

الأمن السيبراني كظاهرة اجتماعية وتنظيمية في المؤسسة المعاصرة *Cybersecurity as a social and organizational phenomenon in the modern institution*

حسبية فجيري^{1*}

¹ جامعة مولود معمري تيزي-وزو (الجزائر).

تاريخ الاستلام: 08 مارس 2026 ؛ تاريخ المراجعة: 25 ماي 2026 ؛ تاريخ القبول: 23 جويلية 2026

ملخص:

يهدف هذا البحث إلى تحليل موضوع الأمن السيبراني في المؤسسة سيما المعاصرة منها، وذلك من منظور سوسيولوجي، بإبراز أبعاده الاجتماعية والتنظيمية. وقد سعت الدراسة إلى إبراز دور الاتصال التنظيمي في تنسيق الأدوار ونقل سياسات الحماية الرقمية وكذلك تفسير طريقة تشكل معنى الأمن السيبراني عبر تفاعل الأفراد اليومي، أما بالنسبة للمنهجية المعتمدة في هذا الطرح فهي نظرية تحليلية، بحيث نركز على مراجعة مختلف الأدبيات السوسيولوجية التي تتعلق بالأمن السيبراني، التفاعلية الرمزية، الاتصال التنظيمي، والهدف من ذلك استكشاف الأبعاد الأمنية السيبرانية وفق تصور ومنظور اجتماعي وتنظيمي دون أن نلجأ إلى الدراسة الميدانية. ومن بين النتائج التي توصلنا إليها، أن الأمن السيبراني يمثل ممارسة اجتماعية وتنظيمية تتأسس على الثقافة المشتركة والتفاعل اليومي والتعاون داخل المؤسسة. كما أن فعالية الإجراءات التقنية مربوطة بمدى استيعاب أفراد التنظيم لها وادماجها في سلوكياتهم المهنية اليومية.

الكلمات المفتاحية: الأمن السيبراني؛ المؤسسة المعاصرة؛ الاتصال التنظيمي؛ التفاعل الاجتماعي؛ المعاني الرمزية.

Abstract:

This research aims to analyze cybersecurity in institution, particularly modern ones, from a sociological perspective, highlighting its social and organizational dimensions. The study sought to emphasize the role of organizational communication in coordinating roles and conveying digital security policies, as well as to explain how the meaning of cybersecurity is shaped through daily interactions among individuals. As for the methodology adopted in this presentation, it is an analytical theory, whereby we focus on reviewing the various sociological literature related to cybersecurity, symbolic interactionism, and organizational communication. The goal is to explore the cybersecurity dimensions according to a social and organizational perspective without resorting to field studies. Among our findings is that cybersecurity is a social and organizational practice based on shared culture, daily interaction, and collaboration within the institution. Furthermore, the effectiveness of technical measures is linked to the extent to which members of the organization understand and integrate them into their daily professional behaviors.

Keywords: Cybersecurity; the modern institution; organizational communication; social interaction; symbolic meanings.

*Corresponding author: e-mail: hassiba.fedjiri@ummtto.dz.

1- مقدمة:

أصبحت المؤسسة المعاصرة تواجه تحديات كثيرة وذلك بفعل استخدام الأنظمة المعلوماتية والتكنولوجيا الرقمية والتقنيات الحديثة رغم أنها تشكل جوهرًا أساسيًا وعمودًا فقريًا لعملها في مختلف القطاعات، وانتقلت من الأنماط التقليدية التي تعتمد على التواصل المباشر والمعاملات الورقية، إلى البيئات الرقمية المتشابكة والمتراصة والتي في تسيير أنشطتها تستند على قواعد البيانات والشبكات والمنصات الإلكترونية. هذا الانتقال والتحول لم يقتصر على زيادة السرعة والفعالية وتطوير الأداء فقط، إنما في المقابل أفرز تحديات جديدة متعلقة بحماية البيانات والمعطيات والحفاظ على سرية المعلومات وضمان استمرارية الأنظمة. وهذا ما جعل الأمن السيبراني من أبرز القضايا التي تُطرح في السياق التنظيمي، وموضوع اهتمام اجتماعي وإداري في الوقت نفسه.

وتجاوز هذا المفهوم بعده التقني ليصبح مرتبطًا بأنماط الاتصال والهيكل التنظيمي وكذلك التفاعلات اليومية للأفراد في التنظيم. ولم تعد المخاطر السيبرانية تقتصر على الأعطال التقنية أو الهجمات الخارجية، إنما أصبح لها امتداد يشمل السلوكيات اليومية في المؤسسة، ومن بينها ضعف وعي الأفراد بالمخاطر الرقمية وسوء استخدام الأنظمة المعلوماتية وغيرها. وهذا ما يعكس أهمية تبني منظور سوسيولوجي لدراسة موضوع الأمن السيبراني والحاجة إلى المقاربة التحليلية التي تتجاوز النظرة التقنية البحتة والضيقة، لتفسر هذا الموضوع ضمن سياقه الاجتماعي والتنظيمي.

هناك دراسات سابقة تناولت موضوع الأمن السيبراني ولكنها غالبًا تطرقت إليه من منظور إداري أو تقني، مع تركيزها على تطبيق الأنظمة الرقمية وحماية البيانات، ونجد أخرى تركز على الجوانب التنظيمية دون التركيز والتعمق في الجانب الاجتماعي للمعاني الرمزية والتفاعلات اليومية للأفراد في المؤسسة. ومن هنا تبرز الفجوة البحثية التي تجعلنا نهتم بدراسة الأمن السيبراني باعتباره ممارسة تنظيمية واجتماعية متكاملة.

وتتمثل أهمية هذه الورقة البحثية في تقديم إطار نظري يسمح بفهم كيفية اندماج التفاعل الرمزي والاتصال التنظيمي في المؤسسة، وفهم الأمن السيبراني الذي يمكن اعتباره كممارسة تنظيمية واجتماعية تسمح باستيعاب كيفية اندماج التفاعلات الرمزية والاتصالات التنظيمية في تفعيل قواعد الحماية الرقمية ضمن السلوك المؤسسي. ويهدف البحث إلى التطرق لموضوع الأمن السيبراني في المؤسسة المعاصرة وذلك في إطار النظريات السوسيولوجية التي تبرز العلاقة بين التفاعل والاتصال وبناء المعنى.

