Afro-Asian Journal of Scientific Research (AAJSR)
المجلة الأفروآسيوية للبحث العلمي
E-ISSN: 2959-6505
Volume 3, Issue 4, 2025
Page No: 55-62
Website: https://aajsr.com/index.php/aajsr/index
SJIFactor 2024: 5.028 ISI 2025: 0.915 معامل التأثير العربي (AIF) 2025: 0.76

Digital Transformations and Cybersecurity: A Sociological Approach to Understanding Digital Threats and Their Social Dimensions

Souad Naji Yousef Al-Zrebi *
Department of Sociology, Faculty of Arts and Languages, University of Tripoli, Tripoli, Libya

التحولات الرقمية والأمن السيبراني: مقاربة سوسيولوجية في فهم التهديدات الرقمية وأبعادها الاجتماعية

سعاد ناجي يوسف الزريبي *
قسم علم الاجتماع، كلية الآداب واللغات، جامعة طرابلس، طرابلس، ليبيا

*Corresponding author: s.ezrebi@uot.edu.ly

Received: July 08, 2025 | Accepted: October 11, 2025 | Published: October 20, 2025

Abstract:
This research explores cybersecurity from a sociological perspective, emphasizing that digital threats have evolved beyond technical challenges to become complex social phenomena affecting societal structure and stability. The study adopts an analytical approach using conflict and structural functionalist theories to interpret the dynamics of cybersecurity within the digital transformation era. The findings indicate that cybersecurity reflects ongoing struggles over power and knowledge, while the digital divide among nations and social groups reveals new forms of inequality. In the Libyan context, weak institutional structures heighten vulnerability to cyber threats, underscoring the need for a comprehensive approach that transcends purely technical solutions. The study recommends developing a national cybersecurity strategy that integrates social and cultural dimensions, enhancing digital awareness, and promoting sociological research on cybersecurity to strengthen societal resilience in the digital age.

Keywords: Digital Transformations, Cybersecurity, Sociological Approach, Digital Threats, Social Dimensions.

الملخص
يتناول هذا البحث موضوع الأمن السيبراني من منظور سوسيولوجي، انطلاقًا من أن التهديدات الرقمية لم تعد قضايا تقنية بحتة، بل تحولت إلى ظواهر اجتماعية تمس بنية المجتمع واستقراره .اعتمدت الدراسة المنهج التحليلي النقدي لتفسير الظاهرة من خلال توظيف نظريتي الصراع والبنيوية الوظيفية، وربطهما بالتحولات الرقمية المعاصرة .أظهرت النتائج أن الأمن السيبراني يمثل امتدادًا لصراعات القوة والمعرفة في المجتمع، وأن الفجوة الرقمية بين الدول والفئات الاجتماعية تعكس أشكالًا جديدة من عدم المساواة .كما تبين أن ضعف البنية المؤسسية في السياق الليبي يزيد من هشاشة الأمن السيبراني ويجعل الحاجة ملحّة لاعتماد مقاربة شمولية تتجاوز البعد التقني .وأوصى البحث بضرورة صياغة استراتيجية وطنية للأمن السيبراني تراعي الأبعاد الاجتماعية والثقافية، وتعزيز الوعي الرقمي، ودعم البحث العلمي المتخصص في البعد السوسيولوجي للأمن الرقمي، بما يسهم في تحقيق الأمن المجتمعي في العصر الرقمي.

الكلمات المفتاحية: التحولات الرقمية، الأمن السيبراني، مقاربة سوسيولوجية، التهديدات الرقمية، الأبعاد الاجتماعية.

المقدمة

في ظل التحولات الرقمية المتسارعة التي يشهدها العالم المعاصر، أصبح الأمن السيبراني أحد القضايا المحورية التي تتقاطع مع الأبعاد الاجتماعية والسياسية والاقتصادية. فقد أدى التوسع في استخدام الإنترنت والتقنيات الذكية إلى إعادة تشكيل أنماط التفاعل البشري، ليس فقط على مستوى التواصل الشخصي، بل أيضًا في مجالات التعليم، الاقتصاد، والخدمات الحكومية. وبقدر ما وفرت الثورة الرقمية فرصًا هائلة للنمو والتطور، فإنها حملت في طياتها مخاطر متزايدة تتعلق بالجرائم الإلكترونية والهجمات السيبرانية، الأمر الذي جعل حماية الفضاء الإلكتروني قضية أمن قومي وأمن اجتماعي في آن واحد (لاداده، 2021، ص. 45).

يشير لاداده إلى أن "الأمن السيبراني لم يعد مجرد مسألة تقنية، بل أصبح قضية اجتماعية بامتياز، نظرًا لتأثيره المباشر على استقرار المجتمعات وحماية الأفراد" (لاداده، 2021، ص. 45). ويتأكد هذا التوجه في ظل تشكل مفهوم "المجتمع الشبكي "الذي أشار إليه(Castells, 2010) ، حيث أصبحت الحياة اليومية للأفراد، من التجارة إلى الصحة والتعليم، مرهونة بسلامة الفضاء الرقمي. ومن هذا المنطلق، يبرز البعد السوسيولوجي للأمن السيبراني كمدخل حتمي لفهم الديناميات الاجتماعية المصاحبة للتوسع الرقمي، مثل أنماط السلوك الإجرامي عبر الإنترنت، وتغير القيم، وتبدل أشكال الضبط الاجتماعي، وخصوصاً كيفية تشكيل الهوية الرقمية في هذا الفضاء.

