتيكي صديق بالطبيعة للإمبراطورية الأوراسية لأن التقليد الإسلامي أكثر تسييسا وتحديثا من غالبية المذاهب الدينية الأوروبية الأخرى"[131].

وبخصوص قضية الصحراء المغربية، فإن دوغين يربطها بمحددين أساسيين هما: التاريخ الإمبراطوري للمملكة المغربية، والسياسة الاستعمارية والحدود الموروثة عنها (كانت ظالمة للمغرب وما زالت). وما يجعل المغرب "مركزا للتاريخ والحضارة بالمنطقة المغربية "هو تشبثه بحقوقه التاريخية"، وتمسكه بمبادئه". ما يغفل عنه كثير من الناس، منهم مغاربة، هو ما يؤكده دوغين بقوله: "الأمر لا يتعلق بحدود الدولة الوطنية، بل يرتبط بمساحة الإمبراطورية المغربية التي ما زالت حاضرة إلى اليوم". يعاني المغرب وروسيا، بالنسبة للفيلسوف الروسي، من نفس المشكل ( مشكل تآكل أراضيهما من قبل القوى الأوروبية)، وينحوان نفس المنحى في الدفاع عن حقوقهما؛ منحى التمسك بالحقوق التاريخية والتشبث بالمبادئ الخاصة) [132].

وبناء على ما سبق، يمكن استنتاج حقيقة علمية، هو أن النظريات الثلاث تتكامل في ما بينها. لا توجد نظرية قادرة على تفسير جميع الظواهر السياسية بصورة عامة، فهذه ليست وظيفة النظرية، بل حتى الظواهر الصغيرة والمحدودة، قد تفشل النظرية الواحدة في الإلمام

---

[131]-محمد زاوي، نظرية دوغين.. أي موقع للمغرب في فكرة أوراسيا؟، **هوية بريس**، 09.10.2022، رابط المقال: http://bitly.ws/xTR5، تاريخ الدخول: 15.12.2022.

[132]-المرجع نفسه.

بجميع أبعادها في العلوم الاجتماعية. وطالما نتحدث عن ثورة صناعية رابعة لها تداعيات على المجالات كافة، فنحن في حاجة إلى تكامل النظريات؛ حتى يمكن رؤية تداعياتها على الأمن القومي بصورة أوضح[133].

قد تفشل النظريات التقليدية للعلاقات الدولية في الإلمام بجميع أبعاد الأمن في ظل التطورات التكنولوجية؛ وذلك لأنها تغفل البعد القيمي المعياري في العلاقات والذي تؤكده النظريات النقدية، وتجعل-أي النظريات التقليدية- الدولة هي الفاعل الرئيس في العلاقات الدولية، كما أن حالة الحرب التي يمكن القضاء عليها من وجهة نظر المدرسة الليبرالية من خلال الديمقراطية والتجارة الحرة، هي أيضًا محل تهديد في ظل التقنيات الذكية، وهوما يضعف من قدرة النظريات التقليدية على فهم التهديدات الأمنية غير التقليدية[134].

كما لا تقدم النظريات التقليدية أدوات تحليلية لفهم بعض التهديدات الأمنية غير التقليدية؛ فالأسلحة وبخاصة السيبرانية لم تعد حكرًا على الدولة مثلما تحاجج الواقعية، بل أصبحت متاحة للأفراد ويتم استخدامها في شنِّ الهجمات السيبرانية. وبالتالي فإن" الفرد "في حد ذاته قد يصبح هو مستوى التحليل كما ترى النظريات النقدية، وليس الدولة كما في حالة الواقعية، أو النظام الدولي كما في حالة الليبرالية، وقد تصبح "الجماعة "هي مستوى التحليل؛ مثل الحركات الإرهابية والمنظمات الإجرامية، وهناك أيضًا مجموعات تمارس العنف عبر الفضاء السيبراني لدواع قيمة وأهداف إنسانية مثل مجموعة "أنونيموس" Anonymous[135]. وقد يكون مستوى التحليل هو" الشركات "والتي تتبنَّى مبادرات إنشاء المدن الذكية وتشغيلها، مثل "أي بي أم "و"سيسكو "و"سيمنز"، وبالتالي لا يمكن إغفال دورها في تهديد الأمن القومي للدول[136].

ومع ذلك، لا يمكن القول إن النظريات النقدية هي الأقدر على تفسير حالة التهديد السيبراني؛ حيث تواجه قصورًا منهجيًّا؛ فالفاعل قد يكون غير معروف من الأساس، كما أن النظريات النقدية غير قادرة على تفسير حالة الفوضى وعدم اليقين التي تسيطر على الفضاء السيبراني. وهو ما يعني أنه لا تستطيع نظرية واحدة سواء كانت تقليدية أو نقدية تفسير

---

[133]-إيهاب خليفة، الحالة السـيبرانية في نظريات العلاقات الدوليـة: الحاجة إلى مراجعة جديدة، مرجع سابق.
[134]-المرجع نفسه.
[135]- المرجع نفسه.
[136]-المرجع نفسه.

ظاهرة التهديدات السيبرانية؛ لما لها من تعقيدات تكنولوجية وفنية غير مسبوقة، تحتاج إلى تكامل النظريات حتى يمكن فهم أبعادها [137].

ما يمكن استنتاجه أنه لا يمكن قراءة الواقع السيبراني، الجزائري-المغربي، بنظرية واحدة، بل يجب الاعتماد على تلك النظريات الثلاث، للخروج بقراءة شبه متكاملة للدفاع السيبراني في هذين البلدين. بل لابد من الانفتاح على النظريات المتبقية، وإسقاطها على التجربتين معا، حتى تتضح معالم السيبرانية في منطقة شمال إفريقيا؛ المغرب والجزائر نموذجا.

## المبحث الثاني: التهديدات السيبرانية وتداعياتها في المغرب والجزائر

في بانوراما التهديد السيبراني، على سبيل المثال لعام 2022، تستعرض الوكالة الوطنية لأمن أنظمة المعلومات (ANSSI) اتجاهات التهديد السيبراني الرئيسية. تلاحظ أنه على الرغم من انخفاض عدد هجمات برامج الفدية التي تم توجيه انتباه ANSSI إليها، إلا أن خطر التجسس على الكمبيوتر لا يزال كبيرًا على جل الدول، حيث قام مرة أخرى بتعبئة فرق الوكالة بقوة. فالمهاجمون أصبحوا أكثر كفاءة من أي وقت مضى؛ يستلهمون أساليب الجريمة السيبرانية ويستخدمون بشكل متزايد برامج الفدية لأغراض زعزعة الاستقرار في سياق عمليات التخريب الحاسوبي. بل إن استهدافهم آخذ في التغير وهم يسعون الآن للحصول على وصول سري ودائم إلى شبكات ضحاياهم. وبالتالي يحاولون اختراق المعدات الطرفية (جدران الحماية أو أجهزة التوجيه). ينعكس هذا الاستهداف المحيطي أيضًا في نوع الكيانات المعرضة للخطر، ويؤكد اهتمام المهاجمين بمقدمي الخدمات والموردين والمقاولين من الباطن والهيئات التنظيمية والنظام البيئي الأوسع لأهدافهم. وتبقى المكاسب المالية والتجسس وزعزعة الاستقرار أهم الأهداف الأساسية للمهاجمين[138].

للوقوف أكثر على تلك التهديدات، وبالخصوص في المغرب والجزائر، سعت الدراسة إلى تناولها عبر مطلبين؛ المطلب الأول ارتبط بالتهديدات السيبرانية تجاه البلدين، والمطلب الثاني ركز على تصنيف حوادث الأمن السيبراني فيهما.

---

[137]-إيهاب خليفة، الحالة السيبرانية في نظريات العلاقات الدولية: الحاجة إلى مراجعة جديدة، مرجع سابق.

[138]-Agence nationale de la sécurité des systèmes d'information, Un niveau élevé de cyber menaces en 2022, **ANSSI**, 2022, lien de l'article : http://bitly.ws/EWLH, date visite : 20.05.2023.

## المطلب الأول: التهديدات السيبرانية تجاه البلدين

يعاني البلدان، المغرب والجزائر، من تهديدات سيبرانية متفاوتة الخطورة، ما فتئت الجهات الرسمية تقوم بإحصائها والتصريح بها. وغالب تلك التصريحات تكون عبارة عن تهم متبادلة بين البلدين، خصوصا من الجانب الجزائري، حيث يتهم في حالات عدة جاره المغرب دون اعتماد على مرجعية علمية دقيقة في الميدان. وهذا ما أشارت إليه الجهات الرسمية المغربية في مناسبات عدة. غير أن التهديدات في تلك البلدين لا يمكن حصرها في تهديدات خارجية فقط، بل حتى من الداخل يمكن أن تتعرض لتهديدات حقيقية فتاكة.

لهذا السبب ارتأت الدراسة تناول تلك التهديدات من خلال زاويتين؛ واحدة ارتبطت بالتهديدات الداخلية لكلا البلدين( الفرع الأول)، وأخرى ارتقت إلى التهديدات الخارجية(الفرع الثاني).

### الفرع الأول: التهديدات الداخلية

أصبح الفضاء السيبراني منعدم الحدود ومتسع المجال، وأضحت هجماته غير واضحة الجهة المسؤولة عنها. وأمست الهجومات السيبرانية الداخلية، في كثير من الأحيان، أكثر عدوانا وتخريبا من غيرها. حاولت الدراسة تعداد التهديدات السيبرانية على البلدين (الفقرة الأولى)، ودراسة مدى حدتها (الفقرة الثانية).

#### الفقرة الأولى: مقارنة إحصائية للهجمات السيبرانية على البلدين

أصبح الأمن السيبراني مصدر قلق عالمي متزايد؛ والدراسات الإحصائية أثبتت صحة ذلك. وفقًا لدراسة منجزة من طرف Kaspersky[139]، في عام 2020، اكتشفت منتجات Kaspersky 5.7 مليون حزمة تثبيت ضارة، و 156.710 من أحصنة "طروادة" المصرفية عبر الهاتف المحمول الجديدة، و 20708 من برامج الفدية المتنقلة الجديدة[140].

---

[139]-كاسبرسكي: "Anti-Virus kaspersky" برنامج يحمي جهاز الكمبيوتر من التهديدات المعروفة والجديدة وهجمات الشبكة والحيل. لأداء المهام المتعلقة بالحماية الشاملة، يقدم برنامج كاسبرسكي وظائف متنوعة ووحدات الحماية.
تم تطوير وحدات الحماية لحماية أجهزة الكمبيوتر من التهديدات المعروفة والجديدة، هجمات الشبكات والاحتيال. يتم التعامل مع كل نوع من التهديدات بواسطة وحدة نمطية معينة. يمكن تمكين الوحدات النمطية وتعطيلها وتكوينها بشكل مستقل عن بعضها البعض.
(Manuel de l'utilisateur, Kaspersky Anti-Virus, 2015, **Kaspersky**, lien de l'article : http://bitly.ws/KFEg, date visite : 07.07.2023).

[140]-Toms Dumpis, Cybersecurity During the Pandemic, Morocco in Top 5 Most Afflicted, **morocco world news**, 15.05.2021, link: http://bitly.ws/zqjn, seen on: 26.01.2023.

حسبما أشارت كاسبرسكي في تقريرها السنوي لسنة 2020، يعد كل من المغرب والجزائر من بين البلدان الخمس الأولى من نسبة المستخدمين الأكثر تضرراً الذين يتعرضون للهجوم من خلال البرامج الضارة للأجهزة المحمولة[141].

تتصدر إيران الإحصاء باعتبارها الدولة الأكثر تضررًا، حيث اكتشفت شركة Kaspersky أن 67.78٪ من مستخدمي الهواتف المحمولة في البلاد قد تعرضوا لهجمات من قبل البرامج الضارة للأجهزة المحمولة. تليها الجزائر في المرتبة الثانية، مع تضرر 31.29٪ من مستخدمي الهاتف المحمول، وتأتي بنغلاديش في المرتبة الثالثة، حيث تعرض 26.18٪ من مستخدمي الهاتف المحمول للهجوم. وجاء المغرب في المرتبة الرابعة بنسبة 22.67٪، تليه نيجيريا في المرتبة الخامسة، حيث أصيب 22٪ من مستخدمي الهاتف المحمول[142].

وفقًا لشركة الأمن السيبراني "Trend Micro"، فإن رسائل البريد الإلكتروني الخبيثة هي التهديد الرقمي الأكثر شيوعًا في المغرب. أعلنت"Trend Micro" أن برنامجها نجح في حظر أكثر من 16.2 مليون تهديد للبريد الإلكتروني في المغرب في الأشهر الستة الأولى من عام 2020. وأشار الفرع التابع للشركة في المغرب مؤخرا في مؤتمر صحفي لتقديم تقريرها نصف السنوي عن الأمن، أن ثاني أكثر التهديدات الرقمية شيوعًا في المغرب، وفقًا لـ Trend Micro، هو تطبيقات الهاتف المحمول الخبيثة. اكتشف برنامج الشركة أكثر من 4.5 مليون تطبيق للهواتف المحمولة تحتوي على فيروسات، من يناير حتى يونيو. كما منعت Trend Micro الوصول إلى ما يقرب من 600000 رابط إنترنت ضار في نفس الفترة. منتجات الشركة المضادة للفيروسات والأمن السيبراني موجهة بشكل أساسي للأعمال وتستخدم على نطاق واسع من قبل الشركات المغربية، وكذلك بعض المؤسسات العامة[143].

---

[141]-Toms Dumpis, Cybersecurity During the Pandemic, Morocco in Top 5 Most Afflicted, Op.cit.

[142]- Ibid.

[143]-Yahia Hatim, Malicious Emails Represent Most Frequent Digital Threat in Morocco, **Morocco world news**, 16.10.2020, link: http://bitly.ws/zqou, seen on: 27.01.2023.

وبحسب محمود صفوت ، المدير العام لشركة Trend Micro Morocco ، فقد زاد عدد التهديدات الرقمية في البلاد بشكل كبير خلال جائحة COVID-19. وأوصى صفوت "على مديري تقنية المعلومات تكييف استراتيجياتهم الأمنية وشحذها من أجل الاستجابة للتهديدات الجديدة الناشئة". وأضاف: "يجب أن نبدأ في التركيز أكثر على حماية نقاط النهاية البعيدة، وأنظمة السحابة، وأنظمة تعريف المستخدم"[144].

كما شجع خبير تكنولوجيا المعلومات الشركات في المغرب على تنظيم دورات تدريبية من أجل زيادة وعي موظفيها حول التهديدات الرقمية، خاصة وأن عددًا كبيرًا من الشركات قد تحولت إلى العمل عن بعد أثناء الوباء. تعد الزيادة في انتهاكات الأمن السيبراني في المغرب خلال COVID-19 جزءًا من اتجاه عالمي. وفقًا لأرقام Trend Micro، تم اكتشاف أكثر من 27.8 مليار تهديد رقمي في النصف الأول من عام 2020. يمثل الرقم زيادة بنسبة 36٪ مقارنة بما كان عليه قبل ستة أشهر، قبل أن يجبر جائحة COVID-19 ملايين الموظفين حول العالم على العمل من المنزل[145].

غير أنه بالرغم من حقيقة أن المغرب احتل في وقت سابق من العام المرتبة الأولى بين الدول العشر الأولى من حيث الحجم الأكبر من هجمات البرمجيات الخبيثة، وفقًا لدراسة أخرى أجرتها شركة Kaspersky، إلا أن الشركة أشارت إلى أن غالبية الناس في المغرب كانوا غير مبالين بالأمن السيبراني في ذلك الوقت. أفاد التقرير أن فقط 8٪ من الأشخاص الذين تم استجوابهم بأنهم يستخدمون أي نوع من برامج مكافحة الفيروسات. في حين، أشار التقرير إلى أن 18٪ لا يقومون بتحديث هواتفهم المحمولة، وأن ثلاثة من كل أربعة مستخدمين للإنترنت لديهم كلمة مرور واحدة عبر تطبيقات وأجهزة مختلفة. أظهر 12 نوعًا من 22 نوعًا من تهديدات الأجهزة المحمولة زيادة في عدد حزم التثبيت المكتشفة في عام 2020 مقارنة بعام 2019. وقد ظهر النمو الأكثر أهمية بواسطة برامج الإعلانات المتسللة، حيث ارتفعت من 21.81٪ إلى 57.26٪ من جميع تهديدات الأجهزة المحمولة. بشكل عام، شهدت Kaspersky انخفاضًا في عدد الهجمات خلال النصف الأول من العام، "والذي

[144]-Yahia Hatim, Malicious Emails Represent Most Frequent Digital Threat in Morocco, Op.cit.
[145]-Ibid.

يمكن أن يُعزى إلى الارتباك الذي حدث في الأشهر الأولى للوباء"، نظرًا لأن "المهاجمين كان لديهم أشياء أخرى تقلقهم". ومع ذلك ، فقد خلصت الدراسة إلى أن النصف الثاني من العام شهد ارتفاعًا حادًا في تهديدات الأمن السيبراني، لا سيما "زيادة الهجمات التي تشمل المصرفيين عبر الهاتف المحمول"[146].

رغم كل تلك الهجمات، حاول المغرب صد مجموعة من الهجومات السيبرانية. على سبيل المثال، وحسب المعطيات التي صرحت بها المديرية العامة لأمن نظم المعلومات (DGSSI)، على لسان "عبد اللطيف لوديي" ، الوزير المنتدب للدفاع المغربي، فالمديرية العامة لأمن نظم المعلومات المغربية اكتشفت وأحبطت 577 تهديدا للأمن السيبراني في عام2021[147].

وذكر لوديي أن الهجمات استهدفت وزارات ومؤسسات عامة، وأن المديرية العامة للخدمات الأمنية والاجتماعية نفذت إجراءات وقائية لحماية أنظمتها في أعقاب إحباط كل هجوم. وكشف "لودي" عن الأرقام ردًا على سؤال مكتوب في مجلس النواب، مضيفًا أن المديرية العامة للأمن الداخلي تقوم أيضًا بإجراء عمليات تدقيق وتحليل لأمن أنظمة تكنولوجيا المعلومات في الهيئات الحكومية[148].

من أجل الحفاظ على تحديث الأنظمة الأمنية ومنع الهجمات الجديدة، أصدرت المديرية العامة للأمن العام 621 نشرة أمنية في عام 2021، من بينها 188 نشرة تنبّه إلى قضايا أمنية ذات طبيعة حرجة. وقال الوزير المنتدب إن المديرية نجحت أيضًا في اختراع جهاز تشفير لاعتراض الهجمات والبرامج المشفرة عبر اتصالات الفاكس والهاتف. كما تدير الوكالة مركز مراقبة للكشف عن الهجمات التي تشكل خطرًا خاصًا على مؤسسات وأنظمة الدولة. علاوة على ذلك، تعمل DGSSI على تنفيذ نظام إلكتروني آمن لإرسال وتبادل الوثائق بين مختلف الوكالات الحكومية. وقال "لوديي" إن النظام سيتم تنصيبه في جميع الدوائر الوزارية والتشريعية[149].

---

[146]-Toms Dumpis, Cybersecurity During the Pandemic, Op.cit.
[147]-Oussama Aamari, Morocco’s DGSSI Detected, Neutralized Over 500 Cyber Attacks in 2021, **Morocco world news**, 09.05.2021, link: http://bitly.ws/zqn8, seen on: 26.01.2023.
[148]-Ibid.
[149]-Ibid.

نظرًا لأن المغرب أصبح أكثر اعتمادًا على البنية التحتية الرقمية في جميع الجوانب، أصبح الأمن السيبراني أولوية متزايدة خاصةً مع زيادة تعقيد الفيروسات والهجمات السيبرانية. على مدى العامين الماضيين، اتخذ المغرب خطوات لتحسين مكانته في مجال الأمن السيبراني. في عام 2021، وافق الملك محمد السادس على مشروع قانون من شأنه إنشاء إطار قانوني لتحسين نظم المعلومات في جميع أنحاء البلاد، ووضع معايير للأمن السيبراني في المؤسسات العامة. شهد هذا المجال أيضًا استخدام الخبرات الأجنبية، مثل مركز الأمن السيبراني لإفريقيا الذي تم إطلاقه مؤخرًا في مراكش، والذي جاء نتيجة للتعاون بين السياسيين والأكاديميين المغاربة والبريطانيين[150].

## الفقرة الثانية: دراسة مدى حدتها

ظهرت الجرائم السيبرانية كنتاج طبيعي لثورة الاتصالات والتكنولوجيا وسجلت انتشارها الواسع في معظم بلدان العالم [151]. والمغرب هو الآخر لم ينج من تلك الجرائم أو إن صح التعبير تلك الهجمات السيبرانية، ولدراسة مدى حدتها (أي حدة الهجمات السيبرانية)، اعتمدت الدراسة على بعض النماذج التي قامت بدراسة ميدانية في بعض المجالات، وخصوصا الاقتصادية منها. قامت شركة إعادة التأمين المركزية Société Centrale de Réassurance (SCR) في عام 2019، بدراسة موقع المخاطر السيبرانية وتقييم درجة إدراك الشركات المغربية الصغيرة والمتوسطة في هذا المجال. رتبت الدراسة تلك المخاطر السيبرانية على أنها تشكل الخطر الثالث المتصور بعد خطري تغيرات السوق والحرائق[152]. وأبانت الدراسة أن الشركات المغربية تستخدم برامج مكافحة فيروسات / جدار حماية، ويتم فيها استخدام تقنيات VPN [153] والتشفير بشكل أكبر، وتعلن أكثر من نصف الشركات، لا

---

[150]-Oussama Aamari, Morocco's DGSSI Detected, Neutralized Over 500 Cyber Attacks in 2021, Op.cit.

[151]-محمد مسعد حيمد و مصطفى جاد الحق مصفى، رؤية استراتيجية لمكافحة الجرائم السيبرانية: اليمن دراسة حالة، **المجلة العربية الدولية للمعلوماتية**، 2019، رابط المقال: http://search.mandumah.com/Record/1060613، تاريخ الدخول: 25.04.2023، ص.4.

[152]-Brian Brequeville, Les cyberattaques, troisième risque perçu par les PME marocaines (enquête SCR), **MEDIA 24 le boursier**, 11.02.2021, lien de l'article : http://bitly.ws/zrJn, date visite : 27.01.2023, p.10.

[153]- **VPN** شبكة افتراضية خاصة (VPN) آمنة تسمح بنقل البيانات والاتصالات من جهاز الشخص وإليه بشكل آمن عبر نفق مشفر إلى وجهتها. توفر الشبكة الظاهرية الخاصة (VPN) الخصوصية عبر الإنترنت وتُستخدم لإخفاء عنوان بروتوكول الإنترنت (IP) للمستخدم وتشفير البيانات أثناء النقل. يوفر استخدام VPN حماية لأنشطة الإنترنت الخاصة بأي

سيما أكبرها، أنها تجري تدقيقًا داخليًا وخارجيا بانتظام للأمن السيبراني، ولديها خطة موثقة لإدارة الحوادث.

قالت أقلية فقط (13٪) إنهم على دراية بمفهوم التأمين الإلكتروني وفوائده للشركة. ومع ذلك، خلال ورشة العمل حول "مخاطر الإنترنت - حالة المكان وآفاق المستقبل"، اتفق جميع المشاركين على المخاطر التي يمكن أن تسببها الهجمات السيبرانية، لا سيما من حيث الأضرار المالية، وخطر برامج الفدية "Ransomware" والهندسة الاجتماعية" Social engineering"[154]، التي تعد أكبر تهديدين تواجههما الشركات اليوم، وهي برامج ضارة "Malware"[155].

هناك دراسة أخرى ل "بول بيشوف" "PAUL BISCHOFF "[156]، حول " ما هي الدول التي لديها أسوأ (وأفضل) أمن سيبراني؟"[157]

---

فرد منخرط، ويؤمن اتصالات شبكة Wi-Fi العامة، ويتجاوز المواقع المحجوبة. هناك العديد من مزودي خدمات VPN المختلفين الذين يقدمون مستويات مختلفة من الأمان والسرعة والموثوقية والقدرات. يعتمد تسعير خدمات VPN على الميزات المحددة. لا تسجل شبكات VPN الأفضل أنشطة الأفراد عبر الإنترنت أو عناوين IP أو الطوابع الزمنية للاتصال. (Becky McCarty, What are the Benefits of Using VPN Encryption, **Inford collp**, 17.05.2023, link: http://bitly.ws/GJd2, seen on: 02.06.2023).

[154]-**الهندسة الاجتماعية"Social engineering"**: نوع من أنواع الهجوم على السرية، وتنطوي على عملية التلاعب النفسي في أداء الأعمال، أو دفع الضحية للتخلي عن معلومات مهمة. ومن أقرب التعريفات أن نقول إنها استخدام المهاجم حيلا نفسية كي يخدع بها مستخدمي الحاسوب، ليمكنوه من الوصول إلى أجهزة الحاسوب، أو المعلومات المخزنة فيها.
فالهندسة الاجتماعية يجب أن تكون على رأس قائمة وسائل الهجمات السيبرانية، والسبب في ذلك يرجع إلى الآتي:
-الهندسة الاجتماعية من أنجح الوسائل التي يستخدمها المهاجم لسهولتها مقارنة بالوسائل التقنية الأخرى؛
-المتخصصون في مجال أمن المعلومات، وكذلك مستخدمي الحاسوب لا يعيرون خطر الهندسة الاجتماعية اهتماما كبيرا.
أما طريقة شنها، فيرى الباحثون أنها تشن على عدة أصعدة ومنها؛ **الصعيد الحسي** بالتركيز على موضع الهجوم والبيئة المحيطة به، ويدخل ضمن هذا مكان العمل، الهاتف، النفايات، برامج أو تطبيقات في الإنترنت تتطلب كلمة مرور. هناك صعيد آخر وهو **الصعيد النفسي**؛ في هذا المستوى يقوم المهاجم بخلق الأجواء النفسية المناسبة لإيهام الضحية بأنه شخص موثوق به، ولديه صلاحية الاطلاع على المعلومات الحساسة للشخص المستهدف، أو المنشأة المستهدفة.
(دحان حزام القريطي، الأمن السيبراني وحماية أمن المعلومات، مرجع سابق، ص ص، 47-50).

[155]-**برامج ضارة "Malware"**: أي برنامج يكون كل مهامه أو أحدها عمل خبيث من تجسس أو تخريب، أو استنزاف للموارد. تتضمن الأنواع الشائعة من البرامج الضارة برامج التجسس(spyware)،و (keyloggers)، والفيروسات وغيرها. (دحان حزام القريطي، الأمن السيبراني وحماية أمن المعلومات، مرجع سابق، ص. 55.).

[156]-يعد بول محررًا في شركة Comparitech ومعلقًا منتظمًا على موضوعات الأمن الإلكتروني والخصوصي في وسائل الإعلام الوطنية والدولية بما في ذلك New York Times و BBC و Forbes و The Guardian وغيرها كثير. يتمتع Paul بمعرفة عميقة بشبكات VPN، حيث كان من أوائل المتبنين أثناء بحثه عن الوصول إلى الإنترنت المفتوح خلال هذا الوقت في الصين. عمل سابقًا في بكين كمحرر في Tech in Asia، وكان يكتب التقارير عن التكنولوجيا على مدار العقد الماضي. كما تطوع كمدرس لكبار السن الذين يتعلمون أساسيات المعرفة التقنية والوعي السيبراني. يمكنك العثور عليه على Twitter علىpabischoff

[157]-Paul Bischoff, Which countries have the worst (and best) cybersecurity?, **comparitech**, 26.09.2022, link: http://bitly.ws/zsEE, seen on: 27.01.2023

في كل عام ، تبحث تلك الدراسة في أكثر من 60 دولة لمعرفة الأماكن الأكثر "أمانًا على الإنترنت" في العالم. في عام2022، قامت بتحليل 75 دولة، وحكمت على كل منها بقائمة موسعة من 15 معيار (التقارير السابقة كانت تحتوي على 7معايير)[158].

احتلت الجزائر بناء على تلك المعايير المدرجة سالفا، المرتبة 74 فيما يخص الهواتف المحمولة المصابة بالبرمجيات الخبيثة (إيران - 30.29٪، الجزائر - 21.97٪، بنغلاديش - 17.18٪)، في حين احتل المغرب المرتبة 73 من حيث مهاجمة مستخدمي الهاتف المحمول عبر مصادر الويب (الإكوادور - 6.33٪، عمان - 4.98٪، المغرب - 4.51٪). وفي الترتيب النهائي، احتلت الجزائر المرتبة 71 من بين 75 دولة بنسبة ( 32,28%)، في حين جاء المغرب في المركز 65 بنسبة (25,95%)، على اعتبار أن النسبة المئوية كلما زادت، كلما تأخر أمن الدولة السيبراني[159].

**ولتأكيد تأخر الجزائر في ميدان الأمن السيبراني، يمكن الرجوع إلى دراسة أخرى أعدتها نفس المجلة، سنة 2019:** في منشور مدون على موقعها على الويب، أوضحت شركة "Comparitech" أنه بالنسبة لكل معيار، تم منح البلدان نقطة بناءً على تصنيفها بين البلدان ذات التصنيف الأعلى والأدنى. وحصلت البلدان ذات الدرجات الأقل أمانًا على الإنترنت على 100 نقطة، في حين تم تخصيص نقاط صفرية للبلدان التي حصلت على أعلى الدرجات أمانًا عبر الإنترنت. حصلت جميع البلدان الواقعة بين هاتين الدرجتين على درجة على أساس النسبة المئوية، اعتمادًا على المكان الذي رتبت فيه. سارعت شركة Comparitech إلى الإشارة إلى أنها وجدت تباينات كبيرة في عدد من الفئات وأنه لم يكن هناك بلد جاء "على رأس الفئة" في جميع المجالات. وقالت الشركة مع ذلك، "كانت هناك بعض البلدان التي تفتقر بشكل كبير في مجموعة متنوعة من المجالات والبعض الآخر الذي تفوق على غالبية البلدان". وأضافت المقارنة: "مع وضع ذلك في الاعتبار، أنشأنا تصنيفات لهذه البلدان الستين، بدءًا من الأقل أمانًا عبر الإنترنت إلى الأكثر أمانًا عبر الإنترنت"[160]. **اعتُبرت الجزائر الدولة الأقل أمانًا إلكترونيًا** بشكل عام، كونها الدولة الأعلى تصنيفًا بسبب

[158]- Paul Bischoff, Which countries have the worst (and best) cybersecurity?,Op.cit.
[159]-Ibid.
[160]-Michael Hill, Algeria Ranked ‘Least Cyber-Secure’ Country in the World, Japan ‘Most Cyber-Secure’, **info security**, 07.02.2019, link: http://bitly.ws/zsGN, seen on: 27.01.2023.

الافتقار إلى التشريعات ومعدلات البرامج الضارة للكمبيوتر، وحصلت أيضًا على درجة عالية في فئات البرامج الضارة للأجهزة المحمولة والاستعداد للهجمات السيبرانية. تليها إندونيسيا وفيتنام في المرتبة الثانية والثالثة من الدول الأقل أمانًا عبر الإنترنت، بينما احتلت تنزانيا وأوزبكستان المرتبة الرابعة والخامسة الأقل أمانًا عبر الإنترنت، على التوالي.

وعلى العكس من ذلك ، كانت البلدان التي كان أداؤها جيدًا بشكل عام في بحث شركة Comparitech هي اليابان (التي احتلت المرتبة الأكثر أمانًا عبر الإنترنت في العالم، وسجلت "درجة منخفضة بشكل لا يصدق" عبر غالبية الفئات) ، وفرنسا وكندا والدنمارك والولايات المتحدة. احتلت المملكة المتحدة المرتبة الثامنة بين أكثر الدول أمانًا عبر الإنترنت[161].

وبالرجوع إلى التجربة السيبرانية الجزائرية، وبالرغم من أن جل الدراسات العالمية أكدت عن تقهقرها واحتلالها للمراتب المتدنية في مجال الدفاع السيبراني. فهي تربط دائما الهجمات السيبرانية عليها بالمغرب، لا تعتمد في غالب الأحيان على دراسات علمية، وتقفي أثر الهجوم السيبراني بطريقة محكمة. وخير مثال على ذلك، أن الجزائر أعربت، يوم 29.07.2021، عن قلقها بعد تقارير إعلامية عن استخدام برنامج التجسس الإسرائيلي Pegasus للتنصت على المسؤولين والمواطنين الجزائريين. وأول بلد وجهت إليه أصبع اتهامها كان هو المغرب. فمع تصاعد التوتر بالفعل بين الجزائر والمغرب، يمكن لفضيحة برامج التجسس Pegasus أن تزيد من توتر العلاقات بين الجارتين في شمال إفريقيا. أدت فضيحة بيغاسوس إلى مزيد من التوتر في العلاقات بين الجارتين في شمال إفريقيا. نفت الحكومة المغربية الاتهام الموجه إليها. بل ردت في بيان لها أنها "ترفض بشكل قاطع وتدين هذه المزاعم الكاذبة التي لا أساس لها" وستقاضي كل من منظمة العفو الدولية والقصص المحرمة بتهمة التشهير[162].

[161]-Michael Hill, Algeria Ranked ‘Least Cyber-Secure’ Country in the World, Japan ‘Most Cyber-Secure’, Op.cit.

[162]-Abdelkader Cheref, Is Morocco's cyber espionage the last straw for Algeria?, 29.07.2021, link: http://bitly.ws/Dzec, seen on: 27.04.2021.

## الفرع الثاني: التهديدات الخارجية

في ظل التطور الحاصل في المجال السيبراني، وتزامنا مع بعض القوى العظمى الساعية لفرض هيمنتها الرقمية على نطاق واسع؛ الولايات المتحدة الأمريكية والصين نموذجا، تعاني دول شمال إفريقيا عامة، والمغرب والجزائر خاصة من ثغرات في مجالها الرقمي، مما يسمح بين الفينة والأخرى لبعض المتسللين الرقميين ولبعض الديدان الفيروسية المخربة، من التسلل لأنظمتهم الخوارزمية، محدثة إتلافا تتراوح درجة خطورته بين الضعيفة والمتوسطة، لكنها لم ترق إلى القوية، أو الخطيرة جدا والتي يتحول فيها الصراع إلى مواجهة ميدانية بين القوى الصلبة.

للتغلغل أكثر في تلك التهديدات الخارجية ولسبر أغوارها، تناولت الدراسة أنواعها (أي أنواع الجرائم السيبرانية)(الفقرة الأولى)، ودراسة مدى تأثيرها على البلدين(الفقرة الثانية).

### الفقرة الأولى: أنواع التهديدات الخارجية

بالنسبة للتهديدات السيبرانية الخارجية ضد البلدين، يكتفي البلدان بتوجيه التهم بينهما؛ يحاول كل واحد منهما اتهام الأخرى بالهجوم عليه، وبتعريض بعض مواقعه الرسمية وغير الرسمية للاختراق من طرف عناصر هاكرز ينتمون إليه. وهذا يندرج ضمن الصراع غير المباشر، المستمر لعقود بين البلدين. وخصوصا من جانب الجزائر. والأدلة على ذلك كثيرة.

ما يؤكد ذلك، في 11 مارس من سنة 2022، أعلنت الإذاعة الجزائرية الرسمية، عن اختراق حساب وزارة العدل الرسمي على تويتر، متهمة من أسمتهم "قراصنة مغاربة" بنشر تغريدات لا علاقة لها بالمواقف الدولية للجزائر. وقد أوضح ذلك أنه بالتوازي مع التوترات السياسية بين الجزائر والمغرب، هناك مواجهة أخرى تدور رحاها في الفضاء السيبراني، أطلق عليها بعض الخبراء "حرب الظل". نشر قراصنة الحساب الرسمي لوزارة العدل على "تويتر" عدة "تغريدات" تدعم العملية الروسية في أوكرانيا، متهمين الرئيس الأوكراني "فولوديمير زيلينسكي" بـ "النازية وقتل مواطنيه". في 12 مارس، أطلق مجلس

القضاء الجزائري تحقيقا قضائيا في القرصنة، قائلا في بيانه "سيتم إبلاغ الجمهور بنتائج التحقيقات في الوقت المناسب"[163].

جدير بالذكر أن هذه الهجمات السيبرانية ليست الأولى من نوعها. في نوفمبر، تم اختراق موقع الاتحاد العام للمقاولات المغربية (CGEM)، بينما هاجمت مجموعة قرصنة، قيل إنها مغربية، موقع وزارة المالية الجزائرية، في 17 ديسمبر 2020. قام القراصنة بتعطيل الموقع الإلكتروني للوكالة الجزائرية لتقييم الموارد الهيدروكربونية. وقالت وزارة الطاقة في بيان في اليوم التالي إن موقع الوكالة تعرض لهجوم من قراصنة وطالبت المستخدمين بعدم الدخول إلى الموقع حتى يتم وقف الهجوم. وبحسب مراقبين، تصاعدت موجة الهجمات واستهدفت بشكل كبير المواقع الحكومية وبعض المؤسسات الإعلامية[164].

نفى المغرب الاتهامات الجزائرية بشأن الهجمات الأخيرة، وجاء هذا النفي على لسان وزير الخارجية المغربي ناصر بوريطة، بل طالب الجزائر بتقديم أدلة ملموسة إن توفرت عليها. لكن رغم نفي المغرب للاتهامات الجزائرية، زار قراصنة مغاربة مجموعة من المواقع الإلكترونية الجزائرية، خصوصا منها الرسمية، حيث اخترقوا عشرات المواقع التابعة لقطاعات حكومية جزائرية. ويُزعم أن الهجوم الإلكتروني جاء رداً على هجوم شنته قناة "الشروق" على شخص الملك محمد السادس". ونقلا عن المتسللين فقد أكدوا اختراقهم لأكثر من 280 موقعا جزائريا بينها مواقع حكومية. في 8 فبراير 2021، اتهم وزير الاتصالات الجزائري والمتحدث الرسمي باسم الحكومة، عمار بلحيمر، المغرب بتجنيد مئات العملاء في العالم الافتراضي لمهاجمة الجزائر[165].

بدورهم هاجم الجزائريون بعض المواقع المغربية؛ في غشت سنة 2022، تعرض الموقع الرسمي لجامعة ظهر المهراز العلمية بفاس لهجوم سيبراني من قبل متسلل جزائري. المخترق الذي يبدو أنه من الجزائر ترك توقيعه مع العلم الجزائري على الموقع مع تسمية توضيحية تقول "لا سلام بين الأنظمة". ترك المهاجمون الإلكترونيون توقيعهم، مشيرين إلى

[163]-Hamdy Bashir, A Cyber Shadow- War between Algeria and Morocco, Op.cit.
[164]-Ibid.
[165]-Ibid.

أن الجاني من الجزائر. ادعى الجاني على تويتر أنه جمع ثلاثة ملايين سطر من البيانات، بما في ذلك رسائل البريد الإلكتروني وكلمات المرور[166].

ليست هذه هي المرة الأولى التي يتم فيها استهداف موقع إلكتروني مغربي بهجوم سيبراني من قراصنة من أصل جزائري. زعم نفس القراصنة أنهم هاجموا بعض المواقع الرسمية المغربية. في نوفمبر 2021، تعرض الموقع الرسمي للاتحاد المغربي العام للمؤسسات المغربية (CGEM) أيضًا لهجوم سيبراني[167].

قد تكون الدوافع وراء المتسلل المعني غير سياسية حصريًا، بعد أن هاجم في وقت سابق أهدافًا في إيطاليا وبوليفيا، إلا أنها تأتي وسط توتر بين المغرب والجزائر. وكانت الجزائر قد قررت في 21غشت 2021 قطع علاقاتها مع المغرب متهمة الرباط بتقويض أمنها[168].

ونفى المغرب الاتهامات الموجهة إليه وقال إن قيادته تأسف لقرار الجزائر. لكن الدولة الواقعة في شمال إفريقيا شددت على أن البلاد ستظل دائمًا شريكًا مخلصًا وذا مصداقية للجزائريين. وجدد ملك المغرب محمد السادس نداء السلام نفسه خلال خطاب ألقاه بمناسبة عيد العرش في 30 يوليو2022[169].

فمع العلم أن الجزائر تعتبر من أضعف الدول في مجال التكنولوجيات والأجهزة الاتصالية، وبالتالي بنية دفاعها السيبراني ضعيفة، مما سهل كثرة الثغرات السيبرانية فيها، التي عمل نظام متخصص كنظام بيغاسوس للتجسس على استغلالها. لكن النظام الرسمي الجزائري بدل البحث عن المصدر الرسمي لتلك الهجمات، سارع باتهام المغرب. وأكد

---

[166]-Hamdy Bashir, A Cyber Shadow- War between Algeria and Morocco, Op.cit.

[167]-Ibid.

[168]-Ibid.

[169]-الخطاب الملكي بتاريخ 30 يوليوز2022، مناسبة عيد العرش، رابط الخطاب: http://bitly.ws/KFNo، تاريخ الدخول: 07.07.2023.

(مما جاء في الخطاب، قول الملك محمد السادس إن المغرب مستعد للعمل مع الرئاسة الجزائرية لإعادة العلاقات. ودعوته للمغاربة إلى الحفاظ على روح "الأخوة والتضامن وحسن الجوار" مع الشعب الجزائري. ووجه الملك دعوات حوار مماثلة في العديد من خطاباته، مع استجابة قليلة من صناع القرار في الجزائر العاصمة).

باحثوه الأكاديميون أن زيادة حدة توتر العلاقات السياسية بين البلدين مرده استخدام المغرب نظام تجسس بيغاسوس، والذي كان بمثابة القطرة التي أفاضت الكأس بين البلدين[170].

مجموعة من العوامل تفسر تصاعد الاتهامات بين الجزائر والمغرب، نوجزها فيما يلي[171]:

**-توترات واسعة ومتصاعدة بين البلدين**. ترتبط هذه التوترات بالنزاع المستمر منذ عقود بشأن السيادة المغربية على أراضي **"الصحراء المغربية"**. في خطوة تعتبرها الجزائر تصعيدية من جانب المغرب، قدم المندوب الدائم للمملكة المغربية لدى الأمم المتحدة، عمر هلال، ورقة لأعضاء مجموعة عدم الانحياز في يوليوز 2021، دعاهم فيها إلى دعم ما قاله "تقرير المصير لشعب القبايل"[172]، واصفا منطقة القبايل بأنها "تحت الحكم الاستعماري الجزائري". وجاء التحرك المغربي بعد أن أعلنت الجزائر أنها تجري عملية ترسيم الحدود مع جبهة البوليساريو. تصاعدت التوترات بعد إعلان الجزائر قطع العلاقات بين البلدين وحظر الطيران المدني والعسكري المغربي من الأجواء الجزائرية، وكذلك قرار الجزائر الأحادي بوقف اتفاق خط أنابيب الغاز عبر المغرب.

**-الهجمات السيبرانية كرادع غير تقليدي**. أصبحت الهجمات السيبرانية أداة في النزاعات الإقليمية والدولية. يمكن النظر إلى سلسلة الهجمات السيبرانية الأخيرة بين المغرب والجزائر على أنها جزء من مرحلة جديدة من المواجهة غير التقليدية. تتيح هذه الهجمات للخصوم مجالًا أكبر للتغلغل على الجبهة الداخلية، حيث يمكن للهجمات السيبرانية أن تلحق

---

[170]-برج أسمهان وآخرون، الهجمات السيبرانية و أثرها على العلاقات السياسية الدولية- العلاقات الجزائرية المغربية نموذجا، رسالة لنيل شهادة الماستر في علوم الإعلام والاتصال وعلم المكتبات، جامعة 8 ماي 1945 قالمة، كلية العلوم الإنسانية والاجتماعية، الجزائر،2021 -2022، ص ص.53-61.

[171]-Hamdy Bashir, A Cyber Shadow- War between Algeria and Morocco, Op.cit.

[172]-**القبايل**: يأتي مصطلح القبايل من منطقة القبائل، وهي منطقة جبلية تقع شرق الجزائر العاصمة. لذا فإن كونك جزائرياً لا يعني أن تكون عربياً، لأن القبايل هم أمازيغ. يشير هذا المصطلح الأخير إلى شعب أصلي قديم في شمال إفريقيا يشهد على وجوده على الأقل منذ هيرودوت. من التفرد أن تكون اللغة الأمازيغية تُنقل شفهياً، والتي بقيت على قيد الحياة لأكثر من ألفي عام. ينتشر البربر على أراضي العديد من البلدان: المغرب، الجزائر، تونس، ليبيا، مصر، مالي، بوركينا فاسو، النيجر. في الجزائر، التي تضم من 25 إلى 30٪ من المتحدثين الأمازيغية، تعتمد سياسة التعريب في المناطق النائية على الاستقلال، ولا يزال هناك العديد من المتحدثين الأمازيغية المهمين بين مجموعات مثل القبائل، من بينهم، ولكن أيضًا بين الطوارق، الشاويون من الأوراس، المزابيون من ميزاب، تشينويون من جبل تشينوا، إلخ. وبالتالي، فإن البربر ليسوا كلهم من القبائل. كانت القبايل دائمًا في طليعة المطالب الأمازيغية، ولا سيما الخلايا التي تطالب بالاعتراف بحقيقة أن الهوية الجزائرية يمكن اختزالها إلى حدودها.

(Arezki Metref, Algériens… mais pas arabes, **le Monde Diplomatique**, Mars 2014, lien de l'article: http://bitly.ws/HAvi, date visite : 07.06.2023)

الضرر بالبنية التحتية الحيوية، وتشل وتعطل القطاعات الاقتصادية والعسكرية والأمنية المهمة.

**-الفضاء السيبراني كميدان بديل للمواجهة**. على الرغم من تصاعد التحركات العسكرية على الحدود بين البلدين، يعتقد بعض المراقبين أنه من غير المرجح أن تشارك الجزائر والمغرب في صراع كامل، وأن الزيادة في الهجمات السيبرانية تشير إلى ميل لتجنب المواجهة المسلحة و الاعتماد على الوسائل الحديثة والتكنولوجيا الرقمية.

**-حشد الدعم المحلي**. اتهامات الجزائر المتكررة للمغرب بشن حرب إلكترونية دفعت بعض المراقبين إلى القول بأن الحكومة الجزائرية تسعى لتحقيق أهداف سياسية داخلية. وتسعى لإبلاغ الرأي العام الجزائري بأن البلاد تواجه "عدوًا خارجيًا"، وهو المغرب، في محاولة لتقويض الدعوات إلى الاحتجاجات الشعبية.

**-مخاوف بشأن التعاون الأمني السيبراني الإسرائيلي المغربي**. وقعت إسرائيل والمغرب بالفعل اتفاقيات حول التعاون العسكري والتقني في مجال الأمن السيبراني، والتي تعتبرها الجزائر بمثابة قلب لتوازنها العسكري التقني مع المغرب. في فبراير 2021، حذرت الحكومة الجزائرية من تهديدات للسيادة الرقمية الجزائرية واتهمت المغرب بشراء برامج تجسس من شركة المراقبة الإسرائيلية NSO، متهمة باختراق الهواتف المحمولة لأكثر من 1400 مستخدم في 20 دولة. اتهمت الجزائر المغرب بامتلاك برنامج تجسس إسرائيلي الصنع من طراز Pegasus[173] ، الأمر الذي زاد من توتر العلاقات بين الجارتين.

---

[173]-كشفت دراسة استقصائية عالمية أجراها كونسورتيوم من 17 وسيلة إعلامية دولية أن برنامج الشركة الإسرائيلية NSO Groupقد تم استخدامه للتجسس على الصحفيين والمحامين والشخصيات السياسية، بما في ذلك الفرنسيون. وتنفي الشركة هذه الاتهامات. إنها بلا شك واحدة من أكبر فضائح التجسس، وهي بالتأكيد الأهم منذ قضية سنودن، والتي تهم ما لا يقل عن إحدى عشرة دولة في جميع أنحاء العالم. تسلط فضيحة المراقبة العالمية الجديدة هذه، المعتمدة على"مشروع بيغاسوس"، الضوء على ممارسات عشرات البلدان التي تشترك في استخدامها في السنوات الأخيرة، دون أدنى رقابة، برنامج تجسس مهيمن يتم تسويقه من قبل شركة إسرائيلية خاصة، NSO.

**خصائص برنامج التجسس Pegasus من شركة NSO Group الإسرائيلية الهائلة**: لا حاجة للوصول إلى ارتباط تالف، ولا يلزم التلاعب بالمستخدم المستهدف. إذا تم إدخاله في هاتف ذكي، فإنه يجعل من الممكن استرداد الرسائل والصور وجهات الاتصال وحتى الاستماع إلى مكالمات مالكه.

إن "إن إس أو" NSO، التي تتهم بانتظام باللعب في أيدي الأنظمة الاستبدادية، كانت تضمن دائمًا أن برامجها لم يستخدم إلا للحصول على معلومات ضد الشبكات الإجرامية أو الإرهابية. لكن الاستطلاع الذي نشره هذا الكونسورتيوم المكون من سبعة عشر وسيلة إعلام دولية، في عام 2021، بما في ذلك صحيفة لوموند الفرنسية، وصحيفة الغارديان البريطانية، وواشنطن بوست الأمريكية ، يقوض مصداقيتها.

