

المحددات السوسيولوجية للضحية في الفضاء السيبراني

نحو صياغة لنموذج مثلث الاستهداف السوسيو رقمي

Sociological Determinants of Victimization in Cyberspace : Toward a Socio-Digital Targeting Triangle Model

حمزة الدامي

جامعة باجي مختار عنابة - الجزائر -

damih.research@gmail.com

تاريخ الاستلام 2026/03/29 تاريخ القبول 2026/05/31

ملخص

تهدف هذه الدراسة إلى تفكيك "البروفایل السوسيولوجي للضحية السيبرانية" انطلاقاً من أطروحة مفادها أن "الاستهداف الرقمي" ليس نتاجاً لثغرات تقنية عارضة، بل هو نتاج لسياق اجتماعي معقد بفعل تقاطع مجموعة من "المحددات البنيوية والسلوكية". إذ تتبلور إشكالية الدراسة في فهم ميكانيزمات "صناعة الضحية السيبرانية" عبر رصد التفاعل بين الخصائص السوسيوديمغرافية والأنماط السلوكية الروتينية ومخرجات التنشئة الاجتماعية الرقمية. تكمن القيمة المضافة لهذه الدراسة في سعيها نحو تطوير المقاربات السوسيولوجية الكلاسيكية وملاءمتها مع خصوصية الفضاء الرقمي، وذلك من خلال صياغة إطار نظري مركبي أطلق عليه الباحث "نموذج مثلث الاستهداف السوسيو رقمي"؛ إذ يفسر هذا النموذج حالة "الهدف المتاح" كحvisلة لتفاعل ثلاثة أبعاد رئيسية استنبطت وطورت بناءً على أدبيات علم الاجتماع. وقد خلصت الدراسة إلى أن الوقوع في فخ الجريمة السيبرانية ليس حدثاً عارضاً، بل هو نتيجة لتقاطع السمات البنيوية للفرد مع أنماطه السلوكية الرقمية، حيث تبرز الهشاشة المعرفية وقصور التنشئة الرقمية كعاملين أساسيين في إضعاف الحارس الذاتي لدى الضحية السيبرانية.

الكلمات المفتاحية: الضحية السيبرانية، الجاني السيبراني، الجريمة المعلوماتية، الوصم الاجتماعي، الإستهداف السوسيو رقمي.

Abstract

This study aims to deconstruct the "sociological profile of the cyber-victim", based on the thesis that "Digital Targeting" is not merely a byproduct of accidental technical vulnerabilities, but rather the result of a complex social context shaped by the intersection of "structural and behavioral determinants". The research problem focuses on understanding the mechanisms of "Cyber-Victimogenesis" by monitoring the dynamic interaction between socio-demographic characteristics, Routine Activity patterns, and the outputs of Digital Socialization. The added value of this study lies in its endeavor to adapt and re-contextualize classical sociological perspectives to the specificities of the digital sphere, through the formulation of a synthetic theoretical framework introduced by the researcher termed the "Socio-Digital Targeting Triangle Model". This model explains the state of the "Suitable Target" as the cumulative result of three primary dimensions derived and refined from the established sociological and criminological literature. The study concludes that falling into the trap of cybercrime is not an accidental event; rather, it is a consequence of the convergence of an individual's structural traits with their digital behavioral patterns. In this context, "Cognitive Fragility" and the failure of digital socialization emerge as pivotal factors in weakening the "Capable Guardian" (internalized guardianship) of the cyber-victim.

Keys Words: Cyber-Victim, Cyber-Offender, Cybercrime, Social Stigma, Socio-Digital Targeting.

مقدمة:

يشهد العالم المعاصر تحولا جذريا نحو "المجتمع الشبكي" الذي يعتبر بنية اجتماعية تقوم على شبكات يتم تشغيلها بواسطة تقنيات المعلومات والاتصالات القائمة على الميكرو اليكترونيات وشبكات الكومبيوتر الرقمية (Castells, 2005 p:07). حيث انتقلت التفاعلات الإنسانية من الحيز الفيزيائي إلى الفضاء السيبراني وهو ما أدى بدوره إلى عولمة الظاهرة الاجرامية. وفي هذا السياق برزت الحاجة الملحة لتطوير مقاربات سوسولوجية لا تكتفي بدراسة المجرم أو المعتدي بل تغوص في سوسولوجيا الضحية لفهم الآليات الاجتماعية التي تجعل الافراد والمجتمعات عرضة للتهديدات الرقمية. إذ تتمحور إشكالية هذه الدراسة حول تفكيك البروفایل السوسولوجي للضحية السيبرانية انطلاقا من أن الوقوع ضحية للجريمة ليس مجرد ثغرة تقنية ، بل هو نتاج تلاقي مجموعة من "المحددات السوسولوجية" الأساسية التي تتجاوز الخصوصية الثقافية الضيقة لتشكل نمطا عالميا للضحية. وانطلاقا من هذا السياق تتبلور محاولة فهم ميكانيزمات صناعة "الضحية السيبرانية" من خلال طرح التساؤلات التالية انطلاقا من التساؤل الرئيسي المتمثل في :

إلى أي مدى تساهم المحددات السوسيوولوجية في رسم ملامح الضحية السيبرانية ؟ وكيف تتفاعل البنى الاجتماعية والأنماط السلوكية مع مخرجات التنشئة الرقمية في تحويل الفرد من مستخدم عادي إلى هدف متاح؟

ويمكننا بذلك طرح التساؤلات الفرعية التالية:

- كيف تؤثر السمات السوسيوديمغرافية للفرد في رسم بروفایل (ملامح) الضحية السيبرانية ؟
- ما هو الدور الذي تلعبه الأنماط السلوكية والأنشطة الروتينية في خلق فرصة الجريمة ورفع درجة انكشاف الضحية ؟
- إلى أي حد يساهم قصور التنشئة الإجتماعية الرقمية والفجوة المعرفية في اضعاف آليات الحماية الذاتية لدى الفرد وتحويله إلى حالة من الهشاشة الرقمية ؟
- كيف يفسر " نموذج مثلث الاستهداف السوسيوورقمي " حالة الهدف المتاح من خلال تفاعل هذه الأبعاد الثلاثة ؟

فرضيات الدراسة :

الفرضية العامة :

يتحول الفرد لضحية سيبرانية نتيجة التفاعل الديناميكي بين سماته البنيوية وأنماطه السلوكية الرقمية ومستوى هشاشته المعرفية الناتجة عن قصور في التنشئة الإجتماعية الرقمية.

الفرضيات الفرعية :

- تساهم السمات السوسيوديمغرافية في رسم بروفایل الضحية السيبرانية وتحديد نوع الاستهداف.
- يرفع النمط السلوكي والروتين الرقمي من درجة انكشاف الضحية أمام الجاني السيبراني.
- يؤدي القصور في التنشئة الإجتماعية الرقمية إلى انتاج حالة من الهشاشة المعرفية التي تضعف آليات الحماية الذاتية لدى الفرد.

أهمية الدراسة :

- اثراء المكتبة العربية بمفهوم أصيل وهو "نموذج مثلث الاستهداف السوسيوورقمي" كما يمكن أن يكون إضافة للباحثين في العلوم الاجتماعية والجنائية والجريمة الرقمية.
- تكمن الأهمية العلمية للمقال في كونه يسعى للبناء على النظريات الكلاسيكية في علم الجريمة مثل نظرية الأنشطة الروتينية ونظرية الوصم الإجتماعي والعبور بها من سياق الجريمة التقليدية

المحددات السوسيولوجية للضحية في الفضاء السيبراني ————— د. / حمزة الدامي
إلى سياق الجريمة المعاصرة مما يعمل على تحيين للنظريات الكلاسيكية لتستوعب متغيرات "السيولة
الرقمية".

- إعادة توجيه الاستراتيجيات الوقائية مما يوفر لصناع القرار الأمني والتربوي خريطة طريق تركز على
التنشئة الرقمية وتغيير نظرة المجتمع للضحية بدلا من التركيز على الحماية التقنية فقط.

أهداف الدراسة :

- تفكيك ديناميكية الاستهداف وفهم كيف ينتقل مستخدم الإنترنت من حالة "الأمن الرقمي" إلى "حالة
الضحية السيبرانية" عبر بناء نموذج مثلث الاستهداف السوسيورقمي.

- صياغة "نموذج مثلث الاستهداف السوسيورقمي" كأداة تحليلية لفهم الجريمة الإلكترونية من منظور
سوسيولوجي - رقمي.

- تحليل سيرورة التضحية وتتبع مراحل تحول المستخدم إلى ضحية بدء من البروفایل الإجتماعي
وصولا إلى الإستغلال القائم على الوصم.

الجانب المنهجي والمفاهيمي للدراسة :

منهج الدراسة :

تعتمد هذه الدراسة على "المنهج الوصفي التحليلي" كمنهج أساسي لوصف أبعاد الاستهداف
السيبراني للضحية، كما تم الاستعانة "بالمقارنة السوسيولوجية" في مواضع محددة من الدراسة
وذلك لغرض إبراز التباين في مؤشرات "الروتين الرقمي" و "فجوة التبليغ" بين المجتمعات العربية
والمجتمعات الغربية. ولتوضيح أثر "الوصم" كمتغير إجتماعي ثقافي يختلف تأثيره في اتساع "الرقم
الأسود" بين المجتمعات العربية والمجتمعات الغربية.

وقد تم توظيف هذه المناهج ضمن "إطار المراجعة المنهجية" وذلك من أجل تفكيك الأدبيات
والنظريات السوسيولوجية الكلاسيكية والحديثة التي تمحورت حول إشكالية الضحية، ثم إعادة
تركيبها في سياق رقمي. وهذا التحليل يتلاءم مع طبيعة الظاهرة المدروسة التي تتطلب رصدًا
للمحددات السوسيولوجية وتفكيكا للعلاقات التفاعلية بينها.