أما بالنسبة للمنهجية المعتمدة في هذا الطرح فهي نظرية تحليلية، بحيث نركز على مراجعة مختلف الأدبيات السوسيولوجية التي تتعلق بالأمن السيبراني، التفاعلية الرمزية، الاتصال التنظيمي، والهدف من ذلك استكشاف الأبعاد الأمنية السيبرانية وفق تصور ومنظور اجتماعي وتنظيمي دون أن نلجأ إلى الدراسة الميدانية. ومن هنا فموضوع بحثنا يتمحور حول دراسة الأمن السيبراني كظاهرة اجتماعية وتنظيمية في المؤسسة المعاصرة، وذلك بالتركيز على أبعاده الاجتماعية والتنظيمية. ومن هذا المنطلق ينشأ السؤال الرئيسي التالي:

- كيف يمكن للأمن السيبراني أن يتشكل في المؤسسة المعاصرة بوصفه نتاجا للاتصال التنظيمي وللتفاعل الاجتماعي وما هي التحديات المرتبطة به؟

2- تحديد المفاهيم الأساسية للدراسة:

إن المفاهيم مثل المؤسسة، الأمن السيبراني، الاتصال التنظيمي والتفاعل الاجتماعي وغيرها، تتعدد تعريفاتها باختلاف المرجعيات التي تتناولها. لذلك فمن الضروري أن يوضح الباحث المقصود بها ضمن دراسته، حتى لا يكون هناك نوع من الالتباس والغموض حولها وحتى لا تختلط المعاني والدلالات الاجتماعية بالتقنية أو الإدارية وغيرها.

وعلى ضوء ذلك سندعرض أبرز وأهم المفاهيم التي اعتمد عليها هذا البحث، وسنكتفي فقط بالأمن السيبراني، المؤسسة، الاتصال التنظيمي والتفاعل الاجتماعي، باعتبارها الركيزة الأساسية في التحليل دون أن نشأت الانتباه إلى مفاهيم أخرى قد تطيل هذا البحث، مع التركيز على الكيفية التي تتداخل فيها البنية الاجتماعية في تحديد الممارسات والسلوكيات مع البعد التنظيمي.

1.2- الأمن السيبراني:

الأمن السيبراني كمصطلح ظهر في ثمانينات القرن الماضي، وذلك في رواية من روايات الخيال العلمي للأمريكي والكاتب ويليام جيبسون، بحيث وصف هذا القرن بالعصر الرقمي وعصر التطورات التكنولوجية (شلوش، 2018، صفحة 190)

ويُعرفه كل من بيكا نيتانمي ومارتي ليهتو في كتابهما المعنون "الأمن السيبراني، التحليل والتكنولوجيا"، على أنه مجموعة من الإجراءات المتخذة للدفاع ضد الهجمات التي يشنها قراصنة الكمبيوتر، و بما يضمن تنفيذ تلك الإجراءات والتدابير. (مرزوق و حرشاي، 2017، صفحة 66)

أما في بحثنا هذا، فيمكن النظر إلى الأمن السيبراني على أنه مجموعة من الإجراءات والسياسات والممارسات الاجتماعية والتنظيمية التي من هدفها حماية الموارد الالكترونية والمعلومات والبيانات الرقمية في المؤسسة. فهذا المفهوم لا يمكن اختصاره في مجموعة من التدابير أو الوسائل التقنية، إنما عملية تتشكل عبر بناء المعاني المشتركة وتفاعل الفاعلين والتزامهم بالقواعد في ممارساتهم اليومية.

2.2- المؤسسة المعاصرة:

استُخدم مفهوم المؤسسة تاريخيا للإشارة إلى عدة أنماط من التنظيم الاجتماعي التي توجه أدوار الأفراد وتضبط سلوكهم، منها المدرسة، الأسرة، الدين وغيرها. إلا أن هذا الاتساع المفاهيمي يمكن أن يؤدي إلى خلق غموض إذا لم يتم التحديد بدقة للمقصود منه في إطار الدراسة. فمن الضروري إذن أن يوضح الباحث المعنى المعتمد في دراسته. ومن خلال موضوعنا فطبيعته تقتضي زاوية نظر مرتبطة بالعلاقات المهنية ومحيط العمل أكثر من ارتباطها بالتنشئة الاجتماعية التقليدية.

ومن بين التعاريف التي أُعطيت للمؤسسة: "المؤسسة بشكل عام هي تركيبة يبتدعها الإنسان بالتعاون مع الأفراد الآخرين في المجتمع، فالحب مثلا ظاهرة طبيعية، أما الزواج فهو مؤسسة اجتماعية ويشمل مفهوم المؤسسة على كل التنظيمات القائمة في المجتمع كالزواج والعائلة والملكية والمشروع الاقتصادي والهيئات الدينية والسياسية والقانونية" (الحوش، 2024، صفحة 80)

وفي بحثنا هذا سنستعمل مفهوم المؤسسة المعاصرة، ونقصد به منظمة العمل الحديثة المتميزة بالمرونة الهيكلية، استعمال التكنولوجيا الرقمية الحديثة وغيرها، والتي تعتبر الفضاء المنظم للجهود من أجل تحقيق الأهداف المسطرة بعناية، وذلك ضمن البنية الرسمية التي فيها توزيع للمسؤوليات وتحديد لمواقع السلطة وضبط لمسارات التعاون والاتصال. في هذا السياق المؤسسة المعاصرة ليست مجموعة من الإدارات أو مجرد مكان لممارسة العمل فقط، إنما تعتبر شبكة ومجموعة من التفاعلات والعلاقات التي تربط بين الأفراد والعمليات التنظيمية والهيئات. وتتسم بأنواع مختلفة من الاتصال والهيكلية، كذلك بالآليات التي تصنع القرار وتحدد سلوك الأفراد في التنظيم.

وبسبب التحديات المتسارعة التي تعرفها المؤسسة المعاصرة منها الرقمية والاجتماعية، فيجب عليها أن تكون أكثر تعقيدا ومرونة في الوقت ذاته، ما يجعل فهم ممارساتها مرتبطا بقدرتها على التنسيق بين مختلف الأفراد وفهمهم المتبادل للأدوار والمهام. ومن هنا فالمؤسسة يمكن اعتبارها بيئة يُمارس فيها الأمن السيبراني، ويتجلى ذلك في توزيع المسؤوليات والالتزام بالقواعد وتنظيم شتى العمليات اليومية لضمان حماية الموارد الرقمية واستمرارية العمل.

