المدرسة الوطنية العليا للعلوم السياسية "الشهيد زدور محمد إبراهيم قاسم"

السياسة الأمنية الجزائرية في مواجهة التهديدات السيبرانية: البوتات الاجتماعية نموذجا

مذكرة مقدمة لاستكمال متطلبات الحصول على شهادة الماستر في العلوم السياسية **تخصص علاقات دولية**

من إعداد الطالبة:

عبد العزيز مروة

تحت إشراف الدكتور:

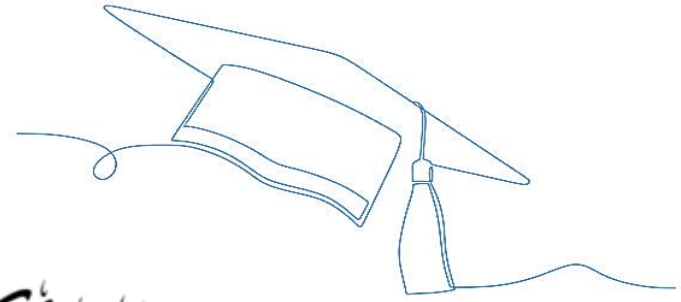
د. حمزاوي ميلود

أعضاء لجنة المناقشة

الاسم واللقب	مؤسسة الانتساب	الصفة
رامي حميد	المدرسة الوطنية العليا للعلوم السياسية	رئيسا
حمزاوي ميلود	المدرسة الوطنية العليا للعلوم السياسية	مشرفا ومقررا
الغنجة هشام داود	المدرسة الوطنية العليا للعلوم السياسية	مناقشا

السنة الجامعية: 2024-2025 م/ 1445-1446 هـ

سورة هود 88



شكر وعرفان

يقول ربنا في محكم التنزيل:

وَقَالَ رَبِّ أَوْزِعْنِي أَنْ أَشْكُرَ نِعْمَتَكَ الَّتِي أَنْعَمْتَ عَلَيَّ وَعَلَى وَالِدَايَّ وَأَنْ أَعْمَلَ صَالِحًا تَرْضَاهُ وَأَدْخِلْنِي بِرَحْمَتِكَ فِي عِبَادِكَ الصَّالِحِينَ ﴿19﴾ سورة النمل

ويقول رسول الله صلى الله عليه وسلم: "**من لم يشكر الناس لم يشكر الله**"

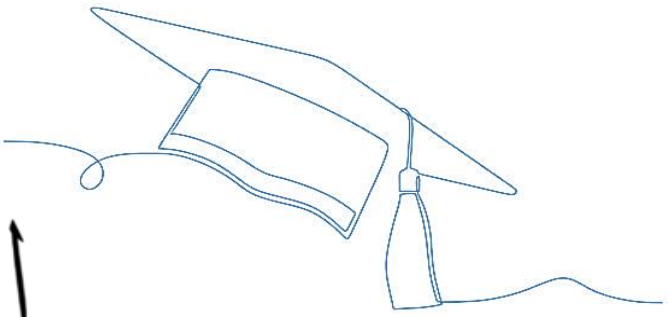
بداية أحمد الله تعالى الذي أنار لنا درب العلم والمعرفة وأعاننا ووفقنا لإتمام هذه المذكرة

كما لا يسعني إلا أن أتقدم بجزيل الشكر وعظيم الامتنان إلى أستاذي المشرف **"حمزاوي ميلود"** الذي منحني من وقته وجهده الكثير، فكان خير ناصح ومشرف وكانت لتوجيهاته الأثر الكبير في إنجاز هذا العمل، أسأل الله أن يبارك في عمره وعلمه وعمله.

وأتوجه بجزيل الشكر لأعضاء لجنة مناقشة هذه المذكرة الأستاذ **"حميد رامي"**، والأستاذ "**هشام داود الغنجة**" الذين سيتفضلون بمناقشة وتقييم هذه المذكرة.

الشكر موصول أيضا إلى كافة أساتذة المدرسة الوطنية العليا للعلوم السياسية على ما قدموه لنا طيلة فترة الدراسة، كما لا ننسى في هذا المقام تقديم الشكر على وجه الخصوص للأستاذة **"ششوي حسناء"** التي ساهمت أيضا في بناء جزء مهم من هذا العمل.

إليكم جميعا خالص شكري وتقديري



الإهداء

﴿وَآتَاكُمْ اللهُ كُلَ مَا سَأَلْتُمُوهُ﴾

فبالله نبلغ ما نرتجيه وبالله ندفع ما لا نطيق

أولا وقبل كل شيء حمدا للذي أوجدني من عدم، وأكرمني بالنعم، وعلمني ما لم أكن أعلم، أحمده سبحانه وتعالى وإليه ينسب الفضل.

أهدي تخرجي إلى من تضيق أسطري وتتبعثر كلماتي في وصف حبي له، إلى سندي قوّتي وفخري "والدي الحبيب"

إلى من سهرت ورعت ودعت ووجهت، إلى نبع الحنان سر الوجود وبسمة الحياة "أمي الغالية"

أطال الله في عمركما وألبسكما لباس الصحة والعافية

إلى من قال الحق فيهم ﴿سَنَشُدُّ عَضُدُكَ بِأَخِيكَ﴾ العقد المتين إخوتي "طارق، رياض، عصام"

إلى من وهبني الله نعمة وجودها في حياتي إلى أنيسة عمري أختي "هدى" وإلى أجمل إضافة لعائلتنا زوجة أخي

إلى زهور البيت، أبناء إخوتي "محمد، كوثر، توبة، عبد البارئ"

إلى من تشاركنا مقاعد الدراسة وقربت بيننا الأيام "ديهية، سميرة، إيمان، وفاء، دلال، ليلى" كانت صحبتكن نعمة وفراقكن ليس بالهين

إلى كل من اتسع لهم قلبي وضاقت هذه الورقة عن ذكرهم، أهديكم عملي هذا عرفانا لكم بالجميل

مروة عبد العزيز

ملخص:

تهدف هذه الدراسة إلى إبراز جوانب الاستجابة الجزائرية للتهديدات التي تطرحها البوتات الاجتماعية، عبر استغلالها للفضاء السيبراني لخدمة أجندات تتعارض مع المصالح الوطنية.

وقد تناولت الدراسة الموضوع من خلال ثلاث فصول، حيث يشتمل الفصل الأول على الإطار المفاهيمي للبوتات الاجتماعية كتهديد سيبراني، فيما يحلل الفصل الثاني الاستراتيجية الجزائرية في مواجهة التهديدات السيبرانية، أما الفصل الثالث فقد خصّ بدراسة الحالة الجزائرية في التصدي للبوتات الاجتماعية، انطلاقا من أولى حالات الاستهداف خلال الحراك الشعبي 2019 وصولا إلى استغلالها في ملفات حساسة، كما بحثت الدراسة في معالم الاستجابة المؤسساتية لهذا التهديد السيبراني، وسعت لقياس نسب الوعي المجتمعي من خلال اعتماد أداة الاستبيان.

وتوصلت الدراسة أن نسبة تهديد البوتات الاجتماعية تختلف وفقا للغرض الذي أُنشِئَت لتؤديه، وتبين كذلك أن الدولة تنتهج استراتيجية متكاملة الأبعاد في مواجهتها للتهديدات السيبرانية عموما، أما بالنسبة للبوتات الاجتماعية فإنها تتصدى لها من خلال رصد المحتويات المضللة وتحييد تأثيرها عبر المنصات والقنوات الرسمية.

الكلمات المفتاحية: السياسة الأمنية، الجزائر، البوتات الاجتماعية، التهديدات السيبرانية.

Abstract:

This study aims to highlight aspects of the Algerian response to the threats posed by social bots, through their exploitation of cyberspace to serve agendas that contradict national interests.

The first chapter includes the conceptual framework of social bots as a cyber threat, the second chapter analyzes the Algerian strategy to confront cyber threats, and the third chapter examines the Algerian case study in addressing social bots, from the first cases of targeting during the 2019 popular movement to their exploitation in sensitive files. The study also examined the institutional response to this cyber threat and sought to measure the levels of societal awareness by adopting a questionnaire tool.

The study found that the threat level of social bots varies according to the purpose for which they were created. It also found that the state adopts an integrated strategy in its response to cyber threats in general, but as for social bots, it addresses them by monitoring misleading content and neutralizing their impact through official platforms and channels.

Keywords: Security policy, Algeria, social bots, cyber threats.

مقدمة:

في خضم التحولات المتسارعة التي يشهدها العالم بفعل الثورة الرقمية، لم يعد مفهوم الأمن محصورا في الدفاع عن الحدود الجغرافية أو حول مقاييس القوة العسكرية الصلبة، بل تحول إلى مفهوم مركب يرتبط بشكل وثيق مع قدرة الدولة على حماية فضائها السيبراني؛ الذي تحول إلى ساحة مركزية تدار فيها الصراعات الحديثة التي تتراوح بين الاختراقات، وحروب المعلومات، وصولا إلى التأثير في وعي الأفراد وتوجيه الرأي العام.

وتعد شبكات التواصل الاجتماعي أبرز تجليات هذا التحول، إذ لم تعد مجرد منصات للتواصل والتفاعل فحسب، بل تحولت إلى فضاءات لصناعة الرأي العام، وتوجيهه في المسائل السياسية والثقافية والأمنية. ومن هنا ينبع التهديد الحقيقي الكامن في هذه الوسائط، والذي عبر عنه "كريستوفر سانج" (Christopher Sung) بقوله:

"لمواقع الشبكات الاجتماعية جانبا شديد الظلمة، فبعيدا عن كونها أداة طوباوية للحقيقة والديمقراطية، هي أيضا أداة بيد أصحاب الأجندات الخفية، وملعبا لمحاولات خبيثة لتضليل الناس وتشجيعهم على الاعتقاد والتصرف بطرق معينة"[1]. هذا الجانب المظلم، يتجسد بشكل خاص من خلال البوتات الاجتماعية (Social Bots)، التي باتت توظف في حملات موجهة لضرب الاستقرار الداخلي للدول وإدارة الحروب السيبرانية عن بعد.

على غرار بقية دول العالم تواجه الجزائر، تحديات متنامية متعلقة بتأمين فضائها السيبراني من تهديدات البوتات الاجتماعية، التي تستهدف أمنها القومي من خلال التحريض والتضليل والتلاعب بالمعلومات. بالتالي وجدت الدولة نفسها أمام ضرورة مراجعة سياستها الأمنية، لبلورة استراتيجية شاملة للأمن السيبراني تستوعب الطابع المركب للتهديدات السيبرانية، وعلى رأسها البوتات الاجتماعية سالفة الذكر.

[1] حيدر إبراهيم المصدر، الدعاية على الشبكات الاجتماعية (فلسطين: مركز الدراسات الإقليمية، 2020)، ص58.

أهمية الدراسة:

الأهمية العلمية:

- معالجة موضوع متعدد الأبعاد يجمع بين المفاهيم المركبة للأمن بما فيها الأمن السيبراني، العلاقات الدولية، التطور التكنولوجي والثورة الرقمية ما يفتح المجال لتداخلات بحثية بين مختلف التخصصات.
- تقييم استجابة السياسات الأمنية الجزائرية للتهديدات الحديثة وعلى رأسها التهديدات السيبرانية ومعاينة مدى جاهزيتها التقنية والمؤسساتية.
- إثراء الدراسات الأكاديمية في مجال الأمن السيبراني، من خلال تقديم نموذج تطبيقي للجزائر، وتحليل مقاربتها في مواجهة تهديدات سيبرانية معقدة.
- معالجة موضوع مستحدث يتعلق بالأشكال الجديدة للدعاية او ما يمكن تسميته "أتمتة الدعاية".

الأهمية العملية:

- توفير إطار عملي لفهم واقع تعامل المؤسسات الجزائرية مع المخاطر السيبرانية.
- إبراز مكامن القوة والضعف لدى السياسة الأمنية الجزائرية في مجال مواجهة تداعيات البوتات الاجتماعية.
- تعزيز الوعي المؤسسي والأكاديمي بخطورة البوتات الاجتماعية وتأثيرها على الأمن القومي الجزائري.
- اقتراح توصيات قابلة للتنفيذ، يمكن أن تستفيد منها الجهات المعنية بصنع السياسات، سيما الأجهزة الأمنية، والمؤسسات الإعلامية.

مبررات اختيار الموضوع:

الأسباب الذاتية:

جاء اختياري لموضوع "السياسة الأمنية الجزائرية في مواجهة التهديدات السيبرانية: البوتات الاجتماعية نموذجا" نتيجة لاهتمام شخصي بمجال الأمن السيبراني، لما يمثله من رهانات حديثة تمس سيادة الدول واستقرارها. كما أن التركيز على الحالة الجزائرية ينبع من دافع وطني يهدف إلى الإسهام في تحليل واقع المنظومة الأمنية في المجال السيبراني، وفهم كيفية تعامل المؤسسات مع هذه التهديدات. ويشكل الموضوع فرصة للجمع بين التحليل النظري والدراسة التطبيقية، بغرض تقديم مقترحات عملية تعزز فعالية الاستجابة الوطنية في هذا المجال الحيوي.

الأسباب الموضوعية:

- ندرة الأبحاث الأكاديمية العربية والجزائرية خصوصا التي تتناول موضوع البوتات الاجتماعية كتهديد سيبراني، بالرغم من تزايد تأثيراتها على الأمن القومي للدول،
- الأهمية الحيوية والاستراتيجية للبحث سواء للأفراد أو المختصين في المجال الأمني والدفاع الوطني.

- تحفيز الباحثين على تناول موضوع الدراسة من جوانب مختلفة، واستغلال المادة العلمية والمنهجية المتبعة فيها كمنطلق لبحوث ودراسات أخرى.

أدبيات الدراسة:

أطروحة دكتوراه باللغة الإنجليزية صادرة عن كلية التجارة بجامعة كوبنهاغن "CBS PhD School" عام 2024، تحمل عنوان "Bots on Social Media: the Past, Present and future" للمؤلف سيبو روسي (Sippo Rossi)، والتي تعد دراسة أكاديمية شاملة عن البوتات الاجتماعية بحيث قدمت رؤية حول تاريخها وتطورها من الأساليب التقليدية إلى الذكاء الاصطناعي التوليدي، واشملت أيضا على الطرق المختلفة لكشفها، واختتمت الأطروحة باستشراف لمستقبل أبحاث البوتات الاجتماعية. إلا أن هذه الدراسة لم تشتمل على جانب التهديدات التي باتت تطرحها البوتات على أمن الدول، واقتصرت على الجانب التقني لكشف البوتات الاجتماعية في مقابل إهمال الجوانب الأخرى.

كتاب بعنوان "الدعاية على الشبكات الاجتماعية قراءة في أدوات السيطرة والتضليل"، صادر عن مركز الدراسات الإقليمية فلسطين، للمؤلف حيدر إبراهيم المصدر، تناول فيه التطور التاريخي للدعاية وصولا إلى ظهور شبكات الاجتماعية، أين برزت الدعاية الحاسوبية كنمط جديد، والبوتات الاجتماعية كأحد مكوناتها. كانت الدراسة من الدراسات القليلة التي تناولت متغير البوتات الاجتماعية باللغة العربية إلا أنها لم تطرح استراتيجيات لمواجهة التحديات التي تطرحها البوتات الاجتماعية.

دراسة الدكتور جمال بوازدية "الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية التحديات والآفاق المستقبلية"، المنشورة بمجلة العلوم القانونية والسياسية، العدد 01 في أفريل 2019، حيث عالج المقاربة الجزائرية لتحقيق الأمن السيبراني، على المستوى الوطني (قانونيا، مؤسساتيا، إداريا وقنيا)، ثم على المستوى الإقليمي (العربي والمتوسطي الأوروبي)، وصولا إلى المستوى الدولي. لكن هذه الدراسة اقتصرت على أنماط معينة من التهديدات السيبرانية دون الإشارة إلى متغير الدعاية الآلية على الرغم من أهميتها المتزايدة في مشهد الأمن السيبراني.

أما هذه الدراسة وعلى خلاف الدراسات السابقة، فستركز بشكل محوري على السياسة الأمنية الجزائرية في مواجهة التهديدات السيبرانية، مع اتخاذ البوتات الاجتماعية كنموذج، من خلال التطرق لجهود مختلف الجهات الفاعلة في التعامل مع هذه الكيانات الرقمية التي تستهدف توجيه الرأي العام وزعزعة الاستقرار الداخلي للدولة.

إشكالية الدراسة:

أمام التحديات التي تفرضها البوتات الاجتماعية على الأمن القومي للدول، تبرز الحاجة إلى فهم مدى استعداد السياسة الأمنية الجزائرية لمواجهتها، وقدرتها على التكيف مع طبيعة التهديدات السيبرانية الحديثة. ومن هنا يبرز السؤال المحوري لهذه الدراسة:

كيف يمكن تكييف السياسة الأمنية الجز ائرية مع التهديدات التي تفرضها البوتات الاجتماعية؟

الأسئلة البحثية:

1. ما ذا نقصد بالبوتات الاجتماعية؟ وكيف يمكن اعتبارها تهديدا سيبرانيا؟
2. فيما تتمثل أهم محاور الاستراتيجية الجزائرية في مواجهة التهديدات السيبرانية؟
3. كيف تتصدى السياسة الأمنية الجزائرية لمخاطر البوتات الاجتماعية وتداعيتها على الرأي العام في القضايا الحساسة؟

فرضيات الدراسة:

الفرضية المركزية:

تتزايد نجاعة السياسة الأمنية الجزائرية في التصدي للتهديدات الناجمة عن البوتات الاجتماعية، بتزايد التنسيق المؤسسي وباعتماد آليات رقابة تقنية وتشريعات قانونية ملائمة.

الفرضيات الفرعية:

1. يعتمد تصنيف البوتات الاجتماعية كتهديد سيبراني على مدى استخدامها في التلاعب بالمحتوى الرقمي وليس على وجودها بحد ذاته.
2. تركز الاستراتيجية الجزائرية في المجال السيبراني على الجوانب التقنية والأمنية، مع إهمال لبعض الجوانب الاجتماعية والتوعوية.
3. تواجه السياسة الأمنية الجزائرية، البوتات الاجتماعية على نحو استباقي، من خلال تكثيف سياسات الرقابة والتحكم في المحتوى الرقمي.

حدود الدراسة:

الحدود المكانية: تركز الدراسة على الفضاء السيبراني الجزائري، وتشمل دراسة استجابة المؤسسات الوطنية المختصة في الأمن السيبراني والبنى التحتية للمعلومات والاتصالات وصولا إلى منصات التواصل الاجتماعي باعتبارها مركز تواجد البوتات الاجتماعية.

الحدود الزمانية: شملت الدراسة الفترة الممتدة من 2019 إلى يومنا هذا (2025)، باعتبار أن 2019 كانت السنة التي شهدت بداية رصد لاستخدام البوتات الاجتماعية كتهديد سيبراني للأمن الوطني، مع بداية الحراك الشعبي الجزائري فيفري 2019.

غير أن التزامنا بهذا المجال الزماني والمكاني لن يكون قطعيا، ذلك أن تداعيات التهديدات السيبرانية العابرة للحدود، والسيرورة التاريخية للسياسة الأمنية الجزائرية، قد تدفع لتجاوزه أحيانا.

منهجية الدراسة:

اقتضت منا دراسة هذا الموضوع استخدام مجموعة من المناهج والاقترابات والأدوات، سنذكر منها على سبيل التمثيل لا الحصر:

المنهج التاريخي: فدراسة السياسة الأمنية الجزائرية في المجال السيبراني، وبالأخص في تفاعلها مع البوتات الاجتماعية، تستدعي اعتماد المنهج التاريخي، لفهم الخلفيات والمرتكزات التاريخية التي أسست لإعادة صياغة أولويات السياسات الحالية.

منهج دراسة الحالة: يعتمد منهج دراسة الحالة على التعمق في فهم ظاهرة محددة ضمن سياقها الواقعي، من خلال جمع معلومات دقيقة وشاملة عنها، سواء من حيث وضعها الحالي أو ماضيها. وقد تم استخدامه في هذا السياق من خلال دراسة التصدي للبوتات الاجتماعية في الجزائر، كحالة تستدعي البحث والإلمام بالجوانب الميدانية والمؤسساتية المعتمدة.

منهج البحث الميداني: يُعنى هذا المنهج بدراسة الظواهر بأبعادها وخصائصها كما هي عليه في الواقع، مما يجعل النتائج المتحصل عليها أكثر موضوعية ومصداقية، ويعتمد منهج البحث الميداني على عدة أساليب وأدوات في جمع البيانات كالمقابلات والاستبيانات، وهو ما اقتضته طبيعة وأهداف هذه الدراسة لضمان الحصول على بيانات دقيقة وموثوقة تعكس الواقع الفعلي للظاهرة المدروسة.

الاقتراب القانوني: الذي يركز على مدى تطابق الفعل مع القاعدة القانونية، وقد تضمنت الدراسة تحليل أبرز القواعد القانونية الجزائرية في المجال السيبراني.

الاقتراب المؤسسي: وهو الذي يركز على المؤسسة كوحدة تحليل أساسية لفهم الظواهر السياسية، وقد برز في مضامين البحث، من خلال التطرق لمختلف المؤسسات التي من شأنها مجابهة التهديدات السيبرانية عموما، والبوتات الاجتماعية على وجه الخصوص.

وقد تم كذلك استخدام أداة **الاستبيان**؛ لقياس نسب الوعي العام بمخاطر البوتات الاجتماعية، وتمت معالجة البيانات عن طريق برنامج التحليل الإحصائي**SPSS V 23** . هذا إلى جانب إجراء **مقابلات شخصية** لدى مختلف المؤسسات الفاعلة في مجال مواجهة التهديدات السيبرانية (المصلحة المركزية لمكافحة الجريمة السيبرانية/ فرقة محاربة الجرائم السيبرانية/ وزارة الاتصال/ مكتب الإعلام والاتصال بأمن ولاية الجزائر/ وكالة الأنباء الجزائرية).

مجتمع البحث:

يعرف مجتمع البحث بأنه مجموعة من المفردات التي يستهدف الباحث دراستها لتحقيق نتائج الدراسة. وفي هذه الدراسة تم اعتماد فئات متنوعة تشمل: أساتذة جامعيين، طلبة، موظفين، وحتى العاطلين عن العمل.

العينة:

تعرف العينة بأنها فئة تمثل مجتمع البحث أو جمهور البحث أي جميع المفردات الظاهرة التي يدرسها الباحث، أو جميع الأفراد أو الأشخاص الذين يكونون موضوع مشكلة البحث.

في هذه الدراسة تم توزيع 200 استبيان، ثم تم تصفية العينة لتركيز التحليل على الأفراد الذين لديهم وعي مسبق بالبوتات، أين تم اعتماد 80 استبيانا أي ما يعادل 40% من العينة الكلية.

مبررات اختيار العينة:

- ✓ الحرص على شمولية الدراسة لفئات متنوعة من حيث الجنس/ العمر/ المستوى التعليمي.
- ✓ استبعاد الإجابات التي ليس لديها معرفة مسبقة بالبوتات للتقليل من التحيز في النتائج.
- ✓ التركيز على العينة الواعية بدلا من تضمين آراء غير مبنية على معرفة مسبقة.

هيكلة الدراسة:

لدراسة الموضوع قسمنا العمل إلى ثلاث فصول، الأول بعنوان "الإطار المفاهيمي للبوتات الاجتماعية كتهديد سيبراني" جاء للبحث في مفهوم التهديدات السيبرانية بصفة عامة، ليتفرع في أنماطها وصولا إلى الضبط المفاهيمي للبوتات الاجتماعية وأنواعها (السياسية، الدعائية، والتضليلية)، كما اشتمل المبحث الثاني منه، على أدوار البوتات الاجتماعية في سياق الحروب السيبرانية وتداعياتها على الأمن الوطني، ليصل إلى استعراض دراسات حالة الصين والولايات المتحدة الأمريكية في التصدي لهذا التهديد الأمني.

أما الفصل الثاني فقد تم تخصيصه لتحليل واقع السياسة الأمنية الجزائرية في مواجهة التهديدات السيبرانية، وذلك بدءا من تحديد مرتكزات هذه السياسة، إلى محاولة تكيفها مع طبيعة التهديدات السيبرانية المستجدة عبر تعزيز الآليات المؤسساتية والقانونية إلى جانب التعاون الدولي في إطار بناء استراتيجية شاملة للأمن السيبراني، وصولا إلى إبراز التحديات التي تواجه الجزائر في هذا المجال.

أما الفصل الثالث بعنوان "البوتات الاجتماعية كجزء من الاستراتيجية الأمنية الجزائرية"، فقط تطرق لحالات استهداف الجزائر بالبوتات في سياقات مختلفة لتأجيج القضايا الداخلية والاخلال بالنظام العام، كما يستعرض آليات المجابهة المؤسساتية والتوعوية، لتختتم الدراسة بعرض نتائج استبيان لقياس محتوى الوعي العام بالبوتات الاجتماعية.

صعوبات الدراسة:

واجهت دراسة الموضوع جملة من الصعوبات، أولها ندرة المراجع العلمية المتخصصة التي تتناول هذه الإشكالية في السياق الجزائري، إذ أن أغلب الأدبيات المتوفرة حول البوتات الاجتماعية منشورة باللغة الإنجليزية، وتركز على دراسة حالات غربية، ما يصعب عملية الاستفادة المباشرة منها. ضف إلى ذلك سرية المعلومات المرتبطة بالإجراءات الأمنية والسياسات السيبرانية الوطنية، بحيث أن هنالك بعض الجوانب التي تحاط بالسرية.

الفصل الأول: الإطار المفاهيمي للبوتات الاجتماعية كتهديدات سيبرانية

تمهيد

يشهد العصر الحالي تزايدا غير مسبوق في هيمنة تكنولوجيا المعلومات والاتصالات على مختلف الميادين، الأمر الذي أدى الى تصاعد ملحوظ في وتيرة وتعقيد التهديدات السيبرانية؛ التي لم تعد مجرد مخاطر افتراضية، بل تحولت إلى أفعال واقعية ومتكاملة الأركان، تنفذ عبر شبكة الإنترنت بأشكال متنوعة، تشمل عمليات القرصنة والاحتيال، التخطيط لأنشطة تخريبية، ونشر المعلومات المضللة. وفي هذا السياق، تبرز البوتات الاجتماعية كأحد أبرز التحديات الأمنية في الفضاء السيبراني، نظرا لقدرتها المتنامية في التأثير على الرأي العام وتوجيه السلوكيات.

يهدف هذا الفصل إلى وضع إطار مفاهيمي شامل للتهديدات السيبرانية عموما، والبوتات الاجتماعية وأنواعها بصفة خاصة، كما سيسعى إلى تحليل الدور المتزايد للبوتات في الفضاء السيبراني؛ مع التركيز بشكل خاص على دورها في الحروب السيبرانية وتأثيراتها على الأمن الوطني. وفي الختام سيستعرض الفصل الاستراتيجيات التي تتبعها بعض القوى الكبرى لمواجهة هذا التحدي الأمني.

المبحث الأول: مفاهيم أساسية

يتطلب أي بحث علمي وأكاديمي البدء في ضبط المفاهيم الأساسية، بما يسمح باستيعاب معنى المصطلحات المراد دراستها وتوضيحها بالشكل الذي يؤدي إلى فك الغموض والتعقيد، لذا سيشتمل هذا المبحث على مفهوم التهديدات السيبرانية والبوتات الاجتماعية، إلى جانب الضبط المفاهيمي لأنواع البوتات الاجتماعية.

المطلب الأول: مفهوم التهديدات السيبرانية

الفرع الأول: تعريف التهديد الأمني

1. تعريف التهديد لغة

يعرف التهديد لغة على أنه: "مشتق من الفعل هدد، يهدد، تهديدا. وهو ناتج عن إلحاق الأذى والضرر، ويتعلق بكل ما يمكن أن يخل بالأمن ويشكل هاجسا"[1]

في حين يشير المعنى اللغوي للتهديد في اللغة الإنجليزية إلى "Threat"، أما في اللغة الفرنسية فهو يشير إلى معنى الخطر "Menace"، وفي اللغة اللاتينية "Trudere" ويردف كلمة الدفع، ووفقا لقاموس وبستر 'Webster's dictionary' فالتهديد هو "دليل على خطر وشيك أو أذى أو شر إلخ، كالتهديد بالحرب"[2]، وقد ورد في قاموس 'Le Petit Robert ' أن كلمة " Menace" تستخدم للإشارة إلى التهديدات اللفظية أو الفعلية، وكذلك للأشياء التي تشكل خطرا أو دلائل تنذر على حدوث شيء سيء.[3]

2. مفهوم الأمن

الأمن في مدلوله اللغوي هو نقيض الخوف، فهو يعني الطمأنينة والاطمئنان إلى عدم توقع المكروه، وفي أصوله اللاتينية اشتق مصطلح الأمن من "Securitas"، المتكونة من "Sine" بمعنى غير، و"Cura" والتي تعني السلامة؛ أي في المجمل غياب السلامة، وهو بذلك على عكس ما يجري تداوله بشأن الأمن.[4]

وقد عرفه قاموس أكسفورد على أنه: "التحرر من الرعاية والخطر أو غياب التهديد".[5]

وقد وردت كلمة الأمن في كثير من الآيات القرآنية منها:

---

[1] ليندة عكروم، تأثير التهديدات الأمنية الجديدة على العلاقات بين دول شمال وجنوب المتوسط، (عمان: دار ابن بطوطة للنشر والتوزيع، 2011)، ص29.

[2] أمينة دير، "أثر التهديدات البيئية على واقع الأمن الإنساني في إفريقيا دراسة حالة -دول القرن الإفريقي-"، مذكرة ماجستير (جامعة محمد خيضر بسكرة: كلية الحقوق والعلوم السياسية، 2014/2013)، ص 28.

[3] Le Petit Robert, Jousette Rey-Debove et Alain Rey (Paris: nouvelle édition millésime 2011), p 1570

[4] عمر سعداوي، "البعد الإقليمي للأمن الوطني الجزائري في ظل الحراك العربي الراهن "، أطروحة دكتوراه (جامعة باتنة 1: كلية الحقوق والعلوم السياسية، 2019-2020)، ص16.

[5] حسام نجيدة، "الأبعاد الجديدة لمفهوم الأمن"، مجلة العلوم الإدارية والسياسية، الكلية العسكرية لعلوم الإدارة، ع2 (ديسمبر 2023)، ص ص 1-39.

قال الله تعالى: {الَّذِي أَطْعَمَهُمْ مِنْ جُوعٍ وَءامَنَهُمْ مِنْ خَوْفٍ}.[1]

بمعنى أنه حسب المدلول القرآني الأمن ضده الخوف.

وقال أيضا: {الَّذِينَ ءَامَنُوا وَلَمْ يَلْبِسُوا إِيمَانَهُمْ بِظُلْمٍ أُولَئِكَ لَهُمُ الأَمْنُ وَهُمْ مُهْتَدُونَ}.[2]

من الآية يظهر أن الإسلام، قد ربط الأمن بالإيمان ولذلك دعا الله -عز وجل- عباده إلى الإيمان ليتحقق لهم الأمن والأمان، وبذلك الأمن في مفهومه العام في الإسلام يعني الطمأنينة والسكينة في النفس وسائر شؤون الحياة.

من التعاريف التقليدية للأمن نجد تعريف "رينيه ديكارت" (René Descartes)* الذي يرى: "الأمن في أعلى درجاته ابتعادا من الخوف واقترابا من التأمين".[3]

ومن التعاريف الحديثة تعريف الباحث الامريكي أرنولد أوسكار ولفرز Arnold Oscar Wolfers الذي يميز بين المعنيين الذاتي والموضوعي للأمن، فيقول: " الأمن في المعنى الموضوعي غياب أي تهديدات تجاه قيم مكتسبة، وفي المعنى الذاتي غياب الخوف من أن يتم المساس بأي من هذه القيم".[4]

ويعد تعريف باري بوزان Barry Buzan للأمن من وأكثر التعريفات تداولا خاصة في فترة ما بعد الحرب، إذ أشار إلى أنه: "السعي للتحرر من كل تهديد"[5] (The pursuit of freedom from threat)، ويعتبر بوزان من الأوائل الذين سعوا إلى تجاوز المعنى الضيق المادي لمفهوم الأمن التقليدي، فقد سمح بإدخال موضوعات جديدة مرجعية ووحدات تحليل مثل: الدولة، المجتمع، الفرد.

كما ميز بين خمسة أبعاد أساسية للأمن تتفاعل مع بعضها البعض، وهي الأمن العسكري، السياسي، الاقتصادي، البيئي، والمجتمعي.[6]

من خلال التعاريف الآنفة الذكر، يلاحظ أن مفهوم الأمن أصبح يتسم بالشمولية فبعد أن كان يدل على محتوى عسكري بحت، أصبحت أبعاده تحوي أبعاد سياسية واقتصادية واجتماعية وحتى بيئية.

---

[1] سورة قريش، الآية 4، القرآن الكريم.

[2] سورة الأنعام، الآية 82، القرآن الكريم

[3] جويدة حمزاوي، "مفهوم الأمن بين عمودية المستويات وأفقية الأبعاد: مفهمة توصيفيه متعددة المستويات"، المجلة الجزائرية للأمن الإنساني، م7، ع2 (جويلية 2022)، ص137-152.

[4] عادل زقاغ، "المعضلة الأمنية المجتمعية: خطاب الأمنية وصناعة السياسة العامة"، دفاتر السياسة والقانون، ع5 (جوان 2011)، ص ص 103-114.

[5] حسام نجيده، مرجع سابق، ص9.

[6] Ken Booth, Theory of world Security, (New York: Cambridge university press, first published, 2007), p161-162.

3. البناء الاصطلاحي لمفهوم التهديد الأمني

يعد مفهوم "التهديدات الأمنية" (Security Threats)، من أكثر المفاهيم ارتباطا بالأمن، بحكم العلاقة التفاعلية التي تربطهما (تأثير وتأثر)؛ فأي محاولة تفسيرية للأمن تستوجب الحديث عن التهديدات من حيث طبيعتها ومصادرها.

يعرف "تيري ديبيل" (Terry Debel) التهديد الأمني على أنه: "عمل نشط وفعال تقوم به دولة معينة للتأثير في سلوك دولة أخرى، ويشترط نجاحه توفر عدة عوامل أبرزها المصداقية والجدية والقدرات التي تتناسب مع التهديد، وهناك ثلاث سمات يتميز بها التهديد وهي: درجة الخطورة ومدى احتمالية وقوع التهديد وعنصر التوقيت".[1]

أما بالنسبة لـ"جان إيشلر" (Jan Eichler)، فيعتبر أن التهديد يتعلق بنية إلحاق الضرر بفاعل (دولة، جماعة، فرد...)، ويشترط فيه توفر العناصر التالية:

- أن يسبب حالة من الهلع والخوف.
- توفر القدرة على الاستهداف سواء الدولة مباشرة أو مواطنيها أو الدول المجاورة لها.
- درجة الخطورة، وتتعلق بطبيعة الخطورة بمعنى أن تكون محتملة أو فعلية أو كامنة، الأمر الذي يتطلب توفر رد فعل سريع من الطرف الذي يقع عليه التهديد.[2]

وقد أشار باري بوزان إلى أن التهديد الأمني مؤداه: "تهديد مؤسسات الدولة من خلال استخدام دولة أخرى للصراع الأيديولوجي، أو لقوتها المادية، وقد يصل إلى حد إعلان الحرب"[3]، كما طرح تصنيفا قطاعيا للتهديدات الأمنية:

القطاع الأول: التهديدات التي تستهدف القطاع العسكري، وتهدد جميع مكونات الدولة بما في ذلك المؤسسات الاجتماعية والاقتصادية، وتمثل محور اهتمامات الدول لحماية أمنها القومي.

القطاع الثاني: التهديدات المتعلقة بالقطاع السياسي، التي هي الأخرى لا تقل خطورة عن نظيرتها العسكرية، إذ أنها تنشأ من التنافس بين الأفكار والمعلومات والتقاليد المختلفة، وتتنوع في شدتها من مجرد وجود دولة تتبنى أيديولوجية مختلفة إلى تدخلات سياسية مباشرة وأنشطة شبه عسكرية.

القطاع الثالث: التهديدات الاقتصادية التي غالبا ما تكون غير مباشرة ويصعب التنبؤ بها، في هذا السياق أشار بوزان إل وجود حالتين يمكن اعتبارهما تهديدات اقتصادية حقيقية للأمن القومي، الأولى هي تهديدات الإمدادات الاستراتيجية؛ الناجمة عن اعتماد دولة ما على موارد استراتيجية حيوية من الخارج، والثانية هي تهديدات الاستقرار

[1] خالد كاظم أبو دوح، "التهديدات الأمنية"، أوراق السياسات العامة، تاريخ المقال: 2022، تاريخ الاطلاع: 2025/02/10.
https://spp.nauss.edu.sa/index.php/spp/article/view/85/66

[2] أميرة بوزار قوادري، "حفظ الأمن الجماعي في ميثاق الأمم المتحدة وإشكالية توسع مفهوم الأمن"، أطروحة دكتوراه (جامعة الجزائر 3: كلية العلوم السياسية والعلاقات الدولية، 2023/2022)، ص ص 99-100.

[3] الصادق جراية، "تحولات مفهوم الأمن في ظل التهديدات الدولية الجديدة"، مجلة العلوم القانونية والسياسية، جامعة الوادي، ع8 (جانفي 2014)، ص ص 17-31

المحلي والتي تنشأ من الاعتماد الكبير على التجارة،[1] ما يعني أن هذا النوع من التهديدات تعرض الدولة لضغوط خارجية أو داخلية تؤثر على اقتصادها بل وحتى خياراتها السياسية.

القطاع الرابع: تهديدات ذات طابع مجتمعي، وتستهدف التكامل الثقافي والاندماج الاجتماعي لمكونات المجتمع، وتشير هذه التهديدات إلى المخاطر التي تستهدف وحدة المجتمع وقيمه الأساسية.

القطاع الخامس: التهديدات البيئية والتي غالبا ما تنجم عن الأنشطة البشرية المتزايدة، ويمكن أن تتجاوز الحدود الوطنية، مما يجعلها قضية دولية[2]؛ ويمثل هذا النوع من التهديدات تحديا وجوديا طويل الأمد، حيث لا تقتصر آثاره على البيئة فحسب، بل تمتد لتشمل جوانب اقتصادية وصحية.

إن فهم معنى التهديد الأمني يستدعي الإلمام بسياق تطوره، فقبل الحرب الباردة اتسمت التهديدات بكونها عسكرية بحتة تستهدف الدول من الخارج، في حين اتسعت دائرة التهديدات الأمنية الجديدة[3] وانتقلنا للحديث عن تهديدات لا تماثلية(Asymmetric Threats) أو غير النمطية (Atypical Threats) أو غير التقليدية أو غير المتكافئة (Non-Conventional or Non-equal Threats) ؛ كنوع من التهديدات الأمنية التي ظهرت بوضوح بعد نهاية الحرب الباردة، وتتميز هذه التهديدات بطبيعتها التي تتجاوز مفهوم المواجهة التقليدية، بحيث تكون بين دول غير متكافئة من حيث القوة، والتنظيم وامتلاك الوسائل، كما تعتمد التهديدات اللاتماثلية على استغلال نقاط ضعف الخصم لتحقيق أهدافها[4].

كما يمكن تعريف التهديدات اللاتماثلية بأنها استراتيجيات وأساليب عمل تهدف إلى تحقيق أهداف معينة من خلال استغلال نقاط ضعف الخصم وتجنب نقاط قوته، بغض النظر عن ميزان القوى التقليدي بين الطرفين، كما يمكن أن تتخذ هذه التهديدات أشكالا متنوعة تشمل العمليات الإرهابية، والجريمة المنظمة العابرة للحدود، والتهديدات السيبرانية، وغيرها من الأساليب التي لا تندرج ضمن المواجهات العسكرية التقليدية بين جيوش نظامية.

وتجدر الإشارة إلى أن هنالك صعوبة في تصنيف التهديدات الأمنية المستجدة إلى تهديدات داخلية وأخرى خارجية على اعتبار وجود تهديدات تتعدى التصنيف نظرا لطبيعتها عبر الوطنية[5].

ومع التطور التكنولوجي الواسع وأمام بروز الفضاء السيبراني كساحة جديدة للتفاعلات والتأثير، برز التهديد السيبراني كأحد أبرز وأخطر أشكال التهديدات اللاتماثلية؛ إذ أنه في الفضاء السيبراني، يمكن لجهات فاعلة مختلفة شن هجمات معقدة ضد أهداف حيوية، مثل البنية التحتية الحساسة، المؤسسات الحكومية، والقطاعات الاقتصادية

[1] Barry Buzan, People, States, and Fear: The National Security Problem in International Relations, (Great Britain: wheatsheaf books, 1983), p75-81.

[2] Barry Buzan, op.cit, p83.

[3] حنان لبدي، "التهديدات الأمنية الجديدة وانعكاساتها على الأمن المجتمعي في الجزائر"، مجلة الساورة للدراسات الإنسانية والاجتماعية، م9، ع2 (2023)، ص190- ص 215.

[4] رياض بن عربية، "التهديدات اللاتماثلية في الفضاء السيبراني: حروب الجيل الرابع نموذجا"، دفاتر البحوث العلمية، م 10، ع1 (2022)، ص ص 459-477.

[5] نوال بلحربي، "التهديدات الأمنية الجديدة وسبل مواجهتها: أي دور للحدود الذكية؟ "، مجلة أبحاث قانونية وسياسية، م7، ع1، (جوان 2022)، ص 1166-1186.

الهامة. لذلك يعد التهديد السيبراني تجسيدا واضحا لمفهوم التهديد اللاتماثلي، حيث يستغل المهاجمون نقاط ضعف الأنظمة الرقمية والاعتماد المتزايد على التكنولوجيا لتحقيق أهدافهم بطرق غير تقليدية وغير متوقعة.

الفرع الثاني: تعريف التهديد السيبراني

السيبرانية لغة مأخوذة من مصطلح "Cyber" الذي يقابله في اللغة اليونانية كلمة "Kibernetes" بمعنى الشخص الذي يدير دفة السفينة، وهي بذلك تعني التوجيه والسيطرة،[1] وقد عرفها قاموس 'Oxford' على أنها: "دراسة فعالية العمل البشري بمقارنتها بفعالية الآلات، تتصل بخصائص الحواسيب وتكنولوجيا المعلومات والواقع الافتراضي"[2].

استعملت كلمة سيبرانية -في مفهومها الحديث- لأول مرة من قبل عالم الرياضيات الأمريكي "نوربرت وينر" (Norbert Winer)* في أواخر الأربعينات وقدم تعريفا لها باعتبارها: "التفاعل بين الانسان والآلة والذي يخلق بديلا للاتصال".[3]

كما تجدر الإشارة إلى أنه هنالك لبس في التمييز بين مصطلحي "الإلكترونية" و"السيبرانية" نظرا للعلاقة الوثيقة بينهما؛ فالإلكترونيات توفر الأدوات والتقنيات اللازمة لتطبيق مبادئ السيبرانية في التحكم بالأنظمة. هذا التداخل يجعل من الضروري فهم أن الإلكترونيات هي جزء أساسي من أدوات السيبرانية، بينما السيبرانية هي مجال أوسع يدرس كيفية استخدام هذه الأدوات للتحكم.

أما بخصوص تعريف التهديدات السيبرانية من الناحية الاصطلاحية، فهي تشير إلى مجموعة واسعة من المخاطر والهجمات التي تستهدف الأنظمة والشبكات والبيانات الرقمية.[4]

وتعرف التهديدات السيبرانية على أنها: أي ظرف أو حدث ينطوي على إمكانية التأثير سلبا على العمليات التنظيمية أو الأفراد من خلال نظام معلومات عن طريق الدخول غير المصرح به أو التدمير أو الكشف أو تعديل الحكومات والخدمات.

كما تعرف أيضا بأنها: "فعل يقوض من قدرات ووظائف شبكة الكمبيوتر لغرض قومي أو سياسي، من خلال استغلال نقطة ضعف ما تمكن المهاجم من التلاعب بالنظام".[5]

---

[1] محمد العيداني، "التهديدات السيبرانية وجرائم المعلومات"، مجلة الاجتهاد للدراسات القانونية والاقتصادية، م13، ع1 (2024)، ص 15-ص 37.

[2] إدريس عطية، "مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري"، كلية الحقوق والعلوم السياسية، جامعة تبسة، ص 100-121.

* نوربرت وينر 'Norbert Winer' (1894-1964) كان رياضي تطبيقي ومنظر أمريكي، له عديد الاسهامات في الهندسة الإلكترونية، الاتصالات الإلكترونية، وأنظمة الحكم، وقد أسس السيبرنطيقا؛ وهو الحقل الذي يقنن فكرة التغذية الاسترجاعية، وله تأثير على الهندسة، تحكم النظم، علوم الحاسب، ونظام المجتمع.

[3] موسوعة السياسة، عبد الوهاب الكيالي (عمان: دار الفارس للنشر والتوزيع، ط2، 1993)، ص 398.

[4] Kim Andreasson, Cybersecurity (Boca Raton: CRC Press, 2012), p29-31.

[5] عبد الغاني شرقي، "التهديدات السيبرانية وإشكالية السيادة: إعادة قراء لسيادة واستفاليا"، مجلة السياسة العالمية، م7، ع2 (2023)، ص 270-286.

هذا وتتميز التهديدات السيبرانية بالسرعة وتحدث في وقت واحد وتتخذ أشكالا عديدة، كما يمكن أن يأتي التهديد من مصادر متنوعة بما في ذلك الدول التي تقوم بعمليات التجسس وحرب المعلومات والقرصنة وقد تنشأ من أفراد أو منظمات أو جماعات إرهابية.[1]

مما سبق ذكره يمكن القول، أن التهديدات السيبرانية محاولات متعمدة لإلحاق الضرر بالأنظمة بشكل غير قانوني، سواء كان ذلك من خلال التأثير على سلامتها أو سريتها أو أمنها. وقد تكون هذه التهديدات داخلية أو خارجية، ومن خصائصها سرعة الانتشار وتنوع الأشكال إلى جانب التطور المستمر.

الفرع الثالث: أنماط التهديدات السيبرانية

تتعدد أشكال التهديدات السيبرانية وتختلف من حيث طبيعتها ومصادرها وأهدافها، إذ نجد:

1. الجريمة السيبرانية: (Cyber Crime)

تعرف بأنها: "الأنشطة الإلكترونية التي ترتكب عمدا بدافع إجرامي لإلحاق ضرر مادي أو معنوي بشخص أو جهة ما، بشكل مباشر أو غير مباشر"، ولا يقتصر هذا النوع من الجرائم على الأفراد والجماعات؛ وإنما قد يمتد إلى مستوى الدول ليهدد أمنها القومي،[2] من خلال الأعمال التي تستهدف المساس بسرية البيانات أو النظم الحاسوبية وسلامتها وتوافرها.

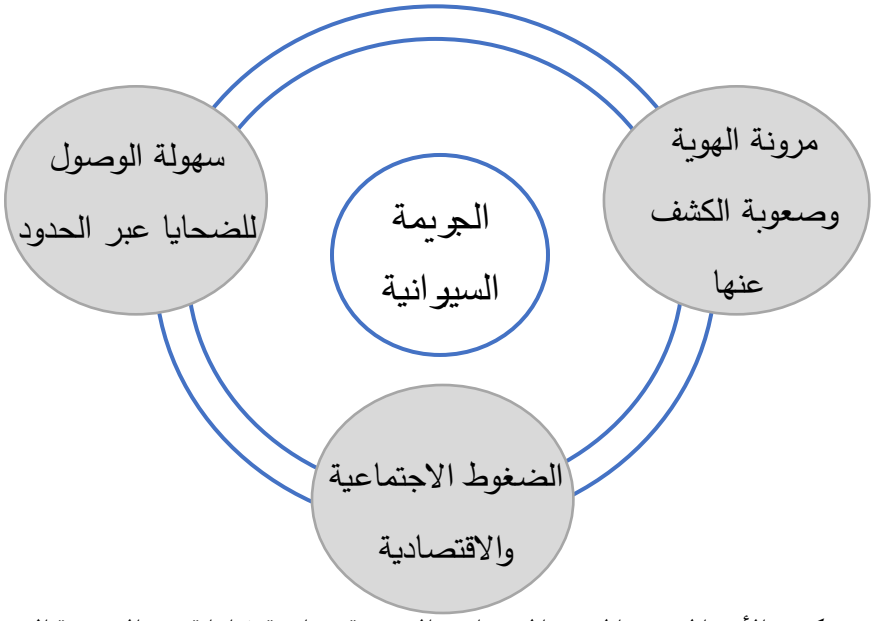
وتشير التقديرات إلى أن مصدر أكثر من 80 ٪ من الجريمة السيبرانية هو شكل من أشكال النشاط المنظم، حيث تقوم الأسواق السوداء للجرائم السيبرانية بإعداد البرمجيات الخبيثة والفيروسات الحاسوبية والتحكم فيها (اعتداءات البوت نت Bot net) [3]، بالتالي لم يعد ارتكاب الجريمة السيبرانية بحاجة إلى مهارات وتقنيات معقدة، مما انعكس على زيادة مستويات هذه الجرائم.

[1] "Cybersecurity Threats", impreva, accessed on: 15/02/2025.
https://www.imperva.com/learn/application-security/cyber-security-threats/

[2] علي زياد العلي، الصراع والأمن الجيوسيبراني في السياسة الدولية "دراسة في استراتيجيات الاشتباك الرقمي"، (عمان: دار أمجد للنشر والتوزيع، ط1، 2020)، ص 81.

[3] الأمم المتحدة، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، دراسة شاملة عن الجريمة السيبرانية، فيفري 2013، ص 22.

شكل 1 : العوامل المرتبطة بتصاعد الجريمة السيبرانية



المصدر: مكتب الأمم المتحدة المعني بالمخدرات والجريمة، دراسة شاملة عن الجريمة السيبرانية، ص12

2. الإرهاب السيبراني (Cyber Terrorism):

يعرف الإرهاب السيبراني بانه الأعمال التي تستخدم التقنيات الرقمية، والفضاء السيبراني، لإخافة وإضعاف الآخرين، ويعرف أيضا بأنه: "اعتداءات على أنظمة المعلومات التي تدير المصالح الحيوية والحرجة للدولة، بصورة قصدية وبنية إلحاق الأذى على أوسع نطاق ممكن، لأسباب إيديولوجية، اجتماعية أو سياسية أو دينية"[1]. وبمعنى آخر، فهو يمثل استغلال الفضاء الرقمي لشن هجمات ذات دوافع عقائدية أو سياسية أو اجتماعية بهدف إحداث ضرر واسع النطاق.