كما اعتمدت الدراسة على "منهج تحليل المحتوى الكيفي" للتقارير الدولية الصادرة عن الهيئات
الأمنية والتقنية وذلك للانتقال من المعطى الرقمي الإحصائي إلى التفسير السوسيولوجي لبناء
نموذج مثلث الاستهداف السوسيورقمي".

أدوات جمع البيانات :

اعتمدت الدراسة في شقها التطبيقي على أدوات منهجية متكاملة شملت المسح الوثائقي الذي يعد وسيلة لجمع المعلومات من المصادر المنشورة (تقارير إحصائية - مقالات علمية ...) المعني بالضحية السيبرانية و إخضاعها للتحليل وذلك لاستخلاص القواعد الإجتماعية المتحكممة في عملية الاستهداف.

كما اعتمدت الدراسة على التحليل السوسيولوجي كأداة إجرائية لتفسير المؤشرات الإحصائية حيث تم الانتقال من الوصف الكمي للبيانات إلى التفسير الكيفي للعلاقة بين المتغيرات (كالبنية - السلوك - التنشئة - الخصائص السوسيوديمغرافية للضحايا كالسن، المكانة الإجتماعية، التمرکز الجغرافي) وذلك لاختبار مدى كفاءة نموذج مثلث الاستهداف السوسيورقمي في تفسير الظاهرة المدروسة .

مجالات الدراسة :

المجال الزماني والمكاني (مصادر البيانات) :

اعتمدت الدراسة على منهجية " تحليل الوثائق والإحصائيات الرسمية " وقد حددت مجالاتها كما يلي:

المجال الزماني :

يمتد النطاق الزمني للتقارير والوثائق الخاضعة للتحليل انطلاقا من سنة 2015 إلى غاية 2025 وقد تم اختيار هذه المدة لتغطية العقد الذي شهد التحول الجذري في السلوك الرقمي وتنامي ضحايا الفضاء السيبراني.

المجال المكاني (الإفتراضي) :

نظرا لطبيعة الظاهرة الاجرامية في الفضاء السيبراني العابرة للحدود، اعتمدت الدراسة على مقارنة سوسيولوجية مقارنة استندت إلى تقارير وبيانات مستقاة من بيئتين متباينتين وذلك وفق الآتي:

أولا - السياق العربي (نموذج الجزائر ودول الخليج العربي) :

تم التركيز في هذا السياق على "الجزائر" كنموذج أساسي للتحليل، بالاعتماد على بيانات تقرير Digital2025Algeria. (Data Reportal,2025) الصادر عن منصة DataReportal العالمية التي تعمل بالتنسيق مع المؤسسات البحثيتين We Are Social و Meltwater واعتمادها على تقاطعات إحصائية دقيقة لمؤسسات دولية كمنظمة الأمم المتحدة UN والإتحاد الدولي للإتصالات ITU وذلك لرصد مؤشر "الروتين الرقمي والانكشاف الارادي". كما تم الاستناد إلى تقرير The Norton Cyber Safety Insights

المحددات السوسيولوجية للضحية في الفضاء السيبراني ————— د. / حمزة الدامي
NCSIR Report 2021. (NortonLifeLock, 2021) فيما يخص دول الخليج العربي تحديداً " السعودية
والإمارات " لرصد تداعيات "الوصمة الاجتماعية" وتأثيرها على ضلع الحارس الكفاء في نموذج مثلث
الاستهداف.

ثانياً - السياق الغربي (نموذج الولايات المتحدة وأوروبا) :

تم الاعتماد على النتائج العالمية لتقرير مؤسسة Norton Life Lock وذلك لفهم الأنماط السلوكية
لضحايا الفضاء السيبراني في المجتمعات الغربية المتقدمة تقنياً. بالإضافة إلى الإحصائيات الجنائية
الرسمية الصادرة عن "مركز شكاوى جرائم الانترنت " (IC3) Internet Crime Complaint Center
التابع لمكتب التحقيقات الفيدرالي الأمريكي (FBI, 2024 p:12-17).
ويهدف هذا السياق إلى فهم حجم التبليغ الرسمي في البيئة الغربية مقابل حجم عدم التبليغ (فجوة
التبليغ) المعبرة عن (الرقم الأسود) في البيئة العربية. كما تم الاعتماد على تقرير Data Breach
Investigations Report (Verizon, 2024). التابع لمؤسسة Verizon العالمية وذلك بصفته مرجعاً
أساسياً في تحليل العنصر البشري في الجريمة السيبرانية، ورصد كيفية استغلال الجناة للثغرات
السلوكية التي تعبر عن الروتين الرقمي للضحايا. كما تم تحليل تقرير Kaspersky Consumer
Threats 2024 لمؤسسة Kaspersky (Kaspersky, 2024). حيث تم التركيز على الترصد الخوارزمي
والنشاط الروتيني للضحية.

تمثيلية العينة ومبررات الاختيار :

تجدر الإشارة منهجياً إلى أن اختيار هذه الدول (الجزائر، السعودية، الإمارات، الولايات المتحدة
الأمريكية) لم يكن مقصوداً لذاته بل جرى التعامل معها بوصفها "نماذج تمثيلية"، إذ تمثل الجزائر
ودول من الخليج العربي كالسعودية والإمارات بيانات إجتماعية تلعب فيها "الوصمة" و"الرقم الأسود"
دوراً مركزياً في حماية الجاني، بينما يشكل النموذج الغربي ممثلاً بالولايات المتحدة الأمريكية بيئة
"الحارس التقني المتطور".

وقد استند هذا الاختيار إلى معيار وفرة وجودة التقارير الإحصائية مما أتاح إمكانية تفكيك اضلاع
"مثلث الاستهداف" واسقاطها على واقع الضحية الرقمية بدقة علمية.

تحديد المفاهيم والمصطلحات :

♦ الجاني السيبراني (Cyber-offender) :

وهو فرد أو شخص يستهدف جهاز كومبيوتر أو جهازا متصلا بالشبكة، حيث تقع معظم الجرائم الإلكترونية على أيدي لصوص أو مخترقين لكسب المال وأحيانا تكون لأسباب سياسية، ويكون بعض هؤلاء المجرمين الإلكترونيين منظمين ويستخدمون التقنيات المتقدمة، وهم ذوي مهارات فنية عالية وبعضهم مجرد مخترقين مبتدئين. (Kaspersky, 2024)

♦ الهندسة الاجتماعية (Social Engineering) :

يعرفها ميتنيك Mitnick على أنها عملية اختراق نفسي تقوم على مبدأ أن العنصر البشري هو الحلقة الأضعف في السلسلة الأمنية. (Hadnagy, 2018 p:03) وبناء على ذلك يتم تعريفها إجرائيا بأنها؛ فن التلاعب بالنماذج العقلية للضحية لخلق واقع زائف يدفعه للتعاون مع المهاجم. (Ibid, p:37) وهي باختصار عملية استبدال الثغرات البرمجية بالثغرات النفسية البشرية.

♦ الترصد الخوارزمي (Algorithmic Surveillance) :

حيث يعرف في فكر زوبوف Zuboff بأنها العملية التي يتم من خلالها تحويل النشاط الإنساني إلى بيانات رقمية عبر وسائط خوارزمية ذكية ليس فقط بغرض المراقبة، بل بهدف التنبؤ بالسلوك المستقبلي وتعديله بما يخدم القوة الآلية المسيطرة. (Zuboff, 2019 p:02-03) وبذلك يسهل على الجاني تصيد الضحية في الفضاء السيبراني.

♦ الإنكشاف الرقمي (Digital Exposure) :

وهو مشاركة البيانات الشخصية على الانترنت سواء عبر منصات أو غيرها بدافع الموثوقية. وقد يحدث ذلك من خلال محادثة شخصية، وقد يكون ذلك من خلال الأثر الذي تتركه بعد انتهاء المحادثة أو مسحها (Silva, 2015 p:208).

كما يعرف الإنكشاف الرقمي وفقا لتقرير وكالة الاتحاد الأوروبي للأمن السيبراني على أنها الحالة الناتجة عن إطلاق معلومات حساسة إلى بيئات غير موثوقة سواء كان ذلك بسبب ثغرات تقنية أو تسريبات غير مقصودة مما يوفر للمهاجمين قاعدة بيانات لاستطلاع الأهداف قبل الهجوم (ENISA, 2023p:48).

كما يؤكد هولت Holt بأن عملية الاستهداف في الفضاء السيبراني لا تعتمد فقط على الثغرات التقنية، بل ترتبط بشكل وثيق بالروتين اليومي الرقمي للضحية، حيث يساهم التفاعل المستمر مع

المحددات السوسولوجية للضحية في الفضاء السيبراني ————— د.د / حمزة الدامي
المنصات الإجتماعية في خلق حالة من الانكشاف التي تجعل من الفرد هدفاً متاحاً للجنة (Holt, 2023
.p:84)

♦ الضحية السيبرانية (Cyber-victim) :

وهو الفرد الذي يتعرض للضرر من خلال المنصات الرقمية بما في ذلك التنمر الإلكتروني والاحتيال عبر الأنترنت وسرقة الهوية والمطاردة الإلكترونية (McKee, 2026) .

♦ الفجوة الرقمية (Digital Divide) :

تعرفه مجموعة الرواد للإدارة والتدريب على موقع RMG بأنه يمثل التفاوت في مستويات الوصول إلى تقنية المعلومات والاتصالات واستخدامها بين مختلف الأفراد والمجتمعات والمناطق الجغرافية والدول (مجموعة الرواد، 2026).