2.3- الاتصال التنظيمي:

هناك الكثير من التعريفات الخاصة بالاتصال التنظيمي، و" ذهب كثير من العلماء والباحثين في مجال الاتصال الى استخدام مصطلح الاتصال التنظيمي بخلاف الاتصال المؤسسي أو الإداري، باعتباره مرتبطا ارتباطا وثيق وأعمق بالسلوك والهيكل والمناخ والثقافة التنظيمية السائدة في المؤسسة، ويعتبر اخرون في نفس المجال "الاتصال" أن تفضيلهم لمصطلح الاتصال التنظيمي لأنه يعبر بشكل دقيق عن العمليات الاتصالية التي تقوم بها منظمات الأعمال اذ يصعب تصور المنظمة وتنفيذ أنشطتها بدون الاتصال." (الأمين، 2016، صفحة 89)

كما يمكن تعريفه كذلك على أنه "التفاعل في التنظيم يعتمد على الاتصال طالما أنه أداة نقل المعلومات والوقائع والأفكار والمشاعر من شخص لآخر ومن مستوى معين إلى مستوى آخر داخل كل التنظيمات وهذا بدوره يجعل من الممكن تحقيق الأهداف التنظيمية" (بوفلجة، 1992، صفحة 35)

أما في بحثنا هذا فالاتصال التنظيمي يمكن اعتباره العملية التي يتم عبرها تبادل التوجيهات، المعلومات وكذلك المعرفة بين المجموعات والأفراد في المؤسسة، ويهدف ذلك إلى تحقيق الفعالية والتنسيق والانسجام في محيط العمل. ولكنه لا يتوقف فقط على نقل الرسائل، إنما يشمل بناء المعنى المشترك، تفسير السياسات وتأثيره على السلوك والثقافة المؤسسية.

ويأخذ الاتصال التنظيمي أشكالاً متعددة في المؤسسة المعاصرة: أفقياً بين الزملاء من أجل تبادل المعلومات والخبرات للتعامل مع التهديدات والمخاطر الرقمية، عمودياً بين الموظفين والإدارة من أجل توضيح السياسات الأمنية السيبرانية، غير رسمي ويشمل تفاعلات الأفراد والجماعات اليومية التي تسعد على تكوين تبني وتبني فهم مشترك للقواعد الأمنية وللمعايير المشتركة. هذه العلاقات والتفاعلات تتيح للأفراد بإعادة الانتاج للمعاني الاجتماعية للأمن السيبراني، أي كيفية تطبيقه وفهمه ضمن الممارسات اليومية لهم وذلك بالطريقة التي تتوافق مع أهداف المؤسسة وقيمها.

ومن هنا فالعلاقة بين الاتصال التنظيمي وموضوع الأمن السيبراني تبين أن هذا الأخير لا يمكن حصره في مجموعة من الإجراءات التقنية، إنما يعتبر مجموعة من العمليات الاجتماعية التي تنشأ وتستمر عبر التفاعل والتواصل الفعال في المؤسسة المعاصرة. وهذا يبرز ويوضح البعد الاجتماعي والتنظيمي في نفس الوقت، ويبين كيف تتحول السياسات والإجراءات الرسمية إلى ممارسات فعالة وراسخة عند تطبيقها وفهمها من قبل أفراد التنظيم.

4.2- التفاعل الاجتماعي:

تعددت التعاريف الخاصة بمفهوم التفاعل الاجتماعي ف" يعرفه سعد جلال بأنه علاقة متبادلة بين فردين أو أكثر، يتوقف سلوك أحدهما على الآخر كفردين، أو يتوقف سلوك كل منهم على سلوك الآخرين إذا كانوا أكثر من اثنين" (جامع، 2019، صفحة 144)

أما في بحثنا هذا فالتفاعل الاجتماعي يقصد به العملية التي يتم عبرها تبادل التأويلات والأفعال في المؤسسة، ما يؤدي إلى تنظيم ممارسات الأفراد اليومية وتشكيل سلوكهم. فالتفاعل هو عبارة عن مسار مستمر يتم من خلاله فهم الأدوار وتفسير القواعد وتحديد ما هو مرفوض وما هو مقبول في سياق التنظيم. وعبر هذه التبادلات الرمزية يتحدد أسلوب اشتغال الأفراد في المنظمة وتعاملهم مع القواعد الخاصة بالحماية الرقمية.

ففي سياق الأمن السيبراني يظهر التفاعل الاجتماعي في الكيفية التي بها يفهم الأفراد سياسات الحماية وبالتالي يعيدون إنتاجها بشكل عملي، فلما يناقشون حادثة اختراق حصلت في مؤسسة أخرى أو عندما يتبادلون التحذيرات المعنية بالرسائل المشبوهة، أو حين تلقى تنبيهات من الإدارة لتحديث كلمات المرور، فإنهم يشاركون في عملية جماعية يُبنى من خلالها معنى الأمن، وهم بذلك لا ينفذون فقط أوامر تقنية. ومن خلال تفاعلاتهم اليومية هذه فالقواعد الرسمية تتحول إلى سلوكيات اعتيادية، كما أن الحماية الرقمية تصبح جزءاً لا يتجزأ من الثقافة التنظيمية للمؤسسة.

وفي هذا الصدد فالتفاعل الاجتماعي يمكن اعتباره كعامل تفسيري لكيفية انتقال الأمن السيبراني من السياسات المكتوبة إلى الممارسات الاجتماعية التي تتجسد في العلاقات المهنية، وكيفية تداول الفاعلين للمعاني ومستوى الثقة في المؤسسة المعاصرة.

3- الأمن السيبراني من منظور التنظيم والتفاعل الاجتماعي:

أصبحت المؤسسات في عصرنا الحالي تواجه تحديات منها حماية الموارد الرقمية والمعلومات، وهذا ما يجعل من موضوع الأمن السيبراني من القضايا الحيوية التي تتجاوز البعد التقني وتصبح من الممارسات المتعددة الأبعاد أو الجوانب بحيث يتكامل فيها التفاعل الاجتماعي للعاملين مع التنظيم.

فإذا عدنا إلى البعد التنظيمي، فالأمن السيبراني يمكن اعتباره كإطار وجانب رسمي من خلاله تتحدد الإجراءات، السياسات وكذلك المسؤوليات داخل المؤسسة. فالإدارة في المؤسسة المعاصرة تقوم بوضع قوانين وقواعد واضحة تحدد من خلالها كيفية حماية البيانات، والإجراءات التي يجب أن يتبعها الأفراد في حال حدوث أي خرق أمني أو تهديد، كما توزع من خلالها الصلاحيات وفق الهيكل التنظيمي الوظيفي. ومن أمثلة ذلك في شركة أو بنك تُحدد صلاحيات من أجل الوصول للمعلومات أو الملفات حسب وظيفة كل فرد وهناك أنظمة تحقق متعددة العوامل تُفرض، بالإضافة إلى ذلك فهناك فرق متابعة من مهمتها مراقبة التزام الفاعلين بمختلف السياسات الأمنية. وهذا التنظيم الرسمي يحول الأمن السيبراني إلى شكل من الممارسات الموحدة والهادفة، ويخلق التكامل والتنسيق بين مختلف الأقسام والمستويات في المؤسسة، ما يعكس البعد التنسيقي وكذلك الهيكل للظاهرة.