(Joanne Massard, Pegasus, un logiciel israélien au coeur d'un scandale mondial d'espionnage, **Euronews**, 20.07.2021, lien de l'article : http://bitly.ws/HB35, date visite : 07.06.2023.)

**السلاح المفضل**

يمكن القول إن تصاعد الهجمات السيبرانية بين المغرب والجزائر هو مظهر آخر من مظاهر التنافس التاريخي بينهما، وخاصة على **"الصحراء المغربية"**. في ضوء التوترات المتزايدة، من المرجح أن تتصاعد هذه الهجمات السيبرانية، وتستهدف المواقع الحكومية والبنية التحتية والمرافق العامة والمواقع العسكرية والاقتصادية، ولا سيما البنية التحتية للنفط والغاز. ويدعم هذا السيناريو تفادي المواجهة العسكرية الصريحة بين البلدين حتى الآن، على الرغم من التنافس على الحصول على أحدث الأسلحة والمعدات العسكرية. يبدو أن كلا الطرفين حريص على تجنب المواجهة الشاملة والمفتوحة. وبالتالي، قد تبدو هذه الحرب السيبرانية خيارًا مناسبًا لتحقيق الأهداف الاستراتيجية للبلدين، بأقل تكلفة ممكنة.

## الفقرة الثانية: دراسة مدى تأثيرها على البلدين

لدراسة مدى تأثير الهجمات السيبرانية على المنطقة موضوع الدراسة، ارتأينا دراسته من زاوية تواجد القوى العظمى في تلك المنطقة –منطقة شمال أفريقيا وبالضبط المغرب والجزائر-، ومدى ارتباط تلك البلدان بالبحث عن الهيمنة السيبرانية في هذين البلدين. وفي هذا الصدد أدرجنا تواجد القوة الصينية وسياستها التوسعية في المنطقة. وما تشكله من مخاطر سيبرانية مستقبلية حقيقية على البلدين معا.

على المدى القصير، قد تخدم طريق الحرير الرقمي"Digital Silk Road"[174] المغرب في تعزيز بنيته التحتية الرقمية، لكن التداعيات طويلة المدى قد تخلق مخاطر

[174]- **(Digital Silk Road (DSR))**: منذ إعلانها في عام 2015 ، تهدف طريق الحرير الرقمي إلى "بناء مجتمع ذي مستقبل مشترك في الفضاء السيبراني "، أصبح جزءًا متزايد الأهمية من أجندة مبادرة الحزام والطريق. وهي تتألف من مجموعة واسعة من الإعلانات الحكومية والتمويل الحكومي و وطموحات الأعمال الخاصة. يشمل DSR الرقمي الاقتصاد، الذكاء الاصطناعي، تكنولوجيا النانو، الحوسبة الكمومية، البيانات الضخمة، الحوسبة السحابية والمدن الذكية. في حين أن البنية التحتية مثل السكك الحديدية والموانئ الجديدة تغير بشكل واضح الجغرافيا والاقتصاد في بنك التسويات الدولية "BRI "، فإن تأثير "الإنترنت الصيني" الذي يمتد من البنية التحتية إلى الأجهزة إلى البرامج والخدمات أقل وضوحًا ويصعب تحليلها. هل تنشئ الصين شبكة إنترنت منفصلة تتمحور حول الصين بين جيرانها وعملاءBRI ؟ هل سيتم تقسيم العالم إلى إنترنت مختلف؟ هل DSR و BRI بشكل عام، تمثل استراتيجية موحدة، أم أنها سلسلة من المشاريع المخصصة التي تندرج تحت نفس المظلة الأيديولوجية، ولكن بنطاق وممثلين وأهداف مختلفة جدًا؟ كلها تساؤلات في حاجة إلى إجابات.

(Nargis Kassenova & Brendan Duprey, Digital Silk Road in Central Asia: Present and Future, 01.06.2021, link: http://bitly.ws/GPmF, seen on: 03.06.2023), p.9.

جسيمة؛ من تجسس سيبراني، وجمع بيانات جماعية، ونفوذ سياسي لا ينبغي تجاهله[175]. في هذا الصدد، يجب أن لا ننسى ما وقع للعراق من وراء الشركات الغربية؛ فبعد احتلاله للكويت، سنة 1990، تبنت الولايات المتحدة الأمريكية عملية "عاصفة الصحراء" لتحرير الكويت، ومن تم الاستحواذ على خيرات المنطقة. لم تكن ستتم هذه العملية لولا اعتمادها على مجموعة من البيانات التي حصلت عليها من عند الشركات الغربية، التي اشتغلت في العراق سابقا[176].

وإذا ما عدنا إلى التجربة المغربية الصينية، نجده أنه يعتبر أول دولة في شمال إفريقيا تلتزم بخطة تنفيذ مبادرة الحزام والطريق الصينية. ونسجل تواجد شركة التكنولوجيا الصينية العملاقة، هواوي. وقد أنشأت الشركة مركزًا لوجستيًا في ميناء طنجة المتوسط، يوفر تكنولوجيا الاتصالات لنظام السكك الحديدية الوطني (ONCF)، كما تشارك بعمق في أنظمة الاتصالات السلكية واللاسلكية في جميع أنحاء البلاد[177].

يتم استخدام التكنولوجيا الصينية والبنية التحتية الرقمية في جميع أنحاء البلاد، عبر العديد من الصناعات. وبينما كتب الكثير عن فعالية مشاريع مبادرة الحزام والطريق المادية في شمال إفريقيا، تم تجاهل أمر مهم، وهو الهيمنة الصينية في القطاع الرقمي المغربي إلى حد كبير. فتداعيات تلك الهيمنة الطويلة المدى للاعتماد على التكنولوجيا الصينية تخلق مخاطر جسيمة للتجسس الإلكتروني، وجمع البيانات الجماعية، والنفوذ السياسي الذي لا ينبغي تجاهله. ظاهريًا، يبدو أنه لا يوجد سبب يدعو للقلق فيما يتعلق بهذه الاستثمارات التقدمية والبصيرة. لكن مخاطر طريق الحرير الرقمي قائمة؛ ستزود DSR الشركات الصينية بكميات هائلة من البيانات من خلال زيادة قدرات التجميع العالمية الخاصة بها[178].

يعتقد الكثيرون أن الصين تستخدم DSR للحصول على امتياز الوصول إلى معلومات الملايين من المستهلكين، مما يمنح بكين فرصًا كبيرة للمراقبة[179].

---

[175]-Bryce F. Neary, China’s Digital Silk Road in Morocco: The Implications of Digital Sector Dominance, 23.05.2022, link: http://bitly.ws/CNjt, seen on: 11.04.2023.

[176]- فرد كابلان، المنطقة المعتمة: التاريخ السري للحرب السيبرانية، مرجع سابق، ص.39.

[177]-Bryce F. Neary, Ibid.

[178]-Ibid.

[179]-Ibid.

قد يكون من المفيد دراسة كيفية استخدام الصين لتقنياتها داخل حدودها. فقد تم تكييف تصميم برنامج الكمبيوتر الخاص بها للمراقبة الداخلية لشعبها، بشكل لا مثيل له في العمق والمدى. في ثانية واحدة فقط، باستخدام الكاميرات الأمنية والذكاء الاصطناعي، يمكن لقواعد البيانات الحكومية تصفية الملايين من صور تسجيل المواطنين للتعرف على الأفراد. كما يخضع الإنترنت الصيني للرقابة الشديدة، وبالتالي، سيكون من غير البديهي افتراض عدم استخدام مثل هذه القدرات لمنفعة الصين عند تنفيذها في الخارج، لا سيما في حالة حدوث أزمة جيوسياسية تكون فيها مثل هذه الأنظمة والاستخبارات حاسمة. فكلما زادت مشاركة الصين مع شركائها، زاد الضغط الذي قد يواجهه الشركاء للانحياز إلى جانب في القضايا المتنازع عليها. على سبيل المثال، قد يكون النزاع الإقليمي بين المغرب والجزائر حول منطقة الصحراء "المغربية" مماثلاً للمشاعر الصينية فيما يتعلق "بهونج كونج" أو "تايوان". فإذا ما سجلنا أن علاقة المغرب مع الصين لا تزال في مراحلها الأولى، نجد أن الصين لديها علاقة قوية ومربحة مع الجزائر منذ عقود. وبالتالي، إذا حدث صراع، فمن المحتمل أن تنحاز الصين إلى جانب، وقد لا تقف إلى جانب المغرب. ستكون أي قدرات مراقبة أو تحكم في البنية التحتية الرقمية أو نفوذ اقتصادي تمتلكه الصين في دولة مضيفة أمرًا محوريًا في وقت الصراع[180].

**يجب أن نشير إلى أن ما يقع للمغرب في شراكته مع الصين، يشابه إلى حد كبير واقع العلاقة الصينية الجزائرية**. ففي إطار المشاركة في مبادرة حزام واحد طريق واحد "O.B.O.R"، وقعت الجزائر والصين، سنة 2021 في بكين، على خلفية المنتدى الثالث للتعاون الصيني الأفريقي، مذكرة تفاهم بشأن انضمام الجزائر إلى مبادرة "الحزام والطريق" الصينية. تمثل هذه المذكرة تعزيز التعاون الجزائري الصيني، وفقًا لروح خطة التنمية المستدامة للأمم المتحدة 2030 وأجندة الاتحاد الأفريقي 2063. وتشمل هذه الشراكة، في صفتها الظاهرية، الحوكمة الرشيدة والأمن والسلام وتكملة التنمية. وتحسين القدرات

[180]-Bryce F. Neary, China’s Digital Silk Road in Morocco: The Implications of Digital Sector Dominance, Op.cit.

الإنتاجية للبلدان الأفريقية من خلال الابتكارات التكنولوجية الصينية[181]. لكن المخاطر الخفية، التي أشارت إليها الدراسة آنفا تبقى قائمة في العلاقة الصينية الجزائرية.

هذه الأخيرة هي الأخرى تسعى من خلال تعاملها مع الشريك الصيني وانضمامها الى مبادرته "الحزام والطريق"، إلى ايجاد حلول لأزماتها الاقتصادية المتعددة، عبر دعم معدلات نموها وتطوير البنية التحتية لاقتصادها الوطني، إضافة الى جذب الاستثمارات الأجنبية المختلفة في إطار المبادرة. وهو ما يؤكده إقدامها على تجديد المخطط الخماسي للتعاون الجزائري-الصيني، للفترة الممتدة ما بين 2019و2023[182].

لكن وعلى الرغم من استراتيجية الخروج الصينية الجديدة عبر مشروع القرن "مبادرة الحزام والطريق "، والذي سعت من خلاله إلى إثبات إمكانية التوطين داخل الدول، دونما تدخل في شؤونها الداخلية بانتهاج أساليب التعاون والتبادل التجاري بين الشركات الحكومية والخاصة، في سبيل تحقيق رباعية من الشراكة الدولية الناعمة؛ والتي تتألف من المساعدات الاقتصادية، التجارة، الاستثمار والمساعدات التقنية في تنفيذ المشاريع التنموية وتطوير البنى التحتية للدول، فإن الطرح الواقعي الجديد يرى وعلى النقيض من ذلك، على غرار– بوزان-، - سيغال -و-مونرو- ، أن الصين غير راضية ببنية النظام الدولي القائم رغم استظهارها لسياسة ناعمة في سلوكياتها الخارجية، وأنها تسعى من خلال مبادراتها التوسعية إلى تحقيق الهيمنة العالمية، ما سيشكل تحديا من الصعب تجنبه، و يخلق لعبة صفرية بين القوى الكبرى قد تؤدي الى حدوث نزاعات وحروب من أجل فرض السيطرة ومن خلال هذا الطرح فإن مشروع مبادرة" الحزام والطريق"، أو" طريق الحرير الصيني الجديد "من المشاريع التنموية الكبرى التي تشهدها المنظومة الدولية، وسياسة استراتجية شاملة تستهدف ميدان الاقتصاد بالدرجة الأولى، تسعى من خلاله الصين الى إبراز قوتها الاقتصادية عالميا وتحقيق أهدافها المسطرة من وراء ذلك[183].

---

[181]-FILALI Ferial, The Future of Sino-Algerian Relationship on “O.B.O.R” (One. Belt. One. road), Democratic Arabic Center, 18.05.2021, link: http://bitly.ws/FC6x, seen on: 26.05.2023

[182]-حنينة رجوح، الشراكة الجزائرية الصينية على ضوء مبادرة الحزام والطريق: المكاسب والمخاطر، مجلة السياسة العالمية، الجزائر،العدد1، 2022، ص.223.

[183]-المرجع نفسه.

وفي إطار استراتيجية بسط قوتها على دول العالم، نسجل التواجد القوي في الجزائر لشركات التكنولوجيا الصينية الكبرى، المعنية بالاقتصادات الرقمية، مثل "Huawei "و "ZTE "و "China Telecom" و "Hikvision "و "Yitu ". هذه الشركات المدعومة جزئيًا من الدولة الصينية، والتي تعتبر رائدة عالميًا في توفير البنية التحتية لتكنولوجيا المعلومات والاتصالات والأجهزة الذكية، هي أيضًا في طليعة تطوير وتجهيز عملائها بأنظمة مراقبة متطورة. في عهد "شي" وتحت رعاية مبادرة الحزام والطريق، كانت تكنولوجيا المعلومات أداة استراتيجية لدعم الأنظمة الحاكمة وتوليد النفوذ في مواجهة الغرب. الجزائر هي واحدة من بين عشرات الدول الإفريقية التي استفادت من تكنولوجيا المراقبة الخاصة بشركة هواوي. في حين أنه من المهم الاعتراف بالدور الإيجابي للصين في تقاسم مكاسب الابتكار الرقمي، من المهم بنفس القدر عدم التقليل من مخاطرها المستقبلية على الأمن السيبراني الجزائري[184].

فالأمن السيبراني هو قضية مهمة للأفراد والمنظمات والحكومات في الجزائر وحول العالم. يمكن أن يكون للهجمات السيبرانية عواقب وخيمة، بما في ذلك الخسارة المالية، سرقة المعلومات الحساسة، الإضرار بالسمعة، تعطيل الخدمات الضرورية. ولكي تكون مساعدة في الحماية من هذه الأنواع من التهديدات، لابد للأفراد والمؤسسات من اتخاذ خطوات لتأمين أنظمتهم وبياناتهم، لكن الجزائر حاليا ليست من بين البلدان التي تعطي أولوية للأمن السيبراني بما فيه الكفاية[185].

في عام 2020، شهدت الجزائر زيادة كبيرة في عدد الجرائم المسجلة. قال سعيد أرزقي مدير الشرطة القضائية، إن هناك 258171 حالة من جميع أنواع الجرائم المبلغ عنها خلال العام، بما في ذلك 5163 حالة حوادث الجرائم السيبرانية، مسجلة ارتفاعًا ب 4210 حالة عن عام 2019. وتشمل هذه الجرائم الإرهاب المعلوماتي والاحتيال والأضرار التي لحقت بالأشخاص ونظم المعلومات. وعلى الرغم من أنه لا تزال هناك فجوة كبيرة بين

[184]-John Calabrese, The New Algeria and China, 26.01.2021, Link: http://bitly.ws/swqE, seen on: 26.05.2023.

[185]-Zoltán Sipos, Cybersecurity in Algeria, **Journal of Security and Sustainability Issues**, ISSN 2029-7017 print/ISSN 2029-7025 online 2023 Volume 13, 30.03.2023, link: http://bitly.ws/CRry, seen on: 12.04.2023, p.65.

الحاجة الملحة لنظام أمن إلكتروني فعال وتنفيذ الجهود، تسجل الجزائر بعض التقدم في سلم ترتيب التطور السيبراني؛ فحسب مؤشر تطوير الحكومة السيبراني، وبعدما احتلت المرتبة 130لعام 2018، سجلت قفزة نوعية في عام 2022، حيث تم تصنيفها في المرتبة 112[186].

غير أن ذلك التقدم يعتبر جد طفيف. فبعد تحقيق أجرته الجمعية الجزائرية لأمن نظم المعلومات (AASSI) مع عدة منظمات، تم التوصل إلى الاستنتاجات التالية[187]:

-1٪ من المؤسسات الجزائرية تستخدم معيار أمن المعلومات ISO؛

- 7.5 ٪ ليس لديهم إجراءات الامتثال لتكنولوجيا المعلومات؛

-10/1 ليس لديهم خطة استئناف النشاط؛

-1٪ لديهم سياسة لإدارة الفجوات.

تواجه الجزائر اليوم تحديات عديدة. الأحداث السياسية المحلية في الماضي القريب، فضلاً عن التهديد المستمر من تنظيم القاعدة في المغرب العربي (AQIM) والدولة الإسلامية (IS)، فضلاً عن التهديد الأجنبي الطويل الأمد. فالتوترات السياسية، تشكل تحديات خطيرة لقيادة البلاد. في خضم هذه الصعوبات، قد يبدو سؤال الأمن السيبراني للوهلة الأولى مهملاً، ومع ذلك، فإن الانتشار الواسع لتقنيات الإنترنت المرتبطة بمخاطر الأمن تتطلب حتما إدخال معايير أمن المعلومات الدولية وخلق الخلفية القانونية اللازمة. نفس القدر من الأهمية يستوجبه تدريب المهنيين المناسبين، وإنشاء أطر تنظيمية لا تقل أهمية عن تعليم النظافة الرقمية للمستخدمين. هذه الشروط ضرورية إذا كانت الدولة تريد زيادة أمنها الداخلي والخارجي وقدرتها التنافسية الاقتصادية[188].

## المطلب الثاني: حوادث الأمن السيبراني وفق أنماط الهجومات السيبرانية وطرق إدارتهما

اختلف في تصنيف حوادث الأمن السيبراني، وانقسم الباحثون إلى ثلاث فئات؛ فئة ربطته بالخطأ البشري، أي أن النظام خال من أي خطأ، أو عيب ويعمل بشكل صحيح. ولكن تم استخدامه بشكل خاطئ. ومثال ذلك، قيام شخص بخطأ أو إهمال أدى لوقوع الحادث. وهناك فئة ربطته بالأفعال الخبيثة الضارة؛ إذ أرجعت الحادث إلى عمل ضار. ومثال ذلك:

[186]-Zoltán Sipos, Cybersecurity in Algeria, **Journal of Security and Sustainability Issues**, Op.cit, p.71.
[187]-Ibid.
[188]-Ibid.

تسبب الهجوم الإلكتروني- أو الهجوم المادي، أو تخريب للمتلكات، أو أي هجوم من الداخل، أو سرقة وما يمكن قياسه على ذلك- في إثارة الحادث. أما الفئة الثالثة فركزت على إخفاقات، أو فشل الطرف الثالث في تقديم خدماته؛ إذ يرجع الحادث إلى إخلال أو انقطاع خدمة طرف ثالث(المؤسسات الخدماتية). ومثال ذلك: تسبب انقطاع التيار الكهربائي – أو انقطاع الإنترنت.....الخ- في إثارة الحادث[189]. غير أن الراجح في تصنيف الهجمات السيبرانية هو الاعتماد على مدى شدتها، وهذا ما ركز عليه (الفرع الأول) من هذا المطلب. بعد ذلك، سعت الدراسة إلى محاولة إسقاط تلك التصنيفات على الحوادث السيبرانية في البلدين(الفرع الثاني)

## الفرع الأول: أنماط الهجمات السيبرانية و تصنيف حوادث الأمن السيبراني بهما

أشار التصنيف الأوروبي إلى أن على الجهات المعنية مراعاة بعض العوامل لدى تقييم شدة التهديد، ومن هذه العوامل؛ نجد دراسة المخاطر بالنسبة للدولة أو الشركات أو الأفراد. لم يغفل كذلك حجم الجهد المطلوب، أو التكاليف اللازمة للتخفيف، أو للحماية، أو لمعاجلة التهديد، أو الخطر. بالإضافة إلى ما ذكر، على الجهات المعنية عدم إغفال مقدار الأضرار المحتملة للدولة أو الشركات أو الأفراد، والتي يمكن أن يكون سببها التهديد. كذلك يجب قياس حجم ومعدل انتشار التهديد (عدوانيته). القيام بدراسة إحصائية على استمرارية الهجمات؛ عددها وتكرارها. وفي الأخير، وجب عدم إغفال أهمية الأنظمة التي يحتمل تأثرها بالتهديد أو الحادث. وغيرها من العوامل المتعلقة بتقييم شدة تأثير التهديد[190].

وانطلاقا من دراسة شدة التهديد يمكن أن نخلص إلى أنماط الهجومات السيبرانية(الفقرة الأولى)، ومدى مطابقة تلك الأنماط للحوادث الأمنية السيبرانية في البلدين؛ المغرب والجزائر.

### الفقرة الأولى: أنماط الهجمات السيبرانية

تتوزع أنواع الحرب السيبرانية على ثلاثة أنماط مختلفة:**النمط الأول**، "يتعلق بأزمات الحرب "السيبراية المنخفضة الشدة": وتعبر عن صراع مستمر بين الفاعلين

---

[189]-محمد الذنيبات وآخرون، تصنيف حوادث الأمن السيبراني، **الذنيبات للمحاماة والخدمات القانونية**، 2019، رابط المقال: http://bitly.ws/Edry، تاريخ الدخول: 09.05.2023، ص.5.

[190]-المرجع نفسه.

المتنازعين، قد تكون ذات بعد تاريخي، أو ديني، أو إيديولوجي، كالصراع العربي الإسرائيلي مثلا، أو صراع الكوريتين، أو الصراع الهندي الباكستاني، وغيرها. ولهذه الحرب السيبرانية الباردة وسائل عدة، منها شن الحروب النفسية، الاختراقات المتعددة، شن حرب الأفكار، التنافس بين الشركات التكنولوجية العالمية وأجهزة الاستخبارات الدولية[191]. في مثل هذه الصراعات تنشط جماعات دولية للقرصنة للتعبير عن مواقف سياسية، أو حقوقية، مثل جماعة "ويكيليكس"و"أنونيموس"، وكذلك أيضا في حالات الأزمات الدولية، مثل التوتر بين إستونيا وروسيا في عام2007، وكذا الاختراقات المتبادلة بين الصين وواشنطن[192].

أما **النمط الثاني**، فيتعلق بنمط "أزمات الحرب السيبرانية متوسطة الشدة: وتبرز عند تحول الصراع عبر الفضاء إلى حرب تقليدية دائرة على الأرض، كما وقع مع أمريكا وإيران عام 2010 وروسيا وأوكرانيا، عام 2016- 2018[193]. ويكون ذلك تعبيرا عن حدة الصراع القائم بين الأطراف، كما قد يمهد لعمل عسكري. هنا، تدور حروب الفضاء الإلكتروني عن طريق اختراق المواقع السيبرانية، تخريبها، شن حرب نفسية ضد الخصوم، وغيرها. يستمد ذلك النوع من الحروب السيبرانية شدته من قوة أطرافه، وارتباطها بعمل عسكري تقليدي، خاصة في ظل بعض التقديرات التي تشير إلى أن تكلفة هذه الحروب أقل من إنفاق نظيراتها التقليدية، قد يصل تمويل حملة حربية كاملة عبر الإنترنت تكلفة دبابة، من الجهة المهاجمة، لكن الجهة المدافعة قد تتلقى خسائر قاسية[194].

وتاريخيا، تم استخدام الحروب السيبرانية، متوسطة الشدة، في هجمات حلف الناتو، عام 1999، على يوغوسلافيا، وأيضا، برزت خلال الحرب بين لبنان وإسرائيل، عام 2006، وكذلك بين روسيا وجورجيا في عام 2008، والمواجهات بين حماس وإسرائيل في

---

[191]-عبد الغفار عفيفي، الأزمات والحروب السيبرانية...تهديدات تتجاوز الفضاء الإليكتروني، مجلة **الأهرام للدراسات السياسية والاستراتيجية**، 2019/02/03، رابط المقال: Https://acpss/ahram.org.eg، تاريخ الدخول: 20.01.2023.

[192]-بن تغري موسى، الحرب السيبرانية والقانون الدولي الإنساني، منصة المجلة العلمية الجزائرية، الجزائر، العدد02، 2020،ص.6.

[193]-عبد الغفار عفيفي، المرجع نفسه.

[194]-عادل عبد الصادق، أنماط الحرب السيبرانية وتداعياتها على الأمن العالمي، السياسة الدولية، 14.05.2017، رابط المقال: http://bitly.ws/zjn6، تاريخ الدخول: 24.01.2023

عامي 2008 و2012[195]. وقد قال محمد المصري مؤسس الوحدة التي حاولت وضع أسسها لاستراتيجية الحرب السيبرانية متوسطة الشدة ضد إسرائيل، "لم يعد من الضروري أن يكون لديك الصواريخ لتدمير منشأة كهربائية. بدلا من ذلك، سيحصل اختراق شبكات العدو وزرع الكود الخاص بك على نتيجة أفضل، ويجنب الخسائر البشرية"[196]. كانت بداية أكتوبر 2000، بمثابة البداية الرسمية للحرب السيبرانية متوسطة الشدة بين الهاكرز العرب والإسرائيليين[197].

أخيرا، **النمط الثالث**، الذي يتعلق ب"أزمات الحرب السيبرانية مرتفعة الشدة وأزماتها كارثية، ويعبر عن نشوء حروب في الفضاء الإلكتروني منفردة، وهي غير متوازية مع الأعمال العسكرية التقليدية، ولم يشهد العالم هذا النوع من الحروب. مع أن بعض الخبراء يرون في الهجوم الإسرائيلي على المنشآت النووية الإيرانية بتعاون مع أمريكا عام 2010 يمكن إدراجها في هذا النوع[198]. في هذا السياق المرتفع الشدة، يتم استخدام الفضاء الإلكتروني للاستعداد لحرب المستقبل، عبر قيام الدول بتدريبات على توجيه ضربة أولية لحواسب العدو، واختراق العمليات العسكرية عالية التقنية، أو حتى باستهداف الحياة المدنية، والبنية التحتية المعلوماتية، والهدف من وراء ذلك تحقيق "الهيمنة السيبرانية الواسعة"[199].

ينطوي هذا النمط الثالث من الحروب، والذي يسميه البعض-الحرب السيبرانية "الساخنة"، على سيطرة البعد التكنولوجي على إدارة العمليات الحربية، حيث يتم استخدام الأسلحة الإلكترونية فقط ضد منشآت العدو، وكذا اللجوء إلى الروبوتات الآلية في الحروب والطائرات دون طيار، وإدارتها عن بعد[200]. وقد لاحظ رئيس الوزراء البريطاني بوريس جونسون، في نوفمبر 2021، في حوار حاد مع توبياس إلوود، رئيس لجنة مجلس العموم التي تشرف على الدفاع، أن "المفهوم القديم لخوض معارك الدبابات الكبيرة على الكتلة

---

[195]- بن تغري موسى، الحرب السيبرانية والقانون الدولي الإنساني، مرجع سابق، ص.6.

[196]-Hasan M.Al-Rizzo, The undeclared cyberspace war between Hezbollah and Israel, **researchGate**, Contemporary Arab Affairs 1(3):391-405, July 2008, link: http://bitly.ws/zkkw, seen on: 24.01.2023.

[197]-Hasan M.Al-Rizzo, The undeclared cyberspace war between Hezbollah and Israel, Op.cit.

[198]-عبد الغفار عفيفي، الأزمات والحروب السيبرانية...تهديدات تتجاوز الفضاء الإليكتروني، مرجع سابق.

[199]-بن تغري موسى، المرجع نفسه، ص.7.

[200]-عادل عبد الصادق، أنماط الحرب السيبرانية وتداعياتها على الأمن العالمي، مرجع سابق.

الأرضية الأوروبية قد انتهى، هناك أشياء كبيرة أخرى يجب أن يستثمر فيها؛مثل الإنترنت - هكذا ستكون حرب المستقبل[201].

والغرب متوجس من هذا النمط من الهجمات السيبرانية، لدرجة خطورته على شركاتهم العملاقة. فعلى سبيل المثال، أطلق جهاز المخابرات العسكرية الروسية، GRU، إحدى عملياته السيبرانية الدورية ضد مجموعة من الأهداف الأوكرانية في ما يسمى هجوم "NotPetya"[202] أخطأ الهجوم وانتشر على مستوى العالم، مما أدى إلى تدمير قدرة العديد من الشركات الغربية على العمل، وتسبب في أضرار تجارية تقدر بحوالي 10 مليارات دولار. تعرضت شركة "ميرسك"، عملاقة الشحن البحري، إلى اضطراب شديد. تعطلت بشدة العديد من الشركات؛ من شركة المحاماة العالمية"DLA Piper" إلى مرافق إنتاج الشوكولاته في" Cadbury" في هوبارت، قبالة الساحل الجنوبي لأستراليا[203]. كان عام 2021 مروعًا للأمن السيبراني الغربي. كان له علاقة كبيرة بروسيا، التي تعد أكبر موطن لمجرمي الإنترنت في العالم. حسبت شركة" Chainanalysis" أن ما يقرب من ثلاثة أرباع الإيرادات المتزايدة بشكل كبير من برامج الفدية في عام 2020 ذهبت إلى الجماعات الإجرامية السيبرانية في روسيا. في الولايات المتحدة كذلك، أدت عملية إجرامية ضد شبكة المؤسسة العادية لخط أنابيب كولونيال إلى قيام الشركة بإيقاف نقل الوقود إلى شرق الولايات المتحدة، مما تسبب في نقص كبير في محطات الوقود. والأسوأ من ذلك، أدى هجوم شنته مجموعة تسمى "Conti ransomware" إلى إغلاق الهيئة الإدارية في إيرلندا المكلفة

[201]-Ciaran Martin, Cyber Realism in a Time of War, **lawfare**, Wednesday, March 2, 2022, link : http://bitly.ws/zkoV, seen on: 25.01.2023.

[202]-**هجوم "NotPetya"**: في يونيو 2017، عندما ظهرت البرامج الضارة "NotPetya" لأول مرة على أجهزة الكمبيوتر في جميع أنحاء العالم، لم يستغرق الأمر وقتًا طويلاً بالنسبة للسلطات في أوكرانيا، حيث بدأت العدوى، لإلقاء اللوم على روسيا في الهجوم السيبراني المدمر الذي تسبب في أضرار بقيمة 10 مليارات دولار عالميا. كان NotPetya أحد مكونات الصراع المستمر بين روسيا وأوكرانيا، ولكن على الرغم من أنه تم تصميمه للتسلل إلى أنظمة الكمبيوتر عبر جزء شائع من برامج المحاسبة الأوكرانية، فقد انتشر الفيروس بعيدًا عن حدود أوكرانيا، مما تسبب في قدر هائل من الأضرار المتنوعة.

(Josephine Wolff, "How the Notpetya attack is reshaping cyber insurance", **Brookings**, 01.12.2021, link: http://bitly.ws/IFbZ, seen on: 16.06.2023)

[203]-Ciaran Martin, Ibid.

بإدارة نظام الرعاية الصحية الوطني مع ما يترتب على ذلك من عواقب مدمرة للغاية، بالنسبة للسرطان وغيرها من العلاجات الصحية الحرجة[204].

في عام 2020، احتج الرئيس بايدن جهارًا أمام الرئيس بوتين في جنيف بشأن "الملاذ الآمن" الذي توفره روسيا لمثل هذا النشاط. ومنذ ذلك الحين، كانت هناك بعض الاعتقالات المسرحية لمجرمي الإنترنت الروس. لكن "دبلوماسية العصابات"، على حد تعبير مدير "CISA"[205] السابق "كريستوفر كريبس"، تقطع كلا الاتجاهين. قد لا يكتفي بوتين المحاصر بالتخفيف من حدة المجرمين فحسب، بل قد يشجعهم على إحداث المزيد من الخراب في الغرب. لذلك لكل من هذين السببين، حذرت منظمات مثل CISA والمركز الوطني للأمن السيبراني في المملكة المتحدة، من أي تهديدات محتملة قد تصل درجتها إلى النمط الثالث المرتفع للحرب السيبرانية[206].

## الفقرة الثانية: إسقاط حوادث الأمن السيبراني في المغرب والجزائر

أشرنا إلى أن التصنيفات الثلاثة لحوادث الأمن السيبراني ترتبط بدرجة حدة الهجمات السيبرانية. وقد انقسمت إلى أزمات حرب سيبرانية منخفضة الشدة، متوسطتها -أي الشدة- ومرتفعتها.

تعتمد هذه الأشكال الثلاثة من الهجومات السيبرانية على أسلحة سيبرانية كثيرة ومتنوعة؛ حيث نجد الفيروسات، الديدان؛ كدودة ميليسا( انتشرت عام 1999)، دودة ستكسنت( انتشرت سنة 2010)، أحصنة طراودة؛ وهي عبارة عن شفرة صغيرة يتم تحميلها مع برنامج رئيسي من البرامج ذات الشعبية العالية، القنابل المنطقية، الماكينات والميكروبات

---

[204]-Ciaran Martin, Cyber Realism in a Time of War, Op.cit.

[205]-CISA: تثبت شهادة CISA **(Certified Information Systems Auditor):** (مدقق نظم المعلومات المعتمد) خبرة المحترف القادر على إجراء عمليات التدقيق، والتحكم في تقنيات وأنظمة تكنولوجيا المعلومات الخاصة بالشركة ومراقبتها. يمكن لحامل شهادة CISA إجراء عمليات تدقيق تكنولوجيا المعلومات، لدعم حوكمة وإدارة تقنيات تكنولوجيا المعلومات، ولكن أيضًا الحصول على أنظمة تكنولوجيا المعلومات وتطويرها وتنفيذها للشركة.
كما أنها قادرة على ضمان مرونة الشركة وأنظمة تكنولوجيا المعلومات وحماية البيانات. هذا هو السبب في أن شهادة CISA معترف بها للغاية في مجال الأمن السيبراني. تتمثل المهمة الرئيسية لخبير تدقيق تكنولوجيا المعلومات في منع الاحتيال وتجنب النفقات غير الضرورية وضمان امتثال الشركة. إذا تم اكتشاف حالة شاذة، فإنه يقدم تقريرًا للمديرين التنفيذيين في المنظمة.
(Adem K, Certification CISA : qu'est-ce que c'est et comment l'obtenir ?, **Cyberuniversity**, 14.03.2022, lien de l'article: http://bitly.ws/HBmc, date visite :07.06.2023

[206]-Ciaran Martin, Ibid.

فائقة الصغر، الأبواب الخلفية، المدافع جيت والرقائق shipping، كلها أسلحة سيبرانية تتراوح شدتها من منخفضة القوة إلى شديدتها[207].

ولإسقاط تلك الأشكال الثلاثة على الصراع السيبراني المغربي-الجزائري، نجد أن ذلك الصراع السيبراني الثنائي بين البلدين ينتمي بنسبة كبيرة إلى النمط الأول، المتصف بانخفاض شدته. ولا يرقى إلى مصاف النمطين المتوسط أو الشديد.

صحيح أن هناك تكاثر للهجمات السيبرانية بين البلدين، مما يسلط الضوء على فتح جبهة جديدة بينهما؛ جبهة الحرب السيبرانية، لكنها حرب لم ترتفع شدتها لكي تتحول إلى حرب تقليدية.

نأخذ بعض الأمثلة في ذلك؛ في 22 نونبر من سنة 2022، تعرض موقع الاتحاد العام للمقاولات المغربية (CGEM) لاختراق كمبيوتري. في غياب القدرة على الوصول إلى محتواه، تمكن مستخدمو الإنترنت من التفكير في علم جزائري مصحوبًا بالنقش: "لا سلام بين الأنظمة". هذا النوع من العمليات له اسم دقيق للغاية بلغة الكمبيوتر: إنه **"التشويه"**، وهي عملية ليست معقدة من الناحية الفنية، وتتألف ببساطة من تعديل الصفحة الرئيسية للموقع. الهدف المنشود ليس سرقة البيانات، ولكن لنقل رسالة، مفادها أن الدولة العدو قادرة على اختراق الدفاع السيبراني للدولة الأخرى. وقد جرت عملية تدقيق لمحاولة تحديد العيوب التي جعلت من الممكن الاستيلاء على الموقع، ولكن أيضًا لضمان عدم حدوث مثل هذا الحادث مرة أخرى[208].

وقد سبق هذا الاختراق الجزائري لبعض مواقع المغرب السيبرانية، اتهام إذاعة راديو إم الجزائرية لمجموعة القراصنة المغاربة "فريق موروكو هاك" بأنهم وراء هجوم سيبراني على موقع وزارة المالية الجزائرية، في 9 نونبر 2022. وسبق أن اتهم وزير الاتصال

[207]-فريدة طاجين، تأثير القوة السيبرانية على الاستراتيجيات الأمنية للدول الكبرى دراسة حالة – الصين، رسالة لنيل شهادة الماستر في ميدان الحقوق و العلوم السياسية، جامعة قاصدي مرباح ورقلة، كلية الحقوق و العلوم السياسية- قسم العلوم السياسية ، الجزائر، السنة الجامعية، 2017-2018، ص ص،31-33.

[208]-Soufiane Khabbachi, Maroc-Algérie : la discorde s'invite sur le front numérique, **Jeune Afrique**, 26.11.2021, lien de l'article: http://bitly.ws/CT8w, date visite : 12.04.2023.

الجزائري السابق والمتحدث باسم الحكومة، عمار بلحيمر، المغرب مرارا بتنفيذ هجمات إلكترونية على مواقع جزائرية[209].

كذلك في ديسمبر 2020، اتُهمت نفس المجموعة –من طرف السلطات الجزائرية- باختراق عشرات المواقع الجزائرية، بما في ذلك بعض مواقع الوزارة الرسمية. هناك أيضًا، يقوم المتسللون بتنفيذ عملية تشويه وترك رسالة: "اخترق "فريق اختراق الثلج م" الموقع. عاشت إمبراطورية المغرب: تاريخنا يتحدث عنا. موريتانيا والجزائر جزء منا "[210].

هنا يطرح السؤال، هل سيكون اختراق CGEM شكلاً من أشكال الانتقام من هذه الهجمات السيبرانية من قبل قراصنة مغاربة؟ وهل فعلا وقع الاختراق من طرف المغاربة؟ أم فقط اتهام جزائري لا أساس له من الصحة؟ ولماذا تم استهداف موقع أرباب العمل المغاربة على وجه التحديد؟

لمؤسسة أرباب العمل المغاربة بعد رمزي، CGEM [211] نشط على الساحة الأفريقية والأوروبية. من خلال تسطيح موقعها، دون القدرة على التأثير حقًا في أفعالها، فإن تقزيم مصداقية المنظمة هي التي يسعى المتسللون إلى تحقيقها. لذلك فإن الهجوم له بعد رمزي قبل كل شيء. بالنسبة ل"علي متعب"، المدير المساعد في شركة " Hyperborée Advisors"[212] والخبير في الاستخبارات الاستراتيجية، يوضح هذا التشويه قبل كل شيء "امتداد الصراع على أساس توازن القوى. تحقق كل ثغرة نقطة لأي شخص يتمكن من استغلالها بشكل فعال". إذا لم يتم وضع مدى هذه الهجمات في الاعتبار، تظل الحقيقة أنها

---

[209]-Soufiane Khabbachi, Maroc-Algérie : la discorde s'invite sur le front numérique, op.cit.

[210]-Ibid.

[211]-CGEM: Confédération Générale des Entreprises du Maroc
هي صوت القطاع الخاص في المغرب. تأسست في عام 1947، وهي تمثل أكثر من 90.000 عضو مباشر ومنتسب. وقد رسخت مكانتها كممثل رسمي للقطاع الخاص مع السلطات العامة والشركاء والمؤسسات الاجتماعية. يحمل CGEM صوت القطاع الخاص من خلال تمثيله، والدفاع عن مصالحه على المستويات الإقليمية والوطنية والدولية والعمل من أجل تحقيق مناخ موات لريادة الأعمال.
(La CGEM, qui sommes nous ?, lien de l'article: http://bitly.ws/KLd5, date visite : 07.O7.2023).

[212]-شركة Hyperborée Advisors: تأسست في عام 2016، وهي شركة استشارات في مجال الاتصالات والاستخبارات الاستراتيجية مقرها في الرباط، المغرب. طموحها الأساسي هو تقديم خبرتها لدعم عملائها في استراتيجيات التنمية الخاصة بهم، سواء في الاتصال المؤسسي أو إدارة المخاطر.
من خلال مختبرها للأفكار، تقدم H-Advisors لقرائها تحليلات تتعلق بكل من القضايا الاستراتيجية الحالية والقضايا القطاعية مثل التمويل والصحة واللوجستيات والدفاع والأمن والطاقة والسياسات العامة.
(Hyperborée Advisors, **Linkedin**, lien de l'article: http://bitly.ws/KLaX, date visite: 07.07.2023)

تنشئ سجلاً جديدًا للصراع بين الجارتين، وهو الحرب الرقمية. لمواجهة التحديات والتهديدات الجديدة المرتبطة بظهور التكنولوجيا الرقمية، ضاعف المغرب على مدى السنوات العشر الماضية الآليات التي تهدف إلى تعزيز أمنه السيبراني[213].

## الفرع الثاني: صد الهجمات السيبرانية

تختلف الطرق المعتمدة بين البلدين في محاولتهما لصد الهجمات السيبرانية، والقضاء على التغرات الرقمية. غير أن الجزائر تختار الطريق الأسرع للوصول إلى مصدر الخطر. وهذا ما حاولت الدراسة تبيانه في هذا الفرع من خلال التطرق إلى الطرق المعتمدة في البلدين(الفقرة الأولى)، ثم مقارنتهما(الفقرة الثانية).

### الفقرة الأولى: الطرق المعتمدة في البلدين

قامت المديرية العامة لأمن أنظمة معلومات الجيش بالمغرب بإنشاء **جهاز تشفير** لحماية بيانات المستخدمين، واستطاعت أن تتوصل إلى أن العديد من الهياكل العامة والخاصة قد تعرضت لهجمات إلكترونية مختلفة. في عام 2021 وحده، احتوى الجيش ما لا يقل عن 400 هجوم، وهو أمر خطير للغاية على أمن مستخدمي الإنترنت. ورصد مركز المراقبة التابع للقوات المسلحة كيف زادت هذه الهجمات، وللتعامل معها ومنعها، تضاعف تواجد الجيش على الشبكة في محاولة لتحييد أي نوع من التهديد، داخليًا وخارجيًا. سيحاول هذا ضمان سرية متصفحي الويب وأمنهم وسيؤكد على حماية الخصوصية أثناء تبادل المعلومات[214].

تحقيقا لهذه الغاية، طورت DGSSI **جهاز تشفير** بالكامل من أصل مغربي 100 ٪، والذي تم توفيره للبنى التحتية الحساسة القائمة على برامج التشفير الوطنية. الهدف من هذه الأداة هو حماية البيانات الخاصة بالمكالمات والتسجيلات الصوتية وما إلى ذلك، بالإضافة إلى النصوص من أجل مكافحة القرصنة[215].

أفاد عبد اللطيف لودي، الوزير المنتدب لدى رئيس الحكومة المكلف بإدارة الدفاع الوطني، أن المديرية العامة للأمن العام قدمت الكثير من المساعدة الفنية للبنية التحتية

---

[213]-Soufiane Khabbachi, Maroc-Algérie : la discorde s'invite sur le front numérique, Op.cit.
[214]-Jorge Ortiz, Moroccan army repels more than 400 cyber-attacks, **Atalayar**, 19.11.2021, link: http://bitly.ws/CRAh, seen on: 12.04.2023.
[215]-Ibid.

الحيوية لتسهيل نشر الوسائل الضرورية لمراقبة ومكافحة الهجمات السيبرانية. وأضاف الوزير أنه بسبب هذه التهديدات الأخيرة للأنظمة التكنولوجية، تم التحقيق في أمن أنظمة الوزارات والمؤسسات العامة والهيئات الاستراتيجية لضمان وتقييم آلياتها الأمنية ضد هجمات القراصنة. تحقيقا لهذه الغاية، تم استخدام الجهاز الجديد للاختبار[216].

يضيف لودي "Loudy" أيضًا، أن DGSSI قد تبنت تدابير مثل دمج برمجيات التشفير المتقدمة للغاية، وتسليط الضوء على القطاعات والهياكل الحكومية داخل الحكومة التي تدعمها، لحماية البيانات والاتصالات[217].

وقادت الحقائق المغرب إلى التقدم في عالم الأمن السيبراني، وبفضل أنظمة الحماية التي تطبقها البلاد، أصبح الآن في المرتبة الخمسين من الدول التي تتمتع بأفضل أمان، بحسب الترتيب الذي أجراه الاتحاد الدولي للاتصالات، من المرتبة 93 حيث كانت آخر مرة تم فيها تنفيذ التقرير. الجدير بالذكر أنه في العصر الذي نعيش فيه وهو جائحة فيروس كورونا ونتيجة لذلك تم رقمنة معظم القطاعات وطريقة تسيير الشؤون المختلفة[218]. برزت جائحة -COVID 19 في وقت سابق من عام2020، وبرز معها انتقال الكثير من سكان العالم إلى الإنترنت، مما أدى إلى تسريع التحول الرقمي الذي كان جاريا منذ عقود، و إلى إبراز الفجوات المتبقية. في حين أن بعضُ الفجوات الرقمية قد تطورت بسرعة في السنوات الأخيرة، إلا أن البعض الآخر لم يواكبها، تاركا بعض الأشخاص وراء الركب في التسريع الرقمي الناجم عن COVID. بالإضافة إلى ذلك، أدى الاعتماد المتزايد على الحلول الرقمية إلى زيادة إلحاح المخاوف بشأن الخصوصية والأمن الرقمي وكيفية تحقيق السيادة الرقمية[219].

إن أهمية الأمن في ذروتها، لا سيما في الأنظمة العامة التي توفرها الحكومة والوزارات، والتي غيرت طريقتها في ممارسة الأعمال التجارية وأصبحت الآن على الإنترنت. في هذه الحركات على وجه التحديد، يتم تبادل وسرقة معظم البيانات الشخصية

---

[216]-Jorge Ortiz, Moroccan army repels more than 400 cyber-attacks, Op.cit.
[217]-Ibid.
[218]-Ibid.
[219]-ياسين مليح، السيادة الرقمية ... تجلياتها وممكنات تحقيقها بالمغرب، مجلة الشرق الأوسط للدراسات القانونية والفقهية، سلسلة مؤلفات وأعمال جامعية، جامعة الحسن الأول، سطات، العدد36، 2021، ص.6.

والمعلومات الخاصة لأسباب متنوعة، سواء كانت تنمرًا عبر الإنترنت أو سرقة الهوية، وما إلى ذلك[220].

أهمية الحماية الفعالة للأنظمة الإلكترونية أمر حيوي. خاصة في الأرشيفات الرقمية للدول، التي يتعرض أمنها واستدامتها للخطر، لأن الهدف الرئيسي للهجمات السيبرانية هو القرصنة وسرقة البيانات والأضرار والحرب السيبرانية. كل هذا يؤدي إلى عواقب سلبية للغاية على البلدان، يمكن أن تكون مدمرة لكل من المنظمات والمواطنين العاديين[221].

فمنذ عام 2012، أبدى المغرب اهتمامًا بتحسين أنظمته ضد هذه الهجمات، وبالتالي، في البحث عن طرق لكبحها وحماية نفسه من خلال التدابير. ولهذه الغاية، تم وضع العديد من القوانين في الإطار القانوني لتعزيز أمن أنظمة المعلومات، وضمان حماية الفضاء السيبراني ومعاقبة أي شخص ينتهك الخصوصية على الإنترنت[222].

**أما بالنسبة للجزائر،** فالمحيط الكمي للإجرام المعلوماتي في الجزائر غير واضح المعالم، لعدم وجود دراسات وبحوث من شأنها كشف اللثام عن أرقام ومؤشرات للخسائر في الجزائر جراء هذا النمط الإجرامي، وإن كانت الجزائر ليست بمنأى عن خطورة الجرائم المعلوماتية طالما أنها تحتل جزءا من الفضاء الإلكتروني، خاصة فيما يتعلق بالحواسيب المالية وبعض الهيئات الحكومية التي يعتبر اختراق مواقعها ضمن حجم الأضرار الناتجة عن الجريمة المعلوماتية[223].

لهذا الشأن أنشأت الجزائر مركز الوقاية من جرائم الإعلام الآلي للدرك الوطني، سنة 2008، ويعتبر الجهاز الوحيد المختص بهذا الصدد في الجزائر، هدف إلى تأمين منظومة المعلومات لخدمة الأمن العمومي، واعتبر بمثابة مركز توثيق ومقره يوجد ب"بئر مراد رايس"، وهذا المركز يعكف على تحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة، وتحديد هوية أصحابها سواء كانوا أشخاصا فرادى أو عصابات، وهذا كله من أجل

---

[220]-Jorge Ortiz, Moroccan army repels more than 400 cyber-attacks, Op.cit.
[221]-Ibid.
[222]-Ibid.
[223]-إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، **مصداقية**، 01.12.2019، رابط المقال: http://bitly.ws/zEZq، تاريخ الدخول 13.04.2023، ص.112.