ووفقا لمارك برنسكي فإن الفجوة الرقمية تعتمد على عامل السن أو الفجوة الجيلية حيث صنفها إلى "المواطنون الرقميون" (الذين ولدوا في العصر الرقمي) وهم الأصغر سنا. و "المهاجرون الرقميون" (الذين تبنا التكنولوجيا لاحقا) وهم الأكبر سنا. اذ يرى برنسكي أن هذه الفجوة تمثل أزمة تواصل وتعلم عندما يستخدم الجيل الأقدم أساليب تقليدية للتواصل والتعليم مع الجيل الأصغر سنا الذين تشكلت عقولهم رقميا (Prensky, 2001).

♦ الإستهداف السوسيو رقمي (Socio-Digital Targeting) :

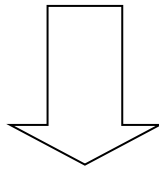
يُصطلح الباحث على هذا المفهوم إجرائيا باعتباره : العملية الديناميكية المركبة التي يتم من خلالها اصطلياد الضحايا والنفاد إليهم عبر استغلال تقاطعات الهشاشة السوسولوجية كالوصمة والروتين الإجتماعي مع آليات الفضاء الرقمي كالترصد الخوارزمي والإنكشاف ، وذلك بغض النظر عن مستوى المهارة أو التفوق التقني للجاني . بل بالتركيز على مدى قدرته على هندسة الثغرات الإجتماعية لتطويق الضحية داخل "مثلث الاستهداف السوسيو رقمي" بما يضمن "شل ارادتها" عن المواجهة وتكريس وضعية "الضحية الصامتة".

ويعد هذا المفهوم في إطار هذه الدراسة تقديمًا مفاهيميًا مستحدثًا يسعى لتجاوز القصور في التعريفات الكلاسيكية التي فصلت بين الفعل التقني والسياق الإجتماعي، فحينما تنتهي قدرة

المحددات السوسيولوجية للضحية في الفضاء السيبراني ————— د. حمزة الدامي

الخوارزمية على التتبع تبدأ قدرة الهندسة الإجتماعية على استغلال المحددات السوسيولوجية للضحية، مما يجعل الإستهداف السوسيورقمي بمثابة الحلقة المفقودة في تفسير صمت الضحية واتساع "الرقم الأسود" في الجريمة السيبرانية.

• يتبع هذا التعريف النموذج المستحدث من قبل الباحث المتمثل في مثلث الاستهداف السوسيورقمي؛ انظر الشكل رقم (1) متبعوفا بتوضيح للإضافة العلمية التي انطلقت من النظريات الكلاسيكية التي تم تطويرها حتى تتناسب مع طبيعة الجريمة السيبرانية . انظر الجدول رقم (1).



انظر الشكل رقم 1 والتحليل الذي يتبعه حتى يمكننا ربط المفهوم المستحدث من قبل الباحث الخاص بالاستهداف السوسيورقمي

نموذج مثلث الإستهداف السوسيورقمي :

الشكل رقم 1: نموذج مثلث الاستهداف السوسيورقمي



المصدر: من إعداد الباحث، 2026

المحددات السوسيولوجية للضحية في الفضاء السيبراني ————— د. حمزة الدامي

يحلل هذا النموذج الجريمة كظاهرة ناتجة عن علاقة تفاعلية بين ثلاثة عناصر في الفضاء السيبراني؛ حيث تبدأ العملية بوجود (جاني سيبراني مُتحفز) يمارس رصدًا سوسيولوجيًا للبروفائلات، مستهدفاً (ضحية رقمية) تعاني من حالة إنكشاف ناتجة عن نمط حياتها وروتينها الرقمي .

وتكتمل البنية الإجرامية عند (غياب الحارس الكفاء)، الذي لا يمثل هنا قصورا أمنيا فحسب، بل هو نتاج لتعطيل فاعلية القانون بفعل الوصمة الإجتماعية؛ فالجاني يستغل خوف الضحية من التمثلات المجتمعية السلبية ليضمن صمتها، مما يحول الفضاء السوسيورقمي إلى بيئة مغلقة يعاد فيها إنتاج الجريمة بعيدا عن مؤسسات الضبط الاجتماعي.

الإضافة العلمية لنموذج مثلث الإستهداف السوسيورقمي :

بناء على التصور البصري الموضح في الشكل رقم (1) أعلاه تنتقل الدراسة إلى مرحلة التأصيل المفاهيمي لبيان كيفية تشكل أضلاع هذا المثلث. وانطلاقا من مبدأ التراكمية العلمية، تم استلھام الركائز الأساسية من نظرية الأنشطة الروتينية مع أداة صياغتها سوسيولوجيا لتتناسب مع ديناميكيات الفضاء السيبراني والمجتمع الشبكي.

كما يوضح الجدول رقم (1) هذا الانتقال النوعي في المفاهيم، حيث تم استبدال العناصر المادية الكلاسيكية بمفاهيم سوسيورقمية مستحدثة تعبر عن واقع الضحية والإنكشاف والضبط في العصر الرقمي.

الجدول رقم 1: الانتقال المفاهيمي من الأنشطة الروتينية إلى نموذج مثلث الإستهداف السوسيورقمي

ماهية التحول السوسيولوجي المقترح	المفهوم المطور في النموذج (الباحث)	المفهوم الكلاسيكي (Felson/Cohen)
الانتقال من الحيز الفيزيائي إلى الفضاء السيبراني حيث يتخفى الجاني خلف الهوية الرقمية.	الجاني الإلكتروني المتحفز ذو الرغبة	الجاني المتحفز (ذو الرغبة)
تحول الملاءمة من القيمة المادية إلى الجاذبية الرمزية والبيانات المنكشفة.	الضحية السيبرانية (الإنكشاف الرقمي)	الهدف المناسب
توسيع مفهوم الحراسة ليشمل البعد القيمي (التنشئة) والبعد القانوني والدرع التقني.	تآكل الضبط السوسيورقمي	غياب الحارس الكفاء

المصدر: من إعداد الباحث بناء على تطوير نظرية الأنشطة الروتينية، 2026

صياغة عامل الإنكشاف الرقمي : حيث كان التقارب في المكان هو الشرط في النظرية الكلاسيكية، أما في النموذج المطور فالشرط هو الإنكشاف في الفضاء الرقمي. حيث تكمن الإضافة الجوهرية في هذا النموذج في مفهوم الإنكشاف الرقمي ; فبينما ركزت الأنشطة الروتينية على التقارب المادي، يرى النموذج الحالي أن التقارب في الفضاء السيبراني هو تقارب معلوماتي رمزي ، الضحية هنا تصبح هدفا مناسباً بقدر ما تتيحه من بيانات سوسولوجية تجعلها مرئية للجاني، وهو ما يحول الإنكشاف من حالة فيزيائية إلى حالة سيوسيوثقنية متمعمة.

وقد تم التركيز أيضا على الحارس الكفاء بإعادة صياغة هذا المفهوم ليكون منظومة ثلاثية الأبعاد: بعد تقني (برمجيات الحماية)، بعد قانوني (التشريعات والردع) وبعد سوسولوجي وهو الأهم ويتمثل في (التنشئة الرقمية): فالحارس في الفضاء الرقمي ليس شخصا فيزيائيا، بل هو وعي جمعي رقمي يحمي الفرد من الإنكشاف السلبي.

الدراسات السابقة :

الدراسة الأولى :

تعرض الدراسة الأولى المعنونة بأسباب ضحية الجريمة السيبرانية : مراجعة أدبية منهجية لأبو طاهر محمد عبد الله و اسراط جناه (Abdullah & Jahan, 2020 p:101-110). حيث تستند هذه الدراسة على نظرية الأنشطة الروتينية كإطار أساسي لفهم الضحية التي توجد عند إلتقاء جاني محتمل وهدف مناسب وغياب حارس كفاء. إذ أن هذه الدراسة تمثل "الجذر الكلاسيكي" الذي انطلقت منه دراستنا لتطوير نموذج مثلث الاستهداف السوسيو رقمي ، حيث ركزت على العوامل الاجتماعية و السلوكية التي تجعل الفرد هدفا مناسباً مثل الروتين الرقمي والخصائص الديمغرافية كالسن مثلا ، إذ وُجِدَ بأن المراهقين هم الأكثر عرضة للتنمر الإلكتروني بينما كبار السن هم الأكثر عرضة للإحتيال عبر الانترنت .

كما تحدثت عن الهشاشة السلوكية و الاجتماعية ، حيث ربطت الدراسة بين الضحية و بين عوامل مثل ضعف الرقابة الذاتية وعدم المساواة الاجتماعية خارج الفضاء الإلكتروني و مقارنتها بالفضاء السيبراني.

الفجوة البحثية :

بالرغم من القيم العلمية التي قدمتها دراسة محمد عبد الله واسراط جناه في حصر محددات الضحية السيبرانية إلا أننا نرى أنها ظلت حبيسة المقارنة الوصفية ، ومن هنا تأتي الاستجابة العلمية لدراستنا الحالية حيث نرى أن "الرقمي" ليس مجرد وسيط ، بل هو محدد سوسيولوجي بحد ذاته ، فحينما ركزت الدراسة السابقة على الجانب الكلاسيكي الذي يرى الضحية هدفا ماديا يضيف "نموذج مثلث الاستهداف السوسيورقمي" بعدا جديدا يتمثل في "الترصد الخوارزمي" و "الهندسة الاجتماعية" محولا مفهوم "الحارس" من مجرد أداة تقنية إلى منظومة سوسيولوجية متكاملة تتعلق بالإرادة والوعي بالوصمة ، وهو ما يسمح بتفسير الظاهرة التي لا يمكن للنظرية الكلاسيكية تفسيرها بمفردها .