أما إذا عدنا إلى الجانب الاجتماعي، نجد أن الأمن السيبراني يصبح من بين العمليات الاجتماعية التي يتم إعادة إنتاجها يوميا كما يتم تفسيرها من خلال التفاعل اليومي للأفراد. وهنا نشير إلى أهمية العلاقات والتفاعلات الاجتماعية فيقول غوفمان "التنظيم الاجتماعي هو الموضوع المركزي، ولكن ما يتم تنظيمه هو التداخل بين الأشخاص والعمليات التفاعلية المؤقتة التي يمكن أن تنشأ عن ذلك" (GOFFMAN, 1967, p. 2). لذلك فالتفاعل الاجتماعي يمثل أساس التنظيم، فقد تتشارك فرقة عمل في مؤسسة مصرفية أو شركة تقنية نصائح تبين كيفية التعامل مع مختلف الرسائل البريدية المشبوهة، أساليب التعامل مع التنبيهات اليومية الأمنية أو تبادل الخبرات حول كلمة المرور التي تكون أكثر أمانا. وانطلاقا من هذه التفاعلات تتكون الثقافة المؤسسية المشتركة التي تعكس الأخذ والالتزام بالقواعد التي تحولها بدورها إلى سلوكيات جماعية مستدامة، يصبح من خلالها الموظفون مشاركون في حماية المحيط الرقمي للمنظمة ولا يبقون مجرد منفذين لأوامر الإدارة.

من هذا التركيب يظهر أن الأمن السيبراني ظاهرة مزدوجة، فمن جهة هناك السياسات والإجراءات والقواعد الرسمية التي توضح مسارات وقنوات المسؤولية في المؤسسة وتشكل الهيكل التنظيمي، من جهة ثانية إعادة إنتاج المعاني والتفاعل الاجتماعي يجعل التزام أفراد التنظيم ممارسة مستدامة وحية تعكس من خلالها الثقافة المؤسسية. ومن الأمثلة الواقعية فالمؤسسات المعاصرة توفر منصات للتواصل بين الأفراد من أجل مشاركة الخبرات والنصائح اليومية، كما تعتمد برامج دورية حول الأمن السيبراني. فالقواعد الرسمية تتجسد بشكل واضح، بينما الموظفون يشاركون في إعادة إنتاج الممارسات هذه اجتماعيا. وهكذا يصبح الأمن السيبراني من الممارسات المستمرة في المؤسسة التي تجمع بين الالتزام الاجتماعي والانضباط التنظيمي، كما يصبح جزءا لا ينفصل عن الهوية المؤسسية وثقافتها.

1.3- الأمن السيبراني كنتاج لفعالية الاتصال:

في نظر برنارد تشستر، فإن المنظمة تعتبر عبارة عن نظام تعاوني، والذي يتكئ على فاعلية التعاون بين مختلف الأعضاء الذين يشكلونه، واستمراره يتوقف على الوسائل اللازمة لتحقيق أهدافه. فالمنظمة وفقا لفكره تعبر عن نظام من القوى الشخصية أو الأنشطة التي يتم تنسيقها بشعور ووعي. ووفقا لذلك فهي تعتبر فرعاً أو جزءاً من نظام أكبر، والذي يشكل علاقة متفاعلة بين الأجزاء التي تكونه. وللعنصر البشري أهمية جمة تتمثل في بناء العلاقات التعاونية التي تسود في المنظمة (الشماع و خضير، 2007، صفحة 90).

ووفقا لتصور برنارد تشستر في النظام التعاوني، فإن المؤسسة تمثل شبكة معقدة من الاتصالات بمختلف أنواعها والتي تضمن التنسيق بين الأنشطة المتنوعة وتحقيق أهداف المؤسسة، كما تشكل الهيكل التنظيمي لها. ومن هذه الرؤية، فالأمن السيبراني يصبح من الأجزاء الجوهرية في البنية التنظيمية داخل المؤسسة سيما المعاصرة منها. فلا يمكن أن تطبق سياسات حماية البيانات والمعلومات الرقمية بشكل فعال إلا إذا كانت عملية توصيلها تتم بوضوح وسلاسة عبر قنوات المؤسسة المختلفة، وكيفية متابعة التقيد والالتزام بها، وتحديد المسؤولين على تنفيذها.

"ولهذا طالب تشيستر برنارد بضرورة التعاون بين الرؤساء والمؤوسين وقيام نظام تشاوري بين العمال والإدارة بقصد الحصول على موافقة العاملين على السياسات المنتهجة في العمل، وكذلك إيجاد توازن بين ما يقدمه العامل للمنظمة في شكل عمل، وقت، ولاء...وبين ما يحصل عليه من المنظمة في شكل راتب، سمعة وحوافز". (بوحوش، 2016، صفحة 24)

ويقسم تشستر الاتصال إلى أنواع عدة داخل المؤسسة، بحيث أن كلا منها له دور أساسي ومحوري يدعم الأمن السيبراني وهي:

- الاتصال الرسمي العمودي:

. ومن أشكال الاتصال الرسمي التي يتخذها نجد الاتصال العمودي الذي يجري عبر السلم الهرمي للتنظيم. وهذا النوع من الاتصال يتدفق عبر قنوات رسمية مثل السياسات المكتوبة، التعليمات، الاجتماعات الدورية وذلك من الإدارة إلى الموظفين. ومن أمثلة ذلك أن تقوم الإدارة في بنك معاصر بإصدار تعليمات واضحة حول إجراءات النسخ وإعداد الكلمات المفتاحية وكيفية التعامل مع البريد الإلكتروني الذي فيه شهادات، وتتابع كذلك الفرقة الإدارية الالتزام بهذه التعليمات والإجراءات، وهذا ما يضمن تطبيق سياسات الأمن بدقة كما يعكس التحكم التنظيمي في هذه المؤسسة.

- الاتصال الأفقي:

وهذا النوع من الاتصال يجري في نفس المستوى التنظيمي بين زملاء العمل من أجل التنسيق الفعال للأنشطة وتنفيذ الإجراءات والتعليمات المشتركة، فالمعلومات حول وجود تهديدات محتملة قد يتبادلها فريق العمل، ويضع

الاستراتيجيات المختلفة من أجل التعامل مع الرسائل الاحتياطية، أو يستطيع مشاركة طرق الحماية للأجهزة المتنوعة للعمل. وهذا الشيء يضمن التطبيق العملي للسياسات الأمنية بشكل فعال كما يعزز الانسجام والتعاون بين مختلف الأقسام في المنظمة.

- الاتصال غير الرسمي:

ويشمل هذا النوع المبادرات التلقائية والعفوية بين الموظفين والمحادثات اليومية التي تكون خارج الإطار الرسمي، ويعد بذلك من الوسائل الفعالة لنشر الوعي بشكل سريع وكذلك نقل المعارف بين الأفراد في التنظيم. ونعطي مثال هنا، فالموظفون مثلاً قد يتشاركون حلولاً لمواجهة الثغرات الأمنية أو البرامج المبتكرة المختلفة للحماية، وهكذا تنتقل الخبرات بشكل سلس وسريع، ويصبح الأمن السيبراني من بين الممارسات اليومية المتجذرة في الثقافة الجماعية للعمل.