3. الصراع السيبراني (Cyber Conflict):

يعبر هذا المفهوم عن "حالة من التعارض في المصالح والقيم بين الفاعلين، سواء كانوا دولا أو غير دول في الفضاء الإلكتروني، وقد يتضمن التجسس والتسلل إلى مواقع الخصوم الإلكترونية وقرصنتها، ويتسم أطرافه بعدم الوضوح"[2]، بعبارة أخرى، هو اشتباك في الفضاء الرقمي بين جهات فاعلة متنوعة حول أهداف متضاربة، ويمكن أن يشمل عمليات سرية واختراقات، مع صعوبة تحديد المسؤولين بشكل قاطع.

[1] منى الأشقر جبور، السيبرانية هاجس العصر، (بيروت: المركز العربي للبحوث القانونية والقضائية، 2013)، ص 85.

[2] عادل عبد الصادق، "أنماط الحرب السيبرانية وتداعياتها على الأمن العالمي"، موقع السياسة الدولية، تاريخ المقال: 2017/05/14، تاريخ الاطلاع: 2025/02/20.
https://www.siyassa.org.eg/News/12072.aspx

4. الحرب السيبرانية (Cyber War):

لتحديد مفهوم الحرب السيبرانية، لابد من البدء أولا بالتعرف على معنى الحرب والتمييز بين أجيالها المتعددة؛ "إن جوهر الحرب يستند إلى كونها عمل من أعمال العنف، يستهدف إكراه الخصم على تنفيذ إرادتنا"[1].

ويمكن تتبع تطور الحروب عبر أربعة أجيال رئيسية؛ إذ في الجيل الأول كان الاعتماد الأساسي على القوة البشرية، ثم تطورت إلى استخدام قوة النيران في الجيل الثاني. وفي الجيل الثالث ظهرت المناورات العسكرية كاستراتيجية رئيسية، أما الجيل الرابع فيقوم على استخدام جملة من الأدوات السياسية والاقتصادية والاجتماعية والنفسية لتحقيق أهداف الحرب[2]. ومع هذا التغير، أصبحت أهداف الحرب أقل مادية تستند بالأساس على العامل النفسي والدعائي، إلى جانب اعتمادها على أسلحة تكنولوجية جديدة تلائم طبيعة السياق التكنولوجي لعصر المعلومات.[3]

وبالمواكبة مع هذا الجيل الرابع من الحرب، ظهرت الحرب السيبرانية (Cyber War) والتي تعرف بأنها: " إجراءات تتخذها دولة أو كيان من غير الدول (الجماعات الإرهابية، الشركات الخاصة، المنظمات الإجرامية العابرة للحدود)، لاختراق أجهزة كمبيوتر وشبكات دولة أخرى؛ لأغراض التسبب في أضرار أو تعطيل نظام ما"[4].

5. التجسس الإلكتروني (Cyber Espionage):

هو استخدام وسائل تقنية المعلومات الحديثة للدخول بشكل غير مسموح وغير قانوني إلى أنظمة المعلومات الإلكترونية الخاصة بالدول أو الأشخاص أو المنظمات، بقصد الحصول على ما لديها من معلومات مهمة تتعلق بنظامها وأسرارها[5]؛ أي أنه استغلال للقدرات الرقمية في اختراق الأنظمة وسرقة المعلومات السرية والحساسة التي تخص الدول أو المؤسسات أو الأفراد بطرق غير قانونية.

6. الذباب الإلكتروني والبروباغندا (Electronic flies and Propaganda):

يعرف الذباب الإلكتروني على أنه روبوتات أو برامج مصممة على أنها أشخاص حقيقية، وظيفتها إدارة حسابات وسائط التواصل الاجتماعي، وتعمل بشكل خاص على إظهار عدد هائل من المنشورات المزيفة (الهاشتاغ)* حتى تبدوا حقيقية، وذات مصداقية بسبب التداول الواسع لها في منصات التواصل الاجتماعي[6]، ويشتمل الذباب الإلكتروني على ثلاث أنوع وهي البوتات الاجتماعية التي تستخدم لنشر التغريدات،

---

[1] كارل فون كلاوزفيتز، الوجيز في الحرب، تر: أكرم ديري والهيثم الأيوبي، (بيروت: المؤسسة العربية للدراسات والنشر، ط2، 1988)، ص84.

[2] المملكة العربية السعودية، شركة آفاق المعرفة للنشر والتوزيع، تقرير ارتيادي سنوي محكم "ما بعد الإنسانية العوالم الافتراضية وأثرها على الانسان"، 2022، ص 234.

[3] محمد عباس محسن، الهجمات السيبرانية ومنطقة الفراغ التشريعي، (ألفا للوثائق، ط1، 2021)، ص 46، 60.

[4] علي زياد العلي وعلي حسين حميد، تكتيكات الحروب الحديثة الأمن السيبراني والحروب المعززة والهجينة، (مصر: العربي للنشر والتوزيع، 2023)، ص143.

[5] عبد الحليم بن بادة ومحمد سعد بوحادة، "جريمة التجسس الإلكتروني نمط جديد من التهديدات السيبرانية الماسة بأمن دول المنطقة"، الملتقى الدولي الأول الموسوم بأمن المعلومات في الفضاء الإلكتروني، (جامعة غرداية: كلية الحقوق والعلوم السياسية، 2020)، ص 5.

* الهاشتاغ Hashtag: نشأ مفهوم الهاشتاغ من التويتر، ففي عام 2007 بدأ المستخدمون بتحديد بعض الكلمات المهمة أو الرئيسية في منشوراتهم باستخدام إشارة (#) لتداولها على نطاق واسع، لتتحول من مجرد رمز إلى أيقونة فاعلة ومؤثرة في الوسط الإنساني.

[6] لمياء زواوي وفهيم رملي، "التهديدات السيبرانية وأمن المجتمع الرقمي: دراسة حالة الجزائر"، المجلة الجزائرية للأمن والتنمية، م12، ع 2 (أفريل 2023)، ص 148-160.

التعليقات، والمشاركات على مواقع التواصل الاجتماعي، وبوتات المحادثة؛ التي تستخدم لنشر رسائل تلقائية، إلى جانب بوتات الأخبار الزائفة[1].

ويعتبر الذباب الالكتروني أداة قوية لنشر البروباغندا والتي تعني في مجملها: نشر ومعلومات أو أفكار بشكل متحيز أو مضلل، بهدف التأثير على آراء أو سلوكيات أكبر عدد من الناس، وذلك من خلال التأثير على الأشخاص المستهدفين عاطفيا، لدفعهم لتبني أفكار أو اتخاذ مواقف معينة[2]. بشكل أساسي، يمثل الذباب الالكتروني الأدوات التقنية التي تستخدم في نشر البروباغندا على نطاق واسع من خلال خلق انطباع زائف بوجود تأييد شعبي، أو التأثير على المشاعر لدعم أهداف دعائية محددة.

المطلب الثاني: ماهية البوتات الاجتماعية

الفرع الأول: تعريف البوتات الاجتماعية

إن كلمة "بوت" (Bot) مشتقة من كلمة (Robot)، ويشير أصل الكلمة إلى الميزة الرئيسية لهذه الأدوات؛ كونها برامج حاسوبية تنفذ مهاما محددة بطريقة تلقائية وبشكل مستقل.[3]

ويطلق عليها هيغليش (Hegelich) وجانيتزكو (Janetzko) اسم "البرامج الآلية التي تحاكي البشر" (Automatic programs that are mimicking humans).[4]

إن أصل كلمة بوت يحتوي على نوع من الغموض؛ ففي الأيام الأولى للحوسبة الشخصية، استخدم المصطلح للإشارة إلى أنظمة برمجيات متنوعة مثل العمليات والبرامج النصية التي تنقل رسائل تحذير للمستخدمين البشريين، أما في العقد الأول من القرن العشرين فقد اكتسبت الكلمة معاني جديدة في أمن الشبكات والمعلومات، حيث استخدمت للإشارة إلى أجهزة كمبيوتر تم اختراقها والتحكم فيها عن بعد بواسطة برامج ضارة.

وبمجرد ظهور تويتر كشبكة اجتماعية، بدأ بعض الباحثين في تسمية الحسابات الآلية لهذه الشبكة بالبوتات.[5]

[1] دعاء أحمد، "حرب الذباب الالكتروني وخطر الاستقطاب المجتمعي"، القاهرة: جامعة عين شمس (ماي 2024)، ص 3.

[2] Noureddine Bensoula, "Electronic flies and public opinion, Al-Naciriya: Journal of Sociological and Historical Studies, Issue 1, Vol 1 (June 2020), p 195-211.

[3] Stefan Bordel, "What is Bot?", MYRA Security, 2020, accessed on 17/02/2025.
https://www.myrasecurity.com/en/knowledge-hub/bot/

[4] Florian Brachten et al, "Do social Bots Dream of Electric Sheep? A Categorization of Social Media Bot Accounts", Australasian Conference on information systems, (2017), p 1-11.

[5] Robert Gorwa and Douglas Guilbeault, "Unpacking the social Media Bot: A typology to guide research and Policy, Research Gate (28 /07/2018), p 1-31.

بالرجوع للمدلول الاصطلاحي، يمكن تعريف البوت بأنه روبوت الويب؛ الذي تغذيه خوادم ذكية، تقوم بمهام متكررة أو تلقائية عبر برنامج ينسق عملها؛ إذ يتم تقسيم مهام تلك الروبوتات عبر حساب أساسي، يوجه بعضها للنشر أو إعادة النشر أو التفاعل مع المشاركين والرد الآلي أو حتى الإعجاب، لتحقيق ما يعرف بالتغذية الغزيرة "Massive feed"[1].

فيما لايزال تعريف البوتات الاجتماعية محل نقاش؛ حيث يتم استخدام مصطلحي "بوت" و"بوت اجتماعي" أحيانا بالتبادل؛ لوصف الحسابات الآلية على مواقع التواصل الاجتماعي.

لكن مع المقالتين المرجعيتين، لروبرت جوروا 'Robert Gorwa' ودوغلاس جيلبو 'Douglas Guilbeault' / ستيفان ستيجليتز 'Stefan Stieglitz' وآخرون؛ حصل نوع من الإجماع في التعريف؛ بحيث تم تعريف البوتات على أنها حسابات أو وكلاء مستقلون يتم تشغيلهم بواسطة برنامج كمبيوتر وليس بواسطة إنسان. في حين عرفت البوتات الاجتماعية بأنها حسابات آلية في مواقع التواصل الاجتماعي تتفاعل مع البشر وتقلد سلوكياتهم[2].

ويصف بوشماف البوت الاجتماعي بأنه: " برنامج أتمتة* يتحكم فيه حساب مملوك للخصم أو مخترق على شبكة اجتماعية معينة، ولديه القدرة على أداء الأنشطة الأساسية مثل نشر رسالة وإرسال طلب اتصال"

هذا ويرى إيغاوا (Igawa) وآخرون أنه "على موقع تويتر، تتظاهر البوتات الاجتماعية بأنها بشر من أجل الحصول على متابعين وردود من المستخدمين المستهدفين والترويج لأجندات ومنتجات أو جدول أعمال[3]"

كما عرف البوت الاجتماعي على أنه برنامج حاسوبي يعتمد على خوارزميات تنتج محتوى تلقائي وتتفاعل مع البشر على وسائل التواصل الاجتماعي، تتسم هذه البوتات بقدرتها العالية على إقناع المستخدمين بأنها بشر، ويشير مصطلح "اجتماعي" إلى تقليد السلوك البشري والتظاهر بأنه إنسان يتفاعل اجتماعيا وليس مجرد بوت [4].

كما يعرف أيضا بأنه: "خوارزمية حاسوبية تنتج محتوى وتتفاعل مع البشر والبوتات الأخرى على وسائل التواصل الاجتماعي بشكل تلقائي أو شبه تلقائي، وتحاول محاكاة أو توجيه سلوك الإنسان"[5].

يلاحظ أن جميع التعاريف تشترك في النقاط التالية:

[1] خالد حمادي، "الدعايات المحوسبة ... الجيل الجديد من حروب الهاشتاغ وصناعة البوتات الرقمية عبر منصات الميديا الجديدة"، مدونة الإعلام والاتصال (أفريل 2022)، ص 1-11.

[2] Sippo Rossi, Bots on social media the Past, present and future (Denmark: Copenhagen Business School, 2024), p11.

* الأتمتة Automation تسمى أيضا "التشغيل الآلي" وفي بعض الأحيان "المكننة"، وهو مصطلح حديث نسبيا ويعني استبدال الأفراد بالآلات وأجهزة الكمبيوتر في المجالات التي تتطلب قدرا ضئيلا من التدخل البشري، ويشمل ذلك أتمتة عمليات مثل تكنولوجيا المعلومات، التصنيع، المهام الإدارية.

[3] Florian Brachten et al, op cit, p 3.

[4] Stefan Stieglitz and Florian Brachten, "How powerful are Social Bots?" Academic society for management and communication, (June 2018) p 1.

[5] Mahmood Sharif and Daniel Kats, "Perceptions of Social Bots and ability to detect them", HAI (December 2022), p1-2

- القدرة على التفاعل مع المستخدمين: بحيث تتفاعل البوتات الاجتماعية مع مستخدمي وسائل التواصل الاجتماعي من خلال النشر أو التعليق أو إرسال الرسائل.
- تقليد السلوك البشري: تسعى البوتات الاجتماعية إلى تقليد السلوك البشري من أجل الظهور بمظهر المستخدمين الحقيقيين.
- الأتمتة: البوتات الاجتماعية هي برامج تعمل بشكل آلي.
- تباين الأهداف: يمكن للبوتات الاجتماعية أن تنشد أهدافا متنوعة؛ بما في ذلك الأهداف السياسية أو التجارية أو الاجتماعية.

أما فيما يتعلق بتاريخ تطور البوتات الاجتماعية فإنه يتم تقسيمها إلى أربع فترات؛ بدأت الفترة الأولى حوالي عام 2010، عندما كانت وسائل التواصل الاجتماعي مثل تويتر وفيسبوك تكتسب شعبية وبدأت المقالات الأولى التي تصف البوتات في وسائل التواصل الاجتماعي في الظهور، واستمرت هذه الفترة حتى حوالي عام 2014 وبالتالي تسبق الاستخدام الواسع النطاق لمصطلح "البوت الاجتماعي".

فيما بدأت الفترة الثانية حوالي عام 2015، أين برز جليا وجود البوتات الاجتماعية والتهديد الذي تشكله للباحثين والمنظمات الحكومية، ويتضح ذلك من خلال تنافس الشركات والجامعات على أدوات للكشف عن البوتات، وهو ما أسفر عن إطلاق "Botmeter" كبرنامج يستخدم التعلم الآلي لتصنيف حسابات تويتر إلى حسابات بشرية أو بوتات، من خلال دراسة خصائص الملف الشخصي، ليخلص إلى منح درجة إجمالية للحساب من (0 إلى 5) بالإضافة إلى عدة درجات أخرى تشير إلى احتمالية كون الحساب بوتا[1].

في عام 2016 واستمرارا حتى عام 2017 ازداد الاهتمام بالبوتات الاجتماعية، نتيجة تداول أخبار بشأن التدخل الروسي في الانتخابات الرئاسية الأمريكية لعام 2016 عبر اعتماد حسابات وهمية وبوتات اجتماعية؛ إذ حدد تويتر علنا 3814 حسابا آليا على تويتر مرتبطا بجيش الانترنت الروسي، وورد أن هذه الحسابات نشطت في العشر أسابيع التي سبقت الانتخابات الأمريكية لعام 2016 نشرت ما يقارب 175.993 تغريدة، منها حوالي 8.4 كانت بخصوص الانتخابات.[2]

شهدت الفترة الثالثة ما بعد 2017 تنافسا حادا وصف على أنه بمثابة "سباق تسلح" في تطوير أساليب الكشف عن البوتات، إلى جانب ظهور دراسات حالة توثق وجود البوتات في سياقات مختلفة.[3]

[1] "Botometer", RAND, accessed on 19/02/2025Retriever from: https://encr.pw/7zsyx

[2] Washington, U S Department of justice, Report on the investigation into Russian interference in the 2016 Presidential election, March 2019, p28.

[3] Sippo Rossi, op cit, p 20.

وصولا إلى الفترة الرابعة والأخيرة التي بدأت في أوائل عام 2023 بعد أن جعلت تويتر استخدام واجهة برمجة التطبيقات الخاصة بها أكثر صعوبة، وتم بناء العديد من أدوات الكشف.[1]

الفرع الثاني: آليات عمل البوتات الاجتماعية

يشتمل سير عمل البوتات الاجتماعية على ثلاث مراحل رئيسية:

1) مرحلة النشر: تركز هذه المرحلة على إنشاء عدد كبير من حسابات التواصل الاجتماعي المزيفة، ويتم استخدام تقنيات متطورة مثل التعرف الضوئي على الحروف، والتعلم الآلي* (Machine Learning) لتجاوز إجراءات الأمان، كما تعتمد هذه المرحلة جمع المعلومات الشخصية من مستخدمين حقيقيين لإنشاء ملفات تعريف مقنعة للبوتات.

2) مرحلة توسيع الشبكة الاجتماعية: تركز هذه المرحلة على بناء شبكة واسعة من المتابعين والتفاعلات للبوتات الاجتماعية؛ وذلك من خلال استخدام زواحف الشبكة* (Online Crawler) والتعلم الآلي، لبناء قدرات التفاعل والتغذية الراجعة للبوتات الاجتماعية عند التواصل مع المستخدمين البشريين، مع تدريب نموذج تصنيف المشاعر* (sentiment classification model) ونموذج توليد النصوص* (text generation model).

3) مرحلة إطلاق التأثير: تهدف هذه المرحلة إلى استخدام البوتات الاجتماعية للتأثير على الرأي العام ونشر المعلومات المرغوبة، أين يتم استخدام استراتيجيات تواصل متقدمة للتلاعب بالمستخدمين ونشر الأخبار المزيفة والمعلومات المضللة.[2]

[1] Sippo Rossi, ibid., p 21.

* التعلم الآلي فرع من الذكاء الاصطناعي، يركز على بناء أنظمة قادرة على التعلم من البيانات وتحسين أدائها بمرور الوقت، دون أن تتم برمجتها بشكل صريح لكل مهمة.

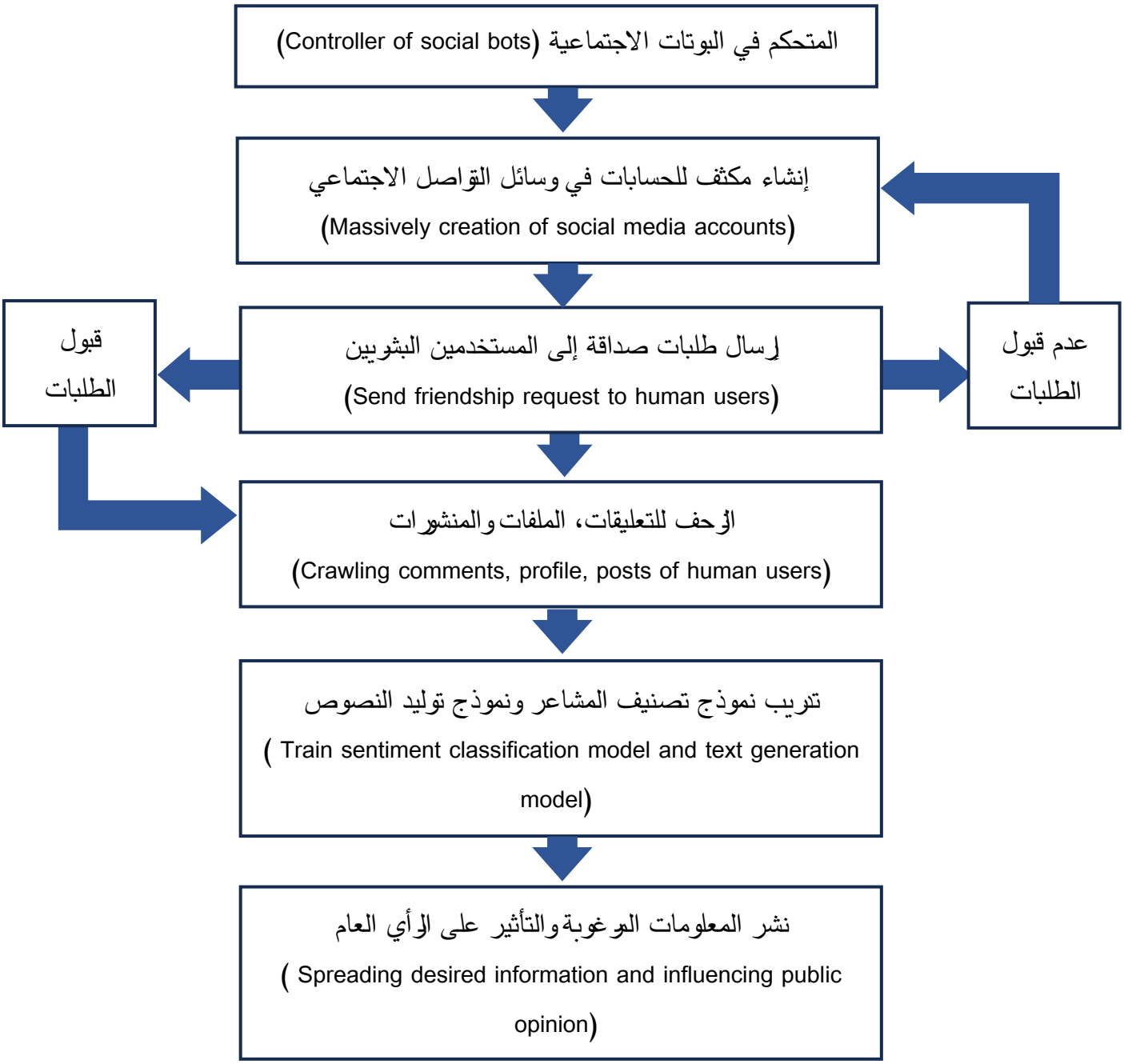
* زاحف الشبكة هو برنامج كمبيوتر مخصص لتصفح جميع مواقع شبكة الويب العالمية وجمع المعلومات بصفة تلقائية، مع القيام بتصنيفها وأرشفتها.

* نموذج تصنيف المشاعر هو نموذج ذكاء اصطناعي يمكنه تحديد المشاعر التي يعبر عنها النص مثلا (إيجابي، محايد، سلبي).

* نموذج توليد النصوص هو نموذج ذكاء اصطناعي يمكنه إنشاء نصوص جديدة تشبه النصوص التي تم تدريبه عليها.

[2] Xu Lingyu, "Research on work strategies and workflow of social Bots", university of Bristol, vol 8 (2023), p 535-564.

شكل 2: مخطط توضيحي لمراحل نشر البوتات الاجتماعية



المصدر: من إعداد الباحثة

الفرع الثالث: تأثيرات البوتات الاجتماعية

أصبحت البوتات الاجتماعية جزءا لا يتجزأ من منظومة وسائل التواصل الاجتماعي، هذه الحسابات الآلية التي تتفاعل وتشارك المحتوى بشكل مستقل، تحمل في طياتها تأثيرات عميقة ومتنوعة على الأفراد أو حتى على مستوى الدول.

1. نشر المعلومات المضللة:

تشارك البوتات فيما يصل إلى 20٪ من محادثات التواصل الاجتماعي، وتشير الاحصائيات إلى وجود حوالي 23 مليون بوت اجتماعي في تويتر، وهو ما يمثل 8.5٪ من إجمالي المستخدمين، وعلى فيسبوك ما يقدر بنحو 140 مليون بوت اجتماعي، وهو ما يقارب 5.5٪ من إجمالي المستخدمين، فيما يقدر عدد مستخدمي انستغرام من البوتات الاجتماعية بحوالي 27 مليون مستخدم (8.2٪)[1]، وهو ما يجعل البوتات الاجتماعية قادرة على نشر الأخبار الكاذبة ونظريات المؤامرة بسرعة وفعالية.

شكل 3: عدد الحسابات المزيفة والبوتات التي تعمل على مو اقع التواصل الاجتماعي

المصدر: ترجمة الباحثة،"Social Media Bots: Laws, Regulations, and Platform Policies" p18

2. النفوذ السياسي:

تؤثر البوتات على الرأي العام بشأن الأحداث السياسية، الصحية، البيئية. فعلى سبيل المثال تستطيع بوتات التواصل الاجتماعي الترويج لمرشحين أو أحزاب أو ايديولوجيات محددة، بحيث تطبق تأثيراتها عبر التغذية الغزيرة لمحتويات متحيزة، قد تؤثر على تصورات الناخبين وقراراتهم.

3. التلاعب بالإدراك:

تستطيع البوتات الاجتماعية تزييف شعبية المحتوى والأفراد؛ عبر تضخيم مقاييس التفاعل، مما يخلق تصورات خاطئة لدى المستخدمين.

[1] Nicholas Berente and Carolina Salge, "Is that social bot behaving unethically? ", Communication of the ACM, VOL 60, NO 9 (September 2017), p 29-30.

4. التوجهات السلوكية:

يمكن للبوتات أن تؤثر بشكل كبير على مشاعر المستخدمين وسلوكياتهم، مما يؤدي إلى تغيير في كيفية تفاعلهم مع العالم من حولهم، وذلك من خلال توليد مشاعر إيجابية أو سلبية، تشكل بدورها تصورات للأفراد اتجاه قضايا وأحداث وأشخاص محددين.[1]

من خلال مجالات تأثير البوتات الآنفة الذكر، والتي تشمل ترويج المعلومات المضللة، والنفوذ السياسي، والتلاعب بالإدراك، والتغييرات السلوكية، تتضح الأهمية المتزايدة للبوتات الاجتماعية في تشكيل ديناميكيات منصات التواصل. فهذه الكيانات الآلية لم تعد مجرد حسابات هامشية، بل أصبحت أدوات قوية قادرة على التأثير بعمق على آراء المستخدمين، وتوجهاتهم السياسية، وحتى سلوكياتهم وتصوراتهم تجاه العالم من حولهم.

<u>الفرع الرابع:</u> أبرز التقنيات المستخدمة للكشف عن البوتات في الشبكات الاجتماعية

تطورت تقنيات الكشف عن البوتات في الشبكات الاجتماعية بشكل كبير في السنوات الأخيرة، وذلك لمواجهة التحديات الناتجة عن استخدام الحسابات الآلية للتلاعب بالمعلومات والرأي العام. فيما يلي أبرز التقنيات والأساليب المستخدمة:

1. التعلم الآلي والذكاء الاصطناعي

- **النماذج القائمة على التعلم العميق**: يتم استخدام نماذج مثل الشبكات العصبية التلافيفية (CNN)* ونماذج التعلم العميق مثل VGG19 لتحليل البيانات النصية والسلوكية للحسابات. هذه النماذج أثبتت فعاليتها في الكشف عن البوتات التي تنشر محتوى ضار أو روابط خبيثة.[2]
- **النماذج الهجينة**: مثل نموذج SVM-NN الذي يجمع بين خوارزميات الشبكات العصبية وخوارزميات دعم المتجهات (SVM)*لتحقيق دقة تصل إلى 98% في تصنيف الحسابات.[3]

2. معالجة اللغة الطبيعية (NLP)

- يتم استخدام تقنيات معالجة اللغة الطبيعية لتحليل النصوص التي تنشرها الحسابات على الشبكات الاجتماعية. على سبيل المثال، تم تطبيق تقنيات NLP خلال الانتخابات الرئاسية البرازيلية لتحليل محتوى التغريدات واستخدامها في تصنيف الحسابات كبوتات أو بشر، مما حقق دقة تصل إلى 91%.[4]

---

[1] Caroline Brisset, "Understanding the influence of Social Media Bots", icuc social. accessed on: 14/03/2025. https://2u.pw/rOfjRMNw

* هي نوع متخصص من الشبكات العصبية "NN" فعالة بشكل خاص في معالجة البيانات الشبيهة بالشبكات، مثل الصور ومقاطع الفيديو.

[2] Sneha, B. "Detecting Malicious Twitter Bots using Machine Learning." *International Journal for Research in Applied Science and Engineering Technology* (2024): n. pag.

* هي خوارزمية تعلم آلي خاضعة للإشراف تصنف البيانات من خلال إيجاد خط مثالي أو مستوى فائق يوسع المسافة الفاصلة بين كل فئة في مساحة متعددة الأبعاد.

[3] Sarah, Neamat El-Tazi et al. "Detecting Fake Accounts on Social Media." *2018 IEEE International Conference on Big Data (Big Data)* (2018): 3672-3681.

[4] Gabriel Ferreira, Estavaringo, Bianca Lima Santos, Marcelo Torres do Ó, Rafael Rodrigues Braz and Luciano Antônio Digiampietri. "Social bots detection in Brazilian presidential elections using natural language processing." *Proceedings of the XVII Brazilian Symposium on Information Systems* (2021): n. pag.

3. التحليل الهيكلي للشبكات الاجتماعية

- **التضمين الهيكلي**: يتم استخراج ميزات من بنية الشبكة الاجتماعية، مثل العلاقات بين الحسابات، لتحديد الحسابات الآلية. أظهرت الدراسات أن هذه الميزات توفر قدرة تنبؤية عالية للكشف عن البوتات.[1]
- **التعلم التباين على الرسوم البيانية**: نموذج BotCL يستخدم تقنيات التعلم التباين لتحليل الرسوم البيانية الاجتماعية، مما يتيح الكشف عن البوتات بناءً على أنماط التفاعل بين الحسابات.[2]

4. تحليل سلوك المستخدم

- يتم استخدام تقنيات لتحليل سلوك الحسابات، مثل أنماط النقر (Clickstream Sequences) والتفاعلات الزمنية. هذه الأساليب أثبتت فعاليتها في الكشف عن البوتات التي تحاكي سلوك المستخدمين الحقيقيين.[3]

5. تقنيات التصنيف شبه المراقب

- يتم استخدام تقنيات التصنيف شبه المراقب لتحديد الحسابات الآلية بناءً على التفاعلات الاجتماعية والاتصالات بين المستخدمين. هذه الطريقة تعتمد على نشر العلامات بين الحسابات بناءً على القرب الاجتماعي.[4]

6. استخدام البيانات الوصفية للحسابات

- يتم تحليل البيانات الوصفية للحسابات مثل عدد المتابعين، عدد التغريدات، وتاريخ إنشاء الحساب لتحديد الأنماط التي تشير إلى وجود بوتات.[5]

مع تطور البوتات لتصبح أكثر تعقيدًا، مثل البوتات التي تستخدم الذكاء الاصطناعي لتقليد السلوك البشري بشكل دقيق، يصبح الكشف عنها أكثر صعوبة. لذلك، هناك حاجة لتطوير تقنيات أكثر تقدمًا تجمع بين الذكاء الاصطناعي، معالجة اللغة الطبيعية، وتحليل الشبكات الاجتماعية لضمان دقة الكشف وتقليل تأثير البوتات على المجتمعات الرقمية.

استخدام الذكاء الاصطناعي لتحسين دقة الكشف عن البوتات

الذكاء الاصطناعي يلعب دورًا حيويًا في تحسين دقة الكشف عن البوتات الاجتماعية على منصات التواصل الاجتماعي. فيما يلي أبرز الطرق التي يتم بها استخدام الذكاء الاصطناعي لتحقيق هذا الهدف، مع الإشارة إلى المصادر.

---

[1] Dehghan, Ashkan et al. "Detecting bots in social-networks using node and structural embeddings." *Journal of Big Data* 10 (2023): n. pag.

[2] Li Yan et al, "Social Bot Detection Model Based on Graph Contrastive Learning."

[3] S, Selvarani and Sahana B.R. "Detecting Malicious Social Bots Based on Clickstream Sequences." *International Journal For Multidisciplinary Research* (2023): n. pag.

[4] Stefano Cresci et al. "Bots in Social and Interaction Networks." *ACM Transactions on Information Systems (TOIS)* 39 (2020): 1 - 32.

[5] Alothali, Eiman, et al, "Detecting Social Bots on Twitter: A Literature Review." *2018 International Conference on Innovations in Information Technology (IIT)* (2018): 175-180.

1. استخدام نماذج التعلم العميق

- **نماذج LSTM**: يتم استخدام الشبكات العصبية طويلة المدى (LSTM) لتحليل الأنماط الزمنية في نشاط الحسابات الاجتماعية. هذه النماذج قادرة على التقاط السلوكيات المعقدة للبوتات والبشر، مما يساهم في تحسين دقة التصنيف.[1]
- **نماذج Transformer**: نماذج مثل BERT وGPT-3 تُستخدم لتوليد تمثيلات نصية عالية الجودة، مما يعزز فعالية الكشف عن البوتات. أظهرت الدراسات أن استخدام هذه النماذج أدى إلى تحسين دقة الكشف بنسبة تصل إلى 93% مقارنة بالطرق التقليدية.[2]

2. الكشف متعدد الوسائط

- نموذج الكشف متعدد الوسائط يستخدم معلومات متنوعة مثل النصوص، الصور، وميزات المستخدم الإحصائية. يتم دمج هذه المعلومات باستخدام تقنية "Cross-Modal Residual Cross-Attention" لتحسين دقة الكشف عن البوتات. هذا النموذج أثبت فعاليته في التجارب باستخدام مجموعة بيانات TwiBot-22.

3. استخدام الرسوم البيانية الديناميكية

- إطار عمل يعتمد على الرسوم البيانية الديناميكية لتحليل الأنماط المتغيرة للبوتات والبشر. يتم استخدام وحدات هيكلية وزمنية لدمج السياق التاريخي وسلوكيات المستخدمين المتطورة، مما يعزز دقة الكشف عن البوتات في الشبكات الاجتماعية.[3]

4. تقنيات اختيار الميزات

- **اختيار الميزات الهجينة**: يتم استخدام تقنيات اختيار الميزات لتحليل بيانات الحسابات مثل عدد التغريدات اليومية وعدد المتابعين. أظهرت الدراسات أن استخدام ميزات مختارة بعناية يمكن أن يحقق دقة تصل إلى 94.3% في الكشف عن البوتات.[4]

---

[1] Arin, Efe and Mucahid Kutlu. "Deep Learning Based Social Bot Detection on Twitter." *IEEE Transactions on Information Forensics and Security* 18 (2023): 1763-1772.

[2] El Arbi Abdellaoui et al. "Fine-Tuned Understanding: Enhancing Social Bot Detection with Transformer-Based Classification." *IEEE Access* 12 (2024): 118250-118269.

[3] Wu, Tingxuan, Zhaorui Ma, Yanjun Cui, Ziyi Zhou and Eric Wang. "MSM-BD: Multimodal Social Media Bot Detection Using Heterogeneous Information." *ArXiv* abs/2501.00204 (2024): n. pag.

[4] Hayawi E et al, feature selection approach to identify optimal features of profile metadata to detect social bots in Twitter. *Soc. Netw. Anal. Min.* **11**, 84 (2021).
https://doi.org/10.1007/s13278-021-00786-4

5. الكشف باستخدام البيانات الهيكلية

- **نماذج الرسوم البيانية**: يتم استخدام نماذج تعتمد على الرسوم البيانية لتحليل العلاقات بين الحسابات. على سبيل المثال، نموذج DGBot يستخدم التعلم التبايني لتحليل المعلومات المحلية في الرسوم البيانية، مما يحسن دقة الكشف عن البوتات.[1]

6. الكشف باستخدام الحركة

- **حركة الماوس**: يتم تحليل أنماط حركة الماوس للكشف عن البوتات في المواقع الإلكترونية. أظهرت الدراسات أن هذه الطريقة فعالة في التمييز بين البشر والبوتات بناءً على أنماط الحركة.[2]

[1] Xu, Junhui, et al "DGBot: A DeGlobalizing Graph Transformer Model for Bot Detection." *2024 IEEE/ACIS 27th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)* (2024): 72-75.

[2] Santiago Folch et al. "Web Bot Detection Using Mouse Movement." *2023 JNIC Cybersecurity Conference (JNIC)* (2023): 1-6.

المطلب الثالث: أنواع البوتات الاجتماعية (البوتات السياسية، الدعائية، التضليلية)

هناك عدة تصنيفات لبوتات التواصل الاجتماعي، منها التصنيف الأول الذي يقسم البوتات إلى حميدة؛ أي التي تقدم خدمات مفيدة وتجمع المحتوى تلقائيا، وخبيثة التي صممت بهدف الإضرار[1]، فيما هنالك تصنيف يستند إلى طبيعة الأغراض التي تستهدفها البوتات بحيث نجد:

الفرع الأول: من حيث الاستخدامات

1. **بوتات اجتماعية حميدة (Benign social bots):** تعد بوتات صريحة، توفر وظائف أو فائدة واضحة للمستخدمين سواء كانت إخبارية أو خدماتية أو ترفيهية مثل نشر الوعي بخصوص قضية ما، إدارة الأزمات من خلال الإعلان الواسع النطاق وإصدار الارشادات.
2. **بوتات اجتماعية خبيثة (Malicious social bots):** هي بوتات سرية تشارك في مهام ضارة، مثل نشر معلومات مضللة أو أنظمة احتيال أو رسائل غير مرغوب فيها.[2]

جدول 1: أنواع البوتات واستخداماتها في مو اقع التواصل الاجتماعي

نوع البوت	الاستخدامات الجيدة	الاستخدامات السيئة
بوت عام (General Bot)	تحسين محركات البحث، جمع البيانات.	نشر المعلومات المضللة، التلاعب بالرأي العام.
البوت السياسي (Political Bot)	الحملات الرقمية، تسهيل التواصل مع الجمهور، تعزيز المشاركة الديمقراطية.	نشر المعلومات لإثارة الغضب عبر الاختلافات الاجتماعية والثقافية والمجتمعية، التلاعب السياسي، التأثير على الانتخابات.
بوت دعائي (Propaganda bot)	نشر الوعي حول القضايا الاجتماعية والإنسانية، إدارة الأزمات.	نشر المعلومات المضللة والرسائل المسيئة والتحريضية، التدخل الأجنبي في الشؤون الداخلية للدول.

المصدر: من إعداد الباحثة

من خلال الجدول، يلاحظ أن التمييز بين أنواع البوتات يعتمد بشكل كبير على الهدف من استخدامها وسلوكها في الفضاء السيبراني، وليس فقط على قدراتها التقنية. فالبوت الواحد قد يمتلك القدرة على أداء وظائف متعددة، والنية الكامنة وراء استخدامه هي التي تحدد تصنيفه الفعلي.

[1] Sippo Rossi, op cit, p 63.

[2] Mahmood Sharif and Daniel, ibid, p2.

الفرع الثاني: من حيث الأهداف

1. البوتات السياسية (Political Bots):

تصف مجموعة من البرامج الآلية المبرمجة لتنفيذ مهام وأغراض سياسية، بدءا من نشر الرسائل والتحديثات الإخبارية الموجهة، والتلاعب بالرأي العام، وصولا إلى الحرب الالكترونية. كما تعرف البوتات السياسية بأنها تقنيات حاسوبية تفاعلية وهادفة تستخدم للتأثير على السيطرة الاجتماعية للمعلومات باستخدام البيانات الضخمة[1].

وقد أصبحت أداة تستخدمها الحكومات والجهات السياسية للتأثير على الخطاب السياسي عبر مواقع التواصل الاجتماعي؛ بحيث يمكن استعمالها لنشر معلومات حقيقية على نطاق واسع (بوتات شرعية) أو لنشر أخبار مزيفة أو تغذية الاختلافات المجتمعية والثقافية (بوتات خبيثة)[2].

وقد أوضحت دراسات سابقة، أن عديد المنظمات والحكومات العالمية تعتمد على البوتات، لتحقيق غايات متنوعة، تتراوح بين زيادة مشاركة المواطنين أو دعم قضية سياسية معينة. وقد أشير إلى أن نجاح البوتات السياسية هو تأثير غير عسكري، ويصعب قياس تأثيرها السياسي والاستراتيجي؛ خاصة وأنه يستعصي تحديد التأثير الذي تحدثه على سلوك التصويت، ومع ذلك تشير تقييمات حملات الدعاية الآلية إلى أنها تعتبر أداة فعالة تؤثر على الجمهور المستهدف.

هذا وتتضمن أهداف البوتات السياسية، تضخيم شهرة شخصية سياسية ما أو ترويج فكرة أو موقف سياسي معين، بالاعتماد على خاصية النشر أو الإعجاب أو المتابعة أو المشاركة. كما يمكن لها التصدي وكبح المواقف السياسية المعارضة، عبر قدرتها على تحديد أماكن تواجد المناقشات أو المنشورات أو التعليقات السلبية بالاستفادة من خدمة "تحديد الكلمات الرئيسية"، ومن ثم الولوج إليها، وإغراقها بمحتوى دعائي مضاد معد سلفا[3].

بالإضافة إلى ما سبق، يقدم عدد من الباحثين تفسيرا مختلفا لدور البوتات السياسية؛ إذ يعتبر ر. غوربا ود. غيلبو البوتات الاجتماعية أداة سياسية قوية ذات طبيعة مزدوجة (إيجابية وسلبية) اعتمادا على أهداف استخدامها. فمن ناحية، يمكن استخدامها في عمليات تلاعب منظمة بما في ذلك التأثير الأجنبي، ومن ناحية أخرى، يممكن أن تهدف إلى تعزيز الديمقراطية، وتوسيع الحقوق والفرص، ودعم المبادرات المدنية في الشبكات الاجتماعية[4]. وبالتالي، فإن تصنيف البوتات الاجتماعية في المجال السياسي يعتمد بشكل أساسي على معايير استخدامها (الأهداف، الوظائف، الطرق).

---

[1] Philip N Howard and Samuel C Woolley, " Political Communication, Computational Propaganda, and Autonomous Agents", International journal of communication 10 (2016), 4882-4890.

[2] Michelle Forelle et al, "Political Bots and the manipulation of public opinion in Venezuela", p2.

[3] حيدر إبراهيم المصدر، مرجع سابق، ص131.

[4] В.В. Василькова, Н.И. Легостаева, "Социальные боты в политической коммуникации", RUDN Journal of Sociology, Vol 19, No 1 (2019), p 121-133.

2. البوتات الدعائية (Propaganda bots):

بداية لابد من الإشارة إلى مفهوم الدعاية الحاسوبية (Computational Propaganda) والتي تعرف بأنها "مجموعة من منصات التواصل الاجتماعي والوكلاء المستقلين والبيانات الضخمة المكلفة بالتلاعب بالرأي العام"[1].

أما بخصوص البوتات الدعائية فتعرف بأنها: كيانات آلية تستخدم في حملات الدعاية الحاسوبية للتلاعب بالمناقشات عبر الانترنت ونشر معلومات متحيزة ومضللة لتعزيز أجندات محددة.

ويمكن تلخيص خصائص البوتات الدعائية على النحو التالي:

- ✓ تستخدم في نشر المعلومات، التي يحتمل أن تكون متحيزة أو مضللة، للتأثير على الرأي العام.
- ✓ تساهم في التحيز الخوارزمي، إذ يمكن أن يؤدي نشاطها إلى تفاقم أو إدخال تحيزات في أنظمة المعلومات عبر الانترنت.
- ✓ تعمل عبر شبكات، مما يشير إلى أنها عملية منسقة وواسعة النطاق.
- ✓ ينظر إلى أنشطتها على أنها إشكالية محتملة وتتطلب رقابة[2].

3. البوتات التضليلية:

قبل الخوض في مفهوم البوتات التضليلية، من الضروري توضيح الفرق بين التضليل والدعاية، لتبيان الاختلافات الوظيفية بين البوتات التضليلية والدعائية؛ فالتضليل هو نشر معلومات خاطئة عمدا بهدف الخداع، بينما الدعاية قد تستخدم معلومات صحيحة لتحقيق هدف سياسي، ما يعني أن الدعاية لا تعتمد بالضرورة على الكذب، على عكس التضليل الذي يرتكز على نشر معلومات غير صحيحة، ويكون العامل الحاسم فيه هو نية الخداع[3].

وتعرف البوتات التضليلية بأنها نوع متخصص من حسابات البوتات الاجتماعية الآلية التي يتم تصميمها وبرمجتها بشكل متعمد لنشر معلومات كاذبة، غير دقيقة، أو مضللة، بهدف التأثير على الرأي العام، تغيير المواقف، تشويه الحقائق، أو التلاعب بالمشاعر في سياقات مختلفة[4].

وبهذا تلعب دورا رئيسيا في نشر الأخبار الكاذبة والمعلومات المضللة على وسائل التواصل الاجتماعي، خاصة خلال المراحل المبكرة لانتشارها، وتقوم باستهداف المستخدمين المؤثرين، مما يجعل البشر عرضة للتلاعب وإعادة نشر هذه الأخبار الكاذبة.

[1] Samuel C Woolley, Bots and Computational propaganda: Automation for communication and control, Cambridge university press, p89- 110.

[2] Phlip N Howard and Samuel C Woolley, op cit, p 4885-4887.

[3] Nathaniel Persily and Joshua A. Tucker, social media and Democracy (New York: Cambridge University Press, First published, 2020), p10-p13.

[4] Minnan Luo, how do social bots participate in misinformation spread? A comprehensive dataset and analysis, BETA, 18 Aug 2024.
https://2u.pw/8zNeE

تتمحور أهداف البوتات التضليلية فيما يلي:

- ✓ تضخيم الأخبار الكاذبة لزيادة انتشارها وتأثيرها.
- ✓ استغلال سهولة وسائل التواصل الاجتماعي والتكلفة المنخفضة لإنشاء حسابات مزيفة لنشر المعلومات المضللة على نطاق واسع.
- ✓ استغلال غرف الصدى لاستهداف الأشخاص الأكثر عرضة لتصديق المعلومات المضللة وتخصيصها لهم[1].

كما تجدر الإشارة أنه في واقع الفضاء السيبراني، غالبا ما تتداخل تصنيفات البوتات الاجتماعية بشكل كبير، خاصة عندما يتعلق الأمر بالبوتات السياسية، الدعائية، والتضليلية؛ فالبوت الواحد أو شبكة البوتات (Botnet) يمكن أن تخدم أهدافا متعددة في آن واحد. على سبيل المثال قد يستخدم بوت سياسي لنشر معلومات كاذبة بهدف التأثير على الرأي العام (تضليل)، وفي الوقت نفسه ترويج صورة إيجابية لمرشح معين (دعاية).

[1] Onur Varol, "The spread of fake news by social bots", Bloomington: Indiana university (24 July 2017), p1-16.

المبحث الثاني: البوتات الاجتماعية كتهديد أمني

أحدثت البوتات تحولا في ديناميكيات الفضاء السيبراني؛ فبقدرتها على محاكاة السلوك البشري ونشر المعلومات على نطاق واسع، أصبحت تشكل تهديدا أمنيا متزايدا. يتناول هذا المبحث الدور المتنامي للبوتات الاجتماعية كتهديد أمني، مع التركيز بشكل خاص على أدوارها في سياق الحروب السيبرانية وتأثيراتها على الأمن الوطني، بالإضافة إلى ذلك سيتم استعراض دراسات حالة عالمية لاستراتيجيات بعض القوى الكبرى في مواجهة هذا التهديد الأمني.

المطلب الأول: أدوار البوتات الاجتماعية في الحروب السيبرانية

أمام المشهد المتطور للحروب السيبرانية، أثبتت البوتات الاجتماعية قوتها المتنامية وتأثيرها الملحوظ، فقد تجاوزت هذه الحسابات الآلية كونها مجرد مضايقات رقمية، لتتحول إلى قوى فاعلة في حملات التأثير الممنهجة، والساعية لتحقيق غايات استراتيجية محددة، وقد برزت أدوارها في سياق الحرب السيبرانية على النحو الآتي:

الفرع الأول: جلب الدعم الشعبي

ففي سياق الحرب السيبرانية وحرب المعلومات*، يبرز جلب الدعم الشعبي كهدف استراتيجي مركزي يتم تحقيقه بفعالية متزايدة عبر استخدام البوتات ومنصات التواصل الاجتماعي، فحسب عديد الدراسات، ورد أن روسيا لطالما وظفت المعلومات كسلاح قوي لتعبئة مواطنيها وتقويض الثقة في الخصوم الدوليين، ويؤكد هذا التوجه ما ذكره الخبيران العسكريان الروسيان اللواء الروسي المتقاعد "إيفان فوروبيف" والعقيد المتقاعد فاليري كيسيليوف في منشورهما في المجلة العسكرية "Voyennaya Mysl- Military Thought"، حيث صرحا بوضوح بأن المعلومات تعد نوعا من الأسلحة[1]. وتلعب البوتات الاجتماعية دورا حاسما في هذا المسعى من خلال تضخيم الرسائل المؤيدة لجهة معينة، وتقويض المعارضة بالإضافة إلى حشد التأييد الشعبي؛ مما يوفر غطاء شعبيا للعمليات السيبرانية والإجراءات السياسية والعسكرية.

كما أن الفضاء السيبراني أصبح يمتلك قدرة على تشكيل تحالفات في العالم الافتراضي عبر شبكات التواصل الاجتماعي مثل فيسبوك وتويتر، ويمكن لذلك ان يكون له انعكاسات على أرض الواقع، من جانب ان الحشد الشعبي الذي تسببه يمكن ان يسبب فوضى افتراضية2، تنعكس سلبا على الدول غير المتحكمة أو غير القادرة على مراقبة وتوجيه وإدارة الفضاء السيبراني الموجه لشعبها ومواطنيها. من اجل التأثير على شريحة عريضة من المواطنين والجمهور، وحتى لتوجيههم لسلوك عنفي وعدواني ضد أنظمتهم السياسية.

---

* حرب المعلومات: هي مجموع النشاطات المتخذة بهدف إحراز التفوق المعلوماتي، بجمع ومعالجة معلومات وأنظمة معلومات العدو، مع حماية المعلومات وأنظمة المعلومات الصديقة، ويكمن الفرق بينها وبين الحرب السيبرانية هي حول تعطيل وتدمير الأنظمة الرقمية أما حرب المعلومات فهي بخصوص التأثير على المعلومات والرأي العام.

[1] Jasper Schellekens, "Release the bots of war: social media and artificial intelligence as international cyber-attack", Przegląd Europejski, vol 4 (2021), p 1641-2478.

[2] BENAGOUNE Aissa, cybersecurity challenges of Algerian national security and the role of the legal system in confronting them, Psychology and Education, vol 61(3), (2024),pp 140-165.

الفرع الثاني: شن الهجمات المنسقة

إذ يمكن تنسيق عمل مجموعات كبيرة من البوتات لإغراق صفحات التواصل الاجتماعي بالمنشورات، التعليقات والرسائل، لزيادة عدد المشاهدات والتفاعلات مع محتوى معين بشكل آلي، ما قد يؤثر على تصورات الجمهور ويضغط على صناع القرار، وهو ما برز في سياق الصراع الروسي الأوكراني؛ بحيث أصبحت وسائل التواصل الاجتماعي منفذا للرأي العام، وقد اكتُشف ظهور عدد كبير من حسابات بوتات التواصل الاجتماعي، منها حساب @UAWeapons الذي تبين أنه تعزز من خلال "استراتيجية تجميع الشبكات"، التي طبقتها مجموعة أساسية من حسابات بوتات التواصل الاجتماعي، ما يمكن اعتباره شكلا من أشكال الهجوم المنسق لزيادة ظهور وتأثير هذا الحساب.