الدراسة الثانية :

عرضت الدراسة المعنونة ب: "الخوف من الوقوع ضحية للجريمة الإلكترونية دراسة العلاقة بين الخوف والوقوع ضحية" (Sarkki, 2025). حيث وجدت الدراسة أن التعرض الحديث للجريمة السيبرانية يزيد بشكل كبير من مستويات الخوف ، و نتيجة ذلك هي أن الخوف لا يقلل من خطر الوقوع ضحية مستقبلا وهذا ما توصلت إليه دراستنا وهو " شل الإرادة " في مثلث الاستهداف ، فبالرغم من خوف الأفراد إلا أنهم يظلون عاجزين عن حماية أنفسهم. كما توصلت الدراسة إلى "ظاهرة تكرار الضحية" أو تكرار الوقوع ضحية. حيث وجدت أن الضحايا السابقين هم أكثر عرضة بخمس مرات للوقوع ضحايا من جديد .

الفجوة البحثية :

بينما كشفت الدراسة السابقة عن وجود علاقة طردية بين الضحية السابقة وزيادة الخوف إلا أنها تركت تساؤلا حول: لماذا لا يحمي هذا الخوف الضحايا؟ هنا تبرز الإضافة العلمية "لنموذجنا مثلث الاستهداف السوسيورقمي" الذي يفسر هذه المفارقة بأن الجاني لا يهاجم الأجهزة بل يهاجم "المحددات السوسيولوجية كالوصم والهشاشة الاجتماعية" مما يجعل الخوف عنصر شلل لا عنصر حماية وهو ما يفسر بقاء الضحية في دائرة الاستهداف الصامت.

الدراسة الثالثة :

تركز الدراسة المعنونة ب: تحليل تأثير جائحة كورونا (covid19) على ارتفاع معدلات الجرائم السيبرانية في مصر مع التركيز على الضحايا وتجاربهم الرقمية (عبد الفتاح، 2021). حيث اعتمدت

الدراسة على مسح ميداني إلكتروني شمل 400 مستخدم للإنترنت لتقييم انتشار الجرائم السيبرانية قبل وأثناء الجائحة (كالاحتيال، التصيد، الهجمات البريدية، ...) وقد خلصت نتائج الدراسة على أن الجائحة وفرت فرصة (زيادة وقت الاستخدام، العمل من المنزل) لظهور الجريمة "وهذا تفسير سطحي يعتمد على توفر الضحية تقنيا فقط". كما رصدت الدراسة أن الناس تعرضوا للاحتيال بنسبة 600٪، لكنها لم تفسر لماذا استسلمت الضحية أو لماذا صمتت. كما أن هذه الدراسة هي حالة وصفية ترصد واقعا زمنيا معيناً (فترة الكوفيد) أي تنتهي بانتهاء الجائحة.

الفجوة البحثية :

بالرغم من القيمة العلمية للدراسة إلا أنها ركزت بشكل أساسي على كمية التعرض الرقمي وثمرات الأنظمة الرقمية كعوامل مفسرة لزيادة الوقوع كضحية وهنا تبرز الفجوة البحثية التي تسعى الدراسة الحالية لسدها. وذلك في الانتقال نحو الفهم الأعمق لكيفية استغلال الجاني لحالة (الإرتباك الاجتماعي والعزلة السوسيولوجية) التي فرضتها الجائحة لإعادة صياغة استراتيجيات الإستهداف ، حيث تطرح دراستنا تساؤلاً جوهرياً حول "لماذا نجح الاستهداف سوسيولوجياً" وليس فقط "كيف زادت النسبة رقمياً و تقنياً". ومن هنا يسد نموذج مثلث الاستهداف السوسيورقمي هذه الفجوة. وبالتالي لا يفسر نجاح الجريمة بناء على التطور التقني أو نجاح الاختراق تقنياً فحسب بل من خلال ميكانيزمات "شل إرادة الضحية" واستغلال الضغط الاجتماعي خاصة في حالات الابتزاز محولة بذلك الملاحظات المؤقتة المرتبطة بظروف الجائحة إلى نموذج هندسي مستدام وعابر للأزمات، يمكن استخدامه كأداة تحليلية لتفسير أي جريمة سيبرانية مستقبلية تتجاوز في أبعادها حدود السياق الزمني للجائحة.

الجانب النظري للدراسة :

المحددات السوسيولوجية للضحية السيبرانية (البروفایل السوسيولوجي) :

تتجاوز الجريمة السيبرانية في أبعادها السوسيولوجية كونها مجرد "فعل تقني" لتصبح فعلاً يؤدي للانكشاف الناتج عن البنية الاجتماعية. و استناداً لنظرية نمط الحياة لهيندلانغ Hindelang وزملاؤه كما ورد في موسوعة النظرية الجنائية مفادها أن التوزيع غير المتكافئ للمخاطر هو نتاج مباشر لنمط الحياة التي يعيشها الأفراد (موسوعة النظرية الجنائية، 2010 ص: 449). حيث تؤكد النظرية أن هذه الأنماط لا تنشأ من فراغ بل هي محصلة لتفاعل عنصرين بنيويين "التوقعات المرتبطة بالدور الاجتماعي و القيود البنيوية ضمن حدود ما يفرضه عليه موقعه الطبقي و سنه و مركزه الاجتماعي".

المحددات السوسيولوجية للضحية في الفضاء السيبراني ————— د. / حمزة الدامي
وهي محدّدات تجبر فئات معينة على التواجد المكثف في (الفضاءات الرقمية) المفتوحة مما يرفع من احتمالية تصادمها مع الجناة. في هذا الإطار يتحول (البروفایل السوسيولوجي للضحية) إلى ما نسميه بالانكشاف للمخاطر أو كما نعبر عنه بالانكشاف الرقمي. والذي يعتبر مجموعة الأصول الرقمية للأفراد أو المنظمات بما في ذلك البيانات، الهويات، البرمجيات، الأجهزة ... التي يمكن الوصول إليها أو رؤيتها عبر الانترنت والتي تفتقر إلى ضوابط أمنية كافية وذلك ما يجعلها نقطة انطلاق أو ثغرة محتملة للهجمات السيبرانية (Council of Europe, 2026 p:112).

فبناء على نظرية هيندلانغ ترتبط احتمالية أن يقع الفرد ضحية بمدى التقارب الزمني والمكاني (الرقمي) من الجناة، حيث أن نمط الحياة الذي يتميز (بالسيولة الرقمية يعزز من مرئية الفرد كهدف متاح). وفي هذه الحالة فالجاني كفاعل عقلائي يوازي بين الربح والجهد فهو يقرأ في البروفایل السوسيولوجي للضحية مؤشرات الجاذبية الاجرامية، فالمكانة المهنية والسمات الديمغرافية مثلا تمنح الجاني تصورا مسبقا عن حجم العائد المادي أو الرمزي، حيث تتحول الخصائص الشخصية للأفراد إلى كشافات تجذب الفعل الإجرامي في بيئة تفتقر للرقابة الوقائية وأبرز هذه المحددات السوسيولوجية نجد :

المحدد الأول - المحدد السوسيوديمغرافي :

المحدد السوسيوديمغرافي يتضمن عدد من المتغيرات نعمل على دراستها و تسليط الضوء عليها في دراستنا و ننطلق بالمتغير الأول :

1- متغير (السن) :

حيث يظهر التقرير السنوي لسنة 2023 الصادر عن مركز شكاوى الانترنت التابع لمكتب التحقيقات الفدرالي FBI أن فئة كبار السن أي 60 سنة فما فوق قد سجل أعلى حجم خسائر مادية قدر ب 3,4 مليار دولار، بينما الفئة العمرية الممثلة ب 20 سنة كانت أقل خسائر بمقدار 40 مليون دولار (FBI, 2024 p:12-17)

التحليل: هذه الأرقام تثبت أن الجاني يختار ضحيته بناء على عامل السن، وهو يعتبرهم أهدافا ثمينة لأنهم يمتلكون المدخرات وجرايات التقاعد وبالمقابل يعانون من "عزلة رقمية" تجعلهم أكثر تصديقا لانتحال الشخصية. أي أن السن هو مؤشر على "الجاذبية المادية" فعامل السن لا يمثل رقما فقط بل يوضح التموقع الجيلي داخل الفضاء السيبراني.

على عكس فئة الشباب الذين يعتبرون السكان الأصليين الرقميين بسبب كثافة تواجدهم في الفضاء الرقمي بينما نجد انخفاضا في نسبة التواجد لكبار السن، وهذا ما يمكن أن نعبر عليه "بالفجوة الرقمية" إذ يعتبر كبار السن هم "المهاجرون الرقميون" الذين يتم استهدافهم عبر "العزل المعرفي". الجاني يستغل عدم إلمامهم بالتحديات الأمنية المتسارعة، فيستغل هذه الثغرة للإيقاع بهم.

"العزلة الرقمية": غالبا ما يعاني كبار السن من العزلة أو الوحدة، مما يجعلهم أكثر عرضة لجرائم الاحتيال العاطفي.

- كما نجد تباينا في ما يخص مؤشر السن ووجود تفاوت بين المجتمعات الغربية مثل أمريكا وبين المجتمعات العربية، فإن مؤشر السن في المجتمعات الغربية بالنسبة لفئة كبار السن يضعهم في خانة "الهدف المالي" بينما نجد أن الاستهداف في المجتمعات العربية يتجه نحو القاعدة العريضة وهم فئة الشباب مما يحولهم إلى الكتلة الأكثر استهدافا بما أنهم الأكثر عرضة "للإنكشاف الرقمي" ففي المجتمعات الغربية كبار السن مندمجون في الخدمات البنكية والحكومة الرقمية بشكل كامل، مما يجعلهم أهدافا تقنية. بينما في العديد من المجتمعات العربية لا تزال الفئة الشبابية هي المحرك الأكبر للإقتصاد الرقمي والتعاملات الالكترونية. أي أن السن هو محدد بنيوي للإنكشاف الرقمي يعني أن هذه الفئة أي الأصغر سنا هي الأكثر استهدافا بسبب كثافة تواجدها في الفضاء الرقمي وغياب آليات الرقابة.