كما أن توظيف النظريات الاجتماعية المعاصرة، مثل نظرية الصراع والبنيوية الوظيفية، يتيح إطارًا تحليليًا لفهم كيفية تفاعل القوى الاجتماعية مع التحديات الأمنية في الفضاء الرقمي. ففي سياق نظرية الصراع، يمكن النظر إلى الهجمات السيبرانية كأداة يستخدمها فاعلون مختلفون لفرض الهيمنة أو تقويض سلطات قائمة، بينما تركز البنيوية الوظيفية على الدور التكاملي للأمن السيبراني في الحفاظ على توازن النظام الاجتماعي.

إن دراسة الأمن السيبراني من منظور اجتماعي لا تقتصر على رصد التهديدات، بل تمتد إلى تحليل تأثيراته العميقة على البنى والمؤسسات والقيم. وهذا ما يجعل هذا البحث يسعى إلى تقديم قراءة تحليلية معمقة لهذه الظاهرة، مستندة إلى مقاربات نظرية رصينة لفهم أبعادها المعاصرة وكيفية مواجهتها في السياقات المحلية والعالمية.

أولاً: مشكلة البحث

رغم التقدم الكبير في مجال تقنيات الحماية الرقمية، فإن التهديدات السيبرانية تزداد تعقيدًا وانتشارًا، مما يطرح تساؤلات جدية حول كفاية المقاربات التقنية والأمنية البحتة في التصدي لها. فالحلول التقنية وحدها أثبتت عجزها أمام الدوافع البشرية والاجتماعية التي تقف وراء الهجمات. فالهجمات الإلكترونية لم تعد حكرًا على الأفراد أو الجماعات الصغيرة، بل باتت أدوات استراتيجية في النزاعات السياسية والاقتصادية، مستهدفة البنى التحتية الحيوية مثل أنظمة الطاقة، والمصارف، والمطارات، وحتى مؤسسات الدولة السيادية (الزعبي والمنصة، 2010، ص. 112).

تشير الدراسات إلى أن التطور التكنولوجي السريع يخلق فجوة بين قدرات المهاجمين والقدرات الدفاعية للمؤسسات، مما يشكل بيئة خصبة لظهور أشكال جديدة من الجريمة المنظمة في الفضاء الإلكتروني (الزعبي والمنصة، 2010، ص. 112). كما تؤكد الدراسات الأجنبية (Rogers, 2019, p.78) أن التهديدات السيبرانية ليست مجرد مشكلة تقنية، بل هي بالضرورة انعكاس لصراعات اجتماعية واقتصادية وسياسية تتجلى في العالم الرقمي.

في السياق العربي، تبرز تحديات مرتبطة بضعف البنية التحتية للأمن السيبراني، ونقص الكوادر المتخصصة، وتباين الوعي المجتمعي بخطورة التهديدات الرقمية. أما في الحالة الليبية، فإن هشاشة الأوضاع السياسية والأمنية تضاعف من المخاطر، حيث يشير تقرير الاتحاد الدولي للاتصالات (2023) إلى أن ليبيا لا تزال في مراحلها الأولى من بناء استراتيجية وطنية متكاملة للأمن السيبراني، ما يجعلها عرضة لمجموعة واسعة من الهجمات.

من هنا، تتحدد **مشكلة البحث** في السؤال الجوهري :**إلى أي مدى يمكن للنظريات الاجتماعية المعاصرة أن تفسر ظاهرة الأمن السيبراني، وأن تقدم إطارًا لفهم دوافع وأبعاد التهديدات الرقمية في السياقات المحلية والعالمية؟** هذه المشكلة تنطلق من افتراض أن المقاربة السوسيولوجية قادرة على سد فجوة في الأدبيات التي غالبًا ما تتناول الأمن السيبراني من منظور تقني بحت، متجاهلة أبعاده الاجتماعية والثقافية.

ثانياً: أهمية البحث ومبرراته

تنبع أهمية هذا البحث من كونه يتناول قضية الأمن السيبراني ليس بوصفها مجرد إشكالية تقنية أو مسألة أمنية صرفة، بل باعتبارها ظاهرة اجتماعية معقدة، تتشابك فيها الأبعاد التكنولوجية مع البنى الاجتماعية، والثقافية، والسياسية، والاقتصادية. وفي ظل التحولات الرقمية العميقة التي يعيشها العالم المعاصر، فإن فهم الظواهر المرتبطة بالأمن السيبراني من منظور سوسيولوجي أصبح ضرورة علمية ومجتمعية على حد سواء.

ثالثاً: الأهمية النظرية

يوفر هذا البحث إضافة نوعية إلى الأدبيات السوسيولوجية من خلال إدماج النظريات الاجتماعية المعاصرة – مثل نظرية الصراع، والنظرية البنيوية الوظيفية، ونظرية الفعل الاجتماعي –في تحليل الأمن السيبراني. فالمقاربات التقنية وحدها عاجزة عن الإحاطة بجميع أبعاد الظاهرة، بينما يقدم المنظور السوسيولوجي فهمًا أعمق لدوافع السلوكيات الإجرامية في الفضاء الرقمي، وآليات الضبط الاجتماعي، وأشكال السلطة والنفوذ التي تتجسد في البنية الإلكترونية. ويساعد إدراج نظرية الفعل الاجتماعي (Social Action Theory)في فهم الدافع الفردي وراء السلوكيات الإجرامية والوقائية في الفضاء الرقمي، وكيف يختار الأفراد اتخاذ إجراءات معينة في بيئة تكنولوجية متغيرة. وكما يشير(Castells, 2010 ،

ص. 142 (فإن "المجتمع الشبكي يعيد صياغة مفاهيم القوة والسيطرة، حيث تنتقل أشكال الصراع والتنافس من الواقع المادي إلى الفضاء الافتراضي."