هذا ويكشف تحليل محتوى هذا الحساب أنه نشر تغريدات متحيزة لصالح أوكرانيا تحت ستار الحياد، وقد تم إعادة نشر هذه التغريدات بشكل متكرر من قبل البوتات الاجتماعية التي تشاركها نفس الآراء، وهذا يدل على أن البوتات لم تساهم فقط في زيادة عدد المتابعين، بل يمكن اعتبارها أيضا هجوما منسقا لتضخيم رسائل محددة، تخدم أجندات معينة.

بالتالي يمكن توضيح أن البوتات الاجتماعية شاركت في شن هجمات سيبرانية منسقة خلال الصراع الروسي الأوكراني من خلال:

- زيادة مصطنعة في عدد المتابعين لحسابات رئيسية مثل @UAWeapons.
- تضخيم وإعادة نشر المحتوى المتحيز لتعزيز أجندات معينة.
- التنسيق الزمني لنشر التغريدات لتحقيق أقصى قدر من الانتشار.[1]

الفرع الثالث: توسيع نطاق حملات التأثير

إذ حتى عام 2019، كانت البوتات الاجتماعية المستخدمة في حملات التأثير الخبيث والتضليل بسيطة ومحدودة، حيث كانت غير قادرة على توليد تفاعل استراتيجي طويل الأمد، لكن بفضل استخدام أساليب الذكاء الاصطناعي تغير دور البوتات من كونها مجرد أدوات نشر، إلى أن أصبحت قادرة على:

- ✓ تكوين محتوى مزيف بشكل مستقل (نصوص، صور، فيديوهات، deepfakes) دون حاجة لتدخل بشري مباشر في كل خطوة.
- ✓ توليد تفاعل استراتيجي طويل الأمد.
- ✓ تفاعل لغوي طبيعي وأكثر واقعية، مما يجعل من الصعب على المستخدمين التمييز بينها وبين الحسابات الحقيقية.

[1] Liu Qian et al, "Influence of social bots in information warfare: A case study on @UAWeapons Twitter account in the context of Russia- Ukraine conflict", Communication and the public, vol 8 (2023), p 54-80.

✓ أتمتة جوانب مختلفة من حملات التضليل[1].

هذا ما يعني، أن البوتات الاجتماعية كانت في السابق أدوات بسيطة في الحرب السيبرانية، لكن مع التقدم في الذكاء الاصطناعي برز جيل جديد من البوتات أكثر تطورا واستقلالية، قادر على لعب دور أكثر فعالية وتأثيرا في حملات التضليل والتأثير الخبيث.

الفرع الرابع: نشر الدعاية والتضليل المؤيد لأجندات معينة

تعد عمليات التأثير السيبراني "Cyber Influence Operations" أداة محورية في نشر الدعاية والتضليل خلال الحرب السيبرانية، حيث تهدف إلى التأثير على الجماهير المستهدفة وتغيير آرائهم وسلوكهم لتحقيق مصالح وأهداف معينة، وتعتمد هذه العمليات على آليات نفسية ومعرفية مثل:

✓ التحكم الانعكاسي (Reflexive Control): وهو مفهوم روسي يرجع أصله إلى أبحاث فلاديمير ليفبفر Vladimir Lefebvre في علم النفس الحسابي، وقد تطور ليستخدم في تصميم ومراقبة النظم المعقدة قبل أن يعود إلى المجال العسكري، ويعرف على أنه وسيلة للتأثير على قرارات العدو عبر تزويده بمعلومات معدة خصيصا لدفعه على اتخاذ قرارات تخدم مصالح الطرف المبادر. هذا ويعتمد التحكم الانعكاسي على استغلال نقاط ضعف الخصم وتوجيه تفكيره بشكل غير مباشر، وتشمل أساليبه الإلهاء، الحمل الزائد للمعلومات، والخداع، وغيرها[2]. وفي سياق الدعاية والتضليل يعني هذا صياغة معلومات مضللة للتأثير على مورد معلومات الخصم، ونظرته للوضع، مما يجعله يتخذ قرارات تخدم مصلحة الطرف الآخر.

✓ إدارة التصور (Perception Management): هي محاولة التأثير على كيفية فهم الجمهور المستهدف للواقع وتفسيره للأحداث من خلال التحكم في المعلومات التي يتلقونها، بهدف توجيه ردود أفعالهم وسلوكهم بما يخدم أهداف الجهة التي تقوم بعملية التأثير[3].

وتتخذ الدعاية والتضليل أشكالا متنوعة كالأخبار الكاذبة والتزييف السياسي، وغالبا ما تتكامل مع استراتيجيات الحرب الهجينة* وعمليات سيبرانية تقليدية، لخدمة أهداف استراتيجية بدءا من الترويج لأفكار معينة وصولا إلى تقويض الثقة بالحكومة وإضعاف الروح المعنوية للعدو.

---

[1] Kim Hartmann and Keir Giles, "The Next Generation of Cyber-Enabled Information Warfare", Tallinn: NATO CCDCOE Publications (2020), 233-250.

[2] ميلود حمزاوي، مكانة الحرب النفسية في إستراتيجية الولايات المتحدة لمكافحة الإرهاب بعد أحداث 11 سبتمبر، أطروحة دكتوراه، (المدرسة الوطنية العليا للعلوم السياسية، 2022)، ص48- ص50.

[3] David Tayouri, "The Secret War of Cyber Influence Operations and How Identify Them", Cyber, Intelligence, and Security, vol 4, N^0 1 (March 2020), p3-20.

* الحرب الهجينة تشير إلى نوع من أنواع الصراع الذي يجمع بين مجموعة من التكتيكات التقليدية وغير التقليدية، العسكرية وغير العسكرية، لتحقيق أهداف استراتيجية، تتضمن هذه الصراعات عادة مزيجا من الإجراءات مثل الحرب السيبرانية، التضليل، الحرب النفسية، التخريب الاقتصادي، والإرهاب، وأشكال أخرى من النشاط غير التقليدي.

وفي هذا الإطار تلعب البوتات الاجتماعية دورا متزايد الأهمية؛ في تضخيم رسائل الدعاية والتضليل ونشرها على نطاق واسع عبر منصات التواصل الاجتماعي، مما يخلق انطباعات زائفة لدى الرأي العام ويزيد من صعوبة التحقق من المعلومات، وبالتالي تعزيز تأثير عمليات التأثير السيبراني.

المطلب الثاني: تأثير البوتات الاجتماعية على الأمن الوطني

لم يعد الأمن الوطني مفهوما تقليديا محصورا في حماية الحدود الجغرافية فقط، بل امتد ليشمل الفضاء السيبراني الذي بات ساحة جديدة للمخاطر والتهديدات. وفي هذا السياق، تبرز البوتات الاجتماعية كأدوات قوية ذات تأثير متزايد على استقرار الدول وسلامة مجتمعاتها؛ فمن خلال قدرتها على نشر المعلومات على نطاق واسع واستهداف أكبر للجمهور، أصبحت هذه الكيانات الرقمية تشكل تحديا حقيقيا للعمليات السياسية، بدءا من التلاعب بالانتخابات وصولا إلى زعزعة الاستقرار المجتمعي، ومحاولات التحريض على التجمهر والعنف.

الفرع الأول: دور البوتات الاجتماعية في الانتخابات

تلعب البوتات الاجتماعية دورا مؤثرا في العمليات السياسية؛ فمن خلال استغلال نقاط ضعف البنية التحتية لتكنولوجيا المعلومات والاتصالات المستخدمة في الانتخابات، تعمل هذه البوتات كأدوات رئيسية لنشر المعلومات المضللة على نطاق واسع وفق ما يؤثر على الرأي العام، كما تساهم في تضخيم المحتوى المثير للجدل والتلاعب الخوارزمي على المنصات الاجتماعية، مما يخلق انطباعات وهمية بالدعم الشعبي ويؤدي إلى استقطاب الآراء[1]. ونتيجة لذلك، فإن تأثير البوتات على آراء الناخبين وثقتهم في العملية الديمقراطية يصبح كبيرا، مما يعرض نزاهة الانتخابات للخطر، ويشكل تحديا فعليا للأمن الوطني.

هذا وتبرز الانتخابات الأمريكية لعام 2016، والانتخابات النصفية الأمريكية* لعام 2018، والانتخابات الرئاسية الفرنسية لعام 2017، كأبرز النماذج التي تم فيها رصد واستخدام البوتات الاجتماعية بشكل ملحوظ للتأثير على الرأي العام وتوجيه العملية الانتخابية[2].

فقد أظهر التحليل أن البوتات لعبت دورا هاما في توجيه النقاش عبر الانترنت خلال انتخابات 2016، حيث نجحت في تعزيز التفاعلات بنفس معدل المستخدمين البشريين، مما ساهم في انتشار الأخبار الكاذبة.

---

[1] Cristian Cucoreanu, "Cyber Risks to National Security: Manipulation of the Electoral Process Through the Use of Bots and Algorithms on Social Platforms", European Journal of Law and Public Administration, vol 11, Issue 2 (2024), p 226-236.

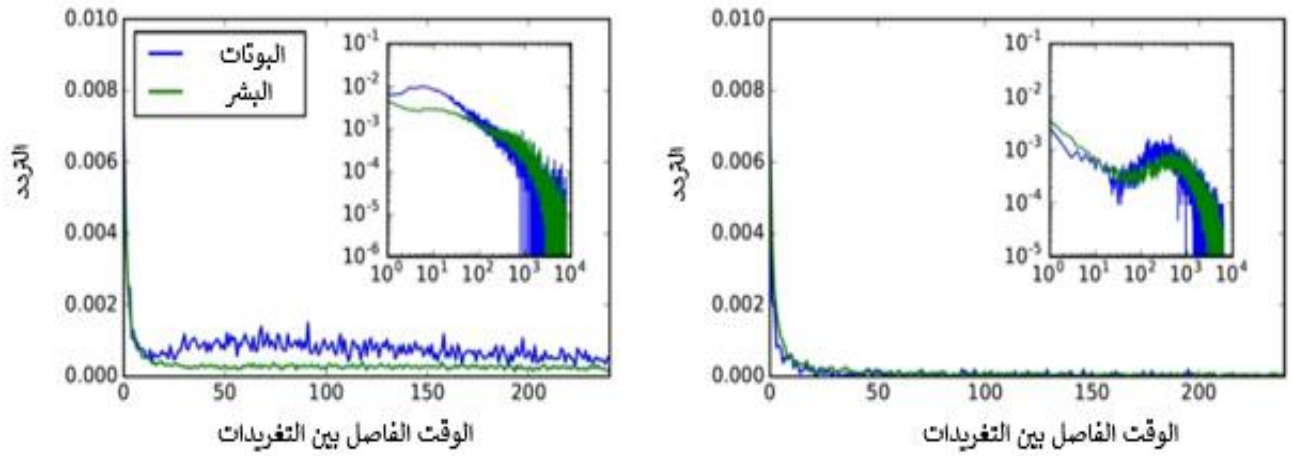
* الانتخابات النصفية في الولايات المتحدة الأمريكية هي الانتخابات العامة التي تجرى في منتصف ولاية الرئيس البالغة أربع سنوات، وتسمح بتجديد جميع مقاعد مجلس النواب، بالإضافة إلى ثلث مقاعد مجلس الشيوخ.

[2] Emilio Ferrara, "Bots, elections, and social media: a brief overview", USC Information Sciences Institute, (Oct 2019), p 1-21.

وفي انتخابات فرنسا 2016، استخدمت البوتات الاجتماعية بشكل مكثف لنشر حملة تضليل إعلامي تحت اسم "MacronLeaks"، وقد تم رصد بداية الحملة على تويتر في 30 أفريل، وبلغت ذروتها قبل يوم من الانتخابات، وقد تبين أن المستخدمين المتفاعلين مع هذه البوتات كانوا في الغالب أجانب. كما تم اكتشاف إعادة استخدام بوتات من انتخابات 2016 في انتخابات 2017، ما فتح احتمالات وتوقعات حول إمكانية وجود سوق سوداء للبوتات السياسية القابلة لإعادة الاستخدام[1].

أما بالنسبة لانتخابات التجديد النصفي الأمريكية لعام 2018، فقد تبين أن البوتات كانت حاضرة بنفس القدر تقريبا كما في الأحداث السابقة، ولعبت البوتات المحافظة دورا مركزيا في شبكة إعادة التغريد. وقد كشفت مقارنة بين عامي 2016 و2018 عن وجود نواة كبيرة من المستخدمين النشطين في كلا الحدثين، كان 12.1 ٪ منهم بوتات. كما أشارت النتائج إلى أن البوتات قد تطورت لتقليد الأنماط الزمنية للنشاط البشري بشكل أفضل[2].

شكل 4: مقارنة وتيرة تغريد البوتات والبشر في الانتخابات الأمريكية (2016 و2018)



المصدر: ترجمة الباحثة لمعطيات Emilio Ferrara, "Bots, elections, and social media: a brief overview", p 15

تظهر هذه الأشكال كيف تطورت أنماط التغريد للبوتات بين عامي 2016 و2018؛ بحيث في عام 2016 (الشكل الأيسر) كان من السهل نسبيا التمييز بين البوتات والبشر خلال الوقت الفاصل بين تغريداتهم، أين كانت البوتات تنشر التغريدات بسرعة متقاربة جدا، مما أدى إلى ارتفاع حاد في التردد عند الفواصل الزمنية، لكن بحلول انتخابات 2018 (الشكل الأيمن) أصبحت البوتات أكثر تطورا وبدأت في تقليد أنماط التغريد البشرية بشكل أفضل، وانخفض التردد العالي للتغريدات السريعة المتتالية، وهو ما جعل سلوكها الزمني أقرب لسلوك البشر ومن الصعب اكتشافه.

[1] Ibid, p 7-11.

[2] Ibid, p 11-15.

بالتالي ومن خلال الأحداث السياسية والانتخابية الآنفة الذكر يتضح دور البوتات الاجتماعية وسعيها الحثيث للتأثير على مسار هذه العمليات؛ فهي تعمل على نشر المعلومات وتضخيمها، وتتبنى سلوكيات تحاكي المستخدمين الحقيقيين بهدف تشكيل الرأي العام والتأثير في نتائج الانتخابات.

الفرع الثاني: البوتات الاجتماعية والإرهاب السيبراني

أضحت البوتات الاجتماعية المدعومة بالذكاء الاصطناعي، أداة متنامية الخطورة في مجال الإرهاب السيبراني. فمع قدرتها المتزايدة على محاكاة السلوك البشري وانتحال شخصيات المستخدمين العاديين، تتيح البوتات للتنظيمات الإرهابية مزايا لتعزيز كفاءة أنشطتها على منصات التواصل الاجتماعي؛ إذ يمكن استخدامها لتجنب الاكتشاف والحظر من قبل المستخدمين والمنصات على حد سواء[1]، إلى جانب ذلك تعلب البوتات الاجتماعية دورا في خلق وهم بالتفاعلات الحقيقية، مما يعزز مصداقية الرسائل المتطرفة ويساهم في التلاعب الاجتماعي وتجنيد أعضاء جدد ونشر الأيديولوجيات[2].

وهذا يمكن للبوتات الاجتماعية أن تساهم في الإرهاب السيبراني من خلال:

- نشر وتوسيع نطاق الأيديولوجيات المتطرفة والمحتوى الإرهابي.
- تجنيد أعضاء جدد من خلال توجيه رسائل مقنعة وتكوين شعور بالانتماء.
- نشر الدعاية لتحسين صورة الإرهاب وتبرير العنف وتشويه صورة الخصوم.
- إنشاء شبكات دعم وهمية لزيادة المصداقية الظاهرية للمحتوى المتطرف.
- التلاعب بالرأي العام ونشر معلومات مضللة لخلق بيئة مؤيدة للتطرف.

كما تجدر الإشارة أنه وبالإضافة إلى الأنشطة المذكورة، يمتد دور البوتات الاجتماعية ليشمل مراحل ما بعد وقوع الهجوم الإرهابي، حيث يكمن استخدامها في نشر سرديات آلية* معينة كالإدانة أو التعاطف، وحتى محاولة التأثير على تفسير الأحداث وتوجهات الرأي العام اللاحقة. وهو ما حدث على خلفية الهجوم الإرهابي الذي وقع في فيينا في 02 نوفمبر2020* ، أين برز استخدام للبوتات الاجتماعية على موقع تويتر؛ والتي تراوحت بين بوتات لنشر الشائعات وأخرى

[1] Daniele Maria Barone, "Social bots and synthetic interactions to stage digital extremist armies", Sicurezza, terrorismo e società, Italian Team for Security, 16 (2022), p87-112.

[2] Marc- André Kaufhold and Christian Rauter, "Social Media Misuse- cultural violence, Peace and Security in digital Networks", Science Peace Security '19, Germany: Conference on Technical Peace and Security Research, 2019, p 61-66.

* السرديات الآلية: هي مجموعة من الرسائل المترابطة حول موضوع معين، يتم نشرها عبر وسائل التواصل الاجتماعي، وتلعب البوتات دورا فعالا في تشكيل هذه السرديات، خاصة في أوقات الأزمات.

* سلسلة من حوادث إطلاق النار المتزامنة في عدة مواقع بوسط مدينة فيينا، أسفرت عن مقتل خمس أشخاص، وإصابة العشرات.

لنشر اتهامات ضد مسؤولين حكوميين من دول مختلفة، والإشارة إلى هجمات إرهابية أخرى، وإبراز نقص الدروس المستفادة، هنا يبرز دور البوتات في تأجيج النقاشات السلبية وتبادل الاتهامات[1].

الفرع الثالث: دور البوتات الاجتماعية في تعزيز الاستقطاب المجتمعي

الاستقطاب المجتمعي يشير إلى الانقسامات الأيديولوجية والثقافية داخل المجتمعات، التي تؤدي إلى تدهور الاستقرار الاجتماعي[2]، وتلعب البوتات الاجتماعية دورا في تعميقه؛ فهي تخلق انطباعات زائفة بوجود أغلبية لرأي ما عبر نشر رسائل مكثفة، مما يؤدي إلى تهميش الآراء المخالفة خوفا من العزلة الاجتماعية؛ وهو ما نجد له تفسيرا في نظرية دوامة الصمت (Spiral of silence Theory)*.

أي أن الترويج الشعبي الزائف، يعمل على تضخيم آراء محددة في مقابل تهميش آراء أخرى، مما يقلل من تنوع النقاش العام ويزيد من حدة الانقسامات الموجودة[3].

بالإضافة إلى ذلك، تستخدم البوتات لنشر معلومات مضللة وأخبار كاذبة بهدف تأجيج المشاعر السلبية تجاه مجموعات معينة وتعزيز وجهات النظر المتطرفة، الأمر الذي يزيد من حدة الاستقطاب ويجعل إيجاد حلول وسط بين الأطراف المتنازعة أكثر صعوبة.

ويرتبط الاستقطاب المجتمعي بشكل وثيق بانتشار المعلومات الخاطئة والمضللة، والذي جاء في المرتبة الأولى ضمن أقوى المخاطر العالمية على المدى القصير؛ وذلك على اعتبار أن المجتمعات المستقطبة تكون أكثر عرضة لتصديق المعلومات التي تؤكد معتقداتها القائمة، بغض النظر عن صحتها[4].

---

[1] Mark Strembeck et al, "Automated Narratives on the Influence of Bots in Narratives during the 2020 Vienna Terror Attack", Austria, p 1-11.

[2] "خطر يهدد الديمقراطية والتماسك.. ما هو الاستقطاب المجتمعي؟ "، الحرة- دبي، 17 جانفي 2024، تاريخ الاطلاع: 2025/04/13.

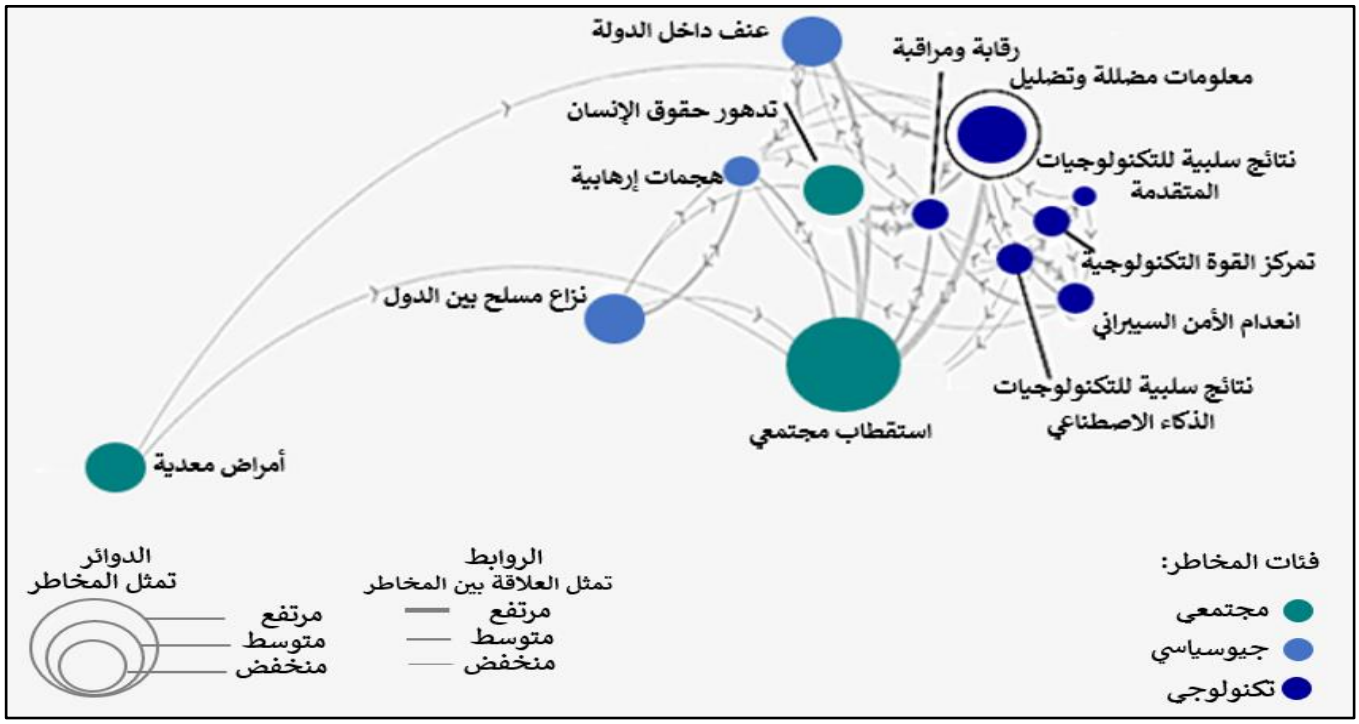
https://2u.pw/awGw6

* نظرية دوامة الصمت: هي نظرية في العلوم السياسية واتصالات الجماهير تفترض أن تصور الفرد لتوزيع الرأي العام يؤثر على استعداده للتعبير عن آرائه، بحيث يميل الأفراد الذين يعتقدون أن آرائهم أقلية إلى الصمت خوفا من العزلة الاجتماعية.

[3] Bjorn Ross et al, "Are social bots a real threat? An agent-based model of the spiral of silence to analyze the impact of manipulative actors in social networks, European Journal of Information Systems, vol 10 (2020), p 1-50.

[4] Switzerland, World Economic Forum, The Global Risks Report 2024 19th Edition, January 2024, p20.

شكل 5: ديناميكيات المخاطر العالمية: تحليل للترابط والتأثيرات المتبادلة



المصدر: "The Global Risks Report 2024 19th Edition", p21

يُظهر الشكل الروابط بين مختلف المخاطر العالمية، ويقع الاستقطاب المجتمعي والمعلومات المضللة والتضليل في مركز الاهتمام، بحكم ارتباطهما الوثيق، بالإضافة إلى تأثيرهما على ديناميكيات المخاطر الأخرى في النظام العالمي.

هذا وتجدر الإشارة إلى أن انتشار البوتات الاجتماعية التي تعمل على تضخيم الأصوات المتطرفة يزيد من حدة هذه المخاطر؛ فالبوتات تعزز من حالة الاستقطاب؛ بحيث يميل الأفراد إلى التفاعل بشكل أكبر مع المعلومات التي تدعم وجهات نظرهم المروجة بشكل مكثف من قبل هذه البوتات، بالتالي يصبح من الصعب عليهم تقبل آراء مناقضة. وكمحصلة نهائية تصبح البوتات الاجتماعية أداة قوية لتكريس الانقسامات المجتمعية وتعميقها.

المطلب الثالث: دراسات حالة عالمية (الولايات المتحدة الأمريكية، الصين)

الفرع الأول: الاستراتيجية الأمريكية في مواجهة البوتات الاجتماعية

تتسم الجهود الأمريكية لمواجهة البوتات الاجتماعية على المستوى الوطني بالتطور التدريجي، فبينما لاتزال القوانين الفيدرالية الشاملة قيد التشريع، توجد محاولات فعلية في الكونغرس لسن قوانين تلزم منصات التواصل الاجتماعي بالكشف عن استخدام البوتات وتقييده في العمليات السياسية، من ضمنها:

1. مشروع قانون الإفصاح والمساءلة عن البوتات (The Bot Disclosure and Accountability Act) في 2018 الذي قدمه السيناتور ديان فأينشتاين Diane Feinstein والذي يحتوي بدوره على جزئين أساسيين:

- إلزام منصات التواصل الاجتماعي بوضع سياسات تأمر المستخدمين بالكشف عن استخدام برامج آلية تنوي الظهور أو العمل كبشر.
- حظر استخدام البوتات من قبل المرشحين السياسيين والأحزاب السياسية.

لكن مشروع هذا القانون لم يتجاوز المراحل الأولية في الكونغرس ليصبح قانونا نافذا[1].

2. طرح مشروع "قانون الدفاع عن الأمن الأمريكي من عدوان الكرملين" (The Defending American Security from Kremlin Aggression Act) الذي كان يحظى بدعم الحزبين في مجلس الشيوخ الأمريكي، وقد تضمن قسما بعنوان "قانون منع الجرائم الإلكترونية الدولية"، الذي سعى إلى تعزيز قدرة السلطات الفيدرالية في قمع شبكات البوتات المستخدمة في مجموعة من الأنشطة غير القانونية، لكنه وعلى غرار المشروع السابق لم يصبح قانونا في شكله العام.

3. نشر ورقة سياسات بيضاء* بعنوان "مقترحات سياسات محتملة لتنظيم شركات وسائل التواصل الاجتماعي والتكنولوجيا" من قبل السيناتور مارك وارنر (Mark Warner) في 2018 والتي اقترح فيها 20 خيارا قانونيا وتنظيميا لحماية مستخدمي وسائل التواصل الاجتماعي ووقف انتشار المعلومات المضللة، وفيما يتعلق بالبوتات اقترحت إجبار المنصات على وضع علامات على البوتات، إلى جانب تحديد الحسابات غير الأصلية ووقفها[2].

كما حددت ثلاث مجالات رئيسة يجب على صانعي السياسات أن يركزوا عليها وهي مكافحة التضليل وحماية المستهلك الرقمي، إلى جانب تعزيز المنافسة والابتكار في قطاع تكنولوجيا الاتصالات ووسائل التواصل الاجتماعي[3].

كنتيجة، يمكن فهم أن مواجهة الولايات المتحدة للبوتات الاجتماعية تتم حاليا وبشكل أساسي من خلال ممارسات الإشراف على المحتوى التي تطبقها منصات التواصل الاجتماعي ذاتها[4]. ومع ذلك هناك نقاش متزايد في الكونغرس حول

---

[1] USA, CNA Information Memorandum, Social Media Bots: Laws, Regulations, and Platform Policies, 2020, p 6-7.

* ورقة السياسات البيضاء هي وثيقة رسمية تصدرها الحكومة أو هيئة حكومية لتوضيح مقترحاتها لسياسات أو تشريعات حول موضوع معين، وهي بمثابة وثيقة استشارية ونقطة بداية للمناقشات، وليست قانونا ملزما.

[2] Ibid, p 7-8.

[3] U. S Sen Mark R. Warner, White Paper "Potential Policy for Regulation of Social Media and Technology Firms", p 1-23.

[4] Cho Clare Y and Zhu Ling, "Social Media Dissemination and Moderation Partices ", Congressional Research Service, March 20, 2025, p 1-23.

إمكانية التدخل التشريعي لتنظيم هذه الممارسات بشكل أكبر، وهو ما قد يؤدي إلى استراتيجيات أكثر تحديدا وفعالية لمواجهة التحديات التي تفرضها البوتات.

الفرع الثاني: الاستراتيجية الصينية في مواجهة البوتات الاجتماعية

يتجلى واقع الاستراتيجية الصينية في مواجهة البوتات الاجتماعية من خلال فهمها المعمق لتعقيد المشهد الرقمي، حيث لم تعد منصات التواصل الاجتماعي مجرد مساحات للتفاعل البشري، بل أصبحت بيئات ديناميكية يتداخل فيها وجود الانسان مع نشاط البوتات الاجتماعية. وتدرك الصين تمام الإدراك الدور المتزايد الذي تلعبه هذه الكيانات الآلية في صياغة الأجندات الإعلامية والتأثير على الرأي العام، مدركة أن هذا التأثير لا يقتصر على البيئة الرقمية بل يمتد ليشمل التصورات الواقعية[1]. وفي هذا السياق، تنطلق الاستراتيجية الصينية من منطق حماية فضائها السيبراني ورأيها العام المحلي من التلاعب الخارجي، مع تبني رؤية استباقية تتجاوز حدود الدفاع التقليدي نحو محاولة التأثير في الرأي العام العالمي.

ويمكن توضيح أهم معالم الاستراتيجية الصينية في مواجهة البوتات الاجتماعية على النحو التالي:

1. **نظام الدفاع (Defense System):**

يهدف هذا الشق إلى حماية الفضاء الإلكتروني الصيني والرأي العام المحلي من التلاعب الأجنبي، ويتضمن عدة تدابير وقائية:

- الفحص القائم على الذكاء الاصطناعي للحسابات الاجتماعية العامة (AI Screening Of Public Social Accounts): استخدام تقنيات الذكاء الاصطناعي لفحص وتحليل الحسابات النشطة على منصات التواصل الاجتماعي الصينية، بغرض تحديد الحسابات المشبوهة التي يحتمل أن تكون بوتات اجتماعية تديرها جهات أجنبية. ويمكن أن يشمل ذلك تحليل أنماط التغريد، ومعدل النشاط، وشبكات التفاعل للكشف عن السلوك الآلي أو المنسق.
- إدخال لوائح ذات صلة لتوحيد سلوك وسائل الإعلام (Introducing Relevent Regulations to Standardize the Behavior of the Media): وضع قوانين ولوائح تنظم عمل وسائل الإعلام ومنصات التواصل الاجتماعي داخل الصين. يمكن أن تهدف هذه اللوائح إلى منع نشر المعلومات المضللة أو التحريضية التي قد تنشرها البوتات الاجتماعية، بالإضافة إلى مساءلة المنصات عن السماح بانتشار مثل هذه الأنشطة.
- منع تدخل رؤوس أموال ودول أخرى وروبوتاتها الاجتماعية (Preventing the interference of other Countries' Capital and Social Bots): اتخاذ إجراءات لمنع التمويل الأجنبي الذي قد يستخدم لدعم أنشطة

[1] Zeyang Feng et al, "Social Robots and Internet Opinion Rights", Journal of New Media and Economics, Vol 1, No 4 (2024), p20-28.

البوتات الاجتماعية أو التأثير على وسائل الإعلام الصينية، ويشمل ذلك أيضا جهودا استخباراتية وأمنية لتحديد وتعطيل شبكات البوتات الاجتماعية التي تديرها دول أخرى بشكل مباشر أو غير مباشر[1].

2. استراتيجية الدفاع الذاتي (Self-Defense Strategy):

يركز هذا الشق على اتخاذ مبادرات استباقية في الفضاء الإلكتروني العالمي، بهدف فهم وتشكيل الرأي العام العالمي.

- النشر النشط للبوتات الاجتماعية في الخارج لفهم المشاعر العامة والرأي العام في الدول الأخرى: أي نشر بوتات على منصات التواصل الاجتماعي الأجنبية، هدفها الظاهري مراقبة وتحليل المشاعر والاتجاهات في الرأي العام للدول الأخرى.
- إظهار سلوك الصين كقوة عظمى وخلق فضاء رأي عام عالمي أكثر انفتاحا وتسامحا: يهدف هذا الجانب إلى استخدام الأدوات الرقمية، بما في ذلك البوتات الاجتماعية المنشورة في الخارج، لتقديم صورة إيجابية عن الصين، وتعزيز وجهات نظرها على الساحة الدولية. كما يهدف إلى المساهمة في خلق بيئة إعلامية عالمية ينظر إليها على أنها أكثر انفتاحا وتسامحا[2].

بالتالي، يتضح أن الاستراتيجية الصينية في مواجهة البوتات الاجتماعية تتشكل عبر نهج شامل؛ يجمع بين بناء دفاعات قوية لحماية فضاءها السيبراني ومحاولة التأثير بشكل استباقي في الرأي العام العالمي. بحيث تعتمد هذه الاستراتيجية على الاستفادة من التكنولوجيا المتقدمة، وتعزيز الأطر القانونية، وتبني رؤية استراتيجية منظمة لإدارة عمليات التأثير في ساحة معركة الرأي العام الرقمي. لكن مع ذلك تثير هذه الاستراتيجية تساؤلات حول الاعتبارات الأخلاقية والقانونية المتعلقة بالتأثير في الرأي العام للدول الأخرى.

[1] Ibid, p21-23.

[2] Ibid, p23-27.

خلاصة

بناء على ما تم تحليله في هذا الفصل، يمكن استخلاص النتائج التالية:

- تعد البوتات الاجتماعية أدوات قوية ومتعددة الاستخدامات في الفضاء السيبراني، وتشكل تهديدا فعليا للأمن والاستقرار على مختلف المستويات.
- يتطلب فهم التهديدات الناجمة عن البوتات الاجتماعية تحليلا دقيقا لأنواعها المختلفة، سواء من حيث الغرض من استخدامها (خبيثة أو حميدة)، أو الأهداف التي تسعى إلى تحقيقها (سياسية، تضليلية، دعائية)، فإن هذا التصنيف يساعد في تحديد طبيعة الخطر وطرق التعامل معه.
- للبوتات الاجتماعية دور محوري في مجريات الحروب السيبرانية، حيث تستخدم كأداة قوة ناعمة للتأثير في الرأي العام وزعزعة الاستقرار الداخلي للدول المستهدفة.
- تشكل البوتات الاجتماعية تهديدا مباشرا للأمن الوطني، من خلال قدرتها على التدخل في العمليات الانتخابية، واسهاماتها في خدمة أنشطة الجماعات الإرهابية، وتعميق الانقسامات المجتمعية.
- تختلف استراتيجيات الدول الكبرى في مواجهة تهديد البوتات الاجتماعية، حيث تتراوح بين النهج القانوني والرقابي في الولايات المتحدة الأمريكية، في مقابل النهج الدفاعي والاستباقي في الصين، مما يعكس اختلاف الأولويات والأنظمة السياسية في التعامل مع هذا التحدي المشترك.

الفصل الثاني: السياسة الأمنية الجزائرية في مواجهة التهديدات السيبرانية

تمهيد

في ظل الأوضاع الأمنية غير المستقرة التي تشهدها المنطقة العربية عموما، ودول الجوار الجزائري خصوصا، بالإضافة إلى التطورات التكنولوجية المتسارعة التي يعرفها عالم اليوم؛ لم تعد السياسة الأمنية الجزائرية مقتصرة على حماية السيادة والوحدة الوطنية، والحفاظ على الاستقرار من خلال الاعتماد على الطرق التقليدية فقط، بل تجاوزتها لتشمل مسألة حماية أمن الدولة والمجتمع من التهديدات الجديدة التي أفرزتها الثورة التكنولوجية الحديثة، من خلال السعي لتحقيق الأمن السيبراني باعتباره أحد أولويات السياسة الأمنية الجزائرية.

وعليه ينطلق هذا الفصل من تحديد الإطار العام للسياسة الأمنية الجزائرية ومحاولة تكيفها مع ما هو مستجد من تهديدات سيبرانية عن طريق تعزيز البنية المؤسساتية والقانونية ومن خلال التعاون الدولي، لبناء استراتيجية وطنية شاملة للأمن السيبراني، ليصل إلى إبراز التحديات التي تواجه السياسة الأمنية الجزائرية في المجال السيبراني.

المبحث الأول: الإطار العام للسياسة الأمنية الجزائرية

تعتبر السياسة الأمنية الجزائرية إطار شاملا لحماية المصالح العليا للبلاد، وتشمل في طياتها اهتماما كبيرا بالأمن السيبراني، ومن خلال الاستراتيجيات المتبعة تسعى الجزائر إلى بناء نظام أمني متكامل وقادر على مواجهة التحديات المتزايدة في عالم رقمي متغير، لذلك يسعى هذا المبحث إلى تحليل كيفية تفاعل السياسة الأمنية الجزائرية بمرتكزاتها التاريخية والجغرافية والإيديولوجية، مع متطلبات الأمن السيبراني وذلك من خلال دراسة الاستراتيجيات المتبعة والمؤسسات المسؤولة عن هذا الملف الحيوي.

المطلب الأول: مرتكزات السياسة الأمنية الجزائرية

بداية نشير إلى أن السياسة الأمنية تحدد بموضوعها وليس بالاسم الذي تحمله، فقد تسمى "خطة"، "استراتيجية"، "عقيدة"، لكن عموما السياسة الأمنية أشمل من العقيدة والاستراتيجية. فالسياسة الأمنية تكون ذات طبيعة شاملة كونها تشمل البعدين الداخلي والخارجي ومختلف قطاعات الأمن (العسكرية، السياسية، المجتمعية، الاقتصادية، البيئية)، في تحديد مختلف المخاطر والتهديدات، بتحديد طبيعتها كما تقرر الاستراتيجيات التي يتعين وضعها والوسائل التي يجب تعبئتها.

كما تعرف السياسة الأمنية بأنها: "مجموع البرامج والخطط المتبعة من السلطات (السياسية والأمنية) لتوفير أكبر قدر من الحماية الداخلية والخارجية للأمن الوطني والقومي بكل أبعاده ومستوياته ومقوماته وذلك بهدف المحافظة على النظام العام، وكذلك استقرار أمن الدولة، وبالتالي الحفاظ على استمرارية فعالية النظام"[1]

تعرف أيضا بأنها: ذلك التصور الأمني المحدد للمنهجية الأمنية للدولة وأفضل السبل لتحقيقها، وفقا لإيديولوجية قائمة على نظام فكري متجانس، يوفر تفسيرات معينة للواقع، ويترتب عن ذلك تبني القوى النافذة في المجال الأمني لهذه التفسيرات والرؤى، وبالتالي تجسيدها كسياسة أمنية لدولة ما"[2]

ترتكز السياسة الأمنية الجزائرية على جملة من العوامل التاريخية والجغرافية والأيديولوجية، وقد مرت بمراحل هامة ساهمت في بلورتها وتكييفها مع المعطيات والظروف المحلية والإقليمية والدولية.

الفرع الأول: المرتكز التاريخي

يعد العامل التاريخي من أهم مرتكزات السياسة الأمنية؛ بحكم أن التجارب التاريخية السابقة تساهم في صياغة تلك السياسة وتحدد أسسها. وبالرجوع للإرث التاريخي الجزائري فهو يتجسد من خلال نضالها ضد كل الامبراطوريات والدول التي احتلتها أو حاولت احتلالها عبر فترات زمنية متعاقبة كالاحتلال الفينيقي (814 ق.م- 146ق.م)، الروماني (146 ق.م-

[1] ولاء الدين سعيد خطاب وعماد مفتاح فرج، "السياسة العامة وعلاقتها بالسياسة العامة الأمنية (دراسة مفاهيمية)"، مجلة المعهد العالي للدراسات النوعية م3، 15ع، (2023)، ص 4615-4650.

[2] الطاهر بن خرف الله، النخبة الحاكمة في الجزائر 1962-1982: بين التصور الإيديولوجي والممارسة السياسية، (الجزائر: دار هومة للنشر والتوزيع، ج1، 2007)، ص105.

429 م)، الوندالي (429م- 534م)، البيزنطي (534م- 647م) وصولا إلى الاستعمار الحديث الذي تجسد في الاحتلال الفرنسي ؛ وبذلك كان إرث المقاومة عامل أساسي ومؤثر في رسم معالم السياسة الأمنية الجزائرية، [1] إذ نجد وبالرغم من أن الاحتلال الفرنسي للجزائر حاول طمس الشخصية والهوية الجزائرية، إلا أن مشروعه فشل بسبب مقاومة الشعب الجزائري لاسترداد السيادة الوطنية، وتمسكه بهويته العربية الإسلامية ومبادئه الوطنية؛ وبذلك تعد الثورة التحريرية ضد الاستعمار بمبادئها وقيمها أحد أهم منطلقات بناء السياسة الأمنية ورسم التزاماتها داخليا وخارجيا.[2]

إذا سياسة الجزائر الأمنية عموما وعقيدتها للأمن القومي خصوصا، هي نتيجة المخيال الثوري للنضال ضد الاستعمار والثورة التحريرية (1954-1962)، فضلا عن الأزمة الأمنية لتسعينات القرن الماضي، كتاريخين مفصليين لعبا دورا حاسما فيما تسميه جوتا والدز *Jutta Weldes "المخيال الأمني" أي بنية معان وعلاقات اجتماعية راسخة، انطلاقا منها تنشأ تمثلات عالم العلاقات الدولية؛ التي تسمح بتوضيح من نحن؟ وماذا نمثل؟ ومن هم أعداؤنا والطريقة التي يهددنا بها هؤلاء وكيف يمكننا أن نفعل ما بوسعنا لمعالجة تلك التهديدات؟ [3]

ومنه نجد أن المتغير التاريخي يظل حاضرا ولا يزال يطبع السياسة الأمنية الجزائرية على نحو دفاعي، ووفقا لقيم ومبادئ تحولت مع مرور الزمن إلى ثوابت، مثل رفض التواجد الأجنبي على التراب الجزائري، وعدم التدخل في الشؤون الداخلية للدول وكذا دعم حركات التحرر العادلة.

الفرع الثاني: المرتكز الجغرافي

الجغرافيا عامل ومرتكز هام في الجانب الأمني، بناء على العلاقة الوطيدة التي تجمع الجغرافيا بالسياسة، فيما يعرف بالجيوبوليتيك* إذ أن الموقع الجغرافي للدولة يساعد بشكل كبير في صياغة السياسة الأمنية للدولة، فموقع الجزائر في نقطة تقاطع استراتيجية مهمة بتوسطها لعدة دول مغاربية، وكذلك توسطها لمنطقتين جغرافيتين مهمتين؛ الأولى في الشمال أو ما يعرف بالبحر الأبيض المتوسط، والثانية في الجنوب ممثلة بالساحل والصحراء الكبرى، جعل الأمن

[1] سليم بوسكين، "العقيدة الأمنية الجزائرية وإشكالية التكيف مع التهديدات الجديدة"، مجلة العلوم القانونية والسياسية، جامعة الجزائر3، م10، ع02 (سبتمبر 2019)، ص1328-1347.

[2] نور الدين فلاك، "دور العقيدة الأمنية الجزائرية في مواجهة التهديدات الأمنية الجديدة"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، م4، ع2، (2019)، ص 1083-1100.

* جوتا والدز Jutta Weldes هي أستاذة علاقات دولية في جامعة بريستول، تركز اهتماماتها البحثية على الثقافة الشعبية والسياسة العالمية، وهي محررة كتاب البحث عن عوالم جديدة: الخيال العلمي والسياسة العالمية.

[3] عبد النور بن عنتر، "سياسة الجزائر الأمنية: تحولات ومعضلات في سياق القلاقل إقليميا والحراك داخليا"، مجلة سياسات عربية م10، ع55، (مارس2022)، ص 24.

* يعد رودلف كيلين Rudalf Kiellen أول من استخدم مصطلح الجيوبوليتيك Geopolitics والتي عرفها بأنها الدور الذي يمكن أن يلعبه الموقع الجغرافي في خدمة الدولة؛ أي بعبارة أكثر دقة كيف يمكن لصانع القرار جعل الموقع الجغرافي كمصدر قوة للدولة في التعبير عن مواقفها السياسية؟

الجزائري ينكشف على عدة جهات، ومنه فإن صياغة السياسة الأمنية الجزائرية دائما ما تأخذ في الاعتبار هذا الانكشاف الأمني.[1]

إن مساحة الجزائر 2.381.741 كلم[2] ، إذ تحتل المرتبة العاشرة عالميا من ناحية المساحة الجغرافية، وتحتل المرتبة الأولى عربيا وإفريقيا بعد التقسيم الذي عرفه السودان سنة 2011م، هذا الموقع له عواقب أمنية على الأمن الوطني مع تزايد انتشار التهديدات اللاتماثلية، فصعوبة التغطية العسكرية للمناطق الحدودية، وخاصة الجنوبية بفعل شساعتها شكل ولا يزال يشكل أكبر التحديات أمام المؤسسة العسكرية ومختلف الأجهزة الأمنية في الجزائر، فمشكلة اتساع الحدود مع صعوبة التنبؤ بتحركات الجماعات الإرهابية والجريمة المنظمة ومشاكل التهريب وحركات الهجرة غير الشرعية.[2]

إن مستويات تأثير عامل الجغرافيا على طبيعة السياسة الأمنية للجزائر متنوعة، فإلى غاية انتهاء الحرب الباردة مثلت قضايا دعم حركات التحرر في العالم والدفاع عن مكانة الجزائر كقوة إقليمية أحد أهم عناصر هذه السياسة، أما في ظل التحولات التي تلت نهاية الحرب الباردة وعلى رأسها الانكشافات الأمنية للجزائر، اتجهت السياسة الأمنية الجزائرية للارتكاز على عناصر جديدة، وعلى رأسها قضايا تتعلق بمواجهة الإرهاب وتجارة المخدرات أمن الدولة [3]

أما في العقود الماضية فقد برزت سلسة من المشاكل والتهديدات جعلت من منطقة الساحل في محور اهتمامات السياسة الخارجية الجزائرية، لذلك تركزت المقاربة الأمنية الجزائرية على التهديدات الآتية من دول منطقة الساحل، وبهذا يمكن تقسيم تفاعلات الجزائر الحالية في بيئتها الإقليمية إلى ثلاث دوائر رئيسية:

- الدائرة المغاربية بتطوراتها العسكرية والسياسية المتتالية التي شهدتها مؤخرا.
- دائرة الساحل الإفريقي التي أصبحت من الدوائر التي تشكل أخطر التهديدات للأمن الجزائري.
- الدائرة المتوسطية ذات الأهمية الاستراتيجية الكبرى للجزائر، لا سيما من منظور اقتصادي.[4]

الموقع الجغرافي للجزائر على الضفاف الجنوبية للمتوسط، على هامش حركيته التاريخية والاستراتيجية المتواصلة، جعل من الدولة ترتبط بدول الجنوب منه وتتقاطع معها في أبعادها الإفريقية والعربية والإسلامية، وترتبط بدول شماله لعوامل تاريخية، ما ترك انعكاسات جيوسياسية على السياسة الأمنية الجزائرية، خصوصا مع تنامي تهديدات ومخاطر عبر وطنية تشترك فيها الجزائر مع غيرها من الدول المتوسطية، كالإرهاب والهجرة غير الشرعية والجريمة المنظمة.[5]

---

[1] ساعد طيايبة وعبد الرحمان بورنان، "تطور العقيدة الأمنية الجزائرية ومواجهة التهديدات الأمنية الجديدة في منطقة المغرب العربي"، مجلة الناقد للدراسات السياسية م6، ع1 (2022)، ص 532-554.

[2] أسامة سليخ، "الدوائر الجيو-أمنية للجزائر بين منطق الجغرافيا وتصادم المصالح"، مجلة الباحث الأكاديمي في العلوم القانونية والسياسية، المركز الجامعي بآفلو/ الأغواط م5، ع2 (2022)، ص12-23.

[3] صالح زياني، "تحولات العقيدة الأمنية الجزائرية في ظل تنامي تهديدات العولمة"، مجلة المفكر، جامعة باتنة، ع5 (2022)، ص 291.

[4] سليم جداي وحورية قصعة، "العمق الجيوبوليتيكي للجزائر في منطقة الساحل الإفريقي (دراسة في المرتكزات والتفاعلات والرهانات)"، المجلة الجزائرية للأمن والتنمية، م11، ع2 (جويلية 2022)، ص29-39.

[5] منصور لخضاري، السياسة الأمنية الجزائرية المحددات-الميادين-التحديات، (الدوحة: المركز العربي للأبحاث ودراسة السياسات، ط1، 2015)، ص31.

الفرع الثالث: المرتكز الإيديولوجي

ظل البعد الإيديولوجي من بين المرتكزات الرئيسية في السياسة الأمنية الجزائرية وذلك منذ الاستقلال، فقد مثلت الاشتراكية ومبادئها المناهضة للاستعمار والاستغلال مصدرا قيما بالنسبة للسياسة الأمنية؛ كما كان لخيار الحزب الواحد -اقتداء بتجارب عديد الدول- دوره في بلوة هذه السياسة.[1] إذ وبحسب هذه الأيديولوجيا تم النظر إلى حزب جبهة التحرير على أنه سبيل لتحقيق الوحدة الوطنية بعد الانشقاقات الأولى التي عرفتها الجزائر عقب حصولها على الاستقلال، وعليه أكدت المواثيق الوطنية على غرار دستور 1963 و1976 أن الاشتراكية كنظام وايديولوجيا هي المنهج الوحيد الكفيل بتحقيق الاستقلال التام والقضاء على الاستغلال. لقد سطرت الإيديولوجية الاشتراكية مبادئ ولأهداف السياسة الأمنية الجزائرية لفترة تقارب ثلاثة عقود منذ الاستقلال، ولعل من أبرز تلك الأهداف دعم حركات التحرر في العالم ونصرة القضية الفلسطينية، والعمل على المحافظة على مكانة الجزائر كقوة إقليمية، وكذلك الاستعانة بالمؤسسة العسكرية في مجهودات التنمية الوطنية.[2]

لكن قبل نهاية الثمانينات بات لزاما أن تتغير توجهات السياسة الأمنية الجزائرية، إثر أحداث أكتوبر 1988* والوضع الأمني الصعب الذي عرفته البلاد آنذاك، فقد حملت تلك الفترة مظاهر اللاإستقرار عقب توقيف المسار الانتخابي وظهور الجماعات الإرهابية مما عمق العنف السياسي، هذا إلى جانب التحولات الدولية في فترة ما بعد الحرب الباردة التي كان لها الأثر البالغ على العقيدة الأمنية الجزائرية؛ فانهيار المعسكر الشرقي وإيديولوجية وانتصار الإيديولوجية الليبرالية جعل من مسألة التكيف مع هذه التحولات والمستجدات أمرا بالغ الأهمية، في إطار عملية التحول المرن نحو الديمقراطية بمباشرة عديد الإصلاحات السياسية والاقتصادية بغرض حماية الأمن الوطني الجزائري.[3]

كما تجدر الإشارة إلى أن مؤسسات الدولة لها دور محوري في وضع وصياغة السياسات الأمنية، وفي الجزائر، تتصدر المؤسسة التنفيذية، بقيادة رئيس الجمهورية ومستشاريه في وزارات الدفاع ووزارة الخارجية والمديرية العامة للأمن الوطني، هذا إلى جانب مؤسسات أخرى غير حكومية مثل الأحزاب السياسية ومنظمات المجتمع المدني المختلفة.[4]

[1] فؤاد خوالدية، "السياسة الأمنية للجزائر أمام التهديدات الأمنية لمنطقتي المغرب العربي والساحل الإفريقي، المجلة الجزائرية للحقوق والعلوم السياسية، 26، ع2 (2021)، ص 849-872.