- كما يظهر التقرير الخاص بالجزائر كأنموذج عن الدول العربية الصادر سنة 2025 إذ بين أن الفئة العمرية ما بين 18 إلى 35 سنة بأنها تشكل الكتلة الأكبر من مستخدمي الانترنت ومنصات التواصل الاجتماعي في الجزائر، أي أكثر من 55 ٪ من اجمالي المستخدمين النشطين.

أي فئة الشباب هي الأكثر تواجدا في الفضاء الرقمي وذلك ما يجعلهم أكثر انكشافا رقميا، فكلما كان المجتمع فتيا زاد مؤشر الضحايا نحو فئة الشباب. هذا بالإضافة إلى الروتين اليومي المكثف الذي يحول الفرد من مستخدم عادي إلى "هدف دائم"، إذ يوضح التقرير بأن الدخول للإنترنت في الجزائر يغطي نسبة 95٪ عبر الهاتف المحمول (Data Reportal,2025). مما يعني أن الضحية (متصل دائم) مما يسهل على الجاني الوصول إليها في أي وقت.

2. متغير (المكانة المهنية كجاذب للجريمة) :

المحددات السوسيوولوجية للضحية في الفضاء السيبراني ————— د. / حمزة الدامي
كما جاء في التقرير الصادر عن مركز (IC3) أن الشكاوى بلغت 21489 شكاوى بخسائر قدرت ب 2,9
مليار دولار. هذا المتغير أي المكانة المهنية هي التي تحدد هوية الضحية، حيث يتم استهداف الأفراد
بناء على صلاحياتهم الوظيفية داخل المؤسسة.

- نلاحظ أن هناك فرق بين دول الغرب والمنطقة العربية ،ففي الوطن العربي الضحية السيبرانية لا
تزال في أغلبها (إجتماعية،عاطفية :إبتزاز، تنمر، سرقة حسابات تواصل اجتماعي) وحتى المبالغ المالية
المسروقة غالبا ما تكون بسيطة (كتعبئة رصيد، مبالغ تحويل صغيرة...) بينما في أمريكا الضحية
الهدف تكون اقتصادية بحتة، لأن النظام البنكي مرتبط كليا بالانترنت والثقافة الادخارية رقمية مما
يجعل وعاء السرقة ضخمة جدا.

وبربط محدد السن مع محدد المكانة المهنية فإن بلوغ خسائر فئة عمرية واحدة (كبار السن) ما
يتجاوز 3 مليار دولار وفق تقرير (FBI, 2024 p:10). IC3. وهو (رقم يضاهي ميزانيات دول بأكملها)، مما
يؤكد أننا أمام تحول بنيوي في طبيعة الجريمة، فالجاني لم يعد يبحث عن خرق تقني بسيط بل
أصبحت الضحية "هدفا استراتيجيا" وهو ما يبرز "الجاذبية المادية للهدف". وبذلك يكون أهم محدد
لهوية الضحية في المجتمعات الرأسمالية الرقمية.

3- المتغير الجغرافي (التمركز الرقمي) :

حيث كشف التقرير الخاص بالجزائر أن نسبة تمركز السكان في المدن يمثل 76٪ بينما 24٪
يعيشون في المناطق الريفية (Data Reportal,2025) . يعني أن الاستهداف السيبراني لا يتوزع
بشكل عشوائي بل يتبع (جغرافيا التمرکز الرقمي والنشاط الإقتصادي)، حيث يظهر تقرير مركز
شكاوى جرائم الانترنت في أمريكا أن عدد الضحايا يرتفع طرديا في الولايات والمناطق ذات الكثافة
السكانية مثل (كاليفورنيا وتكساس) (FBI, 2024 p:27). مما يثبت أن الجغرافيا المادية تحدد "بيئة
الانكشاف".

وفي الجزائر كنموذج عن المغرب العربي نجد تشابها مع البيئة الغربية بالنسبة لهذا المتغير، مما
يعني أن سكان الحضر هم أكثر عرضة للاستهداف نتيجة توفر البنية التحتية الرقمية مما يحول
المدينة إلى فضاء للانكشاف الرقمي الاجرامي.

4- متغير الجندر (النوع الاجتماعي) :

المؤشر الرقمي حسب تقرير Digital 2025 Algeria يبين أن التواجد الرقمي في الجزائر لصالح الذكور إذ يمثل 58٪ مقابل الاناث ب 42٪ (Data Reportal,2025) .

فبالرغم من أن الذكور هم الأكثر تواجدا أي (انكشاف كمي) إلا أن الاناث هم الأكثر (هشاشة) أي (استهداف كيمي) ;بمعنى أن الجندر يتحول إلى محدد للاستهداف بسبب (الوصم الاجتماعي) حيث يستهدف الجاني الأنثى في المجتمعات التقليدية لعلمه بأن كلفة (الفضيحة أو الابتزاز) لديهم تفوق بكثير كلفة الخسارة المادية لدى الذكور. أما الجندر في أمريكا يحدده نوع الطعم الذي يستخدمه الجاني، فالإستهداف يتبع الاهتمامات السلوكية المرتبطة بالنوع الإجتماعي أكثر من ارتباطه بالخوف من المجتمع.

♦ يركز هذا المُحدد على "البروفايل السوسولوجي للضحية السيبرانية" أو ملامح "الهدف المتاح" حيث تتحول الخصائص البنيوية كالسن والمكانة... إلى جاذبية إجرامية تجذب الجاني، فالضحية هنا ليست هدفا عشوائيا بل هي نتيجة تقاطع الموقع الإجتماعي مع الانكشاف الرقمي.

المحدد الثاني - الأنماط السلوكية والنشاط الروتيني (انتاج الفرصة الاجرامية) :

ينتقل التحليل السوسولوجي من "بنية الضحية " إلى "ديناميكية الفعل"، حيث تفسر الجريمة السيبرانية بوصفها نتاجا للنشاط الروتيني اليومي.وبالاستناد إلى نظرية النشاط الروتيني لمارك فيلسون Felson لا تتطلب الجريمة وجود دوافع إجرامية معقدة بقدر ما تتطلب تقاربا في الزمان والمكان الرقمي (FelsonCohen,Felson,2002 p:22-24). تفترض هذه المقاربة أن التغيرات في بنية الأنشطة اليومية كالإنتقال من الفضاءات المادية إلى الفضاءات الافتراضية هي التي تخلق "الفرصة الإجرامية" فالنشاط الروتيني (كالتسوق أو التفاعل الاجتماعي)، ليس مجرد ممارسات تقنية بل هو فعل اجتماعي يجمع وبشكل عفوي بين الضحية والجاني في بيئة تفتقر للرقابة. أما بالنسبة لديناميكية انتاج الفرصة الإجرامية حيث يؤدي نمط الفعل الروتيني إلى تحييد ما يسميه فيلسون بالحارس الكفاء The capable guardian ، وهذا الحارس ليس بالضرورة جهازا أمنيا ،بل هو العين اليقظة التي "تعطلها الضحية عبر تآكل الحذر العقلاني" الناتج عن تكرار الفعل (Felson&Cohen,Felson,2002p:26-27). فالضحية عبر تبنيها لسلوكيات روتينية تتسم بالسهولة والسرعة تقوم آليا بتحييد الرقابة، مما يمنح الجاني المحفز مبررا عقلانيا للاختراق. فالجريمة اذن هنا هي (وليدة الفرصة) التي أوجدها غياب الرقيب السلوكي والتقني في لحظة تقاطع

المحددات السوسيولوجية للضحية في الفضاء السيبراني ————— د. / حمزة الدامي
بين روتين الضحية المنكشف وروتين الجاني المتربص، ولتحقيق هذه المعادلة يجب أن تتوفر
مجموعة من المتغيرات داخل الفضاء السيبراني تتمثل في ما يلي :

1- متغير الإنكشاف الرقمي :

أي أن مدى الإستهداف يرتبط بمدى ظهور الفرد ونشاطه في الفضاء الرقمي. حيث يشير تقرير Verizon إلى أن 68٪ من الخروقات الأمنية سببها العنصر البشري، ليس لضعف التقنية بل بسبب سلوكيات روتينية مثل الضغط على روابط مشبوهة (Verizon, 2024 p:8)؛ مثل روابط "التصيد" أو الوقوع في فخ "الهندسة الاجتماعية" في بيئة التواصل الاجتماعي.

2- متغير الإنكشاف السلوكي عبر (الترصد الخوارزمي) :

في النشاط الروتيني، الجاني لا يبحث عن الضحية بل الخوارزميات هي من تجمعهم، حيث يشير تقرير كاسبيرسكاى أن 40٪ من محاولات التصيد تتم عبر "إعلانات زائفة" على وسائط التواصل الاجتماعي وتستهدف اهتمامات المستخدم (Kaspersky,2024). الضحية تساهم في انكشافها من خلال "التفاعل الروتيني" من خلال (Share,Like) مع صفحات التسوق غير الموثوقة مما يجعل خوارزمية الفايسبوك تضعها في فئة "المهتمين بالشراء" فتظهر لها إعلانات الجناة كجزء من روتينها اليومي. مع "غياب الحارس" وسيكولوجية الدفع المسبق: هنا الجريمة تحدث لأن الضحية تختار سلوكا يفتقر للحماية كاللجوء مثلا للدفع عبر الحوالات البريدية أو الحساب البريدي الجاري ccp في الجزائر مثلا. وهذا ما يعتبر تعطيل طوعي للحارس. الضحية هنا تمارس "الثقة العشوائية" فهي تعتقد أن رقم الحساب هو دليل الهوية بينما يستغل الجاني هذا الروتين لضمان تدفق مالي سريع وغير قابل للاسترداد بمجرد انتهاء اللقاء الرقمي . ونقص غياب الحارس المواقع غير الموثوقة التي لا توفر الأمن للمستخدمين وهو ما توفره منصات التجارة الالكترونية الرسمية.