- الاتصال التبادلي أو التغذية الراجعة:

هذا النوع يسمح للموظفين بالتصريح عن الصعوبات أو المشاكل التي تواجههم عندما يطبقون الإجراءات الأمنية، وهذا يُمكن الإدارة أن تقدم تدريبات إضافية من أجل الالتزام بمختلف المعايير المتعلقة بالأمن، وتعديل السياسات. مثال على ذلك، فلما يتم اكتشاف ثغرة أو فجوة في أنظمة الحماية للبيانات الرقمية، يمكن للموظفين أن يقدموا شتى ملاحظاتهم، فتقوم الإدارة باتخاذ خطوات تصحيحية، وهذا يعكس قدرة الاتصال التنظيمي على التطوير المستمر والمستدام ويعكس مرونته.

ومن هذا التوزيع والتنوع المتكامل والمتراكب للاتصالات في المؤسسة، تتضح لنا الرؤية بأن الأمن السيبراني لا يمكن اعتباره مجرد قواعد وقوانين رسمية جامدة، إنما ممارسة تنظيمية حيوية وحية. فالاتصالات الأفقية في نفس المستويات تمكن من تعزيز التعاون بين مختلف الفرق، والقواعد والقوانين الرسمية تحدد المسؤوليات، كما تساهم الاتصالات غير الرسمية في تبادل الخبرات، وتتطور السياسات بشكل مستمر من خلال التغذية الراجعة. وهكذا فالأمن السيبراني يصبح من بين الأجزاء التي لا تتجزأ من هيكل المؤسسة التنظيمي، ويعتمد على فعالية العملية الاتصالية بين الإدارة والموظفين، ويترجم وجود شكل من أشكال التنسيق المتكامل بحيث يضمن استدامة الممارسات الأمنية في البيئة المهنية والحماية للمعلومات الرقمية في بيئة العمل الوظيفية.

ونظرية برنارد تشستر في النظام التعاوني تعزز القيم الإنسانية مثل الثقة، التعاطف، الاحترام بين الأفراد. فحينما يكون العمل بين الناس غايته تحقيق أهداف مشتركة، فإن شعورهم بالتضامن والانتماء يزداد، وهذا ما يجعل المجتمع أكثر تعاوناً وتوافقاً، ويحس الأفراد بأنهم جزء منه. (القريوتي، 2008، صفحة 85)

2.3 - الأمن السيبراني كمعنى يُبنى يومياً:

قبل تحليل والدخول في موضوع الأمن السيبراني وفق التصور التفاعلي الرمزي، لابد أن نقدم لمحة مختصرة عن هذه النظرية، حيث يمكن أن نقول أنها تأسست على يد جورج هربرت ميد وطورها فيها بعد هيربرت بلومر الذي

يؤكد بدوره أن "ميد أكثر من أي من الآخرين وضع أساس هذا الاتجاه، رغم أنه لم يطور ما ينطوي عليه من منهجية للدراسات الاجتماعية" (الخوراني، 2008، صفحة 28). واهتمام بلومر ينصب بشكل أساسي على أن المجتمع يُبنى من خلال التفاعلات اليومية للأفراد ولا يُبنى فقط من خلال القوانين والقواعد الثابتة أو الجامدة. ووفق هذا التصور، فالمعاني الاجتماعية تُنتج ويُعاد إنتاجها بشكل مستمر من خلال تفسير الأفراد للمعاني والقواعد والرموز والسلوكيات التي يواجهونها في الحياة العملية. وهكذا فالسلوك لا يمكن حصره على أنه مجرد تنفيذ للأوامر فقط، إنما ممارسة لها معنى يتم تطويرها وتداولها اجتماعيا.

وإذا عدنا إلى موضوع الأمن السيبراني في المؤسسة، يتضح جليا أن تطبيق القواعد والالتزام بها لا يمكن أن يكون عبارة عن تنفيذ عقيم للقوانين، بل إنتاج يومي للوعي الأمني وللمعنى من خلال التفاعلات الاجتماعية المهنية. فأفراد التنظيم يفسرون القواعد والقوانين الرسمية ويكيفونها بشكل يتوافق مع طبيعة عملهم، كما يقومون بإعادة إنتاجها ضمن ممارساتهم اليومية. وهذا ما يؤدي لتحويلها إلى جزء من سلوكياتهم المهنية. ففي شركة تقنية ما مثلا إذا قام فريق بتبادل التعليمات والنصائح حول الكيفية التي يتم من خلالها التعرف على الرسائل الالكترونية الاحتمالية، أو الكلمات المفتاحية أو طرق الحماية بشكل يتناسب مع المهام اليومية لهم. وهذه التفاعلات التي تتم بشكل يومي، ينشئ من خلالها الفهم الجماعي لمعنى الالتزام بالأمن السيبراني. ويصبح بذلك جزءا من الثقافة المهنية المتجذرة والمشاركة في بيئة العمل.

ضف إلى ذلك، فهذه المعاني الاجتماعية تتحول بشكل تدريجي إلى ثقافة متجذرة في المؤسسة. وغالبا ما تقوم فرق العمل في المؤسسة ورشات عمل وجلسات تدريبية من أجل مراجعة السياسات الأمنية، كما يتم إنشاء المنصات التي من خلالها يتم تبادل الممارسات العملية والخبرات بين الأفراد، وهذا يعزز إعادة الإنتاج للمعارف الأمنية اجتماعيا في المؤسسة. والنتيجة فالأمن السيبراني يصبح ممارسة مستدامة ومتكاملة وديناميكية في حياة المؤسسة اليومية، فالجميع يشارك في الحفاظ عليه وإنتاج معناه.

وفي هذا الصدد، فإن الأمن السيبراني في المؤسسة المعاصرة يظهر كظاهرة اجتماعية تفاعلية، تعتمد على التواصل الفعال بين أفراد التنظيم، التفسير اليومي للقوانين والقواعد، إعادة إنتاج الممارسات وغيرها، وهكذا فإن السلوك الأمني يكتسب معنى جماعيا وثقافة تنظيمية صلبة ومتينة، "وتعد الثقافة التنظيمية عنصرا أساسيا في المنظمات المعاصرة يفرض على القادة ومديرها أن يفهموا أبعادها وعناصرها الفرعية لكونها الوسط البيئي الذي تعيش فيه المنظمات، فالثقافة التنظيمية نتاج ما اكتسبه العاملون من أنماط سلوكية وطرق تفكير وقيم وعادات واتجاهات ومهارات تقنية قبل انضمامهم للمنظمة التي يعملون فيها." (بركان و جليد، 2017، صفحة 176). وهكذا فهذا التفاعل المستمر يضمن استدامة الممارسة الأمنية، فعالية القوانين والقواعد الرسمية، وتعزيز الوعي بأهمية الحماية لمختلف الموارد والوسائل الرقمية، وهكذا يصبح الأمن السيبراني جزءا هاما وأساسيا من ثقافة المؤسسة اليومية ومن هويتها.