تأمين الأنظمة المعلوماتية والحفاظ عليها، لاسيما تلك المستعملة في المؤسسات الرسمية والبنوك[224].

ويهدف هذا المركز إلى مساعدة الأجهزة الأمنية الأخرى بالتعاون من أجل مكافحة الجرائم المعلوماتية، حيث يعنى المركز بتطوير أساليب التعامل مع هذه الجرائم ووضع قوانين لتنظيم مجال استغلال المعلومة من خلال تنسيق مع وزارة العدل وكذا من خلال معهد خاص بعلم الإجرام، لتطوير مستوى التعامل مع الجريمة بصفة عامة والجريمة المعلوماتية بصفة خاصة[225].

فالجزائر تعمل جاهدة على الاستفادة من خبرات البلدان الأخرى في تأمين المنظومة المعلوماتية وحمايتها من الجرائم ضمن مجموعة من العناصر أهمها[226]:

**الوقاية**: وتشمل حملة تحسيسية وتوعية بالتنسيق مع وزارة التضامن الوطني والأسرة، والعمل على ملتقيات ومحاضرات وأيام دراسية ومنتديات دولية، ومشاركة في منتديات صحفية وحصص تلفزيونية وإذاعية وغيرها من وسائل النشر والإشهار.

**المكافحة**: توعية الجزائريين من خلال استعمالهم لشبكات التواصل واستخدام الأنترنت، وذلك من خلال تعليقاتهم المدافعة عن الجزائر ومعرفة الأخطار بسلوكيات مشبوهة أو اعتداءات عبر نشر فيديوهات توصل إلى الجناة، مما يسهل التحقيق لدى مصالح الدرك وإلقاء القبض على المشبوهين ومرتكبي الجرائم في الوقت المناسب.

**المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني:** مؤسسة عمومية ذات طابع إداري تحت الوصاية المباشرة لوزير الدفاع الجزائري، مكلفة بمهام متعددة كإجراء الخبرات والفحوص في إطار التحريات الأولية والتحقيقات القضائية، ضمان المساعدة العلمية أثناء القيام بالتحريات المعقدة .

يعتبر المعهد أحد المشاريع المنجزة في إطار تطوير سلك الدرك الجزائري "ببوشاوي"، حيث تم إنشاؤه بموجب مرسوم رئاسي 04 / 133 المؤرخ في 26 يونيو

---

[224]-شعيب قاسمي وفؤاد بلغيث، الاستراتيجيات الدولية في مكافحة الجريمة السيبرانية-دراسة حالة الجزائر-، رسالة لنيل شهادة الماستر في العلوم السياسية والعلاقات الدولية، جامعة العربي التبسي-تبسة-، كلية الحقوق والعلوم السياسية، الجزائر، السنة الجامعية 2019-2020، ص.94.

[225]- إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مرجع سابق، صص.113-114.

[226]-المرجع نفسه.

2004، ودخل حيّز الخدمة ابتداءً من فاتح يناير 2009، أما الفترة الممتدة بين 2004 و 2009 فكرست لتكوين الموارد البشرية واقتناء المعدات العلمية والتقنية الضرورية، ويقوم المعهد بالعديد من المهام التي من شأنها تلبية الطلبات الواردة من السلطة القضائية، ضباط الشرطة القضائية والسلطات المؤهلة، قانونيا خاصة أثناء معالجة القضايا المعقدة. والإسهام في تنظيم دورات الإتقان والتكوين ما بعد التدرج في تخصص العلوم الجنائية، يحتوي على العديد من الأقسام والمصالح المختصة من أهمها: مصلحة البصمات؛ مصلحة البيئة؛ في ما يخص مجال الأمن السيبراني هناك **مصلحة الإعلام الآلي**؛ على مستوى هذه المصلحة يتم رصد ومراقبة وتتبع عمليات الاختراق والقرصنة المعلوماتية وكذا اكتشاف المعلومات المسروقة وتفكيك البرامج المعلوماتية.

**المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الجزائري**[227]: استجابة لمطلب الأمن المعلوماتي ومحاربة التهديدات الأمنية الناجمة عن الجرائم السيبرانية قامت مصالح الأمن بإنشاء المصلحة المركزية للجريمة السيبرانية التي عملت على تكييف التشكيل الأمني لمديرية الشرطة القضائية، والتي كانت عبارة عن فصيلة شكلت النواة الأولى لتشكيل أمني خاص لمحاربة الجريمة السيبرانية. وعلى مستوى المديرية العامة للأمن الجزائري والتي أُنشئت سنة 2011 ليتم بعدها إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بقرار من المدير العام للأمن الجزائري وأضيف للهيكل التنظيمي لمديرية الشرطة القضائية في يناير2015؛

**الهيئة الجزائرية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها:** [228]

تشكلت هذه الهيئة بمقتضى المرسوم الرئاسي رقم 261 - 15 وهي سلطة إدارية مستقلة لدى وزير العدل، تعمل تحت إشراف ومراقبة لجنة مديرية يترأسها وزير العدل وتضم أساسا أعضاء من الحكومة معنيين بالموضوع ومسؤولي مصالح الأمن وقاضيين من المحكمة العليا يعينهما المجلس الأعلى للقضاء . وكلفت الهيئة باقتراح عناصر الاستراتيجية

[227]-شعيب قاسمي وفؤاد بلغيث، الاستراتيجيات الدولية في مكافحة الجريمة السيبرانية-دراسة حالة الجزائر-، مرجع سابق، ص.95.
[228]-المرجع نفسه، ص.96.

الجزائرية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما وتنشيط وتنسيق عمليات الوقاية منها، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة هذه الجرائم، من خلال جمع المعلومات والتزويد بها، ومن خلال الخبرات القضائية، وضمان المراقبة الوقائية للاتصالات الإلكترونية، قصد الكشف عن جرائم متعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة. وقد نصت سابقا على إنشاء هذه الهيئة المادة 13 من القانون 04 / 09 المؤرخ في غشت المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها من خلال: «تنشأ هيئة وطنية وتنظيمها وكيفيات سيرها عن طريق التنظيم » أما مهامها فقد أوردت المادة 14 من نفس القانون وتتمثل في[229]:

أ- الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: إن إجراءات الوقاية تكون بتوعية مستعملي تكنولوجيات الإعلام والاتصال بخطورة الجرائم التي يمكن أن يكونوا ضحاياها وهم يتصفحون أو يستعملون هذه التكنولوجيات، ومن أهم هذه الجرائم: التجسس على الاتصالات والرسائل الإلكترونية، التلاعب بحسابات العملاء، اختراق أجهزة الشركات والمؤسسات الرئيسية أو الجهات الحكومية...الخ

ب- مكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال: بحسب نص المادة 14 من القانون 04 / 09 هناك نوعان من المكافحة تقوم بهما هذه الهيئة:- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية المادة 14فقرة( ب )من القانون 09 / 04 ؛ -تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، يقترح المشروع في هذا الفصل إنشاء هيئة جزائرية مختصة تتولى مهام أهمها: تنشيط وتنسيق عملية الوقاية من الجرائم المعلوماتية ومساعدة السلطات القضائية ومصالح الشرطة القضائية من التحريات التي تجريها بشأن هذه الجرائم، وما تقوم

[229]-إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مرجع سابق، صص.113-114.

به أيضا من تجميع المعلومات من نظيرتها في الخارج قصد محاربة هذا النوع الخطير من الإجرام[230].

### الفقرة الثانية: دراسة مقارنة بين البلدين في مجال الحماية السيبرانية

لمقارنة الطرق المعتمدة من طرف البلدين لابد من الإشارة إلى نقطة محورية، تبني عليها الجزائر طرق تعاملها مع الهجومات السيبرانية. وهي ادعاءات الجزائر المتكررة بأن المغرب يستخدم الحرب السيبرانية ضدها، يجادل العديد من الخبراء بأن قيادة البلاد تسعى فقط لتحقيق أهداف سياسية داخلية. إنها تحاول إقناع الجزائريين بأن بلدهم موجود في حرب مع المغرب ، "خصم أجنبي"، في محاولة لإسكات الدعوات إلى احتجاجات واسعة النطاق.

إن الإعلام المغربي يبتعد في أغلب الأحيان عن تقديم أخبار مزيفة تهمّ الجزائر، وأن أغلب ما ينشر يأتي عن طريق "وكالة المغرب العربي للأنباء" الرسمية، لكنه لا يصل إلى درجة الفبركة أو التزييف والتضليل، ويقول: "ربما هناك بعض التهويل في بعض الأحداث، لكنها بعيدة عن اختلاق ما لا وجود له، عكس جرائد ومواقع ووكالة أنباء الجزائر التي تخصص قدراً يومياً لا ينزل عن عشر قصاصات مضادة للمغرب، بل إن بعض المنابر تعمل يومياً على مواضيع بعينها، مثل الهجرة، المخدرات، الملكية، الاحتجاجات الاجتماعية، والاعتقالات..." [231]. كل تلك التصرفات الجزائرية تنبني على معطيات واهية من الصحة، تحاول عن طريقها صرف الرأي العام الجزائري عن مشاكل البلاد الداخلية، وتوجيهه بمعطيات مزيفة عن علاقته مع جاره المغرب.

إن الأطروحات الجديدة للأمن تستوجب علينا التوقف والتمعن في هذا المفهوم بما ينسجم والتغيرات الحاصلة في العالم، لاسيما في ظل التطور الرهيب في مجال الإعلام الآلي وتكنولوجيا الاتصالات والمعلومات. ويتعين على الفاعلين الرسميين الجزائريين، بدل التركيز على المغرب، التوجه نحو "الحوكمة الإلكترونية". إلا أن عدد الجرائم المرتكبة في هذا البلد يوحي بحجم الأخطار التي تتربسها، وهو ما يجعل الجزائر أمام تحديات وعوائق

---

[230]-إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مرجع سابق، ص ص،113-114 .

[231]-سعيدة شريف، المغرب والجزائر... من الجوار الصعب إلى "الحرب الإلكترونية، 15.01.2023، **رصيف22**، رابط المقال:http://bitly.ws/FFno ، تاريخ الخول: 26.05.2023.

جديدة وهو تحقيق الأمن السيبراني حاليا ومستقبلا. إذ تواجه مصالح الدرك و الأمن الجزائريين العديد من العوائق والتحديات التي تعيقها في تحقيق الأمن السيبراني في الجزائر، يمكن أن نذكر أهمها[232]:

-الاستعمال الواسع لشبكات التواصل الاجتماعي، إذ وصل عدد مستعملي هذه المواقع في الجزائر الإلكترونية لأكثر من 13 مليون مستعمل، ما ساهم بشكل كبير في ارتفاع أنواع متعددة من الجرائم السيبرانية مثل القذف، التحرش الجنسي، استغلال القصر، وغيرها وهذا ما يستوجب وضع استراتيجيات جد مكملة لضمان الأمن السيبراني عند استخدام مواقع التواصل الاجتماعي؛

-عمليات التخفي أثناء استعمال خدمات شبكة الأنترنت (Proxy [233])، يعد من أكبر الإشكاليات التي تواجهها الجهات المتخصصة بالتحقيق، ويتطلب تعاون جهات متعددة والتسلح بالوسائل المتطورة التي يمكن لها رصد الجزئيات وفك الشفرات وتطوير البنى الخاصة بالمعلومات، وتحديثها باستمرار، وتصميم برامج عالية التطور؛

-غياب التنسيق بين الدول والحكومات إذ من المعلوم أن الجريمة السيبرانية عابرة للحدود والقارات، وهو ما يعني أن مرتكبيها يمكنهم النفاذ إلى أنظمة الحاسوب في أحد الدول، يتم التلاعب واختراق البيانات في بلد آخر، تسجل النتائج في بلد ثالث ،ناهيك عن أنه من الممكن وكل هذا يساعد المجرم السيبراني في إخفاء هويته ونقل الموارد من خلال قنوات موجودة في بلدان مختلفة، وبالتالي ونتيجة القدرة على التنقل إلكترونيا من شبكة إلى أخرى والنفاذ إلى قواعد البيانات في قارات مختلفة، تصبح عدة دول ومحاكم وقوانين معنية بذلك، ما يشكل تحديا حقيقيا، ولذلك فان المحاربة الفعالة للجريمة السيبرانية تستدعي تعاونا متزايدا، سريعا وفعالا على أعلى درجات التنسيق.

---

[232]-إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مرجع سابق، ص.116-117.

[233]-"Proxy": يأتي proxy من صيغة متعاقد عليها من الكلمة الإنجليزية الوسطى "procuracie" تعني "procuration". قد يشير الوكيل إلى شخص مخول بالتصرف نيابة عن شخص آخر، أو قد يعين وظيفة أو سلطة الخدمة بدلاً من شخص آخر. بالمعنى الأخير، تسبقه عمومًا كلمة ("التصويت بالوكالة"). اتخذ الوكيل مؤخرًا معاني في الحوسبة، حيث يوجد في عبارات مثل الخادم الوكيل، وهو نظام كمبيوتر يسهل تبادل البيانات بين المستخدمين على الشبكة.
(Merriam-Webster, Proxy Noun, **Dictionary**, Link: http://bitly.ws/I6kM, seen on: 12.06.2023).

فالتوجهات العالمية الجديدة تفرض، على الدول العربية، والذي يعد المغرب و الجزائر من بينها، عدة التزامات، منها تنفيذ الخطط العالمية التنموية، ومجابهة التحديات التي تحول دون تنفيذها؛ وذلك من خلال إبداء الالتزام السياسي اللازم وتحديث الاستراتيجيات، لاسيما تكنولوجيا المعلومات والاتصالات، بما يتلاءم مع الأهداف التنموية الجديدة ووفقا لأولويات الدول العربية.

## خلاصة الفصل الأول

سعت الدراسة في فصلها الأول إلى تناول موضوع الدفاع السيبراني في المغرب والجزائر من زاوية نظرية.

اعتمدت في مبحثها الأول، فقط على ثلاث نظريات أساسية؛ الواقعية، الليبرالية والنقدية ، وقامت بإسقاطها على التجربة السيبرانية المغربية-الجزائرية، فتبين أنه لا يمكن الاعتماد على نظرية وإغفال أخرى، بل النظريات الثلاث تتكامل في ما بينها لتعطينا رؤية تصورية حول الحقل السيبراني الشمال إفريقي- المغرب والجزائر نموذجا. وهذا الاستنتاج يشجع على دراسة النظريات المتبقية وتسليطها على التجربتين السيبرانيتين، المغربية والجزائرية، حتى تتضح الرؤية أكثر، حول الواقع السيبراني الشمال إفريقي.

حاولت الدراسة، كذلك، في مبحثها الثاني، التطرق إلى مختلف التهديدات السيبرانية؛ الداخلية والخارجية، التي تؤرق مضجع البلدين. تبين أن صانع القرار الرسمي الجزائري يختصر طريقه في البحث عن أعدائه السيبرانيين، ليوجه أصابع اتهامه لجاره المغرب، دون اعتماده بحثا دقيقا ومستفيضا.

لم تغفل دراسة العلاقة المغربية الجزائرية التطرق إلى خلافاتهما السيبرانية. فتبين أن تلك التصادمات، لا زالت منخفضة الشدة، رغم كثرة الاتهامات بينهما، خصوصا من الجانب الجزائري.

بعد هذا التفصيل النظري في الدفاع السيبراني الشمال إفريقي، المغرب والجزائر نموذجا، سعت الدراسة في فصلها الثاني تناول الهيكلين التنظيميين للدفاع السيبراني في المغرب والجزائر وذلك عبر مبحثين؛ تناولت في المبحث الأول البعد التنظيمي من زاوية بنيته التحتية. أما في المبحث الثاني، فركزت على البعدين المؤسسي والتعاوني، الإقليمي والدولي، للدفاع السيبراني في المغرب والجزائر.

## الفصل الثاني: الهيكل التنظيمي للدفاع السيبراني في المغرب والجزائر

أضحت المعلومات تنقل عبر الشبكات الاجتماعية في غضون ثوان معدودة وبكمية كبيرة، وعلى إثر وفرة تلك المعلومات وسهولة الوصول إليها انبثقت عن ذلك تخوفات من هجمات سيبرانية، فانعدمت الثقة في تلك المعلومات وتوجس المجتمع من غياب الحقيقة ذاتها.[234]

فتحت التغييرات الجارية في الفضاء السيبراني، لا سيما على المستوى التكنولوجي، إمكانيات جديدة للصراع في شروط القتال المعلوماتي. فالسيبرانية هي منطقة نزاع مصطنعة تتجاوز الأرض، أو البحر، أو الجو. توفر إطارًا أصليًا للعمل على التصورات وبواسطة خصائص فريدة ، أهمها إمكانية تمويه هوية الفاعلين ومكان نشوء الهجمات. فالصراع السيبراني هو في جوهره تضارب معلوماتي، بما في ذلك في جوانبه الفنية، ينبني على التخريب والتجسس "sabotage, espionnage, subversion"[235].

ولمقاومة التخريب والتجسس على المعلومات، ومحاربة الهجمات السيبرانية تسعى العديد من البلدان، لتعبئة قواها الحيوية لمكافحة ظاهرة الجريمة السيبرانية وتحصين دفاعها السيبراني. تختلف المبادرات الوطنية من بلد إلى آخر. الأكثر تقدمًا في هذا المجال هي بلا شك الولايات المتحدة الأمريكية. لكن العديد من الدول الأخرى، مثل فرنسا وكندا على سبيل المثال، لا تتوقف عن تطوير ترسانتها الرقمية، حتى يتسنى لها فهم هذه الظاهرة بشكل أفضل. وبدورها تسعى البلدان الناشئة لتطوير دفاعها السيبراني، ومن بينها المغرب والجزائر[236]. ولكي نستوعب أكثر كيفية تطوير قدراتهما الدفاعية في المجال السيبراني، ارتأت الدراسة تناول الفصل الثاني من خلال مبحثين؛ المبحث الأول ارتبط بالبنية التحتية للدفاع السيبراني في المغرب والجزائر، أما المبحث الثاني فاقتصر على المؤسسات المحورية والتعاونات الإقليمية والدولية للدفاع السيبراني في المغرب والجزائر.

---

[234]-Céline Marangé et Maud Quessard, les guerres de l'information à l'ère numérique, l'Institut de Recherche stratégique de l'École militaire, Presses Universitaires de France / Humensis, 2021 ,p.6.

[235]-Ibid ,p.49.

[236]-Ali ELAZZOUZI, La cybercriminalité au Maroc, Impression Bishops Solutions, Casablanca, 01.06.2010, p.132.

## المبحث الأول: البنية التحتية للدفاع السيبراني في المغرب والجزائر

تعتبر حماية البنية التحتية الحيوية للمعلومات مجموعة فرعية من البنية التحتية الحيوية للمعلومات والأمن السيبراني على السواء. ويوفر الدفاع السيبراني الحماية من جميع أشكال الحوادث السيبرانية، من خلال تعزيز سلامة البنية التحتية الحيوية للمعلومات التي تعتمد عليها القطاعات الحساسة، وتأمين الشبكات والخدمات التي توفر الاحتياجات اليومية للمستعملين. ويمكن للحوادث السيبرانية أن تؤثر على البنية التحتية للمعلومات الحيوية وغير الحيوية، وربما تأخذ أشكالاً مختلفة وكثيرة من أشكال الأنشطة الضارة، مثل استخدام روبوتات النت (botnets)[237] في الهجمات المتعلقة برفض الخدمة، ونشر الرسائل الاقتحامية والبرمجيات الضارة(مثل الفيروسات وبرمجيات وورم التخريبية)، التي تؤثر على قدرة الشبكات على العمل. وبالإضافة إلى ذلك، قد تشمل الحوادث السيبرانية أنشطة غير مشروعة، مثل التصيد الاحتيالي (phishing)[238]، والتحايل لسرقة المعلومات الشخصية(pharming)[239]، علاوة على سرقة الهوية. والخطر السيبراني آخذ في الازدياد مع تزايد الأدوات والمنهجيات وتوفرها على نطاق واسع، ومع اتساع نطاق وتطور القدرات التقنية للمجرمين السيبرانيين. وقد تعرضت البلدان على مختلف مراحل تنميتها لهذه المخاطر

---

[237]-**الروبوتات" BOTNET"**: عبارة عن مجموعة من الأجهزة المتصلة بالإنترنت، والتي قد تشمل أجهزة الكمبيوتر الشخصية (أجهزة الكمبيوتر)، الخوادم، الأجهزة المحمولة، أجهزة إنترنت الأشياء (IoT)، المصابة والتحكم فيها بواسطة نوع شائع من البرامج الضارة، وغالبًا ما تكون غير معروفة لمالكها. يتم التحكم في الأجهزة المصابة عن بُعد من قبل الجهات الفاعلة في التهديد، وغالبًا ما يكون مجرمو الإنترنت، وتُستخدم في وظائف محددة، ومع ذلك تظل العمليات الضارة مخفية عن المستخدم. تُستخدم شبكات "البوت نت" بشكل شائع لإرسال رسائل بريد إلكترونية غير مرغوب فيها، وللمشاركة في حملات النقر الاحتيالية وإنشاء حركة مرور ضارة لهجمات رفض الخدمة الموزعة (DDoS).
(Katie Terrell Hanna and others, DEFINITION OF botnet, **TechTarget**, March 2021, link: http://bitly.ws/DU5e, seen on: 03.O5.2023).

[238]-**هجمات التصيد الاحتيالي**: هجمات هندسة اجتماعية، ويمكن أن يكون لها مجموعة كبيرة من الأهداف اعتمادًا على المهاجم. يمكن أن تكون رسائل بريد إلكترونية احتيالية عامة تبحث عن أي شخص لديه حساب PayPal. يمكن أن يكون التصيد أيضًا هجومًا مستهدفًا يركز على فرد معين. غالبًا ما يصمم المهاجم بريدًا إلكترونيًا للتحدث إليك مباشرةً، ويتضمن معلومات لا يعرفها إلا أحد معارفك. عادةً ما يحصل المهاجم على هذه المعلومات بعد الوصول إلى بياناتك الشخصية. إذا كان البريد الإلكتروني من هذا النوع، فمن الصعب جدًا حتى لأكثر المتلقين حذرًا ألا يصبحوا ضحية. حددت شركة "PhishMe Research" أن برامج الفدية تمثل أكثر من 97٪ من جميع رسائل البريد الإلكتروني المخادعة.
(What are the different types of phishing attacks? **TREND business**, link: http://bitly.ws/DU6q, seen on: 03.05.2023**)**.

[239]-**Pharming** : ممارسة احتيال يتم فيها تثبيت تعليمات برمجية ضارة على جهاز كمبيوتر شخصي أو خادم، وإعادة توجيه المستخدمين إلى مواقع ويب احتيالية دون علمهم أو موافقتهم. أطلق على التزييف اسم "التصيد بدون أفخاخ".
Définition Pharming en informatique, **actualité informatique**, lien de l'article :http://bitly.ws/DU7q, date visite: 03.05.2023.

السيبرانية[240]. لهذا السبب، تسعى جل الدول، ومنها المغرب، إلى تطوير ردة فعل دفاعية ضد أي هجوم سيبراني، غير أن الجزائر بنت جل هيكلها الدفاعي على غريمها المغرب.

فالكتابات الأكاديمية الجزائرية تتعاطى مع موضوع السيبرانية بلهجة الفاعلين الرسميين السياسين في البلد، دون اعتماد على مرجعية علمية، هنا تظهر لنا مدى جدية تلك الدولة في تعاملها مع موضوع أمني جد حساس، لازالت حتى الدول العظمى عاجزة عن فرملته بصفة نهائية. فالباحثون الجزائريون، بدل الغوص في مضمار العلم وتقصي منبع الخطر، وبناء استراتيجيتهم الدفاعية، نجدهم يحملون المغرب كامل المسؤولية، ويؤكدون أن الجزائر تعرضت في الآونة الأخيرة لهجمات من طرف المملكة المغربيةٌ، مما أدى حسب قولهم إلى زيادة حدة توتر العلاقات السياسية بين الدولتين، وهذا كان نتيجة استخدام المغرب نظام تجسس بيغاسوس، حسب اعتقاداتهم والتي لا تعتمد على تحر علمي محض، والذي كان بمثابة القطرة التي أفاضت الكأس بين البلدين[241].

وبناء على ماسبق، تناولت الدراسة البنية التحتية للدفاع السيبراني في المغرب والجزائر عبر محطتين؛ الأولى وضحت الاستراتيجيات الأمنية للبلدين(المطلب الأول)، والثانية ساقت القوانين المنظمة لأمن الفضاء السيبراني بهما ومدى تأثيرها(المطلب الثاني).

## المطلب الأول: الاستراتيجيات الأمنية للبلدين

تشكل بعد سنة 2007( تاريخ الهجمات السيبرانية الضخمة التي هزت أستونيا) وسنة 2010( تاريخ إصدار برنامج الألعاب الأولمبية)، حدثان أساسيان كانا وراء نشر العديد من الوثائق الاستراتيجية في جميع أنحاء العالم تقريبا[242]. ففي عام 2007، كانت إستونيا هدفاً لحرمان من الخدمة السيبرانية، أدى إلى شلل خدمات إدارتها وانقطاع المعاملات من بنوكها عبر الإنترنت. وقع هذا الهجوم على خلفية توتر مع روسيا حول مشروع نقل نصب تذكاري (الجندي البرونزي)، تكريمًا للجنود السوفييت. أما في عام

---

[240]-حنين جميل أبو حسين، الإطار القانوني لخدمات الأمن السيبراني (دراسة مقارنة) ، رسالة لنيل شهادة الماستر في القانون الخاص، جامعة الشرق الأوسط، كلية الحقوق، الأردن، السنة الجامعية 2020-2021، ص.49.

[241]-برج أسمهان، الهجمات السيبرانية و أثرها على العلاقات السياسية الدولية-العلاقات الجزائرية المغربية نموذجا، مرجع سابق، ص. 53.

[242]-دانيال فونتير، الاستراتيجية السيبرانية، ترجمة أيمن منير، سلسلة عالم المعرفة، المجلس الوطني للثقافة والفنون والآداب، الكويت، عدد 473، 01.06.2019، ص ص. 69.

2008، في جورجيا، فتم اختراق شبكات الكمبيوتر وظهرت الكتابة على جدران المواقع الحكومية، عندما كانت البلاد في صراع مع روسيا[243].

وهكذا، منذ ذلك الهجومين تم اعتبار الفضاء الإلكتروني كمسرح للعمليات، يضاهي حدة العمليات الجوية والبرية والبحرية. لا يُنظر إلى الصراع في هذه البيئة على أنه مواجهة في التقنيات، ولكن كـ "استخدام الوسائل الرقمية لغرض التحكم في إرادة الخصم"، والانضمام إلى الصيغة الشهيرة للمنظر الألماني "كارل فون كلاوزفيتز "الحرب ليست سوى امتدادا للسياسة بوسائل أخرى"[244].

بدأ هذا الفضاء السيبراني يعرف استراتيجيات متطورة، وانقسمت تلك الاستراتيجيات إلى وطنية، إقليمية، دولية، دفاعية ومتخصصة في مكافحة الجريمة السيبرانية. وارتبطت الاستراتيجية السيبرانية بالاعتداء والقوة والحرب السيبرانية والصراع السيبراني، فضلا عن أنها تعد وقائية ونشطة واستباقية وعمومية وشاملة، وقد تعمل على تحديد وسائل، أو طرق الكشف عن الهجمات، أو الردع، أو الرد على الهجمات السيبرانية. ويبدو أنها تنطوي على إعادة تعريف للاستراتيجية التقليدية من أجل التكيف مع خصوصيات الفضاء السيبراني. هذا الفضاء أضحى نقطة الانطلاق لصياغة الاستراتيجيات السيبرانية المبنية على انعدام السيادة الدولية فيه، بحيث لازال المهاجمون السيبرانيون يتمتعون بمميزات تفوق إمكانات المدافعين؛ لا من حيث المفاجأة ولا من حيث القدرة على إخفاء الآثار[245]. وحتى تتضح الرؤية حول استراتيجيتي البلدين في المجال السيبراني، استحضرت الدراسة استراتيجيتي البلدين على المستوى الوطني(الفرع الأول)، وعلى المستوى الإقليمي والدولي(الفرع الثاني).

### الفرع الأول: على المستوى الوطني

توقعت قلة من الدول التحدي الاستراتيجي الذي يمكن أن يمثله التوسع السريع في نظم المعلومات والاتصالات والربط بينها على المدى الطويل. قلة فقط، مثل روسيا والصين، أو الولايات المتحدة، المتواجدة في طليعة التقدم التكنولوجي، والتي بدأت التفكير الاستراتيجي

---

[243]- Mourad El Manir, L'Afrique face aux défis protéiformes du cyberespace, Op.cit, p.9.

[244]-دانيال فونتير، الاستراتيجية السيبرانية، مرجع سابق، ص.69-71.

[245]-المرجع نفسه.

في وقت مبكر جدًا[246]. لكن جل الدول راحت تعود بقوة في الفضاء السيبراني باسم الدفاع عن سلطاتها السيادية. أولاً، من المرجح أن تؤثر صعوبة وقف الهجمات السيبرانية على قدرتها على توفير الأمن القومي والدفاع عن الوطن. وتتعلق الشواغل بشكل خاص بحماية ما يسمى بالبنى التحتية الحيوية، والتي قد يؤدي تعطيلها أو تخريبها إلى تعريض السكان المدنيين للخطر. يتساءل أوليفييه كيمبف "Olivier Kempf"عن مفهوم الإرهاب السيبراني واستراتيجية الدول لوقفه، كما يحلل رودريغو نيتو غوميز "Rodrigo Nieto Gomez " الدور الأمريكي الذي يمكن أن يؤديه في السياسات الأمنية السيبرانية[247].

تقود القضايا الأمنية الحكومات إلى مراقبة ما يحدث في الفضاء السيبراني بفاعلية، مع مخاطر التجاوزات وانتهاك الحريات الفردية التي كشفت عنها قضية "إدوارد سنودن". بالنسبة للدول الاستبدادية، تعد مراقبة الفضاء السيبراني والسيطرة عليه أمرًا ضروريًا لحماية نظامها لأن التهديد الرئيسي من المحتمل أن يأتي من الداخل. يمكن أن يؤدي التدفق المتزايد للمعلومات إلى إضعاف الأنظمة الاستبدادية، لكن الشبكات هي أيضًا أدوات مهمة للكشف عن المنشقين أو أو رصدهم أو تحديد الأشخاص السيئين المحتملين للنظام[248].

هذا السرد التقديمي يقودنا إلى طرح سؤالين اثنين مرتبطين بالمغرب والجزائر ؛ فإذا تأكد أنه بالنسبة لدول شمال إفريقيا، هي الأخرى تسعى جاهدة وتصارع الزمن لإثبات الذات في الفضاء السيبراني، محليا ودوليا. فماهي الاستراتيجيات الأمنية المعتمدة من طرف هذين البلدين على المستوى الوطني؟ ومن هي الأقوى فيهما من حيث الفعالية؟

## الفقرة الأولى: استراتيجيتا البلدين الوطنيتين

إن تزايد التهديدات والتحديات المرتبطة بالمجال السيبراني لم يستثن أي دولة تعتمد في أنشطتها الاقتصادية والاجتماعية والثقافية على شبكة الأنترنت[249]، والمغرب هو الآخر

---

[246] -Frédérick Douzet, La géopolitique pour comprendre le cyberespace, Op.cit, pp. 9-10.
[247]-Ibid.
[248]-Ibid.
[249]-عبد الواحد البيدري، استراتيجية الأمن السيبراني: دراسة حالة المغرب، مجلة الدراسات الاستراتيجية والعسكرية، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين، ط1، 2021، ص ص،108-109.

لم يسلم من استخدام حيل بعض الدول الرقمية للإضرار بفضائه السيبراني. لهذا السبب، يتبين أن المغرب غير محصن ضد التهديدات السيبرانية، وقد تعرض لها عدة مرات[250].

وفي هذا السياق، ومراعاة للتحديات والمخاطر المرتبطة بالفضاء السيبراني، وجد المغرب نفسه ملزما بوضع استراتيجية وطنية لأمنه السيبراني، منذ سنة 2012[251]. ومن بين المحاور الأساسية التي جاءت بها تلك الاستراتيجية، نجد تقييم المخاطر بالنسبة لنظم المعلومات الخاصة بالإدارات والمؤسسات الحكومية والبنيات التحتية ذات الأهمية. وقد تم تحديد برنامجين أساسين لتنفيذ هذا المحور وهما؛ وضع خطط لتقييم المخاطر والتهديدات، و وضع الأدوات الضرورية للمساعدة في اتخاذ القرار[252].

إن خطة الاستجابة للحوادث السيبرانية تستلزم مراقبة تدفقات المعلومات المدخلة والمخرجة. فمن المهم تحديد الحادث في أقرب وقت ممكن من خلال إضفاء الطابع الرسمي على التعامل مع الحوادث انطلاقا من الكشف إلى المعالجة[253]. ولتحقيق ذلك، قرر المغرب إنشاء اللجنة الاستراتيجية لأمن نظم المعلومات (CSSSI) (21 سبتمبر 2011) والمديرية العامة لأمن نظم المعلومات (DGSSI)[254].

ومن أجل مكافحة جرائم الإنترنت بشكل أفضل، أتاح المغرب داخل مؤسساته الأكاديمية العديد من الدورات التدريبية الهندسية لضمان تدريب المسؤولين عن أمن أنظمة معلومات الأمن السيبراني. ومن أمثلة هذه التدريبات، قام المركز المغربي للبحوث والابتكار البوليتكنيك (CMRPI) بتنفيذ حملة توعية ذات صلة بالسيبرانية، على مدى 4 سنوات(من 2014-2017) تسمى الحملة الوطنية لمحاربة جرائم الإنترنت[255].

من ناحية أخرى، وبالإضافة للفاعلين الوطنيين، انفتح قطاع الأمن السيبراني المغربي على شركات أجنبية، استثمرت في الدفاع السيبراني في المغرب. على سبيل المثال، شاركت

---

[250]-M.MOUHIR& Mme.MOKHTAR, Stratégie de Cyber défense marocaine: du public au privé, enjeux et perspectives, **Ecole de Guerre Economique**, 08.02.2023, lien de l'article : http://bitly.ws/FIqM, date visite : 27.05.2023

[251]-عبد الواحد البيدري، استراتيجية الأمن السيبراني: دراسة حالة المغرب، مرجع سابق، ص ص،108-109.

[252]-المرجع نفسه.

[253]-المرجع نفسه.

[254]-Administration de la Défense Nationale, stratégie nationale en matière de cybersecurité, lien de l'article : http://bitly.ws/zwwi, date visite : 29.01.2023, p.7.

[255]-M.MOUHIR& Mme.MOKHTAR, Ibid.

كوريا الجنوبية في تطوير "maCert" في عام 2011. و في عام 2013، وقعت المديرية العامة للجرائم الاقتصادية والاجتماعية و"ANSSI " اتفاقية تعاون، بالإضافة إلى تصديق الممثلين المغاربة في عام 2018 على اتفاقية بودابست بشأن الجرائم السيبرانية. خلال العام نفسه، تم دمج المملكة في مشروع تعاون "سايبر ساوث" "Cybersouth" مع الاتحاد الأوروبي ودول البحر الأبيض المتوسط الأخرى. أخيرًا، في يوليوز 2021، وقع المدير العام للمديرية الإلكترونية الإسرائيلية ونظيره المغربي "الجنرال مصطفى ربيع" اتفاقية بشأن التعاون العملياتي والبحث والتطوير وتبادل المعلومات[256].

أما بالنسبة للفاعلين الخاصين، نجد هناك: الشركات الأمريكية مثل؛(Symantec، Fortinet، Palo Alto Networks). الفاعلون الأوروبيون مثل؛(Bitdefender، Kaspersky). الشركات الفرنسية؛(Orange-Morocco و Orange-Cyberdéfense و Thales و Devoteam و Atos). وهناك أيضًا فاعلون متوسطو الحجم في السوق المغربي، مثل:"cure6": الناشر الفرنسي لحلول مكافحة "DDoS"[257] الموجودة في السوق، والتي مكنت الشركات والمشغلين المغاربة من إنشاء مساحات رقمية موثوق بها. وكذلك"Systancia": خبير فرنسي في المحاكاة الافتراضية والأمن السيبراني والثقة الرقمية. لاننسى الشركة القبرصية [258]"Secmentis" التي تخدم المغرب على أساس

[256]-M.MOUHIR& Mme.MOKHTAR, Stratégie de Cyber défense marocaine: du public au privé, enjeux et perspectives, Op.cit.

[257]-**هجوم DDoS**، أو هجوم الحرمان الموزع للخدمة، هو نوع من الهجمات الإلكترونية التي تحاول جعل موقع ويب أو مصدر شبكة غير متاح عن طريق إغراقه بحركة مرور ضارة لمنعه من العمل.

في هجوم رفض الخدمة الموزع (DDoS)، يغمر المهاجم هدفه بحركة مرور الإنترنت غير المرغوب فيها، بحيث لا يمكن لحركة المرور العادية الوصول إلى وجهتها.

من منظور عام، يعتبر هجوم DDoS أو DoS بمثابة ازدحام مروري غير متوقع ناتج عن مئات الطلبات الوهمية لمرافقي المركبات. تبدو الطلبات مشروعة لخدمات مشاركة الركوب، لذا فهم يرسلون السائقين لنقل الركاب، الأمر الذي يسد حتمًا شوارع المدينة. ثم يتم إعاقة حركة المرور العادية المشروعة ولا يمكن للأشخاص الوصول إلى وجهتهم.

[258]-**Secmentis**: هي شركة استشارية للأمن السيبراني متخصصة في اختبار الاختراق وذكاء التهديدات والدفاع الاستباقي للبنية التحتية لتكنولوجيا المعلومات بالكامل (الخارجية أو الداخلية)، بما يتماشى تمامًا مع المعايير المعترف بها في الصناعة.

تحمي Secmentis بشكل استباقي علامتك التجارية وأسرارها التجارية من خلال اختبار الاختراق وعمليات الفريق الأحمر، والتي تهدف إلى محاكاة هجمات القرصنة الحقيقية والمصرح بها ضد البنية التحتية لتكنولوجيا المعلومات التي تواجه الجمهور (مثل مواقع الويب العامة أو تطبيقات الويب المصممة خصيصًا، أو البوابات أو الأجهزة الداخلية، وما إلى ذلك)، بهدف الكشف عن نقاط الضعف لفهم مدى الضرر الذي قد يتسبب فيه مهاجم ضار حقيقي في عملك.

(SECMENTIS LTD, **U.S. Embassy In Cyprus,** 10.06.2022, link: http://bitly.ws/GXSi, seen on: 04.06.2023).

مخصص من مقرها الرئيسي في ليماسول. وهي متخصصة في اختبار الاختراق وذكاء التهديدات والدفاع الاستباقي للبنية التحتية لتكنولوجيا المعلومات[259].

يهدف المغرب، من خلال جغرافيته الاستراتيجية المذكورة أعلاه، إلى أن يصبح المركز الرقمي الأول في إفريقيا الناطقة بالفرنسية والثاني في القارة[260]. وحتى تتحقق تلك الغاية المنشودة، حددت الاستراتيجية كيانات الحكومة الرئيسية المشاركة في الأمن السيبراني والمتمثلة في DGSSI. وأبرز أولوياتها الاستراتيجية تتمثل في؛ تقييم المخاطر والحماية والدفاع على نظم معلومات الوكالات الحكومية والمنظمات العامة والبنى التحتية ذات الأهمية الحيوية، وتقوية أسس أمن نظم المعلومات (الإطار القانوني، التوعية، التدريب، تفعيل الاستراتيجية)[261] .

لكن، وعلى الرغم من كل الجهود المبذولة من طرف المغرب في مكافحة الجرائم السيبرانية وإنشاء الثقة الرقمية، إلا أنها تظل جهودا غير كافية. فقد لوحظ أن القطاع الخاص والنسيج الاقتصادي المغربي بشكل عام، وخاصة الشركات الصغيرة والمتوسطة الحجم، لا يزالان متخلفين نسبيًا من حيث استراتيجية الأمن السيبراني[262].

**أما على المستوى الجزائري**، فرغم تخلفها في هذا المجال، تشير بعض الدراسات الجزائرية أن الجزائر اهتمت بأمنها السيبراني، وعليه توجهت هي الأخرى إلى رسم استراتيجيتها مركزة على النقاط التالية؛ تحديد المخاطر، اتخاذ التدابير اللازمة، تحديد الهيئات المكلفة بإدارة الأمن، تحديد الهيئات المكلفة بالتنسيق، تحديد الهيئة المكلفة بالجانب التقني للبحث عن الثغرات وتوجيه التحقيق[263].

---

[259]-M.MOUHIR& Mme.MOKHTAR, Stratégie de Cyber défense marocaine: du public au privé, enjeux et perspectives, Op.cit.

[260]-Ibid.

[261]-Melissa Hathaway and Francesca Spidalieri, kingdom of morocco cyber readiness at a glance, **Potomac Institute for Policy Studies**, December 2018, link of book: http://bitly.ws/zC8E, seen on: 31.01.2023, pp, 10-13..

[262]-M.MOUHIR& Mme.MOKHTAR, Ibid.

[263]-جمال بوازدية، الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية "التحديات والآفاق المستقبلية"، **مجلة العلوم القانونية والسياسية**، 03.02.2019، رابط المقال: http://bitly.ws/zEBs، تاريخ الدخول:02.01.2023. ص ص،1277-1278.

ولضمان التنفيذ الفعلي لمختلف التدابير الهادفة لتحقيق الأمن السيبراني، أوكلت السلطات الجزائرية هذه المهمة إلى هيئات متخصصة ضمن أسلاك الأمن، من بين هذه الهيئات، نذكر ما يلي[264]:

1-المصلحة المركزية لمكافحة الجريمة المعلوماتية: (SCLC) التابعة لمديرية الأمن الوطني؛

2- مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية (CPLCIC): التابعة للقيادة العامة للدرك الجزائري، لا تختلف كثيرا عن نظيرتها التابعة للأمن الجزائري؛

3- المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الجزائري (INCC).

حاولت الجزائر تبني منظومة دفاعية سيبرانية على مستوى قواتها المسلحة، تمثلت تلك المنظومة في:

-الجيش الوطني الشعبي: مصلحة الدفاع السيبراني و مر اقبة أمن الأنظمة[265]؛

-مركز الوقاية من جرائم الإعلام الآلي للدرك الجزائي: أنشئ في سنة 2008[266]؛

-المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الجزائري: مؤسسة عمومية ذات طابع إداري تحت الوصاية المباشرة لوزير الدفاع الجزائري، دخل حيز الخدمة ابتداء من فاتح يناير2009 [267]؛

-المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الجزائري[268]؛

-الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[269].

---

[264]- جمال بوازدية، الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية "التحديات والآفاق المستقبلية"، مرجع سابق، ص ص،1277-1278.

[265]-يوسف بوغرارة، الأمن السيبراني :الاستراتيجية الجزائرية للأمن و الدفاع في الفضاء السيبيري، مجلة الدراسات الأفريقية وحوض النيل، المركز الديمقراطي العربي، برلين، العدد 03، 2018، ص ص،114-115.

[266]-إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مرجع سابق، صص.13-15.

[267]-المرجع نفسه.

[268]-المرجع نفسه.

[269]-المرجع نفسه.

### الفقرة الثانية: مقارنة مدى فعاليتهما

لدراسة درجة فعالية الاستراتيجيتين المغربية والجزائرية في الدفاع السيبراني على المستوى الوطني، لابد من الاعتماد على دراسات أكاديمية تقارن بينهما، وترجح كفة احديهما على الأخرى، أو تجعلهما متساويتين من ناحية الدفاع السيبراني.

والطريقة المثلى لمقارنتهما هي الاعتماد على مؤشر الأمن السيبراني العالمي(Global Cybersecurity Index)، الذي يرمز له اختصارا بالرمز (GCI). تم إطلاق مبادرة GCI لأول مرة في عام 2015، وتتبعت كيفية إدارة البلدان لشبكاتها على الإنترنت وتأمين معلومات مستخدمي الإنترنت. أبانت المبادرة أن جميع البلدان تتأثر إلى حد ما بالفجوة الرقمية، لهذا يجب أن يولى الأمن السيبراني أولوية قصوى، كما جاء في التقرير[270].

صنف هذا المؤشر، سنة 2020، المغرب في المرتبة 50 من أصل 181 دولة حول العالم. يهتم التقرير في المقام الأول بتقدم البلدان في التزاماتها بالاستجابة لتحديات الأمن السيبراني، ويصنف التقرير البلدان بناءً على مجموعة متنوعة من المعايير المتعلقة بالأمن السيبراني. وفقًا لـ GCI، "يرسم الفهرس 82 سؤالًا حول التزامات الدول الأعضاء بالأمن السيبراني عبر خمس ركائز: التدابير القانونية، التدابير التقنية، التدابير التنظيمية، تدابير تنمية القدرات، وتدابير التعاون"[271].

حصل المغرب على درجة 18.40 في التدابير القانونية، و 17.94 في التدابير الفنية، و 12.37 في التدابير التنظيمية، و 15.24 في تنمية القدرات، و 18.46 في تدابير التعاون[272]. بالإضافة إلى ذلك، تسببت COVID-19 في المغرب زيادة حركة المرور على الإنترنت بنسبة 30٪. حيث عمل مستخدمو الإنترنت من المنزل عبر مواقع مؤتمرات الفيديو عبر الإنترنت، وبالتالي، "هناك إدراك متزايد بمخاطر الأمن السيبراني"[273].

---

[270]-Michael Sauers, Global Cyber security Index 2020 Ranks Morocco at 50th Globally, **Morocco World News**, 05.07.2021, link: http://bitly.ws/zHWZ, seen on: 02.02.2023.
[271]-Ibid.
[272]-Indice mondial de cybersécurité, **Union internationale des télécommunications Secteur du développement**, 2020, lien de l'article: http://bitly.ws/HdnQ, date visite: 05.06.2023, p.93.
[273]-Michael Sauers, Ibid.

فيما يتعلق بالتصنيفات الإقليمية، احتل المغرب المرتبة الثامنة في منطقة الشرق الأوسط وشمال إفريقيا والخامسة في إفريقيا. المتصدر العالمي هو الولايات المتحدة بمجموع 100 درجة تليها المملكة المتحدة والمملكة العربية السعودية متعادلان بـ 99.54[274].

كان لتقرير عام 2020 "مستوى قياسي من مشاركة الدول الأعضاء، من 105 ردود في تكرار 2013-2014 ، إلى 181 استبيانًا تم إرجاعها في عام 2020"[275].

وحسب نفس مؤشر الأمن، تنزوي الجزائر في المرتبة الـ104 عالميا ضمن 181 دولة، برصيد 33.95؛ حيث حصلت على 07،25 في تدابير التعاون، و10،07 في تعزيز القدرات، و44،01 في التدابير التنظيمية، و73،02 في التدابير الفنية، و12،46 في التدابيرالقانونية[276]. كما احتلت المركز الحادي عشر 11 في منطقة الشرق الأوسط وشمال إفريقيا، فيما احتلت العربية السعودية المرتبة الثانية عالميا بمجموع 99،54، و الأولى عربيا متفوقة على دول عظمى أمثال اليابان التي نالت المركز السابع برصيد 97.82 درجة، كندا «الـ8، بـ 97.67 درجة»، فرنسا «الـ9، بـ 97.6 درجة»، والهند «الـ10، بـ 97.5 درجة»[277].

تبين تلك المقارنة مدى تقدم المغرب على الجزائر في الترتيب العالمي، المتعلق بالدفاع السيبراني. هذا الأمر، مع أمور أخرى لا يسعنا المجال لسردها، خلق عند الجزائر حقدا على المغرب وجعلها تتهجم عليه، مرارا وتكرارا، بمجموعة من الاتهامات المتعلقة بالهجمات السيبرانية.

### الفرع الثاني: على المستوى الإقليمي والدولي

على المستوى الإقليمي، تكثر المبادرات لمواجهة التهديدات والتحديات المتزايدة للجرائم السيبرانية في القارة. في وقت مبكر من عام 2019، أطلقت مفوضية الجماعة الاقتصادية لدول غرب إفريقيا (ECOWAS)، مشروع استجابة غرب إفريقيا للأمن

[274]-Michael Sauers, Global Cyber security Index 2020 Ranks Morocco at 50th Globally, Op.cit.
[275]-Soufiane Khabbachi, Maroc-Algérie : la discorde s'invite sur le front numérique, Op.cit.
[276]-Indice mondial de cybersécurité, Op.cit, p.88.
[277]-Ibid, p.41.