اذن فالضحية تمارس "انكشافا سلوكيا" عندما تتفاعل مع (السعر غير المنطقي أو المنتج النادر)، فالجاني يعتمد على الاستعجال لإجبار الضحية على تحويل المال (عبر البريد مثلا) قبل ضياع الفرصة.

3- متغير غياب الحارس (إنكشاف الضحية في الفضاءات الرقمية غير المحمية) :

يمثل جوهر الانتقال من "الأمن القني إلى الأمن السوسيولوجي". في هذا السياق لم يعد الحارس مجرد برامج حماية أو جدار حماية، بل هو بروتوكول اجتماعي حمائي يغيب تماما عند الانتقال من مواقع التجارة الرسمية إلى الفايسبوك. ووفقا لنظرية الأنشطة الروتينية: تكتمل الجريمة عند غياب

الحارس، أي في مواقع التسوق الرسمية مثل (Amazon) مثلا يوجد حارس مؤسساتي يتمثل في: نظام تتبع الشحنات - سياسة استرجاع الأموال - تشفير الدفع الالكتروني. أي عند انتقال الضحية للتسوق عبر الفايسبوك هي تقوم (بتجاوز الحارس طوعا) فمنصة التواصل الاجتماعي لا توفر ضمانات تجارية بل هي فضاء للدردشة تحولت إلى سوق غير منظم وهذا الفراغ الرقابي هو ما يستغله الجاني. حيث يشير تقرير Kaspersky إلى أن الجناة يفضلون المنصات الاجتماعية لأنها تسمح بالهندسة الاجتماعية المباشرة. ففي المنصة الاجتماعية يقل حذر الضحية لأنها في بيئة صديقة، الجاني يكسر الحارس النفسي للضحية من خلال المحادثة المباشرة عبر Messenger أو WhatsApp مثلا مما يبني ثقة زائفة تجعل الضحية تقبل بشروط دفع غير آمنة مثل التحويل البريدي. ويمكن أن نفسر كيف تساهم "الهندسة الاجتماعية المباشرة" في الإيقاع بالضحية في ثلاثة نقاط:

- **كسر حواجز الحذر:** في مواقع التجارة الرسمية تكون العلاقة "جامدة" مجرد أزرار وملئ للخانات، أما في الفايسبوك فالعلاقة "تفاعلية" حيث يتيح تطبيق Messenger للجاني التحدث مع الضحية مباشرة واستخدام لغة عاطفية أو دارجة مقنعة مما يبني ثقة زائفة تجعل الضحية يقبل بتحويل المال عبر البريد أو أي وسيلة تحويل مالي إلكتروني.

- **تزييف القبول الاجتماعي:** المنصات الاجتماعية تعطي شعورا بالأمان فالضحية عندما ترى التعليقات Comments (المزيفة أصلا) وعدد الإعجابات Likes ، فهذا النوع من الهندسة الاجتماعية يقيد التفكير النقدي لدى الضحية ويجعلها تعتقد أن "الجميع يشتري" و راض فلا داعي لأية ضمانات.

- **التكيف اللحظي:** الجاني يراقب ردود أفعال الضحية في المحادثة، فإذا خافت الضحية يقوم بطمأننتها بأسلوب الهندسة الاجتماعية مثلا (إرسال صورة بطاقة هوية مزيفة أو فيديو للسلعة التي يروج لها) لإقناع الضحية بأن العملية آمنة تماما.

♦ يركز هذا المُحدد السوسولوجي على الممارسات الروتينية وإنتاج الفرصة الإجرامية، وهنا نسلط الضوء على "الفعل"، حيث تتحول الممارسات اليومية الرقمية للضحية إلى آلية " لتحديد الحارس الكفاء". وبالتالي تتحول عفوية الروتين الاستهلاكي كالدفع غير الآمن هي التي تصنع "الفرصة الإجرامية" محولة السلوك العادي إلى ثغرة تسمح للجاني بالإختراق.

المحدد الثالث - قصور التنشئة الاجتماعية الرقمية (التمثيلات الاجتماعية للضحية وآليات الوصم) :

المحددات السوسيولوجية للضحية في الفضاء السيبراني ————— د. / حمزة الدامي
هنا ننتقل بالتحليل من "الفعل الإجرامي" إلى "صدى الفعل" داخل البناء الاجتماعي ، وبلاستناد إلى ما قاله غوفمان Goffman بما يتعلق "بنظرية الوصم" فإن الضحية السيبرانية لا يلحقها الضرر كخسارة مادية فحسب بل كعملية "تلوث للهوية".

اذ يرى أن المجتمع يضع تصنيفات مسبقة لما يجب أن يكون عليه الفرد (الطبيعي و العاقل) ، و عندما يقع الفرد ضحية للإحتيال مثلا فإنه يكتسب "سمعة" تجعله مختلفا سلبيا عن الآخرين مما يؤدي إلى التخفيض من صورته في الوعي الجمعي من انسان كامل الأهلية إلى انسان موصوم Stigmatized بالسذاجة أو نقص التقدير (Goffman, 1963 p:3).

وقد أعطى غوفمان تصورا سوسيولوجيا يمكن أن نفسر به ديناميكية إدارة الهوية والتحصين الإجرامي ، حيث تكمن الخطورة السوسيولوجية للوصم في دفع الضحية لممارسة ما يسميه غوفمان (بإدارة المعلومات Information control أو إدارة الانطباعات) حيث يلجأ المتضرر إلى الصمت المتعمد وإخفاء ما حل به "لتجنب تلوث الهوية" أمام الجماعة. هذا التمثل الاجتماعي الذي يربط بين وقوع الفرد ضحية والفشل العقلي أو الطمع، ويعمل كآلية رقابة اجتماعية قمعية تحقق حصانة غير مباشرة للجاني المحفز (Ibid, p:4-5).

فمن خلال لوم الضحية يضمن الجاني صمت ضحاياه، مما يحول البيئة الثقافية إلى درع يحمي "مثلث الاستهداف" من الانهيار ويحول الجريمة من حدث يستوجب العقاب إلى وصمة تستوجب الخجل. ومن أهم هذه التمثلات السلبية نجد التنشئة الاجتماعية الرقمية الخاطئة أبرزها ما يلي :

1- قصور التنشئة وتأثير التمثلات الاجتماعية :

وفي هذا السياق يشير تقرير GTC إلى أن الفجوة الكبرى عالميا ليست في القوانين، بل في الوعي البشري ونقص برامج التنشئة الموجهة للأفراد (Global Tech Council, 2025). اذن بما أن التنشئة الرقمية قاصرة ومختلة فإن المجتمع يطور "تمثلات خاطئة عن الضحية" من أهم هذه التمثلات "الوصم" أي بدلا من نقد نظام التنشئة أو لوم الجاني، نجد أن المجتمع يلوم الضحية ويتهمها (بالغباء أو الطمع).

هذا القصور في التنشئة يؤدي إلى تكرار الوقوع كضحية، لأن هذه الأخيرة لا تدرك جذور خطئها السلوكي وتخشى لوم المجتمع فتفضل هدفا سهلا، وهذا التمثل يحول الجريمة من "فعل إجرامي إلى فشل شخصي للضحية".

2- ثُمُّل "القانون لا يحمي المغفلين" (الوصمة القانونية - الإجتماعية) :

هذه المقولة منتشرة في العديد من الدول العربية، ففي هذه الحالة يُنظر للضحية التي تبلغ عن متحيل فايسبوكي لدى السلطات على أنها تضع نفسها في موضع سخريّة. حيث يشير التقرير Gi 2024 للمنطقة العربية إلى أن "ضعف الثقافة السيبرانية" يؤدي إلى "فجوة في التبليغ" (GCI, 2024 p:33). سوسولوجيا هذه الفجوة ليست تقنية بل هي هروب من الوصم. الضحية تفضل أو تجبر على خسارة المال على خسارة صورتها الاجتماعية كإنسان عاقل وهذا ما تفسره نظرية الوصم للعالم غوفمان.