[2] ساعد طايبة وعبد الرحمان بورنان، مرجع سابق، ص 541-542.

* هي أحداث شهدتها الجزائر في أكتوبر 1988، من خلال مظاهرات واحتجاجات في مختلف الولايات الجزائرية للمطالبة بإصلاحات اجتماعية وسياسية واقتصادية، وانتهت بإقرار دستور جديد أنهى مرحلة الأحادية الحزبية وفتح باب التعددية.

[3] صالح زياني، مرجع سابق، ص291-292.

[4] فؤاد خوالدية، مرجع سابق، ص 856.

ساهمت مرتكزات عديدة في بلورة السياسة الأمنية الجزائرية على غرار التاريخ والجغرافيا، والأيديولوجيا؛ التي كان لها الأثر البالغ في رسم الخطوط العريضة للإستراتيجية الأمنية، كتحدٍ لقدرة الدولة على البقاء والاستمرار في ظل تزايد حدة التهديدات (التماثلية واللاتماثلية) التي تهدد كيانها مما يؤثر على أمنها واستقرارها سواء داخليا أو خارجيا.

المطلب الثاني: الهيئات والمؤسسات المسؤولة عن الأمن السيبراني في الجزائر

لضمان التنفيذ الفعلي والجدي لمختلف التدابير الهادفة لتحقيق الأمن السيبراني، أوكلت السلطات العليا للدولة هذه المهمة إلى هيئات مختصة ضمن أسلاك الأمن، نذكر منها ما يلي:

الفرع الأول: مؤسسة الدفاع الوطني وسياسات تحقيق الأمن السيبراني في الجزائر

لقد وضعت قيادة الدفاع الوطني الأمن السيبراني أحد أولوياتها سيما في ظل التطورات الجديدة للميدان الرقمي؛ أين أضحى تأمين المجال السيبراني ضرورة حتمية من أجل مواجهة كل أشكال المخاطر والتهديدات التي تستهدف الأنظمة والحساسة والحيوية للدولة[1].

ولتجسيد ذلك باشرت الدولة الجزائرية وفي مقدمتها مؤسسة الدفاع الوطني، إعداد برامج خاصة لمواجهة التحديات الإلكترونية وإنشاء أجهزة جديدة مجهزة ومتأهبة في هذا المجال، تمتلك الوسائل والتقنيات اللازمة لمجابهة هذه المخاطر، والتي يمكن حصرها كالآتي:

- توافر أحدث المعدات التكنولوجية في مجال الإعلام الآلي، الاتصالات اللاسلكية.
- التمتع بقاعدة بيانات واسعة محدثة باستمرار.
- القدرة على تصميم البرامج المعلوماتية وتطويرها.[2]

تنمية وتعزيز القدرات البشرية المكلفة بهذا المجال، وهذا ما أشار إليه رئيس الجمهورية الجزائرية عبد المجيد تبون خلال مراسم افتتاح الملتقى الوطني حول الأمن السيبراني في 07 جوان 2023؛ أين أكد أن كسب رهان الأمن السيبراني يعتمد في الأساس على تثمين العنصر البشري الذي تنبثق منه الكفاءات المتمرسة.[3]

ومن ضمن المصالح والوحدات التي أنشئت على مستوى مؤسسة الدفاع الوطني نجد:

[1] ن. بوكراع، "من أجل جزائر صامدة سيبرانيا"، مجلة الجيش الوطني الشعبي ع719 (جوان 2023)، ص 8-9.

[2] سمير بارة، "الأمن السيبراني في الجزائر السياسات والمؤسسات"، المجلة الجزائرية للأمن الإنساني 4 (جويلية 2017)، ص255-280.

[3] ن. بوكراع، مرجع سابق، ص 9.

1. مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة:

استحدثت بتاريخ 11 جوان 2015 على مستوى دائرة الاستعمال والتحضير لأركان الجيش الوطني الشعبي، وأوكلت لها مهمة، حماية المنظومات والمنشآت الحيوية للبلاد ضد كل أنواع التهديدات السيبرانية، ومن بين المحاور التي تناولتها الأرضية العملياتية لهذه المصلحة نذكر ما يلي:

توجيه، تنفيذ وتأطير الأعمال في هذا المجال لا يجب أن يتعدى الإطار الوظيفي أو التنظيمي.

تعزيز المنظومة القانونية لتفادي التجاوزات أثناء استخدام التكنولوجيا وضمان حماية منظومات الإعلام.

اعتماد التكوين التقني والعلمي لإنتاج الكفاءات القادرة على خلق نظام الدفاع السيبراني في كافة أنشطة المؤسسة العسكرية.

تكييف القدرات التقنية للحماية والكشف وردع الهجمات السيبرانية باستمرار، مع يقظة دائمة فيما يخص الوسائل المستعملة من طرف المهاجمين.

الاعتماد بطريقة مستمرة على البحث العلمي لتطوير وسائل الدفاع، والاستجابة للتطورات الحاصلة في مجال التكنولوجيا.

فتح مجال التعاون الدولي مع المؤسسات العسكرية الأجنبية، خاصة تلك التي لها رصيد في المجال لتبادل الخبرات والاستفادة من تجاربهم في هذا المجال.[1]

2. مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها للدرك الوطني (CPLCIC)

أنشئ هذا المركز سنة 2008، واعتبر بمثابة مركز توثيق ومقره متواجد ببئر مراد رايس، يسعى هذا المركز إلى تأمين منظومة المعلومات لخدمة الأمن العمومي، من خلال تحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة وتحديد هوية أصحابها، سواء كانوا أشخاصا فرادى أو عصابات.[2]

كما يتعبر هذا المركز نقطة اتصال وطني؛ إذ يعمل على توفير المساعدة التقنية للمحققين ويتم على مستواه حفظ الأدلة، بالإضافة إلى معاينة الجرائم ومراقبة البحث عن الجرائم وخصوصا على مستوى الإرهاب والقرصنة المعلوماتية.[3]

---

[1] جمال بوازدية، "الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية 'لتحديات والآفاق المستقبلية' " مجلة العلوم القانونية والسياسية 01 (أفريل 2019)، ص 1262-1293.

[2] سمير بارة، "الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر: الدور والتحديات"، تاريخ الاطلاع: 2024/12/30

https://2u.pw/8lanG

[3] سفيان حديدان، "الدخول أو البقاء عن طريق الغش في نظام المعالجة الآلية للمعطيات"، مجلة الأستاذ الباحث للدراسات القانونية والسياسيةم2، ع4 (ديسمبر 2017)، ص 672-687.

ومن بين مهام هذا المركز:

- ضمان المراقبة الدائمة والمستمرة على شبكة الانترنت.
- القيام بمراقبة الاتصالات الإلكترونية بما يسمح به القانون لفائدة وحدات الدرك الوطني والجهات القضائية.
- المشاركة في قمع الجرائم المعلوماتية، من خلال التعاون مع مختلف الأمن والهيئات الوطنية.
- مساعدة الوحدات الإقليمية للدرك الوطني في معاينة الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال والبحث عن الأدلة.[1]

هذا واستطاعت قيادة الدرك الوطني من خلال التكوين المستمر لأفرادها، والملتقيات الدولية والوطنية وكذا تبادل الخبرات مع دول أخرى أن توفر الهياكل المؤهلة وذات الكفاءة من مهندسي الإعلام الآلي، رجال قانون، بغية الفهم الصحيح للجريمة المعلوماتية والتصدي لها.[2]

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

مؤسسة عمومية تابعة للقيادة العامة للدرك الوطني؛ تقع تحت الوصاية المباشرة لوزير الدفاع الوطني، تم إنشاؤها بموجب المرسوم الرئاسي رقم 04-183 المؤرخ بتاريخ 26 جوان 2004، مكلفة بمهام متعددة نذكر منها:

- إجراء الخبرات والفحوص العلمية في إطار التحريات الأولية والتحقيقات القضائية.
- المشاركة في تحديد سياسة جنائية مثلى لمكافحة الإجرام.
- إجراء بحوث متعلقة بالإجرام الذي يعتمد على التكنولوجيات الدقيقة.
- العمل على ترقية أساليب التحري في ميادين الإجرام والأدلة الجنائية.
- المشاركة في جميع الملتقيات والندوات على الصعيدين الوطني والدولي لتطوير مستوى مستخدمي المعهد.
- العمل على ترقية البحوث التطبيقية وأساليب التحريات التي أثبتت فعاليتها في ميادين علمي الإجرام والأدلة الجنائية على المستويين الوطني والدولي.[3]

يحوي المعهد الوطني للأدلة الجنائية وعلم الإجرام على عديد الأقسام والمصالح المختصة من ضمنها: مصلحة البصمات، مصلحة الوثائق، مصلحة الإعلام الآلي. هذه الأخيرة، يتم على مستواها رصد ومراقبة عمليات الاختراق والقرصنة المعلوماتية إلى جانب تفكيك البرامج المعلوماتية.[4]

---

[1] سميحة بلقاسم وحميد بوشوشه، "الجريمة الإلكترونية بعد جديد للإجرام في الجزائر.. واقعها وآليات مجابهتها، مجلة العلوم الإنسانية لجامعة أم البواقي م10، ع1 (جوان 2023)، ص 532-561.

[2] سمير بارة، مرجع سابق، ص 435.

[3] جمال دندن، "الاستراتيجية الأمنية للدولة الجزائرية في مكافحة الجرائم السيبرانية"، مجلة صوت القانون م7، ع7 (نوفمبر 2020)، ص 980-994.

[4] سمير بارة، مرجع سابق، ص 271-272.

وبهذا يعد المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني مكسب يدعم قدرات الدرك الوطني في مكافحة الجريمة بجميع أشكالها وذلك بإدراج العلوم في العدالة الجزائية، كما أن التحكم في التقنيات الحديثة من شأنه أن يدعم قدرات المؤسسة لمكافحة الإجرام المتطور باستمرار والذي يعتمد على التكنولوجيات الحديثة.[1]

الفرع الثاني: الهيئات المكلفة بالأمن السيبراني التابعة لمديرية الأمن الوطني

كغيرها من الأجهزة الأمنية، أولت القيادة العليا للأمن الوطني أهمية قصوى لضرورة تحقيق الأمن السيبراني، من خلال تجنيد إمكانياتها المادية والبشرية في التصدي لكل أشكال الجرائم والتهديدات السيبرانية، عبر إنشاء الوحدات والمصالح التالية:

1. المصلحة المركزية لمكافحة الجرائم السيبرانية:

استجابة لمطلب الأمن المعلوماتي ومحاربة التهديدات الأمنية الناجمة عن الجرائم الإلكترونية، قامت مصالح الأمن بداية بإنشاء المصلحة المركزية للجريمة المعلوماتية (SCLC) سنة 2011؛ التي عملت على تكييف التشكيل الأمني للشرطة القضائية، ليتم بعدها إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بمديرية الشرطة القضائية سنة 2015، لتتحوّل فيما بعد إلى المصلحة المركزية لمكافحة الجرائم السيبرانية؛ والتي تعد مصلحة عملياتية مجهزة بالموارد البشري المتخصص والوسائل التقنية العالية المستوى، وتضم المصلحة بدورها فرقا مركزية؛ كالفرقة المركزية لمكافحة جرائم المساس بأنظمة المعالجة الآلية للبيانات، الفرقة المركزية لمكافحة الإجرام عبر الانترنت، والفرقة المركزية لليقظة ومعالجة التبليغات[2]، ويأتي عمل المصلحة في إطار مسعى الارتقاء بالعمل الأمني في مواجهة التحديات المرتبطة بكل أشكال الجرائم المعلوماتية والتهديدات السيبرانية، التي أفرزتها حروب الجيل الخامس.[3]

تضم الهيكلة الحالية للمصلحة المركزية لمكافحة الجرائم السيبرانية هياكل متخصصة ومكاتب للدعم، تشمل تحت لوائها نخبة من الكفاءات المتخصصة التي تعمل في مجال التصدي للجرائم السيبرانية، يتم انتقائهم من المصالح العملياتية أو من مدارس الشرطة ليتم بعدها تكوينهم على مستوى المصلحة على نحو ثلاث فئات:

- تكوين محققين مختصين في مجال محاربة الجرائم السيبرانية.
- تكوين متدخلين أوليين في مجال الجرائم السيبرانية.
- تكوين متخصص في مجال التفتيش الالكتروني.[4]

---

[1] "المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني"، موقع وزارة الدفاع الوطني، تاريخ الاطلاع: 2024/12/31 https://www.mdn.dz

[2] محافظ شرطة، مقابلة شخصية، المصلحة المركزية لمكافحة الجرائم السيبرانية، تاريخ: 2025/03/25.

[3] "تدشين المقر الجديد للمصلحة المركزية لمكافحة الجرائم السيبرانية"، موقع النهار، تاريخ المقال: 25 أكتوبر 2023، تاريخ الاطلاع: 2025/01/02 https://2u.pw/6Q5bM

[4] " SCLC... العصب الرقمي لصد الجرائم المعلوماتية "، مجلة الشرطة ع 158 (ماي 2024)، ص18-19.

ومن ضمن المحاور التي تشملها هذه المصلحة نذكر ما يلي:

- تعزيز التكوين في إطار التعاون الوطني والدولي، كالتعاون الشرطي مع عديد الدول في مجال مكافحة الجرائم السيبرانية، والمشاركة في الدورات التي تطرحها منظمة الإنتربولINTERPOL.[*1]
- التنسيق الفعال مع مختلف فرق مكافحة الجرائم السيبرانية المتواجدة عبر كافة ربوع الوطن، لضمان الإشراف العملياتي الدائم والمستمر لهذه الفرق المحلية.
- إطلاق حملات تحسيسية حول جرائم الانترنت، بالتنسيق مع مختلف المصالح الأمنية على غرار الدرك الوطني.

سجلت المصلحة المركزية لمكافحة الجرائم السيبرانية خلال الفترة الممتدة من 01 جانفي 2023 إلى غاية 31 ديسمبر 2023 معالجة 5136 قضية متصلة بتكنولوجيا الإعلام والاتصال تورط فيها 6146 شخص.

جدول 2: حصيلة مقارنة للقضايا المسجلة لدى المصلحة المركزية لمكافحة الجرائم السيبرانية لسنتي 2023/2022

القضايا	عدد القضايا المسجلة		عدد الأشخاص المتورطين	
	2022	2023	2022	2023
المساس بالأشخاص عبر شبكة الانترنت	1999	2046	1796	1905
المساس بأنظمة المعالجة الآلية للمعطيات	323	331	217	202
النصب والاحتيال عبر شبكة الانترنت	1130	801	1958	1318
المساس بالأطفال عبر شبكة الانترنت	113	56	124	78
نشر محتويات مخالفة للنظام عبر شبكة الانترنت	1066	1083	1332	1427
بيع السلع المحظورة عبر شبكة الانترنت	110	115	181	159
جرائم أخرى	395	286	538	496
المجموع	5136	4718	6146	5567

المصدر: مجلة الشرطة ع 158 (ماي 2024)

[*] المنظمة الدولية للشرطة الجنائية(INTERPOL)-The International Criminal Police Organization، تعرف باسم الإنتربول وهي منظمة دولية تأسست بهدف تسهيل التعاون الشرطي في جميع أنحاء العالم ومكافحة الجريمة بأنواعها، يقع مقرها فسي فرنسا، ولها سبعة مكاتب إقليمية في جميع أنحاء العالم، ومكتب مركزي وطني في 195 دولة.

[1] "مجلة الشرطة تسلط الضوء على موضوع الأمن السيبراني "، وكالة الأنباء الجزائرية، تاريخ المقال: 2024/06/05، تاريخ الاطلاع: 2025/01/02
Https://2u.pw/W5eb8

جدول 3: القضايا المعالجة على المستوى الوطني في مجال مكافحة الجرائم السيبرانية خلال الخمس سنوات الأخيرة

السنوات	عدد القضايا المسجلة
2020	5163
2021	4400
2022	4629
2023	5138
2024	5298

المصدر: المصلحة المركزية لمكافحة الجريمة السيبرانية

كما تولي المصلحة أهمية قصوى للتعاون الدولي في مجال عملها، ويتجسد ذلك بوضوح من خلال استضافتها للمكتب المركزي للإنتربول ومصلحة مركزية للتعاون الدولي، وتعد الشراكة مع منظمة الإنتربول تحديدا من أبرز وأكثر أوجه هذا التعاون فعالية[1].

وقد تمكنت المصلحة، من رصد وصد عديد الهجمات السيبرانية، وتلقت إشادات واسعة على المستوى الوطني والدولي على غرار منظمة الإنتربول التي أثنت في عديد المناسبات على جهود المديرية العامة للأمن الوطني في سبيل تعزيز التعاون الدولي وتقديم التجارب في مجال مكافحة الجرائم السيبرانية بمختلف أنواعها.[2]

2. المصالح والفرق المتخصصة التابعة للمصلحة المركزية لمكافحة الإجرام المتعلقة بتكنولوجيات الإعلام والاتصال:

تندرج هاته الفرق ضمن إطار مساعي المديرية العامة للأمن الوطني لتطوير ميكانيزمات التصدي للجرائم المعلوماتية، عبر تسخير تشكيل أمني مؤهل وكفء، يصبو إلى تحقيق التوازن بين ثنائية الردع والوقاية مع الحرص الدائم على التكيف مع كافة التحولات السريعة للفضاء السيبراني، فالتطور الهائل الذي تشهده تكنولوجيات الإعلام والاتصال التي أصبحت مرتعا لبعض الأطراف الإجرامية لارتكاب مختلف الجرائم والهجمات الالكترونية، وبيئة خصبة لنشر الأخبار المضللة والأفكار التحريضية التي من شأنها المساس بأمن الوطن والمواطن[3].

ومن مهام المصالح المختصة لمكافحة الجرائم المعلوماتية وفرقها العملياتية التابعة للشرطة القضائية ما يلي:

[1] محافظ شرطة، مرجع سابق.

[2] " SCLC... العصب الرقمي لصد الجرائم المعلوماتية "، مرجع سابق، ص 19-20-21.

[3] كريمة نعمان، "الشرطة الجزائرية تتصدى لصناع الكراهية عبر المنصات الرقمية"، مجلة الشرطة 149 (أكتوبر 2021)، ص 32.

- المشاركة في تأمين وحماية الأنظمة المعلوماتية والفضاء السيبراني الوطني.
- التعاون والمشاركة في التحقيقات ذات البعد الوطني والدولي في مجال مواجهة الجرائم الإلكترونية.
- المبادرة بعمليات التحسيس لفائدة مستعملي الإنترنت، بالتنسيق مع المصالح الأمنية الأخرى.
- اليقظة المعلوماتية والبحث عبر الشبكات المفتوحة عن كل محتوى غير شرعي عبر الانترنت، يشكل في حد ذاته جريمة في قانون العقوبات.[1]

وبهذا يمكن التوصل إلى أن جهود المصالح الأمنية تأتي مواصلة لجهود الدولة الجزائرية الرامية إلى ضرورة تكثيف التعاون والتنسيق بين كافة الأسلاك القضائية والمؤسسات الأمنية لمجابهة كل أشكال التهديدات السيبرانية، والتي وضعت ضمن قمة أولويات السلطات العليا للبلاد وفي قلب استراتيجياتها.

المطلب الثالث: الاستراتيجيات المتبعة لمواجهة التهديدات السيبرانية

استجابة لمختلف التهديدات السيبرانية، وضعت الجزائر استراتيجية شاملة للأمن السيبراني، تهدف إلى حماية البنية التحتية الرقمية للبلاد، وتعزيز الوعي بأهمية الأمني السيبراني لدى المؤسسات والمواطنين، وكذا بناء قدرات وطنية مؤهلة لمواجهة التحديات المتزايدة في هذا المجال.

قبل التطرق إلى حيثيات هذه الاستراتيجية، لابد بداية من توضيح التصنيف العالمي للجزائر حسب مؤشر الأمن السيبراني العالمي * Global Cybersecurity Index 2024حيث جاءت الجزائر في الفئة الثالثة (T3) كدولة في مرحلة التأسيس.[2]

وورد في التقرير المحاور الرئيسية التي يتم على أساسها التقييم:

- التدابير التنظيمية: الاستراتيجيات الوطنية للأمن السيبراني، والأطر التنظيمية.
- التدابير القانونية: قوانين حماية البيانات، والخصوصية، والتشريعات المتعلقة بالجرائم السيبرانية.
- التدابير التقنية: إنشاء فرق الاستجابة للحوادث السيبرانية، ومراقبة الشبكات.
- تنمية القدرات: التعليم والتدريب، وبناء الوعي.
- التعاون: الشراكات الدولية وتبادل المعلومات.

وبالعودة إلى واقع الاستراتيجية الجزائرية المعتمدة في مواجهة التهديدات السيبرانية فإنها تتوزع على النحو التالي:

[1] نفس المرجع، ص33.

* مؤشر الأمن السيبراني العالمي (GCI): هو تقرير يصدره الاتحاد الدولي للاتصالات لتقييم التزامات الدول حول العالم بتعزيز الأمن السيبراني، يهدف إلى زيادة الوعي بأهمية الأمن السيبراني وتشجيع الحكومات على اتخاذ إجراءات لحماية البنية التحتية الرقمية، البيانات الشخصية، والمؤسسات من التهديدات السيبرانية.

[2] "Global Cybersecurity Index 2024- 5th Edition", International Telecommunication Union (ITU Publications), 2024, p27

الفرع الأول: التدابير التنظيمية

اعتمدت الدولة الجزائرية في دفاعها السيبراني على استراتيجية متكاملة بين الوحدات العسكرية والأمنية، من خلال تكثيفها لأجهزة مراقبة الأنظمة، ومتابعة حالة تقدم نشاطات لتجسيد السياسة الشاملة للدفاع السيبراني، الرامية لضمان فعالية الحماية ضد التهديدات السيبرانية التي تستهدف أنظمة المعلومات ومنظومات الاتصال وكذا منظومة أسلحة الجيش.[1]

تبنت الاستراتيجية الدفاعية الجزائرية تنشيط الدفاع الوقائي السيبراني من خلال:

- محاولة الجمع بين الاستباقية والوقاية لضمان جاهزية أكبر في حالات خطر الاختراق أو التجسس أو التخريب.
- تثمين العنصر البشري الذي تنبثق منه الكفاءات عبر تدريب أشخاص مكلفين بحماية الأنظمة الأمنية الالكترونية.
- المشاركة في فعاليات المؤتمرات والملتقيات الدولية، بغية تبادل الخبرات والتقنيات الدولية.
- وضع أنظمة تأمين إضافية للولوج إلى بيانات وبرامج معينة، ووضع أنظمة رقابة للحماية من اختراق الأنظمة الالكترونية.[2]

ولتفادي الوقوع في تداخل الصلاحيات بين مختلف الأجهزة الفاعلة في مسائل الأمن والدفاع الوطني، حرص المشرع الجزائري على وضع ضوابط لاحترام الإطار الإداري المنظم لصلاحيات الهيئات المدنية، العسكرية والتقنية في إدارة الاستراتيجية الجزائرية للأمن السيبراني، وذلك من خلال إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والتي نصت على استحداثها، المادة 13 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وحسب نص المادة الثانية من المرسوم الرئاسي 19-127، تعتبر "الهيئة مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلالية المالية توضع تحت سلطة وزارة الدفاع"[3]، نص المشرع بأن الهيئة تتكون من مجلس توجيه ومديرية عالمة، حيث يرأس مجلس التوجيه وزير الدفاع الوطني أو ممثله وتتشكل من الوزارات التالية:

- وزارة الدفاع الوطني.
- وزارة العدل.
- الوزارة المكلفة بالداخلية.

---

[1] نجمة شريط، "الأمن السيبراني في العقيدة الدفاعية الجزائرية: الفرص والقيود"، المجلة الجزائرية للسياسة والأمن م2، ع2 (ديسمبر 2023)، ص 73-92.

[2] إكرام بركان وفهيم رميلي، "واقع وإشكالات الأمن السيبراني في الجزائر"، (ورقة بحثية مقدمة للمؤتمر العلمي الوطني، جامعة قسنطينة 3، كلية العلوم السياسية، 2024)، ص 13.

[3] سميحة بلقاسم وحميد بوشوشه، "الجريمة الالكترونية بعد جديد للإجرام في الجزائر.. واقعها وآليات مجابهتها"، مجلة العلوم الإنسانية لجامعة أم البواقي 01 (جوان 2023)، ص553.

- الوزارة المكلفة بالاتصالات السلكية واللاسلكية.[1]

هذا وتكلف الهيئة بالمهام التالية:

- تحديد الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- ضمان المراقبة الوقائية للاتصالات الالكترونية قصد الكشف عن الجرائم التي تمس بأمن الدولة كالأعمال الإرهابية والتخريبية.
- السهر على تطوير تبادل المعلومات والتعاون في مجال اختصاصاتها على المستوى الدولي.
- تطوير التعاون مع المؤسسات والهيئات الوطنية في مجال الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.
- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيا الإعلام والاتصال.[2]

من خلال هذه المهام، نجد أن المشرع قد منح للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مهام في أغلبها استشارية ورقابية وأخرى متعلقة باتخاذ قرارات إدارية، إلا أنها لا تمتلك صلاحيات قمعية، ما يجعل وظيفة الهيئة وقائية بالدرجة الأولى وليست عقابية.

الفرع الثاني: الجانب القانوني

اعتمد المشرع الجزائري على ثلاثة معايير لمواجهة الجريمة السيبرانية وهي:

- وسيلة الجريمة المتمثلة في استخدام تكنولوجيا الاتصال.
- موضوع الجريمة المتمثل في المساس بالأنظمة المعلوماتية.
- الجانب الشرعي والمتمثل في العقوبات التي حددها القانون.

ومن خلال القراءة التحليلية لمواد القوانين المستحدثة، يتضح أن المشرع الجزائري قد طرح تصورا يتوفر على العلاج الوقائي والردعي لمحاصرة الجرائم السيبرانية، بما يتطابق مع ما جاء في التشريعات الدولية وخاصة اتفاقية بودابست* المبرمة بتاريخ 2001/11/23، فعلى الرغم من عدم مصادقة المشرع الجزائري على هذه الاتفاقية بسبب أن البنية

[1] المادة 06 من المرسوم الرئاسي رقم 183/20، المؤرخ في 13 جويلية 2020، الجريدة الرسمية للجمهورية الجزائرية ع40 (18 جويلية 2020)، ص6.

[2] سهيلة بوزبرة، "دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال"، المجلة الدولية للبحوث القانونية والسياسية، م5، ع3 (2021)، ص 12- ص31.

* اتفاقية بودابست The Budapest Convention: أبرمت في عاصمة المجر بتاريخ 2001/11/23 تضمنت الجرائم السيبرانية، وتعتبر هذه الاتفاقية المرجعية القانونية لكل التشريعات الدولية الصادرة في هذا المجال.

التنظيمية والتشريعية الجزائرية في هذا المجال لا زالت في طور التشكيل[1] إلا أنه نهج نهجها والتزم بتشريعها خاصة فيما يتعلق بالجانب الموضوعي لمواجهة الجريمة السيبرانية.[2]

ومن بين النقاط التي شملتها المطابقة:

- استعمال المصطلحات المعمول بها في مجال الإعلام الآلي وتكنولوجيات الاتصال، لتسهيل عمل المختصين.
- المسؤولية المعنوية للجهات المكلفة بتسيير مجالات تكنولوجيا الإعلام تبقى قائمة، لأنهم في نظر القانون الضامن الوحيد على حسن وسلامة الأنظمة المعلوماتية.
- الحصول على المعطيات بطريقة غير شرعية من شأنه أن يحول من مسار المعلومة في جانبها المهني أو الشخصي، وهذه الخطوة من أخطر التهديدات السيبرانية، وقد تضمنتها المادة الرابعة من الاتفاقية والمادة 394 مكرر قانون العقوبات الجزائري.
- التعاون الدولي من أجل سلامة الإجراءات القانونية (الانابة القضائية، تسليم المجرمين).[3]

الفرع الثالث: تنمية القدرات البشرية والتقنية

اتجهت الدولة الجزائرية لدعم الجانب البشري في تخصص الأمن السيبراني، من خلال تنظيم دورات تدريبية على مستوى الجامعات الجزائرية والمعاهد ومراكز التكوين، لتوضيح مفاهيم وأبعاد الأمن السيبراني ومؤسساته وسبل الوقاية من التهديدات السيبرانية، كما استحدثت الجزائر وفق المرسوم الرئاسي رقم 24-181 المدرسة الوطنية العليا في الأمن السيبراني، التي تعمل بالتنسيق مع وزارة الدفاع الوطني، لضمان توحيد الجهود ومضاعفة الفعالية من أجل تحصين الأمن القومي الجزائري.[4]

وقد كلفت المدرسة وبالتعاون مع وكالة أمن الأنظمة المعلوماتية، بما يأتي:

- المساهمة في المجهود الوطني للبحث العلمي والتطوير التكنولوجي في مجال أمن الأنظمة المعلوماتية وتقديم حلول مبتكرة ذات تقنيات عالية.
- تطوير العلوم وتعزيز القدرات التقنية في مجال الأمن السيبراني.
- وضع بنيتها التحتية ووسائلها في خدمة تعزيز أمن الأنظمة المعلوماتية الوطنية.[5]

---

[1]

[2] سليمان قطاف وعبد الحليم بوقرين، "الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري"، المجلة الأكاديمية للبحوث القانونية والسياسية م6، ع1 (2022)، ص334- 358.

[3] جمال بوازدية، مرجع سابق، ص1279.

[4] "صدور المرسوم الرئاسي المتعلق بإنشاء المدرسة العليا في الأمن السيبراني"، وكالة الأنباء الجزائرية، تاريخ المقال:2024/06/09، تاريخ الاطلاع: 2025/01/07.
https://2u.pw/yAJcU

[5] المادة 5 من المرسوم الرئاسي رقم 24-181 المؤرخ في 5 جوان 2024، الجريدة الرسمية للجمهورية الجزائرية، ع39 (8 جوان 2024)، ص 6.

وبهذا تعتبر المدرسة مكسبا هاما لمواكبة التطورات التكنولوجية العالمية وتكوين كفاءات عالية في أمن الأنظمة المعلوماتية.

وبحكم انفراد التهديدات السيبرانية بمميزات خاصة كانعدام الحواجز الجغرافية، وصعوبة الكشف عن هوية المستخدم، أصبح لزاما التسلح بأحدث الوسائل التقنية للتمكن من مجابهتها، ويمكن حصر أهم عناصر الاستراتيجية الجزائرية لتحقيق الأمن السيبراني تقنيا في العناصر التالية:

- السعي إلى تسخير التدابير اللازمة التي من شأنها توفير أكبر درجة حماية لبنيتها المعلوماتية التحتية، وتحقيق أمنها السيبراني وفقا للتحولات الرقمية الجارية في إطار عصرنة قطاعات الدولة.
- توفير أحدث المعدات التكنولوجية؛ إذ تزود مخابر "دائرة الإشارة وأنظمة المعلومات والحرب الالكترونية"* الضباط العاملين بأحدث الوسائل والأجهزة التي تستجيب للمعايير الدولية، إلى جانب اهتمام مؤسسة الجيش بمسألة الذكاء الاصطناعي وفعاليته في مجال الدفاع السيبراني، وكذا التقنيات المعتمدة في حروب الجيل الخامس G5** مثل الذبابات الصغيرة التي تسير الصواريخ، والروبوتات التي تقتحم ميادين المعارك وغيرها. [1]
- تفعيل نشاطات الاستعلام حول الثغرات الأمنية والبرامج الضارة والخبيثة.
- الكشف عن التقنيات والأساليب المستخدمة من قبل منفذي الهجمات الالكترونية ودوافعهم، لاتخاذ الحلول اللازمة لحماية أنظمة الاستخدام على مستوى الجيش الوطني الشعبي وكذا المؤسسات الحيوية في البلاد.
- تكوين مورد بشري تقني ذي كفاءة عالية في مجال الدفاع السيبراني.
- التمتع بقاعدة بيانات واسعة محدثة باستمرار.
- القدرة على تصميم البرامج المعلوماتية وتطويرها.
- الوقاية والتحسيس من الأخطار السيبرانية المحتملة ذات الصلة من خلال استخدام تكنولوجيا الإعلام والاتصال.[2]

بالتالي تركز الجزائر في تطبيق استراتيجيات مواجهة التهديدات السيبرانية، على أن ذلك من مهام ومسؤوليات جميع فئات وأجهزة الدولة الجزائرية، وذلك من خلال استراتيجية وطنية شاملة للأمن السيبراني، تبدأ من وعي المواطن بالمخاطر

* هي هيئة تابعة للمدرسة العليا للإشارة يتم على مستواها تكوين الضباط العاملين في تخصص "الإشارة"، "الحرب الالكترونية"، و"منظومات الإعلام والقيادة".

** مع ظهور الانترنت في العصر الرقمي واختراع طرق لضرب الخصوم بهجمات سيبرانية، دخل العالم في مرحلة حروب الجيل الخامس وهي مزيج من النشاط غير الحركي، مثل الهندسة الاجتماعية، وحملات التضليل والاستدراج، واستخدام التقنيات المتطورة مثل تكنولوجيا المعلومات والذكاء الاصطناعي لشن الهجمات الالكترونية والسيبرانية، كما تدخل المعلومات والدعاية والأخبار الزائفة في هذا الشكل من الحروب.

[1] ليلى بن برغوث، "الأمن السيبراني وحماية خصوصية البيانات الرقمية في الجزائر في عصر التحول الرقمي والذكاء الاصطناعي التهديدات، التقنيات، التحديات وآليات التصدي"، المجلة الدولية للاتصال الاجتماعي م10، ع1 (2023)، ص 443-457.

[2] ب. عيمور، "التكوين والتعاون في الميدان السيبراني "، مجلة الجيش 715 (فيفري 2023)، ص50.

الموجودة على الفضاء السيبراني، ثم المختصين والتقنيين في المجال وصولا إلى المسؤولين على كافة المؤسسات الفاعلة في الدولة.

الفرع الرابع: التعاون الدولي

تدرك الجزائر أهمية التعاون الدولي في مواجهة التهديدات السيبرانية، وتسعى إلى تعزيز هذا التعاون مع مختلف الدول والمنظمات الدولية، من خلال تبادل المعلومات والخبرات للاستفادة من أفضل الممارسات العالمية وتطوير قدراتها الخاصة، وكذا المشاركة في المؤتمرات والندوات الدولية المتعلقة بالأمن السيبراني للاطلاع على أحدث التطورات في هذا المجال.

إلى جانب التزامها بقواعد معاقبة وتسليم المجرمين، فعند تحديد هوية مرتكب جريمة سيبرانية متواجد في دولة أجنبية، يتم التنسيق مباشرة مع سلطات تلك الدولة عبر القنوات الرسمية. وتعتمد عملية معاقبة المجرم على مبدأ التجريم المتبادل للفعل في كلا البلدين، مع تبادل المعلومات حول الإجراءات المتخذة.

أما في الحالات التي تهدد أمن الدولة ووحدتها الترابية، أو عندما يتعلق الأمر بالإرهاب السيبراني وأنظمة معالجة البيانات الحساسة، يصبح طلب التسليم أداة ضرورية لضمان تحقيق العدالة. ومع ذلك، ونظرا لتباين مواقف الدول بشأن تسليم المجرمين، فإن الأجهزة الأمنية الجزائرية تؤكد على مبدأ المعاملة بالمثل في تعاملها مع طلبات التسليم الواردة من الدول التي لا تلتزم بتسليم المجرمين المطلوبين من طرف الدولة الجزائرية[1].

كذلك يطرح إشكال في مسألة التعاون الدولي، باعتبار أنها على قدر ما توفر من مزايا للدولة من أجل الاحتكاك بالدول والمنظمات الرائدة في مجال الأمن السيبراني، بقدر ما قد يحمله من تبعات سلبية تؤثر على السيادة الوطنية والأمن القومي، فقد يكون مسار التعاون مغلفا بأجندات خطيرة على الداخل الوطني، خاصة وأن التعامل مع التكنولوجيا والرقمنة أضحى يتطلب الحذر واليقظة المستمرة من الدول المتقدمة في هذا المجال.

[1] محافظ شرطة، مرجع سابق.

المبحث الثاني: تقييم استجابة الجزائر للتهديدات السيبرانية

تدرك الجزائر أهمية الأمن السيبراني وتسعى لتعزيز قدرتها في هذا المجال؛ من خلال اتخاذ خطوات جادة لمواجهة التهديدات السيبرانية، عبر وضع تشريعات وقوانين، وكذا بناء شراكات إقليمية ودولية. لكن لاتزال هناك تحديات كبيرة تواجه السياسة الأمنية الجزائرية في هذا المجال.

في هذا الإطار يهدف هذا المبحث إلى تقييم استجابة الجزائر للتهديدات السيبرانية، من خلال تحليل الجهود المبذولة في مجال التشريعات والقوانين، والتعاون الإقليمي والدولي، وصولا إلى التحديات التي تواجه السياسة الأمنية الجزائرية في المجال السيبراني.

المطلب الأول: جهود الجزائر في مجال التشريعات والقوانين السيبرانية

لقد أقر المشرع الجزائري جملة من القوانين والتنظيمات، التي تؤطر النشاطات سواء المتعلقة بتكنولوجيا المعلومات أو بالأمن السيبراني:

القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات: إذ قام المشرع الجزائري بتعديل قانون العقوبات الذي تمم الفصل الثالث من الأمر رقم 156/66 المتضمن قانون العقوبات الجزائري بقسم سابع مكرر عنوانه "المساس بأنظمة المعالجة الآلية للمعطيات" ويشمل المواد من 194مكرر إلى 394 مكرر 7.[1]

وقد نصت أحكام المادة 394 مكرر 03 على مضاعفة العقوبات المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد.[2]

هذا التعديل القانوني يمثل خطة هامة نحو تعزيز الأمن السيبراني في الجزائر، من خلال تجريم أفعال المساس بأنظمة المعالجة الآلية للمعطيات وتشديد العقوبات في الحالات التي تستهدف مصالح الدولة الحيوية.

القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها: تم إصداره في 05 أوت 2009 والذي كان يهدف بالدرجة الأولى إلى الوقاية من الجرائم المعلوماتية والسيبرانية التي تقع في الفضاء الالكتروني.[3]

جاء القانون مقسما إلى ستة فصول تضمنت ما يلي:

[1] إيمان بغدادي، "أثر تعديل قانون العقوبات الجزائري في التصدي للجريمة الإلكترونية"، مجلة آفاق للبحوث والدارسات سداسية، دولية محكمة- المركز الجامعي إيليزي، ع4 (جوان 2019)، ص 184-192.

[2] المادة 394 مكرر 03 من القسم السابع مكرر "المساس بأنظمة المعالجة الآلية للمعطيات"، قانون العقوبات ص113.

[3] حنان مباركة كركوري، "التأصيل القانوني للجرائم السيبرانية المرتكبة عبر الوسائط الرقمية"، المجلة الافريقية للدراسات القانونية والسياسية م7، ع1 (جوان 2023)، ص 119-142.

- أشار الفصل الأول إلى الأهداف المتوخاة من القانون، وحدد مفهوم المصطلحات التقنية الواردة فيه، بحيث عرف الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بأنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية".[1]
- وتضمن كذلك مفهوم المنظومة المعلوماتية، المعطيات المعلوماتية، مقدمو الخدمات، المعطيات المتعلقة بحركة سير المنظومة المعلوماتية، والاتصالات الالكترونية. كما نصت المادة 3 من القانون على مجال تطبيق أحكامه.

أما الفصل الثاني فقد نص على الحالات التي يسمح فيها باللجوء إلى المراقبة الالكترونية وحددها كالآتي:

الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

- في حالة توفر معلومات عن احتمال وقوع اعتداء على منظومة معلوماتية، على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
- لمقتضيات التحريات والتحقيقات القضائية.
- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.[2]

وبخصوص الفصل الثالث فقد تضمن القواعد الإجرائية الخاصة بالتفتيش والحجز في مجال الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وفقا للمعايير العالمية المعمول بها.

أما الفصل الرابع فقد اشتمل على الالتزامات المتعلقة بمقدمي الخدمات في إطار تقديم المساعدة للسلطات القضائية في مواجهة الجرائم وكشف مرتكبيها.[3]

- وفيما يخص الفصل الخامس فقد نص على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، مع تبيان مهامها.
- آخر فصل وهو السادس أشار إلى التعاون والمساعدة القضائية الدولية فيما يتعلق بالاختصاص القضائي مع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل.

[1] المادة 2 من القانون رقم 09-04 المؤرخ في 05 أوت 2009، الجريدة الرسمية للجمهورية الجزائرية، ع47 (16 أوت 2009)، ص 5.

[2] المادة 4 من القانون رقم 09-04، ص 6.

[3] المادة 10 من القانون رقم 09-04، ص7.

- وتضمن أيضا القيود الواردة على طلبات المساعدة القضائية الدولية في حال مساسها بالسيادة الوطنية أو النظام العام، إلى جانب أنه يمكن أن تكون الاستجابة مقيدة بشرط المحافظة على سرية المعلومات أو بشرط عدم استعمالها في غير ما ينص عليه الطلب.[1]

يلاحظ أن المشرع الجزائري خطى خطوة إيجابية بسن هذا القانون وتنظيمه، إلا أنه غير كاف نتيجة إهمال الجوانب التقنية الكفيلة بتصنيف الجرائم السيبرانية وفي تحديد العقوبة المناسبة في حق مرتكبيها، ما يجعل تجسيد بنوده على أرض الواقع محدودا.

قانون رقم 15-04 المؤرخ في سنة 01 فيفري 2015: يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين[2]؛ وقد نص هذا القانون على تجريم الأفعال المرتبطة بالبيانات والمعلومات ذات الطابع الشخصي مثل:

- جريمة إفشاء البيانات الشخصية أو إساءة استعمالها.
- جريمة الإخلال بسرية المعلومات.
- جريمة جمع البيانات الشخصية دون موافقة المعني.[3]

بشكل عام، يعتبر هذا القانون خطوة إيجابية نحو تنظيم الفضاء الرقمي وحماية حقوق الأفراد، ولكنه قد يحتاج إلى مزيد من التفصيل في بعض جوانبه لضمان فعالية تطبيقه.

المرسوم التنفيذي رقم 16-134 المؤرخ في 25 أفريل 2016: والذي يحدد تنظيم المصالح التقنية والإدارية للسلطة الوطنية للتصديق الإلكتروني وسيرها ومهامها[4]، ويعد إجراء أساسيا لتفعيل نظام التصديق الإلكتروني في الجزائر، ومنحه الإطار القانوني والتنظيمي اللازم.

القانون رقم 18-04 المؤرخ في 10 ماي 2018: المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، الذي وضع مجموعة آليات للتصدي للجرائم الالكترونية واستحدث سلطة ضبط وظيفتها إرساء الأحكام القانونية والتنظيمية المتعلقة بالبريد والاتصالات الالكترونية والأمن السيبراني[5].

وبهذا يعتبر هذا القانون، إطارا شاملا ينظم قطاع البريد والاتصالات الالكترونية في الجزائر. بالإضافة إلى ذلك، يتضمن جوانب تتعلق بمكافحة الجرائم الإلكترونية وإنشاء هيئة تنظيمية لضمان تطبيق القوانين وتعزيز الأمن السيبراني.

[1] المادة 18 من القانون رقم 09-04، ص8.

[2] ليلى بن عيسى وجمال زمورة، "أهمية حوكمة الأمن السيبراني لضمان تحول رقمي آمن للخدمات العمومية في الجزائر"، مجلة البحوث الاقتصادية المتقدمة م7، ع2 (2022)، ص414- ص429.

[3] سعاد واجعوط، "مكافحة الجريمة السيبرانية على المستوى الوطني"، مجلة دفاتر البحوث العلمية م12، ع1 (2024)، ص 416-431.

[4] المرسوم التنفيذي رقم 16-134 المؤرخ في 17 رجب 1437 الموافق لـ 25 أفريل 2016، الجريدة الرسمية للجمهورية الجزائرية 26 (28أفريل 2016)، ص6.

[5] رضا مهدي، "الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري"، مجلة إيليزا للبحوث والدراسات م6، ع2 (2021)، ص 111-125.

المرسوم الرئاسي رقم 19 -172 المؤرخ في 06 جوان 2019: جاء تطبيقا للمادة 13 من القانون رقم 09-04، ويهدف هذا المرسوم إلى تحديد تشكيلة "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها" وتنظيمها وكيفيات سيرها.[1]

يأتي هذا المرسوم في إطار سعي الدولة الجزائرية إلى تنظيم وتنسيق الجهود بين مختلف الأطراف (وزارة الدفاع الوطني، الوزارة المكلفة بالداخلية، وزارة العدل، الوزارة المكلفة بالاتصالات السلكية واللاسلكية)، لمواجهة التحديات المتزايدة في الفضاء السيبراني. ومع ذلك فإن فعالية هذه الهيئة ستعتمد بشكل كبير على الصلاحيات الممنوحة لها، وكذا مدى التنسيق بين مختلف الجهات المعنية.

المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي 2020: يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية الموضوعة لدى وزارة الدفاع الوطني، والتي تعتبر أداة للدولة في مجال أمن الأنظمة المعلوماتية، وتشكل الإطار التنظيمي لإعداد الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية وتنسيق تنفيذها.[2]

حيث تشمل المنظومة الوطنية لأمن الأنظمة المعلوماتية:

- مجلس وطني لأمن المنظومة المعلوماتية: والذي يكلف بإعداد الاستراتيجية الوطنية والموافقة عليها وتوجيهها.
- وكالة لأمن الأنظمة المعلوماتية: تكلف بتنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية.[3]

تأسيسا على ما سبق يمكن القول إنه وبالرغم من تأخر الجزائر في الانضمام إلى الدول الرائدة في مجال السياسات السيبرانية، إلا أنها قد اتخذت خطوات جادة في السنوات الأخيرة، وقد تجلى ذلك في إصدار العديد من القوانين والمراسيم التي تواكب التطور المتسارع لتكنولوجيا المعلومات والاتصالات. وعلاوة على ذلك، تبنت الجزائر رؤية جديدة للأمن السيبراني تتجاوز المقاربة الدفاعية التقليدية، وتسعى إلى التفتح على الجوانب الاقتصادية والاجتماعية في سياساتها السيبرانية.

[1] المادة 1 من المرسوم الرئاسي رقم 19-172، المؤرخ في 6 جوان 2019، الجريدة الرسمية للجمهورية الجزائرية ع 37 (9 جوان 2019)، ص5.

[2] المادة 2 من المرسوم الرئاسي رقم 20-05، المؤرخ في 20 جانفي 2020، الجريدة الرسمية للجمهورية الجزائرية ع4 (26 جانفي 2020)، ص6.

[3] إ جنادي، "التحول الرقمي رهان سيادي"، مجلة الجيش الوطني الشعبي 726 (جانفي 2024)، ص35.

المطلب الثاني: الشراكات والتعاون الإقليمي والدولي في مجال الأمن السيبراني

بحكم طبيعة التهديدات السيبرانية العابرة للحدود، فإن المقاربة القانونية وحدها غير كافية لمواجهتها، لذلك تعمل الجزائر على تعزيز التعاون الدولي في مجالات تبادل المعلومات والأدلة وتسليم المجرمين بين الدول، ويكمن توضيح ذلك من خلال:

الفرع الأول: التعاون الإقليمي في مجال الأمن السيبراني

1. آليات العمل العربي المشترك في مجال الأمن السيبراني

إن تباين الأوضاع القانونية والتنظيمية للدول العربية في مجال الأمن السيبراني، لم يمنع من قيام تعاون عربي مشترك تجسد في إنشاء أطر تنظيمية ومؤسساتية متنوعة، تهدف إلى دعم وتنفيذ رؤية عربية موحدة للأمن السيبراني.

جدول 4: تصنيف الدول العربية حسب تقرير مؤشر الأمن السيبراني العالمي لعام 2024

الفئة الأولى 'T1' (دول قائدة-نموذج) تحصلت على تقديرات إجمالية تتراوح بين 95-100 درجة	الفئة الأولى 'T2' (دول في مرحلة التقدم) تحصلت على تقديرات إجمالية تتراوح بين 85-95 درجة	الفئة الأولى 'T3' (دول في مرحلة التأسيس) تحصلت على تقديرات إجمالية تتراوح بين 55-95 درجة	الفئة الأولى 'T4' (دول في مرحلة التطور) تحصلت على تقديرات إجمالية تتراوح بين 20-55 درجة	الفئة الأولى 'T5' (دول في مرحلة البناء) تحصلت على تقديرات إجمالية تتراوح بين 0-20 درجة
الإمارات		الجزائر	فلسطين	اليمن
السعودية		الكويت	لبنان	
قطر		تونس	العراق	
مصر		ليبيا	جيبوتي	
البحرين			موريتانيا	
عمان			السودان	
الأردن			سوريا	
المغرب			الصومال	
			جزر القمر	

المصدر: من إعداد الباحثة بالاعتماد على المعطيات المقدمة في: Global Cybersecurity Index 2024

يظهر الجدول أن هنالك تفاوت كبير في مستوى الأمن السيبراني بين الدول العربية، حيث تتراوح الدول بين "قائدة نموذج" في الفئة 'T1' وصولا إلى "دول في مرحلة البناء" في الفئة 'T5'، ومن الملاحظ أن بعض الدول العربية وفق ما جاء في التقرير قد حققت تقدما ملحوظا في مجال الأمن السيبراني على غرار قطر والسعودية والإمارات، في حين لا تزال العديد من الدول العربية في المراحل الأولى من التطوير.