4- التحديات الاجتماعية والتنظيمية المرتبطة بالأمن السيبراني:

إن دراسة موضوع الأمن السيبراني تحيل إلى أن الباحث يجب عليه الانتباه إلى مختلف العراقيل والتحديات، وسنركز في بحثنا هذا حول التحديات التنظيمية والاجتماعية منها دون غيرها، لأن الهدف ليس أن نحلل مختلف الجوانب الهندسية أو التقنية للحماية الرقمية، إنما كي نكشف أن الحماية الرقمية لا تعتبر قراراً فورياً، إنما نتيجة لتفاعلات دينامية للفاعلين الاجتماعيين في المؤسسة المعاصرة، ووفقاً لذلك فسوف نتطرق إلى أبرز هذه التحديات.

1.4- التحديات التنظيمية:

قبل عرض كل تحدٍ تنظمي كل على حدة فإن التحديات التنظيمية تعكس باختصار تعقيد المؤسسة المعاصرة البنوي، ومسؤوليات على نطاق واسع، وهذا ما يلزم بتطبيق سياسات الأمن السيبراني بشكل حساس ودقيق فالبيئة التنظيمية المعاصرة تتداخل فيها مختلف المستويات الإدارية ولا تقتصر على التسلسل الهرمي الصارم، وهناك مسؤوليات وصلاحيات مختلفة ومحددة يتحملها كل مستوى. مما يجعل انتقال التعليمات الأمنية والمعلومات تحدياً كبيراً، فأي خلل أو التباس في الاتصال أو عدم الفهم قد ينجر منه تنفيذ خاطئ أو جزئي للإجراءات، وهذا ما يخلق ثغرة بين الممارسة الفعلية والقواعد الرسمية. ومن أبرز التحديات التنظيمية ما يلي:

- تحدي فعالية الاتصال

"عملية الاتصالات في المنظمات عملية معقدة-معقدة لأننا كأفراد لنا خصوصيتنا، وتحيزنا، وقدراتنا. ومعقدة بوجود الخصائص التنظيمية مثل التسلسل الهرمي والتخصصية ومع ذلك، فالاتصالات داخل المنظمات رئيسية بالنسبة للعمليات الأخرى كالقوة، والقيادة، وصناعة القرار، وتشكل الاتصالات بواسطة الهيكل التنظيمي وتستمر في تشكيل الهيكل." (هال، 2001، صفحة 411) فمن شروط وجود السياسة الأمنية هو توفر الاتصال الفعال، إلا أن واقع المؤسسة يظهر أن التعليمات لا تتم بالصورة التي تتخيلها الإدارة دائماً، فقد تبدو الرسائل واضحة في قمة الهرم التنظيمي، غير أنها وأثناء عبورها أو مرورها عبر مختلف المستويات الإدارية قد تخضع للقصور أو الإهمال حتى وإن لم يكن مقصوداً، أو تتعرض لإعادة التبسيط والتفسير. "ونتيجة لهذه التأثير يمكن أن تضخم لبعض المعلومات أو إخفاء بعض المعلومات أثناء انتقالها في سلسلة الاتصالات. والتصفية للمعلومات لا تتم فقط عند تدفق المعلومات من أعلى لأسفل ولكن أيضاً يمكن أن تتم أثناء انتقال المعلومات من أسفل لأعلى" (المغربي، 2020، صفحة 16)

ومع تعدد المصادر التوجيهية، فالموظفون قد يفقدون القدرة والكفاءة على التمييز بين الثانوي والجوهري، وهذا ما يؤدي بتحول القواعد إلى تعليمات روتينية لا تدفع الأفراد إلى ضرورة الالتزام بها. وهذا ما يخلق التفاوت في تطبيقها، بحيث يمكن لبعض الأفراد بأن يتقيدوا بها بشكل دقيق، أما آخرون فيكتفون بالحد الأدنى حيث يسمح

لهم ذلك بالاستمرار في العمل. ومن هنا يظهر أن الأمن السيبراني يعتمد بشكل أساسي على جودة وفعالية العملية الاتصالية التي تعطيها المعنى وتضمن الاستيعاب المشترك لها، ولا يعتمد على وجود القواعد فقط.

- تحدي المسافة بين الممارسة الفعلية والنص الرسمي

إن الحياة العملية اليومية تُظهر فروقات بين ما يحصل في الواقع وبين السياسات المكتوبة. ففي العمل هناك علاقات وضغوط قد تدفع بالأفراد في بعض الأحيان إلى تعديل السلوك بشكل يسمح بإنجاز مهامهم بسرعة كبيرة. وقد تتحول إلى أعراف مع تكرار هذه التعديلات، ويتم تداولها في التنظيم، وهكذا تتشكل ثقافة يمكن ألا تكون في تناسق وانسجام مع القواعد المعلنة. ومن هنا فالأمن السيبراني يصبح كنتيجة توازنات مستمرة بين ما يعتبره الموظفون ممكنا وعمليا في ظروفهم اليومية وبين ما تريده الإدارة في المؤسسة.

- تحدي التكيف مع التغيرات المستمرة

المجال الرقمي من مميزاته الحركية، لذلك فالمؤسسات تعرف تحديثا دائما ومستمرًا لمختلف إجراءاتها. فالتغيير في المنظمة عبارة عن عملية مستمرة عبر الزمن وليس عملية ثابتة، في هذا الصدد فجون كوتريناكش في كتابه "Leading change" وفي بداية الفصل الأول منه بأن عملية التحول في المنظمات هي عملية مستمرة وتستغرق مراحل وتحتاج الى وقت وتخطيط وكذلك المشاركة الفعالة من أفراد التنظيم، وليست حدثا عابر تحدث دفعة واحدة (KOTTER, 2012).

إلا أن هذا التحديث قد يولد إحساسا بعدم الاستقرار لدى الأفراد، خاصة عندما لا يرافقه التفسير الوافي والكافي للأسباب التي تشكله أو التدريب والتكوين المناسب على طرق تطبيقه. فأفراد التنظيم يبنون العادات المهنية التي يمكن أن تمنحهم الشعور بالفعالية والكفاءة، وأن أي تغيير مفاجئ قد يؤدي إلى تهديد هذا الاستقرار والتوازن. ومن هذا يبدو أن الأمن السيبراني لا يمكن اعتباره مجرد تجديد أو تحديث تقني، إنما يعتبر من بين العمليات الاجتماعية التي تعيد بناء العادات المهنية في محيط العمل والتي تحتاج إلى تواصل ووقت وافي وإقناع.