3- وصمة الإبتزاز العاطفي الجنسي :

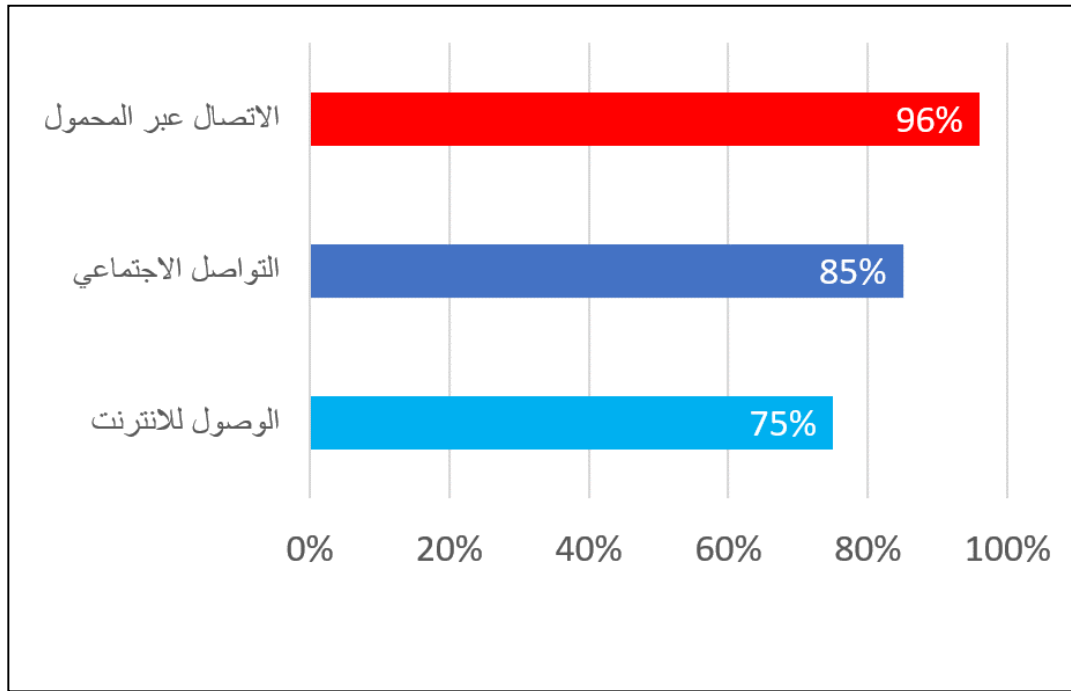
هنا الوصمة لا تمس الذكاء بل تمس الشرف والسمعة سواء كانت ذكرا أو أنثى تخشى الوصم الأخلاقي الذي لا يرحم، في هذه الحالة تمارس الضحية "الإخفاء القسري" لأن المجتمع لا يرى المبتز كجاني فقط بل يرى الضحية كشريك لأنها سمحت لنفسها بالتواصل معه منذ البداية، حيث يشير تقرير IC3 إلى أن هذا النوع من الجرائم يسجل أقل نسبة تبليغ عالميا بسبب "الخجل والوصم" (FBI, 2024 p:18).

♦ يغلق هذا المُحدد السوسولوجي الخاص بالتمثيلات الإجتماعية وآليات الوصم الضلع الثالث في نموذج مثلث الاستهداف بربط الوصم الإجتماعي بتحسين الجاني السيبراني المتحفز، فمن خلال لوم الضحية ووصمها بالسذاجة يجبر المجتمع الضحية على الصمت لحماية صورتها الإجتماعية، هذا الصمت هو الضمانة التي تسمح للجاني بإعادة انتاج نشاطه الإجرامي في بيئة آمنة من الملاحقة.

الجانب التطبيقي للدراسة :

- مؤشرات الإنكشاف السوسيورقمي وعلاقتها بالضحية السيبرانية :

الشكل رقم 2 : مؤشرات الإنكشاف السوسيورقمي في الجزائر 2025



المصدر: من إعداد الباحث بناء على البيانات الإحصائية لتقرير Digital Algeria 2025

- **قراءة في دلالات الروتين الرقمي:** تظهر البيانات الإحصائية الموضحة في الشكل رقم (2) أن المجتمع الجزائري انتقل من "الاستخدام العرضي" للإنترنت إلى مرحلة "الرقمنة البنيوية"؛ حيث تعكس نسبة 96% للاتصال عبر الهاتف المحمول أي أن الفعل الرقمي أصبح ملازماً للحياة اليومية (الروتين). سوسيولوجياً، هذا يعني أن "المجال الخاص" للفرد (بيته، تنقلاته، أسرارته) أصبح متاحاً في المجال العام الرقمي على مدار الساعة، مما يلغي الحواجز المادية التي كانت تحمي الضحية سابقاً. كما تشير نسبة 85% المتعلقة بالنشاط عبر منصات التواصل الاجتماعي إلى أن الفرد الجزائري يقضي معظم روتينه في بيئات افتراضية "مفتوحة". هذا المستوى العالي من التفاعل الاجتماعي الرقمي يخلق ما نسميه "الإنكشاف الإرادي"؛ حيث تقوم الضحية بتزويد الجاني المتحفز بكمية من البيانات (الصور، الأماكن، الآراء، شبكة العلاقات) دون وعي أمني، مما يسهل عملية "الرصد السوسيولوجي" للضحية قبل استهدافها.

- العلاقة بمثلث الإستهداف (الجاني - الضحية):

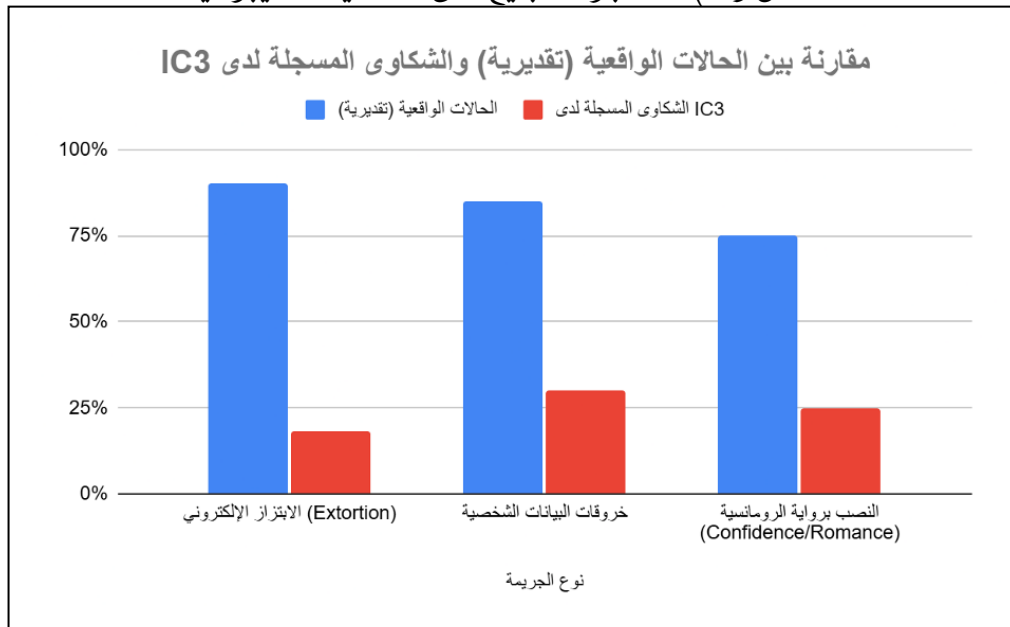
يؤكد الرسم البياني أن التكنولوجيا في الجزائر وفرت "الفرصة المهيأة" للجريمة. فبينما يمثل النفاذ للشبكة 75٪ البنية التحتية، يمثل الهاتف المحمول 96٪ أداة الانكشاف الدائم. هذا التقاطع يقلص المسافة السوسيولوجية بين الجاني والضحية؛ فالجاني لا يحتاج لبذل جهد في البحث عن ضحاياه، بل يكفي بمراقبة الروتين الرقمي المكثف والمنكشف الذي تظهره الأعمدة البيانية، لاختيار اللحظة المناسبة للاختراق أو الابتزاز.

- **الاستنتاج السوسيولوجي:** نستخلص من الشكل البياني أن مشكلة الاستهداف في الجزائر ليست تقنية محضة، بل هي ناتجة عن فجوة وعي؛ فبينما تطورت معدلات الاتصالية بشكل انفجاري، ظل الوعي بمخاطر الانكشاف ثابتاً، مما جعل من الضحية "هدفاً سهلاً" في فضاء سيبراني يفتقر إلى الرقابة الذاتية أو الضبط الاجتماعي الكافي.

- مؤشرات الرقم الأسود في الجرائم السيبرانية وعلاقتها بالضحية :

يوضح لنا الشكل رقم 3 والشكل رقم 4 تفسيرات سوسيولوجية لوجود الرقم الأسود في الجرائم السيبرانية مما يوسع من دائرة الاستهداف الإلكتروني للضحية.

الشكل رقم 3 : فجوة التبليغ لدى الضحية السيبرانية



المصدر: من إعداد الباحث بناء على البيانات الإحصائية لتقرير مركز الشكاوى IC3

FBI /

المحددات السوسيولوجية للضحية في الفضاء السيبراني ————— د. حمزة الدامي

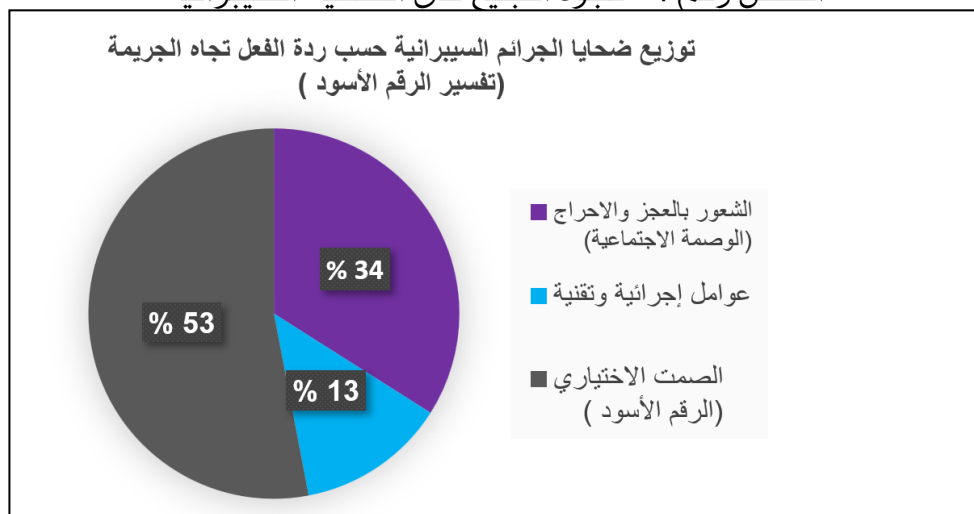
- تحليل فجوة الابتزاز الإلكتروني (أعلى فجوة): تظهر البيانات أن هناك تفاوتاً حاداً في جريمة الابتزاز؛ فبينما تقع بنسبة 90٪ في الواقع الافتراضي، لا تتجاوز نسبة التبليغ الرسمي لدى مركز الشكاوى 18٪. سوسيولوجياً، هذه الفجوة التي تبلغ 72٪ تمثل الرقم الأسود في أبهى صورهِ؛ حيث ينجح الجاني في تحويل الوصمة الاجتماعية إلى جدار صمت يمنع الضحية من المطالبة بحقوقها، مما يجعل الجريمة تمر دون أثر قانوني.