السيبراني ومكافحة الجريمة السيبرانية، وفي الوقت نفسه، يعمل الاتحاد الأفريقي (AU) على تطوير وتنفيذ استراتيجيته الخاصة للأمن السيبراني[278].

غير أنه إذا كانت هذه الجهود الإقليمية لتطوير وتنفيذ استراتيجية سيبرانية جديرة بالاهتمام، إلا أنها لن تكون فعالة إلا إذا حفزت التنسيق والتعاون على نطاق واسع على المستوى الوطني، لمكافحة الجريمة السيبرانية المنظمة العابرة للحدود والتطرف العنيف والأنشطة الخبيثة التي ترعاها الدول في الفضاء السيبراني[279].

لسوء الحظ، كان التقدم في تطوير وتنفيذ استراتيجية الأمن السيبراني على المستوى الوطني في أفريقيا محدودًا. وفقًا لأحدث البيانات التي جمعها الاتحاد الدولي للاتصالات (ITU) التابع للأمم المتحدة، طورت حوالي ثلث (17) دول أفريقية البالغ عددها 54 دولة استراتيجية وطنية للأمن السيبراني، وهو ما يمثل أقل من نصف المتوسط العالمي. لهذا السبب المرتبط بغياب الاستراتيجيات الوطنية، غالبًا ما تجد الحكومات نفسها غير قادرة على تطوير استراتيجيات إقليمية ودولية[280].

وحتى تتضح معالم البنية التحتية للدفاع السيبراني في المغرب والجزائر على المستويين الإقليمي والدولي، قسم هذا الفرع إلى مستويين؛ مستوى ارتبط بالساحة الإقليمية، ومستوى آخر امتد إلى الساحة الدولية.

### الفقرة الأولى :على المستوى الإقليمي

لا تعتبر الدبلوماسية المغربية الأمن السيبراني على رأس قائمة السياسة الخارجية ولم تعط الأولوية لهذا المجال ضمن وزارة الخارجية والتعاون إلا منذ عام 2003. ومع ذلك، يعتبر المغرب تكنولوجيا المعلومات والاتصالات والأمن السيبراني عنصرين مهمين من أمنه القومي والاقتصادي، بما في ذلك في التجارة الدولية والمفاوضات التجارية، ويفترض دورا أكثر بروزًا في الترويج الإقليمي للتعاون والتوعية في مجال الأمن السيبراني[281].

---

[278]-Abdul-Hakeem Ajijola et Nate D.F. Allen, Leçons d'Afrique en matière de cyber-stratégie, **Centre d'Etudes Stratégiques de l'Afrique**, 18.03.2022, lien de l'article : http://bitly.ws/DhIj, date visite, 21.04.2023.

[279]-Ibid.

[280]-Ibid.

[281]-Melissa Hathaway and Francesca Spidalieri, kingdom of morocco cyber readiness at a glance, Op.cit, pp. 22-23.

وكجزء من هذه الجهود، يقوم المغرب بانتظام، باستضافة الأحداث المتعلقة بالأمن السيبراني للبنك الدولي والاتحاد الدولي للاتصالات وحلف الناتو للعلوم؛ برنامج السلام والأمن " Peace and Security Program". بالإضافة إلى ذلك، توفر وزارة الخارجية المغربية - الأكاديمية الدبلوماسية- التدريب للبلدان الشريكة بما في ذلك بنين وجمهورية أفريقيا الوسطى وتشاد والجابون وغينيا ومدغشقر[282].

كما شارك المغرب في عدد من الحوارات رفيعة المستوى مع الدول الأوروبية، الولايات المتحدة و أعضاء مجلس التعاون الخليجي، في القضايا الأمنية، عمليات مكافحة الإرهاب واستخدام الفضاء السيبراني من قبل الإرهابيين وغيرهم من المجموعات الإجرامية. قيمته الاستراتيجية، ليس فقط من أجل موقعه بين أوروبا وأفريقيا، ولكن أيضًا لأهميته داخل منطقة المغرب العربي وعلاقاته بالعالم العربي الأكبر، تجعله شريكا أمنيا رئيسيا في المنطقة[283].

بالإضافة إلى ما سبق، نسجل تعاون الوكالات المغربية ونظيراتها الأوروبية، خاصة مع إسبانيا وفرنسا، بانتظام وتبادلهما للمعلومات وأفضلها الممارسات المتعلقة بقضايا الأمن، بما في ذلك الأمن السيبراني، ويعتبرون المغرب حليفا استراتيجيا موثوقا به في المنطقة[284]. فالحلف شمال الأطلسي، مثلا، أصبح يعتبر المغرب شريكا استراتيجيا لا محيد عنه في الحوار المتوسطي، لمواجهة التحديات التي تهدد جنوب المتوسط. يأتي تطور العلاقة بين المملكة المغربية والحلف الأطلسي، تتمة للعلاقات المغربية –الأمريكية المتميزة، فالولايات المتحدة منحت، منذ سنة 2004، المغرب صفة حليف استراتيجي خارج الحلف الاطلسي[285].

وقد عرفت لقاءات الجانبين تقدما ملحوظا، حيث نظم الحلف بتعاون مع وزارة الشؤون الخارجية والتعاون في 25 يناير 2019، ندوة تحت عنوان "الحوار المتوسطي والمفهوم الاستراتيجي الجديد لحلف الشمال الأطلسي"، في هذه الندوة تم التأكيد على الدور

---

[282]-Melissa Hathaway and Francesca Spidalieri, kingdom of morocco cyber readiness at a glance, Op.cit, pp. 22-23.

[283]-Ibid.

[284]-Ibid.

[285]-سمير قط، خصوصية الشراكة الأطلسية – المغاربية في إطار الحوار المتوسطي للحلف ، **أكاديميا العربية**، رابط المقال : https://bitly.ws/wph2، تاريخ الدخول: 10.12.2022.

الفعال والأساسي للمغرب في معالجة مختلف القضايا المتعلقة بالإرهاب والهجرة تجاه الغرب، والهجمات السيبرانية[286].

تؤكد استراتيجية المغرب الرقمية 2020 على موقع المغرب الاستراتيجي كمحور رقمي إقليمي وبوابة لأفريقيا. لكن يجب على المغرب استخدام الموقع الرئيسي للبلد لتعزيز التدفق الحر للسلع وخدمات البيانات ورأس المال عبر الحدود. لا تتعلق الدبلوماسية السيبرانية فقط بقواعد الاشتباك وتقييد السلوكيات، بل ترتبط أيضًا بتعزيز التجارة من خلال التدفق الحر للمعلومات. تحقيق التوازن بين هدفي الازدهار الاقتصادي والأمن القومي يتطلب هيئة دبلوماسية متطورة والتزاما بقيادة المنطقة لتحقيق أهداف رؤية المغرب الرقمية[287].

من جهتها سعت الجزائر هي الأخرى لتوقيع العديد من الاتفاقيات الثنائية والمتعددة الأطراف مع الدول العربية في إطار الاتفاقية العربية لمكافحة الإرهاب لسنة 1998، والاتفاقية العالمية لمكافحة الجريمة المنظمة العابرة للحدود لسنة 2000. وجسدت شراكتها الأورو-متوسطية مع الدول الأعضاء في الوحدة الأوروبية عبر توقيعها، بتاريخ 2002.04.22، شراكة تعاون في المجال الأمني والقضائي لمحاربة مختلف الجرائم. كما أبرمت اتفاقا مع فرنسا، بتاريخ2003.10.25، تضمن التعاون في مجال الأمن ومكافحة الإجرام المنظم[288]. غير أن ذلك الاهتمام الجزائري الإقليمي في المجال السيبراني لم يرق بعد إلى المبتغى. وما يؤكد على ذلك، أي على عدم نضج الجارة الجزائر بعد في الفضاء السيبراني، الاتهامات المتكررة لجارها المغرب؛ اتهامات لا تشجع على خلق مبادرة دفاعية سيبرانية إقليمية في منطقة شمال إفريقيا، بل تزيد في تأجيج نار العداوة بين الجارين الاثنين.

### الفقرة الثانية: على المستوى الدولي

أدى التطور الكبير في وسائل المواصلات بصفة عامة والشبكة المعلوماتية بصفة خاصة إلى انتقال المجرمين من بلد إلى آخر. وقد أدرك المجتمع الدولي أنه بات من

---

[286]-أمين النية، الأمن في السياسة الخارجية المغربية، **أكاديميا العربية**، 01.01.2020، رابط المقال: https://bitly.ws/wp3z، تاريخ الدخول: 17.11.2022.

[287]-Melissa Hathaway and Francesca Spidalieri, kingdom of morocco cyber readiness at a glance, Op.cit, pp. 22-23.

[288]-جمال بوازدية، الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية "التحديات والآفاق المستقبلية"، مرجع سابق، ص.1286.

المستحيل على أي دولة أن تقوم بالقضاء على الجرائم العابرة للحدود، ذلك أن الإجراءات العامة لأجهزة الشرطة في كل دولة لا تجعل لجهازها الأمني تعقب المجرمين ومتابعتهم إذا ما عبروا حدود الدولة[289]. وعليه، وحتى يسهل لكل دولة الاستمرار والعيش مع غيرها من الدول، لابد من وجود تعاون دولي على المستوى الإجرائي الجنائي، بحيث يسمح بالاتصال المباشر بين أجهزة الشرطة في الدول المختلفة، وذلك بإنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم السيبرانية[290].

فالحاجة إلى تعاون أجهزة الشرطة فيما بين الدول وتنسيق العمل فيما بينها لمطاردة المجرمين باتت واجبة أكثر من أي وقت مضى[291] . أضف إلى هذا، حتمية تبادل المعلومات المتعلقة بالجريمة السيبرانية والمجرمين بأقصى سرعة ممكنة، مع تعقب المجرمين الفارين من وجه العدالة[292]. وفي هذا الصدد، نسجل سعي المغرب الدائم للتعاون مع غيرها والانفتاح على التجارب الدولية الرائدة في مجال الدفاع السيبراني.

فالمملكة المغربية لا تكتفي بتأدية دور حاسم في الحفاظ على الأمن والاستقرار في منطقة شمال إفريقيا فقط، بل تعمل بشكل وثيق مع الدول الأوروبية والولايات المتحدة وأعضاء مجلس التعاون الخليجي في القضايا الأمنية وعمليات مكافحة الإرهاب. المعضلات الأمنية التي تواجهها هذه الدول وفيرة. كان هناك نفوذ داعشي - وإن كان ضعيفًا - (واحد من المنظمات الإرهابية التابعة لها تنظيم الدولة الإسلامية) ومنظمات إرهابية آخرى. كان هناك إرهابيون من شمال أفريقيا نفذوا هجمات داخل أوروبا. ابتليت المنطقة باقتصاد ليبي منهار وميليشيات محلية متنافسة على السلطة[293].

لذلك، فالولايات المتحدة والدول الأوروبية ودول مجلس التعاون الخليجي لديها مصلحة قوية في فهم تهديدات الأمن التي تنبثق من شمال أفريقيا، وفي العمل مع دول شمال

---

[289]-عبد الواحد البيدري، استراتيجية الأمن السيبراني: دراسة حالة المغرب، مرجع سابق، ص.105.

[290]-محمد علي محمد التوني، استراتيجية مكافحة الهجمات السيبرانية، دار الفكر الجامعي، الإسكندرية، ط1، 2023، ص ص، 111-112.

[291]-عبد الواحد البيدري، المرجع نفسه، ص.105.

[292]-محمد علي محمد التوني، المرجع نفسه، ص.113.

[293]-Melissa Hathaway and Francesca Spidalieri, Kingdom of Morocco cyber readiness at a glance, Op.cit, p.23.

إفريقيا بصفة عامة، وعلى وجه الخصوص، مع المغرب الذي يعتبر واحدا من الشركاء الرئيسيين لأوروبا والولايات المتحدة في المنطقة في المجال الأمني.

يعمل المغرب أيضًا مع الناتو كجزء من ذلك "الحوار المتوسطي" لاستكشاف التعاون في مجال الدفاع السيبراني، ولا سيما من خلال تبادل الخبرات والتدريب، ويشارك في عدة تمارين مع الشركاء الدوليين، بما في ذلك التمرين البحري المتوسطي المسمى "فينيكس". تم تصميم هذا التمرين لتحسين التعاون الإقليمي، وزيادة الوعي بالمجال البحري، وممارسات تبادل المعلومات، والقدرات التشغيلية من أجل بدل الجهود لتعزيز السلامة و الأمن في البحر الأبيض المتوسط. علاوة على ذلك، يستضيف المغرب تمرينا عسكريا سنويا مشتركا "الأسد الأفريقي" منذ 2005. وفي عام 2018 شاركت فيه15 دولة، بما في ذلك بوركينا فاسو، كندا، تشاد، مصر، فرنسا، ألمانيا، إيطاليا، مالي، موريتانيا، السنغال، إسبانيا، تونس، المملكة المتحدة والولايات المتحدة. كان هذا التمرين مصمما لتحسين إمكانية التشغيل البيني والتفاهم المتبادل بين التكتيكات والتقنيات والإجراءات، وما إلى ذلك من خطط لدمج حقن الأمن السيبراني والتخطيط في التكرارات المستقبلية[294].

في نوفمبر 2017، أصبح المغرب أول دولة في شمال إفريقيا تطلق قمرًا صناعيًا للمراقبة عالي الدقة (سمي على اسم الملك محمد السادس) وقادرا على إعطاء صور متعددة الأغراض. وفي نوفمبر 2018، أطلق المغرب قمرا صناعيا ثانيا (اسمه محمد السادس ب) الذي يهدف إلى تزويد المغرب بقدرة أقوى على تجميع المخابرات، ومراقبة حدودها، وخريطة الأرض وأنشطة المسح والوقاية وإدارة الكوارث الطبيعية ورصد تغيرات البيئة والتصحر[295].

في يوليوز من سنة 2021، وفي إطار تطبيع العلاقات مع إسرائيل، وقع المغرب اتفاقية تعاون في مجال الأمن السيبراني مع تل أبيب. قد تسمح هذه الاتفاقية له في النهاية

[294]-Zoltán Sipos, Cybersecurity in Algeria, Op.cit, p.71.
[295]-Melissa Hathaway and Francesca Spidalieri, Kingdom of Morocco cyber readiness at a glance, Op.cit, pp.23-24.

بالوصول إلى المعرفة الأمريكية، لأن الولايات المتحدة والدولة اليهودية تتعاونان بشكل وثيق في هذا القطاع[296].

**أما الجزائر**، فالتوجهات العالمية الجديدة تفرض تحقيق خطة التنمية لعام 2030. وأهدافها، التي تعد الجزائر من بينها، عدة التزامات منها تنفيذ الخطط العالمية التنموية، ومجابهةّ القمة العالمية لمجتمع المعلومات. على عاتق الدول العربية التحديات التي تحول دون تنفيذها. وذلك من خلال إبداء الالتزام السياسي اللازم، وتحديث الاستراتيجيات، لا سيما تكنولوجيا المعلومات والاتصالات، بما يتلاءم مع الأهداف التنموية الجديدة ووفقا لأولويات الدول العربية بما فيهم الجزائر. بالإضافة إلى الجريمة السيبرانية، يجب أن تهتم الجزائر بالإرهاب السيبراني والحرب السيبرانية، ويجب أن تضمن استراتيجية حقيقية شاملة ل "الدفاع السيبراني"، كما أنه من التحديات المستقبلية ستشمل على نحو متزايد صراعات في الفضاء السيبراني في جميع الأبعاد، وبما أن "الفضاء السيبراني" هو مسرح جديد للعمليات في القرن الحادي والعشرين، فإن القوات المسلحة الحديثة لا يمكنها ببساطة أن تعمل بفعالية دون وجود شبكة اتصالات ومعلومات مؤثرة بها ومرنة، لذلك من المهم أن تتمتع الدولة الجزائرية بقدرة على التحكم في الفضاء السيبراني ويعد إطلاق الجزائر أول قمر صناعي للاتصالات بالتعاون مع الصين خطوة مهمة نحو تأمين مؤسساتها وتحقيق الأمن السيبراني[297].

## المطلب الثاني: القوانين المنظمة لأمن الفضاء السيبراني بهما ومدى تأثيرها

يشكل وجود أطر قانونية فعالة- على المستويات الدولية والإقليمية والوطنية- أحد ركائز الحكم الرشيد؛ إنه أيضًا شرط أساسي لاحترام مبدأ سيادة القانون. بشكل عام، فإن الأطر القانونية تؤدي دورًا حاسمًا في تنظيم السلوك القانوني وحظر أو تجريم الأنشطة غير المشروعة. يلعب الفضاء السيبراني أيضًا دورًا أساسيًا في ضمان احترام حقوق البشر[298].

---

[296]-Zoltán Sipos, Cybersecurity in Algeria, Op.cit, p.71.

[297]-إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مرجع سابق.

[298]-Guide pour la bonne gouvernance pour la cyber sécurité, **DCAF - Le Centre pour la gouvernance du secteur de la sécurité**, Genève – 2019, lien de l'article : http://bitly.ws/Df8a, date visite, 19 .04.2023, p.45.

تبقى مسألة تطبيق تلك الأطر القانونية على الفضاء السيبراني والعمل على تنفيذها، موضوع نقاش ساخن يولد قدرا كبيرا من الارتباك. من قبل طبيعته، يثير الفضاء السيبراني تحديات للحوكمة، والتي يتم تحديدها تقليديًا بواسطة الدولة الإقليمية. في الواقع، إذا كان من الممكن أن تكون البنية التحتية المادية للفضاء السيبراني، مع مراعاة اختصاص وسلطة الدولة، فإن الأخيرة بالكاد تستطيع من ناحية أخرى ممارسة "سيطرة فعالة" على تدفق البيانات والمعلومات الواردة فيه المنقولة والتي تعبر باستمرار الحدود الإقليمية. أدى هذا الأمر بالعديد من الجهات الفاعلة للدعوة إلى تطوير أنظمة معيارية جديدة من أجل تنظيم الفضاء السيبراني[299].

وبناء على ماسبق، سعت الدراسة إلى محاولة سرد جل القوانين المعمول بها في البلدين؛ لا القوانين الداخلية ولا القوانين الدولية، للتأكد من مدى مواكبة البلدين للخطر السيبراني، ومدى جدية تلك القوانين في تطبيقها. تناولت الدراسة في الفرع الأول(القوانين الداخلية المنظمة لأمن الفضاء السيبراني وجدية تطبيقها)، أما في الفرع الثاني، فركزت على(القوانين الدولية المنظمة لأمن الفضاء السيبراني ودرجة فعاليتها).

### الفرع الأول: القوانين الداخلية المنظمة لأمن الفضاء السيبراني وجدية تطبيقهما

الإنترنت هو مساحة افتراضية يجب أن تحكمها قواعد احترازية تهدف إلى حماية شبكات الكمبيوتر وشبكات الاتصالات ومستخدميها. من المفترض أن توفر هذه المجموعة من القواعد الوقائية، التي يمكن تشبيهها بقانون الأمن السيبراني، الحماية من الهجمات السيبرانية. تلك الهجمات عادة ما يكون هدفها الرئيسي هو الإضرار عمدا أو عن غير قصد بالأشخاص الطبيعيين والاعتباريين وأحيانا الدول[300].

مع زيادة هجمات الكمبيوتر هذه، أصبح إنشاء قانون محدد للأمن السيبراني أمرًا ضروريًا على مستوى كل دولة وكذلك على المستوى الدولي. لأنه، في معظم الحالات، لا

[299]-Guide pour la bonne gouvernance pour la cyber sécurité, Op.cit.

[300]-Med Taher SBIHI, Cyber security law in Morocco, LTE **magazine**, 01.01.2023, link: http://bitly.ws/FNWj, seen on 17.O4.2023.

يقيم المهاجم الإلكتروني في نفس البلد الذي يوجد فيه ضحية الهجوم. وبالمثل، فإن البعد العالمي للإنترنت يعقد تطبيق القانون الكلاسيكي وحده[301].

في هذا الفرع، تم البحث عن القوانين الداخلية للمغرب والجزائر، المعتمدة في كبح جماح الهجومات السيبرانية داخل هذين البلدين ومدى جدية تطبيقها.

### الفقرة الأولى: القوانين الداخلية المنظمة للفضاء السيبراني بهما

اضطر المشرع المغربي إلى إثراء قانون العقوبات من خلال أحكام يحتمل أن تنطبق على الجرائم التي يعرفها فضاؤه السيبراني. هكذا كان ميلاد مجموعة من القوانين، سنة 2003، جاءت مكملة لقانون العقوبات المتعلقة بأنظمة معالجة البيانات الآلية[302].

وضع المغرب، إذن، مجموعة من الإجراءات الوطنية للأمن السيبراني، وذلك راجع لتعرضه لظاهرة الهجمات السيبرانية مثل جميع دول العالم[303]. كما عمل على تعزيز إطاره القانوني والتنظيمي إلى الأفضل، لحماية مجتمعه من الجرائم السيبرانية والمواءمة مع الدول الشريكة[304]. ومن بين الإجراءات التي بادر المغرب بإحداثها نسجل إنشاءه في عام 2011، لكيانات مسؤولة عن إنشاء ترسانة قانونية وتقنية كاملة لضمان أمن أنظمة المعلومات[305].

وفي عام 2016 صدر مرسوم حماية حساسية نظام المعلومات والبنية التحتية، التي فرضت بيانات صارمة لمتطلبات الحماية، بما في ذلك الحد من تدفقات البيانات عبر الحدود وإنشاء متطلبات إقامة البيانات[306]. كذلك سن المشرع المغربي ترسانة قانونية. ففي سنة 2013، غير قانون رقم 24.96 بقانون رقم 93.12[307]، هذا القانون الجديد قضى بنقل

---

[301]-Med Taher SBIHI, Cyber security law in Morocco, Op.cit.
[302]-Ali ELAZZOUZI, La cybercriminalité au Maroc, Op.cit, p.113.
[303]-Ibid, p.118.
[304]-Melissa Hathaway and Francesca Spidalieri, Kingdom of Morocco cyber readiness at a glance, Op.cit, 2018, p. 16.
[305]-Ali ELAZZOUZI, Ibid, p.113.
[306]-بوبكر سبيك وآمال برقية، الأمن السيبراني.. الجيل الجديد من التحديات الأمنية، مجلة الشرطة، المديرية العامة للأمن الوطني المغربي، العدد 42، دجنبر 2021، ص.15.
[307]-القانون رقم 93.12، القاضي بتغيير القانون 24.96 والمتعلق بالبريد والمواصلات، الصادر بتنفيذه الظهير الشريف رقم 1.13.56، المؤرخ في 08 شعبان 1434 الموافق ل 17 يونيو 2013، المنشور بالجريدة الرسمية عدد 6166، الصادرة في 25 شعبان 1434 الموافق ل 04 يوليوز 2013، صفحة. 4874.

وتحويل مجموعة من صلاحيات الوكالة الوطنية لتقنين المواصلات إلى الوزارة المنتدبة لدى رئيس الحكومة، المكلفة بإدارة الدفاع الوطني[308].

وفي إطار تعزيز الترسانة القانونية التي تحكم الأمن السيبراني، قررت الحكومة المغربية في 15 مايو 2014، بموجب المرسوم رقم 881-13-02، أن تكون جميع الأنشطة المتعلقة بالتشفير تحت رعاية إدارة الدفاع الوطني (ADN) وبشكل أكثر دقة التوجيه العام لأمن نظم المعلومات[309].

في عام 2016، أصدرت المديرية العامة لأمن نظم المعلومات DGSSI أيضًا مرسومًا يحدد نظام حماية أنظمة المعلومات الحساسة للبنية التحتية الحيوية. تم الانتهاء من هذا النص من خلال صياغة مرسوم من قبل رئيس الحكومة، في عام 2018[310].

هذه جل الإجراءات التي قام المغرب بها. أما القوانين التي سنها فيمكن سرد ما يلي:

-**القانون رقم 03-07**[311]، يعتبر هذا القانون بمثابة أول نص في القانون المغربي يتعامل مع جرائم تكنولوجيا المعلومات ويعاقب على مخالفات أنظمة تكنولوجيا المعلومات [312]. كما يتيح إمكانية تجريم ومعاقبة جميع التدخلات غير المصرح بها والتدليسية في نظام معالجة البيانات الآلية للمعطيات، و يميز بين الوصول والصيانة الاحتيالية[313].

-**القانون رقم 53.05**[314]، يحدد النظام المطبق على البيانات القانونية المتبادلة إلكترونيًا( التشفير) والتوقيعات الإلكترونية، كما يحدد الإطار القانوني المطبق على العمليات التي يقوم بها مقدمو خدمات التصديق الإلكتروني، وكذلك القواعد التي يجب مراعاتها من قبل هؤلاء وحاملي الشهادات الإلكترونية الصادرة[315] ؛

---

[308]-يوسف عنتار، الأمن الرقمي المغربي في ظل تنامي الاعتداءات السيبرانية، المجلة المغربية للدراسات الدولية والاستراتيجية، المغرب، العدد 01، 2019، ص.22.

[309]-Med Taher SBIHI, Cyber security law in Morocco, Op.cit.

[310]-Ibid.

[311]-القانون رقم **07.03** المتعلق بجرائم نظم المعالجة الآلية، الصادر بتنفيذه الظهير الشريف رقم 1.03.197بتاريخ 16 من رمضان1424 الموافق ل11 نوفمبر2003، والمنشور بالجريدة الرسمية عدد5171، الصادرة بتاريخ 27 شوال 1424 الموافق ل 22 ديسمبر 2003، ص.4284.

[312]-Med Taher SBIHI, Ibid.

[313]-Ali ELAZZOUZI, La cybercriminalité au Maroc, Op.cit, p.113.

[314]-القانون رقم **53.05** المتعلق بالتبادل الإلكتروني للمعطيات القانونية، الصادر بتنفيذه الظهير الشريف رقم 1.07.129 بتاريخ 19من ذي القعدة 30 الموافق ل 1428 نوفمبر2007، والمنشور بالجريدة الرسمية عدد5584، الصادرة بتاريخ 25 ذو القعدة 1428 الموافق ل 6 ديسمبر 2007، ص.3879.

[315]-بوبكر سبيك وآمال برقية، الأمن السيبراني.. الجيل الجديد من التحديات الأمنية، مرجع سابق، ص.15.

-**القانون رقم 09.08**[316]، هو القانون المتعلق بحماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية. فبعد تحديدها، يسن القانون المبادئ الأساسية لحمايتها. تتمثل هذه المبادئ في؛ موافقة صاحب البيانات، الغرض من المعالجة، مبدأ التناسب، والولاء في العلاج(حيث يجب إبلاغ الأشخاص المعنيين باستخدام بياناتهم وضمانات حمايتهم) [317].

-**القانون رقم 31.08**[318]، الذي ينص على إجراءات حماية المستهلك، بما في ذلك الحماية على شبكة الإنترنت[319] ؛

-**القانون رقم 88.13**[320]، يشير إلى كون الصحف الإلكترونية تخضع لأحكام القانون (المادة 33)[321]، ويعاقب على الاستخدام غير المشروع للبيانات الشخصية لأغراض الدعاية والإعلان، بغرامة تصل إلى 20000 درهم (المادة 64)[322].

---

[316]-القانون رقم **09.08** المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، الصادر بتنفيذه الظهير الشريف رقم 1.09.15 بتاريخ 22 من صفر 1430 الموافق ل 18فبراير 2007، والمنشور بالجريدة الرسمية عدد5711، الصادرة بتاريخ 27 صفر 1430 الموافق ل 23 فبراير 2009، ص.552.
الصادر بالظهير رقم 1-09-15 المؤرخ في 18 فبراير 2009، الموافق ل 22 صفر 1430

[317]-Abderrahman BELGOURCH et autres, Le cyberspace Diversité des menaces & difficultés de régulation, Op.cit, pp.239-240.

[318]-القانون رقم **31.08** المتعلق بتحديد تدابير لحماية المستهلك، الصادر بتنفيذه الظهير الشريف رقم 1.11.03 بتاريخ 14 من ربيع الأول 1432 الموافق ل 18فبراير 2011، والمنشور بالجريدة الرسمية عدد5932، الصادرة بتاريخ 03 جمادى الأولى 1432 الموافق ل 07 أبريل 2011، ص.1072.

[319]-بوبكر سبيك وآمال برقية، الأمن السيبراني.. الجيل الجديد من التحديات الأمنية، مرجع سابق، ص.15.

[320]-القانون رقم 13-88 المتعلق بالصحافة والنشر، الصادر بتنفيذه الظهير الشريف رقم 1.16.122 بتاريخ 6 من ذي القعدة 1437 الموافق ل 10 يوليوز 2016، والمنشور بالجريدة الرسمية عدد 6491، الصادرة بتاريخ 11 ذي القعدة 1437 الموافق ل 15 يوليوز 2016، ص.5966.

[321]-المادة (33) : حرية خدمات الصحافة الإلكترونية مكفولة ومضمونة ، لا يجوز اعتبار خدمات التواصل مع العموم على شبكة الإنترنت التي يكون غرضها الأساسي تقديم وصلات إشهارية أو إعلانات كيفما كان شكلها أو مضمونها، صحفا إلكترونية. تلتزم الصحف الإلكترونية بالمقتضيات الواردة في القانون رقم 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي الصادر بتنفيذه الظهير الشريف رقم 1.09.15 بتاريخ 22 من صفر 1430 (18 فبراير 2009).

[322]-المادة (64) : مع مراعاة حرية الإبداع، يمنع كل إشهار في الصحافة المكتوبة أو الإلكترونية يتضمن: - تحريضا على الكراهية أو الإرهاب أو جرائم الحرب أو الجرائم ضد الإنسانية أو الإبادة الجماعية أو التعذيب؛
-إساءة وتحقيرا للأشخاص بسبب الدين أو الجنس أو اللون؛
-إساءة وتحقيرا للمرأة أو ينطوي على رسالة من طبيعتها تكريس دونية المرأة أو يروج للتمييز بسبب جنسها؛
-إساءة وتحقيرا للنشء، أو ينطوي على رسالة من طبيعتها أن تتضمن إساءة لشخص الطفل القاصر أو تتضمن تغريرا به أو مسا به أو ترويجا للتمييز بين الأطفال بسبب الجنس؛
-إساءة وتحقيرا للأشخاص في وضعية إعاقة؛
-ترويجا للتدخين عبر استعمال التبغ أو منتوجات التبغ وكذا المشروبات الكحولية في العملية الإشهارية لصالح مؤسسة أو خدمة أو نشاط أو أي منتوج آخر من غير التبغ أو المشروبات الكحولية يتضمن إشارة مميزة لهما أو مذكرة بهما بالصورة أو الاسم أو العلامة أو بأي صيغة أخرى؛
-استعمالا غير قانوني للمعطيات الشخصية ولأهداف إشهارية.

-**القانون رقم 75.12** المتعلق بالمصادقة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، و **القانون رقم 46.13** بالمصادقة على الاتفاقية الأوروبية 108 المتعلقة بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، وأيضا **القانون رقم 136.12** [323] بالمصادقة على الاتفاقية الأوروبية 185 المتعلقة بمكافحة الجرائم السيبرانية الموقعة ببودابست في 23 نوفمبر 2001[324].

-**القانون رقم79.12**[325] القاضي بتتميم القانون رقم 2.00، يرمي إلى تعزيز وحماية الملكية الفكرية وضمان حقوق المؤلفين وذوي الحقوق، لجبر الضرر الذي يلحق المؤلفين جراء أعمال التقليد والاستنساخ غير المشروع[326].

-**القانون رقم 121.12** [327] المغير والمتمم للقانون رقم**24.96** . يتمثل الغرض من هذا القانون في تحديد الإطار القانوني الذي يحدد المشهد الجديد لقطاع البريد والاتصالات السلكية واللاسلكية، ولاسيما شبكات الاتصالات الرقمية[328]؛

-**القانون رقم 05.20** [329]، يهدف إلى وضع إطار قانوني يتضمن الحدود الدنيا من القواعد والتدابير الأمنية لضمان موثوقية ومرونة أنظمة المعلومات. كما يهدف إلى تطوير الثقة الرقمية ورقمنة الاقتصاد وضمان استمرارية الأنشطة الاقتصادية والمجتمعية في

---

[323]-القانون رقم 136.12 الموافق بموجبه على اتفاقية الجرائم المعلوماتية، الموقعة ببودابست في23 نوفمبر2001 وعلى البروتوكول الإضافي لهذه الاتفاقية، الموقع بستراسبورغ في 28 يناير2003، الصادر بتنفيذه الظهير الشريف رقم 1.14.85 بتاريخ 12 من رجب 1435 الموافق ل 12ماي 2014، والمنشور بالجريدة الرسمية عدد6260، الصادرة بتاريخ 29 رجب 1435 الموافق ل 29 ماي 2014، ص.4711.

[324]-ياسين مليح، السيادة الرقمية ... تجلياتها وممكنات تحقيقها بالمغرب، مرجع سابق، ص ص،14-15.

[325]-القانون رقم 79.12 المتعلق بحقوق المؤلف والحقوق المجاورة، الصادر بتنفيذه الظهير الشريف رقم 1.14.97 بتاريخ 20 من رجب 1435 الموافق ل 20ماي 2014، والمنشور بالجريدة الرسمية عدد6263، الصادرة بتاريخ 11 شعبان 1435 الموافق ل 09 يوليوز 2014، ص.4849.

[326]-بوبكر سبيك وآمال برقية، الأمن السيبراني.. الجيل الجديد من التحديات الأمنية، مرجع سابق، ص.15.

[327]-القانون رقم 121.12 المتعلق بالبريد والمواصلات، الصادر بتنفيذه الظهير الشريف رقم 1.19.08 بتاريخ 18 من جمادى الأولى 1440 الموافق ل 25 يناير 2019، والمنشور بالجريدة الرسمية عدد6753، الصادرة بتاريخ 12 جمادى الآخرة 1440 الموافق ل 18 فبراير 2019، ص.775.

[328]-بوبكر سبيك وآمال برقية، الأمن السيبراني.. الجيل الجديد من التحديات الأمنية، مرجع سابق، ص.15.

[329]-القانون رقم 05.20 المتعلق بالأمن السيبراني، الصادر بتنفيذه الظهير الشريف رقم 1.20.69بتاريخ 04 من ذي الحجة 1441 الموافق ل 25 يوليو 2020، والمنشور بالجريدة الرسمية عدد6904، الصادرة بتاريخ 09 ذي الحجة 1441 الموافق ل 30 يوليوز 2020، ص.4160.

المغرب بشكل عام، فضلا عن تطوير نظام بيئي مغربي للأمن السيبراني[330]. وقد تم تعزيز قانون الأمن السيبراني، في المغرب وتحديثه من خلال تنفيذ هذا القانون (رقم 20-05 ) [331].

**أما بالنسبة للجزائر**

لقد أبدت الجزائر هي الأخرى استعدادها لمكافحة الجرائم السيبرانية والمعلوماتية، وقامت بإعداد مجموعة من النصوص القانونية، نذكر منها:

-**القانون رقم04-15** المؤرخ في 27 رمضان عام 1425 الموافق ل10 نوفمبر 2004المعدل والمتمم للأمر رقم 66/ 156 المتضمن لقانون العقوبات. حيث بادر المشرع الجزائري إلى تعديل قانون العقوبات بإدراج القسم السابع مكرر المتعلق بالمساس بأنظمة المعالجة الآلية لمعطيات بمحتوى المادة 394 مكرر إلى 394 مكرر 7 والذي نص على العقوبات التالية:[332]

-المادة 394 مكرر1: عقوبة إدخال معطيات بالغش في نظام المعالجة الآلية، أو إزالة، أو تعديل بطريق الغش المعطيات التي يتضمنها؛

-المادة 394 مكرر2: عقوبة من يقوم عمدا وعن طريق الغش بتصميم، أو بحث، أو تجميع، أو توفير، أو نشر، أو اتجار في معطيات مخزنة، أو معالجة، أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها إحدى الجرائم المنصوص عليها في هذا القسم، و حيازة، أو إفشاء، أو نشر، أو استعمال لأي غرض كان، المعطيات المتحصل عليها؛

-المادة 394 مكرر3:مضاعفة العقوبات المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني، أو الهيئات و المؤسسات الخاضعة للقانون العام ؛

-المادة 394 مكرر4: معاقبة الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل ( 05 مرات) الحد الأقصى للغرامة المقررة للشخص الطبيعي؛

---

[330]-بوبكر سبيك وآمال برقية، الأمن السيبراني.. الجيل الجديد من التحديات الأمنية، مرجع سابق، ص.15.

[331]-Med Taher SBIHI, Cyber security law in Morocco, Op.cit.

[332]-نورة العقون، واقع الفضاء السيبراني و إشكالية الدفاع الوطني في الجزائر، رسالة لنيل شهادة الماستر في ميدان الحقوق والعلوم السياسية، جامعة قاصدي مرباح-ورقلة، كلية الحقوق والعلوم السياسية، الجزائر، السنة الجامعية، 2018-2019، ص ص،53-54.

-المادة 394 مكرر5: معاقبة كل من شارك في مجموعة، أو في اتفاق تألف بغرض الإعداد لجريمة، أو أكثر من الجرائم المنصوص عليها في هذا القسم، وكان هذا التحضير مجسدا بفعل، أو عدة أفعال مادية، بنفس العقوبات المقررة للجريمة ذاتها؛

-المادة 394 مكرر6:مصادرة الأجهزة، البرامج و الوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم ؛

-المادة 394 مكرر7: عقوبة الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها.

ورغم نص المشرع الجزائري على هذه المواد، إلا أنه لم يتطرق إلى جرائم القذف والسب الالكتروني، أو المطاردة عبر الأنترنت أو الغش المعلوماتي، و إنما اكتفى بالنصوص العقابية التقليدية التي لا تتوافق مع طبيعة الجرائم السيبرانية ولا تتماشى مع مبدأ شرعية الجرائم والعقوبات وحظر القياس[333].

استحدث المشرع الجزائري بموجب قانون الإجراءات الجزائية مجموعة من الإجراءات الخاصة التي تتماشى مع العالم الافتراضي وتتمثل في اعتراض المراسلات والتقاط الصور وتسجيل الأصوات، و إجراء التسرب ، فقط لمقتضيات التحري والتحقيق في جرائم محددة حصرا، ومن بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[334].

أما **القانون رقم 09- 04**، المؤرخ في 14 شعبان عام 1430، الموافق ل 05 غشت سنة 2009، فقد تضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. جاء في 19 مادة تندرج تحت ستة (06) فصول[335]. ومن بين الإشارات التي تطرق إليها المشرع الجزائري في هذا القانون؛ نجده قد أشار بموجب المادة الثالثة من هذا القانون 09-04، إلى ضرورة احترام سرية المراسلات[336].

---

[333]-مهدي رضا، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري، مجلة إيليزا للبحوث والدراسات، الجزائر، العدد02، 2021، ص ص،111-125.

[334]-المرجع نفسه.

[335]-نورة العقون، واقع الفضاء السيبراني و إشكالية الدفاع الوطني في الجزائر، مرجع سابق، ص.55.

[336]- المرجع نفسه، صص.111-125.

ويعتبر القانونان 09-04 و 15-04 أهم قانونين سنتهم الجزائر في مكافحة الجريمة السيبرانية بصفة عامة. هذا بالإضافة إلى قوانين أخرى أقرها المشرع الجزائري في مجال الجريمة السيبرانية والمتعلقة بمؤسسات الدولة، تمثلت في[337]:

- **قانون البريد والاتصالات السلكية واللاسلكية:** حيث نصت عدة مواد منه ما يخص المجال السيبراني؛كالمادة 87، والتي نصت على سهولة إجراء التحويلات المالية إلكترونيا.

-**قانون التأمينات:** وقد نص هذا القانون على تنظيم الجريمة السيبرانية من خلال مؤسسات و هيئات الضمان الاجتماعي، و ذلك في عدة نصوص تخص البطاقة الإلكترونية.

-**القوانين اللاحقة المدعمة للقانون 09-04 للحد من الإجرام السيبراني[338]:**

-**القانون 18-04** المتعلق بالقواعد العامة، المتعلقة بالبريد والاتصالات الإلكترونية؛

-**القانون رقم 18-07** المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، الصادر بالجريدة الرسمية عدد 34، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[339].

وقد تم تعريف الجريمة السيبرانية و إدراجها ضمن الأعمال المعاقب عليها قانونا، (المادة 02 ) من القانون رقم09- 04 المؤرخ في2009.05.09، كما تم مطابقة التشريع الداخلي الجزائري مع ما جاء في التشريعات الدولية، وخاصة مع اتفاقية **بودابيست**[340].

## الفقرة الثانية: محدودية الإطار القانوني

حقق المغرب تميزاً قانونياً وتقنياً في مكافحة الجرائم السيبرانية. ومع ذلك، لا تزال الترسانة التنظيمية مقصورة على المنظمات الحيوية، وتتجاهل معظم القطاع الخاص. اعتمد البرلمان المغربي، على سبيل المثال، القانون 05-20 المتعلق بالأمن. ويمثل هذا القانون خطوة مهمة نحو تعزيز القدرات الوطنية في مجال الأمن السيبراني، من خلال دمج الفئات النشطة الأخرى، مثل الجمهور من مشغلي شبكات الاتصالات، ومقدمي خدمات الأمن السيبراني، وموفِّري الخدمات الرقمية. ويهدف إلى وضع إطار لتبادل البيانات، والتعاون بين

---

[337]-نورة العقون، واقع الفضاء السيبراني و إشكالية الدفاع الوطني في الجزائر، مرجع سابق، ص ص،57-58.

[338]-مهدي رضا، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري، مرجع سابق، ص ص،111-125.

[339]-المرجع نفسه، ص ص،121-122.

[340]-بوازدية جمال، الأمن السيبراني، محاضرات مقدمة لطلبة السنة الثانية ماستر، تخصص دراسات استراتيجية وأمنية، جامعة الجزائر-3- ، كلية العلوم السياسية والعلاقات الدولية، الجزائر، السنة الجامعية: 2020–2021، ص. 78.

الهيئة الوطنية للأمن السيبراني والأجهزة المختصة لمكافحة الجرائم السيبرانية، وأخيراً يوفر أرضية قانونية للتعاون الدولي في مجال الأمن السيبراني[341].

وقد حظيت هذه الجهود بتقدير من مجلس أوروبا الذي يعتمد على المغرب في دعم نشر ترسانة قانونية مُحدَّثة قادرة على التصدي للجرائم السيبرانية في منطقة الشرق الأوسط وشمال أفريقيا في إطار مشروعيها: الإجراء العالمي بشأن الجرائم السيبرانية+ (GLACY) ومشروع سايبر ساوث ( CyberSouth)، ويمكن في المغرب حاليّاً تقديم شكوى ضد أي جريمة سيبرانية إلى الفريق المغربي للاستجابة للطوارئ الحاسوبية ( maCERT)، وهو مركز للكشف عن هجمات الكمبيوتر و جزء من إدارة الدفاع الوطني. يتيح مكتب المساعدة التابع للفريق المغربي للاستجابة للطوارئ الحاسوبية لأي مواطن الإبلاغ عن حادثة عبر الإنترنت. ولدى الفريق المغربي للاستجابة للطوارئ الحاسوبية خط ساخن أيضاً. ومع ذلك، يتخلف المغرب عن الركب فيما يتعلق بهياكله التنظيمية، لعدم وجود استراتيجية مُحدَّثة للأمن السيبراني[342].

كذلك، لايجب أن نغفل أن الجرائم السيبرانية أدت إلى ظهور سلوكيات جديدة لا يمكن أن يعاقب عليها معاقبة الجرائم المنصوص عليها في قانون العقوبات التقليدي. بالطبع، توجد العديد من النصوص القانونية التي تجرم جرائم الكمبيوتر، ولكن يتم التحايل عليها في حالات كثيرة ؟[343].

فرغم خضوع القانون الجنائي المغربي لمجموعة من المبادئ التي تشكل أساسه؛ من بين هذه المبادئ، هناك مبدأ الشرعية الجنائية والتفسير الصارم للقانون الجنائي. ومع ذلك ، فإن هذه المبادئ الأساسية تقوضها آفة الجريمة السيبرانية[344]. وإدراكا لخطورة آفة الجريمة السيبرانية، سن المشرع المغربي القانون الجديد 20-05 المتعلق بالأمن السيبراني. دون أن ننسى أن المشرع قد أعطى مكانة مهمة للأخلاق في القانون. فالإنترنت أداة حقيقية للتنمية

---

[341]-باتريك باولاك وآخرون، توقعات كبيرة: تعريف أجندة الأمن السيبراني عبر البحر الأبيض المتوسط، الترجمة من الإنجليزية: رجائي برهان، المعهد الأوروبي للبحر الأبيض المتوسط، إسبانيا، العدد 22، تموز 2021، ص.20.

[342]-المرجع نفسه، ص.20.

[343]-Mohamed Karim MISSAOUI et Abdelaziz ELHILA, Criminal law and ethics put to the test of cyber crime - Le droit pénal et l'éthique à l'épreuve de la cybercriminalité, **Journal d'Economie, de Management, d'Environnement et de Droit**, **(JEMED)-ISSN 2605-6461 Vol 4. N° 2**, Mai 2021, lien de l'article: http://bitly.ws/D2yr, date visite : 17.05.2023

[344]-Ibid.

وفي نفس الوقت تثير العديد من المشاكل الأخلاقية[345]. باختصار، احترام الأخلاق ومبادئ القانون الجنائي هو حجر الزاوية في الأمن السيبراني الفعال[346].

غير أنه ورغم وجود بعض النصوص القانونية المؤطرة، فلا تزال الجرائم السيبرانية تمثل تحديًا حقيقيا للأمن المغربي. فهذه الترسانة القانونية غير كافية لمحاربة الجرائم السيبرانية. ما يلاحظ أن الجريمة السيبرانية تتطور بنفس وتيرة تطور تكنولوجيا المعلومات والاتصالات، في حين يأخذ الإطار القانوني المغربي الكثير من الوقت للخروج إلى الوجود. ما يبين وجود تناقض على مستويين؛ أولا، بين التطور السريع لتكنولوجيا المعلومات والاتصالات والجرائم السيبرانية ، وبين تنفيذ الإطار القانوني الهادف إلى مواجهة الجرائم السيبرانية. فإذا أخذنا على سبيل المثال قانون العقوبات، تتمثل المشكلة التي تفرض نفسها وتحد من دور ذلك القانون في مكافحة الجريمة السيبرانية، في صعوبة تبرير جرائم معينة، تبرير النية، تحديد الجناة وملاحقة الجرائم المرتكبة عبر الإنترنت[347].

لذلك، تم الكشف عن دور الدولة الذي يجب أن يضمن احترام المبادئ التي تحكم القانون الجنائي، ثم الخوض في الجزء الثاني على تدابير الأمن والأخلاق لتعزيز الإطار القانوني للأمن السيبراني، مستوحى من التشريعات الفرنسية[348].

**بالنسبة للجزائر،** وعلى الرغم من أن المشرع الجزائري أسس لمنظومة تشريعية ومؤسساتية للتصدى للجرائم السيبرانية، إلا أن الظاهرة في استفحال مخيف، خاصة بسبب نقص التكوين وآليات التصدي لها، زد على ذلك تطور وسائل الإجرام السيبرانية[349].

غير أن الجزائر، كما أشرنا في السابق، لا تكلف نفسها عناء البحث والتحري في الهجمات السيبرانية التي استهدفتها في الآونة الأخيرة. فما يعني البحث عن المجرم يعني القيام بتحريات تقنية وعلمية، وتطبيق قوانين في هذا الصدد، ويعني كذلك دراسة مدى نجاعة تلك القوانين في ردعها للفعل الإجرامي. لكن الجزائر لا تكلف نفسها كل ذلك العناء، بل ما

---

[345]-Mohamed Karim MISSAOUI et Abdelaziz ELHILA, Criminal law and ethics put to the test of cyber crime - Le droit pénal et l'éthique à l'épreuve de la cybercriminalité, Op.cit.

[346]-Ibid.

[347]-Fátima Roumate, les mécanismes légaux de lutte contre la cybercriminalité au maroc, **com.unifié**, lien de l'article : http://bitly.ws/yutH, date visite : 10.05.2023, p.4.

348- Mohamed Karim MISSAOUI et Abdelaziz ELHILA, Ibid.

[349]-مهدي رضا، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري، مرجع سابق، ص.123.

تقتصر عليه، هو توجيه أصبع اتهامها لجارها المغرب. هذه الكراهية الدفينة لدى الفاعلين الجزائرين الرسميين تقابلها مد يد مغربية لبناء جسر التعاون وتظافر الجهود، قصد إحياء شراكة دول المغرب العربي ونفض الغبار عليها.