2.4 - التحديات الاجتماعية:

التحديات التي ترتبط بالأمن السيبراني تتجاوز البعد الاجرائي والتقني في المؤسسة المعاصرة، لتصل لعمق بنيتها الاجتماعية، حيث أن المعايير الأمنية والالتزام بالقواعد تتشكل من خلال تبادل المعاني بين الموظفين، التفاعلات اليومية، وبناء التصورات والتفسيرات المشتركة حول ما هو غير مقبول وما هو مقبول. فالأمن الرقمي يمكن اعتباره نتيجة لعملية تفاعل فيها وتنتج باستمرار ممارسات الأفراد عبر الاتصال والحوار غير الرسمي وتقديراتهم حول فعالية الإجراءات وقياساتهم الذاتية للمخاطر، ولا يمكن اعتباره مجرد مجموعة من التعليمات فقط. بناء على هذا الفهم نجد أن دراسة التحديات الاجتماعية تعتبر ذات أهمية كبرى في فهم كيفية تحول الأمن السيبراني من قاعدة رسمية إلى ممارسات فعلية ومدمجة في الثقافة المهنية اليومية، وتبين كيف أن هناك تفاعل للقيم

والتمثلات والمعايير لكي ينتج في الأخير الواقع الأمني المستدام في المؤسسة المعاصرة. ومن بين التحديات الاجتماعية ما يلي:

- تحدي بناء المعاني المشتركة بين الفاعلين

الأمن السيبراني لا يحمل نفس المعاني لدى كل الفاعلين من الناحية الاجتماعية، فبعضهم ينظرون إليه باعتباره يوفر استقرار المؤسسة ويضمن مستقبلها، بينما يعتبره آخرون مجرد عبء ثقيل وإضافي يفرض قيودا على المرونة والسرعة. فيقول ويليام توماس: "إذا عرف الأفراد الوضعيات كحقيقة، فإنها تصبح حقائق في انعكاساتها". (THOMAS, 1976, p. 572)

هذا الاختلاف في تمثيلات الأفراد يحول الالتزام بالقاعدة الأمنية إلى قناعات جماعية تتشكل عبر التفاعل والنقاش ويحولها إلى موضوع للتفاوض اليومي، وليس عبر الأوامر الإدارية فقط. وهكذا ففي حال غياب هذا المعنى المشترك، تصبح الإجراءات هشة التطبيق، ويمكن تجاوزه في كل مرة تبرز فيه ضغوط العمل أو ضرورة تحقيق سرعة النتائج. وفي هذا الصدد فإن التحديات الحقيقية تكمن في أن تكون للمؤسسة قدرة على أن تخلق وتتبنى تصورا موحدا بواسطته يكون للأمن السيبراني القيمة المهنية التي يعمل بها ويتبنّاها الجميع في المؤسسة.

- تحدي الانتقال إلى الثقافة

هناك العديد من المؤسسات سيما المعاصرة منها، تبقى كأسيرة لمنطق تفرضه الرقابة، بحيث أن الأمن السيبراني يُمارس بسبب الخوف من العقوبات أكثر مما يكون مُمارسا من قناعات داخلية للأفراد. إلا أن هذا النوع لا يضمن الاستمرارية، فالالتزام سرعان ما يتراجع بغياب عنصر الرقابة. أما التغير الحقيقي فيكون عندما يصبح الأمن جزءا لا يتجزأ من الثقافة المهنية. بمعنى أوضح، عند اندماجه في تصورات الموظفين اليومية حول ما هو سلوك مسؤول ومقبول. ولكي تبني المؤسسة هذه الثقافة فيتطلب ذلك استثمارا طويلا المدى في التدريب والتواصل والتكوين وتمكين المبادرات، وذلك حتى يحس الأفراد بالشراكة في الحماية ولكي يتجنبوا شعور الخضوع لها. وفي ذات المعنى يقول سانج "المنظمات لا تتعلم إلا من خلال الأفراد الذين يتعلمون". (SENGE, 1990, p. 139)

- تحدي الشرعية والثقة

تمثل الثقة دورا بارزا ومهما ومحوريا، فهي تحدد درجة انخراط الأفراد في السياسات الأمنية. فالموظفون إذا اعتبروا بأن الإجراءات والتعليمات تهدف بشكل فعلي إلى حماية الجميع في المؤسسة، فإنهم يتعاونون ويقومون بمبادرات. بالعكس، فإذا ارتبطت في تصوراتهم بالتشكيك في قدراتهم وكفاءتهم وكذلك بالمراقبة، فهنا يميلون إلى نوع من الالتزام الذي يتسم بالشكلية ونوع من التحايل غير المعلن وهنا يبرز عنصر هام وهو الثقة التنظيمية، بحيث "تذكر أدبيات الثقة التنظيمية أنها العلاقات المتبادلة التي تتواجد عندما يكون طرف محدد لديه ثقة في تكامل واعتمادية الطرف الآخر المشارك. والثقة هي التوقعات التي تنشأ داخل الجماعة الدائمة، والأمانة، والسلوك التعاوني والذي يبني على مشاركة العادات المألوفة كجزء من معتقدات الجماعة" (برطال، 2022، صفحة 343).

ومن هنا فالأمن السيبراني في المؤسسة يصبح مرآة تعكس طبيعة العلاقات الاجتماعية القائمة، كما أن نجاحه سيتوقف على الشعور الجماعي المشترك بأن القواعد عادلة وضرورية، ف"الأفراد الجدد يتعلمون المعاني المشتركة من خلال عملية التطبيع الاجتماعي، سواء أكان ذلك من خلال التدريب الرسمي أم التفاعل غير الرسمي بين الأعضاء. لهذا فإننا كأفراد داخل المنظمة نتعلم كيف نفكر وكيف نتصرف مثل بقية الأعضاء" (الفروخ، 2010، صفحة 28)

5- الخلاصة:

إن التحليل السوسيولوجي لموضوع الأمن السيبراني في المؤسسة المعاصرة، أظهر أن المسألة لا تُختزل في البعد الاجرائي أو التقني، إنما تتجاوز ذلك، فهي عبارة عن سيرورة اجتماعية وتنظيمية معقدة تتداخل فيها تمثيلات الأفراد، شبكات الاتصال وطبيعة العلاقات والتفاعلات المهنية. كما بينت هذه الورقة البحثية أن الحماية الفعلية الرقمية في المؤسسة لا يمكن أن تتحقق بمجرد توفير وسائل أو إصدار قوانين، ولكن لها ارتباط أساسي بقدرة الفاعلين على تداول وفهم القواعد مع إعادة إنتاجهم لها ضمن الممارسات اليومية. فمن خلال التفاعل الدائم والمستمر يتشكل الأمن السيبراني في الواقع، وتمنح التعليمات المعاني المختلفة التي تضعف الالتزام أو تعززه وفقا للسياق التنظيمي والاجتماعي.