وبالرجوع إلى واقع التعاون العربي في مجال الأمن السيبراني، فإن أول المبادرات كانت المصادقة على "الاتفاقية العربية لمكافحة جرائم تقنية المعلومات" التي تم إقرارها في 21 ديسمبر 2010، وتم إيداع وثائق التصديق عليها من قبل سبع دول عربية، [1] بما في ذلك الجزائر التي وقعت عليها في إطار الاجتماع المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة. وقد دخلت هذه الاتفاقية حيز التنفيذ في 06 فيفري 2014.[2]

سعت هذه الاتفاقية إلى بعث سبل التعاون القضائي والقانوني بين الدول المصادقة عليها في مجالات كتنازع الاختصاص، تسليم المجرمين، المساعدة القضائية المتبادلة.[3] هذا وقد أضحت الاتفاقية مرجعا هاما للدول العربية في سعيها لمكافحة الجرائم الالكترونية؛ حيث استندت إليها العديد من الدول في صياغة قوانينها الخاصة لمواكبة التطور التقني في مجال تكنولوجيا المعلومات.[4]

فيما بعد تركزت المبادرات العربية في شكل قوانين إرشادية في مجال الأمن السيبراني مثل القانون الإرشادي العربي في جرائم تقنيات المعلومات والقانون الإرشادي للإثبات بالتقنيات الحديثة والقانون الإرشادي للمعاملات التجارية الإلكترونية. [5]

هذا وقد برز دور المركز العربي للبحوث القانونية والقضائية من خلال إعداد مسودة الاتفاقية العربية لحماية الفضاء السيبراني في عام 2018، والتي حظيت بمصادقة مجلس وزراء العدل العرب بجامعة الدول العربية، وشملت المحاور التالية:

- بناء الثقة في الفضاء السيبراني.
- تعزيز القدرات التقنية لمواكبة التطور المتسارع لثورة المعلومات.
- حماية أمن المجتمعات العربية في العصر الرقمي.

[1] كمال الرزقي وآخرون، الرؤية العربية للأمن السيبراني، (تونس: المنظمة العربية لتكنولوجيا الاتصال والمعلومات، 2021)، ص15.

[2] الأمانة العامة لجامعة الدول العربية، إدارة الشؤون القانونية، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، 2010، ص17.

[3] وردة شرف الدين، "التعاون القضائي والقانوني لمكافحة جريمة غسل الأموال والمرتكبة بواسطة تقنية المعلومات" مجلة الباحث للدراسات الأكاديمية م8، ع2 (2021)، ص 638- 658.

[4] محمد أحمد لبيب أحمد وآخرون، "دور الاتفاقيات الدولية والإقليمية في مجال الأمن السيبراني وموقف الدولة المصرية منها"، الحوكمة والوقاية من الفساد ومكافحته 1 (سبتمبر 2024)، ص154

[5] كمال الرزقي وآخرون، مرجع سابق، ص16.

وفي هذا السياق سارعت الجزائر إلى توقيع العديد من الاتفاقيات الثنائية والمتعددة الأطراف مع الدول العربية، ودعمت كل المبادرات المطروحة لمواجهة الجرائم الالكترونية، ومن بين إسهاماتها الهامة مشاركتها بفريق من خبراء القانون في العديد من الدورات لأشغال مركز البحوث التابع للجامعة العربية لمناقشة الاتفاقيات والقوانين المطروحة للتكيف مع التطورات المتسارعة.

كما وسعت الدولة من دائرة تعاونها لتشمل تبادل الزيارات الميدانية والدورات التكوينية بغية تبادل الخبرات في المجال التشريعي والتقني، والتعرف على الآليات التقنية المستخدمة في مجال مكافحة التهديدات السيبرانية، إلى جانب تطوير القدرات البشرية العاملة في هذا المجال.[1]

2. واقع الجهود الإقليمية لضبط الأمن السيبراني الأورو متوسطي:

يشكل الأمن السيبراني تحديا ملحا للدول الأورو متوسطية في بعدها العام والجزائر بصفة خاصة، حيث يتأثر أمنها بشكل مباشر بموقعها الجغرافي الذي أفرز تداعيات أمنية أبرزها:

- تداعيات الانكشاف الأمني للبنى الإستراتيجية للدولة بما في ذلك نظم الاتصالات.
- تداعيات إضعاف البنى الاقتصادية لهذه الدول.
- تداعيات تفكيك السيادة الوطنية، كمحصلة نهائية لتراكم التهديدات الأمنية، خاصة تلك المتعلقة بنشر المعلومات المضللة ومدى تأثيراتها على التماسك الوطني والاجتماعي للدول.[2]

استجابة للتداعيات المطروحة، وتجسيدا لمبدأ الشراكة الأور ومتوسطية* الذي وقعت عليه الجزائر المتضمن التعاون في المجال الأمني والقضائي لمحاربة مختلف الجرائم، توجهت الجزائر إلى تجسيد "التعاون لمواجهة الجرائم السيبرانية في الضفة الجنوبية"، من خلال عقد لقاءات تجمع المؤسسات الفاعلة والخبراء الأجانب، وذلك للاستفادة من الخبرة الأوروبية في هذا الشأن.[3]

[1] جمال بوازدية، مرجع سابق، ص1285-1286.

[2] كريم رقولي ولخضر نويوة، "الأمن السيبراني المتوسطي بين الواقع والرهانات الأمنية"، مجلة طبنة المركز الجامعي بريكة، م2، ع2 (2019)، ص70-ص84.

* هي شراكة بين الاتحاد الأوروبي والبلدان المطلة على البحر الأبيض المتوسط في شمال إفريقيا وغرب آسيا، بدأت عام 1995 من خلا مؤتمر برشلونة الأورو متوسطي، وتهدف إلى تعزيز التعاون والاستقرار في المنطقة.

[3] جمال بوازدية، مرجع سابق، ص1286.

وفي سياق آخر، تم إقرار التعاون الأمني بين وكالة الشرطة الأوروبية "أوروبول" *Europol والجزائر لبعث سبل التعاون في مجال تبادل المعلومات والبيانات الشخصية للأفراد كدعامة فعالة في مجال التحقيقات والملاحقات التي تقوم بها السلطات القضائية الوطنية، خاصة فيما يتعلق بالإجرام الإلكتروني.[1]

3. الدور الإقليمي لآلية الأفريبول في مواجهة الجريمة السيبرانية

آلية الإتحاد الإفريقي للتعاون الشرطي 'The African Union Mechanism for Police Cooperation' أو ما تعرف اختصارا بـ: "الأفريبول" هي هيئة تقنية لدى الاتحاد الافريقي، مهمتها تعزيز التعاون بين أجهزة الشرطة في الدول الأعضاء في الاتحاد الافريقي في مجال الوقاية ومكافحة الجريمة المنظمة العابرة للحدود الوطنية والإرهاب والجرائم الإلكترونية،[2] وتتخذ هذه الآلية من الجزائر العاصمة مقرا رسميا لها.

وفي إطار سعيها لمواجهة التحديات السيبرانية، بادرت إلى تنظيم عدة نشاطات تكوينية في هذا الخصوص، نذكر منها:

تنظيم ورشة حول: "تعزيز القدرات في مجال الجريمة المنظمة العابرة للحدود الوطنية، الجريمة السيبرانية والإرهاب" بتاريخ 24و25 أكتوبر 2017، بمقر المراقبة التابع للمديرية العامة للأمن الوطني بالجزائر.

عقد اجتماع حول "تعزيز التعاون في مجال مكافحة الجريمة الإلكترونية" بتاريخ 13و14 ديسمبر 2017 بمقر أفريبول، والذي خلص إلى توصيات بخصوص تبادل الخبرات والممارسات وإنشاء فريق من الخبراء.[3]

هذا وقد أبرمت الأفريبول اتفاقية شراكة استراتيجية مع منظمة الشرطة الجنائية الدولية (الانتربول)، بهدف دعم التعاون الإقليمي والدولي في مجال إنفاذ القانون وتبادل المعلومات، والاستفادة من الخبرات التي يتيحها الانتربول، بما في ذلك شبكة الاتصالات العالمية وقواعد البيانات الأمنية.[4]

وفي إطار الجهود العالمية لمكافحة الجرائم الإلكترونية، وقعت أفريبول وشركة كاسبرسكيKaspersky * اتفاقية تعاون لمدة خمس سنوات، تهدف إلى تعزيز التعاون بينهما في مجال منع الجرائم السيبرانية ومكافحتها، وذلك من خلال تبادل

*أوروبول 'The European Union Agency for law enforcement cooperation' هي وكالة إنفاذ القانون التابعة للاتحاد الأوروبي، تأسست عام 1998، ومقرها لاهاي بهولندا، وتعمل كمركز لتنسيق الاستخبارات الجنائية ودعم الدول الأعضاء في الاتحاد الأوروبي في جهودها لمكافحة مختلف أشكال الجريمة المنظمة.

[1] آسيا لعمراني، "التعاون الدولي في مواجهة الجرائم السيبرانية: الجزائر نموذجا"، المجلة الجزائرية للعلوم السياسية والعلاقات الدولية م5، ع2 (ديسمبر 2010)، ص 54-94.

[2] Mécanisme de l'Union Africaine pour la coopération policière (AFRIPOL), AFRIPOL, 07/09/2023.
https://2u.ppw/BDu42R

[3] خديجة خالدي، "آلية الاتحاد الافريقي للتعاون الشرطي "أفريبول"، مجلة العلوم الاجتماعية والإنسانية م 11، ع 1 (2018)، ص65-79.

[4] عبد العزيز لزعر ورشيد زياني، "آلية الاتحاد الافريقي للتعاون الشرطي (الأفريبول) ودورها في مكافحة الجريمة الإلكترونية، مجلة متون م14، ع3 (2021)، ص251-270.

* Kaspersky هي شركة عالمية للأمن الإلكتروني والخصوصية الرقمية تأسست عام 1997، مقرها الرئيسي في العاصمة الروسية موسكو، ولها مكاتب إقليمية في الصين، اليابان، ألمانيا....

معلومات التهديدات حول أحدث أنشطة المجرمين السيبرانيين، وتسعى هذه الشراكة إلى دعم جهود أفريبول في حماية الدول الإفريقية من التهديدات السيبرانية المتزايدة.[1]

الفرع الثاني: التعاون الدولي في مجال الأمن السيبراني

أبرمت المنظمات والهيئات الدولية العديد من الاتفاقيات، كمحاولة لترسيخ التعاون الدولي لمواجهة الهجمات لضمان الحماية للفضاء السيبراني.

فكانت البدايات الأولى للاهتمام بهذا المجال من خلال القرار الصادر عن الأمم المتحدة بشأن جرائم الكمبيوتر، خلال المؤتمر الثامن لمكافحة الجريمة ومعاملة المجرمين المنعقد بالعاصمة الكوبية 'هافانا' في أوت 1990، الذي عممت توصياته لتشمل التعاون للحد من آثار التهديدات ذات الصلة بوسائل الإعلام الآلي والشبكات الحاسوبية الخاصة بالعدالة الجنائية والأحكام المتعلقة بحجز العائدات المالية للجريمة المنظمة.[2]

كذلك أصدرت الهيئة العامة للأمم المتحدة قرارا خاصا حول الأمن السيبراني عام 2003، ركز على مكافحة الجريمة السيبرانية، ومن ثم أصدرت قرارات حول ذات الموضوع عام 2010 ملحقا لضرورة أن تلجأ الدول إلى إجراء تقييم ذاتي بمحض إرادتها لمعرفة مدى تناسب أطرها التشريعية وقدرتها على مواكبة التطورات الحاصلة في مجال تقنيات المعلومات والاتصالات، كما اهتمت الأمم المتحدة بالبناء المؤسسي فقامت بإنشاء بعض الكيانات كالشركة التعددية ضد التهديدات السيبرانية عام 2009، كأول منظمة تدعمها الأمم المتحدة للتحالف لتحقيق الأمن السيبراني.[3]

وهذا وتعتبر منظمة الإنتربول INTERPOL من قبيل المنظمات الدولية المتخصصة التي تهتم بالتعاون الدولي بين أعضائها في مجال مكافحة العابرة للحدود الوطنية، والتي من ضمنها تلك الواقعة في الفضاء الالكتروني.[4]

إلى جانب المنظمات الدولية، اهتمت المجالس الإقليمية بوضع اتفاقيات للتصدي للجريمة السيبرانية، كالاتفاقية التي أبرمها مجلس أوروبا واعتمدت في بروكسل في 23 نوفمبر 2001، للتعاطي مع الطابع الدولي للجريمة السيبرانية، ودخلت تلك الاتفاقية حيز السريان في جويلية بعد مصادقة خمسة بلدان عليها.

[1] "كاسبرسكي وأفريبول تعززان شراكتهما في مكافحة الجرائم السيبرانية بتوقيع اتفاقية تعاون جديدة"، موقع Kaspersky، تاريخ المقال: 19-11-2024، تاريخ الاطلاع: 28-02-2025.

https://2u.pw/g3rym

[2] "مؤتمر الأمم المتحدة لمنع الجريمة والعدالة الجنائية"، موقع الجزيرة، تاريخ المقال: 2015/04/21، تاريخ الاطلاع:2025/01/23.

https://2u.pw/SHplxs

[3] هبة جمال الدين، "الأمن السيبراني والتحول في النظام الدولي، مجلة كلية الاقتصاد والعلوم السياسية م24، ع1(2023)، ص199-230

[4] عبد العزيز لزعر، مرجع سابق، ص258.

وتضمنت قواعد التعاون الدولي المتصلة بـ: تسليم المجرمين/ المساعدة المتبادلة لأغراض التحقيق/ الإجراءات الخاصة بالأعمال الجنائية ذات الصلة بنظم الحاسوب والبيانات/ إنشاء شبكة مساعدة متبادلة، ذات مراكز اتصال وطنية للتدخل الفوري في حال وقوع المخالفات.

من جهته أعلن الاتحاد الدولي للاتصالات والتحالف السيبراني العالمي في 09 جويلية 2018 التوقيع على بيان مشترك يشمل القواعد التالية:

- التعاون لباء مجتمع معلومات آمن ومفيد لجميع الأعضاء.
- القيام بمشاورات متبادلة لوضع آليات واستراتيجيات تمكن أعضاء الاتحاد من تحسين مستوى تأهبها للتهديدات السيبرانية.
- استعراض التقدم المحرز في مجال التعاون بين الأطراف، مع إمكانية وضع تدابير إضافية لتكثيف هذا التعاون.[1]

وبالرجوع إلى الجزائر فقد سعت إلى تكريس التعاون الدولي في الفضاء السيبراني من خلال طرح مبادرات وبناء شراكات منها:

في ديسمبر 2022، نظمت دائرة الاستعمال والتحضير لأركان الجيش الوطني الشعبي، ممثلة في مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة، الطبعة الأولى من التمرين السيبراني عالي المستوى لمبادرة "5+5 دفاع"* تحت عنوان "محاكاة أزمة سيبرانية واسعة النطاق تستهدف البنى التحتية الحساسة"، وقد تناول هذا التمرين عدة محاور رئيسية، من بينها آلية تبادل الخبرات في مجال الدفاع السيبراني، بالإضافة إلى مسائل السيادة في الفضاء السيبراني وحماية البنى التحتية الحساسة.[2]

وفي خطوة هامة لتطوير القدرات التقنية للجيش الجزائري، تم توقيع مذكرة تفاهم بين وزارة الدفاع الوطني وشركة هواوي الصينية في 2021؛ تقضي بإنشاء أكاديمية رقمية للامتياز في المدرسة العسكرية المتعددة التقنيات، بهدف تطوير مهارات الكوادر العسكرية في مجال تكنولوجيا الملومات والاتصالات.

ما يدل على أن الدولة الجزائرية وسعت من دائرة التعاون لتشمل تبادل الزيارات والدورات التكوينية والشراكات الدولية، في المجالات التي شملتها السياسة الجنائية لمكافحة الإجرام عامة، والاستفادة من خبرات الدول الرائدة في مجال الأمن السيبراني.

[1] ب عيمور، "الدفاع والأمن السيبراني: مقاربات متكاملة"، مجلة الجيش الوطني الشعبي 715 (فيفري 2023)، ص45.

* هي مبادرة تعاون إقليمي بين دول حوض البحر الأبيض المتوسط، تهدف إلى تعزيز التعاون في مجال الدفاع والأمن ومواجهة التهديدات المشتركة، تأسست عام 2004 وتضم عشرة دول، خمسة منها من الضفة الشمالية: إيطاليا، فرنسا، مالطا، البرتغال، إسبانيا، وخمسة من الضفة الجنوبية: الجزائر، ليبيا، موريتانيا، المغرب، وتونس.

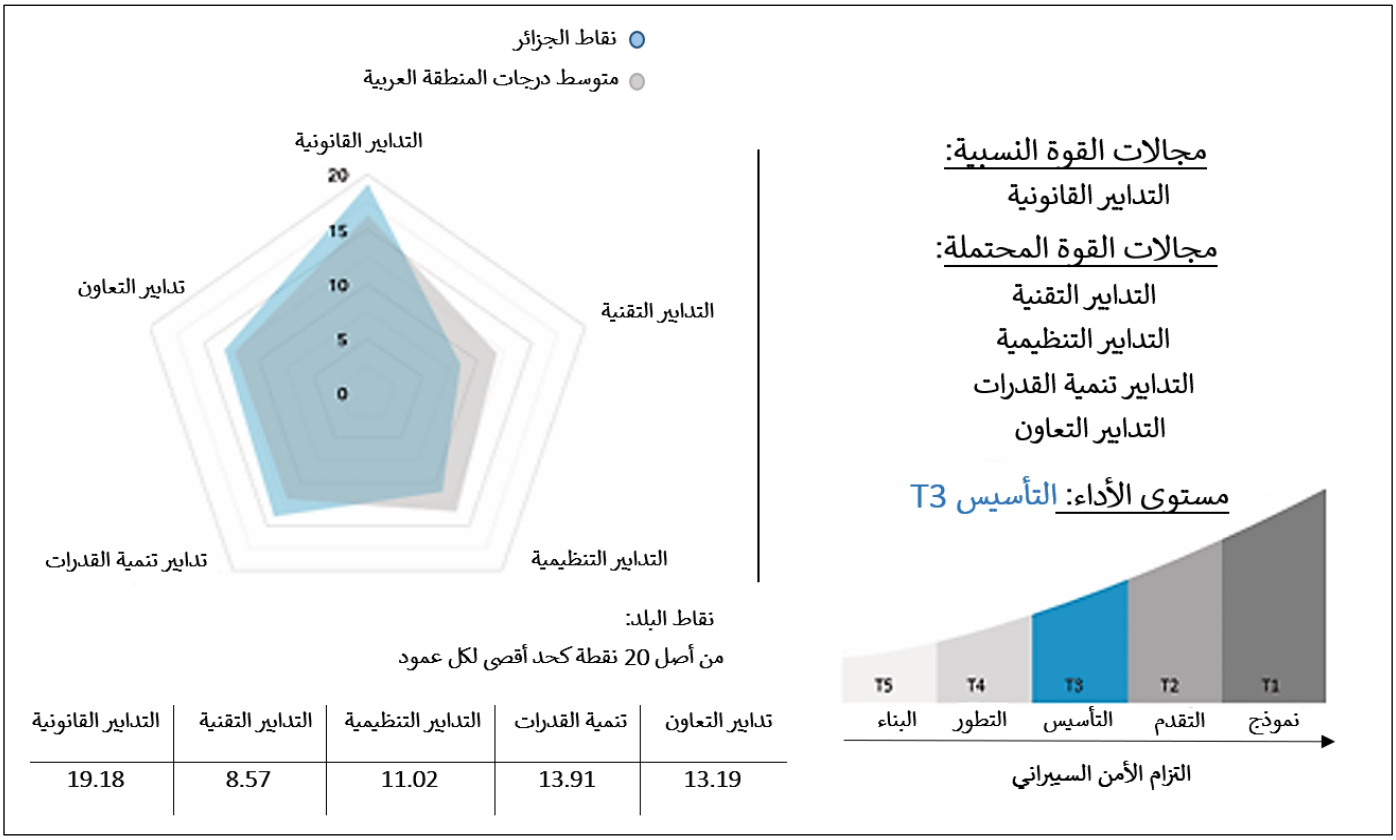
[2] ب عيمور، نفس المرجع، ص 51.

المطلب الثالث: التحديات التي تواجه السياسة الأمنية الجزائرية في المجال السيبراني

على الرغم من الجهود الجزائرية المبذولة لتحقيق الأمن السيبراني والاستعداد لمواجهة التهديدات المستقبلية، لا تزال الجزائر تفتقر إلى استراتيجية وطنية شاملة للأمن السيبراني، ويرجع ذلك إلى جملة من العوامل الخارجية كشدة تعقيد البيئة الالكترونية، سيما مع الازدياد المتسارع لمستخدمي الانترنت عبر العالم، ناهيك عن طبيعة التهديدات السيبرانية العابرة للحدود والتي أفرزت إشكاليات في تحديد الأطراف المسؤولة عن الهجمات السيبرانية.[1]

هذا بالإضافة إلى جملة من العوامل الداخلية التي أوضحها الملف التعريفي للجزائر في مقياس الأمن السيبراني العالمي على النحو التالي:

شكل 6: مكانة الجزائر ضمن مقياس الأمن السيبراني العالمي



التدابير القانونية	التدابير التقنية	التدابير التنظيمية	تنمية القدرات	تدابير التعاون
19.18	8.57	11.02	13.91	13.19

المصدر: من إعداد الباحثة استنادا على Global Cybersecurity Index 2024, 5th Edition, p70

من خلال مؤشرات GCI يتضح أن الجزائر لديها مستوى قبول من ناحية التدابير القانونية، في حين أنه من جانب التدابير التقنية لاتزال جهود الجزائر متواضعة جدا، إلى جانب المؤشرات التنظيمية التي تعد غير كافية حسب ما ورد في التقرير، أما فيما يخص بناء القدرات والتعاون الدولي فقد صنفت الجزائر في درجة مقبولة نظرا لمحاولاتها الجادة في

[1] إكرام بركان وفهيم رملي، مرجع سابق، ص 19.

مجال التكوين والاستثمار في العنصر البشري، إلى جانب انخراطها في عديد الاتفاقيات لتدعيم العلاقة مع الدول والمنظمات في مجال الأمن السيبراني.

بالتالي هنالك جملة من المعيقات والتحديات التي تواجه عمل الأجهزة الأمنية والمؤسسات الفاعلة في الأمن السيبراني من ضمنها:

- زيادة عدد المشتركين في شبكة الانترنت في الجزائر حيث بلغ 33.49 مليون بداية عام 2024، حسب ما أورده تقرير "Digital 2024" والاستعمال الواسع لشبكات التواصل الاجتماعي، الذي وصل إلى 24.85 مليون حسب ذات التقرير،[1] وهو ما ساهم بشكل كبير في ارتفاع نسب الجرائم الالكترونية، وهو ما يستوجب وضع آليات محكمة لضمان الأمن السيبراني عند استخدام مواقع التواصل الاجتماعي.
- انتشار تكنولوجيا الاتصال فائقة السرعة والتدفق، ما أسهم في سرعة تنفيذ الجرائم ووضع الجهات الأمنية المختصة أمام تحدي سرعة مباشرة التحقيقات والتسلح بالأجهزة المتطورة والبرامج الحديثة سريعة الخدمة.
- تعتبر عمليات التخفي أثناء استخدام خدمات الأنترنت (Proxy) من أكبر التحديات التي تواجه جهات التحقيق المختصة، ما يتطلب تعاونا متعدد الجهات واستخدام وسائل متطورة لرصد التفاصيل وفك الشفرات، بالإضافة إلى تطوير البنية التحتية المعلوماتية وتحديثها باستمرار.[2]
- ارتفاع حجم التهديدات السيبرانية وتمكن فاعليها من تطوير أدواتهم وآلياتهم، ما تسبب بأضرار بالغة تسببت بخسائر مادية مقارنة بإجراءات الجهاز الأمني لتحقيق الأمن السيبراني.
- غياب التنسيق بين الأجهزة الأمنية الوطنية والدولية ما يعيق تأمين الشبكات من الهجمات السيبرانية والإرهاب الالكتروني الدولي، هذا إلى جانب ما يحويه الفضاء السيبراني من صراع وحروب إلكترونية بين الوحدات الدولية3.
- مشكل الاختلاف في تعريف الجريمة السيبرانية بين الدول؛ فما تعتبره دولة فعلا إجراميا يستوجب العقاب، قد لا يحظى بنفس التجريم في دولة أخرى. هذا التباين القانوني يضعف آليات التعاون الدولي في القبض على المجرمين وتسليمهم للعدالة، وينشئ ثغرات يستغلها المجرمون السيبرانيون للإفلات من المساءلة في الدول المتساهلة قانونيا[4].

[1] Simon Kemp, DIGITAL 2024 : ALGERIA, DATAREPORTAL, 23 February 2024.
https://2u.pw/fsolXB7

[2] سمير بارة، مرجع سابق، ص275-276.

[3] نجمة شريط، مرجع سابق، ص87

[4] محافظ شرطة، مرجع سابق.

خلاصة

فيما سبق من مضمون هذا الفصل نجد تفصيلا للنتائج التالية:

تستند السياسة الأمنية الجزائرية إلى جملة من المرتكزات الأساسية كالعوامل التاريخية والجغرافية والإيديولوجية، وقد مرت هذه السياسة الأمنية بعدة مراحل منذ الاستقلال إلى يومنا هذا حاولت من خلالها الجزائر، التكيف مع الظروف والمستجدات المحلية والتطورات الإقليمية والعالمية وهذا لأجل ضمان وحماية الاستقرار الوطني.

يشكل التهديد السيبراني تحديا جديدا للسياسة الأمنية في الجزائر، حيث تزايدت أهمية هذا التحدي مع التطور التكنولوجي السريع، ومع التحول الرقمي لمؤسسات الدولة وتكثيف الاعتماد على أدوات تكنولوجيا المعلومات والاتصالات.

من الجانب المؤسساتي، ظهرت جهود الجزائر لتحقيق الأمن السيبراني من خلال استحداث هيئات ومراكز تضطلع بأدوار هامة في مجابهة التحديات السيبرانية والتي من بينها المصلحة المركزية لمكافحة الجريمة السيبرانية ومصلحة الدفاع السيبراني ومراقبة أمن الأنظمة.

من الجانب القانوني، ولتدارك الفراغ التشريعي في مجال مكافحة الجرائم المعلوماتية قام المشرع الجزائري بإدراج تعديلات خاصة على قانون العقوبات الجزائري، واستحدث عدة قوانين ومراسيم لتقليص هذه الجرائم المستحدثة والعابرة للحدود.

لقد عملت الجزائر على تطوير استراتيجية متعددة الجوانب (التشريعية، التنظيمية، البشرية، المؤسساتية)، بالموازاة مع العمل لتعزيز التعاون الإقليمي والدولي، إلا أنه وبالرغم من الجهود المبذولة لاتزال تشهد تحديات سيما من الناحية التقنية والتطبيقية.

الفصل الثالث: البوتات الاجتماعية كجزء من الاستراتيجية الأمنية الجزائرية

تمهيد:

إن التوظيف الممنهج للبوتات الاجتماعية في ترويج الأخبار المضللة عبر مواقع التواصل الاجتماعي، قد أضحى يشكل معركة أمن قومي، وذلك من خلال استهدافها للاستقرار المجتمعي وعملها على زرع الفتنة وتقويض الثقة بين مؤسسات الدولة والشعب، وهو ما يستلزم تطوير استراتيجية أمنية شاملة، تتجاوز رصد هذه الحملات المضللة والتصدي لها، لتشمل تعزيز الوعي المجتمعي كدرع أساسي لحماية الأمن القومي.

يسعى هذا الفصل إلى فهم معمق لكيفية استخدام هذه البرامج الآلية لنشر المعلومات المضللة واستغلالها في تقويض الثقة في المؤسسات الوطنية وزعزعة الاستقرار الداخلي، كما يستعرض الإجراءات الدفاعية المتخذة من قبل الدولة الجزائرية، لمكافحة هذا التهديد من خلال تعزيز القدرات المؤسساتية وتوعية المجتمع بمخاطر التضليل السيبراني.

المبحث الأول: تأثير البوتات الاجتماعية على الجزائر

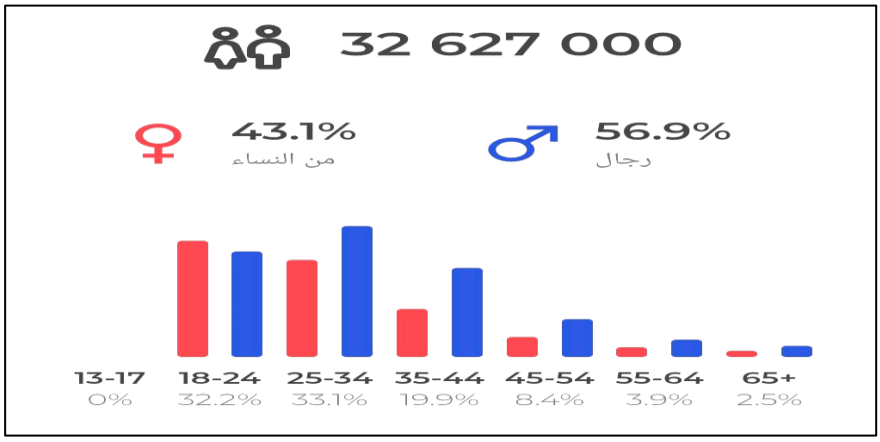
يشهد الفضاء السيبراني الجزائري تزايدا ملحوظا في التوظيف الخبيث للبوتات الاجتماعية؛ التي باتت تشكل أدوات مؤثرة تنطوي على تهديدات للأمن والاستقرار. وسيسعى هذا المبحث إلى تحليل تأثير هذه البوتات في سياقات مختلفة؛ بدءا من محاولات استغلالها خلال الحراك الشعبي وفي التأثير على المشاركة الانتخابية، إلى دورها في تأجيج القضايا الداخلية وزعزعة الاستقرار المجتمعي، وصولا إلى توظيفها لخدمة توجهات الإرهاب السيبراني.

المطلب الأول: حالات التهديد السيبراني في الجزائر باستخدام البوتات الاجتماعية

قبل الشروع في تحليل الحالات التي صرحت فيها الأجهزة الأمنية الجزائرية المختصة في المجال السيبراني، عن استخدام البوتات الاجتماعية كتهديد للأمن السيبراني الجزائري، سيتم أولا تبيان مدى انتشار منصات التواصل الاجتماعي في الجزائر.

بحيث تشير الإحصائيات أن عدد مستخدمي موقع فيسبوك في الجزائر قد تجاوز 32 مليون مستخدم في مارس 2025، ليشكل بذلك حوالي 69 ٪ من عدد السكان[1].

شكل 7: توزيع مستخدمي فيسبوك في الجزائر حسب الجنس والفئات العمرية



المصدر: ترجمة الباحثة لـ: " Social media users in Algeria "

يظهر الشكل أن غالبية مستخدمي فيسبوك في الجزائر هم من الذكور (56.9 ٪)، وأن الفئة العمرية (25-34 عاما) تمثل الشريحة الأكبر من مستخدمي فيسبوك في الجزائر، تليها الفئة العمرية (18-24 عاما)، ما قد يجعل من الفئات الشابة أكثر عرضة للمعلومات المضللة التي تنتشر عبر المنصة. كما سُجِّل ما يتجاوز 11 مليون مستخدم لموقع

[1] "Social media users in Algeria", NapoleonCat, March 2025, Accessed on : 30/04/2025.
https://2u.pw/v1pbP

انستغرام، أي ما يمثل 25.1 ٪ من إجمالي السكان، فيما تخطى مستخدمو منصة إكس (تويتر سابقا) مليون مستخدم وهو ما يعادل 2.4 ٪ من إجمالي السكان[1].

وبالنظر إلى العدد الكبير لمستخدمي فيسبوك في الجزائر، فإنه يمثل المنصة الأوسع لانتشار المعلومات المضللة وحسابات البوتات الناشطة في ترويجها· هذا الانتشار يجعله المصدر الأساسي للأخبار الزائفة في البلاد، خاصة مع ميل بعض وسائل الإعلام لنقل الأخبار من هذه المنصات دون تدقيق كاف، مما يضاعف من سرعة انتشارها وتأثيرها السلبي على المجتمع[2].

أمام هذا الانتشار الواسع لمنصات التواصل الاجتماعي في الجزائر، بات لزاما تحديد نطاق تأثيراتها المختلفة، سيما تلك المتعلقة باستخدام البوتات الاجتماعية وتداعياتها المحتملة على الأمن السيبراني الجزائري.

الفرع الأول: البوتات الاجتماعية والحراك الجزائري: تحليل للدوروالتأثير

يمثل الحراك الشعبي الجزائري حركة احتجاجية واسعة النطاق، بدأت في 22 فبراير 2019، كرد فعل على ترشح الرئيس عبد العزيز بوتفليقة لعهدة خامسة[3]. تميز هذا الحراك بطابعه السلمي والحضاري وبمشاركة واسعة من مختلف فئات الشعب الجزائري، مطالبين بالتغيير الجذري للنظام السياسي ومكافحة الفساد وإقامة دولة القانون.

وقد اعتبرت وسائل التواصل الاجتماعي، وفي مقدمتها فيسبوك، كوسيط ميديولوجي* ينقل صوت الحراك الشعبي الجزائري ومطالبه. بيد أن، هذا الفضاء الرقمي لم يسلم من الآثار السلبية، إذ برز دور البوتات الاجتماعية في إحداث انقسام إيديولوجي حاد خلال تفاعلها مع الحراك، بهدف خلق هوة بين مؤيدي الجيش وبين المتوجسين من قراراته. وإن تباينت الآراء حول من يقف وراء هذه الحسابات الوهمية، فإن المتعارف عليه أن هذه الفئات تظهر عادة خلال الأزمات والمراحل التي تشهد استقطابا في وجهات نظر سياسية وإيديولوجية معينة[4].

وتجدر الإشارة إلى أن وظيفة شبكات البوتات الاجتماعية لم تقتصر على تأجيج الاستقطاب السياسي والمجتمعي عبر ترويج روايات متناقضة وتضخيم الخلافات، بل كانت أيضا أداة فعالة في نشر الأخبار الزائفة 'Fake News'والمعلومات

[1] Simon Kemp, Ibid.

[2] رياض شعباني، "هيئة جزائرية لمحاربة الإشاعات الإلكترونية.."،IJnet ، تاريخ المقال: 6 سبتمبر 2021، تاريخ الاطلاع: 30 أفريل 2025.

https://2u.pw/14S0T

[3] محمد حمشي، حراك 22 فبراير 2019 في الجزائر انتفاضة واحدة ومقاربات شتى، (قطر: المركز العربي للأبحاث ودراسة السياسات، ط1، 2023)، ص 21.

* ظهر مصطلح الميديولوجيا (La médiologie) أول مرة سنة 1979م، مع الفرنسي ريجيس دوبراي (Régis Debray) ، ويقصد به ذلك الحقل الدراسي الذي يهتم بدراسة الوسائط التي تحمل الرسائل والأفكار وتنشرها، كما يركز على تأثير هذه الوسائط المادية والتقنية على الثقافة والمجتمع، أما مصطلح "وسيط ميديولوجي" فهو الأداة التي تعمل كقناة لنشر الأفكار والمعلومات والتأثيرات الثقافية.

[4] هجيرة حمادي، "الرأي العام السيبراني في الجزائر: بين الميديولوجيا والأيديولوجيا قراءة في مضمون صفحات فيسبوكية أثناء فترة الحراك الشعبي"، مجلة المعيار، م26، ع5 (2022)، ص.ص 570-582.

المضللة. فمن خلال حسابات وهمية منظمة، عملت هذه البوتات على تداول الشائعات والأكاذيب بكثافة، مستغلة حساسية الأوضاع لتقويض الثقة وتوجيه الرأي العام.

وبهذا كانت مواقع التواصل الاجتماعي عموما وموقع فيسبوك بصفة خاصة، فضاء حيويا لتبادل الأخبار والآراء والنقل المباشر للوقائع والأحداث، لكن سرعان ما تحول إلى ساحة للتضليل؛ حيث استغلته جهات مغرضة لإنشاء ونشر أخبار كاذبة ومغلوطة. وقد تفاقمت خطورة الأمر مع تدخل شبكات البوتات الاجتماعية التي عملت على تضخيم هذه الأخبار الزائفة وتسريع انتشارها[1].

وتتعدى تأثيرات الأخبار الكاذبة، التي تعمل البوتات الاجتماعية كمحفز رئيسي لانتشارها، نطاق الفضاء السيبراني لتصل إلى الواقع؛ فعبر التداول الواسع النطاق، يكتسب الزيف تأثيرا متزايدا، مما يؤدي إلى تحوله في الإدراك الجمعي إلى حقائق راسخة.

وما فاقم حجم المشكلة، تبني بعض المؤسسات الإعلامية هذه المعلومات المضللة؛ فبدلا من الالتزام بالمعايير المهنية المتمثلة في استقاء المعلومات من مصادر موثوقة والتحقق من صحتها قبل النشر، تسارع هذه المؤسسات إلى تداول بيانات ووقائع غير مدققة، بمنطق المنافسة على السبق الزمني. مما يقوض دورها في نقل الحقائق وتنوير الرأي العام[2].

وقد أحدثت الأخبار المزيفة التي كثيرا ما يتم ترويجها وتوسيع نطاق تأثيرها، بشكل ممنهج بواسطة البوتات الاجتماعية، آثارا سلبية على عديد الجوانب، يذكر منها:

- إثارة حالات الذعر الجماعي: إذ عملت الأخبار الكاذبة، التي يرجح أن البوتات الاجتماعية لعبت دورا في تنسيقها ونشرها، على إثارة القلق في أوساط المجتمع. وقد ظهر ذلك -على سبيل المثال- في انتشار خبر كاذب عن خروج مظاهرات في العاصمة تم تفريقها بالقوة من قبل الدولة، مع ادعاءات عن إصابات لا أساس لها من الصحة[3]. يعكس هذا الغرض الواضح من وراء هذه الأخبار المضللة المتمثل في تشويه صورة الأجهزة الأمنية وتقويض ثقة الشعب بها.
- تفكيك المجتمع وتشتيته: فبتعدد المواقف المتعارضة داخل المجتمع، تنشأ خلافات فكرية عميقة، وتزيد البوتات من حدة هذه الخلافات؛ عبر نشرها لمحتويات مضللة ومتحيزة تخدم أجندات معينة.
- صعوبة التمييز بين الحقيقة والإشاعات: لا سيما في أوساط الجمهور الذي يعاني من نقص في الوعي السياسي والثقافي والتعليمي، فمع انتشار الأخبار المزيفة وتداخلها مع المعلومات الحقيقية، يصبح هذا الجمهور أكثر

[1] ضابط شرطة، مقابلة شخصية، فرقة محاربة الجرائم السيبرانية بأمن ولاية الجزائر التابعة للشرطة القضائية، 17 أفريل 2025.

[2] عبد الجبار بوطمين وعادل جربوعة، "الأخبار الزائفة والحراك الشعبي في الجزائر"، مجلة المعيار، م25، ع54 (2021)، ص.ص 207-223.

[3] المرجع نفسه، ص220.

عرضة للتضليل، خاصة البيئة الرقمية التي يشوبها استخدام البوتات الاجتماعية، التي تستغل الأزمات والأحداث السياسية لنشر معلومات مغلوطة[1].

- التشويش على مطالب الحراك: يلحظ المراقب لتطورات الحراك الشعبي، تراجعا ملحوظا في وحدته وتماسك مطالبه، ويرد هذا التحول بشكل كبير إلى تراكم الأحداث والوقائع والكم الهائل من الأخبار المتداولة، أين عملت البوتات في كثير من الأحيان كقوة تشويش وتضليل، انعكست آثارها على إضعاف وحدة المطالب الأساسية للحراك.

لقد مثلت الأخبار الزائفة -ولا تزال- تهديدا على الأمن الوطني الجزائري، وقد تجلى ذلك بوضوح خلال الحراك الشعبي، أين شهدت الجزائر من حملة منظمة من هذه المعلومات المغلوطة، لعبت البوتات الاجتماعية دورا فعالا في انتشارها وتأثيرها، تحت مسعى توجيه الرأي العام وتضليله بهدف تغيير مسار الحراك، الأمر الذي شكل تهديدا فعليا للأمن القومي الجزائري.

الفرع الثاني: البوتات الاجتماعية والمشاركة الانتخابية في الجزائر

بينما ترتكز الحملات الانتخابية في جوهرها على التنافس بين البرامج وكسب التأييد الشعبي ضمن الأطر القانونية، يمثل الفضاء السيبراني بطبيعته المنفتحة، ميدانا للدعاية الانتخابية بمختلف أشكالها، بما في ذلك الدعاية المضادة التي قد تتضمن خطاب الكراهية وتشويه المنافسين[2]، وتصل إلى حد التشجيع على العزوف الانتخابي. وتزداد هذه المخاطر مع الاستخدام المتزايد للبوتات الاجتماعية التي تساهم في نشر هذه الأساليب على نحو يصعب التحكم فيه.

إذ برزت وسائل التواصل الاجتماعي كأداة رئيسية في تضليل الرأي العام في سياق الانتخابات الرئاسية الجزائرية لعام 2019، أين احتدمت حرب جيوش إلكترونية بين فريق يمثل الحراك الشعبي حذّر من الانتخابات ودعا الجزائريين لمقاطعتها، وآخر حث على ضرورة المشاركة فيها بكثافة[3].

وقد تميز هذا الصراع السيبراني باستخدام استراتيجيات تواصلية متنوعة، بما في ذلك نشر المعلومات، والتأثير النفسي، والتلاعب بالرأي العام، كما لوحظ انتشار واسع لمعلومات غير موثوقة وأخبار زائفة خاصة في منصة فيسبوك باعتبار أنها الأكثر استخداما في الجزائر، وكذا في منصة X (تويتر سابقا).

[1] خالد بومخيلة، "واقع الحملات الانتخابية في فضاء التواصل الاجتماعي -دراسة حالة الجزائر-"، المجلة الجزائرية للأبحاث والدراسات، م4،ع4 (2021)، ص.ص 370-386.

[2] عثمان لحياني، "انتخابات الجزائر: "فيسبوك" ميدان الحملات والدعاية المضادة"، العربي الجديد، تاريخ المقال: 23 نوفمبر 2019، تاريخ الاطلاع: 05-05-2025.
https://2u.pw/YbggI

[3] منية غانمي، "الجزائر.. الانتخابات الجزائرية تشعل حربا إلكترونية بين الحراك والسلطة"، العربية. نت، تاريخ المقال: 20 ماي 2020، تاريخ الاطلاع: 2025/05/06.
https://2u.pw/78lt4

ويشير تحليل المنشورات والتغريدات السائدة آنذاك، إلى وجود حملات منسقة (Coordinated campaigns) تدخلت فيها أطراف خارجية معادية للجزائر، لتشكيل تصورات لدى الجمهور بأن نتائج العملية الانتخابية محسومة مسبقا وحثت على المقاطعة.

ولزيادة مدى انتشار هذه الرسائل، تضمنت هذه الحملات استخدام حسابات وهمية (Bot accounts and Sockpuppet accounts)؛ وهو ما كشف عنه قياس درجات الأتمتة لأبرز التغريدات التحريضية، من خلال موقع بوتوميتر "Botometer".

شكل 8: واجهة موقع بوتوميتر "Botometer"

المصدر: https://botometer.osome.iu.edu/

شكل 9: طريقة عرض نتائج بوتوميتر "Botometer" على الموقع

المصدر: المرجع نفسه.

يبرز الشكلان 8 و9 واجهة موقع بوتوميتر "Botometer"، أين يتم إدخال حسابات المستخدمين المشبوهة، في خانة "اسم المستخدم @"، ثم من خلال تحليل الموقع لميزات الحساب (الملف الشخصي، الأصدقاء، الشبكة، النشاط الزمني، المحتوى، المشاعر، اللغة)، يعين Botometer نتيجة (تتراوح من 0 إلى 5) وتزيد احتمالية كون الحساب بوتا كلما كانت دلالة التقييم مرتفعة.

بالتالي، هنا يظهر الارتباط المباشر بين المحتوى الذي يحمل طابعا تحريضيا والطبيعة الآلية للحسابات التي تنشره، وهو ما يؤكد الدور المحوري الذي تضطلع به وسائل التواصل الاجتماعي بصفة عامة، والبوتات الاجتماعية خصوصا في عملية تضليل الرأي العام، والتأثير على مسار الانتخابات.

وهو ما أكد عليه رئيس لجنة الشؤون الخارجية والتعاون الدولي بمجلس الأمة "محمد عمرون"، خلال محاضرة نظمتها السلطة الوطنية المستقلة للانتخابات، أين استعرض أساليب التدخل الأجنبي وتداعياته الخطيرة على الأمن الوطني والمسار الديمقراطي، مؤكدا على الدور المحوري لمواقع التواصل الاجتماعي في نشر حجم هائل من المعلومات المغلوطة يوميا كأحد أبرز هذه الأساليب. كما أشار إلى أشكال أخرى للتدخل تشمل الهجمات السيبرانية، والفوضى الآلية وصولا إلى الضغوط الاقتصادية والدبلوماسية التي تستغل هذه المنصات. وأوضح أن أهداف هذه التدخلات تتمحور حول توجيه الانتخابات وفرض أجندات خارجية وزرع الانقسام الداخلي عبر هذه المنصات[1].

وبالاسقاط على واقع البوتات الاجتماعية، يلاحظ بوضوح كيفية استغلال هذه البرامج الآلية من طرف الجهات الخارجية الساعية للتدخل في الشؤون الداخلية للدول بهدف إضعاف الثقة في مخرجات العملية الانتخابية، وتشويه المسار الديمقراطي.

[1] برقية من وكالة الأنباء، موقع Fileworx، تاريخ البرقية: 2025/04/22، 14:11، تاريخ الاطلاع: 2025/04/29.

المطلب الثاني: دور البوتات الاجتماعية في تأجيج القضايا الداخلية

بداية، يشار إلى أن التنوع سمة أساسية للمجتمع الجزائري؛ حيث يضم أفرادا ذوي انتماءات جهوية وعروشية وحتى طائفية متباينة. وعلى الرغم من هذا التعدد، فإن هذه الانتماءات الفرعية تتكامل في نهاية المطاف لتكوّن هوية وطنية شاملة، ضمن سياق مجتمع موحد ونظام سياسي واحد. إذ أنه تاريخيا، لم يشهد هذا التنوع الإثني، الذي يضم العرب والشاوية والقبائل والطوارق والميزابيين، صراعات عرقية واضحة. ورغم المساعي الاستعمارية الفرنسية لزرع الفتنة والانقسام بين هذه المكونات، بهدف إضعافها وتشتيتها عن هدف التحرر، إلا أن تلك المحاولات باءت بالفشل، وهو ما تجلى بوضوح في وحدة الصف الوطني خلال الثورة التحريرية، التي جسدت نقطة التقاء وتوحيد لمختلف الجهات الجزائرية في مواجهة المستعمر[1].

الفرع الأول: البوتات الاجتماعية ونشر التطرف وخطاب الكراهية

مع التطورات الحديثة، وتحديدا مع الاستخدام الموسع لوسائل التواصل الاجتماعي، برزت تحولات جديدة في إدارة التفاعلات الاجتماعية والسياسية الداخلية. فبينما تتيح هذه المنصات فرصا لتعزيز التعبير عن التعددية الثقافية وتبادل الآراء بشكل بناء، فإنها قد تمثل بيئة خصبة لتأجيج بعض القضايا الداخلية الحساسة، إذ يمكن لجهات مختلفة استغلال هذه الوسائل لنشر خطابات ترويجية للكراهية والتعصب، بالاعتماد على استثارة الانتماءات الجهوية بهدف خلق حالة من الاستقطاب المجتمعي.

وفي امتداد لمحاولات قوى خارجية لزعزعة استقرار المجتمع الجزائري عبر تاريخه، يظهر في العصر الرقمي الراهن، تحدي توظيف البوتات في وسائل التواصل الاجتماعي بغرض نشر الفوضى وتقويض التماسك الاجتماعي.

فبعد فشل محاولات أطراف معادية للجزائر في زرع الفتنة بين مكونات المجتمع الجزائري عبر تاريخيه، تأتي اليوم هذه الكيانات الرقمية لتنفيذ أجندات مماثلة عبر نشر معلومات مضللة وتأجيج الفتن وخطاب الكراهية بين مكونات المجتمع الجزائري، ما يمثل تهديدا مباشرا للأمن الوطني الجزائري[2].

إلى جانب ما سبق، يبرز الإرهاب السيبراني كأحد أبرز التهديدات التي تلقي بتداعياتها على الأمن القومي الجزائري واستقراره الداخلي، ويتجلى هذا في استغلال التنظيمات المتطرفة لوسائل التواصل الاجتماعي والمواقع الإلكترونية للتحريض على العنف والتطرف، وتجنيد الشباب[3].

فخلال الثلاثي الأول من سنة 2017، تلقت مصالح الأمن الجزائرية ما يزيد عن 2000 بلاغ يتعلق بأنشطة مشبوهة ذات صلة بالإرهاب، تحدث عبر مختلف المنصات الإلكترونية، وورد أن غالبية هذه الإخطارات التي وردت إلى الأجهزة

[1] وليد شايب الدراع ونجيب بخوش، "الهوية الثقافية الجزائرية بين التنوع ورهانات الوحدة الوطنية"، مجلة معالم، م15، ع 2 (2022)، ص.ص 175-188.

[2] ضابط شرطة، مرجع سابق.

[3] سلمى بلخير ومحمود شرقي، أثر مواقع التواصل الاجتماعي على الأمن المجتمعي الجزائري"، المجلة الجزائرية للأمن والتنمية، م12، ع2 (أفريل 2023)، ص.ص 172-182.

الأمنية تحت بند "شبهات إرهابية"، تركزت بشكل أساسي في رصد دعوات تستهدف تجنيد أفراد جدد لصالح تنظيمات إرهابية، إلى جانب محاولات لاختراق حسابات المستخدمين على شبكات التواصل الاجتماعي.

كما تضمنت هذه البلاغات تنبيهات وتحذيرات بشأن منشورات دعائية تروج لأفكار متطرفة[1]، وفي هذا السياق، يبرز دور البوتات كأداة تساهم في تفاقم خطر الإرهاب السيبراني على الاستقرار الداخلي الجزائري. فمن خلال قدرتها على نشر المحتوى المتطرف على نطاق واسع، وأتمتة حملات التجنيد، تصبح البوتات كقوة مضاعفة لدى التنظيمات الإرهابية.

وقد أكد اللواء مناد نوبة، القائد العام للدرك الوطني الجزائري، على خطورة الإرهاب الإلكتروني الذي يستهدف الجزائر عبر تنامي مظاهر الترويج للعنف والتطرف باستعمال أحدث التقنيات التكنولوجية، داعيا إلى تعزيز إجراءات الرقابة لحماية الشباب بشكل خاص[2].