رابعاً: الأهمية التطبيقية

يمكّن هذا البحث صناع القرار، وواضعي السياسات، والجهات الأمنية من تطوير استراتيجيات أكثر شمولية للتصدي للتهديدات السيبرانية، من خلال الأخذ في الاعتبار العوامل الاجتماعية والثقافية المؤثرة في السلوكيات الرقمية. فالتهديدات الإلكترونية لا تنشأ في فراغ، بل تتغذى على بيئات اجتماعية قد تتسم بعدم المساواة، أو الاضطرابات السياسية، أو ضعف الوعي الرقمي. وتشير دراسة (Anderson et al., 2019) ، (إلى أن الدول التي تعتمد على مقاربات شمولية – تجمع بين الأبعاد التقنية والاجتماعية – تحقق نتائج أفضل في إدارة المخاطر السيبرانية.

خامساً: الأهمية الإقليمية والمحلية

في السياق العربي، تتضاعف أهمية دراسة الأمن السيبراني من منظور اجتماعي نظرًا لوجود فجوات في التشريعات، وضعف البنية التحتية للأمن الرقمي، وغياب برامج التوعية المجتمعية الشاملة. أما في الحالة الليبية، فإن الأوضاع السياسية غير المستقرة، وتحديات بناء المؤسسات، تجعل من الأمن السيبراني مجالًا حساسًا ومرتبطًا بالأمن الوطني والاجتماعي في آن واحد. ووفقًا لتقرير الاتحاد الدولي للاتصالات (2023)، فإن ليبيا سجلت درجات متواضعة في مؤشر الجاهزية السيبرانية، ما يشير إلى الحاجة الماسة لإدماج مقاربات متعددة المستويات في مواجهة المخاطر.

سادساً: المبررات العلمية

- ندرة الدراسات السوسيولوجية التي تتناول الأمن السيبراني، حيث تتركز معظم الأبحاث على الجانب التقني أو القانوني.
- الحاجة إلى إطار نظري قادر على تفسير أنماط التهديدات الرقمية في ضوء التحولات الاجتماعية المعاصرة.
- تزايد التحديات التي تواجه المجتمعات النامية، خاصة في ظل الاندماج المتسارع في الاقتصاد الرقمي العالمي.

سابعاً: المبررات المجتمعية

- ارتفاع معدلات الجرائم الإلكترونية وتأثيرها على الثقة المجتمعية في الفضاء الرقمي.
- انتشار استخدام التكنولوجيا بين جميع فئات المجتمع، بما في ذلك الفئات الهشة مثل النساء والأطفال، ما يستدعي توفير بيئة رقمية آمنة.
- ارتباط الأمن السيبراني بحماية الخصوصية والبيانات الشخصية، وهي قيم أساسية لاستقرار الحياة الاجتماعية.

انطلاقًا من ذلك، يسعى هذا البحث إلى تقديم مساهمة أكاديمية وعملية في آن واحد، عبر تحليل الأمن السيبراني من منظور النظريات الاجتماعية المعاصرة، بما يتيح فهمًا أكثر شمولًا لهذه الظاهرة ويعزز من قدرة المجتمع على مواجهتها بفعالية . ويتم تناول ذلك في الفصول والمحاور التالية للبحث، بدءاً بتحديد المصطلحات، مروراً بالدراسات السابقة، ثم التحليل النظري والنتائج والتوصيات.

ثامنًا: المصطلحات والمفاهيم المستخدمة في البحث

الأمن السيبراني(Cybersecurity)

التعريف النظري/المصطلحي :يُعرف الأمن السيبراني بأنه "مجموعة السياسات والإجراءات والتقنيات التي تهدف إلى حماية نظم المعلومات، البيانات، والشبكات من الهجمات أو الوصول غير المصرح به، لضمان سرية وسلامة واستمرارية المعلومات" (جبريل بن حسن العريشي، 2018، ص. 45).

التعريف الإجرائي :يُقصد بالأمن السيبراني في هذه الدراسة قدرة المجتمع والمؤسسات على حماية بنيتها التحتية الرقمية وبيانات الأفراد من التهديدات الإلكترونية، وذلك من خلال منظومة متكاملة من التقنيات والإجراءات القانونية، والوعي الاجتماعي والثقافي، لضمان استقرار الحياة الاجتماعية والاقتصادية في الفضاء الرقمي.

الجريمة السيبرانية(Cybercrime)

التعريف النظري/المصطلحي :هي "أي فعل أو نشاط يُرتكب باستخدام شبكة الإنترنت أو الأجهزة الإلكترونية بهدف التعدي على حقوق الآخرين أو النظم المعلوماتية، بما يشمل الاختراق، السرقة، أو نشر محتوى ضار" (نورهان محمد الربيعي، 2024، ص. 22).

التعريف الإجرائي :يُقصد بها في الدراسة أي سلوك إجرامي يقوم به الفرد أو الجماعة باستخدام الوسائل الرقمية بشكل غير قانوني ويؤثر على بيانات أو أنظمة معلوماتية بغرض الضرر أو المكاسب غير المشروعة، وتُمثل انعكاساً للسلوكيات الاجتماعية المنحرفة التي استغلت تطور الفضاء الافتراضي كبيئة جديدة للضرر.

القرصنة الإلكترونية(Hacking)

التعريف النظري/المصطلحي :هي "الوصول غير المصرح به إلى أنظمة الحاسوب أو الشبكات بهدف التلاعب بالمعلومات أو استخدامها بطريقة غير قانونية" (محمد موسى شوقي ومحمد سعيد عبد العاطي، 2024، ص. 77).