### الفرع الثاني: القوانين الدولية المنظمة لأمن الفضاء السيبراني ودرجة فعاليتها

يعتبر القانون الوسيلة الأولى في تنظيم التعاملات بين أفراد المجتمعات المختلفة، و إحدى الو سائل الهامة في تنظيم العلاقات بين الدول، سواء لتأمين الاستقرار ومنع النزاعات والحد منها، أو لحماية الحقوق ومنع الجريمة. لذا كان من الطبيعي، أن تهتم الحكومات المختلفة، بوضع إطار تشريعي وتنظيمي، لترتيب الأوضاع الجديدة الناشئة، نتيجة لبروز نشاطات جديدة وأشكال جديدة من الجرائم، رافقت التحول نحو مجتمع المعلومات والمعرفة. فلطالما حكمت القوانين الوطنية والقوانين الدولية، العديد من الأوضاع والحالات والعلاقات بين الدول، بما يحقق حماية المجتمعات، لاسيما في المجالات التي تطال مجتمعات متعددة، أو التي يمكن أن تعني الإنسانية ككل، والتي يمكن أن تقع تحت اختصاصات قضائية مختلفة، مثل النقل الدولي، الاتصالات، الجريمة المنظمة، الجريمة العابرة للحدود والفضاء الخارجي. ولا تخرج الجرائم السيبرانية عن هذه القاعدة، حيث لا بد من تطبيق القوانين الوطنية، والقانون الدولي، والاتفاقات المتعددة الأطراف، والثنائية، ولا نغفل العلاقات الدبلوماسية[350].

ومن هذا المنطلق، سعت الدراسة في هذا الفرع إلى التركيز على القوانين الدولية المنظمة للمجال السيبراني(الفقرة الأولى)، ثم عرجت على المعيقات التي تحول دون تطبيق تلك القوانين الدولية لا في المغرب ولا في الجزائر(الفقرة الثانية).

#### الفقرة الأولى: القوانين الدولية المنظمة

إذا كان هدف أي قانون يتجسد في السعي إلى تحقيق مصالح محددة، عبر التطرق لجزئياتها وتأطيرها تأطيرا منطقيا يحمي جميع الأطراف المستهدفة من التشريع، فالقانون الدولي العام يرمي هو الآخر إلى الهدف ذاته، وهو التعاون في تنظيم العلاقات بين أشخاص القانون الدولي العام، رغم عدم الاتفاق على سلطة تشريعية موحدة عالميا كما هو الشأن في

[350]-منى الأشقر جبور، السيبرانية هاجس العصر، **المركز العربي للبحوث القانونية والقضائية**، 19غشت 2016، رابط الكتاب: http://bitly.ws/DTBH، تاريخ الدخول: 14.04.2023، ص.102.

القوانين الداخلية للبلدان[351]. يتخذ هذا التعاون في المجال القانوني صورا مختلفة، مثل تسليم المجرمين، المساعدة القضائية، الاعتراف المتبادل بقوة القضية المحكمة، والتنسيق غير الرسمي بين الأجهزة العسكرية والأمنية المعنية[352]. هذه هي الطريقة المعتمدة بين الدول في ما يتعلق بالقضايا التقليدية.

أما بالنسبة للقضايا التي ترتبط بالعالم السيبراني، فعلى الرغم من الاندفاع الكبير لتكديس الترسانات الإلكترونية الوطنية، لا نسجل لحد الساعة إجماعا دوليا على تطبيق "قانون النزاع المسلح" (LOAC، يشار إليه في بعض الحالات باسم LOW أو "قانون الحرب") على الهجمات السيبرانية، في أغلب الأحيان تعتبر شكلاً من أشكال "الهجمات غير النظامية". ينبع هذا الالتباس من الانتشار السريع للهجمات السيبرانية، وعدم وجود سابقة لتوجيه العالم وتنظيمه في عمليات اقتحام الفضاء السيبراني[353].

كما أن طبيعة الأدلة السيبرانية والتي تتطلب ردا فوريا، تفترض الحصول على المعلومات الضرورية، الأمر الذي يعني القدرة على إطلاق عملية تحقيقات متخصصة، كرصد الاتصالات ومتابعتها والحفظ الآني للبيانات. تلجأ الدول، في غالب الأحيان، إلى طلب رسمي من الدول الأخرى، للحصول على البيانات، لاستخدامها كدليل في إثبات الجرم، وذلك ضمن إطار من الاتفاقات الثنائية التي تنظم التعاون فيما بينها. ولكن اللجوء إلى هذه الآلية التقليدية، يتطلب وقتا طويلا، نسبيا، يمكن أن يمتد لشهور، وهذا ما لا يتناسب وطبيعة الجريمة السيبرانية وأدلتها التي تحتم الإسراع لإثباتها[354].

يضاف إلى ما سبق تحول الفضاء السيبراني إلى جبهة رئيسية في كل من النزاعات التقليدية و غير التقليدية. الأعداء في الفضاء السيبراني يشملون الدول وغير الدول، ويتراوحون من الهواة البسطاء لقراصنة محترفين. من خلال الفضاء السيبراني، يستهدف الأعداء الصناعة والأوساط الأكاديمية والحكومة بالإضافة إلى الجيش في المجالات الجوية والبرية والبحرية والفضائية. من أبرز سمات النظام السياسي العالمي الزيادة الكبيرة في

---

[351]-أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، مرجع سابق، ص.78.

[352]-منى الأشقر جبور، السيبرانية هاجس العصر، مرجع سابق، ص.102.

[353]-Rex Hughes, A treaty for cyberspace, 2 Blackwell Publishing Ltd, Oxford, The Royal Institute of International Affairs, International Affairs Journal, N° 86, 2010, p.533.

[354]-منى الأشقر جبور، المرجع نفسه، ص.103.

أعداد وأهمية الكيانات غير الحكومية. صعود تلك الجهات الفاعلة غير الحكومية تشكل تحد حقيقي لافتراضات المناهج التقليدية للعلاقات الدولية، التي تفترض أن الدول هي الوحدات المهمة الوحيدة في النظام الدولي[355].

بناء على كل ما ذكر أعلاه، تستوجب الظرفية إيجاد آليات وقنوات للتعاون، تضمن سرعة التجاوب والرد الفوري، على المستويين الإقليمي والدولي[356]. ومن بين الاجتهادات الدولية، التي تعرف حضورا قويا في المجال السيبراني نسجل ما يلي:

في العام 2002، وضعت مجموعة بلدان الكومنولث، التي تضم 56 دولة، قانونا نموذجيا لمكافحة الجريمة السيبرانية، حرصت على أن يأتي منسجما، مع الاتفاقية الأوروبية لمكافحة الجريمة السيبرانية[357]. كما وضعت قانونا نموذجيا آخر، حول الإثبات الرقمي، نظرا لأهمية الإثبات في القانون[358].

وفي العام 2009، بادرت المجموعة الاقتصادية لغرب إفريقيا، المؤلفة من 15 دولة عضوا، إلى إقرار توصية لمكافحة الجريمة السيبرانية، تشكل الإطار القانوني لعمل الدول الأعضاء[359]. تبع ذلك، مبادرة من قبل السوق المشتركة لشرق وجنوب أفريقيا، في العام2011، لوضع قانون نموذجي حول مختلف جوانب الجريمة السيبرانية. وكان الاتحاد الدولي للاتصالات والاتحاد الأوروبي قد اشتركا في دعم وضع قانون وسياسة نموذجيين، في العام 2010. على خط مواز، وضعت منظمة الدول الأميركية عددا من التوصيات حول الجريمة السيبرانية، لكن التنفيذ على المستوى الوطني لم يتم إنجازه بعد[360].

على المستوى الأوروبي، أقر عدد من التوصيات، واتخذ العديد من القرارات لتحقيق الانسجام بين التشريعات الوطنية للدول الأعضاء في الاتحاد، والتي تكافح الجريمة

---

[355]-Christopher D. DeLuca, The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors, Pace International law Review Online, Volume 3, Number 9, Winter 2013, p.279.

[356]-منى الأشقر جبور، السيبرانية هاجس العصر، مرجع سابق، ص.103.

[357]-المرجع نفسه.

[358]-المرجع نفسه.

[359]-المرجع نفسه.

[360]-المرجع نفسه.

السيبرانية. فأقر المجلس الأوروبي، المؤلف من 47 دولة عضو، اتفاقية لمكافحة الجريمة السيبرانية، في العام 2001، والبروتوكول الإضافي لها، في العام2003[361].

وهناك من يرى إمكانية تطبيق أحكام القانون الدولي الإنساني على الهجمات السيبرانية، وهذا راجع لعدة أسباب؛ منها الطبيعة المرنة لنصوصه ومبادئه، ولعل أهمها "مبدأ مارتنز"[362] الذي يعتبر صمام الأمان والحل الأمثل لإخضاع الهجمات السيبرانية لأحكام القانون الدولي الإنساني[363].

رغم تلك الاجتهادات المعتمدة في القانون الدولي العام لتطويق خطر الهجمات السيبرانية وردعها، هناك تحديات حقيقية تعيق جل المبادرات الدولية المحدثة لمحاصرة الخطر السيبراني.

### الفقرة الثانية: معيقات تطبيق القوانين الدولية المنظمة في كلا البلدين

لتوضيح المعيقات التي تحول دون تطبيق القوانين الدولية في المجال السيبراني للبلدين-المغرب والجزائر- يمكن الرجوع إلى تلك المعيقات التي تقف حجرا عثرا في تطبيق القوانين الدولية في الحقل السيبراني بصفة عامة.

عالج ميثاق الأمم المتحدة القيود القانونية على استخدام القوة في القانون الدولي والعلاقات الدولية بين الدول، حيث نصت الفقرة الرابعة من المادة الثانية من ميثاق الأمم المتحدة على أنه: "يمتنع أعضاء الهيأة جميعا في علاقاتهم الدولية عن التهديد باستعمال القوة، أو باستخدامها ضد سلامة الأراضي، أو الاستقلال السياسي لأي دولة، أو على وجه

---

[361]-منى الأشقر جبور، السيبرانية هاجس العصر، مرجع سابق، ص.103.

[362]-**مبدأ مارتينز"Martins principle"**: ظهر شرط مارتينز لأول مرة من خلال الرأي الذي أدلى به فيورد فيورج مارتينز مندوب قيصر روسيا (نيكولاس الثاني) في مؤتمر السلام لسنة 1899، والذي عد وقتها أقوى الحيل الدبلوماسية التي استخدمت في المفاوضات الدولية حول الوضع القانوني للمدنيين، وذلك بعد أن فشل المندوبون في الاتفاق على مسألة مركز المدنيين الذين يشهرون السلاح بوجه قوات الاحتلال، إذ كانت الدول الكبرى ترى طالما أنه لا توجد قواعد قانونية تحكم وضعهم فيجب أن يعامل هؤلاء على أنهم جنود غير نظاميين ويخضعون لعقوبة الإعدام، في حين رأت الدول الصغيرة أنه يجب أن يتم معاملتهم بوصفهم مقاتلين نظاميين ويخضعون لقوانين الحرب، ونتيجة لذلك الخلاف قام مارتينز بطرح رأيه هذا بقوله " إنه في الحالات غير المشمولة بالأحكام يبقى المدنيون في حماية وسلطان مبادئ قانون الأمم التي استقر عليها الحال بين الشعوب المتمدنة وقوانين الإنسانية ومقتضيات الضمير العام". ولقد لقي هذا الشرط صدى كبير في الأوساط الدولية. في الحقيقية إن تفسير مبدأ مارتينز تفسيراً واسعاً سيكشف إن الغرض منه هو ليس تنظيم وضع السكان المدنيين أثناء النزاعات المسلحة حصراً، وإنما هدفه تغطية الحالات التي لا يغطيها القانون الدولي الإنساني الاتفاقي والعرفي.
(آيات محمد سعود، شرط مارتينز في القانون الدولي الانساني، **الحوار المتمدن**، 09.03.2018، رابط المقال: http://bitly.ws/I6eB، تاريخ الدخول: 12.06.2023).

[363]-محمد السامرائي، دور القانون الدولي في مكافحة الهجمات السيبرانية، مرجع سابق، ص ص .140-141.

آخر لا يتفق ومقاصد الأمم المتحدة". وهنا ارتبطت القوة بالقوة الكلاسيكية الصلبة، لكن مع التطورات التكنولوجية غير المسبوقة ظهرت قوة جديدة؛ القوة السيبرانية، وظهر معها ارتياب في كيفية التعامل معها[364]. من البديهيات، إذن، أن نتوقع انجذاب انتباه علماء العلاقات الدولية، أيضا، بهذه الظاهرة السيبرانية الجديدة[365]. صار منطقيا تطور منظومة القانون الدولي المعنية بتنظيم الحروب، تزامنا مع تطور الحرب السيبرانية، إلا أنها مع تزايد الهجمات السيبرانية، تجلت معضلة التكييف القانوني لهذه الهجمات[366].

فرضت هذه الظاهرة الجديدة" الحرب السيبرانية" تحديا حقيقيا في ميدان القانون الدولي حول التأطير القانوني لهذا النوع من الهجمات. وبرزت بالتحديد معضلة معرفة الجهة الفاعلة (المعتدية)عكس طرق الحرب الأخرى، فبعض الأدوات السيبرانية تنتشر عشوائيا على نطاق واسع، وبطريقة لا يمكن معرفة فاعلها[367]. والمعضلة الأكبر تتمثل في توقيت إبرام الاتفاقيات التي صاغت مبادئ وقواعد القانون الدولي، التي تعود إلى منتصف القرن التاسع عشر وما بعده. وأهم هذه الاتفاقيات نجد اتفاقية لاهاي الأولى عام 1899، والثانية عام 1907، ومن تم اتفاقيات جنيف لعام 1949، والبروتوكولات الإضافية لعام 1977. إذ لم يكن للهجمات السيبرانية خلال إبرامها جميعا أي وجود يذكر[368].

وحتى إذا نظرنا في الأنظمة القانونية القائمة في كثير من الدول لمواجهة الجرائم السيبرانية، يتضح لنا من خلالها عدم وجود اتفاق عام مشترك بين الدول حول نماذج إساءة استخدام شبكة الإنترنت الواجب تجريمها، فما يكون مباحا في أحد الأنظمة قد يكون مجرما في أنظمة أخرى. وهناك عائق آخر وهو عائق الاختصاص؛ قد ترتكب الجريمة في إقليم دولة معينة من قبل أجنبي، فهنا تكون الجريمة خاضعة للاختصاص الجنائي للدولة الأولى استنادا إلى مبدأ الإقليمية، وتخضع كذلك لاختصاص الدولة الثانية على أساس الاختصاص

---

[364]-عبد الوهاب كريم، الأمن السيبراني-القيود والتحديات في ضوء قواعد القانون الدولي، 05.11.2021، رابط المقال: http://bitly.ws/D3te، تاريخ الدخول: 15.04.2023، ص ص، 321-322.

[365]-Col PEC Martin, Cyber warfare schools of thought: bridging the epistemological ontological divide, Op.cit, p.8.

[366]-صلاح حيدر عبد الواحد، حروب الفضاء الالكتروني دراسة في مفهومها وخصائصها وسبل مواجهتها، رسالة لنيل شهادة ماستر، جامعة الشرق الاوسط، كلية الآداب والعلوم ،الأردن، السنة الجامعية،2021- 2020، ص.48.

[367]-القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة، ورقة موقف اللجنة الدولية للصليب الأحمر، 2019، اللجنة الدولية للصليب الأحمر، رابط المقال: http://bitly.ws/FWna ، ص.5.

[368]- صلاح حيدر عبد الواحد، المرجع نفسه، ص.48.

الشخصي في جانبيه، وقد تكون هذه الجريمة من الجرائم التي تهدد أمن وسلامة دولة ثالثة فتدخل عندئذ في اختصاصها استنادا إلى مبدأ العينية[369].

ورغم ذلك، يحاول القانون الدولي أن يجتهد و يقدم إلى الدول ضحايا الأعمال العدائية، سواء نُفذت بوسائل سيبرانية أم لا، بعض الاستجابات. تختلف هذه الاستجابات حسب خطورة الفعل. سنركز أولاً على الردود المتاحة ضد هجوم سيبراني يعادل استخدامًا محظورًا للقوة. عندما يصل هجوم سيبراني إلى مستوى خطورة هجوم مسلح، يحق للدولة الضحية، حسب المادة 51 من القانون الدولي، اللجوء إلى الدفاع عن النفس. حق الدفاع عن النفس معترف به أيضًا كقانون عرفي. غير أن هذه الحالات تشكل استثناءً، وفي معظم الأحيان، يُسمح للدولة فقط باللجوء إلى التدابير المضادة أو الترافع على أساس حالة الضرورة. كما يمكن للدولة أن تلجأ إلى نظام الأمن الجماعي الذي أنشأه ميثاق الأمم المتحدة وأن تناشد مجلس الأمن اتخاذ التدابير[370].

لكن ما يعاب على المادة 51، أنها لم تشر إلى أي سلاح بعينه؛ لذلك نلاحظ أن بعض المفكرين يرون أنه لا يوجد فرق على ما إذا كان الهجوم قد نُفذ بالوسائل التقليدية أو بالوسائل السيبرانية. هذا أيضًا هو الاستنتاج الذي توصل إليه محررو دليل تالين، الذين يقترحون استخدام معايير الأبعاد والتأثيرات لمعرفة متى ترقى الهجمات السيبرانية إلى مستوى هجوم مسلح. تمت صياغة القاعدة 13 على النحو التالي: "يجوز للدولة التي تكون هدفًا لعملية سيبرانية بمستوى يعادل هجومًا مسلحًا أن تمارس حقها الطبيعي في الدفاع عن النفس". يتوقف ارتفاع العملية السيبراية إلى مستوى الهجوم المسلح على أبعادها وتأثيراتها. من هنا يبرز غياب نص صريح مؤطر لتلك الهجمات السيبرانية[371].

فالقانون الدولي عالج قضايا كثيرة وعديدة، ارتبطت بحماية حقوق الإنسان أثناء النزاعات المسلحة الدولية، أو غير الدولية، وركز على الحقوق الفردية؛ حيث جاءت اتفاقيات جنيف الأربع كأساس قانوني لحماية الأشخاص المدنيين في زمن الحرب( اتفاقية جنيف الرابعة)، وهو رغم ذلك بحاجة إلى مراجعة من قبل فقهاء لجنة القانون الدولي في

---

[369]-محمد علي محمد التوني، استراتيجية مكافحة الهجمات السيبرانية، مرجع سابق، ص ص،161-164.

[370]-Camille Rabussier, l'application du droit international dans le cyberespace, Op.cit, pp. 62-63.

[371]-Ibid, p. 67.

الأمم المتحدة، بسبب المتغيرات المتسارعة وطبيعة الحرب الحديثة، المرتبطة بالهجمات السيبرانية وتعدد المفاهيم الجديدة، مثل –مبدأ سيادة الدولة و المسؤولية الدولية[372].

أضاف التطور العلمي المذهل الذي شهده العصر الحديث عوامل مهمة جديدة، كان لها، وسيكون، أثر عميق في تطوير قواعد القانون الدولي وتغيير معالمه؛ إنها العوامل التكنولوجية. غير أنه مازالت جهود وضع قواعد قانونية، قادرة على تنظيم استخدام الفضاء السيبراني كوسيلة حرب، لم ترق بعد إلى مصاف القواعد القانونية الملزمة[373].

حاليًا، لا توجد معاهدة دولية تنظم الفضاء السيبراني. تستلهم كل دولة من تشريعاتها الخاصة لتطوير استراتيجياتها الدفاعية وتطوير سياستها في الدفاع السيبراني: تحدد الدولة احتياجاتها، توقعاتها، أنواع التهديدات التي تتعرض لها وكذلك وسائل منعها وحمايتها من تلك التهديدات. هذا الاهتمام المتزايد بالقوانين الداخلية وإغفال الدولية منها، جعل الترسانة القانونية الحاكمة للفضاء السيبراني ممزقة بين الداخلي والدولي، ودفع بالدول إلى تفضيل تطوير سياسة داخلية، في حين أن المفاوضات الدولية، التي تهدف إلى إنشاء، تحت رعاية الأمم المتحدة، " تدوين عالمي للفضاء السيبراني" انحى إلى المرتبة الثانية[374].

تتمثل المخاطر إذن، في غياب الأمن القانوني، أو حتى في تناقض الأحكام والقوانين، وتنازع الأنظمة القانونية، من جهة أولى، وفي اتساع إمكانات نشوء جنبات للجريمة السيبرانية، من جهة ثانية، ويرتفع منسوب هذه المخاطر، مع انعدام التعاون بين البلدان المختلفة، أو حتى مع وجود تعاون لا يضمن ملاحقة فاعلة[375] .

وتبقى الجهود الدولية، من مقررات وتوصيات، سواء منها تلك التي صدرت عن القمة العالمية، أو عن المنتديات الدولية لحوكمة الأنترنت، وبالرغم من قيمتها السياسية والإعلامية، على المستوى الدولي، غير كافية ولا فاعلة، نظرا لعدم إلزاميتها القانونية ولعدم إتاحتها إمكانات العقاب في حال مخالفتها. هذا عدا عن الهوة الرقمية، التي ما زالت تزداد

---

[372]-عبد الوهاب كريم، الأمن السيبراني-القيود والتحديات في ضوء قواعد القانون الدولي، مرجع سابق، ص ص،321-322.

[373]-المرجع نفسه، ص.324.

[374]-abderrahman BELGOURCH et autres, Le cyberspace Diversité des menaces & difficultés de régulation, Op.cit, pp. 226-227.

[375]-عبد الوهاب كريم ، المرجع نفسه، ص.325.

اتساعا بين الدول[376]. وعليه، يبدو التوصل إلى إقرار نظام عالمي، اليوم وفي المستقبل القريب، بعيد المنال .فكيف يمكن لجميع دول العالم، وإن اتفقت في إطار الأمم المتحدة على مكافحة الجريمة السيبرانية، أن تتفق على تحديد واحد للأعمال السيبرانية الشرعية وغير الشرعية، سواء منها تلك التي تقوم بها الدول، أم تلك التي يقوم بها الأفراد؟ وكيف سيتم الاتفاق على مرجعية لحل الخلافات؟ وما هي آلية فرض قراراتها، لاسيما على الدول المارقة أو المخالفة؟[377].

في ضوء هذه التطورات، من المشكوك فيه ما إذا كانت القواعد الحالية كافية بالنظر إلى الأهمية المتزايدة للهجمات السيبرانية. الفضاء السيبراني ليس بالتأكيد فضاء "الخروج على القانون"، ومع ذلك، فإننا نرى أن التطبيق عن طريق القياس للقواعد المصممة لتنظيم النزاعات البرية والبحرية والجوية ليس دائمًا بسيطًا. إن المقترحات الإبداعية التي قدمها بعض المؤلفين لاستخدام مفاهيم قليلة الاستخدام في القانون الدولي - مثل مبدأ الاجتهاد أو حالة الضرورة - تثبت أن الإطار المعياري الحالي ليس مناسبًا تمامًا[378].

في الواقع، لا تزال الاستجابات للهجمات السيبرانية محدودة، لا سيما بسبب مشكلة تحديد تلك الهجمات السيبرانية وعزوها. ومن المرجح أن يلجأ المزيد من الجهات الفاعلة من غير الدول إليها، فضلاً عن الدول، ولا يمكن اللجوء إلى الدفاع عن النفس أو اتخاذ تدابير مضادة إلا في ظل شروط صارمة. إن اللجوء إلى حالة الضرورة، حتى لو كان مثيرًا للاهتمام، يبدو مقيدًا للغاية لأنه يتعلق فقط بمواقف استثنائية. وبالتالي، فإن هذا الأمر يترك الدول في وضع حرج، حيث لا يمكنها اللجوء إلى استخدام القوة أو التدابير المضادة حتى تتمكن من عزو هجوم سيبراني إلى دولة ما[379].

لكن المشكلة العويصة، تتمثل في كون من خصائص الجرائم السيبرانية، أنها جرائم لا تعترف بأي خصوصية، أو سيادة للدول، وعند وقوعها غالبا ما يكون الجاني في بلد والمجني عليه في بلد آخر، كما قد يكون الضرر في بلد ثالث. فكثير من دول العالم لم تستطع التصدي للجرائم السيبرانية وتعرضت لاختراقات خطيرة، على سبيل المثال؛ الولايات

---

[376]-منى الأشقر جبور، السيبرانية هاجس العصر، مرجع سابق، ص.107.

[377]-المرجع نفسه.

[378]-Camille Rabussier, l'application du droit international dans le cyberespace, Op.cit, p. 92.

[379]-Ibid.

المتحدة الأمريكية: في بداية حكم الرئيس "جو بايدن"، تعرض البيت الأبيض، وزارات الخارجية والتجارة والخزانة والأمن الداخلي، ووكالات فدرالية أخرى لهجمات سيبرانية تعد الأخطر والأشد تعقيدا في السنوات الخمس الأخيرة. كما أشارت البرمجيات الأمريكية "مايكروسوفت"، في يوم الأربعاء الموافق ل 29 يونيو 2022م، أن قراصنة روس بدأوا في شن هجمات سيبرانية واسعة النطاق على حلفاء أوكرانيا الغربيين. حذرت شركة البرمجيات من أن القراصنة يستهدفون أجهزة الكمبيوتر الحكومية في الدول الأعضاء في حلف شمال الأطلسي (ناتو) على وجه الخصوص، مضيفة أنه رغم أن الهدف الرئيسي لهم هو الولايات المتحدة، فإن خبراء مايكروسوفت اكتشفوا ما يقارب 128 هجمة منظمة ضد دول مختلفة خارج أوكرانيا. وأوضحت الشركة أن القراصنة الروس نجحوا في اختراق 29% من الشبكات التي حاولوا مهاجمتها، مضيفة أنه في ربع الهجمات الناجحة على الأقل تم الاستيلاء على البيانات. ومساء الأحد الموافق 3 يوليوز 2022م، أعلنت وزارة الدفاع البريطانية عن خرق حسابات الجيش على تويتر ويوتيوب. أدرجت هذه الأمثلة في الاختراقات السيبرانية، لتبيان أن الدول حتى العظمى منها تعرضت لقرصنة سيبرانية، ولم تستطع حماية أهم مؤسساتها من الاختراقات السيبرانية[380]. هنا يطرح السؤال حول كيف ستحمي الدول النامية في شمال إفريقيا، المغرب والجزائر ضمنها، مجالاتها السيبرانية والدول العظمى لم تستطع حمايته؟

## المبحث الثاني: المؤسسات المحورية والاتفاقيات الإقليمية و الدولية للدفاع السيبراني في المغرب والجزائر

في ظل التوجه الدولي الكبير أصبحت قضية أمن المعلومات السيبرانية لها تحديات كبرى على الصعيدين الإقليمي والعالمي، ومع تزايد التهديدات الأمنية السيبرانية في المغرب والجزائر وغيرهما من الدول العربية، وجب على كل دولة حماية منظومتها المعلوماتية، بوعي مؤسساتها بمفهوم الأمن السيبراني، أهميته، عناصره و ضوابطه، تنفيذ أدوات الأمن

[380]-جلال فضل محمد العودي، مقالات في الجريمة السيبرانية، **الأمن الإلكتروني**، 21غشت 2022، رابط المقال، http://bitly.ws/EuCB ، تاريخ الدخول: 13.05.2023، ص ص،11-13.

السيبراني، تدريب موظفيها، تطوير أساليب إدارة المخاطر وتحديث الأنظمة التقنية باستمرار[381].

فجميع المؤسسات سواء المغربية أو الجزائرية أضحت في حاجة ملحة - بغض النظر عن الحجم - إلى تبني موقف قوي عندما يتعلق الأمر بالأمن السيبراني وحماية أصولها الأكثر أهمية. تستغل الجهات الفاعلة السيبرانية المتطورة والدول القومية نقاط الضعف لسرقة المعلومات والأموال وتطور قدرات لتعطيل، أو تدمير، أو تهديد تقديم الخدمات الأساسية. يتطلب تنفيذ أفضل ممارسات الأمن السيبراني التنظيمي التنسيق عبر المؤسسة من القيادة إلى تكنولوجيا المعلومات إلى الاتصالات والموارد البشرية. من الحوكمة إلى تحديث التكنولوجيا، يتطلب الأمن السيبراني نهجًا شاملاً يبدأ غالبًا بتوجيهات القيادة[382].

للتعرف أكثر على تلك المؤسسات المتوفرة لدا البلدين، تطرقت الدراسة إلى المؤسسات التنظيمية لكلا البلدين ودرجة تأثيرهما في (المطلب الأول)، ثم عرجت على الاتفاقيات السيبرانية الإقليمية والدولية ومدى حمايتهما لكلا البلدين(المطلب الثاني).

## المطلب الأول: المؤسسات التنظيمية لكلا البلدين ودرجة تأثيرها

تستلزم أي عملية وظيفية للدولة ضرورة توفر البنية المؤسسية الضامنة لتفعيل الأداء، بحيث يسمح ذلك للنظام السياسي للقيام بمهامه بشكل مؤسسي وقانوني، يضمن الأمن ويوفر الحقوق للمواطنين، ولا يتأتى ذلك إلا من خلال التركيز على العملية البنيوية والإيفاء بجميع متطلباتها سواء في المجال القانوني والسياسي أو الاقتصادي[383]، لهذا السبب تناولت الدراسة في هذا المطلب من خلال فرعه الأول، المؤسسات المعتمدة لدى البلدين على المستوى الداخلي، في حين ركزت في الفرع الثاني على تلك المؤسسات المعتمدة من طرف المغرب والجزائر على المستوى الخارجي.

---

[381]-سارة محمد روحي فتحي غزال، الأمن السيبراني ودرجة وعي المؤسسات بأهميته، المجلة العربية للنشر العلمي، مركز البحث وتطوير الموارد البشرية رماح ، الأردن، العدد 47، 2022، ص.2.

[382]-**C**ybersecurity & **I**nfrasructure **S**ecurty **A**gency, **Organizations and Cyber Safety**, link: http://bitly.ws/F4IJ, seen on: 21.05.2023.

[383]-سعيدي ياسين، التحديات الأمنية الجديدة في المغرب العربي، مرجع سابق، ص.115.

### الفرع الأول: على المستوى الداخلي

تواجه مؤسسات اليوم تزايد التهديدات الأمنية وتقليل عدد موظفي تكنولوجيا المعلومات والأمن. تتوقع جارتنر"gartner"[384] أن معظم المؤسسات ستشهد قفزة في التهديدات أو التنبيهات السيبرانية منذ بداية COVID-19. لهذا السبب أصبحت فرق الأمن في حاجة ماسة إلى طريقة أسهل لفرض الأمن في كل مكان[385]. لم تخرج من حلقة ذلك التوقع، كلتا البلدين المغرب والجزائر. لهذا السبب نجد سعي البلدين لتطوير مؤسساتهما التنظيمية الداخلية(الفقرة الأولى)، لكن السؤال الذي يتبادر إلى دهن الباحث هو هل لتلك المؤسسات صيت وتأثير في المنظومة الدفاعية للبلدين؟(الفقرة الثانية).

#### الفقرة الأولى: المؤسسات التنظيمية الداخلية للبلدين

**بالنسبة للمغرب**: في خضم التهديدات الأمنية الإقليمية وضغط المنظمات الأمنية الكبرى، وتطور وتشابك الجرائم العابرة للحدود وتنوع الوسائل المعتمدة في ارتكابها، والتي تستدعي استراتيجية ورؤية واضحتين لتدبيرها، نص دستور 2011 المغربي في فصله 54 على إحداث المجلس الأعلى للأمن كمؤسسة دستورية استشارية بشأن استراتيجيته للأمن الداخلي والخارجي للبلاد، وتدبير حالات الأزمات والسهر على مأسسة ضوابط الحكامة الأمنية الجيدة[386].

يرأس الملك هذا المجلس، وله أن يفوض إلى رئيس الحكومة صلاحية رئاسة المجلس على أساس جدول أعمال محدد. يضم المجلس الأعلى للأمن في تركيبته، بالإضافة إلى رئيس الحكومة، رئيس مجلس النواب، رئيس مجلس المستشارين، الرئيس المنتدب للمجلس الأعلى للسلطة القضائية، الوزراء المكلفين بالداخلية، الشؤون الخارجية، العدل وإدارة الدفاع الوطني، وكذا المسؤولين عن الإدارات الأمنية، ضباط سامين بالقوات المسلحة الملكية وكل

---

[384]-**Gartner**: شركة بحثية واستشارية في مجال تكنولوجيا المعلومات مشهورة عالميًا، تجري أبحاثًا حول التقنيات المختلفة وتوفر رؤى ونصائح وأدوات قابلة للتنفيذ للقادة في مجال تكنولوجيا المعلومات والتمويل والموارد البشرية وخدمة العملاء والدعم. تأسست شركة Gartner في عام 1979، ولديها أكثر من 15000 موظف في 100 دولة وهي شركة مطروحة للتداول العام في بورصة نيويورك. تتبع Gartner منهجيات صارمة لإجراء أبحاث سوق متعمقة ، مما يساعد قادة الأعمال على اتخاذ قرارات استراتيجية للمضي قدمًا في منافساتهم.

(Maheen Kanwal, what is gartner?,**webopedia**, 11.08.2022, link : http://bitly.ws/F5eV, seen on : 21.05.2023.)

[385]-Cisco Umbrella, How Modern Security Teams Fight Today's Cyber Threats – Is your workplace protected?, link: http://bitly.ws/F4Ve, seen on: 21.05.2021

[386]-يوسف عنتار، الأمن الرقمي المغربي في ظل تنامي الاعتداءات السيبرانية، مرجع سابق، ص ص،27-229.

شخصية أخرى يعتبر حضورها مفيدا لأشغال المجلس[387]. تشكل مسألة حضور شخصيات سياسية غير حكومية كرئيسي مجلس النواب ومجلس المستشارين، جدلا حيث يرى البعض أنه لا يجب التنصيص عليهم كأعضاء أساسيين للمجلس. وقد تبدو هذه الرؤية مقبولة، لكون الشخصيات سياسية لا تمتلك رؤية أمنية، غير أن طبيعة النظام السياسي المغربي، التي هي ملكية دستورية برلمانية، تفسر حضور هذه الشخصيات الراجع إلى تواجد المساهمة البرلمانية في صناعة القرار العام، ونحى المغرب منحى التوجه البريطاني الذي يعتبر رئيس مجلس العموم عضوا أساسيا في مجلس الأمن القومي[388].

يشرف هذا المجلس على إضفاء الطابع المؤسسي على معايير الحوكمة الأمنية الجيدة. فإنشاء المجلس، في هذه المرحلة الحرجة من التهديدات وتطلعات المواطنين ينبغي أن يشكل دعامة أساسية للأمن، بمعناه الأوسع، وفرصة لتطوير وتنفيذ استراتيجيات ومعايير الحكم الديمقراطي للأمن، بحيث يكون هذا المجلس أيضا هيئة حقيقية من التنظيم والضمانات، لحماية الحقوق والحريات والسلامة الجسدية والمعنوية للمواطنين[389].

فضمان الأمن على صعيد التراب الوطني هو هدف رئيسي لجميع الإجراءات بمبادرة من الدولة، خضع هذا المفهوم لتوجهات جديدة تراعي التهديدات الجديدة الناشئة عن عوامل داخلية وخارجية (الإرهاب، الحركات الاجتماعية، مشاكل الحدود ...)، ولهذا السبب شرعت بلادنا في إجراء إصلاحات في هذا المجال الأمني، مثل إعادة هيكلة المديرية العامة للأمن الوطني، المديرية العامة للدراسات والمستندات(DGED[390])، مؤسسة المديرية العامة لأمن نظم المعلومات، وإنشاء المكتب المركزي للتحقيق القضائي (BCIJ)[391]... ولكن كان الابتكار الرئيسي هو دمج مجلس الأمن الأعلى في دستور 2011[392].

---

[387]-منعم أمشاوي، المجلس الأعلى للأمن القومي بالمغرب: دراسة على ضوء التجارب المقارنة، **مجلة البحثية**، 2017، رابط المقال: http://bitly.ws/FYub، تاريخ الدخول: 30.04.2023، ص.10.

[388]-المرجع نفسه، ص.12.

[389]-Rachid ATTAHIR, le conseil supérieur de sécurité : quelle voie pour la concrétisation ?, **Institut Marocaine de l'Information Scientifique et Technique IMIST**, 2017, lien de l'artcile : http://bitly.ws/FYLh, date visite : 29.04.2023, p. 96.

[390]-DGED : Direction Générale des Etudes et de la Documentation.

[391]-BCIJ: Office Central des Recherches Judiciaires.

[392]-Rachid ATTAHIR, Ibid.

لكن ما يعاب على تأسيس هذا المجلس، أنه قد مرت عليه أكثر من ثلاث عشرة سنة، إلا أنه إلى حد الآن لم يظهر إلى الوجود، ولم يدرج في أجندة المخطط التشريعي للحكومة في إطار تنزيل مقتضيات الدستور من خلال القوانين التنظيمية. غير أن التهديدات الحالية من قبيل الجرائم الماسة بالنظم السيبرانية المدنية والعسكرية تلقي بتحدياتها السلبية على الأمن القومي المغربي، مما يستدعي التركيز بالأساس على الأهداف التي يتوخى من المجلس تحقيقها، وعلى قيمة الاستراتيجيات والتكتيكات الأمنية لمواجهة كل المخاطر التي تحتاج إلى طريقة تعامل خاصة وبرامج إلكترونية وخبرة للتصدي لها.

ففي ظل التطورات الأمنية المتسارعة التي نعيشها اليوم، وكثرة المخاطر والتحديات الداخلية والخارجية التي تطوق بلادنا أضحى من الواجب التعجيل، قبل أي وقت مضى، إلى إخراج هذه المؤسسة الدستورية إلى الوجود، عبر مأسسة ضوابط الحكامة الأمنية الجديدة، في أقرب فرصة ممكنة، وإخراج المجلس الأعلى للأمن إلى حيز الوجود ليكون الأداة المؤسساتية التي تدير رحى السياسات الكبرى في مجال الأمن القومي[393].

**أما الجزائر**، فهي الأخرى تتوفر على مجلس أعلى للأمن، منصوص عليه في دستور البلاد ضمن المادة 173، التي أشارت إلى: "تأسيس مجلس أعلى للأمن يرأسه رئيس الجمهورية، مهمته تقديم الآراء إلى رئيس الجمهورية في كل القضايا المتعلقة بالأمن الوطني"، كما يوجد مرسوم رئاسي يتضمن تنظيم المجلس الأعلى للأمن وعمله، ويتكوّن من 13 مادة، الأولى، تحدد أعضاءه والرابعة، تفيد بأنه يعطي الرأي للرئيس في كل مسألة تتعلق بالأمن وتشمل ميادين النشاط الوطني أو الدولي، وتمنح مادة أخرى، للرئيس وحده صلاحية استدعاء المجلس في أيّ وقت. ومن بين أبرز الشخصيات التي تشارك في اجتماعات المجلس الأعلى للأمن، وزير الدفاع أو من ينوب عنه، رئيس أركان الجيش، مسؤول جهاز المخابرات، وزير الداخلية وشخصيات حكومية أخرى[394].

ما يلاحظ على الدستور الجزائري، أنه كان أكثر غموضًا في نص مادته 173، عند إشارته أن مجلس الأمن الأعلى مسؤول عن إبداء الرأي لرئيس الجمهورية في جميع

---

[393]-عثمان تالمة، تشكيل المجلس الأعلى للأمن على ضوء أزمة كوفيد-19، **مجلة القانون والأعمال الدولية**،15.04.2020، رابط المقال:http://bitly.ws/FZjS ، تاريخ الدخول: 29.05.2023.

[394]-عاطف قدادرة، الشارع الجزائري يرفض تكليف ناطق باسمه والمجلس الأعلى للأمن يتخذ قرارات، **عربية Independant**، 09.03.2021، رابط المقال:http://bitly.ws/FZq2 ، تاريخ الدخول: 30.05.2023.

المسائل المتعلقة بالأمن القومي وأساليب التنظيم والتشغيل. هذه اللجنة محددة بالمرسوم رقم 84-62 المؤرخ في 10 مارس 1984 المعدل عام 1984 م. وفي1989 وطبقاً للمادة 4 من مرسوم عام 1989، فإن هذا المجلس الأعلى أعطى رأيه لرئيس الجمهورية في أي مسألة أمنية تؤثر على مجالات النشاط الوطني أو الدولي، ولا سيما فيما يتعلق بما يلي: تحديد الأهداف من حيث أمن الدولة، تقييم الوسائل والشروط العامة لاستخدامها، تدابير التنسيق العامة في تنفيذ الموارد والوسائل في هذا المجال[395].

إذا ما استثنينا الغموض الذي لف الدستور الجزائري حول مجلسه الأعلى للأمن، بحيث وسع مجاله ولم يحدده بالضبط، نجد أن الجزائر شهدت إضفاء الطابع المؤسساتي على مكافحة الجرائم السيبرانية. وهناك تركيز تدريجي على الكفاءة داخل وزارة الدفاع الجزائرية، وقد تمّ في السابق تكليف إدارة المخابرات والأمن بالمراقبة الإلكترونية من خلال مجموعة التحكم في الشبكة. وكانت الهيأة الجزائرية للوقاية من الجرائم المُتَّصلة بتكنولوجيا المعلومات والاتصال ومكافحتها، تابعة لوزارة العدل حتى يوليوز 2019، عندما تم تحويلها إلى وزارة الدفاع الجزائري. ومع ذلك، فإن مراقبة الجرائم السيبرانية والإبلاغ عنها تقع تحت مسؤولية مركز منع ومكافحة جرائم الكمبيوتر والجرائم السيبرانية، التابع لقيادة الدرك الجزائري، أو تحت مسؤولية خلايا الأمن السيبراني التابعة للمديرية العامة للأمن القومي. ووفقا للإحصاءات الرسمية، عالجت هذه الأخيرة أكثر من 3000 قضية متعلقة بالأمن السيبراني في عام 2018[396].

اكتسبت الجزائر تدريجياً وسائل مكافحة الجريمة السيبرانية منذ عام 1997، ووفقاً لمجلس أوروبا (CoE)، فإنّ الترسانة القانونية المعمول بها تجعل من الممكن مكافحة بعض جرائم الكمبيوتر المذكورة في اتفاقية بودابست بشأن جرائم الإنترنت. لكن لا تزال مواطن الضعف قائمة في مجالات القانون الإجرائي والتعاون الدولي. ولا توجد حاليّاً أي جهة وطنية مسؤولة عن حماية نظم المعلومات ورفع مستوى الوعي حول هذا الموضوع، على الرغم من أنّ الافتقار إلى أمن تكنولوجيا المعلومات يمثل مشكلة كبيرة للبلاد. وقد صدر

[395]-Rachid ATTAHIR, le conseil supérieur de sécurité : quelle voie pour la concrétisation ?, Op.cit, p. 100.

[396]-باتريك باولاك وآخرون، توقعات كبيرة: تعريف أجندة الأمن السيبراني عبر البحر الأبيض المتوسط، مرجع سابق، ص ص،18-19.

مرسوم رئاسي بتاريخ 20 يناير 2020 بهدف معالجة بعض أوجه القصور التي تم تحديدها سابقاً فقط، من خلال وضع إطار عمل لأمن نظم المعلومات الجزائرية، الذي ينص على إنشاء ثلاث منظمات لتطوير استراتيجية أمن نظم المعلومات الجزائرية وتنسيق تنفيذها. وسيتألف هذا الهيكل المؤسساتي من كيانات جديدة، تحت إشراف وزارة الدفاع الجزائرية تضمّ :المجلس الوطني لأمن نظم المعلومات الجزائري، ووكالة أمن أنظمة الكمبيوتر، وأول فريق جزائري للاستجابة للطوارئ الحاسوبية (CERT)، أي المركز التشغيلي الجزائري لأمن الكمبيوتر.

بدأت مجموعات العمل الأولى المسؤولة عن تنفيذ هذا الإصلاح المؤسسي عملها، لكنّ اتضحت محدوديتها مع جائحة كورونا. غير أن هذه التركيبة الأمنية الجزائرية تعد مهمة في توليفتها، إذ ستساهم في توفير المزيد من الوضوح بشأن الحوكمة السيبرانية في الجزائر، حيث سيجمع العديد من الجهات الفاعلة تحت مظلة واحدة، لأنّها تبدو صاحبة الشأن الحكومي الرئيسي للمشاركة في مجال مكافحة الجرائم السيبرانية[397].

### الفقرة الثانية: درجة تأثيرها

يتفق الخبراء على ثلاثة أوجه قصور في نظام الدفاع السيبراني الجزائري الحالي: أولاً، لم يكتمل النظام المعياري والتنظيمي بعد، كما أنّ إنشاء هيئات مراقبة الجرائم السيبرانية المنصوص عليها في النصوص يتم ببطء. ثانياً، هناك نقص في الموارد اللوجستية والبشرية لتحسين هذا الإطار المؤسسي الجديد. ثالثًا، الميل إلى المركزية المفرطة في الاستجابة للجرائم السيبرانية يعيق التكامل مع القطاع الخاص والمجتمع المدني اللذين من شأنهما توفير الموارد والدعم للإدارة فيما يتعلق بهذه القضايا[398].

أما المغرب، فقد عزز قدراته الوطنية في مجال الأمن السيبراني، ووسع نطاق أمن نظم المعلومات من خلال دمج الفئات النشطة الأخرى، مثل الجمهور من مشغلي شبكات الاتصالات، ومقدمي خدمات الأمن السيبراني، وموفِّري الخدمات الرقمية. كما وضع إطارا لتبادل البيانات، والتعاون بين الهيأة الوطنية للأمن السيبراني والأجهزة المختصة لمكافحة

---

[397]-باتريك باولاك وآخرون، توقعات كبيرة: تعريف أجندة الأمن السيبراني عبر البحر الأبيض المتوسط، مرجع سابق، ص ص،18-19.

[398]-المرجع نفسه.

الجرائم السيبرانية وإساءة استخدام البيانات الشخصية، وأخيراً وفر في المحصلة أرضية قانونية للتعاون الدولي في مجال الأمن السيبراني. ويمكن في المغرب حاليّاً تقديم شكوى ضد أي جريمة سيبرانية إلى الفريق المغربي للاستجابة للطوارئ الحاسوبية( maCERT)، وهو مركز للكشف عن هجمات الكمبيوتر ولاتخاذ إجراءات بصددها، وهو جزء من إدارة الدفاع الوطني والمديرية العامة لأمن نظم المعلومات. ويتيح مكتب المساعدة التابع للفريق المغربي للاستجابة للطوارئ الحاسوبية لأي مواطن الإبلاغ عن حادثة عبر الإنترنت، من خلال استكمال نموذج الإبلاغ عن الحادث وإرساله بالبريد الإلكتروني أو الفاكس. ولدى الفريق المغربي للاستجابة للطوارئ الحاسوبية خط ساخن أيضاً[399].

ومع ذلك، يتخلف المغرب عن الركب فيما يتعلق بهياكله التنظيمية، لعدم وجود استراتيجية مُحدَّثة للأمن السيبراني، والفشل في مراقبة المؤشرات الإحصائية، وهي عيوب رئيسية في كفاءة نظام مكافحة الجرائم السيبرانية[400].

ورغم تلك السلبيات المرتبطة بهياكله التنظيمية، أشارت الاستراتيجية المغربية للأمن السيبراني، على المستوى الوطني، إلى تطوير التعاون الوطني في مجال الأمن السيبراني وتنسيق أعمال كل المتدخلين في هذا الموضوع. وقد تم إسناد مهمة الإشراف على استراتيجية الدولة للأمن السيبراني والتنسيق بين القطاعات الوزارية المعنية إلى المديرية العامة لأمن نظم المعلومات التابعة لإدارة الدفاع الوطني، كما تم تكليف هذه المديرية بضمان الرصد التكنولوجي من أجل التعرف ومتابعة الابتكارات في مجال أمن نظم المعلومات، وإحداث، بمعية القطاعات الأخرى، نظام الرصد والإنذار المتعلق بالأحداث المتوقعة والتي من المحتمل أن تؤثر على أنظمة الأمن داخل الدولة[401].

أما فيما يتعلق بالتعاون الدولي، وبالنظر إلى أن الأمن السيبراني يعد ظاهرة عبر وطنية، فإن المغرب صادق في فبراير 2014 على اتفاقية بودابست لمكافحة الجرائم السيبرانية والتي تعتبر أول معاهدة دولية في هذا المجال، كما سبقت الإشارة إلى ذلك. هذا وقد شارك المغرب في مبادرة" سيبر جنوب" cyberSud"، وهو مشروع أوروبي للتعاون

---

[399]-باتريك باولاك وآخرون، توقعات كبيرة: تعريف أجندة الأمن السيبراني عبر البحر الأبيض المتوسط، مرجع سابق، ص ص،18-19.

[400]-المرجع نفسه.

[401]-عبد الواحد البيدري، استراتيجية الأمن السيبراني: دراسة حالة المغرب، مرجع سابق، ص.113.