لكن تجدر الإشارة إلى أنه وبالرغم من محدودية تأثير المواقع الإلكترونية الإرهابية على المجتمع الجزائري، لعدة أسباب منها المتعلقة بالذاكرة والتحصين الثقافي، إلا أن الاستخدام المتزايد للبوتات الاجتماعية يمثل تحديا جديدا يتطلب يقظة مستمرة، وتطوير آليات فعالة لمكافحة هذه التهديدات السيبرانية.

<u>الفرع الثاني:</u> البوتات الاجتماعية وتأثيراتها على ثقة المجتمع في مؤسسات الدولة

لعل من أبرز القضايا التي تستهدفها البوتات الاجتماعية، خفض المعنويات وزعزعة الثقة بين المواطن والمؤسسات الرسمية للدولة، وذلك انطلاقا من نشر أخبار زائفة بشكل آلي ومكثف حول المؤسسات الحكومية، كاتهامها بالفساد أو العجز والتشكيك في نزاهتها، وكذا التركيز على الأزمات كالبطالة، ارتفاع الأسعار[3] بغية تشكيل صورة نمطية في ذهن المواطن بأن الدولة عاجزة عن تسيير الشأن العام وغير قادرة على تلبية مطالبه.

كذلك تستغل البوتات الهفوات أو الأخطاء الفردية داخل المؤسسات التي قد تصدر عن موظف عمومي أو أفراد من الأجهزة الأمنية، أو حتى مسؤولين سياسيين ومحليين، لتقوم فيما بعد بتضخيمها، وعرضها على شكل سلوك يعكس توجه المؤسسة أو الدولة ككل.

وما يغذي عمل البوتات ويجعلها أكثر قابلية للتصديق، هو اعتمادها على نشر صور، مقاطع فيديو، أو وثائق قد تكون مفبركة رقميا أو قديمة ولا علاقة لها بالحدث المعروض، لتقوم فيما بعد بتوظيفها في سياقات سياسية وأمنية حساسة تقدم على شكل أدلة على ممارسات قمع أو عجز لإثارة الرأي العام ولزعزعة الاستقرار.

[1] عتيقة كواشي، "تداعيات الإرهاب السيبراني على الأمن القومي الجزائري"، المجلة الجزائرية للأمن والتنمية، م12، ع3 (جويلية 2023)، ص. ص205-214.

[2] عنترة بن مرزوق والكر محمد، "البعد الالكتروني للسياسة الأمنية الجزائرية في مكافحة الإرهاب"، مجلة العلوم الإنسانية والاجتماعية، ع28 (جوان 2018)، ص. ص 29-50.

[3] ضابط شرطة، مرجع سابق، ص1.

بالتالي تتجاوز هذه الحملات حدود التأثير الفردي، لتصبح جزءا من حرب نفسية شاملة، تستهدف تفكيك المجتمعات من الداخل، دون الحاجة لتدخل عسكري مباشر؛ عبر ضرب الثقة بين الشعب ومؤسسات دولته، سيما منها تلك المعنية بحفظ النظام والدفاع الوطني.

المبحث الثاني: آليات مواجهة التهديدات الأمنية الناجمة عن البوتات الاجتماعية

أمام التهديدات الآنفة الذكر التي باتت تفرضها البوتات الاجتماعية على الأمن القومي الجزائري، تناول هذا المبحث آليات المجابهة، بداية من تعزيز القدرات المؤسساتية، ثم نشر الوعي المجتمعي بمخاطرها، ليختتم بعرض نتائج استبيان لقياس مستوى الوعي العام بالبوتات الاجتماعية.

المطلب الأول: تعزيز القدرات المؤسساتية لمواجهة تداعيات البوتات الاجتماعية

تضطلع المؤسسة التنفيذية الجزائرية بقيادة رئيس الجمهورية، وبالتعاون الوثيق مع الأجهزة الأمنية والاستخباراتية، وبالاستفادة من دور وسائل الإعلام الوطنية، بدور ريادي في رسم السياسة الأمنية وصياغتها. وبفضل قدرات هذه المنظومة المتكاملة، يتم رسم استراتيجية لتعزيز قدرات الدولة المؤسساتية لمواجهة شتى التهديدات الأمنية، بما في ذلك التحديات المتنامية التي تطرحها البوتات الاجتماعية عبر نشر التضليل وزعزعة الاستقرار.

الفرع الأول: الهيئات الحكومية ومواجهة تضليل البوتات الاجتماعية

أولت السلطة التنفيذية الجزائرية، اهتماما خاصا بمجال الأمن السيبراني سيما أمام ارتفاع منحى التهديدات السيبرانية؛ تجلى هذا الاهتمام بوضوح مع إصدار "المرجع الوطني لأمن المعلومات" (Référentiel National de Sécurité de l'information 2020) كمبادرة حكومية تهدف إلى توفير إطار عمل موحد للهيئات الحكومية لحماية أنظمتها وبياناتها الحساسة، وذلك من خلال تحديد الحد الأدنى متطلبات الأمان، وتقديم أفضل الممارسات المعتمدة دوليا. تركز الوثيقة على عدة محاور رئيسية تشمل:

- حوكمة أمن المعلومات، التي تحدد الأدوار والمسؤوليات اللازمة للإدارة الفعالة للأمن.
- إدارة المخاطر السيبرانية، التي تلزم الهيئات الحكومية على تطبيق منهجية للتعامل مع هذه المخاطر.
- التأكيد على أهمية تدريب وتوعية الموظفين، والالتزام بالقوانين واللوائح الوطنية[1].
- تحديد 20 مجالا رئيسيا لأمن المعلومات، بما في ذلك أمن وسائل التواصل الاجتماعي التي تبحث في سبل السيطرة على المخاطر الناجمة عن استخدام شبكات التواصل الاجتماعية، من خلال تنفيذ التدابير الأمنية اللازمة (الاستراتيجية والتكتيكية والتشغيلية). وورد فيه إرشادات تتعلق بالبوتات الاجتماعية، تحث على "تنفيذ آلية للتنبؤ والكشف والحماية من البوتات (حسابات التواصل الاجتماعي المستقلة والآلية)، التي تستخدم في التأثير على الرأي العام"[2].

[1] République Algérienne Démocratique et Populaire, Ministère de la poste, des Télécommunications, Référentiel National de Sécurité de L'information, 2020, p. p6-9.

[2] Ibid, p 69.

هذا ما يبرز إدراك المرجع الوطني للخطر الذي تمليه البوتات على مصداقية المعلومات المتداولة عبر وسائل التواصل الاجتماعي، وخاصة المواقع الرسمية للوزارات، أين يجري العمل لتطوير آليات للتنبؤ بها وتحييد دورها السلبي.

وتجدر الإشارة إلى أن وزارتي "البريد والمواصلات السلكية واللاسلكية"، و"الاتصال" هما الهيئتان الحكوميتان الأقرب لتمكين استراتيجيات مواجهة التضليل السيبراني؛ حيث تختص وزارة الاتصال بمواجهة التضليل الإعلامي؛ وذلك من خلال استنادها على جملة من القوانين، يذكر منها القانون العضوي للإعلام رقم 23-14 المؤرخ في 18 جمادى الأولى 1445 هـ، الموافق لـ 02 ديسمبر 2023، والذي ورد فيه بابا خامسا حول "المسؤولية وحق الرد والتصحيح"، تهدف مواده (من المادة 62 إلى المادة 67) إلى ترسيخ دعائم الشفافية في المشهد الإعلامي؛ فهو يلزم مديري النشر والصحفيين بتحمل مسؤولية ما يتم نشره[1]، ويمنح الأفراد والهيئات التي قد تتأثر سلبا بالمعلومات المنشورة، الحق القانوني في تقديم ردودهم وتصحيح الأخطاء. وهو ما يعني أن هذه المواد تضمن حق الجمهور في الحصول على معلومات دقيقة، وتقي من انتشار الأخبار المضللة التي قد تضر بالمصالح الفردية والعامة.

كما قد أعلن وزير الاتصال محمد مزيان عن إعداد خطة لمواجهة "الأخبار المضللة" التي تستهدف الأمن القومي، وذلك خلال اجتماع "مكتب التنسيق الأمني لشمال إفريقيا" المخصص لتداعيات المعلومات المضللة على أمن واستقرار الدول الإفريقية. وأوضح الوزير أن هنالك توجه لتعزيز التشريعات الوطنية لمكافحة التضليل الإعلامي والأخبار الزائفة التي تستهدف الأمن الوطني، مؤكدا أن محاربة الأخبار الزائفة "معركة مشتركة" تستوجب التنسيق بين الدول الإفريقية وتبادلا فعالا للمعلومات بين الأجهزة الأمنية والإعلامية[2].

وفي إطار سعي وزارة الاتصال لمواجهة التهديدات السيبرانية، تتولى مديرية التطوير مهمة تأمين البنية التحتية الرقمية من خلال تطبيق تقنيات كجدار النار (الحماية)، وشهادات تأمين المواقع SSL. أما فيما يتعلق بمواجهة البوتات الاجتماعية التي تروج للأخبار الزائفة؛ فإن الوزارة تعتمد استراتيجية تتسم بالوضوح والشفافية من خلال إصدار بيانات رسمية عبر حساباتها الموثقة وموقعها الإلكتروني الرسمي، لدحض الادعاءات وتزويد المواطنين بالمعلومات الصحيحة وتعزيز الوعي العام[3].

[1] المادة 62 من القانون رقم 23-14 المؤرخ في 2 ديسمبر 2023، الجريدة الرسمية ع77 (2ديسمبر 2023)، ص10.

[2] "الجزائر تعد خطة للتصدي للأخبار المضللة"، الشرق الأوسط صحيفة العرب الأولى، تاريخ المقال: 21 أفريل 2025، تاريخ الاطلاع: 16 ماي 2025.

https://2u.pw/LuOPR

[3] عبد القادر علان، مدير التطوير بوزارة الاتصال، مقابلة شخصية، وزارة الاتصال، 2025/05/08، ص 1-2.

بينما تضع وزارة البريد والمواصلات السلكية واللاسلكية استراتيجية شاملة لمجتمع المعلومات*، وذلك من خلال تنفيذ الإجراءات التالية:

1. **تطوير المحتوى والخدمات عبر الانترنت، و انترنت الأشياء (Iot):** يهدف هذا المحور إلى توفير البنية التحتية اللازمة للإنترنت من خلال:
   - توسيع وتحسين عناوين الإنترنت.
   - وضع سياسة وطنية لتخصيص معرفات هوية الأشياء (OID).
   - وضع الإطار المعياري المتعلق بمجتمع المعلومات.
   - ضمان التكامل بين أنظمة معلومات القطاع[1].
2. **الأمن السيبراني والمرونة وبيئة الثقة:** لضمان سلامة ومرونة البنية التحتية للاتصالات والمساهمة في بناء بيئة ثقة في استخدام تكنولوجيا المعلومات والاتصالات، تسعى الوزارة إلى:
   - إنشاء مركز قطاعي للرصد والإنذار والاستجابة للحوادث المعلوماتية، في إطار التعاون مع جمهورية كوريا الجنوبية.
   - تطبيق المرجع الوطني لأمن المعلومات في المؤسسات والهيئات التابعة للقطاع،
   - تنظيم تمارين لإدارة الأزمات السيبرانية لتقييم الجاهزية والاستجابة للحوادث.
   - وضع خريطة للمخاطر المتعلقة بأنظمة معلومات القطاع لتقييم تأثير الحوادث وتحديد الإجراءات الأمنية اللازمة[2].

بالتالي، تعد وزارة البريد والمواصلات السلكية واللاسلكية جهة فاعلة رئيسية، تعمل على نحو استباقي من أجل تعزيز الأمن السيبراني وخلق بيئة رقمية آمنة وموثوقة للمواطنين والقطاعات المختلفة، مما يدعم مسار التحول الرقمي في البلاد. كما تلتزم الوزارة بمكافحة انتشار المعلومات المضللة والتأثيرات المغرضة التي قد تستغل الفضاء السيبراني لزعزعة الثقة والوعي العام.

* يعرف الاتحاد الدولي للاتصالات مجتمع المعلومات على أنه مجتمع يستطيع كل فرد فيه استحداث المعلومات والمعارف، والنفاذ إليها واستخدامها وتقاسمها، ويتمكن من تسخير كامل إمكاناتهم للنهوض بتنميتهم المستدامة ولتحسين نوعية حياتهم وذلك انطلاقا من مقاصد ومبادئ ميثاق الأمم المتحدة.

[1] "استراتيجيتنا في مجال مجتمع المعلومات"، وزارة البريد والمواصلات السلكية واللاسلكية، تاريخ الاطلاع: 2025/05/15.

https://2upw/igWZj

[2] المرجع نفسه.

الفرع الثاني: تعزيز قدرات الأجهزة الأمنية لمواجهة التضليل السيبراني

انطلاقا من تصريحات العميد رشيد فتحي موساوي، المدير العام للوثائق والأمن الخارجي ورئيس إقليم شمال إفريقيا للجنة أجهزة الاستخبارات والأمن الإفريقية 'سيسا' (CISSA)، فإن الجزائر تضع مكافحة المعلومات المضللة في صميم جهودها لحماية استقرارها الوطني، واستقرار القارة الإفريقية عموما. إذ أكدت الجزائر، باستضافتها لأشغال ورشة إقليمية بعنوان: "المعلومات المضللة والأخبار الزائفة وتداعياتها على أمن واستقرار الدول"، على إدراكها التام للخطر الوجودي لهذه المعركة التي أصبحت تتعدى حدود الإعلام، لتمثل تهديدا مباشرا لسيادة الدول ووحدتها[1].

ولمواجهة هذا التهديد الأمني، تتكامل جهود الأجهزة الأمنية الجزائرية، من قيادة وزارة الدفاع وجهاز المخابرات إلى مصالح المديرية العامة للأمن الوطني، ضمن رؤية استراتيجية وتفكير استباقي لمواجهة هذه الحرب السيبرانية التي تستهدف في المقام الأول صورة الجزائر ومؤسساتها ورموزها[2].

ففي سياق مسؤوليتها لحماية الأمن القومي والوحدة الوطنية، تضطلع وزارة الدفاع الوطني بدور محوري في مواجهة الدعاية التي تستهدف القضايا الحساسة. وهو ما أكده الفريق أول السعيد شنقريحة خلال زيارة عمل وتفقد إلى الناحية العسكرية الرابعة أين أكد على: "ضرورة التصدي للاستخدام الخطير الدعاية الهدامة والمضللة في ظل التطور الهائل لتكنولوجيات الاتصال ووسائل التواصل الاجتماعي والمنصات الرقمية، فالأخبار الكاذبة والتلاعب بالمعلومات، أصبحت أسلحة فتاكة تستخدم لتحقيق أهداف سياسية مشبوهة"[3]. كما دعا لمواجهة هذه الحروب السيبرانية والإعلامية، من خلال تعزيز الوعي الأمني واليقظة الوطنية، إلى جانب تأسيس ثقافة إعلامية وطنية صلبة، تستند إلى المصادر الموثوقة، وتقي من الانسياق وراء المحتوى المضلل.

من جهتها المخابرات الجزائرية، ممثلة في جهازيها الرئيسيين؛ المديرية العامة للوثائق والأمن الخارجي ومديرية الأمن الداخلي، تضطلع بدور مركزي في منظومة الأمن القومي الجزائري؛ إذ تعمل هذه الأجهزة كخط دفاع لرصد شتى التهديدات الهجينة التي تستهدف الاستقرار المؤسساتي والمجتمعي، وذلك من خلال اعتماد استراتيجيات استباقية للكشف عن حملات التضليل التي غالبا ما تكون مدعومة بتقنيات الذكاء الاصطناعي[4]، إلى جانب أتمتة التفاعل من خلال البوتات الاجتماعية لتضخيم الرسائل السلبية وتوجيه الرأي العام.

---

[1] "مواجهة المعلومات المضللة: الجزائر ستظل في طليعة المدافعين عن القارة الإفريقية"، الإذاعة الجزائرية، تاريخ المقال: 2025/04/20، تاريخ الاطلاع: 2025/05/16.
https://2u.pw/Uqu4v

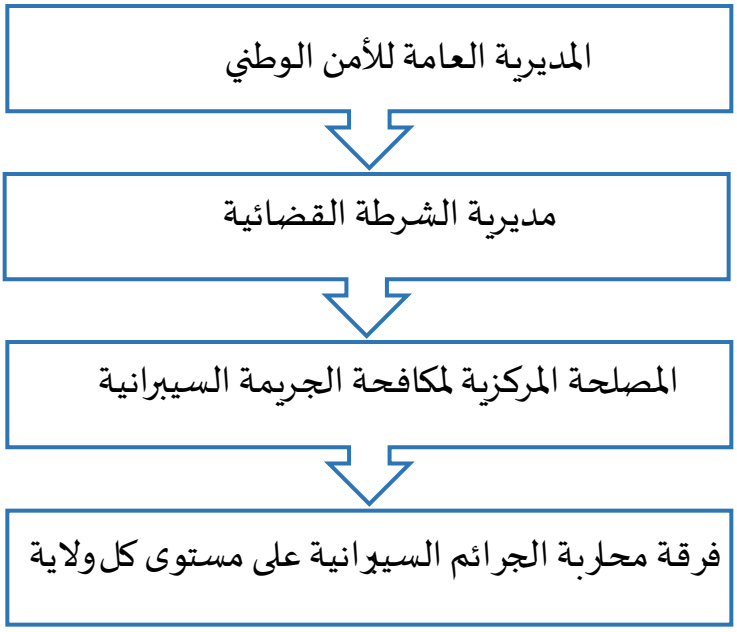
[2] "مؤسسات الجمهورية على خط واحد لمجابهة الدعاية المضللة"، موقع بوابة الجزائر، تاريخ المقال: 29 أفريل 2025، تاريخ الاطلاع: 2025/05/16.
https://2u.pw/QQRoG

[3] "الفريق الأول سعيد شنقريحة: ضرورة التصدي للاستخدام الخطير للدعاية الهدامة والمضللة"، الشروق نيوز، يوتيوب، نشرت في 28 أفريل 2025، من 0:00 -0:33.
https://2u.pw/dSSgc

[4] "مؤسسات الجمهورية على خط واحد لمجابهة الدعاية المضللة"، مرجع سابق.

أما بخصوص المديرية العامة للأمن الوطني فقد تبنت استراتيجية تقوم على التنسيق بين المصلحة المركزية لمكافحة الجرائم السيبرانية ومختلف فرق مكافحة الجرائم السيبرانية المتواجدة عبر كافة ولايات الوطن، وتتمتع الجزائر العاصمة بخصوصية وجود فصائل لمكافحة الجرائم السيبرانية على مستوى 13 دائرة[1].

شكل 10: الهيكل التنظيمي لمكافحة الجرائم السيبرانية ضمن المديرية العامة للأمن الوطني



المصدر: من إعداد الباحثة

ولمواجهة تهديد البوتات الاجتماعية، تختص الفرقة المركزية لليقظة ومعالجة التبليغات، التابعة للمصلحة المركزية لمكافحة الجريمة السيبرانية، بالمتابعة الدورية لشبكة الانترنت ولمحتويات مواقع التواصل الاجتماعي، بهدف رصد الأنشطة المشبوهة التي تستهدف المساس بالأمن الوطني وتحديد مصادرها، ثم إصدار محضر معاينة تقنية بخصوصها، لمباشرة الإجراءات القانونية[2].

أما على مستوى فرق مكافحة الجرائم السيبرانية، فتوجد ثلاث فصائل:

- **فصيلة اليقظة التكنولوجية:** هي الجهة المكلفة بمراقبة المحتوى الرقمي، ورصد أي أنشطة مشبوهة تحاول استهداف الأمن القومي الجزائري، عبر منصات التواصل الاجتماعي.
- **فصيلة المساعدات التقنية:** توكل إليها مهمة تحري لتحديد هوية مستعملي الحسابات المُجَرَمة إلى جانب تقديم المساعدات التقنية لمختلف المصالح.

[1] ضابط شرطة، مرجع سابق، ص1.
[2] محافظ شرطة، مرجع سابق، ص2.

- **فصيلة التحقيقات:** هي الجهة المسؤولة عن كشف الجرائم السيبرانية، وتحليل أدلتها الرقمية، وتتبع المجرمين في الفضاء السيبراني[1].

كما تجدر الإشارة إلى أن فرقة مكافحة الجرائم السيبرانية، فور رصدها لهجمات موجهة بالبوتات ضد وزارة أو هيئة حكومية، تقوم بإبلاغ الجهة المعنية بتفاصيل الهجوم وطبيعته. وعلى إثر ذلك، تتولى الجهة المستهدفة مسؤولية توضيح الحقائق للجمهور، وذلك بنشر المعلومات الصحيحة عبر صفحاتها الرسمية على مواقع التواصل الاجتماعي، لقطع الطريق أمام أي محاولات لتضليل الرأي العام[2].

بالتالي، فإن المديرية العامة للأمن الوطني، في مواجهتها للتهديدات السيبرانية عموما، وللتضليل عبر مواقع التواصل الاجتماعي بصفة خاصة، تعتمد على تنسيق بين المصلحة المركزية لمكافحة الجريمة السيبرانية التي تشرف على العمليات الوطنية والدولية، وبين الفرق الولائية لمكافحة الجرائم السيبرانية؛ التي تتولى التحقيقات المحلية وتحديد مصادر الهجمات، وكل ذلك يتم بتنسيق وثيق مع الهيئات الحكومية، لضمان تبادل سلس للمعلومات، يعزز القدرة على التصدي لأي جهة تستهدف أمن الجزائر ومؤسساتها ورموزها.

لكن تجدر الإشارة إلى أنه وبحكم طبيعة التهديدات السيبرانية العابرة للحدود، فإن قواعد تسليم المجرمين السيبرانيين الدوليين، تفرض عقبات أمام الأجهزة الأمنية الجزائرية؛ فعلى سبيل المثال وفي حال ثبت أن مصدر هجمة منسقة بالبوتات من أطراف أجنبية، فإن مجرى التحقيق وتسليم المجرم يبقى مرهونا بموافقة الدولة التي يتواجد بها.

الفرع الثالث: وكالة الأنباء الجزائرية والمواجهة الإعلامية للبوتات الاجتماعية

1. نبذة عن وكالة الأنباء الجزائرية:

تعد وكالة الأنباء الجزائرية (وأج) المؤسسة الإعلامية الوطنية الرسمية الرائدة في الجزائر، لما لها من دور في نقل الأخبار وتشكيل المشهد الإعلامي في البلاد، وتعتبر الوكالة المصدر الأساسي للأخبار الموثوقة، حيث تقوم بجمع الأخبار من شبكة واسعة من المراسلين والمصادر المحلية والدولية، ثم تعالجها وتوزعها على مختلف وسائل الإعلام والجمهور. تم إنشاء وكالة الأنباء الجزائرية في 01 ديسمبر 1961 بتونس، بهدف نشر بيانات جيش وجبهة التحرير الوطنيين إبان الثورة التحريرية، وبعد الاستقلال تم نقل مقرها بشكل طبيعي إلى الجزائر العاصمة أين استأنفت عملها بشكل كامل في أواخر 1962[3]، وقد مرت الوكالة بعدة مراحل تؤرخ لتطورها ما جعلها واحدة من أهم المؤسسات الإعلامية في الجزائر.

[1] ضابط شرطة، ص3.

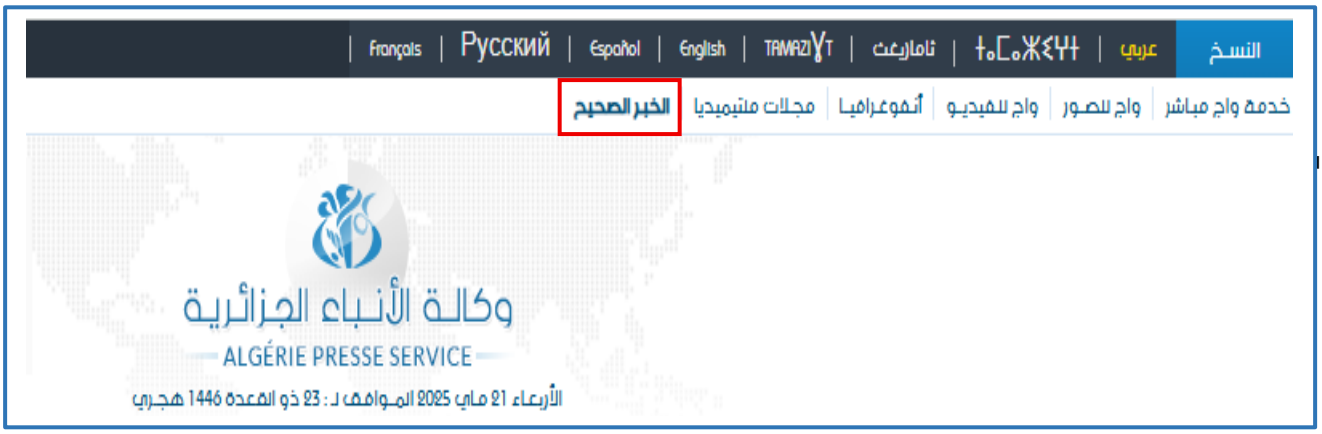
[2] المرجع نفسه.

[3] باديس سعودي، "وكالات الأنباء بين الخضوع لهيمنة الدولة والاستقلالية: دراسة حالة في الجزائر والمغرب"، مجلة العلوم الإنسانية لجامعة أم البواقي، م8، ع3 (ديسمبر 2021)، ص.ص 70-82.

2. استراتيجيات وكالة الأنباء الجزائرية في مواجهة التضليل السيبراني:

- **تعزيز البنية المعلوماتية للوكالة:** وذلك من خلال اعتماد شبكة واسعة من المراسلين، واستخدام أنظمة تكنولوجية حديثة، لجمع الأخبار ومعالجتها[1]، وصولا إلى نشرها عبر مختلف المواقع والمنصات الرقمية؛ وهو ما يعكس حرص الوكالة على توفير تغطية شاملة للأحداث لتقليل الاعتماد على المصادر غير الموثوقة.
- **استحداث قسم اليقظة الإعلامية:** الذي يعمل كوحدة متخصصة تراقب وتدقق بعناية المحتويات الإعلامية المشبوهة التي تستهدف أمن الجزائر واستقرارها، حيث يقوم بفحص وتحليل هذه المواد لكشف الجهات الفاعلة، ليقوم في نهاية المطاف بإصدار بيانات رسمية توضح حقيقية هذه الأخبار لتؤكد أنها زائفة بهدف توعية الجمهور ووقايته من الأكاذيب التي تهدد أمن البلاد[2].
- **تفعيل نافذة "الخبر الصحيح" على الموقع الرسمي للوكالة:** تهدف هذه النافذة إلى أن تكون مرجعا موثوقا للجمهور للتحقق من صحة الأخبار المتداولة، إذ تعمل وفق آلية جمع الأخبار الكاذبة، ثم إحالتها إلى الجهات الرسمية المعنية ذات العلاقة بمضمون الخبر، لتقوم في الأخير بالتصحيح الرسمي بشكل واضح ومدعوم بالمصادر.

شكل 11: نافذة "الخبر الصحيح" على موقع وكالة الأنباء الجزائرية



- **اعتماد مواقع الذكاء الاصطناعي:** من خلال دفع اشتراكات الذكاء الاصطناعي المتخصصة في كشف التضليل في المحتويات الإعلامية والرقمية، ومن ضمن المواقع التي تعتمدها:

[1] عبد القادر دربدي، "تاريخ الإعلام الوكالاتي في الجزائر من خلال وكالة الأنباء الجزائرية"، مجلة الساورة للدراسات الإنسانية والاجتماعية، م7، ع1 (2021)، ص.ص 231-250.

[2] عمار القامة، مستشار المدير العام لوكالة الأنباء، مقابلة شخصية، وكالة الأنباء الجزائرية: 2025/05/07، ص1.

تطبيق Feedly: هو منصة تجميع أخبار (News Aggregator) تتيح للمستخدمين تنظيم ومتابعة مصادر الأخبار حسب اهتمامات الشخص في مكان واحد، ويمكنهم من إضافة مواقع إخبارية، يوتيوب، وملفات بودكاست، وموجزات وغيرها من المصادر[1].

موقع Who is: هو أداة على انترنت، مخصصة لمعرفة معلومات أساسية عن أي موقع ويب، مثل مالكه، مصدره، ومتى تم إنشاؤه.

أداة IN vid: والتي تعتبر أداة للكشف عن جوانب التضليل في المحتوى المرئي، من خلال تحليل مقاطع الفيديو، وتحديد الموقع الجغرافي، وفحص التفاصيل الدقيقة للصورة، مما يساعد على فهم السياق الزماني والمكاني، وصولا إلى تحديد المقاطع المفبركة[2].

هذا ما يعني أن وكالة الأنباء الجزائرية، باعتبارها ركيزة أساسية للإعلام الرسمي، تؤكد التزامها بتطوير قدراتها البشرية والتقنية، في إطار استراتيجية مضادة لأي تضليل أو معلومات مغلوطة تستهدف الجزائر ومؤسساتها، بما يضمن تدفقا مستمرا للحقائق ويعزز الوعي العام.

لكن على الرغم من الدور الذي تلعبه إلا أن الوكالة تفتقد لآليات واضحة وأقسام متخصصة تتكلف بمواجهة التضليل السيبراني عبر منصات التواصل الاجتماعي، ذلك أنها طرحت فكرة مشروع لليقظة التكنولوجية، الذي يقوم على التنسيق بين الوزارات ووكالة الأنباء لمعالجة الأخبار الرقمية المضللة، إلا أن المشروع لم يكلل بالتنفيذ نظرا لنقص الموارد المادية والبشرية.

[1] علاء شهايب، "فيدلي: أداة جديدة في خدمة الصحفيين"، موقع Ijnet، تاريخ المقال: 30 أكتوبر 2018، تاريخ الاطلاع: 2025/05/15.
https://2u.pw/CheND

[2] أسماء قنديل، "دليلك لاستخدام أداة Invid في التحقق من صحة الصور والفيديوهات، موقع Ijnet، تاريخ المقال: 28 جوان 2024، تاريخ الاطلاع: 2025/05/15.
https://2u.pw/02GcacS

المطلب الثاني: مدى الوعي المجتمعي اتجاه تهديدات البوتات الاجتماعية

يأتي هذا الاستبيان في إطار بحث أكاديمي يهدف إلى دراسة تأثير البوتات الاجتماعية على الرأي العام والحياة السياسية والاجتماعية في الجزائر، وذلك كجزء من إنجاز مذكرة تخرج لنيل شهادة الماستر في تخصص "علاقات دولية". يهدف المطلب إلى فهم مستوى الوعي المجتمعي حول البوتات الاجتماعية، وكيفية تعامل الأفراد معها، بالإضافة إلى تقييم دورها في تشكيل الرأي العام والتأثير على القضايا الوطنية مثل السياسة والأمن والاقتصاد.

الفرع الأول: الإطار المنهجي للدراسة الميدانية

في هذا الفرع، سنتناول التعريف بمجتمع وعينة الدراسة، وأداة جمع البيانات. بداية باختيار منهجية الدراسة الذي يعتمد على طبيعة الموضوع المستهدف وأهدافه. حيث يعرف المنهج بأنه الطريقة التي يتبعها الباحث في استقصاء الحقيقة والإجابة على الأسئلة التي يطرحها البحث. بناء على ذلك، اعتمدنا على مجموعة من الإجراءات البحثية التي تتكامل لوصف الظاهرة من خلال جمع وتصنيف وتحليل البيانات بشكل دقيق لاستخلاص دلالات محددة والوصول إلى استنتاجات وتعميمات حول الظاهرة المدروسة.

- ✓ **مجتمع البحث:**

تكون مجتمع الدراسة من فئات متنوعة تشمل:

- الأساتذة الجامعيين (لخبرتهم الأكاديمية وتحليلهم النقدي).
- الطلبة (كمستخدمين نشطين لوسائل التوال الاجتماعي).
- الموظفين والعاملين (كممثلين للقطاع المهني المتأثر بالسياسات الرقمية).
- أفراد من فئات أخرى لضمان تنوع الآراء (مثل الحرفيين والعاطلين عن العمل).

- ✓ **معايير اختيار العينة:**

- التنوع الديمغرافي: حرصت على تشمل العينة توزيعا متوازنا من حيث: الجنس (ذكور/إناث)، الفئة العمرية (من أقل من 18 سنة إلى أكثر من 50 سنة) والمستوى التعليمي (من غير متعلمين إلى حاملي شهادات عليا).
- المعيار الرئيسي – المعرفة المسبقة بالبوتات الاجتماعية: تم توزيع 200 استبيان، ثم تم تصفية العينة لتركيز التحليل على الأفراد الذين لديهم وعي مسبق بالبوتات، حيث أن الهدف هو تقييم تأثيرها وليس قياس الانتشار العام. حيث تم اعتماد 80 استبيانا (40% من العينة الكلية) ممن أجابوا بـ "نعم" على سؤال: "هل سمعت من قبل عن البوتات الاجتماعية؟"

- طريقة جمع البيانات: تم توزيع الاستبيان عبر:

الوسائل المباشرة (مقابلات مع أساتذة وطلبة في المدرسة والجامعة)، والكترونيا (نشر الاستبيان في منصات التواصل الاجتماعي والبريد الإلكتروني).

✓ **تبرير منهجية الاختيار:**

- التركيز على العينة الواعية: يعكس اختيار الأفراد المدركين للبوتات قدرة على تحليل تأثيرها بدقة، بدلا من تضمين آراء غير مبنية على معرفة.
- ضمان الصلاحية العلمية: استبعاد المشاركين الذين لم يسمعوا بالبوتات يقلل من التحيز في النتائج، إذ أن آراءهم قد تكون غير مستنيرة بموضوع البحث.

باختيار هذه العينة، سعيت إلى تحقيق توازن بين الشمولية والدقة، مع التركيز على الفئات القادرة على تقديم تحليل واعٍ لتأثير البوتات الاجتماعية. هذه المنهجية تخدم أهداف البحث في تقييم الوعي والمخاطر المحتملة، وتوفر أساسًا لمقترحات عملية لمواجهة هذه الظاهرة في السياق الجزائري.

✓ **أداة الدراسة (الاستبيان):**

أداة الدراسة هي الاستبيان (Questionnaire) وهو أحد أدوات جمع البيانات الكمية والنوعية، حيث يتكون من مجموعة من الأسئلة المعدة مسبقا لقياس آراء أو معارف أو سلوكيات العينة تجاه ظاهرة محددة، وهي في هذه الحالة **البوتات الاجتماعية وتأثيرها على الرأي العام في الجزائر**.

حيث تناول الاستبيان عدة محار رئيسية، منها:

- **مستوى الوعي حول البوتات الاجتماعية:** كيفية تعرف المشاركين عليها وتقييمهم لدورها.
- **التأثيرات السلبية المحتملة:** مثل نشر الأخبار الزائفة، التلاعب بالرأي العام، وتعزيز الانقسامات الاجتماعية.
- **الإطار المؤسسي والقانوني:** تقييم سياسات الجزائر في مواجهة التهديدات السيبرانية ومدى ثقة المواطنين في قدرة المؤسسات المختصة.
- **دور البوتات في النقاشات السياسية:** خاصة فيما يتعلق بالانتخابات والقرارات الوطنية.

وكانت الأسئلة المستخدمة متنوعة على الشكل التالي:

- **أسئلة مغلقة (اختيار من متعدد):** "مثل كيف تعرفت على البوتات الاجتماعية؟" (مع اختيار من متعدد).
- **أسئلة نعم/لا:** مثل "هل تعتقد أن البوتات تؤثر على استقرار المجتمع الجزائري؟"
- **أسئلة تقييمية (مقياس ليكرت):** مثل "ما مدى خطورة البوتات؟" (تهديد كبير/متوسط/ضئيل).
- **أسئلة مفتوحة محدودة:** مثل "ما الجوانب القانونية التي يجب تطويرها" (مع خيارات مسبقة + أخرى...).

حيث أن ما يميز الاستبيان المطروح من خلال الدراسة:

- **الشمولية** غطت جميع جوانب البحث (الوعي، التأثير، الإطار القانوني).
- **الوضوح** استخدام لغة بسيطة وتجنب المصطلحات المعقدة.
- **السرية** تأكيد سرية البيانات لضمان صدق الإجابات.
- **التنظيم** تسلسل منطقي من الأسئلة العامة إلى الخاصة.

من خلال هذا الاستبيان، نسعى إلى جمع آراء متنوعة تساعد في تحليل واقع البوتات الاجتماعية وتأثيرها على المجتمع الجزائري، مع تقديم توصيات قد تساهم في تعزيز الوعي ومواجهة التحديات المرتبطة بها. حيث كان أداة مناسبة لتحقيق أهداف البحث، جمع بين الكمي (تحليل النسب المئوية للإجابات) والنوعي (فهم الآراء العميقة)، مع مراعاة التنوع الديموغرافي وتركيز التحليل على العينة الواعية بالظاهرة.

الفرع الثاني: صدق وثبات أداة البحث و اتباعها للتوزيع الطبيعي

لضمان جودة البيانات وموثوقية النتائج، خضعت أداة الدراسة لاختبارات دقيقة لقياس **الصدق والثبات**، حيث تم التحقق من صدق المحتوى من خلال مراجعة الخبراء، وقياس الثبات باستخدام معامل ألفا كرونباخ. كما تم اختبار توزيع البيانات للتأكد من مطابقها **للتوزيع الطبيعي** باستخدام الاختبارات الإحصائية المناسبة، وذلك لضمان صلاحية تطبيق الأساليب الإحصائية المستخدمة في التحليل.

1. ثبات الاستبيان:

يقصد بثبات الاستبيان الاستقرار في النتائج وعدم تغيرها بشكل كبير لو تم إعادة تطبيقها على نفس أفراد العينة عدة مرات وفي نفس الظروف والشروط خلال فترة زمنية معينة، ولقياس مدى ثبان أداة الدراسة (الاستبيان) استخدامنا معامل ألفا كرونباخ Cronbach Alpha، وتتراوح قيم هذا المعامل ما بين 0 و1، وأصغر قيمة مقبولة هي 0.7، والجدول رقم () يوضح معاملات ثبات أداة الدراسة.

جدول 5: معامل ألفا كرونباخ لقياس ثبات أداة الدراسة

Statistiques de fiabilité

Alpha de Cronbach	Nombre d'éléments
,900	38

المصدر: من إعداد الباحثة بالاعتماد عل مخرجات SPSS V 23

تم التحقق من ثبات الاستبيان باستخدام معامل ألفا كرونباخ حيث بلغت قيمته (0.900) وهي أكبر من القيمة المقبولة (0.70)، مما يشير إلى درجة ثبات ممتازة واتساق داخلي عالٍ بين بنود الأداة، ويعكس موثوقية كبيرة في قياس الظاهرة

المدروسة، مع التأكيد على أن هذه النتيجة لا تغني عن ضرورة التحقق من صدق الأداة بشكل منفصل لضمان قدرتها على قياس الهد البحثي بدقة.

2. **صدق الاستبيان:** يقصد بصدق أداة الدراسة، أن تقيس عبارات الاستبيان ما وضعت لقياسه في الأصل، حيث اعتمدنا لقياس صدق الاستبيان على طريقتين: الصدق الظاهري والصدق البنائي.

✓ **الصدق الظاهري:**

ويقوم على فكرة مدى مناسبة عبارات الاستبيان لما يقيس ولمن يطبق عليهم ومدى علاقتها بالاستبيان ككل، ومن هذا المنطلق يتم عرض الاستبيان في صورته الأولية على عدد من المحكمين من ذوي الخبرة والاختصاص (مجموعة من الأساتذة الجامعيين بما فيهم المؤطر) للحكم على صلاحيتها في قياس الخاصية المراد قياسها، ولأخذ وجهات نظرهم و الاستفادة من آرائهم في تعديله والتحقق من مدى ملائمة كل عبارة للمحور الذي ينتمي إليه، ومدى سلامة ودقة الصياغة اللغوية والعلمية لعبارات الاستبيان ووضوحها، ومدى شمول الاستبيان لمشكلة الدراسة وتحقيق أهدافها، وفي ضوء أراء الخبراء والمحكمين تتم إعادة وتعديل صياغة بعض الفقرات، وحذف وإضافة فقرات أخرى لتحسين أداة الدراسة.

✓ **الصدق البنائي:**

يعتبر صدق الاتساق البنائي أحد مقاييس صدق أداة الدراسة، حيث يقيس مدى تحقق الأهداف التي تسعى الأداة الوصول إليها، ويبين صدق الاتساق البنائي مدى ارتباط كل محور من محاور أداة الدراسة بالدرجة الكلية لفقرات الاستبيان مجتمعة.

قمنا بإجراء اختبار الصدق البنائي لأداة الدراسة عن طريق حساب معاملات الارتباط بيرسون بين كل بعد من أبعاد المتغير والمتغير نفسه، فإذا كان معامل الارتباط قويا ومعنوي نقول أن الاستبيان يتمتع بدرجة عالية من الصدق البنائي، والجدول التالي يوضح ذلك:

جدول 6: اختبار الصدق البنائي – معاملات الارتباط بيرسون بين محاور الاستبيان والاستبيان ككل

Corrélations

		مستوى_الوعي	تقييم_التهديد	السياسات_الجزائرية	الرأي_العام_الوعي	الاستبيان_ككل
مستوى_الوعي	Corrélation de Pearson	1	,220*	,151	,229*	,841**
	Sig. (bilatérale)		,050	,180	,041	,000
	N	80	80	80	80	80
تقييم_التهديد	Corrélation de Pearson	,220*	1	,168	,391**	,773**
	Sig. (bilatérale)	,050		,136	,000	,000
	N	80	80	80	80	80
السياسات_الجزائرية	Corrélation de Pearson	,151	,168	1	,162	,872**
	Sig. (bilatérale)	,180	,136		,151	,000
	N	80	80	80	80	80
الرأي_العام_الوعي	Corrélation de Pearson	,229*	,391**	,162	1	,739**
	Sig. (bilatérale)	,041	,000	,151		,000
	N	80	80	80	80	80
الاستبيان_ككل	Corrélation de Pearson	,841**	,773**	,872**	,739**	1
	Sig. (bilatérale)	,000	,000	,000	,000	
	N	80	80	80	80	80

*. La corrélation est significative au niveau 0,05 (bilatéral).

**. La corrélation est significative au niveau 0,01 (bilatéral).

المصدر: من إعداد الباحثة بالاعتماد عل مخرجات SPSS V 23

كشفت نتائج اختبار الصدق البنائي باستخدام معامل ارتباط بيرسون عن وجود علاقات ارتباطية ذات دلالة إحصائية بين محاور الاستبيان الرئيسية، حيث أظهرت النتائج ارتباطًا موجبًا قويًا بين الاستبيان ككل وجميع المحاور (بين 0.739 و0.872) عند مستوى دلالة 0.01)، مما يشير إلى تماسك داخلي عالٍ واتساق بين الأبعاد المختلفة للأداة ومدى قدرتها على قياس الظاهرة المدروسة بشكل شامل، حيث سجل محور "تقييم التهديد" أعلى ارتباط بالاستبيان الكلي (0.872)، يليه محور "الرأي العام/الوعي" (0.841)، ثم "السياسات الجزائرية" (0.773)، وأخيرا "مستوى الوعي" (0.739)، وتؤكد هذه النتائج بشكل قاطع صلاحية الأداة وموثوقيتها في قياس البناء المفترض للظاهرة، وقدرتها على تحقيق الأهداف البحثية المرجوة.

3. اختبار التوزيع الطبيعي:

قبل الشروع في التحليل الإحصائي للبيانات، كان من الضروري التحقق من افتراض التوزيع الطبيعي للاستجابات، حيث يعد هذا الشرط الأساسي لتطبيق العديد من الأساليب الحائية البارامترية. ولذلك تم إجراء اختبارين متكاملين للتحقق من التوزيع الطبيعي، هما اختبار كولموجوروف – سميرنوف (Kolmogorov-Smirnov) واختبار شابيرو – ويلك (Shapiro-Wilk)، حيث يعد الأول أكثر ملاءمة للعينات الكبيرة نسبيا، بينما يعرف الثاني بحساسيته العالية في كشف الانحرافات عن الطبيعي خاصة مع العينات الغيرة والمتوسطة. جاءت هذه الخطوة التحليلية التمهيدية لضمان ملاءمة

الاختبارات الإحصائية المستخدمة لاحقا، ولتأكيد مدى تمثيلية العينة لمجتمع الدراسة، مما يعطي مصداقية أعلى للنتائج المتوصل إليها. نبين النتائج من خلال الجدول التالي:

جدول 7: اختبارات التوزيع الطبيعي

Tests de normalité

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistiques	ddl	Sig.	Statistiques	ddl	Sig.
الاستبيان_ككل	,111	80	,616	,954	80	,506

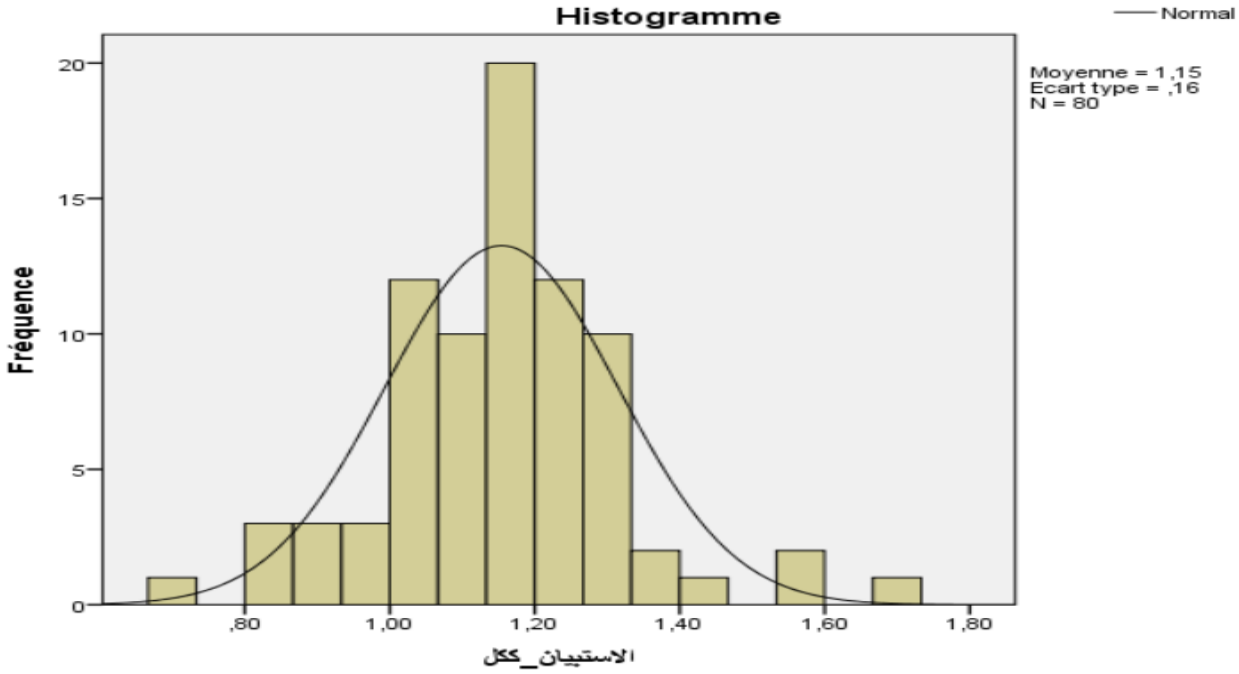
a. Correction de signification de Lilliefors

المصدر: من إعداد الباحثة بالاعتماد عل مخرجات SPSS V 23

أظهرت نتائج اختبارات التوزيع الطبيعي باستخدام كل من اختبار كولموجوروف – سميرنوف (Kolmogorov-Smirnov) واختبار شابيرو – ويلك (Shapiro-Wilk) أن بيانات الاستبيان تتبع التوزيع الطبيعي، حيث كانت قيمة مستوى الدلالة أكبر من 0.05 (0.616 لاختبار كولموجوروف – سميرنوف و0.506 لاختبار شابيرو – ويلك)، كما بلغت قيمة الاحصائية لشابيرو – ويلك (0.954) وهي قريبة من الواحد الصحيح، مما يؤكد عدم وجود انحراف كبير عن التوزيع الطبيعي، ويدعم صلاحية استخدام الأساليب الإحصائية البارامترية لتحليل البيانات، ويعزز مصداقية النتائج المستخلصة من الدراسة.

ويمكن لنا إدراج التمثيل البياني للاختبار الذي يؤكد هو الآخر على صحة النتائج السابقة الذكر لاختبار التوزيع الطبيعي.

شكل 12: التمثيل البياني للتوزيع الطبيعي



المصدر: من إعداد الباحثة بالاعتماد عل مخرجات SPSS V 23

يؤكد الهيستوجرام نتائج اختبارات التوزيع الطبيعي السابقة، حيث يظهر شكلاً جرسياً مقارباً للمنحنى الطبيعي مع تركيز واضح للبيانات حول المتوسط (1.15) وانحراف معياري مقبول (16)، مما يدعم تطابق البيانات مع افتراض التوزيع الطبيعي. يُلاحظ توافق هذه النتائج البصرية مع مؤشرات اختباري كولموجوروف – سميرنوف (0.616) واختبار شابيرو – ويلك (0.506)، حيث تؤكد جميع الأدلة معا غياب انحراف جوهري عن الطبيعي، مما يبرر استخدام الاختبارات البارامترية في التحليل اللاحق للبيانات.

الفرع الثالث: عرض وتحليل خصائص العينة

فيما يلي سنتناول دراسة خصائص المشاركين في عينة الدراسة وفقا للمتغيرات الشخصية والوظيفية.

✓ **الجنس:**

أظهرت نتائج توزيع العينة حسب متغير الجنس أن الإناث يشكلن الأغلبية بنسبة 56.3% (45 فردا) مقارنة بالذكور الذين مثلوا 43.8% (35 فردا) من إجمالي العينة البالغ 80 مشاركا. يلاحظ أن التوزيع يقترب من التوازن النسبي مع تفوق طفيف للإناث، مما يشير إلى تمثيل معقول لكلا الجنسين في العينة.

✓ **الفئة العمرية:**

توزيع العينة حسب الفئة العمرية يظهر تركيزا واضحا على الشباب، حيث مثلت فئة 18-25 سنة النسبة الأعلى (36.3%)، تليها فئة 26-35 سنة (26.3%)، بينما كانت الفئات العمرية الأكبر (36-50 سنة وما فوق) أقل تمثيلا. هذا التوزيع يعكس طبيعة مجتمع الدراسة واهتماماته الرقمية، مع ملاحظة تمثيل معقول لجميع الفئات العمرية الأساسية في التحليل.