التعريف الإجرائي :يُقصد بها أي محاولة أو فعل يقوم به الشخص لاختراق أنظمة المعلومات أو الشبكات الرقمية بدون تصريح، بهدف الحصول على بيانات أو تعديلها أو استخدامها بشكل غير مشروع، وهي تندرج ضمن الأفعال العدوانية ضد الملكية الرقمية وتُعبّر عن صراع حول السيطرة على المعرفة والوصول غير المتكافئ للمعلومات.

الهجوم السيبراني(Cyberattack)

التعريف النظري/المصطلحي" :أي عملية هجومية تستهدف الأنظمة الرقمية، الشبكات، أو البيانات بهدف تعطيلها أو سرقتها أو التلاعب بها" (جاب الله حكيمة، 2021، ص. 655).

التعريف الإجرائي :يُقصد بها أي فعل عدائي مُنظم وموجه يهدف إلى الإضرار بالأنظمة الرقمية أو تعطيلها أو السيطرة على البيانات، بما يشمل الهجمات عن طريق الفيروسات أو البرمجيات الضارة أو محاولات الاختراق، وغالباً ما تحمل دوافع استراتيجية كبرى كالسياسية أو الاقتصادية، مما يجعلها أداة في صراع القوى الدولية والمحلية.

الفضاء الرقمي(Cyberspace)

التعريف النظري/المصطلحي :هو "البيئة الافتراضية التي تتضمن الشبكات والأنظمة الرقمية التي يتم من خلالها تبادل المعلومات والبيانات" (جبريل بن حسن العريشي، 2018، ص. 52).

التعريف الإجرائي :يُقصد به البيئة الاجتماعية والتقنية الافتراضية الشاملة التي تُنقل عبرها البيانات والمعلومات وتُدار فيها الأنشطة الإلكترونية، والتي يشملها البحث من حيث المخاطر السيبرانية والتهديدات، وتُشكل مسرحاً جديداً للتفاعل الاجتماعي والتنظيم وبناء السلطة والمقاومة.

تاسعاً: الدراسات السابقة

تُعد الدراسات السابقة حجر الأساس لأي بحث أكاديمي، إذ تتيح للباحث فهم الإطار النظري والتطبيقي للموضوع، وتحديد الثغرات البحثية التي يمكن للبحث الحالي معالجتها. وفي مجال الأمن السيبراني، يبرز دور الدراسات السابقة في توضيح البُعد الاجتماعي والثقافي والتشريعي لهذه الظاهرة، وتقديم رؤية شاملة للتحديات والفرص المصاحبة للتوسع الرقمي .وتتميز الدراسات الحديثة في المجال العربي بالتركيز على ثلاثة محاور رئيسية:

1. **البُعد الاجتماعي والقيمي :**تحليل تأثير الجرائم الإلكترونية على المجتمع وقيمه وأمنه الثقافي، ومدى تآكل الثقة الاجتماعية في الفضاء الرقمي.
2. **البُعد الإعلامي والتقني :**رصد العلاقة بين الأمن السيبراني وحماية المحتوى الإعلامي والمعلومات الرقمية، ودور الإعلام في التوعية الأمنية والرقمية.
3. **البُعد التشريعي والأخلاقي :**تفسير الأمن السيبراني وفق المبادئ الشرعية والقيم الأخلاقية، وتوضيح مدى انسجامها مع التشريعات الحديثة، لا سيما فيما يتعلق بجرائم المحتوى الرقمي والخصوصية.

ويُتيح هذا الترتيب للباحث رسم صورة متكاملة للأمن السيبراني في العالم العربي، مع إبراز الدور الاجتماعي والقيمي والأخلاقي، قبل الانتقال إلى الدراسات الأجنبية أو التحليل المقارن، **مما يبرر تركيز** هذا البحث على سد الفجوة في التحليل السوسيولوجي العميق.

أ- الدراسات السابقة العربية

1. **الأمن السيبراني: الأبعاد الاجتماعية والقانونية :(2019)** أُجريت في مصر وركزت على الأبعاد الاجتماعية والأخلاقية للجرائم الإلكترونية (فوزي، 2019، ص. 99–139). استخدم الباحث المنهج الوصفي التحليلي وتحليل الوثائق القانونية والمجتمعية. وأظهرت الدراسة أن الجرائم السيبرانية تهدد البنية التحتية والقيم المجتمعية، مما يستدعي تعزيز التعاون التشريعي الدولي ووضع أطر حماية اجتماعية فعالة .وتقدم هذه الدراسة إطاراً مرجعياً هاماً لدراسة العلاقة بين القانون والمجتمع في مواجهة التهديدات الرقمية.
2. **الأمن السيبراني وعلاقته بالمضمون الإعلامي في ظل رؤية مصر 2030 :(2021)** تركزت الدراسة على العلاقة بين الأمن السيبراني والمضمون الإعلامي في إطار رؤية مصر 2030، باستخدام المنهج الوصفي التحليلي واستبيان لعينة من 32 متخصصًا (السيد، 2021، ص. 484–514). وأوضحت النتائج ضرورة تعزيز الأمن السيبراني لحماية المحتوى الإعلامي، مع ضرورة تطبيق التشريعات الرقابية .وتسهم هذه الدراسة في فهم دور الوعي والإعلام كأبعاد اجتماعية وقائية من المخاطر السيبرانية.
3. **الأمن السيبراني من المنظور الإسلامي :(2024)** أُجريت دراسة وصفية تحليلية على مصادر شرعية وقانونية لتفسير الأمن السيبراني وفق المبادئ الإسلامية (البلوشي، 2024، ص. 1677–1729). وخلص البحث إلى أن الحفاظ على الضروريات الخمس (الدين والنفس والعقل والنسل والمال) يمثل أساسًا لتحقيق الأمن السيبراني، مع ضرورة ترسيخ القيم الأخلاقية والتعليم الديني .ويؤكد هذا المنظور على أهمية البعد الثقافي والقيمي في تشكيل استراتيجيات الردع والوقاية.