في مجال مكافحة الجرائم السيبرانية مع دول الجوار في الضفة الجنوبية للبحر الأبيض المتوسط، والتي تم الإعلان عليه رسميا في مارس 2111 بتونس. والهدف الأساسي لهذا المشروع هو تعزيز التشريعات الوطنية والقدرات المؤسساتية في مجال الجرائم السيبرانية والأدلة الإلكترونية، طبقا للمتطلبات المتعلقة بحقوق الإنسان ودولة القانون. كما حصل المغرب إلى جانب بعض الدول العربية وهي تونس ومصر والسعودية وعمان والإمارات، على عضوية منتدى فرق الأمن والاستجابة للحوادث، وهي مجموعة دولية من فرق التصدي لحوادث أمن الحواسب التابعة للقطاعين العام والخاص، والتي تكونت لتبادل المعلومات والمعرفة وأفضل الممارسات والتصدي للحوادث[402].

أما فيما يخص التعاون الثنائي في مجال الأمن السيبراني، نذكر على سبيل المثال لا الحصر توقيع مذكرة تفاهم بين المغرب والهند، تحدد الإطار العام للتعاون في مجال الأمن الإلكتروني بين إدارة الدفاع الوطني المغربية ونظيرتها الهندية، ويشمل هذا التعاون بالأساس تبادل الخبرة في مجال تكنولوجيا الأمن السيبراني وتبادل أفضل الممارسات والتكوين، وجاء ذلك على إثر الزيارة التي قام بها الوزير المنتدب لدى رئيس الحكومة المغربي، المكلف بالدفاع الوطني إلى الهند من 24 إلى 27 سبتمبر 2018[403].

### الفرع الثاني: على المستوى الخارجي

ركزت الدراسة على استحضار بعض المؤسسات الخارجية(الاتحاد الأوروبي وناتو نموذجا) وكيفية تعاملها في مجالها السيبراني (الفقرة الأولى). كما سعت هذه الدراسة إلى تبيان العلاقة التي تربط تلك المؤسسات بدول شمال إفريقيا(المغرب والجزائر نموذجا)، وهل استفاد هذان البلدان من تلك التجارب المتقدمة في الدفاع السيبراني(الفقرة الثانية) .

#### الفقرة الأولى: المؤسسات الخارجية

لنأخذ على سبيل المثال التجربة الأوروبية وكيفية تعاملها مع "القضية السيبرانية". يبدو الدفاع السيبراني الجماعي مناسبًا بشكل خاص في أوروبا، لأنه يعتمد على شبكات ثقة متينة وموجودة مسبقًا. حيث يشترك حلف الناتو والاتحاد الأوروبي في غالبية الأعضاء

---

[402]-عبد الواحد البيدري، استراتيجية الأمن السيبراني: دراسة حالة المغرب، مرجع سابق، ص ص،112-113.
[403]-المرجع نفسه، ص ص،112-113.

المشتركين، وبالتالي فإن لديهم منطق عمل متشابه جدًا. فأمن الناتو وأمن الاتحاد الأوروبي مترابطان[404].

تتمتع أوروبا بمشهد مؤسسي محدد للغاية فيما يتعلق بالأمن والدفاع الجماعي. وهذا يشمل منظمة حلف شمال الأطلسي (الناتو)، وهي منظمة متخصصة في الأمن الجماعي والدفاع منذ إنشائها في عام 1949، وكذلك الاتحاد الأوروبي، الذي بنى هذا المجال بشكل تدريجي، ولا سيما منذ معاهدتي نيس (2001)[405] ولشبونة (2011)[406]. فأين يتجلى الدفاع السيبراني الجماعي لأوروبا؟[407].

يشهد كل من الاتحاد الأوروبي وحلف شمال الأطلسي، إضفاء الطابع المؤسسي على القضايا السيبرانية. قامت كلتا المنظمتين بتكييف هياكلهما وإداراتهما لهذه القضايا الناشئة. وضع كل من هذين الكيانين سياسة الاعتماد على القرارات والنصوص الرقابية والجهات المتخصصة. كلاهما يسعيان لتحقيق نفس الهدف المزدوج: من ناحية، تعزيز أمن الشبكات وأنظمة المعلومات لمؤسساتهما، ومن ناحية أخرى، تحسين الأمن أو تعزيز قدرات الدول الأعضاء. ومع ذلك، لم يطورا سياساتهما بشكل مشترك، فمن الصعب جدا أن نرى ظهور

---

[404]-Morgan JOUY, une Cyberdéfense collective en Europe? l'articulation entre cyber défenses européenne et transatlantique, **Institut de Recherche Stratégique de l' Ecole Militaire "IRSEM",** lien : http://bitly.ws/C8Er, date visite: 26.03.2023, pp ,2-12.

[405]-**معاهدة نيس**: تم التوقيع على معاهدة نيس المعدلة لمعاهدة الاتحاد الأوروبي، والمعاهدات المؤسسة للجماعات الأوروبية وبعض القوانين ذات الصلة، في فبراير سنة 2001 بحضور رئيسة البرلمان الأوروبي، نيكول فونتين. كان الهدف من معاهدة نيس إصلاح الهيكل المؤسسي للاتحاد الأوروبي لمواجهة تحديات التوسيع الجديد. مع معاهدة نيس، تمت زيادة سلطات البرلمان التشريعية والرقابية وتم تمديد تصويت الأغلبية المؤهلة ليشمل المزيد من المجالات داخل المجلس. دخلت حيز التنفيذ بتاريخ 1 فبراير 2003.

(European Parliament, Treaty of Nice, 26.02.2021, link: http://bitly.ws/HiHm, seen on: 05.06.2023).

[406]-**معاهدة ليشبونا:** معاهدة لشبونة المعدلة لمعاهدة الاتحاد الأوروبي والمعاهدة المؤسسة للجماعة الأوروبية ؛ دخلت حيز التنفيذ في 1 ديسمبر 2009.

بدأت معاهدة لشبونة كمشروع دستوري في نهاية عام 2001 (إعلان المجلس الأوروبي حول مستقبل الاتحاد الأوروبي، أو إعلان لاكن "Laeken")، وتبعته في عامي 2002 و 2003 الاتفاقية الأوروبية التي صاغت المعاهدة التي أسست دستورًا لأوروبا (المعاهدة الدستورية). العملية التي أدت إلى معاهدة لشبونة هي نتيجة النتيجة السلبية لاستفتاءين على المعاهدة الدستورية في ماي ويونيو 2005، ردا على ذلك قرر المجلس الأوروبي أن يكون له "فترة تفكير" لمدة عامين. أخيرًا، على أساس إعلان برلين الصادر في مارس 2007، اعتمد المجلس الأوروبي في 21 إلى 23 يونيو 2007 تفويضًا تفصيليًا لمؤتمر حكومي دولي لاحق (IGC)، تحت الرئاسة البرتغالية. اختتمت اللجنة الحكومية الدولية عملها في أكتوبر 2007. ووقعت المعاهدة في المجلس الأوروبي لشبونة في 13 ديسمبر 2007 وصدقت عليها جميع الدول الأعضاء.

(Eeva Pavy, The Treaty of Lisbon, **European Parliament**, 04.2023, link: http://bitly.ws/HiK3, seen on: 05.06.2023).

[407]-Morgan JOUY, Ibid.

عناصر التبعية أو التكامل بين عمليهما. غير أن أمن الاتحاد الأوروبي وأمن الناتو مترابطان[408].

ظهر تعامل الناتو مع التهديد السيبراني وتطور منذ "حرب كوسوفو عام 1999"[409]، والتي شارك فيها التحالف. قرر الناتو آنذاك أخذ هذا التهديد في الاعتبار. ثم تعهدت الدول الأعضاء في قمة براغ في نونبر 2002 بـ "تعزيز قدراتها الدفاعية ضد الهجمات السيبرانية". ومع ذلك، لم تتم معالجة الموضوع، في هذه المرحلة، إلا من زاوية فنية بحتة. علينا أن ننتظر الهجوم السيبراني لعام 2007 ضد إستونيا (عضو الناتو) ليلائم الناتو التهديد السيبراني مع جدول أعماله السياسية. ويتبنى أول سياسة دفاع إلكترونية لحلف الناتو، علامة على أن الإنترنت أصبح مصدر قلق كبير للمؤسسة ودولها الأعضاء. وفي وارسو في يوليوز 2016، تم التعرف على الفضاء السيبراني على أنه "مجال للعمليات التي يجب أن يدافع الناتو فيها عن نفسه بشكل فعال كما يفعل في الجو وعلى الأرض وفي البحر "(الفقرة 70 من بيان القمة). وبالتالي، أصبح الدفاع السيبراني جزءًا لا يتجزأ من الكفاءة الأساسية لحلف الناتو في مسائل الدفاع الجماعي[410].

على عكس حلف الناتو، فإن كفاءات الاتحاد الأوروبي في مجال الدفاع السيبراني لم تتطور نتيجة للحوادث السيبرانية الموجهة ضدها، ولكن تطورها جاء تدريجيًا متسما بالمرونة والاستجابة المنسقة. أصبح الاتحاد الأوروبي على علم تدريجيًا بظهور مخاطر الإنترنت منذ تسعينيات القرن الماضي، وأعلن نفسه فقط في فبراير 2013، مختصا في أمور الدفاع السيبرانية، من خلال استراتيجية الأمن السيبراني للاتحاد الأوروبي: "فضاء إلكتروني مفتوح وآمن"، تم نشرها بالاشتراك بين المفوضية والممثل السامي للشؤون

---

[408]-Morgan JOUY, une Cyberdéfense collective en Europe? l'articulation entre cyber défenses européenne et transatlantique, Op.cit, pp.2-12.

[409]-**نزاع كوسوفو**، (1998-1999) الصراع الذي عارض فيه الألبان العرقيون الصرب وحكومة يوغوسلافيا (بقايا الدولة الفيدرالية السابقة، التي تضم جمهوريتي صربيا والجبل الأسود) في كوسوفو. اكتسب الصراع اهتمامًا دوليًا واسع النطاق وتم حله بتدخل منظمة حلف شمال الأطلسي (الناتو).

(The Editors of Encyclopaedia Britannica, Kosovo conflict Balkan history [1998–1999], **Britannica**, 02.06.2023, link: http://bitly.ws/HjmY, seen on: 05.06.2023).

[410]-Morgan JOUY, Ibid.

الخارجية والسياسة الأمنية التي ينسبها الاتحاد لنفسه في ضوء سياسة الأمن والدفاع المشتركة" Common Security and Defence Policy " "CSDP"[411].

بالنسبة للناتو: فمنذ "قمة وارسو في يوليو 2016"[412]، قامت الدول الأعضاء في الناتو بتحسين دفاعاتهم السيبرانية لضمان مستوى عالٍ من المرونة الجماعية للتحالف بأكمله، أبعد من جهود الدولة الفردية. لدى الناتو قدرات دفاع سيبراني محددة[413]:

-في مقر الناتو، يعتبر قسم التحديات الأمنية الناشئة هو هيئة التحليل الاستراتيجية التي تضمن اتباع نهج منسق لمخاطر الدفاع والأمن الناشئة. القلق "السيبراني" هو من بين التحديات الأمنية الدولية الأخرى مثل الإرهاب، وانتشار أسلحة الدمار الشامل أو انعدام أمن الطاقة؛

-تدعم وكالة الاتصالات والمعلومات التابعة لحلف الناتو (NCIA) عمليات الناتو، وتربط أنظمة الاتصالات والمعلومات، وتدافع أيضًا عن شبكات الناتو؛

-توفر إمكانية الاستجابة لحوادث الكمبيوتر (NCIRC)، الموجودة في المقر الرئيسي الأعلى لشركة Allied Powers Europe (SHAPE)، لحماية شبكة الناتو. تتكون هذه القدرة من حوالي 200 خبير، وهي تراقب باستمرار لمنع الحوادث السيبرانية، وإذا لزم الأمر، للرد عليها. تلعب هذه القدرة دورًا أيضًا في تحليل تحديات المستقبل.

---

411-Morgan JOUY, une Cyberdéfense collective en Europe? l'articulation entre cyber défenses européenne et transatlantique, Op.cit, pp.2-12.

412-**قمة وارسو**: عُقدت قمة منظمة حلف شمال الأطلسي (الناتو) لعام 2016 في وارسو، بولندا، من 8 إلى 9 يوليو 2016. كانت القمة هي الاجتماع الثاني لرؤساء دول التحالف وعددهم 28 رئيسًا منذ عام 2014، عندما ضمت روسيا شبه جزيرة القرم وبدأت في دعم القوات الانفصالية المقاتلة في أوكرانيا. تصرفات روسيا في أوكرانيا وأوروبا الشرقية على نطاق أوسع، قلبت تحول الناتو رأساً على عقب. خلال السنوات الأخيرة، اتخذ الناتو خطوات رئيسية لتعزيز قدراته الدفاعية الإقليمية مرة أخرى ولردع روسيا. أدى تركيز الناتو المتجدد على الدفاع الجماعي والردع إلى خلق بعض التوترات داخل دول التحالف، لا سيما بين تلك الدول الأعضاء الأكثر حساسية للتهديد الروسي-خاصة في أوروبا الشرقية - وتلك ، مثل ألمانيا، التي لها تاريخ طويل من العلاقات الوثيقة مع روسيا. بالإضافة إلى ذلك، تصاعدت المخاوف بشأن عدم الاستقرار في الشرق الأوسط وشمال أفريقيا، فتسببت في توتر بين هؤلاء الحلفاء القلقين أكثر بشأن التهديدات الأمنية من جنوب الناتو وأولئك الذين يواصلون إعطاء الأولوية لردع روسيا وإدارتها. في قمة وارسو، سعى قادة الناتو إلى موازنة هذه المخاوف من خلال معالجة كل من التهديد لشرق الناتو والتهديد على جنوبه. على هذا النحو، ركزت القمة في المقام الأول على موضوعين عامين اثنين:

- تعزيز الردع، في المقام الأول من خلال الانتشار الأمامي في أوروبا الشرقية، وإرساء الاستقرار خارج حلف الناتو، ولا سيما في منطقة الشرق الأوسط وشمال إفريقيا.

(Paul Belkin, NATO's Warsaw Summit: In Brief, **Congressional Research Service**, 14.11.2016, link: http://bitly.ws/HjQM, seen on: 06.06.2023, p.3.)

413-Morgan JOUY, Ibid.

-أخيرًا، تقرر إنشاء مركز العمليات السيبرانية (CyOC) في عام 2018 من قبل رؤساء الدول المجتمعين في القمة في بروكسل. يسمح للحلف بامتلاك قدرات استجابة إلكترونية حقيقية، إلى جانب القدرات التقليدية (البرية والجوية والبحرية) التي توفرها الدول الأعضاء. وبالمثل، في سياق مهامه وعملياته، سيتمكن الناتو من الاستفادة من قدرات تكنولوجيا المعلومات الوطنية .

أما على مستوى الاتحاد الأوروبي، فتوجد أيضًا مجموعة من الوسائل المؤسسية لتحقيق ذلك وبناء المرونة في الفضاء السيبراني. إذا كان من الممكن إنشاء التوازي مع وكالات الناتو، فالمنظمة المؤسسية للاتحاد تقوم على مفهوم مختلف: فهي مبنية بشكل أساسي حول الأمن السيبراني، وليس على وجه التحديد الدفاع السيبراني. تجعل استراتيجية 2013 السيبرانية من المرونة والأمن السيبراني ركائز العمل الأوروبي. وبالتالي، في الجوانب الثلاثة المذكورة أدناه، يبدو من الضروري فهم وسائل الدفاع السيبراني كقدرة مدرجة في هياكل الأمن السيبراني الأوسع[414]:

يتم ضمان دور التحليل والمراقبة الاستراتيجية على مستوى الاتحاد الأوروبي أولاً على مستوى مركز تحليل الاستخبارات التابع للاتحاد الأوروبي (INTCEN)[415] في

---

[414]-Morgan JOUY, une Cyberdéfense collective en Europe? l'articulation entre cyber défenses européenne et transatlantique, Op.cit, pp.2-12.

[415]- يؤدي مركز الاستخبارات والموقف التابع للاتحاد الأوروبي (**EU INTCEN**) "وظيفة استخبارات مدنية" تابعة للاتحاد الأوروبي. من الناحية الهيكلية، فهي مديرية تابعة لخدمة العمل الخارجي (EEAS) وترفع تقاريرها مباشرة إلى الممثل الأعلى للاتحاد الأوروبي للشؤون الخارجية والسياسة الأمنية. تنص المادة 4 من معاهدة الاتحاد الأوروبي صراحة من بين أمور أخرى، على أن "الأمن القومي يظل المسؤولية الوحيدة لكل دولة عضو". تستند المنتجات التحليلية لـ EU INTCEN إلى معلومات استخباراتية من خدمات الاستخبارات والأمن في الدول الأعضاء في الاتحاد الأوروبي.
تعود جذور برنامج EU INTCEN إلى السياسة الأوروبية للأمن والدفاع فيما كان يُطلق عليه آنذاك مركز الموقف المشترك. في أعقاب الهجمات الإرهابية على نيويورك وواشنطن في 11 سبتمبر 2001، قررت استخدام مركز العمليات المشتركة الحالي لبدء إنتاج تقييمات سرية تستند إلى معلومات استخبارية. في عام 2002 ، بدا مركز الموقف المشترك في أن يكون منتدى لتبادل المعلومات الحساسة بين أجهزة الاستخبارات الخارجية في فرنسا وألمانيا وإيطاليا وهولندا وإسبانيا والسويد والمملكة المتحدة. كانت مهمة المركز في ذلك الوقت: المساهمة في الإنذار المبكر (بالاشتراك مع أعضاء المجلس العسكريين الآخرين) من خلال المواد مفتوحة المصدر والاستخبارات العسكرية وغير العسكرية والتقارير الدبلوماسية؛ إجراء مراقبة الحالة وتقييمها؛ توفير التسهيلات لفريق العمل المعني بالأزمات ؛ ولتوفير نقطة اتصال تشغيلية للممثل السامي. بناءً على طلب الممثل الأعلى خافيير سولانا، وافق مجلس الاتحاد الأوروبي في يونيو 2004 على إنشاء خلية مكافحة الإرهاب داخل .SITCEN تم تكليف هذه الخلية بإنتاج تحليلات استخباراتية لمكافحة الإرهاب بدعم من أجهزة الأمن في الدول الأعضاء.
منذ عام 2005، استخدم SITCEN بشكل عام اسم .EU Situation Center في عام 2012 ، تم تغيير اسمه رسميًا إلى مركز تحليل الاستخبارات التابع للاتحاد الأوروبي (EU INTCEN) افترضت اسمها الحالي في عام 2015. منذ يناير 2011، أصبح EU INTCEN جزءًا من خدمة العمل الخارجي الأوروبي (EEAS) تحت سلطة الاتحاد الأوروبي.
**( رابط المقال:http://bitly.ws/HjU3** ).

بروكسل (بلجيكا)، تم إنشاؤه في عام 2011. المعهد الأوروبي للدراسات الأمنية (EUISS) في باريس (فرنسا)، وهي مؤسسة فكرية مستقلة لـ CSDP، تساهم أيضًا في تحليل المصدر المفتوح والتنبؤ بالمخاطر في المجال السيبراني. العديد من منشورات هذه المنظمة لها هدف دراسة الدفاع السيبراني الأوروبي؛

-ENISA ، في هيراكليون (اليونان)، هي الشبكة الأوروبية ووكالة أمن المعلومات. تقدم توصيات وتدعم تطوير وتنفيذ السياسة السيبرانية؛

-تم ضمان قدرة استجابة الاتحاد منذ عام 2012 من قبل فريق دائم، استجابة لطوارئ الكمبيوتر (CERT-UE). وهي تتعاون مع قدرات الاستجابة للدول الأعضاء والقطاع الخاص من أجل الاستجابة للحوادث السيبرانية بجميع أنواعها[416].

سياسة الاتحاد الأوروبي هي الإجراء الأكثر فاعلية في آلية كفاءة التنسيق بين الجهات الفاعلة الوطنية والأوروبية في مجال الدفاع السيبراني، وبين المجتمعات السيبرانية العسكرية والمدنية، وبين القطاعين العام والخاص. وبالإضافة إلى الهياكل القائمة، يعتزم صانعو السياسة في الاتحاد الأوروبي إنشاء مركز تنسيق الدفاع السيبراني للمساهمة في تحسين الوعي بالموقف داخل مجتمع الدفاع. إنهم يريدون أيضًا إنشاء شبكة تشغيلية لفرق الاستجابة للطوارئ الحاسوبية العسكرية - تسمى CERTs. كما سيتم وضع إطار عمل جديد، CyDef-X، لدعم تمارين الدفاع السيبراني للاتحاد الأوروبي. ومع ذلك، من المتوقع أن يكون أهم تطور لمسؤولي الاتحاد الأوروبي هو الوعي بالموقف وقدرات الاستجابة من خلال مراكز العمليات الأمنية التي يديرها المدنيون (SOCs)[417] .

[416]-Morgan JOUY, une Cyberdéfense collective en Europe? l'articulation entre cyber défenses européenne et transatlantique, Op.cit, pp.2-12.

[417]-Luca Bertuzzi, L'UE présente sa politique de cyberdéfense, 14.11.2022, **EURACTIV**, lien de l'article: http://bitly.ws/G6yb, date visite : 30.05.2023

### الفقرة الثانية: درجة تعاونها مع البلدين

اتخذت البلدان في جميع أنحاء المنطقة خطوات لتعزيز تعاونها ضد الجرائم السيبرانية على المستوى الإقليمي، بالتزامن مع الجهود الوطنية[418]. في البداية نركز على التجربتين المذكورتين أعلاه الاتحاد الأوروبي وناتو.

**من جهة الاتحاد الأوروبي**: هناك مجموعة من الثوابت والمتغيرات التي تتحكم في تحديد الموقع الأمني للمغرب في علاقاته بالاتحاد الأوروبي، وفي مقدمتها موقعه الجغرافي القريب من أوروبا، وإرثه التاريخي، علاوة على المقومات السياسية و الاستراتيجية التي يتوفر عليها و التي جعلته مخاطبا أساسيا للعديد من القوى الأوروبية في المجال الأمني. خاصة بعد إفرازات الربيع العربي[419].

أما من الزاوية الجغرافية، فالانتماء المتوسطي للمغرب وقربه الجغرافي من القارة الأوروبية، يفرض عليه الدخول مع دول الاتحاد الأوروبي في علاقات متعددة الأبعاد، ترتبط بالسيبرانية، تيارات الهجرة غير المشروعة، شبكات الاتجار في المخدرات، والإرهاب والعمق الاستراتيجي الإفريقي، على اعتبار أن استقرار دول شمال البحر الأبيض المتوسط يرتبط بالضرورة باستقرار جنوبه. فالاتحاد الأوروبي يرى في المغرب الجار المستقر الأكثر قربا والبوابة الأولى لصد التهديدات التي قد تطال أمنه، ولذلك فالمغرب يعد من الأرقام الصعبة في المعادلة الأمنية الأوروبية، لأن موقعه الاستراتيجي يؤهله للعب دور "الحارس الأمين" للحدود الأوروبية من المخاطر الأمنية والحفاظ على أمن المتوسط[420].

وهكذا نسجل من جهة الاتحاد الأوروبي في الآونة الأخيرة، اهتمامه بالمغرب والدور الريادي الذي يمكن أن يؤديه في مقاومة الإرهاب، وهذا ما خلصت إليه اللجنة البرلمانية المشتركة بين المغرب والاتحاد الأوروبي في يونيو 2018. هذه الرؤية الجديدة للاتحاد الأوروبي تجاه المغرب عرفت النور لأن "النموذج الديني المغربي القائم على إسلام الوسط

---

[418]-Morgan JOUY, une Cyberdéfense collective en Europe? l'articulation entre cyber défenses européenne et transatlantique, Op.cit, pp.2-12.

[419]-كريمة الهلالي، التعاون الأمني بين المغرب والاتحاد الأوروبي، **أكاديميا العربية**، رابط المقال: https://bitly.ws/wPxl، تاريخ الدخول: 30.11.2022.

[420]-المرجع نفسه.

يجب أن يكون مصدر إلهام لمحاربة التطرف العنيف"[421]. وقد كان هناك تعاون كبير في هذا المجال، خصوصا من الجانب المغربي، الذي نوهت بعمله مجموعة من الدول الأوروبية. هذا العمل صراحة يتطلب إلماما معمقا بالمجال السيبراني، وتتبع تحركات المجرمين؛ سواء كانوا إرهابيين أو غيرهم، في الفضاء السيبراني حتى يتم توقيفهم متلبسين. استفادت مجموعة من دول الاتحاد الأوروبي من التجربة المغربية، لكن السؤال الذي نبحث على جوابه، هل المغرب حقق مكتسبات من التجارب السيبرانية الأوروبية؟.

على الرغم من إحجام الدول الأوروبية غير المتوسطية، واصلت منظمة الأمن والتعاون في أوروبا (OSCE) والدول الواقعة على الساحل الجنوبي للبحر الأبيض المتوسط تعاونهما. منذ إعلان بودابست لعام 1995، تجسد هذا الارتباط مع إنشاء مجموعة اتصال مكونة من ممثلين من شمال إفريقيا، الجزائر والمغرب ضمنهم، يتعاونون مع منظمة الأمن والتعاون في أوروبا، ولا سيما مجلسها الدائم. تدريجيًا، تمت دعوة الشركاء المتوسطيين إلى المزيد من الاجتماعات وبالتالي شاركوا في اتخاذ المزيد من القرارات. في عام 2007، تم إنشاء صندوق شراكة لتمويل مشاريع منظمة الأمن والتعاون في أوروبا (OSCE) مع شركاء آخرين. أخيرًا، منذ عام 2010، تشارك دول البحر الأبيض المتوسط في اجتماعات عملية، تتناول القضايا الرئيسية المتعلقة بالأمن الأوروبي الأوسع[422].

**أما بالنسبة لحلف ناتو**: تم إضفاء الطابع المؤسسي على العلاقات بين المغرب والناتو في عام 1994، عندما توجس الحلف من غياب الأمن جنوب حدوده. يجمع هذا الحوار عدة دول جنوبية (**المغرب، الجزائر**، مصر، إسرائيل، الأردن، موريتانيا وتونس). وفي عام 2004، خلال قمة اسطنبول، تم اقتراح تحسين الحوار، من خلال زيادة مجالات التعاون (ولا سيما الكفاح ضد الإرهاب) ولقاءات بين الطرفين. وأخيرا، فإن التطور الخاص للمنظمة الدولية واعتماد مفهوم استراتيجي جديد في نوفمبر 2010، مع إدراج الأمن التعاوني، عزز من وتيرة ومحتوى التعاون بين دول البحر الأبيض المتوسط. فيما يتعلق بالمغرب، فإن

[421]-Domingo.Torrejon , La cooperation en matière de sécurité entre le Maroc et l'Europe : l'Union Européenne est-elle incontournable?, 2018, **Journal of International Law and International Relations, Universidad de Cádiz, España,** Link : http://bitly.ws/G7L5, date visite : 30.05.2023.

[422]-Ibid.

التعاون بين الكيانين يتجسد بطريقتين مختلفتين. من ناحية، من المهم التأكيد على زيادة الروابط المؤسسية، مما يحسن الحوار بين الممثلين الاثنين، ومن ناحية أخرى، غالبًا ما تكون المملكة المغربية مرشحة للمشاركة في بعض مهام الناتو في أوروبا[423]. وما يؤكد رغبة المغرب في إقامة علاقات متينة مع الحلف: تنظيم ندوات وزيارات لمنشآت عسكرية مغربية من قبل سلطات الناتو، توقيع اتفاقات لتيسير تبادل المعلومات السرية و المشاركة في برامج الناتو للسلم والأمن[424].

وإذا كانت التهديدات السيبرانية لأمن الحلف تعتبر معقدة ومدمرة وقسرية بطبيعتها ومتكررة بشكل متزايد، فالناتو يواصل التكيف مع المشهد المتغير لهذه التهديدات. تعتمد المنظمة والحلفاء(**المغرب** واحد منهم باعتباره حليفا استراتيجيا من خارج الناتو major Non-NATO ally, MNNA)، منذ قمة الناتو في ويلزسنة 2014، على أصول دفاع سيبراني قوية ومرنة لإنجاز المهام الأساسية للحلف المتمثلة في الدفاع الجماعي وإدارة الأزمات والأمن التعاوني. أرست سياسة 2014 مبدأ أن الدفاع السيبراني هو جزء من مهمة الحلف الأساسية للدفاع الجماعي، وأيدت أن القانون الدولي ينطبق على الفضاء السيبراني، وعززت قدرات الناتو وحلفائه. وفي قمة وارسو في عام 2016، أعاد الحلفاء التأكيد على التفويض الدفاعي لحلف الناتو، واعترفوا بالفضاء السيبراني باعتباره بيئة التشغيل التي يجب أن يدافع فيها الناتو عن نفسه بفعالية كما يفعل في الجو والبر والبحر. وفي عام 2021، في قمة الناتو في بروكسل، أقر الحلفاء سياسة دفاع سيبراني شاملة جديدة، والتي تساهم في المهام الأساسية الثلاث لحلف الناتو (الدفاع الجماعي، وإدارة الأزمات والأمن التعاوني) وفي موقفه العام المتمثل في الردع والدفاع[425].

أما بالنسبة للجزائر، فتبقى من البلدان التي قد يتوجس منها الناتو لعدة اعتبارات، أهمها مشكل الإرهاب. فناتو يتوجس من الإرهاب الذي قد يجد في الجزائر مرتعا له، ومن تلك المنطقة يمكن أن يصل إلى الدول الحليفة للناتو. لا ننسى كذلك، التقارب القوي بين

[423]-أمين النية، الأمن في السياسة الخارجية المغربية، مرجع سابق.

[424]-Javier Roldan Barbero, la coopération en matière de sécurité entre le maroc et l'europe: l'union europeenne est-elle incontournable?, 2018, lien de l'article: http://bitly.ws/xHdf, date visite, 10.12.2022.

[425]-Cyberdéfense, 17.04.2023, **Organisation du Traité de l'Atlantique Nord**, lien de l'article: http://bitly.ws/Gb8x, date visite : 30.05.2023.

الجزائر وروسيا، العدو المباشر لأغلبية دول الناتو، هذا التقارب الجزائري-الروسي لا يشجع حلف ناتو على تطوير علاقاته الأمنية مع الجزائر. على العكس من ذلك فهو في علاقة أمنية جيدة مع المغرب.

تبين لنا في هذا المطلب أن أوروبا ممثلة باتحادها الأوروبي والناتو، تربطها علاقة جيوسياسية وطيدة مع المغرب، بل اعتبرته حليفا استراتيجيا قويا من خارج ناتو. وكلما طور الاتحاد الأوروبي وناتو منظومته الدفاعية السيبرانية، كلما استفاد المغرب منها بناء على تلك الشراكة التي تربطه بهما.

## المطلب الثاني: الاتفاقيات السيبرانية الإقليمية والدولية ومدى حمايتهما لكلا البلدين

عرفت العقود الثلاثة الأخيرة تحولات واضحة، عصفت باستقرار النماذج المجتمعية السائدة وبعثرت انتظام المفاهيم والمعاني، كالزمان، المكان، الهوية، الذات والآخر، محدثة ما يسمى بالمجتمع الشبكي (Networking Society)، المعروف بغزارة التدفقات المعرفية وهيمنة تكنولوجيات المعلومات والاتصالات، واهتزاز المؤسسات ( shaking Institutions) ، والثقافات المتحولة(Transforming Cultures) [426].

فطن المجتمع الدولي إلى تلك التغيرات المجتمعية، وبالضبط ما يتعلق بالجرائم السيبرانية، واتضح له أن مرتكبي الجرائم المعلوماتية أصبحوا يبسطون نفوذهم على جميع أرجاء العالم، بفضل ما يملكونه من قوة ونفوذ ودهاء، لذا بادر المجتمع الدولي إلى الاهتمام بضرورة التعاون الدولي، لمكافحة الجرائم عامة -والجرائم المعلوماتية خاصة -واتخاذ الإجراءات التي تهدف إلى مكافحتها. وتتأكد حتمية التعاون الدولي لمواجهة ازدياد ضراوة الإجرام وظواهره المختلفة في كل بلاد العالم، حتى صارت كل دولة مهما بلغت درجتها من القوة والحضارة لا تستغني عن الدخول في علاقات تعاونية متبادلة مع غيرها من الدول، ولم تعد جهودها الداخلية في مكافحة، أو ملاحقة الجرائم، كافية لتحقيق منع الجريمة أو تقليص حجمها[427].

---

[426]-محمد سويلمي، في الإسلام الرقمي كيف ارتحل المسلمون إلى الفضاء السيبراني، مرجع سابق، ص. 285 .

[427]-عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، **بنك المعرفة المصري**، 2014، رابط الكتاب: http://bitly.ws/yvYJ، تاريخ الدخول: 02.05.2023

وهكذا ظهرت إلى الوجود عدة مبادرات من قبل العديد من المنظمات، كالاتحاد الدولي للاتصالات (ITU)، الإنتربول/يوروبول، منظمة التعاون الاقتصادي والتنمية (OECD)، مؤسسة الإنترنت للأسماء والأرقام المخصصة (ICANN)، المنظمة الدولية لتوحيد المقاييس (ISO)، اللجنة الكهروتقنية الدولية (IEC)، فرق عمل هندسة الإنترنت "FIRST"، منتدى الاستجابة للأحداث، مجموعات الأمن لآسيا والمحيط الهادئ، منظمة التعاون الاقتصادي للمحيط الهادئ وآسيا (APEC)، منظمة الدول الأميركية (OAS)، رابطة دول جنوب شرق آسيا (ASEAN)، جامعة الدول العربية والاتحاد الأفريقي[428].

في هذا المطلب، سعت الدراسة إلى البحث عن الاتفاقيات السيبرانية الإقليمية والدولية، ثم حاولت تبيان الدور المؤدى من تلك الاتفاقيات في إطار حماية كلا البلدين؛ المغرب والجزائر.

## الفرع الأول: على المستوى الإقليمي

أصبحت الجريمة السيبرانية عابرة للحدود وغير مكترثةٍ بالحواجز الطبيعية، أو الثقافية، وما يدل على ذلك الطريقة التي تنتشر بها فيروسات الكومبيوتر بسرعة و على نطاق واسع، و لأن مرتكبيها غالبا ما يكونون متواجدين في أماكن غير تلك التي تُنتِج فيها الجريمة آثارها، فقد اقتضى الأمر من دول العالم التنسيق والتعاون في مجال محاربتها ووضع التصورات والسيناريوهات المشتركة بشأنها، و ذلك من خلال أطر التعاون و التكتل الإقليمي[429]، و في هذا السياق جاءت الاتفاقيات والمبادرات العربية والإفريقية لوضع آليات تعاون خاصة بها. فماهي تلك الاتفاقيات العربية والإفريقية؟ وما مدى تأمينها السيبراني للبلدين؟

### الفقرة الأولى: الاتفاقيات والمبادرات العربية والإفريقية

**الاتفاقيات العربية:** في المنطقة العربية تم وضع الاتفاقية العربية في 21 دجنبر 2010 لمكافحة جرائم تقنية المعلومات، وقعت عليها واحد وعشرون دولة(21) من بينها المغرب

[428]-مراد مشوش، الجهود الدولية لمكافحة الإجرام السيبراني، مجلّة الواحات للبحوث و الدراسات المجلد، سلسلة مؤلفات وأعمال جامعة غرداية، الجزائر، العدد 2، 2019، ص.709.

[429]-سيدي محمد الأمين الراظي، الجريمة السيبرانية وتكاملية النص الوطني، الإقليمي و الدولي، مجلة القانون والأعمال الدولية، سلسلة مؤلفات وأعمال جامعة الحسن الثاني، المغرب، العدد 23، غشت 2019، ص.31.

والجزائر، وصادقت عليها فقط سبع دول[430]. تهدف هذه الاتفاقية، بحسب مقتضيات مادتها الأولى الى تعزيز التعاون بين الدول الأعضاء في مجال مكافحة جرائم تقنية المعلومات بما تمثله من خطر على أمن و مصالح الدول و المجتمعات و الأفراد[431]. تضمنت هذه الاتفاقية خمسة فصول أساسية وثلاث وأربعين مادة؛ تناول الفصل الأول أحكاما عامة حول الاتفاقية، وتضمن الفصل الثاني التجريم وقام بعرض أنواع الجرائم المرتبطة بالاستخدام السيء لتقنية المعلومات، كما تطرق الفصل الثالث للأحكام الإجرائية، في حين تناول الفصل الرابع التعاون القانوني والقضائي بين الدول الموقعة لهذه الاتفاقية. أما الفصل الخامس والأخير، فتطرق لأحكام ختامية[432]. كما حددت الاتفاقية مجال تطبيقها في أربع نقاط وردت على النحو التالي[433]:

-إذا ارتكبت إحدى هذه الجرائم في أكثر من دولة؛

-إذا كانت الجريمة المرتكبة في الدولة العضو قد تم التخطيط والإعداد لها أو الإشراف والتوجيه بشأنها، في دولة أو دول أخرى؛

-إذا كانت الجهة الضالعة في ارتكاب الجريمة، جماعة إجرامية منظمة، لها أنشطة في أكثر من دولة؛

-إذا كان للجريمة المرتكبة في إحدى الدول آثار بالغة الخطورة و الضرر على دولة أو دول أخرى.

كما أعدت الإسكوا في إطار مشروع" تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية "، المنفذ خلال الفترة 2009-2012 ، "إرشادات الإسكوا للتشريعات السيبرانية "، والتي تعتبر بمثابة نماذج تشريعية لدول المنطقة. وهذه الإرشادات تشمل، إضافة إلى الجرائم السيبرانية، الاتصالات الإلكترونية وحرية التعبير، والتواقيع الإلكترونية. والمعاملات الإلكترونية، والتجارة الإلكترونية وحماية المستهلك، ومعالجة

---

[430]-عبد الواحد البيدري، استراتيجية الأمن السيبراني: دراسة حالة المغرب، مرجع سابق، ص ص، 105-106.

[431]-سيدي محمد الأمين الراظي، الجريمة السيبرانية وتكاملية النص الوطني، الإقليمي و الدولي، مرجع سابق، ص.31.

[432]-جامعة الدول العربية، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، القاهرة جمهورية مصر العربية، 21.12.2010، رابط المقال: http://bitly.ws/yuxK، تاريخ الدخول: 08.05.2023، ص ص،1-17.

[433]-سيدي محمد الأمين الراظي، المرجع نفسه، ص ص،31-32.

البيانات ذات الطابع الشخصي، وحقوق الملكية الفكرية في المجال المعلوماتي والسيبراني[434].

**الاتفاقيات الأفريقية:** تم تبني اتفاقية حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي من قِبل دول الاتحاد الإفريقي، وتمت المصادقة عليها من طرف مجموعة من الدول الإفريقية من ضمنها المغرب؛ فهو الآخر أعد قانونا رقم 52.21 يوافق بموجبه على تلك الاتفاقية المعتمدة بمالابو (غينيا الاستوائية)[435]. هذه الاتفاقية تم إبرامها على عدة مراحل من إطلاق المشروع وصياغة الاتفاقية الأولية، إلى اعتمادها وفتح باب التوقيع عليها[436].

تشكل هذه الاتفاقية أداة تعاون قارية، ولا يمكن إلا للدول الأعضاء في الاتحاد الأفريقي التصديق عليها. وهدفها هو تعزيز ومواءمة التشريعات الحالية للدول الأعضاء والمجموعات الاقتصادية الإقليمية، في مجال تكنولوجيا المعلومات والاتصالات، مع احترام الحريات الأساسية وحقوق الإنسان والشعوب. وتهدف أيضًا إلى إنشاء إطار معياري مناسب يتوافق مع البيئة القانونية والثقافية والاقتصادية والاجتماعية الأفريقية، وتؤكد أن حماية البيانات الشخصية والخصوصية هي قضية رئيسية. كما أنها تضمن تعزيز واستخدام تكنولوجيا المعلومات والاتصالات، ومصلحة الجهات الفاعلة العامة والخاصة. كما تنص على أن يتعهد كل صاحب مصلحة باعتماد تدابير تشريعية أو تنظيمية لتحديد القطاعات التي تعتبر حساسة لأمنه القومي[437].

وتتكون الاتفاقية الأفريقية من ديباجة طويلة، تضمنت أهداف الاتفاقية والأسباب التي دفعت رؤساء الحكومات والدول لاعتمادها، إلى جانب 38 مادة موزعة على أربعة فصول كالتالي: المعاملات الإلكترونية (الفصل الأول المادة 2 إلى المادة 7)، حماية البيانات الشخصية ( الفصل الثاني المادة 8 إلى المادة 23)، تعزيز الأمن السيبراني ومكافحة الجريمة

---

[434]-عبد الواحد البيدري، استراتيجية الأمن السيبراني: دراسة حالة المغرب، مرجع سابق، ص ص، 105-106.

[435]-المرجع نفسه، ص.32.

[436]-مريم لوكال، قراءة في اتفاقية الاتحاد الأفريقي حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة 2014، مجلة الدراسات القانونية والاقتصادية، سلسلة مؤلفات وأعمال جامعة امحمد بوقرة، بومرداس، الجزائر، 2021، ص ص،657-661.

[437]-Christelle HOUETO, "Bilan de la ratification de la convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère", 15.02.2023, **Africa cybersecurity Magazine**, lien de l'article: http://bitly.ws/GbJL, date visite : 31.05.2023.

السيبرانية(الفصل الثالث المادة 24 إلى المادة 31)، أحكام ختامية(الفصل الرابع من المادة 32 إلى المادة38)[438].

### الفقرة الثانية: مدى تأمينها السيبراني للبلدين

تواجه إفريقيا بصفة عامة، والمغرب والجزائر بصفة خاصة، مجموعة متزايدة من التهديدات السيبرانية من التجسس، تخريب البنية التحتية الحيوية، مكافحة الابتكار والجريمة المنظمة. فلا يزال يتعين على معظم البلدان الأفريقية تطوير استراتيجية وطنية للأمن السيبراني. تفشل العديد من البلدان التي لديها استراتيجيات في تحقيق تأثير ذي مغزى لأن خططها تفتقر إلى العناصر التأسيسية ولا تتكيف مع مشهد التهديد المتغير[439].

من ناحية أخرى، تعاني القارة من نقص صارخ في الدفاع السيبراني. ما يشهد على ذلك، الحادث الذي كشف عن قيام الصين بالتجسس على مقر الاتحاد الإفريقي من يناير 2012 إلى يناير 2017، أي لمدة خمس سنوات. الحالة التي أوردتها الصحافة العالمية، تنص على أن الأجهزة الصينية وضعت في مكان بناء الاتحاد الأفريقي، من قبل الشركات الصينية، أجهزة كمبيوتر مجهزة بأنظمة تجسسيه، بمقدورها نقل المحتوى الكامل لـخوادم "serveurs" في مبنى المنظمة الأفريقية، لأجهزة الكمبيوتر الموجودة في شنغهاي كان للدولة الصينية حق الوصول، ليس فقط إلى جميع الوثائق من قبل المنظمة، ولكن أيضًا تركيب خطوط الهاتف وميكروفونات التداول بالفيديو في الموقع. إن القيادة الأفريقية مستهدفة بشكل صارخ من قبل الدول الأخرى، كما أوضحت الصحيفة "لوموند" الفرنسية التي نشرت استطلاعًا على منصات البحث الغربية لـمعلومات عن كبار المديرين التنفيذيين الأفارقة[440].

لهذا السبب، هناك حاجة ماسة إلى مزيد من التعاون الإقليمي لإنشاء أنظمة جديدة للكابلات البحرية ومراكز البيانات وتحديث البنية التحتية، وكذلك لزيادة قدرة اتصالات النطاق العريض، وإدارة ازدحام الشبكة، وضمان استمرارية الخدمات العامة الحيوية،

---

[438]-مريم لوكال، قراءة في اتفاقية الاتحاد الأفريقي حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة 2014، مرجع سابق، ص ص،662-665.

[439]-Abdul-Hakeem Ajijola et Nate D.F. Allen, Leçons d'Afrique en matière de cyber-stratégie, Op.cit.

[440]-Mourad El Manir, L'Afrique face aux défis protéiformes du cyberespace, Op.cit, p.15.

وتعزيز التقنيات المالية الرقمية. وقد أظهرت أزمة كورونا أنه لا يمكن تجاوز أصحاب المصلحة المتعددين على المستويين الوطني والعالمي إلا من خلال العمل المشترك، وتبادل المعرفة، وتعبئة الموارد، وتبادل المعلومات، والتعاون والتنسيق الدوليين من أجل بناء المناعة والقدرة على الصمود في مجال الفضاء السيبراني. يجب على منطقة شمال أفريقيا( المغرب والجزائر نموذجا) والاتحاد الأوروبي تطوير استراتيجية الأمن السيبراني لعموم أوروبا والبحر الأبيض المتوسط، ليس فقط للقطاع العام والبنى التحتية الحيوية، بل لمساعدة المشغلين الاقتصاديين والقطاع الخاص في مواجهة التحديات المتزايدة في التهديدات السيبرانية أيضاً. ويجب أن تُشكّل منطقة الاتحاد الأوروبي وشمال أفريقيا كتلة اقتصادية رقمية، وأن تنشئ رابطة بين فِرَق الاستجابة للطوارئ الحاسوبية في كلتا المنطقتين. وأخيراً، يمكن للاتحاد الأوروبي–من خلال شراكة مع منظمة التعاون الرقمية Digital Cooperation Organization" **(DCO)** ")[441] الجديدة – تطوير الاقتصاد الرقمي في منطقة شمال أفريقيا، وتحقيق أهداف التنمية المستدامة لعام 2030[442].

صحيح أن هناك تعاون إقليمي في مجال الدفاع السيبراني، لكن هذا التعاون يبقى ضعيف الفعالية، إن لم نقل عديمها، وخير دليل على ذلك "اتفاقية مالابو".

الغريب في أمر اتفاقية مالابو، أنه تم اعتمادها سنة 2014 لكنها لم تدخل حيز التنفيذ إلى غاية اليوم، وهو ما يدل أن العديد من البلدان الأفريقية مازالت تعتبر الأمن السيبراني مسألة غير حيوية، ما يزيد من تفاقم المشكلة. فالدول التي صادقت على تلك الاتفاقية لا يتعدى عددها عشر دول من بين خمسة وخمسين دولة أفريقية. انحصرت هذه الدول في أنغولا، غانا، غينيا، الموزمبيق، موريشيوس، ناميبيا، رواندا، سينغال، التوغو، وآخر دولة مصادقة هي الكونغو بتاريخ 20 غشت 2020. كذلك من سلبياتها، على عكس الاتفاقية

---

[441]- **منظمة التعاون الرقمي (DCO):** هيئة عالمية متعددة الأطراف تهدف إلى تمكين الازدهار الرقمي للجميع من خلال تسريع النمو الشامل للاقتصاد الرقمي. تضم عضوية DCO عددًا إجماليًا من السكان يصل إلى أكثر من نصف مليار شخص. يجمع DCO بين الحكومات والقطاع الخاص والمنظمات الدولية والمنظمات غير الحكومية والمجتمع المدني لتمكين التحول الرقمي الأكثر شمولاً ونمو الصناعات الرقمية. (Digital Cooperation Organization, **Linkedin**, link: http://bitly.ws/GdPo, seen on:31.05.2023)
بالإضافة إلى المغرب الذي انضم إليها سنة 2022، تضم هذه المنظمة الرقمية، البحرين والكويت ونيجيريا وعمان وباكستان والأردن ورواندا والمملكة العربية السعودية. (Riyadh: Morocco Joins Digital Cooperation Organization, **Maghreb Arab Press**, link: http://bitly.ws/GdVA, seen on:31.05.2023.

[442]-باتريك باولاك وآخرون، توقعات كبيرة: تعريف أجندة الأمن السيبراني عبر البحر الأبيض المتوسط، مرجع سابق، ص.84.

الأوروبية في مادتها 36/1، فإن الاتفاقية الأفريقية مفتوحة للانضمام فقط للدول الأفريقية، كما أنها لم تتعرض لإنشاء آليات للتعاون بين الدول الأفريقية في المسائل الجنائية ذات الصلة بالجريمة السيبرانية، والمشكل الأكبر أنها لم تطرق باب الأشكال الأخطر من الإجرام السيبراني؛ وهو الحرب السيبرانية وربما يرجع هذا الأمر لحداثة المفهوم عالميا، أو ضعف تكنولوجيا المعلومات أفريقيا[443].

## الفرع الثاني: على المستوى الدولي

في التدرج من الوطني للإقليمي للدولي نصل الى ما يمكن اعتباره أقدم وأهم إطار قانوني للتعاون الدولي لمكافحة الجريمة السيبرانية والمتمثل في الاتفاقيات والمبادرات الدولية[444].

ونظرا لأهمية تلك الاتفاقيات والمبادرات الدولية، سارعت الدراسة لتخصيص فرع كامل لهما، خصص لتتبع الاتفاقيات والمبادرات الدولية(الفقرة الأولى)، ومدى جديتهما الأمنية تجاه البلدين(الفقرة الثانية).