✓ **المستوى التعليمي:**

يظهر توزيع المستوى التعليمي للعينة هيمنة واضحة للحاصلين على التعليم الجامعي (78.8%)، يليهم حمل الدراسات العليا (18.8%)، بينما مثل مستوى ثانوي نسبة ضئيلة (2.5%). هذا التركيز العالي على المؤهلين أكاديميا يعكس ملائمة العينة لدراسة ظاهرة البوتات الاجتماعية التي تتطلب وعيا تقنيا ومعرفيا، ويؤكد قدرة المشاركين على تقديم إجابات مدروسة حول الموضوع، مع الإشارة إلى محدودية تمثيل الشرائح الأقل تعليما في النتائج.

✓ **الوظيفة/المهنة:**

يظهر توزيع العينة حسب المهنة هيمنة الموظفين (52.5%) والطلاب (32.5%)، بينما مثل الأساتذة الجامعيون والعاطلون عن العمل نسبًا ضئيلة (8.8% و5% على التوالي). هذا التوزيع يعكس طبيعة العينة المستهدفة في دراسة البوتات الاجتماعية، حيث يعتبر الموظفون والطلاب الفئات الأكثر تفاعلا مع المنصات الرقمية، مع ملاحظة محدودية تمثيل المهن الأخرى التي قد تقدم منظورا مختلفا للظاهرة المدروسة.

1. عرض وتحليل نتائج الدراسة:

تجدر الإشارة هنا إلى أن التفصيل سيكون لأغلبية للإجابات التي لها صلة مباشرة مع مدى وجود وعي مجتمعي اتجاه البوتات الاجتماعية.

✓ **كيف تعرفت على البوتات الاجتماعية؟**

أظهرت تحليل مستوى الوعي بالبوتات الاجتماعية أن 40% من المشاركين تعرفوا عليها عبر الانترنت ووسائل التواصل الاجتماعي، بينما ذكر 25% أنهم سمعوا بها من خلال الأخبار والتقارير الإعلامية. كما أفاد 20% أنهم تعرفوا عليها عبر الأصدقاء والزملاء، بينما نسب 15% معرفتهم بها إلى الدراسات الأكاديمية والمحاضرات. هذه النتائج تكشف أن المنصات الرقمية تمثل القناة الرئيسية لتوعية بهذه الظاهرة، مع دور ملحوظ للمصادر التقليدية كالإعلام والشبكات الاجتماعية. ويعكس هذا التوزيع طبيعة انتشار الظاهرة الرقمية وطرق تداول المعلومات في العصر الحديث.

✓ **كيف تصف البوتات الاجتماعية بناء على معرفتك بها؟**

أظهرت النتائج تباينا في تصورات المشاركين حول البوتات الاجتماعية، حيث وصفها 45% بأنها "برامج للتفاعل الآلي"، بينما رآها 30% كـ "حسابات وهمية"، واعتبر 15% أنها "أدوات لتحسين الخدمات الرقمية"، في حين أفاد 10% بعدم امتلاكهم معرفة دقيقة. هذه التصورات المختلفة تعكس تعدد جوانب الظاهرة وتأثر الفهم بمدى التعرض لها، حيث يبدو أن الغالبية تدرك الطبيعة الآلية للبوتات، بينما تبرز أقلية بتطبيقاتها الإيجابية في تحسين الخدمات.

✓ **هل تعتقد أن البوتات الاجتماعية تستخدم لأغراض سيئة مثل التلاعب بالرأي العام أو نشر الأخبار الزائفة؟**

أظهرت النتائج أن 65% من المشاركين يعتقدون أن البوتات الاجتماعية تستخدم لأغراض سيئة مثل التلاعب بالرأي العام ونشر الأخبار الزائفة، بينما لم يكن 25% على يقين من ذلك، في حين رأى 10% أنها لا تستخدم لهذه الأغراض. هذه النتائج تكشف عن وجود قلق واسع بين أفراد العينة حول الاستغلال السلبي للبوتات، مما يعكس وعيا ملحوظا بمخاطرها المحتملة على النقاش العام وانتشار المعلومات، مع وجود شريحة لا تزال غير مدركة لهذه التهديدات.

✓ **إلى أي مدى تعتبر البوتات الاجتماعية تهديدا للحياة العامة؟**

أظهرت النتائج أن 45% من المشاركين يرون البوتات الاجتماعية تهديدا متوسطا للحياة العامة، بينما اعتبرها 35% تهديدا كبيرا، مما يشير إلى إدراك واسع لمخاطرها المحتملة مع تفاوت في تقدير مستوى الخطورة، بالمقابل اعتبر 15% أنها تشكل تهديدا ضئيلا، في حين لم يرها 5% تهديدا على الإطلاق، ويعكس هذا التباين اختلاف التجارب والخلفيات المعرفية للمشاركين حول تأثير البوتات، حيث يبدو أن الغالبية تدرك وجود التهديد دون أن تبالغ في تقدير حجمه، بينما تظهر أقلية أكثر تحفظا على تأثيرها السلبي. هذه النتائج تؤكد الحاجة إلى مزيد من الدراسات لفهم طبيعة هذا التهديد الرقمي وآليات الحد من آثاره.

✓ **في رأيك ما هي أخطر استخدامات البوتات الاجتماعية؟ (اختر جميع الخيارات المناسبة).**

أظهرت النتائج أن 60% من المشاركين يرون أن أخطر استخدام للبوتات الاجتماعية هو نشر الأخبار الزائفة، بينما اعتبر 30% أن التلاعب بالانتخابات والقرارات السياسية هو الأكثر خطورة، وذهب 25% إلى تعزيز خطاب الكراهية والانقسامات الاجتماعية يمثل التهديد الأكبر. هذه النسب تعكس وعيًا واضحًا لدى العينة بالمخاطر الرئيسية للبوتات، خاصة في مجال التضليل الإعلامي وتأثيرها السلبي على الاستقرار السياسي والاجتماعي، مما يؤكد الحاجة الملحة لتعزيز آليات الرقابة والتوعية لمواجهة هذه التهديدات.

✓ **هل تعتقد أن البوتات الاجتماعية يمكن أن تؤثر على استقرار المجتمع الجزائري؟**

أظهرت النتائج أن 55% من المشاركين يرون أن البوتات الاجتماعية يمكن أن تؤثر على استقرار المجتمع الجزائري، بينما لم يوافق 7% على هذا الرأي، وأبدى 38% ترددهم بإجابة "لا أعلم". هذه النسب تكشف عن قناعة أكثر من نصف العينة بخطورة هذه الظاهرة الرقمية، مع وجود شريحة كبيرة غير متأكدة من تأثيرها، مما يشير إلى حاجة ملحة لتعزيز الوعي المجتمعي بآليات عمل البوتات ومخاطرها المحتملة على الأمن المجتمعي.

✓ **هل تعتقد أن البوتات الاجتماعية تؤثر على آرائك؟ إذا كانت إجابتك "نعم"، كيف ترى هذا التأثير؟**

أظهرت الإجابات على هذا السؤال أن ما يقارب نصف عدد المشاركين 47%، يرون أن البوتات الاجتماعية لا توثر على آرائهم، بينما أبدى 35% ترددهم بإجابة "ربما"، وأقل نسبة 17% فقط هم من يقرون بالتأثر، وعند سؤالهم عن انعكاس هذا التأثير، جاءت إجابة الشريحة الأكبر 37.8 % أن البوتات، تُقَلِل من ثقتهم بالمعلومات المتاحة. هذه النتائج تشير إلى أن المشاركين يميلون إلى الاعتقاد بعدم تأثر آرائهم بشكل جذري بالبوتات، لكنها قد تؤثر على ثقتهم في مصادر المعلومات.

✓ **هل تعتقد أن وسائل التواصل الاجتماعي عموما تؤثر على النقاشات حول القضايا الوطنية؟ وأيهما أكثر تأثيرا البوتات أم البشر؟**

أظهر تحليل مستوى تأثير وسائل التواصل الاجتماعي على النقاشات الوطنية أن أغلبية المشاركين81 % يقرون بتداعياتها على القضايا الوطنية، بينما لم يكن 17% على يقين من ذلك من خلال إجابتهم بـ"ربما"، في حين اعتبر 2 % أنها لا تؤثر، هذه النسب تعكس إدراكا واسعا لدور هذه الوسائل في تشكيل الرأي العام وتوجيه الحوارات حول الشؤون الداخلية للبلاد، وفي سياق سؤال آخر حول من يؤثر أكثر الحسابات البشرية أم البوتات أقر ما يقارب نصف عدد المبحوثين أن البوتات الاجتماعية أضحت تفوق الحسابات البشرية من ناحية التأثير في القضايا الوطنية.

✓ **في رأيك، ماهي أفضل طريقة لمكافحة تأثير البوتات الاجتماعية السلبي؟ (اختر جميع الخيارات المناسبة)**

أظهرت النتائج أن 69 % يجدون أن زيادة الوعي العام هي الحل للتصدي الفعال لتأثير البوتات الاجتماعية السلبي، في حين تحبذ فئة كبيرة تقارب 65 % الاستجابة القانونية، فيما ترى نسبة 48 % أن تمكين الأفراد بالمهارات اللازمة لتقييم

مصداقية المصادر أمرا بالغ الأهمية، بالتالي تعكس إجابات المبحوثين، أن الاستجابة للبوتات لا يمكن أن تكون محصورة على جانب واحد، وإنما تتطلب استراتيجية متكاملة الأبعاد (توعوية، قانونية، تعليمية).

- ✓ **هل تعتقد أن الجزائر تمتلك سياسات واضحة لمواجهة البوتات الاجتماعية؟**

أظهرت النتائج أن أكبر شريحة من المبحوثين 39 % لا تعلم ما إن كانت الجزائر تملك سياسات واضحة لمواجهة البوتات الاجتماعية، بينما كانت 31 % من الإجابات بـ"نعم"، تشير إلى وجود ثقة في السياسات الأمنية، ما يعكس أنهم قد يكونون على دراية ببعض المبادرات أو التصريحات الرسمية، وبنسبة مقاربة جاءت الإجابة بـ"لا" لتمثل 30% من إجمالي المشاركين؛ لتبين اعتقادا سائدا بأن الجهود القائمة غير كافية، أو غير فعالة في مواجهة هذه الظاهرة المعقدة.

- ✓ **ما مدى ثقتك في قدة الهيئات الجزائرية المختصة على التعامل مع التهديدات السيبرانية؟ وهل سمعت من قبل عن هيئات رسمية مختصة بالأمن السيبراني؟**

تراوحت غالبية الإجابات بين وجود ثقة "متوسطة إلى مرتفعة" مع فئة قليلة أبدت أن ثقتها ضعيفة ومنعدمة، وهو ما يعكس أن المبحوثين لهم نظرة إيجابية وحذرة في آن واحد، بشأن قدرة الهيئات الجزائرية في التعامل مع التهديدات السيبرانية، كما اختلفت درجة معرفة المبحوثين بهذه الهيئات، وتركزت معظم الإجابات حول معرفتهم لبعض الأجهزة الأمنية سواء التابعة لوزارة الدفاع الوطني أو مصالح الشرطة، تليها أيضا إجابات متكررة تذكر المدرسة الوطنية العليا للأمن السيبراني، كما اشتملت الإجابات على بعض الهيئات الحكومية كوزارة الاتصال، السلطة الوطنية لحماية البيانات ذات الطابع الشخصي ANPDP، والوكالة الوطنية لأمن نظم المعلومات، هذا إلى جانب بعض الإجابات التي حددت شركة "إلكترون كروب" كمؤسسة ناشئة مختصة في الأمن السيبراني.

- ✓ **في رأيك، هل يتمتع المواطن الجزائري بالوعي الكافي لتمييز البوتات والمعلومات المضللة؟**

أظهرت النتائج أن 49% من المشاركين، يعتبرون أن المواطن الجزائري لا يملك الوعي الكافي لتمييز البوتات والمعلومات المضللة، فيما أقرت نسبة 42% بمحدودية قدرته على التمييز، وصولا إلى أقل فئة 9% ترى أن المواطن الجزائري له القدرة على التمييز، هذه النسب تعكس على أن الوصول السهل لمنصات التواصل الاجتماعي لكافة شرائح المجتمع يزيد من احتمالية تحقيق البوتات لأغراضها التضليلية، ذلك أمام وجود فئات أقل وعيا يسهل استهدافها والتأثير على آرائها.

- ✓ **ما هي الوسائل التي تعتقد أنها الأهم لرفع الوعي حول البوتات الاجتماعية؟**

أظهرت النتائج أن وجود ميل مواضح لدور منصات التواصل الاجتماعي ذاتها في رفع الوعي حول البوتات وذلك بنسبة 42%، هذه النسبة نابعة من اعتبار المبحوثين أن منصات التواصل الاجتماعي وبحكم انتشارها الواسع وكونها مركز تواجد البوتات، لها المسؤولية المباشرة لتوفير حلول ناجعة لرفع الوعي العام. يلي ذلك وبنسبة 28 % إقرار بأهمية التعليم والمدارس والجامعات كاستثمار في المورد البشري لبناء النظرة النقدية لدى هذه الفئات، فيما أشار ربع المشاركين (25 %) إلى دور الحملات الإعلامية في رفع الوعي العام، وصولا إلى فئة 5 % كانت لهم آراء أخرى لم تشملها الخيارات الرئيسية.

✓ **هل تعتقد أن بعض الدول تستخدم البوتات الاجتماعية كجزء من حروب سيبرانية ضد الجزائر؟**

أظهرت النتائج أن هنالك احتمالية كبيرة أن بعض الدول تستخدم البوتات الاجتماعية كجزء من حرب سيبرانية موجهة ضد الجزائر، بحيث أن ما يزيد عن 74 % كانت اجابتهم "نعم"، ثم تأتي نسبة 23% ممن اختاروا "ربما" لتعكس حالة من عدم اليقين لكن دون استبعاد هذا الاحتمال، في حين أن نسبة ضئيلة جدا 3% هي التي نفت هذا الاستخدام. وهو ما يوحي بوجود قلق لدى فئة كبيرة من المشاركين بخصوص استغلال البوتات الاجتماعية ضد الجزائر.

✓ **ما مدى احتمالية أن تُستخدم البوتات الاجتماعية في إثارة الفتن أو النزاعات داخل الجزائر؟**

أظهرت النتائج عن وجود احتمالية كبيرة لاستخدام البوتات الاجتماعية في نشر خطابات الفتنة والعنف في الجزائر؛ فالجزء الأكبر من الاجابات (47% و36%)، يصف هذه الاحتمالية بأنها "عالية" أو "متوسطة"، في حين تتشكل النسب الأقل، ممن يرون أن هنالك احتمالية "منخفضة" أو "غير ممكنة". هذه النسب تستلزم النظر بجدية في الآثار المحتملة لهذه الظاهرة على الأمن المجتمعي الجزائري، ويدعو إلى اتخاذ إجراءات استباقية لمواجهة هذه التحديات.

بالتالي، يظهر من مجمل نتائج الاستبيان، أن نسب الوعي العام بالبوتات الاجتماعية منخفضة، ذلك أنه من عينة يبلغ عددها 200، تم تحديد 80 فقط من الإجابات لديهم معرفة مسبقة بالبوتات الاجتماعية أي ما يشكل 40 %. كذلك تبين من خلال التركيز على هذه العينة الواعية بمخاطر البوتات الاجتماعية أن المواطن الجزائري لا يملك الوعي الكافي لتمييز هذه الحسابات الآلية التي تستهدف القضايا الحساسة، وتغذي الانقسامات المجتمعية والنزاعات، هذا ما يستدعي تبني استراتيجية تركز الجوانب التوعوية بالدرجة الأولى، ذلك أن السياسات الأمنية مهما بلغت من تحكم تقني وقانوني ومؤسساتي، يبقى الوعي المجتمعي خط الدفاع الأول أمام التعقيدات التي تشهدها هذه الظاهرة.

المطلب الثالث: دور الوعي المجتمعي في مواجهة التضليل السيبراني

لم تعد مجابهة التهديدات السيبرانية حكرا على الأنظمة الدفاعية والتشريعات فقط؛ بل أصبحت تستلزم نهجا شاملا يرتكز على تعزيز الوعي المجتمعي، وذلك من خلال برامج تعليمية وتثقيفية متكاملة تمتد من المؤسسات التعليمية إلى كافة القطاعات، إلى جانب دور وسائل الإعلام في نشر الثقافة الأمنية الرقمية بين المواطنين[1]، إذ يمثل الوعي حصانة جماعية، ويبرز كهدف استراتيجي لمختلف المؤسسات الأمنية على غرار:

الفرع الأول: مكانة المؤسسات الأمنية في تعزيز الوعي المجتمعي

على سبيل المثال، اضطلعت المديرية العامة للأمن الوطني بمسؤولية تكثيف جهودها التوعوية لمجابهة تداعيات الجرائم السيبرانية التي أصبحت تشكل تهديدا للأمن الوطني، سيما عبر بث الأخبار المغلوطة، وترسيخ الأفكار السوداوية، والتحريض على سلوكيات منحرفة.

هذه الحملات التوعوية الشاملة تستهدف كافة شرائح المجتمع، مع إيلاء اهتمام خاص للفئات الأكثر عرضة للاستغلال السيبراني، مثل المراهقين، والشباب[2]. وتتجلى أبرز جهودها كالآتي:

- نشر محتوى توعوي عبر مختلف وسائل الإعلام التقليدية والرقمية، بما في ذلك المحطات الإذاعية والتلفزيونية، ومختلف المنصات الرقمية.
- استغلال منصات المديرية العامة للأمن الوطني الاتصالية الرقمية المتطورة بفعالية، مثل موقعها الرسمي وصفحاتها الرسمية، لضمان وصول رسائل الوعي بسرعة وفعالية إلى أوسع نطاق ممكن من الجمهور.
- التزام الشفافية الإعلامية في عرض قضايا الجرائم السيبرانية، كنهج يؤكد التزام الجزائر الصارم بالتصدي لكل من يحاول المساس بثوابت الدولة وأمنها واستقرارها.[3]

إلى جانب ذلك، تنظم المديرية العامة للأمن الوطني بانتظام ملتقيات توعوية متخصصة، بالتعاون مع الفاعلين في المجتمع المدني، والخبراء الأمنيين، والأكاديميين. وذلك بهدف:

- ✓ تعميق الوعي بمخاطر الجرائم المرتكبة عبر منصات التواصل الاجتماعي.
- ✓ تعزيز السلوكيات الإيجابية والقيم الأخلاقية الصحيحة لدى مستخدمي مواقع التواصل الاجتماعي.
- ✓ غرس قيم المواطنة، والمسؤولية لدى المواطن بأنه شريك فاعل في حمية ثوابت الدولة.

---

[1] أحمد الشرقاوي، "خبير أمن المعلومات: الوعي المجتمعي هو سلاح مواجهة الحروب التكنولوجية"، الوطن، تاريخ المقال: 12 فيفري 2025، تاريخ الاطلاع: 2025/05/21.
https://2u.pw/Uir7m

[2] العيشاوي مهدي، ضابط شرطة رئيسي، مقابلة شخصية، مكتب الإعلام والاتصال بأمن ولاية الجزائر 08-05-2025، ص2.

[3] المرجع نفسه، ص2.

- ✓ تكريس ثقافة التبليغ عن أي ممارسات مشبوهة أو تهديدات سيبرانية، انطلاقا من مبدأ أن "تحقيق الأمن هو مسؤولية جماعية لا فردية"[1].

وبالإضافة إل جهود التوعية المجتمعية، تسعى المديرية العامة للأمن الوطني لتكريس الوعي داخل الأجهزة الأمنية ذاتها، باعتبارها خط الدفاع الأول للوطن، وذلك من خلال:

- تنظيم دورات تكوينية لفائدة أفراد الشرطة، تركز على أحدث أساليب التضليل السيبراني وكشفه.
- إطلاع موظفي القطاع، أن أي تصرف حتى لو كان بسيطا أو غير مقصود، يعكس مباشرة صورة الدولة بأكملها وسمعتها على الصعيدين الداخلي والخارجي.
- توضيح أن أي ثغرة أمنية أو تصرف خاطئ، قد يتم استغلاله من قبل أطراف معادية، وقد يغذى باستخدام البوتات والحسابات الوهمية عبر الفضاءات الرقمية، ليتحول في وقت وجيز إلى قضية رأي عام، تهدد الأمن القومي وتزعزع الثقة في مؤسسات الدولة[2].

بالتالي، تركز مصالح المديرية العامة للأمن الوطني سعيها المتواصل على تعزيز اليقظة والحس النقدي للمجتمع الجزائري، بهدف مواجهة الهجمات التي تحاك ضمن الفضاءات السيبرانية، والتي تستهدف زعزعة استقرار البلاد وتهديد أمنها القومي.

كذلك من جهتها تعمل وزارة الدفاع الوطني وبالتنسيق مع المديرية العامة للأمن الوطني في إطار استراتيجية شاملة لتعزيز الوعي المجتمعي؛ وذلك من خلال تأطير برامج توعية مكثفة تستهدف مختلف شرائح المجتمع، تشمل محاضرات، ملتقيات، وورشات عمل لترسيخ ممارسات آمنة في العامل مع الفضاء السيبراني، وتنمية التفكير النقدي لدى الأفراد اتجاه محتويات المنصات الرقمية[3].

أما على الصعيد التنظيمي فتتولى مصلحة الدفاع السيبراني ومراقبة أمن الشبكات التابعة لدائرة الاستعلام والتحضير لأركان الجيش الوطني الشعبي، مهمة القيام بأنشطة تحسيسية لفائدة مستخدمي الجيش الوطني الشعبي، من خلال الاستفادة من دورات تكوينية والحصول على نشريات إخبارية بشكل منتظم للتعامل مع المخاطر السيبرانية الجديدة على النحو الأفضل[4].

[1] نصر الدين بويحي، "التوعية الأمني الدرع الواقي في مواجهة الإجرام السيبراني"، مجلة الشرطة ع 149 (أكتوبر 2021)، ص33.

[2] العيشاوي مهدي، مرجع سابق، ص2.

[3] محافظ شرطة، مرجع سابق، ص 1.

[4] شريف فضيل، "المخاطر السيبرانية أهمية التحسيس"، مجلة الجيش ع715 (فيفري 2023)، ص55.

الفرع الثاني: مكانة المؤسسات الاعلامية في تعزيز الوعي المجتمعي

وإلى جانب المؤسسات الأمنية، تبرز وسائل الإعلام كشريك أساسي في بناء الوعي المجتمعي لمواجهة التضليل السيبراني، فبينما يكتسح الفضاء السيبراني بكم هائل من المعلومات، يصبح دور الإعلام حاسما في تمكين الأفراد من التمييز بين الحقيقة والزيف. وذلك من خلال:

- **توفير معلومات دقيقة وموثوقة:** إذ يعمل الإعلام كمصدر أساسي للحقائق، مما يقلل من الاعتماد على المصادر غير الموثوقة الهادفة للتضليل.
- **شرح الآليات المعتمدة في التضليل:** من خلال تسليط الضوء على الأساليب المعتمدة من قبل مروجي التضليل مثل (التلاعب بالصور، العناوين المضللة، التغذية الآلية لنشر واسع النطاق)، مما يساعد الأفراد على تطوير التفكير النقدي.
- **تشجيع التحقق من المصادر:** بإرشاد الجمهور إلى أهمية التحقق من مصداقية المعلومات قبل تصديقها أو إعادة مشاركتها[1].
- **كشف حملات التضليل المنظمة:** من خلال تحديد الجهات التي تقف وراء حملات التضليل وأهدافها، ما يزيد من وعي المجتمع بخطورة هذه الممارسات.

بناء عليه، لا يقتصر دور الإعلام على مجرد نقل الأخبار، بل يمتد ليشمل بناء حصانة مجتمعية ضد التضليل السيبراني، من خلال رفع مستوى الوعي، وتطوير المهارات النقدية لدى الأفراد، وتحصينهم ضد مخاطر المعلومات المضللة.

[1] وديع محمد العزعزي، "الإشاعات وشبكات التواصل الاجتماعي، المخاطر وسبل المواجهة"، مجلة الإعلام والعلوم الاجتماعية للأبحاث التخصصية المملكة العربية السعودية، م1، ع3 (أكتوبر 2016)، ص.ص 28-50.

خلاصة

من خلال ما تم تقديمه في هذا الفصل حول الاستراتيجية الأمنية الجزائرية ومواجهتها لتهديدات البوتات الاجتماعية يمكن استخلاص النقاط الآتية:

- الانطلاقة الفعلية لرصد استخدام البوتات الاجتماعية في التأثير على الأمن الوطني الجزائري، كانت مع الحراك الشعبي سنة 2019؛ أين برز دور هذه اللجان المدعومة غالبا من أطراف خارجية معادية، في القيام بحملات تضليلية لتغيير مسار الحراك السلمي.
- البوتات الاجتماعية تعمل على نشر خطابات التعصب والكراهية، من خلال استثارة الانتماءات الجهوية بهدف نشر الفوضى وتقويض التماسك المجتمعي، ناهيك عن استهدافها لزعزعة ثقة المجتمع بالمؤسسات الرسمية للدولة.
- الانتخابات من ناحيتها أيضا، تعد فرصة لتدخل جهات خارجية عبر أتمتة النشر والتفاعل لإضعاف الثقة في مسار العملية الانتخابية والتحريض على المقاطعة.
- من الجانب المؤسساتي حث "المرجع الوطني لأمن المعلومات" على تنفيذ آلية للتنبؤ والكشف والحماية من البوتات الاجتماعية، لكن يلاحظ أن الهيئات الحكومية لم تخط هذا المسار بعد، إذ تتراوح استراتيجيتها بين تكذيب الأخبار المضللة عبر صفحاتها الرسمية وإصدار بيانات رسمية لنشر معلومات موثوقة.
- المؤسسات الأمنية في استراتيجيتها لمواجهة البوتات الاجتماعية، تعتمد على رصد مصدر الهجمات، إلى جانب إخطار المؤسسات الإعلامية والهيئات الحكومية المسؤولة، لتكذيب الأخبار المضللة.
- أوضح الاستبيان انخفاضا في نسب الوعي المجتمعي بالبوتات الاجتماعية، ما يستلزم تبني نهجا متكاملا يشمل الجوانب التحسيسية والقانونية والتعليمية، للحد من تداعيات استعمالها وتحييد أدوارها التحريضية والتضليلية.

الخاتمة

لقد تبين من خلال هذه الدراسة أن التهديدات السيبرانية لم تعد مجرد خطر افتراضي، بل أصبحت أداة استراتيجية توظف للتأثير على الأمن القومي للدول، كما هو الحال بالنسبة للبوتات الاجتماعية التي تمثل شكلا من أشكال الحروب السيبرانية. وبالتركيز على تحليل السياسة الأمنية الجزائرية في مواجهة تحديات البوتات الاجتماعية، توصلت الدراسة إلى أن الدولة تنتهج استراتيجية دفاعية ترتكز على الشفافية بالدرجة الأولى، وذلك من خلال دحض المعلومات المضللة سواء عبر القنوات الإعلامية أو المنصات الرسمية التابعة لمختلف الهيئات الوطنية، ومع ذلك فإنها لا تزال بحاجة إلى مزيد من الجهود الاستباقية في الجانب التقني والقانوني، سيما أمام نقص الوعي المجتمعي بهذه الظاهرة.

ومن مجمل دراستنا لموضوع "السياسية الأمنية الجزائرية في مواجهة التهديدات السيبرانية: البوتات الاجتماعية نموذجا" خلصنا إلى **النتائج التالية:**

- مع تغير طبيعة التهديدات، شهدت قطاعات الأمن توسعا تدريجيا لتبرز التهديدات السيبرانية، كأحد أخطر التحديات التي تواجه السياسات الأمنية للدول.
- تحديد نوع البوت الاجتماعي والغرض منه، يعد خطوة أساسية لمعرفة مستوى التهديد الذي يشكله في الفضاء السيبراني.
- الاستخدام السلبي للبوتات الاجتماعية كأدوات للدعاية الرقمية، يحمل في طياته تهديدا فعليا لأمن واستقرار الدول.
- السياسة الأمنية الجزائرية تاريخيا، لطالما سعت لمواكبة الرهانات التي تفرضها البيئة الإقليمية والدولية، وضمن هذا المسعى وجدت نفسها أمام ضرورة اعتبار تحقيق الأمن السيبراني على رأس أولوياتها.
- الجزائر في مواجهتها للتهديدات السيبرانية تنتهج استراتيجية متعددة الأبعاد، تشمل الجوانب القانونية، والمؤسساتية، إلى جانب اهتمامها بتنمية القدرات البشرية وتعزيز التعاون الدولي.
- رغم الاستراتيجية الشاملة التي تنتهجها الجزائر لتحقيق الأمن السيبراني، إلا أن المراتب التي تحتلها دوليا وعربيا، تشير إلى أنها بحاجة إلى مزيد من الجهود سيما في الجانب التقني.
- البوتات الاجتماعية في الحالة الجزائرية، غالبا ما توظف من قبل أجندات خارجية معادية، تسعى لضرب الاستقرار من خلال استهداف قضايا حساسة كالحراك الشعبي الجزائري، الانتخابات، نشر خطابات الكراهية والتعصب، وكذا تقويض الثقة في مؤسسات الدولة.
- جهود الأجهزة الأمنية الجزائرية، من قيادة وزارة الدفاع وجهاز المخابرات إلى مصالح المديرية العامة للأمن الوطني، تتكامل وفق رؤية استراتيجية موحدة للوقاية من أي تضليل سيبراني يستهدف صورة الجزائر ومؤسساتها ورموزها.

- وكالة الأنباء الجزائرية، باعتبارها ركيزة أساسية للإعلام الرسمي في البلاد، تعمل على ضمان التدفق المستمر للأخبار الموثوقة، لكنها تفتقد لآليات واضحة لمواجهة التضليل السيبراني عبر منصات التواصل الاجتماعي.
- نقص الوعي العام بالبوتات الاجتماعية الذي أوضحه الاستبيان، يفرض على المؤسسات الأمنية والإعلامية تبني نهج استباقي في التعامل من خلال تكثيف الحملات التحسيسية بمخاطر التضليل السيبراني.

التوصيات:

- الاهتمام بجوانب التنشئة الاجتماعية، لما لها من دور في مواجهة التضليل الممنهج بواسطة البوتات الاجتماعية؛ فالأسرة، المدارس، الجامعات، وحتى تنظيمات المجتمع المدني يمكن أن تسهم في بناء رؤية نقدية لمضامين منصات التواصل الاجتماعي، من خلال الحث على عدم الانسياق في المحتويات التحريضية، والتحلي بروح المواطنة.
- إنشاء مرصد وطني يعنى بتتبع التهديدات السيبرانية بمختلف أشكالها، مع تركيز خاص على البوتات الاجتماعية، لرصد وتحليل أنشطتها، والتصدي لتأثيراتها على الأمن الوطني.
- إطلاق بوابة إلكترونية أو تطبيقات تكون بمثابة قنوات رسمية للتبليغ عن المحتويات المشبوهة، وحسابات البوتات التي تحمل معلومات مضللة من شأنها المساس بالأمن الوطني.
- تحديث القوانين المتعلقة بالأمن السيبراني لتشمل الإشارة ولو ضمنيا للبوتات الاجتماعية والأنشطة الضارة المرتبطة بها مثل (نشر الأخبار الزائفة، التضليل، التلاعب بالرأي العام).
- تكثيف الحملات التوعوية الموجهة لمختلف شرائح المجتمع، بهدف رفع الوعي العام بمخاطر البوتات الاجتماعية والدور الذي تؤديه في نشر المعلومات المضللة والتأثير في الرأي العام.
- تأسيس مراكز بحث وطنية تعمل على تطوير حلول تقنية محلية تتلاءم مع خصوصية الفضاء الرقمي الجزائري.
- تشجيع الجامعات والمؤسسات الناشئة على الانخراط الفعال في تطوير خوارزميات قادرة على رصد المحتوى الرقمي المضلل الذي تنشره البوتات الاجتماعية.
- إنشاء منصات إلكترونية ومواقع انترنت وحتى برامج إعلامية مخصصة، تقدم إرشادات عملية حول الأمن السيبراني، مع التركيز على تهديدات البوتات.
- دمج مفاهيم الأمن السيبراني في المناهج التعليمية، لتعزيز التفكير النقدي وثقافة اليقظة الرقمية لدى الأجيال القادمة.
- وضع آليات اتصال مباشرة بين المؤسسات الإعلامية والهيئات الأمنية للاستجابة السريعة في حال انتشار حملات تضليل ممنهجة.

قائمة الجداول والاشكال

قائمة الجداول

قائمة الأشكال:

قائمة المصادر والمراجع

المصادر:

القرآن الكريم:

سورة الأنعام، الآية 82.

سورة قريش، الآية 4.

الوثائق الرسمية:

القوانين:

1. الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 09-04 المؤرخ في 05 أوت 2009، الجريدة الرسمية للجمهورية الجزائرية، ع47 (16 أوت 2009).
2. الجمهورية الجزائرية الديمقراطية الشعبية، المادة 394 مكرر 03 من القسم السابع مكرر "المساس بأنظمة المعالجة الآلية للمعطيات"، قانون العقوبات.
3. الجمهورية الجزائرية الديمقراطية الشعبية، القانون العضوي للإعلام رقم 23-14 المؤرخ في 2 ديسمبر 2023، الجريدة الرسمية ع77 (2ديسمبر 2023).

المراسيم الرئاسية:

1. الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم الرئاسي رقم 19-172، المؤرخ في 6 جوان 2019، الجريدة الرسمية للجمهورية الجزائرية ع 37 (9 جوان 2019).
2. الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم الرئاسي رقم 20-05، المؤرخ في 20 جانفي 2020، الجريدة الرسمية للجمهورية الجزائرية ع4 (26 جانفي 2020).
3. الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم الرئاسي رقم 24-181 المؤرخ في 5 جوان 2024، الجريدة الرسمية للجمهورية الجزائرية، ع39 (8 جوان 2024).
4. الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم الرئاسي رقم 183/20، المؤرخ في 13 جويلية 2020، الجريدة الرسمية للجمهورية الجزائرية ع40 (18 جويلية 2020).

المراسيم التنفيذية:

الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم التنفيذي رقم 16-134 المؤرخ في 17 رجب 1437 الموافق لـ 25 أفريل 2016، الجريدة الرسمية للجمهورية الجزائرية 26 (28أفريل 2016).

أولا: المراجع باللغة العربية:

الكتب:

1. العلي زياد، علي. الصراع والأمن الجيوسيبراني في السياسة الدولية "دراسة في استراتيجيات الاشتباك الرقمي". عمان: دار أمجد للنشر والتوزيع، ط1، 2020.
2. العلي زياد علي وحميد علي حسين. تكتيكات الحروب الحديثة الأمن السيبراني والحروب المعززة والهجينة. مصر: العربي للنشر والتوزيع، 2023.
3. المصدر، حيدر إبراهيم. الدعاية على الشبكات الاجتماعية، فلسطين: مركز الدراسات الإقليمية، 2020.
4. الرزقي كمال وآخرون. الرؤية العربية للأمن السيبراني. تونس: المنظمة العربية لتكنولوجيا الاتصال والمعلومات، 2021.
5. بن خرف الله، الطاهر. النخبة الحاكمة في الجزائر 1962-1982: بين التصور الإيديولوجي والممارسة السياسية. الجزائر: دار هومة للنشر والتوزيع، ج1، 2007.
6. بويحي، نصر الدين. "التوعية الأمني الدرع الواقي في مواجهة الإجرام السيبراني". مجلة الشرطة ع 149 (أكتوبر 2021).
7. جبور، منى الأشقر. السيبرانية هاجس العصر. بيروت: المركز العربي للبحوث القانونية والقضائية، 2013.
8. محمد، حمشي. حراك 22 فبراير 2019 في الجزائر انتفاضة واحدة ومقاربات شتى. قطر: المركز العربي للأبحاث ودراسة السياسات، ط1، 2023.
9. عكروم، ليندة. تأثير التهديدات الأمنية الجديدة على العلاقات بين دول شمال وجنوب المتوسط. عمان: دار ابن بطوطة للنشر والتوزيع، 2011.
10. كلاوزفيتز، كارل فون. الوجيز في الحرب، تر: أكرم ديري والهيثم الأيوبي. بيروت: المؤسسة العربية للدراسات والنشر، ط2، 1988.
11. لخضاري، منصور. السياسة الأمنية الجزائرية المحددات-الميادين-التحديات. الدوحة: المركز العربي للأبحاث ودراسة السياسات، ط1، 2015.
12. محسن، محمد عباس. الهجمات السيبرانية ومنطقة الفراغ التشريعي. ألفا للوثائق، ط1، 2021.

الأطروحات العلمية:

1. بغدادي، إيمان. "أثر تعديل قانون العقوبات الجزائري في التصدي للجريمة الإلكترونية". مجلة آفاق للبحوث والدارسات سداسية، دولية محكمة- المركز الجامعي إيليزي، ع4 (جوان 2019).
2. بن برغوث، ليلى. "الأمن السيبراني وحماية خصوصية البيانات الرقمية في الجزائر في عصر التحول الرقمي والذكاء الاصطناعي التهديدات، التقنيات، التحديات وآليات التصدي". المجلة الدولية للاتصال الاجتماعي م10، ع1 (2023).

3. بوزار قوادري، أميرة. حفظ الأمن الجماعي في ميثاق الأمم المتحدة وإشكالية توسع مفهوم الأمن. أطروحة دكتوراه، جامعة الجزائر 3: كلية العلوم السياسية والعلاقات الدولية،2022.

4. بوزبرة، سهيلة. "دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال". المجلة الدولية للبحوث القانونية والسياسية، م5، ع3 (2021).

5. حمزاوي ميلود. مكانة الحرب النفسية في إستراتيجية الولايات المتحدة لمكافحة الإرهاب بعد أحداث 11 سبتمبر. أطروحة دكتوراه، (الجزائر: المدرسة الوطنية العليا للعلوم السياسية، 2022).

6. دير، أمينة. أثر التهديدات البيئية على واقع الأمن الإنساني في إفريقيا دراسة حالة -دول القرن الإفريقي-. مذكرة ماجستير، جامعة محمد خيضر بسكرة: كلية الحقوق والعلوم السياسية، 2014/2013.

7. سعداوي، عمر. البعد الإقليمي للأمن الوطني الجزائري في ظل الحراك العربي الراهن. أطروحة دكتوراه، جامعة باتنة 1: كلية الحقوق والعلوم السياسية، 2019-2020.

المجلات والدوريات:

باللغة العربية:

1. العيداني، محمد. "التهديدات السيبرانية وجرائم المعلومات". مجلة الاجتهاد للدراسات القانونية والاقتصادية، م13، ع1 (2024).

2. بارة، سمير. "الأمن السيبراني في الجزائر السياسات والمؤسسات". المجلة الجزائرية للأمن الإنساني، ع4 (جويلية 2017).

3. بلحربي، نوال. "التهديدات الأمنية الجديدة وسبل مواجهتها: أي دور للحدود الذكية؟ ". مجلة أبحاث قانونية وسياسية، م7، ع1، (جوان 2022).

4. بلخير سلمى وشرقي محمود. "أثر مواقع التواصل الاجتماعي على الأمن المجتمعي الجزائري". المجلة الجزائرية للأمن والتنمية، م12، ع2 (أفريل 2023).

5. بلقاسم سميحة وبوشوشه حميد، "الجريمة الإلكترونية بعد جديد للإجرام في الجزائر.. واقعها وآليات مجابهتها". مجلة العلوم الإنسانية لجامعة أم البواقي م10، ع1 (جوان 2023).

6. بن مرزوق عنترة والكر محمد، "البعد الالكتروني للسياسة الأمنية الجزائرية في مكافحة الإرهاب". مجلة العلوم الإنسانية والاجتماعية، ع28 (جوان 2018).

7. بن عربية، رياض. "التهديدات اللاتماثلية في الفضاء السيبراني: حروب الجيل الرابع نموذجا". دفاتر البحوث العلمية، م 10، ع1 (2022).

8. بن عنتر، عبد النور. "سياسة الجزائر الأمنية: تحولات ومعضلات في سياق القلاقل إقليميا والحراك داخليا". مجلة سياسات عربية م10، ع55، (مارس2022).

9. بن عيسى ليلى وزمورة جمال. "أهمية حوكمة الأمن السيبراني لضمان تحول رقمي آمن للخدمات العمومية في الجزائر". مجلة البحوث الاقتصادية المتقدمة م7، ع2 (2022).

10. بوازدية، جمال. "الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية 'لتحديات والآفاق المستقبلية". مجلة العلوم القانونية والسياسية 01 (أفريل 2019).

11. بوطمين عبد الجبار وجربوعة عادل. "الأخبار الزائفة والحراك الشعبي في الجزائر". مجلة المعيار، م25، ع54 (2021).

12. بوسكين، سليم. "العقيدة الأمنية الجزائرية وإشكالية التكيف مع التهديدات الجديدة". مجلة العلوم القانونية والسياسية، جامعة الجزائر3، م10، ع02 (سبتمبر 2019).

13. بوكراع، ن. "من أجل جزائر صامدة سيبرانيا". مجلة الجيش الوطني الشعبي ع719 (جوان 2023).

14. بومخيلة، خالد. "واقع الحملات الانتخابية في فضاء التواصل الاجتماعي -دراسة حالة الجزائر-". المجلة الجزائرية للأبحاث والدراسات، م4، ع4 (2021).

15. جراية، الصادق. "تحولات مفهوم الأمن في ظل التهديدات الدولية الجديدة". مجلة العلوم القانونية والسياسية، جامعة الوادي، ع8 (جانفي 2014).

16. جمال الدين، هبة. "الأمن السيبراني والتحول في النظام الدولي، مجلة كلية الاقتصاد والعلوم السياسية م24، ع1(2023).

17. جنادي، إ "التحول الرقمي رهان سيادي". مجلة الجيش الوطني الشعبي 726 (جانفي 2024).

18. حديدان، سفيان. "الدخول أو البقاء عن طريق الغش في نظام المعالجة الآلية للمعطيات". مجلة الأستاذ الباحث للدراسات القانونية والسياسيةم2، ع4 (ديسمبر 2017).

19. حمادي، خالد. "الدعايات المحوسبة ... الجيل الجديد من حروب الهاشتاغ وصناعة البوتات الرقمية عبر منصات الميديا الجديدة". مدونة الإعلام والاتصال (أفريل 2022).

20. حمادي، هجيرة. "الرأي العام السيبراني في الجزائر: بين الميديولوجيا والأيديولوجيا قراءة في مضمون صفحات فيسبوكية أثناء فترة الحراك الشعبي". مجلة المعيار، م26، ع5 (2022).

21. حمزاوي، جويدة. "مفهوم الأمن بين عمودية المستويات وأفقية الأبعاد: مفهمة توصيفية متعددة المستويات". المجلة الجزائرية للأمن الإنساني، م7، ع2 (جويلية 2022).

22. خالدي، خديجة. "آلية الاتحاد الافريقي للتعاون الشرطي "أفريبول". مجلة العلوم الاجتماعية والإنسانية م 11، ع 1 (2018).

23. خطاب ولاء الدين سعيد وفرج مفتاح عماد. "السياسة العامة وعلاقتها بالسياسة العامة الأمنية (دراسة مفاهيمية)". مجلة المعهد العالي للدراسات النوعية م3، 15ع، (2023).

24. خوالدية، فؤاد. "السياسة الأمنية للجزائر أمام التهديدات الأمنية لمنطقتي المغرب العربي والساحل الإفريقي، المجلة الجزائرية للحقوق والعلوم السياسية، 26، ع2 (2021).

25. دريدي، عبد القادر. "تاريخ الإعلام الوكالاتي في الجزائر من خلال وكالة الأنباء الجزائرية". مجلة الساورة للدراسات الإنسانية والاجتماعية، م7، ع1 (2021).

26. دندن، جمال. "الاستراتيجية الأمنية للدولة الجزائرية في مكافحة الجرائم السيبرانية". مجلة صوت القانون م7، ع7 (نوفمبر 2020).

27. رقولي كريم ونويوة لخضر "الأمن السيبراني المتوسطي بين الواقع والرهانات الأمنية". مجلة طبنة المركز الجامعي بريكة، م2، ع2 (2019).

28. زقاغ، عادل. "المعضلة الأمنية المجتمعية: خطاب الأمنية وصناعة السياسة العامة". دفاتر السياسة والقانون، ع5 (جوان 2011).

29. زواوي لمياء ورملي فهيم. "التهديدات السيبرانية وأمن المجتمع الرقمي: دراسة حالة الجزائر". المجلة الجزائرية للأمن والتنمية، م12، ع 2 (أفريل 2023).

30. زياني، صالح. "تحولات العقيدة الأمنية الجزائرية في ظل تنامي تهديدات العولمة". مجلة المفكر، جامعة باتنة، ع5 (2022).

31. سعودي، باديس. "وكالات الأنباء بين الخضوع لهيمنة الدولة والاستقلالية: دراسة حالة في الجزائر والمغرب". مجلة العلوم الإنسانية لجامعة أم البواقي، م8، ع3 (ديسمبر 2021).

32. سليخ، أسامة. "الدوائر الجيوأمنية للجزائر بين منطق الجغرافيا وتصادم المصالح". مجلة الباحث الأكاديمي في العلوم القانونية والسياسية، المركز الجامعي بآفلو/ الأغواط م5، ع2 (2022).

33. شرف الدين، وردة. "التعاون القضائي والقانوني لمكافحة جريمة غسل الأموال والمرتكبة بواسطة تقنية المعلومات". مجلة الباحث للدراسات الأكاديمية م8، ع2 (2021).

34. شرقي، عبد الغاني. "التهديدات السيبرانية وإشكالية السيادة: إعادة قراء لسيادة واستفاليا". مجلة السياسة العالمية، م7، ع2 (2023).

35. شريط، نجمة. "الأمن السيبراني في العقيدة الدفاعية الجزائرية: الفرص والقيود"، المجلة الجزائرية للسياسة والأمن، م2، ع2 (ديسمبر 2023).

36. طيايبة ساعد وبورنان عبد الرحمان. "تطور العقيدة الأمنية الجزائرية ومواجهة التهديدات الأمنية الجديدة في منطقة المغرب العربي". مجلة الناقد للدراسات السياسية م6، ع1 (2022).

37. عطية، إدريس. "مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري". كلية الحقوق والعلوم السياسية، جامعة تبسة.

38. عيمور، ب. "التكوين والتعاون في الميدان السيبراني ". مجلة الجيش 715 (فيفري 2023).

39. عيمور، ب. "الدفاع والأمن السيبراني: مقاربات متكاملة". مجلة الجيش الوطني الشعبي 715 (فيفري 2023).

40. فضيل، شريف. "المخاطر السيبرانية أهمية التحسيس"، مجلة الجيش الوطني الشعبي ع715 (فيفري 2023).

41. فلاك، نور الدين. "دور العقيدة الأمنية الجزائرية في مواجهة التهديدات الأمنية الجديدة". مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، م4، ع2، (2019).

42. قطاف سليمان وبوقرين عبد الحليم. "الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري". المجلة الأكاديمية للبحوث القانونية والسياسية م6، ع1 (2022).

43. كركوري، حنان مباركة. "التأصيل القانوني للجرائم السيبرانية المرتكبة عبر الوسائط الرقمية". المجلة الافريقية للدراسات القانونية والسياسية م7، ع1 (جوان 2023).

44. لبدي، حنان. "التهديدات الأمنية الجديدة وانعكاساتها على الأمن المجتمعي في الجزائر". مجلة الساورة للدراسات الإنسانية والاجتماعية، م9، ع2 (2023).

45. لبيب أحمد محمد أحمد وآخرون. "دور الاتفاقيات الدولية والإقليمية في مجال الأمن السيبراني وموقف الدولة المصرية منها". الحوكمة والوقاية من الفساد ومكافحته 1 (سبتمبر 2024).

46. لزعر عبد العزيز وزياني رشيد. "آلية الاتحاد الافريقي للتعاون الشرطي (الأفريبول) ودورها في مكافحة الجريمة الإلكترونية". مجلة متون م14، ع3 (2021).

47. لعمراني، آسيا. "التعاون الدولي في مواجهة الجرائم السيبرانية: الجزائر نموذجا". المجلة الجزائرية للعلوم السياسية والعلاقات الدولية م5، ع2 (ديسمبر 2010).

48. مهدي، رضا. "الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري". مجلة إيليزا للبحوث والدراسات م6، ع2 (2021).

49. نجيدة، حسام. "الأبعاد الجديدة لمفهوم الأمن". مجلة العلوم الإدارية والسياسية، الكلية العسكرية لعلوم الإدارة، ع2 (ديسمبر 2023).

50. نعمان، كريمة. "الشرطة الجزائرية تتصدى لصناع الكراهية عبر المنصات الرقمية". مجلة الشرطة 149 (أكتوبر 2021).

51. واجعوط، سعاد. "مكافحة الجريمة السيبرانية على المستوى الوطني". مجلة دفاتر البحوث العلمية م12، ع1 (2024).

52. " SCLC... العصب الرقمي لصد الجرائم المعلوماتية ". مجلة الشرطة ع 158 (ماي 2024).

التقارير الرسمية:

1. الأمانة العامة لجامعة الدول العربية، إدارة الشؤون القانونية، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، 2010.
2. الأمم المتحدة، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، دراسة شاملة عن الجريمة السيبرانية، فيفري 2013.
3. المملكة العربية السعودية، شركة آفاق المعرفة للنشر والتوزيع، تقرير ارتيادي سنوي محكم "ما بعد الإنسانية العوالم الافتراضية وأثرها على الانسان"، 2022.

القواميس:

1. الكيالي، عبد الوهاب. موسوعة السياسة. عمان: دار الفارس للنشر والتوزيع، ط2، 1993.

الملتقيات والندوات:

1. بركان إكرام وفهيم رميلي. "واقع وإشكالات الأمن السيبراني في الجزائر". ورقة بحثية مقدمة للمؤتمر العلمي الوطني، جامعة قسنطينة 3، كلية العلوم السياسية، 2024.
2. بن بادة عبد الحليم وبوحادة محمد سعد. جريمة التجسس الإلكتروني نمط جديد من التهديدات السيبرانية الماسة بأمن دول المنطقة. الملتقى الدولي الأول الموسوم بأمن المعلومات في الفضاء الإلكتروني، جامعة غرداية: كلية الحقوق والعلوم السياسية، 2020.