كما أن المناقشة كشفت أن المؤسسة المعاصرة تواجه تحديات تتمحور أساسا حول بناء المعنى المشترك، فعالية الاتصال، مرافقة التغيير، ترسيخ الثقافة، وتقليص المسافة أو الفجوة بين الممارسة والنص. وكل هذه العناصر تبين أن الأمن السيبراني ليس في حالة جمود وثبات، إنما هو عبارة عن بناء في تجدد دائم ويتكى على العلاقات الإنسانية الدينامية في بيئة العمل. ومن هنا فالسياسات مهما بلغت من تطور تقني، فإنها تبقى محدودة التأثير إذا لم تراعي هذا الجانب الاجتماعي.

ومن هذه النتائج التي توصلنا إليها، سنقترح مجموعة من الاقتراحات والتوصيات التي بإمكانها أن تعزز الفعالية الأمنية السيبرانية في المؤسسة المعاصرة وهي:

- ضرورة الاستثمار في تطوير القنوات الاتصالية لتتسلسل الرسائل بشكل واضح.
- تبادل التغذية الراجعة وذلك بين المستويات التنظيمية المختلفة.
- تشجيع الآليات التشاركية في تصميم وتفعيل الإجراءات الأمنية وذلك بإدماج الأفراد فيها، لتعزيز الإحساس بالانتماء والمسؤولية.
- تحويل الأمن السيبراني إلى ثقافة مؤسسية مهنية من خلال التدريب المستمر والتكوين وتعزيز السلوكيات الإيجابية عوض اللجوء لمنطق العقوبة.
- تامين الشفافية والثقة في الإجراءات وفي تطبيقها بدل العقاب والرقابة.

وانطلاقاً من هذا، يتبين في الأخير أن المقاربة السوسيولوجية تقوم بتقديم إضافة نوعية للمجال المتعلق بالأمن السيبراني، لأنها تكشف وتُظهر بحق أن الحماية الرقمية لا يمكن اعتبارها مسألة تقنية أو قضائية أدوات ووسائل فقط، إنما هي قبل كل شيء تتعلق بالمعنى والتفاعل والتنظيم، أي مسألة اجتماعية وإنسانية بامتياز.

6- المراجع:

- 1- الأمين مرتضى البشير، (2016). الاتصال التنظيمي، الأردن: دار أمواج للنشر والتوزيع.
- 2- الحوراني، عبد الكريم، (2008). النظرية المعاصرة في علم الاجتماع، الأردن: دار مجدلاوي للنشر والتوزيع.
- 3- الحوش سليمان مازن، (2024). "المؤسسة الجزائرية بين النظرية والتطبيق". مجلة الباحث في العلوم الإنسانية والاجتماعية، جامعة قاصدي مرباح ورقلة، المجلد 16 (العدد 04)، ص.ص 79-94.
- 4- الشماع، خليل محمد حسن وخضير كاظم محمود، (2007). نظرية المنظمة، الأردن: دار المسيرة.
- 5- الفروخ فايز عبد الرحمن، (2010). التعلم التنظيمي وأثره في تحسين الأداء الوظيفي، الأردن: دار جليس الزمان للنشر والتوزيع.
- 6- القريوتي، محمد قاسم، (2008). نظرية المنظمة والتنظيم، الأردن: دار وائل للنشر والتوزيع.
- 7- المغربي بشير محمود محمد الفاتح، (2020). الاتصال التنظيمي، مصر: دار حميثرا للنشر.
- 8- بركان أسماء وجليد نور الدين، (2017). "أثر الثقافة التنظيمية على الابداع الإداري". مجلة الاقتصاد الجديد، جامعة ابن خلدون -تيارت، المجلد 02 (العدد 17)، ص.ص 175-184.
- 9- بن برطال عبد القادر، (2022). "الثقة التنظيمية كمتغير وسيط في العلاقة بين إدارة المعرفة وتحسين أداء هيئة التدريس لدى أساتذة كلية العلوم الاقتصادية-جامعة الأغواط-". مجلة البحوث الاقتصادية المتقدمة، جامعة عمار ثليجي- الأغواط، المجلد 07 (العدد 02)، ص.ص 340-357.
- 10- بن جامع صبرينة، (2019). "التفاعل الاجتماعي-دراسة نظرية تشخيصية". مجلة التكامل، (العدد 05)، ص.ص 142-177.
- 11- بن مرزوق، عنتره وحرشاي، محي الدين، (2017). "الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية". مجلة دفاتر السياسة والقانون، جامعة قاصدي مرباح، ورقلة، المجلد 02 (العدد 02)، ص.ص 65-80.
- 12- وحوش، عمار، (2016). نظريات الإدارة الحديثة في القرن الواحد والعشرين، لبنان: دار الغرب الإسلامي.
- 13- بوفلجة، غياث، (1992). مقدمة في علم النفس التنظيمي، الجزائر: ديوان المطبوعات الجامعية.
- 14- شلوش، نورة، (2018). "القرصنة الالكترونية في الفضاء السيبراني، التهديد المتصاعد لأمن الدول". مجلة مركز بابل للدراسات الإنسانية، جامعة بابل- العراق، المجلد 08 (العدد 06)، ص.ص 206-285.
- 15- هال ريتشارد، 2001، المنظمات، هياكلها، عملياتها، ومخرجاتها، ترجمة سعد بن حمد الهاجري، المملكة العربية السعودية: معهد الإدارة العامة.

- 16- GOFFMAN Erving, (1967). Interaction Ritual: Essays on Face-to-Face Behavior, USA: Alding Publishing Company.
- 17- KOTTER Paul John, (2012). Leading change: why transformation efforts fail, USA: Harvard businness review press.
- 18- SENGE Peter Michael, (1990). The fifthe disipline: the art & practice of the Learning organization, USA: Currency/Doubleday.
- 19- THOMAS William Ishaac & THOMAS Dorothy, (1976). The child in America: Behavior Problems and Programs, USA: Alfred A. Knopf.

كيفية الاستشهاد بهذا المقال حسب أسلوب APA :

فجييري حسيبة ، (2026)، الأمن السيبراني كظاهرة اجتماعية وتنظيمية في المؤسسة المعاصرة ، مجلة أنسنة للبحوث والدراسات، المجلد 17 (العدد 1)، الجزائر : جامعة زيان عاشور الجلفة، ص.ص 113-99.