### الفقرة الأولى: الاتفاقيات والمبادرات الدولية

من أبرز مظاهر التعاون على المستوى الدولي نجد اتفاقية مجلس أوروبا لمكافحة الجرائم السيبرانية (Convention sur la cybercriminalité - Conseil de l'Europe)، التي اعتمدتها لجنة وزراء مجلس أوروبا في دورتها التاسعة بعد المائة المنعقدة بتاريخ 23 نوفمبر 2001، وهي أول معاهدة دولية بشأن الجرائم السيبرانية، التي دخلت حيز التنفيذ في 1 يوليوز2004 و المعروفة باتفاقية بودابيست. ولم تقتصر هذه الاتفاقية على الدول الأعضاء في مجلس أوروبا بل إنها قد سمحت بالتوقيع عليها من دول من خارج المجلس، بما جعل منها آلية دولية لمكافحة الإجرام المرتكب بوسائل تقنيات المعلوماتية وضدَّها[445].

وتهدف هذه الاتفاقية إلى تنسيق التشريعات الوطنية حول الجرائم السيبرانية وتحسين القدرات الوطنية للتحقيق في هذه الجرائم والتعاون في هذا المجال، وهي تعنى بجمع الأدلة المعلوماتية في مختلف أنواع الجرائم، وليس في الجرائم السيبرانية فقط. ولغاية شهر مارس

---

[443]-مريم لوكال، قراءة في اتفاقية الاتحاد الأفريقي حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة 2014، مرجع سابق، ص،667.

[444]-سيدي محمد الأمين الراظي، الجريمة السيبرانية وتكاملية النص الوطني، الإقليمي و الدولي، مرجع سابق، ص.33.

[445]-المرجع نفسه.

2021، صادقت65 دولة على الاتفاقية في حين وقعت ثلاث دول أخرى عليها لكنها لم تصادق عليها إلى الآن[446].

تمت صياغتها بهدف تكثيف التعاون الدولي و السعي، على سبيل الأولوية، إلى تحقيق هدف مشترك يتمثل في حماية المجتمع من الجرائم السيبرانية، من خلال اعتماد التشريعات المناسبة وتعزيزها لتعاون دولي فعال. وعلى الرغم من أن فتح التوقيعات على هذه الاتفاقية بدأ في نهاية عام 2001، إلا أنها تظل الاتفاقية الأكثر أهمية عند الحديث عن أي جدول أعمال مشترك دولي حول التعاون ومكافحة الجريمة الرقمية[447].

شكلت تلك الاتفاقية الأوروبية لمكافحة الجريمة السيبرانية، خطوة رائدة على مستوى التعاون بين الدول، لمواجهة هذا الخطر. وهي الوحيدة حتى اليوم، من حيث حجم الدول المنضمة إليها، ومن حيث مداها. وكانت هذه الاتفاقية، قد اتبعت ببروتوكول، دخل حيز التطبيق في مارس 2006، ويهدف إلى تجريم المحتوى العنصري وكراهية الأجانب على الأنترنت، و تجريم التهديدات والشتائم المبنية عليهما[448].

تنبني الفكرة المهيمنة لهذه الاتفاقية على مبدأ أولوية "حمايتك وحماية حقوقك في الفضاء السيبراني"[449]. وتتكون تلك الاتفاقية من أربعة فصول؛ (أ)فصل حول المصطلحات، (ب)وفصل آخر حول التدابير التي يتعين اعتمادها على المستوى الوطني، (ج) وفصل ثالث حول التعاون الدولي و (د) وفصل رابع حول الأحكام النهائية. وعلى الرغم من كونها معاهدة تمت مناقشتها وصياغتها في سياق المجلس الأوروبي، أنشأت اتفاقية بودابست نفسها كنص قانوني رئيسي بشأن التعاون الدولي لغرض الملاحقة القضائية ومكافحة الجرائم السيبرانية[450] .

---

[446]-عبد الواحد البيدري، استراتيجية الأمن السيبراني: دراسة حالة المغرب، مرجع سابق، ص ص، 105-106.

[447]-Bruna Martins dos Santos, Budapest Convention on Cybercrime in Latin America: A brief analysis of adherence and implementationin Argentina, Brazil, Chile, Colombia and Mexico, English Translation: Gonzalo Bernabó, May 2022, **Derechos Digitales América Latina**, link: http://bitly.ws/FUp7, seen on 29.05.2023, p.4.

[448]-منى الأشقر جبور، السيبرانية هاجس العصر، مرجع سابق، ص ص، 106-115.

[449]-Alexander Seger, The Budapest Convention on Cybercrime: a framework for capacity building, 07.12.2016, **Global Forum on Cyber Expertise**, link: http://bitly.ws/FV4T, seen on: 29.05.2023.

[450]-Bruna Martins dos Santos, Ibid, p.6-7.

وزعت الاتفاقية الجرائم التي ترتكب بواسطة الإنترنت، على أربع مجموعات كبرى، تضم الأولى: الجرائم التي تتعرض لخصوصية وسلامة وتوفر الأنظمة والبيانات، وتضم المجموعة الثانية: جرائم التزوير والاحتيال، بينما تندرج في الثالثة، الجرائم المتصلة بالمحتوى، مثل: إنتاج وتوزيع وحيازة مواد إباحية يستخدم فيها الأطفال، وفي المجموعة الرابعة، جرائم الاعتداء على الملكية الفكرية والحقوق المجاورة[451].

وبناء على ما حققته تلك الاتفاقية، يمكن اعتبارها مثالا ناجحا لكيفية موازنة مصالح إنفاذ القانون مع حقوق الإنسان والديمقراطية وسيادة القانون. كانت اتفاقية بودابست تهدف في البداية إلى مواءمة قوانين الجرائم السيبرانية ومعالجة العدد المحدود للتحقيقات عبر الحدود في جرائم الإنترنت ومقاضاة مرتكبيها. في الآونة الأخيرة، تحول التركيز إلى معالجة تحديات جمع الأدلة الرقمية[452].

وما يؤشر أيضا إلى نجاح هذه الاتفاقية والبروتوكول التابع لها، انضمام العديد من الدول غير الأوروبية إليها، واتخاذها صفة الأداة الدولية، بانضمام الولايات المتحدة الأميركية، اليابان، أستراليا، جنوب افريقيا، وكندا وغيرها. فمع نفاذ هذه الاتفاقية في كافة الدول التي وقعتها، تتحول إلى أداة لإدارة المخاطر والتهديدات السيبرانية. وترتكز أهمية هذه الاتفاقية بفعاليتها على إقرارها إجراءات عملية، تلتزم الدول المنضمة بإدراجها في قوانينها الوطنية[453].

**كما يتم التعاون الدولي عبر آليات أخرى؛ من بينها تعاون السلطات القضائية للدول** فيما بينها، أو عبر منظمة الشرطة الجنائية الدولية" الإنتربول"وظهور العديد من صور وأشكال ووسائل التعاون بين أجهزة الشرطة مثل؛ **شرطة الويب الدولية** عام 1986 لتلقي شكاوى مستخدمي الشبكة وملاحقة الجناة والقراصنة إلكترونيا والبحث عن الأدلة ضدهم وتقديمهم للمحاكمة، ومركز بلاغات احتيالات الإنترنت الذي تم إنشاؤه في الولايات المتحدة

---

[451]- منى الأشقر جبور، السيبرانية هاجس العصر، مرجع سابق، ص ص، 106-115.

[452]-Casper Klynge, Cooperating against cybercrime: 20 years on from the Budapest Convention, 16.11.2021, link: http://bitly.ws/FVur, date visite:29.05.2023.

[453]-منى الأشقر جبور، المرجع نفسه، ص.106.

الأمريكية، سنة 2000، ليتعاون مع مكتب التحقيقات الفيدرالي "Federal Bureau of Investigation" "FBI" و المركز القومي لجرائم ذوي الياقات البيضاء[454].

بالإضافة إلى ما سبق، وعلى الرغم من عدم ذكر منطقة شمال أفريقيا بشكل صريح، كان الاتحاد الأوروبي شريكا رئيسيا في دعم المنطقة في مكافحتها للجرائم السيبرانية. والسبب الأساسي لهذه المشاركة هو دعم شركاء الجوار الجنوبي (SN ) في جهودهم للانضمام إلى حوار أصحاب الشأن المتعددين حول الجرائم السيبرانية من خلال الاستفادة من خبرة الاتحاد الأوروبي[455].

بدأ التعاون الإقليمي بشأن الجرائم السيبرانية بين الاتحاد الأوروبي ومنطقة الشرق الأوسط وشمال أفريقيا من خلال مشروع "يوروميد للشرطة 4" (Euromed Police 4)، وتم تنفيذه من فبراير 2016 إلى يناير 2020 من قبل اتحاد مشترك عام-خاص. كان هدف المشروع دعم الشرطة والدرك لدول الجوار الجنوبي للاتحاد الأوروبي؛ **المغرب، الجزائر**، مصر، إسرائيل، الأردن، لبنان، فلسطين وتونس. كانت الجريمة السيبرانية على رأس جدول الأعمال[456].

وبالتعاون مع مجلس أوروبا، منذ عام 2014، دعم الاتحاد الأوروبي الإجراء العالمي بشأن الجرائم السيبرانية (GLACY)[457]، وتلاه مشروع الإجراء العالمي الموسع بشأن الجرائم السيبرانية (GLACY+)[458]. والهدف من الإجراء العالمي بشأن الجرائم السيبرانية هو تعزيز قدرات 15 دولة، بما في ذلك **المغرب**، لتطبيق التشريعات المتعلقة بالجرائم السيبرانية والأدلة الإلكترونية. وكدليل على مشاركة المغرب الطويلة في التعاون الدولي

---

[454]- منى الأشقر جبور، السيبرانية هاجس العصر، مرجع سابق، ص.106.

[455]-ألكسندرا ماريون يمنى لبن، الاقتصاد الرقمي والجرائم السيبرانية، الترجمة من الإنجليزية: رجائي برهان، **المعهد الأوروبي للبحر الأبيض المتوسط**، إسبانيا، العدد 22، يوليوز 2021، ص.23.

[456]-المرجع نفسه، ص.24.

[457]-الهدف المحدد لـ **GLACY** هو:" تمكين سلطات العدالة الجنائية من الانخراط في التعاون الدولي في مسائل الجرائم الإلكترونية والأدلة الإلكترونية على أساس اتفاقية بودابست بشأن الجرائم الإلكترونية". امتدت مدة هذا المشروع من 1 نوفمبر 2013 إلى31 أكتوبر 2016.

(Action Globale sur la Cybercriminalité, **Conseil de l'Europe**, lien de l'article : http://bitly.ws/GeEJ, date visite: 31.05.2023)

[458]-مشروع العمل العالمي بشأن الجرائم الإلكترونية الممتدة **(GLACY +):** مبادرة مشتركة بين الاتحاد الأوروبي ومجلس أوروبا لتعزيز القدرات السيبرانية لـ 12 دولة ذات أولوية في إفريقيا وآسيا والمحيط الهادئ وأمريكا اللاتينية ومنطقة البحر الكاريبي. وهو يعتمد على نتائج أول مشروع GLACY الذي انتهى في عام 2016.

("GLACY+", **Interpol**, Link : http://bitly.ws/GeR2, seen on: 31.05.2023).

بشأن الجرائم السيبرانية، مشاركة قضاة مغاربة في أوراش عمل تدريبية في بلدان الاتحاد الأوروبي[459] .

عمل مشترك آخر للاتحاد الأوروبي ومجلس أوروبا، وهو مشروع سايبر ساوث، بدأ في عام 2017، استهدف منطقة الشرق الأوسط وشمال أفريقيا على وجه التحديد: **المغرب، الجزائر**، الأردن، لبنان وتونس، والهدف منه هو تعزيز قدرات سلطات العدالة الجنائية بشأن الجرائم السيبرانية ، والميزة الإقليمية المهمة لهذا المشروع هي الاستفادة من تجربة **المغرب** في مكافحة الجرائم السيبرانية، حيث إنه البلد الأكثر تقدما على المستوى الإقليمي، بينما يستفيد المغرب بتلقي الدعم[460].

كذلك، ورغم كون **المغرب** والهند متباعدين ثقافيا، دينيا، لغويا وحتى قاريا، يبدو أن هناك القليل جدًا من القواسم المشتركة. ومع ذلك، فمع نهاية 2018، وقعت هاتان الدولتان على مذكرة تفاهم من أجل التعاون على عدة جبهات. الجريمة السيبرانية هي واحدة من المشاكل التي تشترك الدولتان فيها. وتشير مذكرة التفاهم إلى أن البلدين سوف يتعاونان في مجال الأمن السيبراني. يوافق هدف البروتوكول على تشجيع المزيد من التعاون لتبادل المعلومات والخبرة، فيما يتعلق بالكشف والقرار والوقاية من الحوادث الأمنية في كلا البلدين[461].

كذلك لا يمكن إغفال مشروع قانون قدم من طرف مجموعة من أعضاء مجلس الشيوخ الأمريكي، من الحزبين الجمهوري والديمقراطي، في السنة الجارية(2023م) والذي يخدم المغرب في مجال دفاعه السيبراني. ففي فبراير/شباط أعلنت وزارة الأمن الداخلي الأمريكية أنها ستوسع تعاونها مع دول "اتفاقيات أبراهام"[462] كمجموعة لتشمل الأمن

---

[459]-ألكسندرا ماريون يمنى لبن، الاقتصاد الرقمي والجرائم السيبرانية، مرجع سابق، ص.25.

[460]-ألكسندرا ماريون يمنى لبن، المرجع نفسه، ص ص، 25-26.

[461]-Personnel d'ADF, L'Afrique combat la cybercriminalité, **Africa Defense Forum**, Headquarters U.S.africa command, Volume 12, 2ème trimestre, 21.08.2019, lien du magazine :http://bitly.ws/EJD2, date visite : 18.05.2022.

[462]-**اتفاقيات أبراهام**: لا يخفى على أحد أن معظم دول شمال إفريقيا لا تحب إسرائيل. عندما تم إنشاء الدولة اليهودية عام 1948، لم تعترف بها أي دولة في شمال إفريقيا. ونتيجة لذلك، أُجبر اليهود الذين يعيشون في شمال إفريقيا - الجزائر ومصر وليبيا والمغرب وتونس- على الفرار أو تركوا بمحض إرادتهم لأنهم لم يعودوا يشعرون بالأمان. بين عام 1948 وأوائل سبعينيات القرن الماضي، تشير التقديرات إلى أن حوالي ثمانمائة ألف يهودي طردوا أو تركوا أوطانهم العربية.
كان عام 2020 بمثابة نقطة تحول في هذا الفصل من التاريخ. في 13 أغسطس 2020، وقعت الإمارات العربية المتحدة والبحرين اتفاقيات إبراهيم، التي تعترف رسميًا بدولة إسرائيل. وسرعان ما حذت دول عربية وإسلامية أخرى حذوها. بعد

السيبراني. يهدف هذا المشروع إلى تعزيز التعاون في مجال الأمن السيبراني بين الولايات المتحدة ودول اتفاقية أبراهام- إسرائيل والإمارات العربية المتحدة والبحرين و**المغرب**-. ويهدف مشروع القانون خصيصا للمساعدة في الدفاع ضد التهديدات السيبرانية القادمة من جهة إيران وغيرها من "الجهات الفاعلة السيبرانية المعادية". وبهذه الاتفاقية الجديدة يكون المغرب قد خطا خطوة جريئة في تأمين حقله السيبراني، ضد أي تقارب إيراني جزائري في المجال السيبراني[463].

### الفقرة الثانية: مدى جديتها الأمنية تجاه البلدين

انتشرت "الهجمات السيبرانية" بين الدول انتشار النار في الهشيم، وباتت تشكل تحد حقيقي للمعاهدات والاتفاقيات الدولية[464]. تظهر محدودية تلك الاتفاقيات الدولية في توفير الأمن السيبراني لبلدان العالم بصفة عامة، و**للمغرب والجزائر بصفة خاصة**، من خلال اكتشافات" إدوارد سنودن "لعام 2013، حول برنامج المراقبة الجماعية للإنترنت (NSA)[465]التابع للولايات المتحدة. أبانت تلك الاكتشافات أن تقنيات أي بلد تبقى عرضة لهيمنة الدول الأخرى في مجال تكنولوجيا المعلومات والاتصالات. تسببت اكتشافات "إدوارد سنودن" في فقدان الثقة في هذه التقنيات وفي الأنشطة الإلكترونية الأمريكية. أثارت قضية سنودن موجة من الغضب وانعكاس الغضب والتفكير بين الدول حول كيفية حماية سيادتهم السيبرانية. فسيادة الدول قد انتهكت من خلال هذه التدخلات وحملات التجسس الضخمة[466].

---

أشهر، في 10 ديسمبر 2020 ، وقع المغرب اتفاقية تطبيع مع إسرائيل، لتصبح ثاني دولة في شمال إفريقيا - بعد مصر في عام 1978 مع اتفاقيات كامب ديفيد - تعترف بالدولة اليهودية. كما وقعت إسرائيل اتفاقية مع السودان في 23 أكتوبر 2020 كجزء من الاتفاقات. في حين أن اتفاقيات إبراهيم قرّبت بعض الدول العربية من الغرب وإسرائيل، إلا أنها خلقت بلا شك صدوعًا مع الآخرين. **أثار الاتفاق بين إسرائيل والمغرب سلسلة من الأحداث المتسلسلة في دول شمال إفريقيا المجاورة التي من المحتمل أن يكون لها عواقب دائمة على العلاقات الاقتصادية والأمنية والاجتماعية والسياسية في المنطقة.**
(Karim Mezran and Alissa Pavia, Morocco and Israel are friendlier than ever thanks to the Abraham Accords. But what does this mean for the rest of North Africa?, **MENASource**, 07.10.2021, link: http://bitly.ws/IBPo, seen on: 16.06.2023).

[463]-Barak Ravid, New bill aims to boost cybersecurity cooperation between U.S., Abraham Accords nations, **AXIOS**, 31.05.2023, link: http://bitly.ws/GnJj, seen on: 16.06.2023.

[464]-Clémentines Bories, Appréhender la cyberguerre en droit international. Quelques réflexions et mises au point, OpenEdition, 04.12.2014, adresse de l'article : http://bitly.ws/F92Y, date visite : 22.05.2023

[465]-وكالة الأمن القومي **(NSA)** هي وكالة حكومية تابعة لوزارة دفاع الولايات المتحدة مسؤولة عن استخبارات الإشارات وأمن أنظمة المعلومات الحكومية الأمريكية. أنشأها الرئيس هاري ترومان عام 1952 ، وتعتبرهي و وكالة المخابرات المركزية ومكتب التحقيقات الفدرالي، من بين أهم منظمات الاستخبارات في الولايات المتحدة.

[466]-ياسين مليح، السيادة الرقمية ... تجلياتها وممكنات تحقيقها بالمغرب، مرجع سابق، ص.228.

في هذا السياق، نشير إلى أنه رغم الاتفاقيات التي أبرمها **المغرب** مع مجموعة من الدول في مجال الأمن المعلوماتي، فإنه مازال يعرف ثغرات أمنية في ما يتعلق بأمن مجموعة عديدة من مواقعه في الشبكة العنكبوتية، ذلك أن هذه الاتفاقيات أسفرت عن إحداث مراكز انحصر دورها فقط في الإنذار وتدبير الحوادث المعلوماتية، وليس استباق الهجمات ومنع حدوثها. نشير هنا على سبيل المثال إلى الاتفاقية التي أبرمها **المغرب** مع كوريا الجنوبية، والتي أحدث بموجبها المركز المغربي للإنذار وتدبير الحوادث المعلوماتية من قبل الوزارة المكلفة بالصناعة، التجارة والتكنولوجيا الحديثة والوكالة الكورية للتعاون الدولي[467].

تعاني تلك الاتفاقيات كذلك من محدوديات أخرى. فاتفاقية بودابست، مثلا، لها حدان مهمان؛ الأول جغرافي، حيث صادقت 49 دولة فقط على هذا النص، والثاني يتعلق بواقع الانتشار ووجود الأسواق على الويب العميق والويب المظلم حيث، تأخذ على وجه الخصوص، هذه المنتديات في الاعتبار خصائص أدوات الحوسبة الخبيثة والخدمات ذات الصلة، وتبين أن قمع إساءة استخدام الأجهزة صعب بشكل خاص[468].

إضافة إلى ما سبق، نجد أن التعاون الدولي في الفضاء السيبراني ينحصر فقط في مواجهة الجرائم السيبرانية، ولا يتعداها إلى مواجهة التهديدات التي تشنها دول ضد دول أخرى، كون الدول العظمى التي تتبنى الآليات الهجومية لتحقيق أهدافها لا يخدمها تأطير تلك الهجمات، يضاف إلى ذلك اختلاف الرؤى حول كيفية تنظيم الفضاء السيبراني[469].

كذلك يمكن اعتبار معضلة انعدام الثقة بين البلدان العظمى في المجال السيبراني، الولايات المتحدة الأمريكية والصين نموذجين، أنها ساهمت بشكل كبير في تأخر إبرام عدة اتفاقيات دولية[470]. وحتى لمكافحة تأخر إبرام بعض الاتفاقيات الدولية، نسجل وجود عوائق

---

[467]-يوسف عنتار، الأمن الرقمي المغربي في ظل تنامي الاعتداءات السيبرانية، مرجع سابق، ص ص، 22-23.

[468]-Aude Gery, Droit international et prolifération des cyber armes, **Institut Français des Relations Internationales IFRI**, France, Vol. 83, No. 2, 2018, pp. 43-54.

[469]-يوسف عنتار، المرجع نفسه.

[470]-**أحمد** عبيس نعمة الفتلاوي، الهجمات السيبرانية دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، مرجع سابق، ص.105.

تحول دون ذلك بل وتجعل من هذا التعاون صعب المنال، ويمكن إيجاز ذلك في الأسباب التالية[471]:

أولا: عدم وجود نموذج واحد متفق عليه فيما يتعلق بالنشاط الإجرامي، بسبب اختلاف الأنظمة القانونية في بلدان العالم، وعدم اتفاقها على تعريف محدد للنشاط المفروض تجريمه، وهذا راجع إلى قصور التشريع ذاته في كافة بلدان العالم، وعدم مسايرته لسرعة التقدم المعلوماتي ومن تم للجريمة المعلوماتية؛

ثانيا: عدم وجود معاهدات ثنائية أو جماعية بين الدول على نحو يسمح بالتعاون المثمر في المجال السيبراني، وحتى إن وجدت فهي تبقى غير قادرة لتحقيق الحماية المطلوبة.

لكن ومع كل تلك السلبيات المذكورة أعلاه، نسجل جدية في تلك الاتفاقيات المتواجدة، وإن قلت. يمكن دراسة تلك الجدية – أي جدية التعاون الدولي- بناء على معطيات ميدانية، تتجلى في أين وصلت درجة الاحتراز واليقظة لذا تلك البلدين، المغرب والجزائر.

**بالنسبة المغرب:** نسجل تحقيقه للمركز السابع في مؤشر الأمن العربي، وللمركز الخمسين في مؤشر الأمن السيبراني العالمي. كما تمكن من الحصول على نسبة 100 % في مؤشر تنمية تكنولوجيا المعلومات والاتصالات، والمركز الواحد والثلاثين(31) من بين مائة وستين (160) دولة في مؤشر جاهزية الشبكة لعام2022. وسجل حضورا مهما في باقي التقييمات[472].

**أما بالنسبة للجزائر،** فتحتل المركز الثامن والتسعين في مؤشر الأمن السيبراني الوطني، والمركز الرابع بعد المائة في مؤشر الأمن السيبراني العالمي. أما بالنسبة لمؤشر تطوير التصوير المقطعي المحوسب فتمركزت في المركز الثاني بعد المائة. وفي ما يخص بمؤشر جاهزية الشبكة لعام 2021، فأثبت المؤشر عن جاهزيتها % 100[473].

---

[471]-قطاف سليمان، مواجهة الجرائم السيبرانية في ضوء االتفاقيات الدولية، مختبر البحث في الحقوق والعلوم السياسية- جامعة عمار ثليجي الأغواط، الجزائر، 03.05.2022، رابط المقال:http://bitly.ws/D6K3، تاريخ الدخول: 17.04.2023، ص.21.

[472]-Indice de Cybersécurité, **Africa Cybersecurity Magazine**, fevrier 2022, lien de l'adresse : http://bitly.ws/GfGd, date visite : 31.05.2023.

[473]-Algeria-NCSI, **National Cyber Security Index**, 26.04.2021, link : http://bitly.ws/Gi9d, seen on: 31.05.2023.

من خلال قراءة طفيفة لنتائج تلك المؤشرات العالمية، يظهر جليا تقدم المغرب على الجارة الجزائر في الميدان السيبراني. لكن ومقارنة مع باقي دول العالم، نسجل تأخر دول شمال إفريقيا بصفة عامة، والمغرب والجزائر بصفة خاصة، في مواكبة الركب السيبراني العالمي.

**فإذا ما حاولنا تصفح الإطار المغربي للمناعة السيبرانية، نسجل مايلي[474]:**

أولا، أقر مجلس النواب المغربي في 14 يوليو 2020 القانون 20 – 05 بشأن الأمن السيبراني الذي صاغته وزارة الدفاع الوطني؛

ثانياً، تصدّر المغرب الدول العشر الأولى من حيث حجم هجمات البرمجيات الخبيثة في عام 2020، إذ اكتشف كاسبرسكي (Kaspersky ) ما مجموعه 13,4مليون هجوم سيبراني بين أبريل ويونيو 2020. وأفاد 8 ٪ فقط من الأشخاص الذين تم استجوابهم بأنهم يستخدمون نوعاً من برامج مكافحة الفيروسات، وأشار 18 ٪ إلى أنهم لا يقومون بتحديث هواتفهم المحمولة، و 33 ٪ فقط من المستجيبين يثقون في أجهزتهم المحمولة لتخزين البيانات السرية، بينما أشار 76 ٪ إلى أنهم خائفون من سرقة صورهم الشخصية أو مقاطع الفيديو الخاصة بهم، وأن 39 ٪ ممن شملهم الاستطلاع يخشون التجسس عليهم من خلال الكاميرا؛

ثالثا، قام المغرب بتكييف البحث والابتكار ليصبح قوة دافعة للتنمية الاقتصادية في سياق تنافسي بشكل خاص. ويهدف المغرب إلى أن يكون مركزاً تكنولوجيّاً بين أوروبا وأفريقيا، ورائداً في تقنيات الطاقة النظيفة، وتعزيز صناعات التكنولوجيا المستدامة.

رابعا، شارك المغرب أيضاً في مبادرة سايبر ساوث (CyberSouth) في 18 مايو 2017، خلال محادثات المغرب مع الناتو، وتمّ فحص آفاق التعاون في المستقبل في مجال الأمن السيبراني، ولا سيّما من خلال تبادل الخبرات والتدريب.

أخيراً، يخطط مشروع" المغرب الرقمي "ليوجد للبلد مكاناً بين البلدان الناشئة والدول الحيوية (National Cyber Security Strategy of Morocco,2013 )، لكن تلك

---

[474]-باتريك باولاك وآخرون، توقعات كبيرة: تعريف أجندة الأمن السيبراني عبر البحر الأبيض المتوسط ، مرجع سابق، ص ص، 82-83.

الاتفاقيات تعاني من بعض الصعوبات، التي تحول دون الحصول على المبتغى الذي من أجله عرفت النور.

## خلاصة الفصل الثاني

ركزت الدراسة في فصلها الثاني على كيفية تنظيم الدفاع السيبراني في المغرب والجزائر وذلك عبر مبحثين؛ تناولت في المبحث الأول البعد التنظيمي من زاوية بنيته التحتية. أما في المبحث الثاني، فركزت على البعدين المؤسسي والتعاوني، الإقليمي والدولي، للدفاع السيبراني في المغرب والجزائر.

سعت الدراسة في مبحثها الأول، إلى التطرق إلى البنية التحتية للدفاع السيبراني في البلدين؛ لا على المستوى الوطني، ولا على المستوى الإقليمي والدولي. تبين أن البلدين معا يسعيان جاهدين لتحقيق ذاتهما في الفضاء السيبراني، ويتبنيان استراتيجيات أمنية على المستوى المحلي، الإقليمي والدولي وإن اختلفت في ما بينهما. كما أن للبلدين قوانين داخلية منظمة لحقلهما السيبراني. أما على المستوى الخارجي، وعلى غرار باقي دول العالم، لازالت القوانين الدولية لم تفعل بطريقة صريحة في الفضاء السيبراني بصفة عامة، وفي المجال السيبراني المغربي-الجزائري بصفة خاصة. فالعالم السيبراني بأسره يشكو الضبابية والعشوائية، وغياب القوانين الدولية المباشرة لفرملة الخروقات السيبرانية.

واعتمادا على المؤشرات العالمية في مجال تقييم مكافحة الهجومات السيبرانية، لا على الدراسات العشوائية المعتمدة من باحثي الجارة الجزائر الذين ما فتئوا يهاجمون المغرب بكونه هو من وراء الهجمات السيبرانية على منشآتهم الحيوية، تبين مدى تجاوز المغرب لجارته الجزائر في مجالات عدة للتنظيم السيبراني.

أما في المبحث الثاني، حاولت الدراسة التطرق إلى المؤسسات المحورية والاتفاقيات الهامة المؤطرة للمجال السيبراني في البلدين، لا على المستوى الوطني، ولا على المستوى الإقليمي أو الدولي.

استنتج كذلك مجموعة من الخبراء أن الجزائر تشكو قصورا في نظامها الدفاعي السيبراني، في حين نجد أن المغرب عزز قدراته الوطنية في هذا المجال. وحتى على المستوى الإقليمي أو الدولي، طور المغرب علاقاته مع مجموعة من المؤسسات الإقليمية والدولية؛ على سبيل المثال لا الحصر، علاقته مع حلف ناتو. لا ننسى كذلك، سعيه الدائم لربط اتفاقيات ثنائية مع دول رائدة في هذا المجال، كوريا الجنوبية وإسرائيل نموذجا.

وفي ما يتعلق بالاتفاقيات الإقليمية والدولية، نسجل تواجد المغرب في أغلبها، وحتى الجزائر. لكن ما يعاب على تلك الاتفاقيات، إذا ما استثنينا اتفاقية بودابيست، فهي اتفاقيات لم تثمر بعد في تأطير المجال السيبراني.

## خاتمة

تبين أن المغرب يضع أولويات استراتيجية مهمة لتعزيز دفاعه السيبراني، ومن بين تلك الأولويات نجد بالأساس؛ تقييمه للمخاطر التي تثقل كاهل نظام المعلومات داخل الإدارات، الهيئات العامة الرئيسية والبنية التحتية الحيوية. ونسجل كذلك سعيه الدائم لحماية تلك المؤسسات الحيوية عن طريق تعزيزه لأسس أمنه؛ المتمثلة أساسا في الإطار القانوني والتوعية والتدريب وتجويد البحث. وإحداثه لمؤسسات مختصة تسهر على حماية البلد ضد أي آفة سيبرانية. وأخيرا، بحثه الدائم والمستمر لتعزيز وتطوير التعاون الوطني والدولي[475].

كما تبين من الجانب الجزائري، أن الفاعلين الرسميين بالبلاد ما فتؤووا يحملون المغرب المسؤولية الأولى والأخيرة على أي هجوم سيبراني على مؤسساتهم الخاصة والعامة. لا ينحصر الأمر على الجهات الرسمية، بل يتعداها إلى الأكاديميين الجزائريين الذين يهاجمون المغرب بدون خبرة علمية، خصوصا وأن الهجمات السيبرانية يصعب إدراك منبعها الأصلي. فإذا كانت الدول ذات الباع العريض في هذا المجال تحتار في معرفة مصدر الهجمات السيبرانية التي استهدفتها، فما بالك بدول العالم الثالث-الجزائر واحدة منها- أن تتأكد من مصدر الهجمات السيبرانية عليها.

**استنتاجات**

**بالنسبة للمغرب،** ورغم جهوده المبذولة في إطار التعاون الدولي بهدف زيادة الوعي الوطني بالأمن السيبراني، نسجل عدم مساهمة تلك الجهود في تقريب المغرب من المؤشر العالمي لقياس قدرات الأمن السيبراني الذي وضعه الاتحاد الدولي للاتصالات، والذي يعتمد على خمس ركائز؛ قانونية تنبني على حتمية وجود مؤسسات وأطر قانونية، تقنية تقاس على أساس وجود مؤسسات تقنية وتنظيم برامج تحقيق الأمن، تنظيمية تقاس بضرورة وجود مؤسسات واستراتيجيات لتنسيق السياسات المعتمدة لتنمية الأمن السيبراني على المستوى الوطني، بناء القدرات والتي يتم قياسها على أساس وجود برامج البحوث، التطوير، التعليم،

[475]-Administration de la Défense Nationale, Stratégie nationale en matière de cyber sécurité, Op.cit, p.3.

التدريب للمهنيين المعتمدين ووكلاء النظامين العام والخاص، تعاونية تتأسس على وجود شراكات وأطر تعاونية وشبكات تبادل المعلومات داخليا وخارجيا[476].

**بالنسبة للجزائر**، تبين أنها حاليا ليست من بين البلدان التي تعطي الأولوية بما فيه الكفاية للأمن السيبراني[477]. ما يؤكد التأخر الجزائري في ميدان الدفاع السيبراني، المؤشرات العالمية في المجال السيبراني، والتي منحت الجزائر رتبا جد متأخرة، تقريبا في جميع الميادين التقنية المرتبطة بتقييم الفضاء السيبراني بدول العالم.

**توصيات الدراسة**

بناء على ما سبق من استنتاجات، يمكن الخروج بالتوصيات التالية؛ العالمية منها و الهادفة إلى تشجيع الدول، ومنها بالخصوص المغرب، على التعاون الدولي الرقمي، ومن أجل التزام الحكومات بتنفيذ المعايير اللازمة لحماية المدنيين على شبكة الإنترنيت في أوقات السلم، يدعو الكثير من الباحثين في مجال الأمن السيبراني إلى اعتماد معاهدات رقمية مماثلة لمعاهدة جنيف لعام 1949(اتفاقية جنيف الرقمية) المختصة في النزاعات المسلحة عقب انتهاء الحرب العالمية الثانية. في نفس الاتجاه، يدعو بعض الباحثين الآخرين إلى **إحداث منظمة محايدة مستقلة** تتبع معايير مستقلة، هدفها تحديد التهديدات السيبرانية، بحيث تملك القوة اللازمة للتحقيق، فتجبر الحكومات على نشر تقارير حول الثغرات الأمنية[478]. ولتحقيق هذا المبتغى يجب تكييف القوانين القديمة مع التقنيات السيبرانية الجديدة، رغم كون تلك العملية تعتبر صعبة بشكل خاص عندما يتعلق الأمر بالقانون الدولي الإنساني، لأنه ينظم حالات النزاع المسلح بشكل طبيعي ويثير مواقف متناقضة بين الدول. في الواقع، نادرًا ما تصل الدول بشأن مثل هذه الأمور إلى الإجماع اللازم التي تنص على الأحكام الرئيسية للقانون الدولي الإنساني. فالقانون يتطور ببطء، عكس وسائل وأساليب الحرب التي تتطور باستمرار وتكون ساحة المعركة سريعة التغيير. سد الفجوة الزمنية والسياقية بين اللحظة من تشكيل القانون ولحظة تطبيقه تصبح بذلك تحدٍ متزايد باستمرار وأكثر إلحاحًا. مما يجب

[476]-يوسف عنتار، الأمن الرقمي المغربي في ظل تنامي الاعتداءات السيبرانية، مرجع سابق، ص.27.

[477]-Zoltán Sipos, Cybersecurity in Algeria, Op.cit, p.71.

[478]- يوسف عنتار، المرجع نفسه، ص.25.

الاشتغال عليه لتجسير تلك الفجوة والربط بين القانون المنظم والتطور السريع لميدان المواجهة[479].

**ولاكتساب المناعة السيبرانية لذا المغرب، لابد من التركيز على المزيد من التعاون الإقليمي والأورومتوسطي:**

تمّ دمج منطقة شمال أفريقيا في الجهود الإفريقية في مجال المناعة السيبرانية، إذ تعتبر اتفاقية مالابو 2014 ركيزة مهمة لدعم الأمن السيبراني. وتمت الموافقة على استراتيجية للأمن السيبراني والجرائم السيبرانية في أفريقيا في عام 2016 من قبل وزراء الاتصالات الأفارقة. وفي عام 2018 عقد الاتحاد الإفريقي (AU) مؤتمراً سنويّاً حول الأمن السيبراني، بالتعاون مع مجلس أوروبا، مع الأخذ في الاعتبار أنّ الأمن السيبراني جزء من استراتيجية أفريقيا2063[480].

كما تم إحراز تقدم في التعاون الثنائي والإقليمي في منطقة الشرق الأوسط وشمال أفريقيا في مجال بناء القدرات. وقد لعب المركز الإقليمي العربي للأمن السيبراني التابع للاتحاد الدولي للاتصالات ( ITU-ARCC ) دوراً في هذا الشأن، بالإضافة إلى مبادرات التعاون بين المنطقة والاتحاد الأوروبي مثل مبادرة سايبر ساوث أو مبادرة الاتحاد الأوروبي سايبردايركت ( Cyber Direct). وتُعَدّ الحوسبة السحابية، ومراكز البيانات، وتطبيقات المدن الذكية فرصاً مهمة أيضاً للتعامل مع مختلف المخاطر والتحديات[481].

ومع ذلك ورغم كل تلك المجهودات، هناك حاجة ملحة إلى مزيد من التعاون الإقليمي لإنشاء أنظمة جديدة للكابلات البحرية ومراكز البيانات وتحديث البنية التحتية، وكذلك لزيادة قدرة اتصالات النطاق العريض، وإدارة ازدحام الشبكة، وضمان استمرارية الخدمات العامة الحيوية، وتعزيز التقنيات المالية الرقمية. وقد أظهرت أزمة كورونا أنه لا يمكن تجاوز أصحاب المصلحة المتعددين على المستويين الوطني والعالمي إلا من خلال العمل المشترك، وتبادل المعرفة، وتعبئة الموارد، وتبادل المعلومات، والتعاون والتنسيق الدوليين من أجل

---

[479]-Eitan Diamond, Applying International Humanitarian Law to Cyber Warfare, **JSTOR,** Institute for National Security Studies, 2014, link: http://bitly.ws/Eker, seen on: 10.05.2023.

[480]-عادل عبد الصادق، الملحق :الرقمنة والمناعة السيبرانية، **المعهد الأوروبي للبحر الأبيض المتوسط**، إسبانيا، العدد 22، يوليوز 2021، ص ص، 83-84.

[481]-المرجع نفسه.

بناء المناعة والقدرة على الصمود في مجال الفضاء السيبراني. يجب على شمال أفريقيا والاتحاد الأوروبي تطوير" استراتيجية الأمن السيبراني لعموم أوروبا والبحر الأبيض المتوسط" (PEMCS)، ليس فقط للقطاع العام والبنى التحتية الحيوية، بل لمساعدة المشغلين الاقتصاديين والقطاع الخاص في مواجهة التحديات المتزايدة في التهديدات السيبرانية أيضاً. ويجب أن تُشكّل منطقة الاتحاد الأوروبي وشمال أفريقيا كتلة اقتصادية رقمية، وأن تنشئ رابطة بين فِرَق الاستجابة للطوارئ الحاسوبية في كلتا المنطقتين. وأخيراً، يمكن للاتحاد الأوروبي – من خلال شراكة مع منظمة التعاون الرقمية (DCO) الجديدة – تطوير الاقتصاد الرقمي في منطقة شمال أفريقيا، وتحقيق أهداف التنمية المستدامة لعام 2030[482].

بالإضافة إلى ما سبق، وجب على صانعي السياسات العامة إعطاء الأولوية لجمع البيانات واعتبارها خطوة ضرورية لتقييم مخاطر الجرائم السيبرانية. كذلك، يؤكد جل الخبراء على ضرورة تعزيز المشاركة الشاملة للقطاع الخاص والمجتمع المدني في صياغة السياسات العامة السيبرانية ورصدها. كما أنه يجب تعزيز قدرات منطقة شمال إفريقيا من خلال الشبكات القائمة، وإعطاء الأولوية للصحة السيبرانية في منطقة شمال إفريقيا؛ عن طريق توعية المستخدمين بمخاطر الأنترنت من خلال حملات تحسيسية، تدريبات إلكترونية، مسابقات الأمن السيبراني، مشاركات في يوم الأنترنت الآمن. ويجب أن تتسم تلك الحملات بالدوام والاستمرارية[483].

كذلك، من بين التوصيات الأساسية التي لا يجب إغفالها؛ أولاً، لكي تعتبر حملة الدفاع السيبراني فعالة، يجب أن يراها أكبر عدد ممكن من الأشخاص. ثانيًا، بالإضافة إلى الرؤية، يوصى بإجراء تقييم أفضل لاحتياجات العملاء وتوقعاتهم فيما يتعلق بالأمن عبر الإنترنت. سوف تسمح هذه البيانات لمواءمة رسائل الحملة بشكل صحيح مع الاحتياجات الحقيقية المعبر عنها. ثالثا، يجب أن تستخدم حملة الوقاية وسائل بسيطة، أو نصائح كلاسيكية و سهلة الفهم لدى الجميع (عرض، وثائق عبر الإنترنت). رابعا، بما أن حملات الوقاية التفاعلية غير شائعة، قد يثير هذا فضول الأفراد ويقودهم إلى الحديث عنها مع من حولهم، وهذا يشكل نقطة إيجابية لتعميم الفائدة على نسبة كبيرة من الناس. خامسا، بالإضافة إلى الوسائل

[482]-عادل عبد الصادق، الملحق :الرقمنة والمناعة السيبرانية، مرجع سابق، ص ص،83-84.
[483]-ألكسندرا ماريون يمنى لبن، الاقتصاد الرقمي والجرائم السيبرانية، مرجع سابق، ص ص،27-28.

المستخدمة لنقل المعلومات، من المفيد مراجعة تنوع الموضوعات التي تتناولها الحملة، حتى لا تكون الحملة ضيقة الجوانب. سادسا وأخيرا، يجب أن تهدف حملات الوقاية بشكل أساسي إلى إعلام العملاء والجمهور حول وسائل الحماية المتاحة لهم وتوعيتهم بأهمية استخدامها[484].

كذلك، إذا ما تعلق الأمر بالجانب الأمني الذي يتسم بطابع التمدد إذا ما وجد بيئة مساعدة لذلك، فالوضع في الإقليم المغاربي بات يستدعي ضرورة إيجاد سياسة أمنية مشتركة، تمكن دول المنطقة من التعاطي الفعال والمثمر للجهود المبذولة في هذا الشأن وتمكينها في إطار تكاملي من بلوغ الهدف الرئيسي لاستقرار المنطقة، وبذلك يكون دور التكامل في بعث الاستقرار الأمني دافعا آخر لتفعيل العمل التكاملي في جوانبه المعطلة بالمنطقة[485].

ولإحراز تعاون دولي، ومن ضمنهم المغرب، في مجال مكافحة الجريمة السبرانية يجب تحقيق مظهرين، المظهر الأول يتعلق بضرورة التعاون في إنفاذ القانون لملاحقة ومتابعة ومعاقبة المجرمين بعد ارتكاب الجريمة والتي تعتبر اختصاصات قضائية متعددة ذات نظم قانونية مختلفة، ويتمثل في التعاون القضائي[486]. ففعالية التحقيق والملاحقة القضائية في الجرائم السيبرانية غالبا ماتقتضي تتبع أثر النشاط الإجرامي عبر مجموعة متنوعة من خدمات الإنترنت، أو الشركات المقدمة لتلك الخدمات. قد يتطلب تحديد مصدر الجريمة اعتماد أجهزة إنفاذ القانون على السجلات التاريخية التي تبين متى أجريت تلك التوصيلات ومن أين ومن الذي أجراها. وعندما يكون مقدمو الخدمات خارج نطاق الولاية القضائية للمحقق وهو ما يحدث غالبا، فإن أجهزة إنفاذ القانون تكون بحاجة إلى مساعدة من نظرائها في ولايات قضائية أخرى؛ بمعنى الحاجة إلى ما يسمى التعاون القضائي[487].

---

[484]-Cameron Coutu, La prévention de la cybercriminalité: résultats d'une enquête sur les effets perçus d'une campagne de prévention réalisée par une institution financière, Mémoire de l'obtention du grade de Maîtrise ès sciences (M.Sc) en criminologie, Université de Montreal, Ecole de criminologie, Faculté des arts et des sciences, 01.08.2019, pp.80-83.

[485]-سعيدي ياسين، التحديات الأمنية الجديدة في المغرب العربي، مرجع سابق، ص.147.

[486]-مراد مشوش، الجهود الدولية لمكافحة الإجرام السيبراني، مرجع سابق، ص.702.

[487]-محمد علي محمد التوني، استراتيجية مكافحة الهجمات السيبرانية، مرجع سابق، ص.111.

أما المظهر الثاني من مظاهر التعاون الدولي في مجال مكافحة الإجرام السبراني فهو التعاون الفني، إذ لا يقتصر هذا التعاون الدولي على المساعدة القضائية المتبادلة فحسب، وإنما يشمل كذلك المساعدة التقنية وتبادل الخبرات بين الدول[488]. هذا التعاون الدولي يمكن من خلاله إيجاد الإجابات على الشرطين الأساسيين، اللذين بتحقيقهما يمكن أن يقع الهجوم السيبراني تحت القانون الدولي ويؤدي إلى البحث عن المسؤولية. الشرط الأول يرتبط بتحديد الجاني: هل الهجوم السيبراني الذي ارتكبه فرد أو تدعمه دولة ؟. أما الشرط الثاني، فيتمثل في تحديد طبيعة هذا الهجوم: هل الهجوم مشابه لعدوان بالمعنى المقصود في القانون الدولي أم فقط فعل منعزل[489].

بالإضافة إلى ما ذكر، لابد من الاعتماد على طرق علمية للقيام بدراسات استشرافية حول مخاطر الهجومات السيبرانية المحدقة بالمغرب. ومن بين الطرق المحكمة للقيام بتحليلات استراتيجية نجد طريقة (SWOT analysis)، لدراسة نقاط القوة والضعف في البيئة الداخلية، وكذلك نقاط الفرص والتهديدات في البيئة الخارجية –لغرض معالجتها أو التقليل منها، لرفع كفاءة أداء المنظومة الأمنية السيبرانية، وإمكانية التنبؤ بكافة الفرص المتاحة لها. هذه التحليلات الاستراتيجية يجب أن تهتم بالبعد التعليمي، من خلال إدراج أنظمة مكافحة الجرائم السيبرانية ضمن المناهج التعليمية. يجب كذلك أن لا تغفل البعد الأمني لحماية البنية التحتية الرقمية. ومن الأولويات، استحضار البعد التقني وكيفية مجابهة تلك التحديات السيبرانية باستخدام تقنيات وبرامج حماية متقدمة للبريد الإلكتروني وللحسابات الرسمية، تطوير برمجيات المقاومة، عمل شفرات لاكتشاف الهجمات المحتملة وتتبعها، تشفير البيانات والمعلومات الحساسة والتركيز على التقنية السحابية، التدريب المستمر للكوادر الفنية، عقد ورشات تدريبية وباستمرار عن الذكاء السيبراني الاستراتيجي وكيفية توظيفه في جميع قطاعات الدولة الحيوية، لتقليل مخاطر التهديدات السيبرانية المحتملة. لاننسى البعد الإعلامي، فدوره مهم، يتمثل في التوعية والتصدي لتلك الجرائم، من خلال استضافة المتخصصين والخبراء في هذا المجال، التوعية الدائمة لمستخدمي المنصات

[488]-مراد مشوش، الجهود الدولية لمكافحة الإجرام السيبراني، مرجع سابق، ص.702.

[489]-Abderrahman BELGOURCH et autres, Le cyberspace Diversité des menaces & difficultés de régulation, Op.cit, pp. 222-223.

الرقمية بالطرق التي يمكن للقراصنة اختراق الأنظمة والبيانات الحساسة والكشف عن الأساليب والحيل والتكتيكات المستخدمة. أما البعد التشريعي، فيبقى من الأولويات التي يجب أن تواكب وتتغير باستمرار مع تغير تلك التهديدات والمخاطر السيبرانية. والبعد الأهم، يبقى البعد الدولي، الذي يتطلب استحضار مجموعة من الآليات التي يجب مراعاتها على الصعيد الدولي، والتي من شأنها الحد والتقليل من انتشار تلك الجرائم، من بين تلك الآليات عقد شراكات واتفاقيات دولية في حماية البنى المعلوماتية العالمية وإنشاء مركز دفاع دولي، التعاون القضائي المشترك بين الدول ووضع تدابير قانونية دولية من سن قوانين مشتركة للتعامل مع تلك الجرائم والحفاظ على الاستقرار والأمن الدولي، عقد مؤتمرات وندوات دولية لمناقشة الأمن السيبراني وتقييم التجارب السابقة في مكافحة الهجمات السيبرانية، وإنشاء هيئة استخبارات دولية لجمع وتبادل المعلومات الاستخباراتية عن الهجمات السيبرانية المحتملة. التعزيز الدولي لمعايير البنية التحتية، وتبادل المعلومات عن التهديدات السيبرانية ووضع عقوبات دولية لردع منفذي تلك الهجمات. التدريب الدولي المشترك والوقوف على أحدث التكتيكات وامتلاك المعارف حول التدابير الوقائية المختلفة للحد من تلك الجرائم وحماية المعلومات الحساسة[490].