ب- الدراسات السابقة الأجنبية

1. **الأمن السيبراني والسلوك الاجتماعي :(2020)** أُجريت هذه الدراسة في الولايات المتحدة الأمريكية وركزت على تأثير الأمن السيبراني على سلوك الأفراد في الفضاء الرقمي، مع تحليل كيف تؤثر الهجمات الإلكترونية على العلاقات الاجتماعية والثقة بين الأفراد والمؤسسات. استخدم الباحث المنهج الوصفي التحليلي، مع تحليل بيانات من استبيانات ومصادر إعلامية وتقارير رسمية .(Smith, 2020, 45–78) وأظهرت الدراسة أن ضعف الوعي الرقمي يزيد من احتمالية التعرض للهجمات السيبرانية، وأن التفاعل الاجتماعي عبر الإنترنت يعزز من انتشار المخاطر .وتعزز هذه الدراسة من اختيار المقاربة السوسيولوجية لتركيزها على علاقة الأمن السيبراني بالثقة والسلوك الفردي.

2. **حوكمة الأمن السيبراني في العصر الرقمي :(2019)** أُجريت هذه الدراسة في أوروبا، وركزت على الحوكمة الأمنية الرقمية وأطر السياسات المتعلقة بالأمن السيبراني على مستوى المؤسسات والدول. استخدم الباحث المنهج التحليلي المقارن، مع مراجعة التشريعات الوطنية والدولية وأطر السياسات العامة–(Rogers, 2019, 112 145).وخلص البحث إلى أن التنسيق بين الجهات الحكومية والمؤسسات الخاصة ضروري لتعزيز الأمن السيبراني، وأن الأطر القانونية الحديثة تحتاج إلى مرونة للتعامل مع التغيرات التكنولوجية السريعة .وتقدم هذه الدراسة مدخلاً لتحليل البنية المؤسسية للأمن السيبراني في الحالة الليبية في ضوء تحديات الحوكمة.

عاشرًا: المنهج المستخدم

اعتمد هذا البحث على المنهج الوصفي التحليلي بوصفه الأنسب لدراسة الظواهر الاجتماعية المعاصرة ذات الطابع المركّب، مثل ظاهرة الأمن السيبراني. ويقوم هذا المنهج على جمع البيانات والمعلومات المتعلقة بالجوانب النظرية والاجتماعية للظاهرة وتحليلها علميًا بهدف فهم أبعادها وتفسير علاقاتها ضمن سياقها الاجتماعي والسياسي والثقافي.

فالتحليل الوصفي يسمح برصد مكونات الظاهرة كما هي في الواقع، في حين يتيح التحليل التفسيري إمكانية فهم العوامل التي تسهم في تشكّلها وتطورها في ضوء النظريات السوسيولوجية المختارة، وهو ما يتوافق مع طبيعة هذا البحث الذي يهدف إلى فهم الأمن السيبراني كقضية اجتماعية تتقاطع فيها الأبعاد التقنية والبشرية والثقافية.

كما اعتمد البحث على المنهج المقارن بدرجة محدودة، من خلال مقارنة بعض التجارب والممارسات الدولية والعربية في مجال الأمن السيبراني، بهدف استجلاء أوجه التشابه والاختلاف بين السياقات المختلفة، واستخلاص الدروس التي يمكن الإفادة منها في الحالة الليبية لتقديم رؤى استراتيجية عملية.

الحادي عشر: نظرية الصراع الاجتماعي ودورها في تفسير موضوع البحث

تُعد نظرية الصراع الاجتماعي من أبرز الأطر النظرية التي قدمت تفسيرًا للعلاقات الاجتماعية في ضوء التفاوتات القائمة بين الأفراد والجماعات. إذ يرى كارل ماركس أن المجتمع يقوم على صراع مستمر بين الطبقات حول السيطرة على الموارد الاقتصادية والمعرفية، حيث يشكل هذا الصراع المحرك الأساسي للتغيير الاجتماعي. وقد أكد ماركس أن "تاريخ كل مجتمع حتى يومنا هذا هو تاريخ صراعات طبقية" (ماركس وإنجلز 1970، 23).

وفيما بعد، طور رالف داهريندوف (Dahrendorf) النظرية بتأكيده على أن الصراع لا ينشأ فقط من التفاوت الاقتصادي، بل من البنية السلطوية داخل المؤسسات، حيث تسعى الجماعات المسيطرة إلى الحفاظ على امتيازاتها بينما تعمل الجماعات الخاضعة على تغيير الوضع القائم (داهريندوف 1959، 112). كما أضاف لويس كوزر (Coser) بُعدًا آخر حين اعتبر الصراع عاملًا وظيفيًا يمكن أن يسهم في تعزيز التماسك الاجتماعي من خلال كشف التوترات الكامنة وتعديل البنى الاجتماعية (كوزر 1964، 151). تقوم النظرية إذن على مجموعة من المرتكزات النظرية الأساسية:

1. المجتمع ليس وحدة متجانسة، بل ميدان لصراعات بين جماعات متباينة المصالح.
2. القوة والهيمنة من أبرز مصادر الصراع، حيث تسعى الفئات المسيطرة للحفاظ على امتيازاتها.
3. الصراع ليس دائمًا سلبيًا، بل يمكن أن يؤدي إلى التغيير وإعادة التوازن الاجتماعي.