المو اقع الالكترونية:

1. أحمد الشرقاوي، "خبير أمن المعلومات: الوعي المجتمعي هو سلاح مواجهة الحروب التكنولوجية"، الوطن، تاريخ المقال: 12 فيفري 2025.

https://2u.pw/Uir7m

2. بارة، سمير. "الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر: الدور والتحديات".

https://2u.pw/8lanG

3. عبد الصادق، عادل. "أنماط الحرب السيبرانية وتداعياتها على الأمن العالمي"، موقع السياسة الدولية، تاريخ المقال: 2017/05/14.

https://2u.pw/JKXTUa

4. أبو دوح، خالد كاظم. "التهديدات الأمنية". أوراق السياسات الأمنية، تاريخ المقال: 05 أوت 2022

https://2u.pw/lX2nr8w

5. "الجزائر تعد خطة للتصدي للأخبار المضللة"، الشرق الأوسط صحيفة العرب الأولى، تاريخ المقال: 21 أفريل 2025.

https://2u.pw/LuOPR

6. "المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني"، موقع وزارة الدفاع الوطني، تاريخ الاطلاع: 2024/12/31.

https://www.mdn.dz

7. "الفريق الأول سعيد شنقريحة: ضرورة التصدي للاستخدام الخطير للدعاية الهدامة والمضللة"، الشروق نيوز، يوتيوب، نشرت في 28 أفريل 2025، من 0:00 -0:33.

https://2u.pw/dSSgc

8. "تدشين المقر الجديد للمصلحة المركزية لمكافحة الجرائم السيبرانية"، موقع النهار، تاريخ المقال: 25 أكتوبر 2023.

https://2u.pw/6Q5bM

9. "خطر يهدد الديمقراطية والتماسك.. ما هو الاستقطاب المجتمعي؟"، الحرة- دبي، 17 جانفي 2024.
https://2u.pw/awGw6

10. علاء شهايب، "فيدلي: أداة جديدة في خدمة الصحفيين"، موقع IJnet، تاريخ المقال: 30 أكتوبر 2018.

https://2u.pw/CheND

11. "صدور المرسوم الرئاسي المتعلق بإنشاء المدرسة العليا في الأمن السيبراني"، وكالة الأنباء الجزائرية، تاريخ المقال:2024/06/09.

https://2u.pw/yAJcU

12. غانمي، منية. "الجزائر.. الانتخابات الجزائرية تشعل حربا إلكترونية بين الحراك والسلطة"، العربية. نت، تاريخ المقال: 20 ماي 2020.

https://2u.pw/78It4

13. قنديل، أسماء. "دليلك لاستخدام أداة Invid في التحقق من صحة الصور والفيديوهات، موقع IJnet، تاريخ المقال: 28 جوان 2024.

https://2u.pw/02GcacS

14. كاسبرسكي وأفريبول تعززان شراكتهما في مكافحة الجرائم السيبرانية بتوقيع اتفاقية تعاون جديدة"، موقع Kaspersky، تاريخ المقال: 19-11-2024.

https://2u.pw/g3rym

15. لحياني، عثمان. "انتخابات الجزائر: "فيسبوك" ميدان الحملات والدعاية المضادة". العربي الجديد، تاريخ المقال: 23 نوفمبر 2019.

https://2u.pw/YbggI

16. "مؤتمر الأمم المتحدة لمنع الجريمة والعدالة الجنائية"، موقع الجزيرة، تاريخ المقال: 2015/04/21.
https://2u.pw/SHpIxs

17. "مؤسسات الجمهورية على خط واحد لمجابهة الدعاية المضللة"، موقع بوابة الجزائر، تاريخ المقال: 29 أفريل 2025.

https://2u.pw/QQRoG

18. "مجلة الشرطة تسلط الضوء على موضوع الأمن السيبراني "، وكالة الأنباء الجزائرية، تاريخ المقال: 2024/06/05.

https://2u.pw/W5eb8

19. "مواجهة المعلومات المضللة: الجزائر ستظل في طليعة المدافعين عن القارة الإفريقية"، الإذاعة الجزائرية، تاريخ المقال: 2025/04/20.

https://2u.pw/Uqu4v

ثانيا: باللغة الإنجليزية:

A. Books :

1. Andreasson, Kim. Cybersecurity. Boca Raton: CRC Press, 2012.

2. Buzan, Barry. People, States, and Fear: The National Security Problem in International Relations. Great Britain : wheatsheaf books, 1983.

3. Booth, Ken. Theory of world Security. New York: Cambridge university press, first published, 2007.

4. Persily Nathaniel and Tucker Joshua A. Social Media and Democracy. New York : Cambridge University Press, First published, 2020.

b. Theses:

1. Rossi, Sippo. Bots on social media the Past, present and future. Danemark : Copenhagen Business School, 2024.

C. Review Articles:

1. Abdellaoui, El Arbi et al. “Fine-Tuned Understanding: Enhancing Social Bot Detection with Transformer-Based Classification.” IEEE Access 12 (2024).

2. Ashkan, Dehghan et al. “Detecting bots in social-networks using node and structural embeddings.” Journal of Big Data 10 (2023)

3. Barone, Daniele Maria. "Social bots and synthetic interactions to stage digital extremist armies". Sicurezza, terrorismo e società, Italian Team for Security, 16 (2022).

4. Bensoula, Noureddine. "Electronic flies and public opinion. Al-Naciriya: Journal of Sociological and Historical Studies, Issue1, Vol1 (June 2020).

5. Berente, Nicholas and Salge, Carolina. "Is that social bot behaving unethically ? ". Communication of the ACM, VOL 60, NO 9 (September 2017).

6. Brachten, Florian et al. "Do social Bots Dream of Electric Sheep ? A Categorisation of Social Media Bot Accounts". Australasian Conference on information systems, (2017).

7. B. Sneha, “Detecting Malicious Twitter Bots using Machine Learning.” International Journal for Research in Applied Science and Engineering Technology (2024)

8. Cho Y Clare and Ling Zhu. "Social Media Dissemination and Moderation Partices ". Congressional Research Service, March 20, 2025.

9. Cresci Stefano, et al. “Bots in Social and Interaction Networks.” ACM Transactions on Information Systems (TOIS) 39 (2020).

10. Cucoreanu, Cristian. "Cyber Risks to National Security : Manipulation of the Electoral Process Through the Use of Bots and Algorithms on Social Platforms". European Journal of Law and Public Administration, vol 11, Issue 2 (2024).

11. Efe Arin, and Mucahid Kutlu. “Deep Learning Based Social Bot Detection on Twitter.” *IEEE Transactions on Information Forensics and Security* 18 (2023).

12. Eiman, Alothali et al, “Detecting Social Bots on Twitter: A Literature Review.” *2018 International Conference on Innovations in Information Technology (IIT)* (2018).

13. Feng Zeyang et al. "Social Robots and Internet Opinion Rights". Journal of New Media and Economics, Vol 1, No 4 (2024).

14. Ferreira, Gabriel Estavaringo, Bianca Lima Santos, Marcelo Torres do Ó, Rafael Rodrigues Braz and Luciano Antônio Digiampietri. “Social bots detection in Brazilian presidential elections using natural language processing.” Proceedings of the XVII Brazilian Symposium on Information Systems (2021).

15. Ferrara, Emilio. "Bots, elections, and social media : a brief overview". USC Information Sciences Institut, (Oct 2019).

16. Santiago Folch et al. “Web Bot Detection Using Mouse Movement.” *2023 JNIC Cybersecurity Conference (JNIC)* (2023).

17. Forelle, Michelle et al. "Political Bots and the manipulation of public opinion in Venezuela".

18. Gorwa, Robert and Guilbeault Douglas. "Unpacking the social Media Bot : A typology to guide research and Policy. Research Gate (28 /07/2018).

19. Hartmann Kim and Keir Giles. "The Next Generation of Cyber-Enabled Information Warfare". Tallinn : NATO CCDCOE Publications (2020).

20. Howard Phlip N and Woolley Samuel C. " Political Communication, Computational Propaganda, and Autonomous Agents". International journal of communication 10 (2016).

21. Lingyu, Xu. "Research on work strategies and workflow of social Bots". University of bristol, vol 8 (2023).

22. Liu Qian et al, "Influence of social bots in information warfare : A case study on @UAWeapons Twitter account in the context of Russia- Ukraine conflict", Communication and the public, vol 8 (2023).

23. Ross Bjorn et al. "Are social bots a real threat? An agent-based model of the spiral of silence to analyse the impact of manipulative actors in social networks, European Journal of Information Systems, vol 10 (2020).

24. Schellekens, Jasper. "Release the bots of war : social media and artificial intelligence as international cyber-attack". Przegląd Europejski, vol 4 (2021).

25. Selvarani S, and Sahana B.R. "Detecting Malicious Social Bots Based on Clickstream Sequences." International Journal for Multidisciplinary Research (2023).

26. Sharif, Mahmood and Daniel, Kats. "Perceptions of Social Bots and ability to detect them". HAI (December 2022).

27. Stieglitz, Stefan and Brachten, Florian. "How powerful are Social Bots?" . Academic society for management and communication, (June 2018).

28. Strembeck, Mark et al. "Automated Narratives On the Influence of Bots in Narratives during the 2020 Vienna Terror Attack". Austria.

29. Tayouri, David. "The Secret War of Cyber Influence Operations and How Identify Them", Cyber, Intelligence, and Security, vol 4, N^0 1 (March 2020).

30. Tingxuan Wu, et al. "MSM-BD: Multimodal Social Media Bot Detection Using Heterogeneous Information." *ArXiv* abs/2501.00204 (2024).

31. Varol, Onur. "The spread of fake news by social bots". Bloomington : Indiana university (24 July 2017)

32. Warner, Mark R. White Paper "Potential Policy for Regulation of Social Media and Technology Firms".

33. Woolley, Samuel C. Bots and Computational propaganda: Automation for communication and control, Cambridge university press.

34. Yan, Li et al. "Social Bot Detection Model Based on Graph Contrastive Learning."

C. Report :

1. Switzerland, World Economic Forum, The Global Risks Report 2024 19th Edition, January 2024.

2. USA, CNA Information Memorandum, Social Media Bots Laws, Regulations, and Platform Policies, 2020.

3. Washington, U S Departement of justice, Report on the investigation into Russian interference in the 2016 Presidential election, March 2019.

D. **Scientific Conferences:**

1. Xu, Junhui, et al "DGBot: A DeGlobalizing Graph Transformer Model for Bot Detection." 2024 IEEE/ACIS 27th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD) (2024)

2. Neamat El-Tazi, Sarah et al. "Detecting Fake Accounts on Social Media." 2018 IEEE International Conference on Big Data (Big Data) (2018).

3. Kaufhold Marc- André and Rauter Christian, "Social Media Misuse- cultural violence, Peace and Security in digital Networks", Science Peace Security '19, Germany : Conference on Technical Peace and Security Research, 2019.

E. Web links :

1. Brisset, Caroline. "Understanding the influence of Social Media Bots". Icuc social. https://2u.pw/rOfjRMNw

2. "Botometer", RAND, Retriever from : https://encr.pw/7zsyx

3. "Cybersecurity Threats", impreva : https://2u.pw/OgnlZ

4. Hayawi E et al, feature selection approach to identify optimal features of profile metadata to detect social bots in Twitter. *Soc. Netw. Anal. Min.* **11**, 84 (2021). https://doi.org/10.1007/s13278-021-00786-4

5. Simon Kemp, DIGITAL 2024 : ALGERIA, DATAREPORTAL, 23 February 2024. https://2u.pw/fsoIXB7

6. "Social media users in Algeria", NapoleonCat, March 2025, Accessed on: 30/04/2025. https://2u.pw/v1pbP

ثالثا: باللغة الفرنسية:

A. Encyclopédies et Dictionnaires :

1. Le Petit Robert, Jousette Rey-Debove et Alain Rey, Paris : nouvelle édition millésime 2011.

B. Rapports :

1.République Algérienne Démocratique et Populaire, Ministère de la poste, des Télécommunications, Référentiel National de Sécurité de L'information, 2020.

C. Les Cites :

1. Mécanisme de l'Union Africaine pour la coopération policière (AFRIPOL), AFRIPOL, 07/09/2023. https://2u.ppw/BDu42R

رابعا: باللغة الروسية:

1. В.В. Василькова, Н.И. Легостаева. "Социальные боты в политической коммуникации". RUDN Journal of Sociology, Vol19, No1 (2019).

الملاحق

الملحق رقم 01: استمارة الاستبيان

في إطار إنجاز مذكرة تخرج لنيل شهادة ماستر تخصص "علاقات دولية" نوجه لكم وبكل شكر هذا الاستبيان، ونرجو منكم التعاون معنا في الحصول على معلومات دقيقة. للعلم أن المعلومات المقدمة من سيادتكم ستحظى بالسرية التامة، ولن توظف إلا في إطار البحث العلمي. وفي الأخير تقبلوا منا فائق التقدير والاحترام.

المحور الأول: المعلومات الشخصية

الجنس:

ذكر ☐ أنثى ☐

الفئة العمرية:

أقل من 18 عاما ☐

18-25 عاما ☐

26-35 عاما ☐

36-50 عاما ☐

أكثر من 50 عاما ☐

المستوى التعليمي:

غير متعلم ☐ ابتدائي ☐ ثانوي ☐ جامعي ☐ دراسات عليا ☐

الوظيفة/المهنة:

طالب ☐ أستاذ جامعي ☐ موظف ☐ أعمال حرة ☐ عاطل عن العمل ☐

المحور الثاني: مستوى الوعي حول البوتات الاجتماعية

هل سمعت من قبل عن البوتات الاجتماعية؟

نعم☐ لا☐

كيف تعرفت على البوتات الاجتماعية؟ (اخترجميع الخيارات المناسبة)

من خلال الأخبار أو التقارير الإعلامية ☐

من خلال الإنترنت أو وسائل التواصل الاجتماعية ☐

من خلال أصدقاء أو زملاء ☐

من خلال دراسات أو محاضرات ☐

آخر ☐

كيف تصف البوتات الاجتماعية بناء على معرفتك بها؟ (اخترالإجابة الأنسب لك)

برامج تستخدم للتفاعل الآلي على وسائل التواصل الاجتماعي ☐

حسابات وهمية تنشر محتوى معين ☐

أداة لتحسين الخدمات الرقمية ☐

لا أعرف بشكل دقيق ☐

هل تعتقد أن البوتات الاجتماعية تستخدم لأغراض سيئة مثل التلاعب بالرأي العام أونشرالأخبارالزائفة؟

نعم☐ لا☐ لا أعلم☐

المحور الثالث: تقييم البوتات الاجتماعية كتهديد

إلى أي مدى تعتبرالبوتات الاجتماعية تهديدا للحياة العامة؟

تهديد كبير☐ تهديد متوسط☐ تهديد ضئيل☐ لا أعتبرها تهديدا☐

في رأيك، ما هي أخطراستخدامات البوتات الاجتماعية؟ (اخترجميع الخيارات المناسبة)

نشر الأخبار الزائفة ☐

التلاعب بالانتخابات أو القرارات السياسية ☐

التحريض على الكراهية أو العنف ☐

تعزيز خطاب الكراهية أو الانقسامات الاجتماعية ☐

آخر ☐

هل تعتقد أن البوتات الاجتماعية يمكن أن تؤثر على استقرار المجتمع الجزائري؟

نعم☐ لا☐ ربما☐

هل تعتقد أن البوتات الاجتماعية تؤثر على أرائك؟

نعم☐ لا☐ ربما☐

إذا كانت إجابتك "نعم"، كيف ترى هذا التأثير؟

يغير آرائي بشكل كامل ☐

يؤثر بشكل جزئي على آرائي ☐

يجعلني أقل ثقة بالمعلومات المتاحة ☐

آخر ☐

هل تعتقد أن وسائل التواصل الاجتماعي عموما تؤثر على النقاشات حول القضايا الوطنية؟

نعم☐ لا☐ ربما☐

هل تعتقد أن البوتات الاجتماعية تلعب دورا أكبر من البشر في تشكيل النقاشات حول القضايا الوطنية؟

نعم☐ لا☐ ربما☐

في رأيك، ما هي أفضل طريقة لمكافحة تأثير البوتات الاجتماعية السلبي؟ (اختر جميع الخيارات المناسبة)

زيادة الوعي العام حول البوتات الاجتماعية ☐

تعزيز القوانين المتعلقة بالجرائم السيبرانية ☐

تعليم الناس كيفية التحقق من صحة المعلومات ☐

آخر ☐

المحور الرابع: الإطار المؤسسي والسياسات الجزائرية:

هل تعتقد أن الجزائر تمتلك سياسات واضحة لمواجهة البوتات الاجتماعية؟

نعم☐ لا☐ لا أعلم☐

ما مدى ثقتك في قدرة الهيئات الجزائرية المختصة على التعامل مع التهديدات السيبرانية؟

مرتفعة☐ متوسطة☐ ضعيفة☐ لا توجد ثقة☐

هل سمعت من قبل عن أي مؤسسة أو هيئة رسمية جزائرية مختصة بالأمن السيبراني؟

نعم☐ لا☐

إن كانت إجابتك بـ "نعم" اذكر الهيئات التي تعرفها

.....

برأيك، ما الجوانب القانونية التي يجب تطويرها لمواجهة التهديدات السيبرانية؟

تشديد العقوبات ☐

تطوير القوانين الحالية ☐

زيادة التنسيق الدولي ☐

أخرى ☐

المحور الخامس: تأثير البوتات على توجهات الرأي العام والوعي اتجاهها

في رأيك، ما هي القضايا الوطنية التي تتأثر بشكل أكبر بسبب البوتات الاجتماعية؟ (اختر حتى 3 خيارات)

الاقتصاد☐ السياسة☐ الأمن☐ التعليم☐ الصحة☐ آخر☐

كيف ترى تأثير البوتات الاجتماعية على النقاشات السياسية داخل الجزائر؟

يعزز النقاشات بشكل إيجابي ☐

يؤدي إلى تضليل المعلومات ☐

يزيد الانقسامات السياسية ☐

آخر ☐

في رأيك، هل يتمتع المواطن الجزائري بالوعي الكافي لتمييز البوتات والمعلومات المضللة؟

نعم☐ لا☐ إلى حد ما☐

هل تعتقد أن البوتات الاجتماعية تلعب دورا في التأثير على القرارات الانتخابية في الجزائر؟

نعم☐ لا☐ ربما☐

ما هي الوسائل التي تعتقد أنها الأهم لرفع الوعي حول البوتات الاجتماعية؟

حملات إعلامية ☐

التعليم في المدارس والجامعات ☐

منصات التواصل نفسها ☐

أخرى ☐

هل تعتقد أن بعض الدول تستخدم البوتات الاجتماعية كجزء من حروب سيبرانية ضد الجزائر؟

نعم☐ لا☐ ربما☐

ما مدى احتمالية أن تستخدم البوتات الاجتماعية في إثارة الفتن أو النزاعات داخل الجزائر؟

عالية☐ متوسطة☐ منخفضة☐ غير ممكنة☐

ملحق رقم 02: أجوبة مقابلة مع محافظ شرطة في المصلحة المركزية لمكافحة الجريمة السيبرانية

تاريخ المقابلة: 2025/03/25.

الجزء الأول: الإطار العام للسياسة الأمنية

1. كيف تصفون دور المصلحة المركزية لمكافحة الجريمة السيبرانية في تنفيذ السياسة الأمنية الوطنية المتعلقة بمكافحة الجرائم السيبرانية؟

✓ المصلحة المركزية لمكافحة الجريمة السيبرانية في إطار تنفيذها للسياسة الأمنية لمكافحة الجريمة السيبرانية تعمل وفق فرق ولائية، تضم بدورها فصائل مركزية، وتباشر مهامها في إطار مبادرات، حيث أنها تعتمد على المعاينة الدورية بنسبة تقارب 70%، إلى جانب الشكاوى التي تقدر ب 30%.

2. ما هي الأطر القانونية والتنظيمية التي تعتمدون عليها في مكافحة الجريمة السيبرانية؟ وهل هناك خطط لتحديث هذه القوانين لتواكب التطورات الحديثة؟

✓ نستند إلى قانون العقوبات وقانون الإجراءات، إلى جانب قانون 09_04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

✓ ولمواكبة التطورات نتجه إلى تقديم مشاريع لجهاز العدالة، في حال ملاحظتنا لثغرات قانونية. فعلى سبيل المثال في 2015، لاحظنا أن القوانين المتعلقة بتنظيم داعش تقتصر على الجانب المادي على الرغم من شيوع عديد الجرائم السيبرانية، كالتجنيد عبر الانترنت، الترويج والتحريض للانتماء إلى الجماعات الارهابية، ما جعلنا نطرح الأمر أمام الوزارة الوصية، وأسفر ذلك عن صدور المادة 87 مكرر11، 12 من قانون العقوبات.

3. هل هناك استراتيجية وطنية شاملة لمكافحة الجريمة السيبرانية؟ إذا كانت موجودة، كيف يتم تنسيق الجهود بين مختلف الجهات المعنية (مثل الجيش، الشرطة، القطاع الخاص)؟

✓ هنالك إستراتيجية شاملة لأن المعالجة تقضي التنسيق والتعاون بين مختلف القطاعات سيما ما يتعلق بحملات التحسيس.

الجزء الثاني: البوتات الاجتماعية كتحدي أمني

4. كيف تتعاملون مع ظاهرة استخدام البوتات الاجتماعية في نشر الأخبار الزائفة أو التلاعب بالرأي العام؟

✓ نتعامل في إطار خطة مضادة، تتراوح ما بين تحسيس المواطن إلى إنشاء بوت مضاد من قبل تقنيين لدحض الأخبار الزائفة.

- ✓ يوجد على مستوى المصلحة فرقة مركزية لليقظة ومعالجة التبليغات، تقوم بالمتابعة الدورية لشبكة الانترنت في كل ولاية، في حالة رصدها لمنشورات من شأنها التلاعب بالرأي العام والمساس بالقضايا الحساسة للدولة، تقوم بإصدار محضر معاينة تقنية، وتباشر الاجراءات القانونية.

5. هل تم رصد حالات استهداف الجزائر باستخدام البوتات الاجتماعية؟ إذا كانت الإجابة بنعم، هل يمكنكم تقديم أمثلة؟
   - ✓ معلومات مغلوطة تمس بأمن الجزائر أو شخصيات بارزة.
   - ✓ فترة الحراك.
   - ✓ الترويج لغلاء الأسعار مثلا، بغرض التحريض.
   - ✓ قضية مجموعات في فيسبوك مخلة بالحياء، ثبت في نهاية التحقيق أنها من طرف دولة المغرب.
6. ما هي التقنيات أو الأدوات التي تستخدمونها لاكتشاف وتتبع البوتات الاجتماعية الضارة؟
   - ✓ (سرية) تشمل تحديد هوية الأشخاص، العناوين، أرقام الهواتف، البرامج.
7. كيف تقيمون مستوى الخطر الذي تشكله البوتات الاجتماعية على الأمن القومي الجزائري؟ وماذا عن تأثيرها على الاستقرار الاجتماعي والسياسي؟
   - ✓ تبرز خطورة الوضع في اتجاه أطراف خارجية لتأجيج الأوضاع الداخلية من خلال دعم وتحريض حركات إرهابية (ماك ورشاد).

الجزء الثالث: التعاون الدولي والإقليمي

8. هل تتعاونون مع دول أخرى أو مؤسسات دولية لمكافحة الجريمة السيبرانية؟ إذا كان الأمر كذلك، أي شراكات تعتبر الأكثر فاعلية؟
   - ✓ نعم تتعاون المصلحة مع الدول المتقدمة في هذا المجال حيث يشتمل مقر المصلحة على المكتب المركزي الوطني (أنتربول)، إلى جانب مصلحة مركزية التعاون الدولي. ولعل الشراكة الأكثر فعالية هي التي تجمعنا مع الانتربول.
9. كيف ترون دور التعاون الإقليمي بين الدول العربية والإفريقية في مواجهة التحديات السيبرانية المشتركة؟
   - ✓ التعاون الإقليمي بين الدول العربية يتجسد في إطار الاتفاقية العربية لمكافحة جرائم تقنية المعلومات اما مع الدول الإفريقية فمن خلال الآلية التي تعتبر حديثة (أفريبول).
10. هل توجد برامج تبادل خبرات أو تدريب مشترك مع دول أخرى أو منظمات مثل الاتحاد الأوروبي أو الأمم المتحدة؟
    - ✓ نعم نوجد دورات تدريبية وتكوينية إلى جانب قواعد لإجراءات معاقبة المجرمين، إذ في حال رصد الهوية الحقيقية لمرتكب الجريمة السيبرانية وتبين أنه في دولة أجنبية، تتم مراسلة بلاد المجرم عبر القنوات

الرسمية التعاون الدولي، وتتم معاقبته بشرط ثبوت أنها جريمة سيبرانية في كلا البلدين، مع التصريح بالإجراءات المتخذة. لكن في حال كانت الجريمة تمس أمن الدولة وسلامة التراب الوطني/ إرهاب سيبراني/ أنظمة المعالجة الآلية للمعطيات، فإن الأمر يقتضي تسليم المجرم.

هنالك دول لا تلتزم بالتسليم ما يجعل من الجزائر ننتهج مبدأ المعاملة بالمثل في حال مطالبة الأولى بتسليم مجرمين.

الجزء الرابع: التحديات والفرص

11. ما هي أكبر التحديات التي تواجهونها في مكافحة الجريمة السيبرانية، خاصة فيما يتعلق بالبوتات الاجتماعية؟

- ✓ سرعة تنفيذ الجريمة.
- ✓ طبيعتها العابرة الحدود.
- ✓ صعوبة تحديد الهوية والمصدر.
- ✓ تقنية التخفي.
- ✓ الاختلاف في تحديد الجريمة السيبرانية من دولة إلى أخرى، بمعنى أنه ما تعتبره دولة على أنه جريمة قد لا يعتبر جريمة في دولة أخرى.

12. كيف تتعاملون مع التحديات الناجمة عن عدم وجود إطار قانوني دولي شامل لمكافحة الجرائم السيبرانية؟

- ✓ هناك اتفاقية دولية وهي قيد التوقيع، بعد أن تمت مناقشة بنودها لمدة سنتين، وتعد الجزائر من المساهمين الرئيسيين فيها وهي "الاتفاقية الدولية الشاملة لمكافحة استخدام تكنولوجيات المعلومات والاتصالات لأغراض إجرامية".

13. هل ترون أن هناك حاجة إلى زيادة الوعي العام حول مخاطر الجريمة السيبرانية؟ إذا كانت الإجابة بنعم، ما هي الخطوات المتخذة لتحقيق ذلك؟

- ✓ نعم زيادة الوعي العام وتحسيس المواطن له أهمية كبيرة، وهذا ما نسعى إليه من خلال حملات التوعية والتحسيس التي نقوم بها، إلى جانب تقديم المحاضرات في مختلف الجامعات، لنشر الوعي بمخاطر هذه الجريمة.
- ✓ حاليا نقوم بحملات توعية واسعة النطاق بخصوص اختراق البطاقة الذهبية لعديد المستخدمين.

الجزء الخامس: الرؤية المستقبلية

14. ما هي رؤيتكم المستقبلية لتطوير قدرات المصلحة المركزية لمكافحة الجريمة السيبرانية؟

- ✓ الاستثمار في العنصر البشري المختص والتركيز على التكوين المتواصل والمستمر.

15. هل هناك خطط لتوظيف تقنيات الذكاء الاصطناعي أو التعلم الآلي في الكشف عن الجرائم السيبرانية، بما في ذلك البوتات الاجتماعية؟

- ✓ طورنا اتفاقيات تعاون مع جامعات، آخرها مع جامعة عين تموشنت في مجال الذكاء الاصطناعي والأمن السيبراني، كذلك نسعى إلى بناء شركات دولية في هذا المجال.

16. كيف ترون تطور التهديدات السيبرانية في السنوات القادمة، وما هي الاستعدادات المتخذة لمواجهتها؟

- ✓ إضافة اتصالات الجزائر لعروض جديدة لسرعة التدفق الفائقة للإنترنت، وفي إطار سعيها لربط المناطق النائية أولا بهذه التقنيات، بغية تعميمها ورقمنة قطاعات الدولة، سيملي ارتفاع عدد مستخدمي الانترنت في الجزائر، ما سينعكس على زيادة مستويات التهديدات السيبرانية.

17. هل تخططون لتعزيز التعاون مع القطاع الخاص، مثل الشركات التكنولوجية الكبرى، لتحسين قدراتكم في مكافحة الجريمة السيبرانية؟

- ✓ نعم هنالك تعاون مع شركات تكنولوجية كبرى سيما على المستوى الخارجي.

ملحق رقم 03: مقابلة مع ضابط شرطة في فرقة محاربة الجرائم السيبرانية

تاريخ إجراء المقابلة: 2025/04/17

1. كيف تقيمون المشهد الحالي للتهديدات والجرائم السيبرانية التي تستهدف الجزائر عبر وسائل التواصل الاجتماعي؟ وما هي أبرز المجالات أو المواضيع التي يكثر استهدافها؟

- ✓ إن الجزائر، بفضل مبادئها مواقفها الثابتة، لطالما كانت مستهدفة من قبل أطراف خارجية معادية تسعى لزعزعة استقرارها وتقويض وحدتها. هذه الأطراف تستغل فضاء مواقع التواصل الاجتماعي، لنشر المعلومات المضللة والأخبار الكاذبة التي تستهدف الرأي العام الجزائري. وكذا القيام بحملات ممنهجة لا تهدف فقط إلى تشويه صورة الجزائر ومواقفها، بل تسعى أيضاً إلى تأجيج القضايا الداخلية الحساسة، وزرع بذور الفتنة بين أبناء الوطن الواحد.

2.ما هي أهم الاستراتيجيات التي تعتمدها الجزائر لتعزيز أمنها السيبراني على وسائل التواصل الاجتماعي بشكل عام، ولمواجهة التهديدات الناجمة عن البوتات الاجتماعية بشكل خاص؟

- ✓ الجزائر اعتمدت إستراتيجية وطنية شاملة لمختلف الجوانب القانونية والتشريعية والمؤسساتية إذ هنالك في كل أمن ولاية فرقة محاربة الجرائم السيبرانية، والجزائر العاصمة بشكل استثنائي تملك فصائل لمكافحة الجرائم السيبرانية على مستوى 13 دائرة، ومن ناحية مصالح العدالة استحدثت القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال أما فيما يخص الاستجابة لتهديدات البوتات الاجتماعية فتضطلع الفرقة بمباشرة التحقيقات مع إخطار الوزارات والهيئات المسؤولة لتفنيد الأخبار المغلوطة.

3.ما هي أبرز الأمثلة أو الحالات التي رصدتم فيها استخدام البوتات الاجتماعية لشن تهديدات سيبرانية على الجزائر عبر منصات التواصل الاجتماعي؟

- ✓ الحراك الشعبي الجزائري.
- ✓ تأجيج القضايا الداخلية.
- ✓ التحريض على الاضرابات.
- ✓ قضايا ارتفاع الأسعار ونسب البطالة.
- ✓ إنشاء حسابات باسم مؤسسات جزائرية من طرف جهات معادية.
- ✓ الانتخابات أين تزيد نسبة الأخبار المغلوطة والإشاعات إعلان مزيف لفوز مترشح، تشويه صورة المترشحين، التشكيك في نزاهة الانتخابات.

4.ماهي خصائص وسائل التواصل الاجتماعي التي يمكن استغلالها من قبل البوتات لتحقيق أهداف المساس بالأمن القومي الجزائري؟

- ✓ سهولة الانتشار والسرعة.
- ✓ ميزة التخفي.

5.كيف يتم استغلال البوتات الاجتماعية لنشر الأخبار الكاذبة والمعلومات المضللة حول الشؤون الجزائرية عبروسائل التواصل الاجتماعي؟

- ✓ البوتات الاجتماعية تستغل من قبل عديد الجهات والأطراف الخارجية في نشر الفوضى المعلوماتية والتأثير السلبي على الرأي العام في الجزائر.

6.ما هي أبرزالقوانين والسياسات الجزائرية التي تنظم المحتوى الرقمي على وسائل التواصل الاجتماعي بهدف مكافحة الجريمة السيبرانية والتضليل؟

- ✓ قانون رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

7.ما هي الجهود التي تبذلها الجزائرلتعزيزقدراتها التقنية والمؤسساتية في مجال رصد وتحليل نشاط البوتات الاجتماعية؟

- ✓ على مستوى فرقة محاربة الجرائم السيبرانية توجد ثلاث فصائل فصيلة التحقيقات " تعنى بمباشرة التحقيق في الجرائم السيبرانية، وفصيلة المساعدات التقنية توكل إليها مهمة تحري لتحديد هوية مستعملي الحسابات المجرمة وتقديم المساعدات التقنية لمختلف المصالح وفصيلة لليقظة التكنولوجيا هي التي تكون مسؤولة عن مراقبة المحتوى الرقمي ورصد أي حالات استهداف ممنهجة عبر وسائل التواصل الاجتماعي.

8. هل هناك أدوات أو تقنيات متخصصة يتم استخدامها لهذا الغرض؟

- ✓ المديرية العامة للأمن الوطني وفرت جميع الإمكانيات اللوجيستيكية والبشرية بحيث، وفرت انترنت عال الجودة للأجهزة التي تباشر هذه المهام، الأجهزة والتقنيات إلى جانب التكوينات المتخصصة لضمان العنصر البشري المتحكم في التقنيات الحديثة.

9.هل هناك تعاون كاف ين مختلف الجهات الحكومية والمؤسسات الأمنية في الجزائر لتبادل المعلومات وتنسيق الجهود لمواجهة البوتات على وسائل التواصل الاجتماعي؟

- ✓ نعم، الجزائر تتعامل بشفافية مع تهديد البوتات الاجتماعية، حيث أنه فور رصد هجوم على مواقع التواصل الاجتماعي بواسطة بوتات يتم بشكل استعجالي إخطار الوزارة أو الجهة الحكومية المستهدفة، لتقوم هذه الأخيرة بتفنيد الخبر على صفحاتها الرسمية على مواقع التواصل الاجتماعي، وفي الوقت ذاته تواصل الأجهزة الأمنية التحقيقات اللازمة.

10.ما هو الدور الذي يلعبه الوعي المجتمعي في الحد من تأثير حملات التضليل التي تنشرها البوتات عبر وسائل التواصل الاجتماعي في الجزائر؟

- ✓ يمثل الوعي المجتمعي في الجزائر خط الدفاع الأساسي لحماية الأفراد والمجتمع من التأثيرات السلبية لحملات التضليل التي تشنها البوتات عبر منصات التواصل الاجتماعي.

11.كيف يمكن للمؤسسات الأمنية ووسائل الإعلام ومنظمات المجتمع المدني التعاون الزيادة الوعي لدى مستخدمي وسائل التواصل الاجتماعي حول كيفية التعرف على الأخبار الكاذبة والحسابات الوهمية وتجنب الوقوع ضحية للتضليل؟

- ✓ نعم، لطالما تم تنظيم حملات تحسيسية مشتركة بين مختلف المصالح الأمنية وخبراء في المجال السيبراني.

ملحق 04: مقابلة بوزارة الاتصال

مع السيد (ة): علان عبد القادر، مدير التطوير بوزارة الاتصال.

بتاريخ: 2025/05/08

1. كيف تقيمون المشهد الحالي للتهديدات السيبرانية التي تستهدف الجزائر عبر وسائل التواصل الاجتماعي؟

- ✓ يشكل المشهد الراهن للتهديدات السيبرانية التي تستهدف الجزائر عبر منصات التواصل الاجتماعي تحديًا شاملا يهدد أمن الأفراد واستقرار المجتمع على حد سواء. وتزيد من حدة هذا التحدي أنشطة لجان التضليل التي تستغل غياب الإطار القانوني المنظم لهذه الشبكات لتحقيق أهدافها.

2.ما هي الاستراتيجية التي تتبعها الوزارة لمكافحة انتشار الأخبار الزائفة والتضليل الإعلامي في الجزائر؟ وهل هنالك مصالح ومديريات على مستوى الوزارة منوطة بهذا الدور؟

- ✓ هنالك إستراتيجية وطنية شاملة، فبمجيء الرئيس عبد المجيد تبون تم إصدار المرسوم الرئاسي رقم 05-20 المؤرخ في 24 جمادى الأولى 1441هـ، الموافق ل 20 جانفي 2020م، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.
- ✓ وعلى مستوى الوزارة، تعنى مديرية التطوير بالأدوار المتعلقة بتأمين البنية التحتية، توظيف مهندسي إعلام آلي، ومختصين في الأمن السيبراني.

3.في حالة وقوع هجمات سيبرانية ممنهجة بواسطة بوتات اجتماعية ما هي إجراءات التي تتخذونها؟ وكيف يتم تنسيق حملات مضادة؟

- ✓ في حال وقوع هجمة سيبرانية بشكل عام، أولا يتم قطع الاتصال بالأنترنت، ثم تحديد مصدر الهجمة لمعالجتها من قبل المختصين، وتجدر الإشارة إلى أن الوزارة لها تقنيات مثل جدار النار (الحماية) كذلك شهادة تأمين المواقع SSL وتتطلب هذه البرامج تحديث كل عام.
- ✓ أما في حال شهدت الوزارة استهدافا بواسطة البوتات الاجتماعية، فيتم إصدار بيان رسمي لتكذيب الأخبار المضللة المتداولة عبر الحسابات الرسمية للوازرة ومواقعها الرسمية، وربما حتى في بعض الجرائد.

4.هل هناك تنسيق بين وزارة الاتصال والجهات الحكومية الأخرى، في مجال مكافحة الأخبار الزائفة؟ وكيف يتم هذا التنسيق؟

نعم هنالك تنسيق من خلال استحداث المحافظة السامية الرقمنة التي تعمل على رقمنة القطاعات الحكومية، وتأمين بياناتها، ولا سيما من خلال الشروع في إنجاز مركز البيانات بالجزائر والشريعة.

5.فيما تتمثل أبرز القوانين المتعلقة بالنشر والإعلام؟ وهل هنالك خطط لمواكبة تحديات البوتات الاجتماعية في الفضاء السيبراني؟

- ✓ القانون العضوي للإعلام رقم 1423 المؤرخ في 18 جمادى الأولى 1445هـ الموافق ل 02 ديسمبر 2023 قد تضمن الباب الخامس منه المسؤولية وحق الرد والتصحيح، إذ نصت المادة 62 " يتحمل مدير النشر وصاحب العمل الصحفي المسؤولية المدنية والجزائية على كل محتوى تم نشره من طرف النشريات الدورية أو الصحف الإلكترونية"، ما يعني أن وسائل الإعلام ملزمة على تحمل المسؤولية في حال بدرت منها معلومات خاطئة ولابد أن تتجه إلى التصحيح على نفس الوسيط الإعلامي أو الوسيلة التي نشرت المعلومة المغلوطة.
- ✓ قانون رقم 20-23 مؤرخ في 18 جمادى الأولى عام 1445 الموافق ل 2 ديسمبر سنة 2023، يتعلق بالنشاط السمعي البصري.
- ✓ قانون رقم 19-23 مؤرخ في 18 جمادى الأولى عام 1445 الموافق ل 2 ديسمبر سنة 2023، يتعلق بالصحافة المكتوبة والصحافة الإلكترونية.

6.ما هو دور الوزارة في تعزيز الوعي المجتمعي لدى المواطنين وتمكينهم من التعرف على الأخبار الزائفة والتحقق من مصداقية المعلومات؟

- ✓ مواجهة الأخبار الزائفة ليست بمسألة تكنولوجيا، يقدر ما هي مسألة ثقافة، ودورنا كوزارة يكون عن طريق إدراج برامج حول الأمن السيبراني، كلمات وخطابات للوزير تخص التضليل الإعلامي والسيبراني.
- ✓ كذلك مسألة توعية الموظفين أمر جد ضروري، بحيث يتم تحسيسهم بإلزامية تجنب المواقع المشبوهة والبريد المزعج، عدم الولوج لحسابات العمل بشبكات انترنت أجنبية.

7.هل هناك برامج أو مبادرات بالشراكة مع الأجهزة الأمنية أو منظمات المجتمع المدني لتعزيز سياسات الرقابة على المحتوى الرقمي ومكافحة المعلومات المضللة؟

- ✓ سياسات الرقابة على المحتوى الرقمي هي من اختصاص وزارة البريد والمواصلات السلكية واللاسلكية.

ملحق 05: مقابلة بوكالة الأنباء الجزائرية

مع السيد: " القامة عمار"، مستشار المدير العام لوكالة الأنباء.

بتاريخ: 2025/08/06

1.كيف تصفون الدور الذي تلعبه وكالة الأنباء الجزائرية في المشهد الإعلام الجزائري؟

- ✓ وكالة الأنباء الجزائرية، ومنذ تأسيسها إبان الثورة التحريرية، كانت تسعى لتلبية تطلعات الشعب الجزائري، ومنذ ذلك الحين وهي تشكل الناطق الرسمي للجزائر، والمصدر الأساسي للأخبار الموثوقة.

2.أمام سرعة انتشار الأخبار الكاذبة، كيف يمكن لـ "واج" أن تستفيد من مكانته كمصدر إخباري وطني موثوق به لتعزيز جهود مكافحة التضليل؟

- ✓ مكانة وكالة الأنباء الجزائرية، تلزمها على اتخاذ خطوات مكثفة للتصحيح والتوجيه، بهدف نشر معلومات موثوقة، فمنحى إصدار البرقية الواحدة يمر على صحفي ثم رئيس التحرير وصولا إلى الأمانة العامة، وذلك حرصا على مراجعتها والتأكد من خلوها من أي هفوات لا تتناسب مع مبادئ الوكالة.
- ✓ مبدأ الوكالة في تحرير البرقية يكون بالإجابة على الأسئلة الخمس (من، ماذا، متى، أين، كيف)، بالتالي فإن معرفة مصدر المعلومة جد ضروري، وبدونه لا يتم طرحها.

3.هل هناك وحدة أو فريق متخصص داخل الوكالة مكلف بمكافحة التضليل السيبراني؟ في حال وجوده، ما هي مهام هذا الفريق؟

- ✓ هنالك قسم يخص التضليل الإعلامي (قسم اليقظة الإعلامية)؛ ويعمل كوحدة متخصصة تراقب وتدقق بعناية المحتويات الإعلامية المشبوهة التي تستهدف أمن الجزائر واستقرارها، ثم الرد عليها في شكل بيانات. لكن بخصوص التضليل السيبراني، فقد كان هنالك مشروع إنشاء فضاء بالتنسيق مع مختلف الوزارات لليقظة التكنولوجية، يعمل لمعالجة الأخبار المضللة، لكن هذا المشروع لم يكلل بالتنفيذ بسبب نقص الإمكانيات المادية والبشرية اللازمة.

4.كيف تستخدم "واج" منصاتها الرقمية الخاصة الموقع الإلكتروني، صفحات التواصل الاجتماعي الرسمية لمواجهة التضليل ونشر الحقائق؟

- ✓ نقوم ببث الأخبار بشكل دوري على منصات التواصل الاجتماعي، ويكون انتقاء الأخبار التي تنشر على حسب أهميتها، بما في ذلك التي تعنى بالرد على الإشاعات المضللة والأخبار الزائفة.

5.كيف تتعاون وكالة الأنباء الجزائرية مع الجهات الحكومية الأخرى أو المؤسسات الأمنية لمواجهة هذه الظاهرة؟

- ✓ هنالك آلية على مستوى الموقع الرسمي لوكالة الأنباء الجزائرية، تعمل بالتنسيق مع مختلف الهيئات الحكومية التي تشهد استهدافا من خلال الأخبار المغلوطة، فتعمل هذه الآلية على معالجة الخبر الزائف مع نشر تصحيحه في إطار أيقونة الخبر "الصحيح".

7.ما هي أبرز التحديات التي تواجه الوكالة في مواكبة التطور المستمر لتقنيات التضليل السيبراني المستخدمة من قبل البوتات؟

- ✓ الوكالة تواجه تحديات البوتات من خلال التعليقات على منصاتها الرسمية؛ هذا التضليل عادة ما يستهدف المساس بصورة الوكالة أو حتى الهيئات العليا والحكومية المشار إليها في فحوى المنشور، لذلك تكون تتجلى الاستجابة من خلال حجب التعليقات في حال تم الاشتباه بوجود تعليقات مشبوهة أو محرضة منشورة بطريقة آلية.

8.كيف يمكن لوكالة الأنباء الجزائرية الاستفادة من التكنولوجيا الحديثة والذكاء الاصطناعي في تعزيز قدرتها على مكافحة التضليل؟

- ✓ قامت الوكالة بدفع اشتراكات الذكاء الاصطناعي المتخصصة في كشف التضليل على غرار:
- ✓ تطبيق Feedly/ محرك البحث Perplexity AI/ موقع Who is/ أداة IN vid

ملحق رقم 06: مقابلة حول دور الوعي المجتمعي في مواجهة التضليل السيبراني

السيد: العيشاوي مهدي، ضابط شرطة رئيسي بمكتب الإعلام والاتصال، أمن ولاية الجزائر.

بتاريخ: 2025/05/08.

1) هل سبق لكم أن قمتم بحملات تحسيسية لتعزيز الوعي المجتمعي بمخاطر التضليل السيبراني؟

- ✓ نعم، كمديرية عامة للأمن الوطني، وعلى مستوى مصالح أمن ولاية الجزائر تحديدا، نقوم بحملات تحسيسية على مدار السنة تخص التضليل السيبراني، والاستعمال العشوائي لشبكة الانترنت سواء في المؤسسات التعليمية، أين يكون انتقاؤنا للمواضيع مرتبط بالفئة العمرية ودرجة استيعاب الفئة المستهدفة (تلاميذ/ طلبة)، أو على المستوى الفضاءات العمومية.

وفي سياق التضليل السيبراني، تتمركز إرشاداتنا حول التحذير من إعادة نشر المعلومات المشتبه في صحتها، لأن ذلك قد تمتد تبعاته لتصل إلى المساءلة القانونية، إلى جانب الحث على تتبع الأخبار من خلال الصفحات الرسمية، لتفادي الوقوع في فخ التضليل.

2) حسب رأيك، ما مدى أهمية الوعي المجتمعي تحديدًا في مواجهة التضليل السيبراني مقارنة بالحلول التقنية؟

- ✓ بطبيعة الحال، الحلول التقنية لوحدها لا تكفي، سيما أمام التطور التكنولوجي الذي عزز من طبيعة الجرائم السيبرانية ما جعل من قدرات الجانب العملياتي محدودة، مقارنة بالوعي المجتمعي الذي يمثل جدار حماية في وجه أي تضليل سيبراني ممنهج يستهدف الأمن الوطني.

3) ما هي الفئات الأكثر عرضة للتأثر بالتضليل السيبراني، وكيف يمكن تصميم برامج توعية تستهدف هذه الفئات بشكل فعال؟

- ✓ فئة الشباب هم الفئة الأكثر استهدافا، وعرضة للتأثر، كون لجان التضليل تستغل نقاط ضعف هذه الفئة، في تغيير آرائهم وإضعاف الروح المعنوية لدى هذه الفئة، على سبيل المثال تشجيعهم على الهجرة غير الشرعية.

لهذا فإن برامجنا كمكتب اتصال بالتنسيق مع فرقة محاربة الجرائم السيبرانية، تكون حسب معطيات الميدان والفئة المراد توعيتها.

4) كيف يمكن للوعي المجتمعي أن يساهم في الحد من انتشار المعلومات المضللة عبر الإنترنت ووسائل التواصل الاجتماعي؟

- ✓ الوعي المجتمعي يسهم في الحد من انتشار المعلومات المضللة من خلال أنه يعمل على تعزيز روح المواطنة والانتماء، ويعمل على تشكيل إدراك جمعي بأن هنالك جهات معادية أجنبية تسعى لتأجيج صراعات مجتمعية، خلق الفوضى والتحريض على سلوكيات عدائية...

هذا الإدراك من ناحيته يعزز نظرة نقدية لدى الأفراد اتجاه محتويات منصات التواصل الاجتماعي، ويجعلهم يتجهون نحو التحقيق من مصادر موثوقة، لاستقاء المعلومة الأصلية.

5) ما هي نصيحتك النهائية للأفراد والمؤسسات لتعزيز الوعي المجتمعي والحد من تأثير التضليل السيبراني؟

بالنسبة للأفراد:

- ✓ التحلي بروح المواطنة.
- ✓ متابعة الصفحات الرسمية والمصادر الموثوقة كالبيانات الرسمية، والتغطيات الإعلامية.
- ✓ ثقافة التبليغ ضد أي أنشطة مشبوهة من شأنها التأثير على النظام العام والأمن الوطني.

بالنسبة المؤسسات:

- ✓ التكوين المتواصل على مستوى المديرية العامة للأمن الوطني.
- ✓ تنظيم مداخلات بخصوص آخر مستجدات التهديدات لتبادل المعلومات والخبرات.
- ✓ إطلاع موظفي القطاع الأمني، أن أي تصرف حتى لو كان غير مقصود، يعكس مباشرة صورة الدولة بأكملها وسمعتها على الصعيدين الداخلي والخارجي، إذ قد يتم استغلاله من قبل أطراف معادية، ليتحول في وقت وجيز إلى قضية رأي عام، تهدد الأمن القومي وتزعزع الثقة في مؤسسات الدولة.

الملحق رقم 07: قياس نسب الأتمتة في تغريدات مضللة عبر استخدام موقع بوتوميتر "Botometer"

قائمة الملاحق

الحراك أمل الشعب الجزائري @... · 24 Dec 24
#مراني_ش_راضي

5 33 104 2.6K

الحراك أمل الشعب الجزائ... · 26 Dec 24
لما تتحول الجزائر إلى سجن كبير #
مراني_ش_راضي#

10 48 200 4.3K

البحث حسب اسم المستخدم أو المعرف:

@FEweZ9x1XJWkz3z

معرف المستخدم

التحقق من المستخدم

@FEweZ9x1XJWkz3z

معرف المستخدم:
1354213973944651776

تقييم البوت: 1.4/5

تاريخ الحساب: 30/05/2023

الحراك أمل الشعب الجزائري @FE... · 5d
الى كل شعوب العالم الشعب الجزائري الحر لم ينتخب ومعندوش رايس....
وتبون مجرد واجهة للجنرالات الحاكم الفعلي للبلاد لي حاكمين الجزائر بالحديد والنار

19 62 766

عيادة الدكتور ROYAL... · 08 Sep 22
الجنرال شنقريحة 🇩🇿 يخصص
400 مليون دولار 🤔
من أجل الحرب الإعلامية ضد المغرب
وانا مواطن مغربي 🇲🇦
اخصص ميزانية 10 dh
لخوض الحرب
فنجان قهوة سوداء
وهاتف و wifi مجاني

الملحق رقم 08: آلية كشف "الخبر الصحيح" عبر موقع وكالة الأنباء الجزائرية

وزير الفلاحة محمد عبد الحفيظ هني لا يحمل ولم يحمل أي جنسية أجنبية

الإثنين, 15 نوفمبر 2021 21:00

الجزائر - نفى مصدر مأذون يوم الاثنين أن يكون وزير الفلاحة والتنمية الريفية محمد عبد الحفيظ هني، المعين مؤخرا في إطار تغيير جزئي للحكومة، حاملا لجنسية أجنبية.

فهرس المحتويات