لاننسى كذلك، أنه لمواجهة الآثار الضارة للهجمات السيبرانية ووضع سياسة دفاع سيبرانية ذات مصداقية وذات صلة ، يُنصح بمراجعة الاستراتيجيات المعمول بها باستمرار ومواءمتها مع الإطار التنظيمي لتحقيق اتساق أفضل. في الواقع، يعمل الدفاع السيبراني المبني على إطار سياسي واقتصادي متين بمثابة ناقل للازدهار الاقتصادي. الانتعاش الاقتصادي القائم على التقنيات الجديدة من خلال إنشاء ميزانية مخصصة لهذه القضية. التكاليف المرتبطة بالهجوم أكبر من الميزانية اللازمة للتعامل معه. وبالمثل، ينبغي النظر في احتمالية الاستثمار العام. بالإضافة إلى ذلك، هناك حاجة للاستثمار في أسواق الأمن السيبراني. هذه الأسواق تنمو وتخلق فرص عمل، والاستثمار في ثقافة الفضاء السيبراني

[490]-أميرة محمد محمد سيد، استراتيجيات مكافحة الجرائم الإلكترونية في العصر المعلوماتي تعزيزا لرؤية مصر 2030: دراسة استشرافية، **مجلة البحوث الإعلامية**، سلسلة مؤلفات وأعمال جامعة الأزهر، كلية الإعلام، مصر، العدد 58 - الجزء الرابع، يوليو 2021، ص ص،1793-1803.

داخل الشركات وبين الوكلاء الاقتصاديين. وتوجيه طلاب المستقبل لمتابعة دراساتهم في مجال الأمن السيبراني[491].

أما التوصية الأخيرة، والتي تبدو أهم توصية يمكن الاشتغال عليها والعمل على تنفيذها، فهي إعادة **ربط جسر التواصل بين دول المغرب العربي بصفة عامة، و بين المغرب والجزائر بصفة خاصة**. كانت محاولة لإنشاء اتحاد المغرب العربي، في 17 فبراير 1989، وهي منظمة سياسية اقتصادية تتألف من الجزائر والمغرب وليبيا وتونس وموريتانيا، سرعان ما أجهضت تلك المحاولة، نتيجة التفككات الحاصلة بين عناصر هذا الائتلاف، خصوصا بين المغرب والجزائر. فالجارة الجزائر لا تولي اهتماما لحسن الجوار بخرجاتها غير المبررة تجاه المغرب؛ ففي مارس 2021، بدأت مواجهتها الإعلامية ضد المغرب، عبر وسائل الإعلام، متهمة إياه باستخدام تهريب المخدرات كوسيلة لزعزعة الاستقرار. وفي الشهر نفسه، منعت الجزائر الفلاحين المغاربة من فجيج من عبور الحدود، وبالتالي الاستفادة من استغلال بساتين النخيل الجزائرية. في 18 يوليوز 2021، اتهمت المغرب باستخدام برنامج "Pegasus"، بغرض التجسس على الصحفيين وكذلك على الشخصيات السياسية والعسكرية الجزائرية، مما يعقد الروابط بين الطرفين مرة أخرى. من جهته، المغرب لا يجاري التصرفات الجزائرية، بل بالعكس يمد يد المصالحة لها، وهذا ماوقع بمناسبة "عيد العرش" في 30 يوليو 2021، حيث حاول محمد السادس دون جدوى تهدئة الأزمة مع الجزائر، مشيدًا بفرصة تحسين العلاقات الثنائية وكذلك إمكانية إعادة فتح الحدود المغلقة منذ أحداث مراكش عام 1994[492].

في نهاية المطاف، فالمغرب والجزائر في مأزق جيوسياسي ودبلوماسي له عواقب وخيمة على اقتصادات البلدين واستقرار منطقة المغرب العربي. وتبقى المصالحة الجزائرية المغربية هي الأمل الوحيد للخروج من هذا المأزق. يجب أن تتغلب السلطات الجزائرية المغربية على هذه المواجهة التاريخية من أجل خلق تعاون أمني واقتصادي على حد سواء،

[491]-M.MOUHIR& Mme.MOKHTAR, Stratégie de Cyber défense marocaine: du public au privé, enjeux et perspectives, Op.cit.

[492]-Edouard Yziquel, Evolution du rapport de forces entre l'Algérie et le Maroc, **Ecole de Guerre Economique**, 25.11.2021, lien de l'article: http://bitly.ws/GEnZ, date visite : 02.06.2023.

وتعزيز التنمية الإقليمية، التي تنطوي على إمكانات كبيرة، دون الوقوع في "فخ ثيوسيديدس[493]،[494] . وبناء على هذا التعاون يمكن التخفيف من الهجمات السيبرانية بينهما، بل يمكن خلق تعاون بناء بينهما للقضاء على الهجمات السيبرانية الدولية المهددة لاستقرارهما الأمني.

**انفتاح**

تواجه البيئة الدفاعية اليوم تهديدات جديدة، تهديدات مرتبطة بالفضاء السيبراني، لهذا السبب بات لزاما إيجاد منظومة دفاعية قوية لمواجهة هذا المتحدي الجديد. منظومة تعتمد على تعاون إقليمي ودولي لحماية المجال السيبراني.

فقد أضحى واجبا على جميع الدول الالتزام والانخراط في ضمان احترام القانون الدولي الإنساني والقواعد القانونية الآمرة في القانون الدولي والتكفل بعدم انتهاكها. والنقطة المهمة التي تسترعي الاهتمام ويجب أن تحصل على اتفاق دولي تام،" تتمثل في واجب عزل البنية التحتية السيبرانية، التي يوجه من خلالها المشارك المباشر انتهاكاته، فضلا عن معاقبة مرتكب الانتهاك وفق مبدأ الاختصاص الشامل في القانون الجنائي، نظرا لخطورة هذه الانتهاكات وطبيعة الهجمات السيبرانية العابرة للحدود والأقاليم[495]".

---

[493]-مصيدة ثوسيديديس: المعضلة التي تواجه قوة مهيمنة ومعضلة صاعدة تهدد تلك الهيمنة. هل الحرب حتمية؟ عندما روى ثوسيديديس الحرب البيلوبونيسية، كتب عن حتمية أن تفكر سبارتا المهيمنة وأثينا الناشئة في المواجهة المسلحة كوسيلة لتسوية الصراع. حقيقة أن هاتين البوليستين اليونانيتين فكرتا بالضرورة في الحرب - وأخيراً شنتها - لا تعني أنه لم يكن لديهما خيارات أخرى. لقد أظهر التاريخ أن هناك بدائل أخرى: عندما هددت ألمانيا بالتغلب على القوة البحرية البريطانية ، أدت محاولة "sorpasso "مصحوبة بعدة ظروف إلى الحرب العالمية الأولى، ولكن عندما تجاوزت إسبانيا البرتغال في ممتلكاتها الخارجية في القرن السادس عشر، أو عندما حلت الولايات المتحدة محل بريطانيا كقوة رائدة في العالم في أواخر القرن التاسع عشر، كان نقل السلطة سلميًا.

(Emili J.Blasco, The prospect of war awaits the US and China-will they avoid it, link: http://bitly.ws/GEzb, seen on:02.06.2023).

[494]-Edouard Yziquel, Evolution du rapport de forces entre l'Algérie et le Maroc, Op.cit.

[495]-علي محمد كاظم الموسوي، المشاركة المباشرة في الهجمات السيبرانية، شركة المؤسسة الحديثة للكتاب، لبنان، ط1، 2019، ص ص،246-247.

## لائحة المراجع

- ✓ **باللغة العربية**
- ✓ **الكتب**


-إبراهيم أبراش، المنهج العلمي وتطبيقاته في العلوم الاجتماعية، دار الشروق للنشر والتوزيع، عمان الأردن، ط1، 2009.

-أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، منشورات زين الحقوقية والأدبية، بيروت، ط غ، 2018.

-أنور محمد فرج، نظرية الواقعية في العلاقات الدولية دراسة نقدية مقارنة في ضوء النظريات المعاصرة، مركز كردستان للدراسات الاستراتيجية، السليمانية، كردستان-العراق، ط غ، 2007.

-أميتاف أشاريا و باري بوزان، تشكيل العلاقات الدولية العالمية أصول حقل العلاقات الدولية وتطوره في ذكراه المئوية، ترجمة عمار بوعشة، سلسلة عالم المعرفة ، المجلس الوطني للثقافة والفنون والآداب، الكويت، عدد502، 2023.

-بيتر سينجر، هيجل مقدمة قصيرة جدا، ترجمة: محمد إبراهيم السيد، مؤسسة هنداوي للتعليم والثقافة، القاهرة، ط1، 2015.

-جوهر الجموسي، الافتراضي والثورة مكانة الإنترنت في نشأة مجتمع مدني عربي، المركز العربي للأبحاث ودراسة السياسات، الدوحة، ط 1، 2016.

-دارن بارني، المجتمع الشبكي، ترجمة أنور الجمعاوي، سلسلة ترجمان، المركز العربي للأبحاث ودراسة السياسات، بيروت، ط1، فبراير2015.

-دانيال فونتير، الاستراتيجية السيبرانية، ترجمة أيمن منير، سلسلة عالم المعرفة، المجلس الوطني للثقافة والفنون والآداب، الكويت، عدد 473، 2019.

-دحان حزام القريطي، الأمن السيبراني وحماية أمن المعلومات، دار الفكر الجامعي، الإسكندرية، ط1، 2021.

-شارل أندري جوليان، تاريخ إفريقيا الشمالية تونس، الجزائر، المغرب الأقصى، من البدئ إلى الفتح الإسلامي 647م، ترجمة محمد مزالي والبشير بن سلامة، مؤسسة تاوالت الثقافية، ليبيا، ط1،2011.

-عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، بنك المعرفة المصري، 2014، رابط الكتاب: http://bitly.ws/yvYJ

-علي الدين هلال ونيفين مسعد، النظم السياسية العربية قضايا الاستمرار والتغيير، مجلة الكتب العربية، رابط الكتاب:http://bitly.ws/KFiT

-علي محمد كاظم الموسوي، المشاركة المباشرة في الهجمات السيبرانية، شركة المؤسسة الحديثة للكتاب، لبنان، ط1، 2019.

-فرد كابلان، المنطقة المعتمة: التاريخ السري للحرب السيبرانية، ترجمة لؤي عبد المجيد، سلسلة عالم المعرفة، المجلس الوطني للثقافة والفنون والآداب، الكويت، عدد 470، 2019.

-عبد العزيز فيلالي، بحوث في تاريخ المغرب الأوسط في العصر الوسيط، دار الهدى-عين المليئة، الجزائر، ط غ، 2020.
-كمال المنوفي، مقدمة في مناهج وطرق البحث في علم السياسة، جامعة القاهرة، ط غ، 2006.
-محمد السامرائي، دور القانون الدولي في مكافحة الهجمات السيبرانية، الذاكرة للنشر والتوزيع، بغداد، ط1، 2023.
-محمد سويلمي، في الإسلام الرقمي كيف ارتحل المسلمون إلى الفضاء السيبراني، الدار التونسية للكتاب، تونس، ط 1،2021.
-محمد علي محمد التوني، استراتيجية مكافحة الهجمات السيبرانية، دار الفكر الجامعي، الإسكندرية، ط1، 2023.
-منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، 2016، رابط الكتاب: http://bitly.ws/DTBH

✓ **الأطاريح والرسائل الجامعية:**

-محمد الطاهر عديلة، تطور الحقل النظري للعلاقات الدولية: دراسة في المنطلقات والأسس، أطروحة لنيل شهادة دكتوراه العلوم في العلوم السياسية والعلاقات الدولية، فـرع العلاقات الدولية، جامعة الحاج لخضر- باتنة، كلية الحقوق والعلوم السياسية قسم العلوم السياسية، الجزائر، السنة الجامعية، 2014-2015.
-برج أسمهان وآخرون، الهجمات السيبرانية و أثرها على العلاقات السياسية الدولية- العلاقات الجزائرية المغربية نموذجا، رسالة لنيل شهادة الماستر في علوم الإعلام والاتصال وعلم المكتبات، جامعة 8 ماي 1945 قالمة، كلية العلوم الإنسانية والاجتماعية، الجزائر،2021-2022.
-حنين جميل أبو حسين، الإطار القانوني لخدمات الأمن السيبراني (د راسة مقارنة)،رسالة لنيل شهادة الماستر في ميدان القانون الخاص، جامعة الشرق الأوسط، كلية الحقوق، الأردن، 2020-2021.
-سعيدي ياسين، التحديات الأمنية الجديدة في المغرب العربي، رسالة لنيل شهادة الماستر في العلوم السياسية والعلاقات الدولية، جامعة وهران محمد بن أحمد 2، كلية الحقوق والعلوم السياسية، الجزائر، السنة الجامعية، 2015-2016.
-شعيب قاسمي وفؤاد بلغيث، الاستراتيجيات الدولية في مكافحة الجريمة السيبرانية-دراسة حالة الجزائر-، رسالة لنيل شهادة الماستر في العلوم السياسية والعلاقات الدولية، جامعة العربي التبسي-تبسة-، كلية الحقوق والعلوم السياسية، الجزائر، السنة الجامعية 2019-2020.
-صلاح حيدر عبد الواحد، حروب الفضاء الالكتروني دراسة في مفهومها وخصائصها وسبل مواجهتها، رسالة لنيل شهادة ماستر، جامعة الشرق الاوسط، كلية الآداب والعلوم ،الأردن، السنة الجامعية،2021- 2020.
-فريدة طاجين، تأثير القوة السيبرانية على الاستراتيجيات الأمنية للدول الكبرى دراسة حالة - الصين، رسالة لنيل شهادة الماستر في ميدان الحقوق و العلوم السياسية، جامعة قاصدي مرباح ورقلة، كلية الحقوق و العلوم السياسية- قسم العلوم السياسية ، الجزائر، السنة الجامعية، 2017-2018.

-قسوم سليم، الاتجاهات الجديدة في الدراسات الأمنية دراسة في تطور مفهوم الأمن عبر منظارات العلاقات الدولية، رسالة لنيل شهادة الماستر في العلوم السياسية والعلاقات الدولية، جامعة الجزائر، كلية العلوم والإعلام قسم العلوم السياسية والعلاقات الدولية، الجزائر، السنة الجامعية، 2009-2010.

-نورة العقون، واقع الفضاء السيبراني و إشكالية الدفاع الوطني في الجزائر، رسالة لنيل شهادة الماستر في ميدان الدراسات الأمنية والاستراتيجية، قسم العلوم السياسية، جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية، الجزائر،2018-2019.

✓ **المجلات**

-ألكسندرا ماريون يمنى لبن، الاقتصاد الرقمي والجرائم السيبرانية ، الترجمة من الإنجليزية: رجائي برهان، المعهد الأوروبي للبحر الأبيض المتوسط، إسبانيا، العدد 22، يوليوز 2021.

-أميرة محمد محمد سيد، استراتيجيات مكافحة الجرائم الإلكترونية في العصر المعلوماتي تعزيزا لرؤية مصر 2030: دراسة استشرافية، مجلة البحوث الإعلامية، سلسلة مؤلفات وأعمال جامعة الأزهر، كلية الإعلام، مصر، العدد 58 - الجزء الرابع، يوليوز 2021.

-باتريك باولاك وآخرون، توقعات كبيرة: تعريف أجندة الأمن السيبراني عبر البحر الأبيض المتوسط، الترجمة من الإنجليزية: رجائي برهان، المعهد الأوروبي للبحر الأبيض المتوسط، إسبانيا، العدد 22، يوليوز 2021.

-بن تغري موسى، الحرب السيبرانية والقانون الدولي الإنساني، منصة المجلة العلمية الجزائرية، الجزائر، العدد02، 2020.

-بوبكر سبيك وآمال برقية، الأمن السيبراني.. الجيل الجديد من التحديات الأمنية، مجلة الشرطة، المديرية العامة للأمن الوطني المغربي، العدد 42، 2021.

-تغريد صفاء و لبنى خميس مهدي، أثر السيبرانية في تطور القوة، مجلة حمورابي، العراق، العدد 33-34، 2020.

-حنينة رجوح، الشراكة الجزائرية الصينية على ضوء مبادرة الحزام والطريق :المكاسب والمخاطر، مجلة السياسة العالمية، الجزائر،العدد1، 2022.

-سارة محمد روحي فتحي غزال، الأمن السيبراني ودرجة وعي المؤسسات بأهميته، المجلة العربية للنشر العلمي، مركز البحث وتطوير الموارد البشرية رماح ، الأردن، العدد 47، 2022.

-عادل عبد الصادق، الملحق :الرقمنة والمناعة السيبرانية، المعهد الأوروبي للبحر الأبيض المتوسط، إسبانيا، العدد 22، 2021.

-عبد الواحد البيدري، استراتيجية الأمن السيبراني: دراسة حالة المغرب، مجلة الدراسات الاستراتيجية والعسكرية، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين، ط1، 2021.

-مراد مشوش، الجهود الدولية لمكافحة الإجرام السيبراني، مجلّة الواحات للبحوث و الدراسات، سلسلة مؤلفات وأعمال جامعة غرداية، الجزائر، العدد 2، 2019.

-مريم لوكال، قراءة في اتفاقية الاتحاد الأفريقي حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة 2014، مجلة الدراسات القانونية والاقتصادية، سلسلة مؤلفات وأعمال جامعة امحمد بوقرة، بومرداس، الجزائر، 2021.

-مهدي رضا، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري، مجلة إيليزا للبحوث والدراسات، الجزائر، العدد 02،2021.

-سيدي محمد الأمين الراظي، الجريمة السيبرانية وتكاملية النص الوطني، الإقليمي و الدولي، مجلة القانون والأعمال الدولية، سلسلة مؤلفات وأعمال جامعة الحسن الثاني، المغرب، العدد 23، 2019.

-يوسف بوغرارة، الأمن السيبراني :الاستراتيجية الجزائرية للأمن و الدفاع في الفضاء السيبيري، مجلة الدراسات الأفريقية وحوض النيل، المركز الديمقراطي العربي، برلين، العدد 03، 2018.

-ياسين مليح، السيادة الرقمية ... تجلياتها وممكنات تحقيقها بالمغرب، مجلة الشرق الأوسط للدراسات القانونية والفقهية، سلسلة مؤلفات وأعمال جامعية، جامعة الحسن الأول، سطات، العدد36، 2021.

-يوسف عنتار، الأمن الرقمي المغربي في ظل تنامي الاعتداءات السيبرانية، المجلة المغربية للدراسات الدولية والاستراتيجية، المغرب، العدد 01، 2019.

✓ **المقالات**

-إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، **مصداقية**، 01.12.2019، رابط المقال: http://bitly.ws/zEZq.

-أمين النية، الأمن في السياسة الخارجية المغربية، **أكاديميا العربية**، 01.01.2020، رابط المقال: https://bitly.ws/wp3z

-آيات محمد سعود، شرط مارتينز في القانون الدولي الانساني، **الحوار المتمدن**، 09.03.2018، رابط المقال: http://bitly.ws/I6eB

-إيهاب خليفة، الحالة السيبرانية في نظريات العلاقات الدولية: الحاجة إلى مراجعة جديدة، **مركز المعلومات واتخاذ القرار-رئاسة مجلس الوزراء**، مصر،02.12.2021، رابط المقال: http://bitly.ws/CibV

-المختار شعالي، نظرية المعرفة عند كانط، **هسبريس**،01.04.2017، رابط المقال: http://bitly.ws/nmQa

-جمال بوازدية، الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية "التحديات والآفاق المستقبلية"، **مجلة العلوم القانونية والسياسية**، 03.02.2019، رابط المقال: http://bitly.ws/zEBs

-جلال فضل محمد العودي، مقالات في الجريمة السيبرانية، **الأمن الإلكتروني**، 21غشت 2022، رابط المقال، http://bitly.ws/EuCB

-حيدر فالح زايد، ا لنظرية النقدية، رابط المقال:http://bitly.ws/zcco

-سعيدة شريف، المغرب والجزائر... من الجوار الصعب إلى الحرب الإلكترونية، 15.01.2023، **رصيف22**، رابط المقال: http://bitly.ws/FFno.

-سمير قط، خصوصية الشراكة الأطلسية – المغاربية في إطار الحوار المتوسطي للحلف، **أكاديميا العربية**، رابط المقال : https://bitly.ws/wph2.

-صباح بالة، مدرسة ويلز (أبريستويث) للدراسات الأمنية، **الموسوعة السياسية الجزائرية**، 09.12.2022، رابط المقال:http://bitly.ws/EUF8

-عادل عبد الصادق، أنماط الحرب السيبرانية وتداعياتها على الأمن العالمي، **السياسة الدولية**، 14.05.2017، رابط المقال: http://bitly.ws/zjn6

-عبد الغفار عفيفي، الأزمات والحروب السيبرانية...تهديدات تتجاوز الفضاء الإليكتروني، **مجلة الأهرام للدراسات السياسية والاستراتيجية**، 2019/02/03، رابط المقال: Https://acpss/ahram.org.eg

-عبد الوهاب كريم، الأمن السيبراني-القيود والتحديات في ضوء قواعد القانون الدولي، 05.11.2021، رابط المقال: http://bitly.ws/D3te

-عثمان تالمة، تشكيل المجلس الأعلى للأمن على ضوء أزمة كوفيد – 19، **مجلة القانون والأعمال الدولية**،15.04.2020، رابط المقال: http://bitly.ws/FZjS

-عاطف قدادرة، الشارع الجزائري يرفض تكليف ناطق باسمه والمجلس الأعلى للأمن" يتخذ قرارات"، **عربية Independant**، 09.03.2021، رابط المقال: http://bitly.ws/FZq2

-عايدة عبد الحميد عبد الرحمن، نظرية المعرفة عند كانط، **بنك المعرفة المصري**، 2017، رابط المقال: http://bitly.ws/EUvt

-قطاف سليمان، مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية، **مختبر البحث في الحقوق والعلوم السياسية**-جامعة عمار ثليجي الأغواط، الجزائر، 03.05.2022، رابط المقال: http://bitly.ws/D6K3

-كريمة الهلالي، التعاون الأمني بين المغرب والاتحاد الأوروبي، **أكاديميا العربية**، رابط المقال: https://bitly.ws/wPxl

-محمد زاوي، نظرية دوغين.. أي موقع للمغرب في فكرة أوراسيا؟، **هوية بريس**، 09.10.2022، رابط المقال: http://bitly.ws/xTR5

-منعم أمشاوي، المجلس الأعلى للأمن القومي بالمغرب: دراسة على ضوء التجارب المقارنة، **مجلة البحثية**، 2017، رابط المقال: http://bitly.ws/DJPw

-محمد مسعد حيمد و مصطفى جاد الحق مصفى، رؤية استراتيجية لمكافحة الجرائم السيبرانية :اليمن دراسة حالة، **المجلة العربية الدولية للمعلوماتية**، 2019، رابط المقال: http://search.mandumah.com/Record/1060613

-محمد الذنيبات وآخرون، تصنيف حوادث الأمن السيبراني، **الذنيبات للمحاماة والخدمات القانونية**، 2019، رابط المقال: http://bitly.ws/Edry

-مروة خليل محمد مصطفى، القدرة التفسيرية للنظرية الليبرالية في عامل متغير "دراسة تقويمية"، 2021، رابط المقال: http://bitly.ws/zdco.

✓ **الخطب الرسمية**

-الخطاب الملكي بتاريخ 30 يوليوز2022، مناسبة عيد العرش، رابط الخطاب: http://bitly.ws/KFNo

✓ **النصوص القانونية**

-القانون رقم 07.03 المتعلق بجرائم نظم المعالجة الآلية، الصادر بتنفيذه الظهير الشريف رقم 1.03.197بتاريخ 16 من رمضان1424 الموافق ل11 نوفمبر2003، والمنشور بالجريدة الرسمية عدد5171، الصادرة بتاريخ 27 شوال 1424 الموافق ل 22 ديسمبر 2003.

-القانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية، الصادر بتنفيذه الظهير الشريف رقم 1.07.129بتاريخ 19من ذي القعدة 30 الموافق ل 1428 نوفمبر2007، والمنشور بالجريدة الرسمية عدد5584، الصادرة بتاريخ 25 ذو القعدة 1428 الموافق ل 6 ديسمبر 2007.

-القانون رقم 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، الصادر بتنفيذه الظهير الشريف رقم 1.09.15 بتاريخ 22 من صفر 1430 الموافق ل 18فبراير 2007، والمنشور بالجريدة الرسمية عدد5711، الصادرة بتاريخ 27 صفر 1430 الموافق ل 23 فبراير 2009.

-القانون رقم 31.08 المتعلق بتحديد تدابير لحماية المستهلك، الصادر بتنفيذه الظهير الشريف رقم 1.11.03 بتاريخ 14 من ربيع الأول 1432 الموافق ل 18فبراير 2011، والمنشور بالجريدة الرسمية عدد5932، الصادرة بتاريخ 03 جمادى الأولى 1432 الموافق ل 07 أبريل 2011.

-القانون رقم 13-88 المتعلق بالصحافة والنشر، الصادر بتنفيذه الظهير الشريف رقم 1.16.122 بتاريخ 6 من ذي القعدة 1437 الموافق ل 10 يوليوز 2016، والمنشور بالجريدة الرسمية عدد 6491، الصادرة بتاريخ 11 ذي القعدة 1437 الموافق ل 15 يوليوز 2016.

-القانون رقم 136.12 الموافق بموجبه على اتفاقية الجرائم المعلوماتية، الموقعة ببودابست في23 نوفمبر2001 وعلى البروتوكول الإضافي لهذه الاتفاقية، الموقع بستراسبورغ في 28 يناير2003، الصادر بتنفيذه الظهير الشريف رقم 1.14.85 بتاريخ 12 من رجب 1435 الموافق ل 12ماي 2014، والمنشور بالجريدة الرسمية عدد6260، الصادرة بتاريخ 29 رجب 1435 الموافق ل 29 ماي 2014.

-القانون رقم 79.12 المتعلق بحقوق المؤلف والحقوق المجاورة، الصادر بتنفيذه الظهير الشريف رقم 1.14.97 بتاريخ 20 من رجب 1435 الموافق ل 20ماي 2014، والمنشور بالجريدة الرسمية عدد6263، الصادرة بتاريخ 11 شعبان 1435 الموافق ل 09 يوليوز 2014.

-القانون رقم 121.12 المتعلق بالبريد والمواصلات، الصادر بتنفيذه الظهير الشريف رقم 1.19.08 بتاريخ 18 من جمادى الأولى 1440 الموافق ل 25 يناير 2019، والمنشور بالجريدة الرسمية عدد6753، الصادرة بتاريخ 12 جمادى الآخرة 1440 الموافق ل 18 فبراير 2019.

-القانون رقم 05.20 المتعلق بالأمن السيبراني، الصادر بتنفيذه الظهير الشريف رقم 1.20.69بتاريخ 04 من ذي الحجة 1441 الموافق ل 25 يوليو 2020، والمنشور بالجريدة الرسمية عدد6904، الصادرة بتاريخ 09 ذي الحجة 1441 الموافق ل 30 يوليوز 2020.

✓ **الاتفاقيات الدولية**

-جامعة الدول العربية، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، القاهرة جمهورية مصر العربية، 21.12.2010، رابط المقال: http://bitly.ws/yuxK.

✓ **ويبوغرافيا**

-محمد تيسير، المنهج المقارن في البحث العلمي، مؤسسة المجلة العربية للعلوم ونشر الأبحاث، 24.11.2022 ، رابط المقال: https://rb.gy/upppw.

✓ **مواقع المنظمات والجامعات**

-بوازدية جمال، الأمن السيبراني، محاضرات مقدمة لطلبة السنة الثانية ماستر، تخصص دراسات استراتيجية وأمنية، جامعة الجزائر-3-، كلية العلوم السياسية والعلاقات الدولية، الجزائر، السنة الجامعية: 2020–2021.

-القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة، ورقة موقف اللجنة الدولية للصليب الأحمر، 2019، اللجنة الدولية للصليب الأحمر، رابط المقال: http://bitly.ws/FWna.

## ✓ English references

### ✓ books

-Christopher D. DeLuca, The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors, Pace International law Review Online, Volume 3, Number 9, Winter 2013.

-Eitan Diamond, Applying International Humanitarian Law to Cyber Warfare, **JSTOR,** Institute for National Security Studies, 2014.

-Melissa Hathaway and Francesca Spidalieri, Kingdom of Morocco cyber readiness at a glance, Potomac Institute for Policy Studies, Virginia, United States, 2018.

-Miranda Grange, cyber warfare and the law of armed conflict, **Victoria University of Wellington**, 2014, link: http://bitly.ws/EkhW.

-Scott Burchill and others, Theories of International Relations, Palgrave Macmillan, Houndmills, Basingstoke, New York, Ed3, 2005.

-Rex Hughes, A treaty for cyberspace, 2 Blackwell Publishing Ltd, Oxford, The Royal Institute of International Affairs, International Affairs Journal, N° 86, 2010.

### ✓ Theses

-Col PEC Martin, Cyber warfare schools of thought: bridging the epistemological ontological divide, Master of defense studies, Canadien Forces College , Canada, 2015.

## ✓ Articles

-Abdelkader Cheref, Is Morocco's cyber espionage the last straw for Algeria?, 29.07.2021, link: http://bitly.ws/Dzec.

-"A European commission of inquiry acquits Morocco of using the spyware “Pegasus”", Breaking latest News, 18.06.2023, link: http://bitly.ws/IQpn.

-Alexander Seger, The Budapest Convention on Cybercrime: a framework for capacity building, 07.12.2016, **Global Forum on Cyber Expertise**, link: http://bitly.ws/FV4T.

-Algeria-NCSI, **National Cyber Security Index**, 26.04.2021, link: http://bitly.ws/Gi9d.

-Alvin Chang, "The Facebook and Cambridge Analytica scandal, explained with a simple diagram", **Vox**, 02.05.2018, link: http://bitly.ws/HGgT.

-Ana Torres-Garcia, US diplomacy and the North African ‘War of the Sands’ (1963), **The Journal of North African Studies**, 01.03.2013, link: http://bitly.ws/yWkg.

-Andrew Moravcsik, Taking Preferences Seriously: A Liberal Theory of International Politics, **Princeton.edu**, 1997, link: http://bitly.ws/zdpH

-ANTHONY J.S. CRAIG & BRANDON VALERIANO, Realism and Cyber Conflict: Security in the Digital Age, **Bristol**, England2018, seen on : 29.03.2023, link: http://bitly.ws/CgVT.

-Barak Ravid, New bill aims to boost cybersecurity cooperation between U.S., Abraham Accords nations, **Axios**, 31.05.2023, link: http://bitly.ws/GnJj.

-Bruna Martins dos Santos, Budapest Convention on Cybercrime in Latin America: A brief analysis of adherence and implementationin Argentina, Brazil, Chile, Colombia and Mexico", English Translation: Gonzalo Bernabó, May 2022, Derechos Digitales América Latina, link: http://bitly.ws/FUp7.

-Bryce F. Neary, China’s Digital Silk Road in Morocco: The Implications of Digital Sector Dominance, 23.05.2022, link: http://bitly.ws/CNjt.

-Becky McCarty, What are the Benefits of Using VPN Encryption, **Inford collp**, 17.05.2023, link: http://bitly.ws/GJd2

-Casper Klynge, Cooperating against cybercrime: 20 years on from the Budapest Convention, 16.11.2021, link: http://bitly.ws/FVur.

-Ciaran Martin, Cyber Realism in a Time of War, **lawfare**, Wednesday, March 2, 2022, link: http://bitly.ws/zkoV.

-Constantine J. Petallides, Cyber Terrorism and IR Theory: Realism, Liberalism, and Constructivism in the New Security Threat, **inquiries journa**l, VOL. 4 NO. 03, 2012, link: http://bitly.ws/CH4T.

-Cisco Umbrella, How Modern Security Teams Fight Today's Cyber Threats – Is your workplace protected?, link: http://bitly.ws/F4Ve.

-Cory Mitchell, GAFAM Stocks, **Investopedia**, 15.09.2022, link: http://bitly.ws/FwIH.

-Digital Cooperation Organization, **Linkedin**, link: http://bitly.ws/GdPo.

-Duncan Bell, Political Realism and International Relations, **CORE**, http://bitly.ws/yQgI.

-Eeva Pavy, The Treaty of Lisbon, **European Parliament**, 04.2023, link: http://bitly.ws/HiK3.

-Emili J. Blasco, The prospect of war awaits the US and China-will they avoid it, link: http://bitly.ws/GEzb.

-European Parliament, Treaty of Nice, 26.02.2021, link: http://bitly.ws/HiHm.

-FILALI Ferial, The Future of Sino-Algerian Relationship on "O.B.O.R" (One. Belt. One. road), **Democratic Arabic Center**, 18.05.2021, link: http://bitly.ws/FC6x.

-"GLACY+", **Interpol**, Link : http://bitly.ws/GeR2.

-Francis Lokherd, Ortega Keith, International Relations Critical Theory, **Researchgate**, 01.07.2021, link: http://bitly.ws/yY8b.

-Hamdy Bashir, A Cyber Shadow- War between Algeria and Morocco, **Arab Wall**, 22.03.2022, link: http://bitly.ws/zsLS.

-Hasan M. Al-Rizzo, The undeclared cyberspace war between Hezbollah and Israel, **researchGate**, Contemporary Arab Affairs 1(3):391-405, July 2008, link: http://bitly.ws/zkkw.

-Jeffrey W. Meiser, Introducing Liberalism in International Relations Theory, **E-international relations**, 18.02.2018, link: http://bitly.ws/ESXc.

-John Calabrese, The New Algeria and China, 26.01.2021, Link: http://bitly.ws/swqE.

-Jonathan Boyd Scott, "Exonerating Morocco disproving the spyware",18. 02.2023, link: http://bitly.ws/Cib3.

-Jorge Ortiz, Moroccan army repels more than 400 cyber attacks, **Atalayar**, 19.11.2021, link: http://bitly.ws/CRAh.

-Josephine Wolff, "How the Notpetya attack is reshaping cyber insurance", Brookings, 01.12.2021, link: http://bitly.ws/IFbZ.

-Karim Mezran and Alissa Pavia, Morocco and Israel are friendlier than ever thanks to the Abraham Accords. But what does this mean for the rest of North Africa?, **MENASource**, 07.10.2021, link: http://bitly.ws/IBPo

-Katie Terrell Hanna and others, DEFINITION OF botnet, **TechTarget**, March 2021, link: http://bitly.ws/DU5e.

-Maheen Kanwal, what is gartner?,**webopedia**, 11.08.2022, link: http://bitly.ws/F5eV.

-Martti Lehto, "The Cyberspace Threats and Cyber Security Objectives in the Cyber Security Strategies", **ResearchGate**, 01.09.2015, link: http://bitly.ws/DkAm.

-Med Taher SBIHI, Cyber security law in Morocco, **LTE magazine**, 01.01.2023, link: http://bitly.ws/D6My.

-Merriam-Webster, proxy noun, **Dictionary**, Link: http://bitly.ws/I6kM.

-Michael Hill, Algeria Ranked 'Least Cyber-Secure' Country in the World, Japan 'Most Cyber-Secure', **info security**, 07.02.2019, link: http://bitly.ws/zsGN.

-Michael Ray, Edward Snowden American intelligence contractor, **Britannica**, 22.05.2023, link: http://bitly.ws/GTjv.

-Michael Sauers, Global Cyber security Index 2020 Ranks Morocco at 50th Globally, **Morocco World News**, 05.07.2021, link: http://bitly.ws/zHWZ.

-Nargis Kassenova & Brendan Duprey , Digital Silk Road in Central Asia: Present and Future, 01.06.2021, link: http://bitly.ws/GPmF.

-Ohman and others, Critical Theory, **The Stanford Encyclopedia of Philosophy** (Spring 2021 Edition), link: http://bitly.ws/ETfJ.

-Paul Bischoff, Which countries have the worst (and best) cybersecurity?, **comparitech**, 26.09.2022, link: http://bitly.ws/zsEE.

-Paul Belkin, NATO's Warsaw Summit: In Brief, **Congressional Research Service**, 14.11.2016, link: http://bitly.ws/HjQM.

-Peter Loshin, DEFINITION: ICANN (Internet Corporation for Assigned Names and Numbers), **TechTarget**, link: http://bitly.ws/Fvtm

-Riyadh: Morocco Joins Digital Cooperation Organization, **Maghreb Arab Press**, link: http://bitly.ws/GdVA.

-SECMENTIS LTD, U.S. Embassy In Cyprus, 10.06.2022, link: http://bitly.ws/GXSi.

-Stephen M Walt, One world many theories, 1998, link: http://bitly.ws/yQ5p.

-The haughty culturist, wargames (1983): winning at death and destruction, 6.01.2021, link: http://bitly.ws/KLCu.

-Toms Dumpis, Cybersecurity During the Pandemic, Morocco in Top 5 Most Afflicted, **Morocco World News**, 15.05.2021, link: http://bitly.ws/zqjn.

-The Editors of Encyclopaedia Britannica, Kosovo conflict Balkan history [1998–1999], **Britannica**, 02.06.2023, link: http://bitly.ws/HjmY.

-What are the different types of phishing attacks?, **TREND business**, link: http://bitly.ws/DU6q.

-Zoltán Sipos, Cybersecurity in Algeria, Journal of Security and Sustainability Issues ISSN 2029-7017 print/ISSN 2029-7025 online 2023 Volume 13, 30 March 2023, link: http://bitly.ws/GAdv.

- ✓ **Websites of organizations and universities**

-Arvind Adityaraj, Political Realism in International Relations, College of Commerce Arts and Science, Patna, india, link: http://bitly.ws/yQgk.

-Cybersecurity & Infrasructure Securty Agency, Organizations and Cyber Safety, link: http://bitly.ws/F4IJ.

-Defense Langage Institute Foreign Language Center, DLIFLC, Cultural Orientation-Moroccan, link: http://bitly.ws/ExDL.

-International federation of Red Cross and Red Crescent Societies, "North Africa", 31.01.2010, link: http://bitly.ws/Dppi.

-ND International Security Center, An Introduction to Realism in International Relations, UNIVERSITY OF NOTRE DAME, 21.07.2022, link: http://bitly.ws/DYIa.

-Steven E. Lobell, Structural Realism/Offensive and Defensive Realism, **International Studies Association And Oxford Univerity Press**, published in print: 01 March 2010, published online: 22 December 2017, link: http://bitly.ws/DYNI.

✓ **News Papers**

-Oussama Aamari, Morocco's DGSSI Detected, Neutralized Over 500 Cyber Attacks in 2021, **Morocco World News**, 09.05.2021, link: http://bitly.ws/zqn8.

-Safaa Kasraoui, Algeria's News Agency Accuses Morocco of Being Behind Latest Cyberattacks, **Morocco World News**, 13.02.2023, link: http://bitly.ws/Ci9q.

-Yahia Hatim, Malicious Emails Represent Most Frequent Digital Threat in Morocco, Morocco world news, 16.10.2020, link: http://bitly.ws/zqou.

## ✓ Références en français

✓ **Livres**

-Abderrahman BELGOURCH et autres, Le cyberspace Diversité des menaces & difficultés de régulation, Imprimerie Papèterie Elwatanya, Mohammedia, Ed1, 2020.

-Ali ELAZZOUZI, la cybercriminalité au Maroc, Impression Bishops Solutions, Casablanca, 01.06.2010.

-Céline Marangé et Maud Quessard, les guerres de l'information à l'ère numérique, l'Institut de Recherche stratégique de l'École militaire, Presses Universitaires de France / Humensis, 2021.

-Ivan LAVALLEE, Cyber Révolution et Révolution Sociale, les temps de Cerises, France, 2022.

-Louis COUFFIGNAL, La cybernétique, presses universitaires de France, Paris Ed.1, 1963.

-Bernard LUGAN, Histoire de l'Afrique du Nord (Égypte, Libye, Tunisie, Algérie, Maroc) Des origines à nos jours, Éditions du Rocher, Monaco, 2016.

-Pascal Boniface, la géopolitique 50 fiches pour comprendre l'actualité, Editions Eyrolles, Paris, Ed.09, 2023

✓ **Thèses**

-Cameron Coutu, La prévention de la cybercriminalité : résultats d'une enquête sur les effets perçus d'une campagne de prévention réalisée par une institution financière, Mémoire présenté à la Faculté des études supérieures et postdoctorales en vue de l'obtention du grade de Maitrise ès sciences (M.Sc) en criminologie, Université de Montréal, 2018-2019.

-Camille Rabussier, l'application du droit international dans le cyberespace, Master Droit comparé, Université Paris II Panthéon Assas, Paris, France, Année Universitaire 2018-2019.

- ✓ **Revue et Magazine**

-Aude Gery, Droit international et prolifération des cyber armes, Institut Français des Relations Internationales IFRI, France, Vol. 83, N° 2, 2018.

-Frédérick Douzet, La géopolitique pour comprendre le cyberespace, revue de géographie et de géopolitique,Cairn.Info, France, N° 152-153, 2014.

-Personnel d'ADF, L'Afrique combat la cybercriminalité, Africa Defense Forum, Headquarters U.S.africa command, Volume 12, 2ème trimestre, 21.08.2019, lien du magazine :http://bitly.ws/EJD2.

- ✓ **Articles**

-Adem K, Certification CISA : qu'est-ce que c'est et comment l'obtenir ?, **Cyberuniversity**, 14.03.2022, lien de l'article: http://bitly.ws/HBmc.

-Arezki Metref, Algériens… mais pas arabes, **le Monde Diplomatique**, Mars 2014, lien de l'article: http://bitly.ws/HAvi.

-Abdul-Hakeem Ajijola et Nate D.F. Allen, Leçons d'Afrique en matière de cyber-stratégie, **Centre d'Etudes Stratégiques de l'Afrique**, 18.03.2022, lien de l'article : http://bitly.ws/DhIj.

-Action Globale sur la Cybercriminalité", **Conseil de l'Europe**, lien de l'article : http://bitly.ws/GeEJ.

-Adriana. L, " Stuxnet : zoom sur la « cyber-arme » et comment s'en protéger", **Cyberuniversity**, 21.11.2021, lien de l'article, http://bitly.ws/EtcL.

-Brian Brequeville, Les cyberattaques, troisième risque perçu par les PME marocaines (enquête SCR), **MEDIA 24 le boursier**, 11.02.2021, lien de l'article : http://bitly.ws/zrJn.

- Christelle HOUETO, "Bilan de la ratification de la convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère", 15.02.2023, **Africa cybersecurity Magazine**, lien de l'article: http://bitly.ws/GbJL.

-Clémentines Bories, Appréhender la cyberguerre en droit international. Quelques réflexions et mises au point, **OpenEdition**, 04.12.2014, lien de l'article : http://bitly.ws/F92Y.

-Christophe Bezes et Maria mercanti-guérin, Stratégies d'acquisition des GAFAM: derrière le contrôle des technologies, celui des corps. Une analyse inspirée par Michel Foucault, 01.10.2021, lien de l'aricle: http://bitly.ws/CK3W.

-Cyberdéfense, 17.04.2023, **Organisation du Traité de l'Atlantique Nord**, lien de l'article: http://bitly.ws/Gb8x.

-Définition Pharming en informatique, actualité informatique, lien de l'article :http://bitly.ws/DU7q.

-Delphine Lacour, Qu'est-ce que le ver Stuxnet ?, 14.09.2022, lien de l'article : http://bitly.ws/Fq6F.

-Domingo.Torrejon , La cooperation en matière de sécurité entre le Maroc et l'Europe : l'Union Européenne est-elle incontournable?, 2018, Journal of International Law and International Relations, Universidad de Cádiz, España, Link : http://bitly.ws/G7L5.

-Edouard Yziquel, Evolution du rapport de forces entre l'Algérie et le Maroc, **Ecole de Guerre Economique**, 25.11.2021, lien de l'article: http://bitly.ws/GEnZ

-Fátima Roumate, les mécanismes légaux de lutte contre la cybercriminalité au maroc, lien de l'article : http://bitly.ws/yutH.

- Hyperborée Advisors, **Linkedin**, lien de l'article: http://bitly.ws/KLaX.

-Indice de Cybersécurité, **Africa Cybersecurity Magazine**, février 2022, lien de l'adresse : http://bitly.ws/GfGd.

-Indice mondial de cybersécurité, **Union internationale des télécommunications Secteur du développement**, 2020, lien de l'article: http://bitly.ws/HdnQ.

-Javier Roldan Barbero, la coopération en matière de sécurité entre le Maroc et l'Europe: l'union européenne est-elle incontournable ?, 2018, lien: http://bitly.ws/xHdf.

-Luca Bertuzzi, L'UE présente sa politique de cyberdéfense, 14.11.2022, **EURACTIV**, lien de l'article: http://bitly.ws/G6yb

-Manuel de l'utilisateur, Kaspersky Anti-Virus, 2015, **Kaspersky**, lien de l'article : http://bitly.ws/KFEg.

-Matthieu Chéreau, Time Well Spent – Pourquoi chacun doit prendre ses responsabilités ?, **Frenchweb.fr**, 13.02.2018, lien de l'article: http://bitly.ws/Fxiv.

-Javier Roldan Barbero, la coopération en matière de sécurité entre le Maroc et l'Europe: l'union européenne est-elle incontournable ?, 2018, lien: http://bitly.ws/xHdf.

-Joanne Massard, Pegasus, un logiciel israélien au coeur d'un scandale mondial d'espionnage, Euronews, 20.07.2021, lien de l'article : http://bitly.ws/HB35.

-Mohammed Boudarham, Région parisienne: un Polisarien à la rue?, Le360, lien de l'article: http://bitly.ws/F9ee.

-Mohamed Karim MISSAOUI et Abdelaziz ELHILA, "Criminal law and ethics put to the test of cyber crime - Le droit pénal et l'éthique à l'épreuve de la cybercriminalité", **Journal d'Economie, de Management, d'Environnement et de Droit**, **(JEMED)- ISSN 2605-6461 Vol 4. N° 2**, Mai 2021, lien de l'article: http://bitly.ws/D2yr.

-Morgan JOUY, une Cyberdéfense collective en Europe? l'articulation entre cyber défenses européenne et transatlantique, **Institut de Recherche Stratégique de l' Ecole Militaire "IRSEM",** lien de l'aricle: http://bitly.ws/C8Er.

-M.MOUHIR& Mme.MOKHTAR, Stratégie de Cyber défense marocaine: du public au privé, enjeux et perspectives, **Ecole de Guerre Economique**, 08.02.2023, lien de l'article : http://bitly.ws/FIqM.

-Mourad El Manir, L'Afrique face aux défis protéiformes du cyberespace, **policy center for the new South**, 01.12.2023, lien de l'article: http://bitly.ws/DcHt.

-Rachid ATTAHIR, le conseil supérieur de sécurité: quelle voie pour la concrétisation ?, **Institut Marocaine de l'Information Scientifique et Technique IMIST**, 2017, lien de l'artcile : http://bitly.ws/DJiB.

-Soufiane Khabbachi, Maroc-Algérie : la discorde s'invite sur le front numérique, **Jeune Afrique**, 26.11.2021, lien de l'article: http://bitly.ws/CT8w.

-Techno-Science.net, "Norber Wienner", lien de l'article: http://bitly.ws/HHup.

-Tilila Sara Bakrim, Rivalité Maroc-Algérie: la guerre des récits Introduction, **Fondation pour la recherche stratégique**, 07.04.2022, lien de l'article: http://bitly.ws/yW9k.

-Yoann ROBERT, Cyber défense : La prise de conscience étatique, **EGE école de guerre économique**, 01.09.2019, lien de l'article : http://bitly.ws/DwSE.

- ✓ **Sites Web d'organisations et d'universités**

-Agence nationale de la sécurité des systèmes d'information, Un niveau élevé de cyber menaces en 2022, **ANSSI**, 2022, lien de l'article : http://bitly.ws/EWLH, date visite : 20.05.2023.

-Administration de la Défense Nationale, stratégie nationale en matière de cyber sécurité, lien de l'article: http://bitly.ws/zwwi.

-Guide pour la bonne gouvernance pour la cyber sécurité, **DCAF - Le Centre pour la gouvernance du secteur de la sécurité**, Genève – 2019, lien de l'article: http://bitly.ws/Df8a.

- La CGEM, qui sommes-nous ?, lien de l'article: http://bitly.ws/KLd5.

# الفهرس