وعند توظيف هذه المرتكزات لفهم الأمن السيبراني، يمكن القول إن الفضاء الرقمي يمثل امتدادًا جديدًا لساحة الصراع الاجتماعي. فالهجمات السيبرانية تُفهم بوصفها أدوات تستخدمها جماعات أو دول لفرض هيمنة أو لزعزعة استقرار الآخرين. وهنا ينسجم ما ذكره لاداده بأن الأمن السيبراني لم يعد قضية تقنية فقط، بل قضية اجتماعية تمس استقرار المجتمعات، إذ يُنظر إلى الأمن الرقمي نفسه كقوة سيطرة تهدف إلى تنظيم وتوجيه سلوك الفاعلين في الفضاء الافتراضي. كما أن التفاوت الرقمي بين الدول المتقدمة والنامية يعكس صراعًا جديدًا حول المعرفة والتكنولوجيا. إذ تؤكد العديد من الدراسات على أن الجرائم الإلكترونية تستغل هشاشة البنى الاجتماعية والثقافية، وهو ما يعكس علاقة غير متكافئة بين من يمتلكون رأس المال الرقمي ومن يفتقرون إليه. ومن جانب آخر يمكن القول إن الصراع يمكن أن يكشف عن الثغرات البنيوية ويدفع نحو إصلاحها، وهو ما يمكن إسقاطه على الحالة الليبية، حيث يمكن لأشكال الصراع الرقمي (كالهجمات المتكررة) أن تدفع نحو بناء منظومات حماية أكثر تكاملًا، مما يحقق توازناً جديداً في بنية السلطة الأمنية الوطنية.

إذن، يساعد منظور الصراع في تفسير مشكلة الأمن السيبراني من خلال:

- كشف علاقات القوة والمعرفة التي تحكم الفضاء الرقمي.
- توضيح كيف تُستخدم الهجمات السيبرانية كوسائل للهيمنة أو المقاومة.
- إبراز أن التفاوت الرقمي يمثل امتدادًا للتفاوتات الاقتصادية والاجتماعية التقليدية.

الثاني عشر: الخصائص السوسيولوجية للجريمة السيبرانية

1. **الطابع العابر للحدود :**تتميز الجريمة السيبرانية بإمكانية ارتكابها من أي مكان في العالم ضد ضحايا في دول أخرى، ما يجعلها ظاهرة عالمية تتطلب تنسيقًا اجتماعيًا وقانونيًا عبر الحدود. سوسيولوجياً، يظهر كيف يعيد الفضاء الرقمي تشكيل العلاقة بين الدولة والفرد، ما يستدعي إعادة نظر في مفهوم "السيادة الأمنية "للدولة أمام فاعلين غير دوليين، ويشير إلى تفكك حدود الضبط الاجتماعي التقليدي (حكيمة 2021، 652)
2. **ارتكاب الجريمة عن بُعد باستخدام أجهزة إلكترونية متطورة :**لا يمكن وصف أي اعتداء إلكتروني كجريمة سيبرانية دون استخدام أجهزة حاسوب أو هواتف ذكية وشبكة الإنترنت، إذ يشكل الجهاز الإلكتروني الوسيلة الجوهرية لتنفيذ الجريمة. سوسيولوجياً، يبرز هذا دور المهارة التقنية والمعرفة الرقمية لدى الجاني، ويشير إلى

أن الجرائم السيبرانية تعتمد على رأس المال البشري المتخصص والمعرفة التقنية النادرة، مما يخلق فئة إجرامية جديدة ذات امتياز معرفي (العريشي 2018، 45).

3. **صعوبة الإثبات والاكتشاف :**الجرائم السيبرانية غالباً لا تترك أثراً مادياً ملموساً، ويصعب اكتشافها أو إثباتها، خصوصاً أن الجاني قد يكون في دولة أخرى عن الضحية، وأن الفعل يتم بسرعة فائقة مع إمكانية محو الأدلة سريعاً. من منظور سوسيولوجي، يضع هذا ضعفاً في آليات الردع التقليدية **القائمة على الأثر** المادي، ويزيد من شعور بعض الأفراد بالإفلات من العقاب(Anomie) ، مما يهدد الثقة في فاعلية العدالة الجنائية (حليم 2022، 12).
4. **التخصصية والمهارة التقنية العالية :**تُرتكب الجرائم السيبرانية من قبل أفراد أو جماعات يمتلكون خبرات تقنية متقدمة، ما يميزها عن الجرائم التقليدية. من منظور سوسيولوجي، يظهر تأثير التفاوت المعرفي والتقني بين الفاعلين والمجتمع، وكيف يمكن للمعرفة الرقمية أن تتحول إلى أداة سلطوية أو أداة صراع تؤثر على الأمن الاجتماعي والاقتصادي، وتُعمّق الفجوة بين النخبة التقنية وباقي فئات المجتمع (العريشي 2018، 48)
5. **تنوع الدوافع والأهداف :**تشمل دوافع الجرائم السيبرانية تحقيق مكاسب مالية، الانتقام، الترفيه، وحتى الإرهاب والاعتداء على الخصوصية. من الناحية السوسيولوجية، يعكس هذا تداخل العوامل الاقتصادية والثقافية والنفسية في تشكيل السلوك الإجرامي، **ويؤكد أن الفضاء الرقمي ليس إلا مرآة لتضاعف الأسباب الاجتماعية للانحراف والتوترات القائمة في الواقع المادي** (حكيمة 2021، 655).

الثالث عشر: أركان الجريمة السيبرانية (تحليل سوسيولوجي)

1. **الركن الشرعي :**يشير إلى وجود نص قانوني يجرم الفعل ويحدد العقوبة وفق مبدأ "لا جريمة ولا عقوبة إلا بنص". يعكس هذا الركن قدرة المجتمع على ضبط الظواهر التقنية الجديدة، غير أن التشريعات غالبًا ما تتأخر عن وتيرة تطور الفعل السيبراني، مما يخلق فراغًا تشريعياً ويضعف الإطار القانوني للردع في مواجهة التطور التكنولوجي المستمر)شوقي وعبد العاطي 2024، 33 .(سوسيولوجياً، يشير هذا التأخر إلى قصور آليات الضبط الرسمي في مواجهة السرعة الرقمية.
2. **الركن المادي :**يمثل الفعل الإجرامي الملموس الذي يضر بالبيانات أو نظم المعلومات أو الشبكة الرقمية، ويتطلب استخدام أدوات تقنية مثل الحواسيب والهواتف الذكية وشبكة الإنترنت. يمكن أن يكون الفعل إيجابياً (اختراق أو سرقة بيانات) أو سلبياً (إهمال أو مخالفة القانون)، ويشكل استخدام الأدوات التقنية شرطاً جوهرياً لقيام هذا الركن . سوسيولوجياً، يُظهر هذا الركن كيف أن الرأسمال التقني (الأجهزة والإنترنت) يتحول إلى أداة لتنفيذ السلوك المنحرف في الفضاء الافتراضي (شوقي وعبد العاطي 2024، 44؛ الربيعي 2024، 37).
3. **الركن المعنوي :**يشمل القصد والنية الجنائية، ويعتمد على العلم والإرادة لدى الجاني. فالقاعدة العامة أنه لا جريمة بلا ركن معنوي، ويجب أن يكون الفعل صادرًا عن شخص طبيعي مسؤول قانونياً. إذا تم الدخول إلى نظام أو شبكة دون علم الجاني بعدم مشروعية الدخول، فإن الجريمة لا تقوم إلا بمجرد إدراكه لاحقاً واستمراره في الفعل (الربيعي 2024، 37). سوسيولوجياً، يبرز هذا الركن أهمية "القصد الاجتماعي "للجاني، إذ تُعد الدوافع (كالمكاسب المادية أو الانتقام أو الصراع الأيديولوجي) هي التجسيد الأعمق للنية الإجرامية في البيئة الرقمية (الربيعي 2024، 37).

الخاتمة

لقد سعى هذا البحث إلى تقديم قراءة سوسيولوجية معمقة لظاهرة الأمن السيبراني في ظل التحولات الرقمية المعاصرة، متجاوزاً الإطار التقني البحت الذي يغلب على الأدبيات الحالية، ليؤكد على الأبعاد الاجتماعية والثقافية والسياسية للتهديدات الرقمية. ومن خلال توظيف المنهج الوصفي التحليلي والاستناد إلى نظريتي الصراع والبنيوية الوظيفية، نجح البحث في بناء إطار تحليلي يفسر دوافع وأنماط الجرائم السيبرانية كـ امتداد للصراعات الاجتماعية التقليدية في الفضاء الافتراضي. وأكدت الدراسة على أن الأمن السيبراني هو انعكاس لاستقرار البنى المجتمعية، وأن هشاشته في سياقات معينة، كالحالة الليبية، ترتبط بشكل وثيق بالضعف المؤسسي والتفاوت المعرفي والاجتماعي. وتختتم الدراسة بالتأكيد على أن تحقيق الأمن الرقمي الشامل لا يمكن أن يتم بمعزل عن بناء مجتمع رقمي واعٍ ومتوازن، قادر على مقاومة الهيمنة الرقمية وتأمين ذاته اجتماعياً وثقافياً قبل أن يؤمنها تقنياً.

النتائج

توصل البحث إلى مجموعة من النتائج المحورية التي تبرر وتدعم المقاربة السوسيولوجية لظاهرة الأمن السيبراني، ويمكن تلخيصها في النقاط التالية:

1. **الأمن السيبراني كصراع على القوة الرقمية :**أثبتت الدراسة أن الهجمات السيبرانية والتهديدات الرقمية تُمثل أداة في صراع القوة والهيمنة، وفقاً لمنظور نظرية الصراع الاجتماعي .فالوصول غير المصرح به للمعلومات والبيانات ليس فعلاً تقنياً فقط، بل هو سعي للسيطرة على "رأس المال الرقمي "(المعرفة، التكنولوجيا، البيانات) كشكل جديد من أشكال الموارد.

2. **تجسيد الفجوة الرقمية لعدم المساواة الاجتماعية :**أكدت النتائج أن الفجوة الرقمية بين الدول النامية (مثل ليبيا) والدول المتقدمة هي في جوهرها شكل جديد من أشكال التفاوت الاجتماعي والاقتصادي .هذا التفاوت يُضاعف من هشاشة البنى التحتية للمجتمعات الأقل جاهزية، ويجعلها هدفاً أسهل للتهديدات السيبرانية.
3. **قِصَر آليات الضبط الاجتماعي التقليدية :**دلت الخصائص السوسيولوجية للجريمة السيبرانية (العابرة للحدود، القائمة على التخصصية والمهارة) على قصور آليات الضبط الاجتماعي والقانوني التقليدية في مواجهة السرعة واللاحدودية للفضاء الرقمي .وهذا يخلق فراغاً معيارياً (Anomie) يزيد من شعور الجناة بالإفلات من العقاب.
4. **ارتباط الهشاشة الأمنية بالبنية المؤسسية :**في السياق الليبي تحديداً، أوضحت النتائج أن ضعف البنية المؤسسية وغياب الإطار التشريعي الموحد يُعد سبباً سوسيولوجياً أساسياً لزيادة مخاطر الأمن السيبراني، بما يتجاوز المشاكل التقنية، ويثبت أن الاستقرار الاجتماعي والسياسي هو الأساس لأي استراتيجية أمن رقمي فعالة.
5. **أهمية الركن المعنوي للجريمة :**التحليل السوسيولوجي لأركان الجريمة السيبرانية أبرز أن **الدوافع الاجتماعية والنفسية** (كالانتقام أو المكاسب غير المشروعة) هي المحرك الأساسي للركن المعنوي، مما يؤكد أن مكافحة هذه الجرائم تبدأ بمعالجة دوافع الانحراف الاجتماعي في البيئة الرقمية.

التوصيات

بناءً على النتائج التي توصل إليها البحث، يقدم الباحث التوصيات التالية التي تهدف إلى تعزيز الأمن السيبراني من منظور شمولي يراعي أبعاده الاجتماعية:

1. **تطوير استراتيجية وطنية سوسيولوجية للأمن السيبراني :**يجب على صناع القرار في ليبيا صياغة استراتيجية وطنية شاملة للأمن السيبراني لا تقتصر على الجانب التقني، بل تدمج الأبعاد الاجتماعية والثقافية والأخلاقية لتعزيز الوعي الرقمي وتحصين المجتمع من الداخل.
2. **تعزيز "المناعة الاجتماعية الرقمية" عبر التعليم :**توصي الدراسة بضرورة إدماج مفاهيم الأخلاقيات الرقمية والوعي السيبراني في المناهج التعليمية بجميع مراحلها، مع التركيز على البعد الوقائي السوسيولوجي الذي يحول دون تحول المعرفة التقنية إلى أداة للانحراف.
3. **دعم البحث السوسيولوجي والقانوني المتخصص :**يجب تخصيص ميزانيات لدعم الأبحاث السوسيولوجية والقانونية التي تدرس ديناميات الجريمة السيبرانية والدوافع الاجتماعية وراءها، لتوفير بيانات ومعلومات تمكّن الأجهزة الأمنية والقضائية من فهم الظاهرة ومواجهتها بأدوات غير تقنية.
4. **بناء جسور الثقة والمشاركة المؤسسية :**يجب على الدولة تعزيز التعاون بين القطاع العام والخاص والمجتمع المدني لمواجهة التهديدات السيبرانية. سوسيولوجياً، يمثل هذا التعاون تفعيلاً لوظيفة التكامل الاجتماعي في الحفاظ على أمن النظام ضد الهجمات الخارجية.
5. **معالجة التفاوتات الرقمية :**ضرورة العمل على سد الفجوة الرقمية عبر توفير الوصول العادل والآمن للتقنية لجميع الفئات، والتركيز على تدريب الفئات الأكثر هشاشة (النساء، الشباب، المناطق النائية)، لتقليل استغلال هذا التفاوت كبوابة للتهديدات.

قائمة المراجع

أولاً: المراجع العربية

1. البلوشي، خ .(2024) .الأمن السيبراني من المنظور الإسلامي .دار الفكر الإسلامي.
2. حكيمة، ج .(2021) .انعكاسات الجريمة السيبرانية على البيئة الرقمية: دراسة في آليات واستراتيجيات مكافحته. [لم يذكر مصدر النشر كاملاً].
3. حليم، ر .(2022) .تصريح لصحيفة المساء بخصوص صعوبة إثبات الجرائم السيبرانية .صحيفة المساء.
4. داهريندوف، ر .(1959) .المجتمع والصراع الطبقي .(ترجمة عربية). الهيئة المصرية العامة للكتاب.
5. الربيعي، ن. م .(2024) .الجريمة السيبرانية وآليات مكافحتها (دراسة مقارنة) .مجلة الفارابي للعلوم الإنسانية، 3.(1)
6. الزعبي، ع.، ومنصة، س .(2010) .الأمن السيبراني في المنظور العربي: تحديات واستراتيجيات .دار الفكر الحديث.
7. السيد، ن .(2021) .الأمن السيبراني وعلاقته بالمضمون الإعلامي في ظل رؤية مصر 2030 .دار الفكر الإعلامي.
8. شوقي، م. م.، وعبد العاطي، م. س .(2024) .الوسيط في مكافحة الجرائم السيبرانية .دار الفكر القانوني.
9. العريشي، ج. ح .(2018، 22 نوفمبر). أثر التطور الرقمي على الجريمة السيبرانية .صحيفة رسالة الجامعة.
10. فوزي، إ .(2019) .الأمن السيبراني: الأبعاد الاجتماعية والقانونية .دار النشر الجامعية.
11. كوزر، ل .(1964) .وظائف الصراع الاجتماعي .(ترجمة عربية). دار النهضة.
12. لاداده، أ .(2021) .الأمن السيبراني والديناميات الاجتماعية: فهم التهديدات الرقمية .دار الدراسات الرقمية.
13. ماركس، ك.، وإنجلز، ف .(1970) .البيان الشيوعي .دار التقدم.

ثانياً: المراجع الأجنبية

1. International Telecommunication Union. (2023). *Cybersecurity status in Libya* (ITU Report).
2. Rogers, M. (2019). *Cybersecurity and social conflicts*. Springer.

3. Rogers, M. (2019). *Cybersecurity governance in the digital age*. Routledge.
4. Smith, J. (2020). *Cybersecurity and social behavior*. Springer.

Compliance with ethical standards

Disclosure of conflict of interest

The authors declare that they have no conflict of interest.