- تحليل فجوة النصب العاطفي والرومانسية: سجلت هذه الفئة فجوة مقدارها 50٪ (بين 75٪ وقوعاً و25٪ تبليغاً). هذا الرقم يعكس "سيكولوجية الخجل"؛ فالضحية هنا لا تخشى القانون، بل تخشى "السخرية الاجتماعية أو فقدان المكانة" إذا عُرف أنها وقعت ضحية تلاعب عاطفي. الجاني المتحفز يدرك هذه النسبة جيداً، ويستخدمها كأداة ضغط لضمان عدم وصول البلاغ إلى الحارس الكفاء.

- مقارنة خروقات البيانات بالجرائم السلوكية: نلاحظ أن فجوة التبليغ في "خروقات البيانات" أقل نسبياً، حيث بلغت نسبة التبليغ 30٪ من أصل 85٪. التفسير السوسيولوجي لذلك هو أن سرقة البيانات غالباً ما تُعتبر "خطأً تقنياً" لا يمس شرف الضحية أو سمعتها الشخصية بشكل مباشر، مما يقلل من حدة الوصمة الاجتماعية ويزيد من جرأة الضحية على التبليغ مقارنة بجرائم الابتزاز.

- علاقة الجاني بالرقم الأسود: لا يحتاج الجاني السيبراني للاطلاع على الإحصائيات ليُدرك وجود الرقم الأسود، بل يستمد ثقته من المناخ الاجتماعي الذي يوصم الضحية ويجبرها على الصمت. إن المعرفة السوسيولوجية للجاني بنقاط ضعف المجتمع (الخوف من الفضيحة) هي المحرك الأساسي الذي يجعله يطمئن لغياب الحارس الكفاء ويستمر في نشاطه الإجرامي.

الشكل رقم 4 : فجوة التبليغ لدى الضحية السيبرانية



المصدر: من إعداد الباحث بناءً على البيانات الإحصائية لتقرير Norton 2021

في علم إجتماع الجريمة، الرقم الأسود ليس مجرد نقص بيانات، بل هو سلوك إجتماعي متعمد وذلك ما سنعتمد عليه في تحليل وتفسير بيانات الشكل رقم 4 الذي يعتمد على مجموعة من النقاط تتمثل في :

صناعة الوصمة (Social Stigma) :

يشير تقرير نورتون إلى أن 34٪ من الضحايا شعروا بالعجز/الضعف. سوسيولوجياً، هذا الشعور يتحول إلى (وصمة) لأن المجتمع الرقمي يقدس (الذكاء التقني). الضحية يخشى أن يُصنف كشخص (جاهل أو ساذج)، فيختار العزلة الاختيارية (الصمت) لحماية مكانته الاجتماعية.

تطبيع الجريمة (Normalization) :

التقرير يظهر أن 53٪ لم يبلغوا. هذا الصمت يؤدي إلى ما نسميه (تطبيع الجريمة السيبرانية)، حيث تصبح الجريمة جزءاً من المخاطر اليومية التي تتحملها الضحية بصمت بدلاً من مواجهتها قانونياً، خوفاً من (الفضيحة أو الوصمة).

ربط النتائج بـ مثلث الإستهداف السوسيورقمي :

تقوم نظرية مثلث الإستهداف على ثلاثة أضلاع: (جاني سيبراني متحفز، ضحية سيبرانية مستهدفة، غياب الحارس الكفاء). في التحليل التالي نلاحظ كيف تنعكس نتائج تقرير نورتون على مثلث الاستهداف :

الضلع الأول: الضحية المستهدفة (Suitable Victim) :

من التقرير يظهر أن الضحايا في المنطقة العربية (الإمارات والسعودية) يقضون ساعات طويلة في إصلاح الأضرار.

التحليل: الوصمة تجعل الضحية هدفاً سهلاً ومثالياً مراراً وتكراراً؛ لأن الجاني يدرك أن الضحية الذي يخجل من التبليغ لن يلاحقه قانونياً. الصمت هنا يحول الضحية إلى "صيد مستمر".

الضلع الثاني: غياب الحارس الكفاء (Absence of Capable Guardian) :

نلاحظ من التقرير أن نسبة التبليغ متدنية ولا تتجاوز 47٪.

التحليل: "الحارس الكفاء" (الشرطة، أنظمة الحماية) يتعطل ليس بسبب نقص القوة، بل بسبب نقص المعلومات. الوصمة الاجتماعية تبني جداراً يعزل الحارس عن الضحية. عندما يختار 53٪ من الضحايا الصمت، فإن "الحارس الكفاء" يصبح أعمى إحصائياً، مما يخلق بيئة آمنة للجاني.

الضلع الثالث: الجاني السيبراني المتحفز (Motivated Offender) :

التحليل: الجاني يستغل الرقم الأسود كدرع حماية، هو يتحفز أكثر عندما يعلم أن الثقافة الاجتماعية (الوصمة) في مجتمع ما تمنع الضحايا من الكلام. هنا، تصبح الوصمة الاجتماعية هي أفضل حليف للجاني. ومن خلال تحليل بيانات تقرير Norton2021، يتضح أن الجريمة السيبرانية لا تكتمل أركانها تقنياً فحسب، بل سوسيولوجياً أيضاً. فبينما يشير التقرير إلى وجود فجوة تبليغ تصل لـ 53٪ (الرقم الأسود)، نجد أن هذا الصمت هو نتاج مباشر للوصمة والشعور بالعجز المشار إليه في الدائرة النسبية أعلاه. وبتطبيق ذلك على مثلث الاستهداف، نجد أن هذه الوصمة تؤدي إلى شلل ضلع الحارس الكفاء، مما يمنحه غياباً حكماً يغري الجاني المتحفز باستمرار استهداف الضحية التي اختارت الاختفاء خلف الرقم الأسود اتقاءً للوصمة الاجتماعية. وبذلك، تصبح الوصمة هي المحرك الأساسي لاستمرار حلقة الاستهداف في الفضاء الرقمي.

نتائج الدراسة

خلصت الدراسة إلى أن عملية التحول إلى ضحية سيبرانية ليست حدثاً تقنياً عارضاً، بل هي نتاج تفاعل بنيوي وسلوكي ومعرفي تكتمل أركانه داخل مثلث الاستهداف الذي سيتم ربط النتائج المستخلصة بكل ضلع من أضلاع هذا المثلث.

1- **ضلع الإنكشاف الرقمي (الروتين الرقمي):** أثبتت الدراسة أن انتقال المجتمع نحو الرقمنة البنيوية بنسبة نفاذ تقدر بـ 96٪ عبر استخدام الهاتف الذكي (في الجزائر كنموذج ممثل للبيئة العربية). ما حول بذلك الفعل الرقمي من ممارسة عارضة إلى روتين يومي ملازم مما أنتج حالة من الإنكشاف الإرادي التي قلصت المسافة السوسيورقمية بين الجاني والضحية داخل مثلث الاستهداف.

- **الربط بنموذج مثلث الإستهداف السوسيورقمي:** تمثل هذه النتيجة الجوهرية لضلع الإنكشاف حيث تحول الفرد من (فاعل اجتماعي إلى هدف مرصود خوارزمياً). إن الروتين الرقمي في المجتمع يغذي هذا الضلع من خلال تزويد الجاني بالمعلومات الكافية لبناء بروفایل الضحية وتوقع سلوكها مما يقلص المسافة السوسيورقمية بين الضحية والجاني ويسهل عملية الاستهداف.

2- **ضلع الإستغلال الرقمي (علاقة الوصم بالرقم الأسود):** كشفت الدراسة عن فجوة تبليغ هائلة (الرقم الأسود) وصلت إلى 72٪ في جرائم الابتزاز، حيث اختار 53٪ من الضحايا الصمت الاختياري، وشعر 34٪ منهم بالعجز. الصمت هنا هو سلوك اجتماعي متعمد ناتج عن الوصمة الاجتماعية، حيث يتم استغلال التمثلات الاجتماعية (الفضحية) كأداة ضغط لشل إرادة الضحية.

- **الربط بنموذج مثلث الإستهداف السوسيورقمي:** يمثل هذا تفعيلًا لضع الاستغلال الرقمي، فالتنشئة الرقمية القاصرة والهشاشة المعرفية جعلت الضحية تستسلم لآليات الوصم، مما حول الوسيط الرقمي من أداة تواصل إلى أداة عزل اجتماعي.

3- **ضع الجاني السيبراني المتحفز (استغلال غياب الحارس الكفاء):** خلصت الدراسة إلى أن الجاني يمارس نوعًا من المناورة، فهو يستمد قوته الإجرامية من "الحصانة الاجتماعية" التي يمنحها له صمت الضحية داخل المجتمع. حيث تتدنى نسبة التبليغ الرسمي إلى 18٪ في جرائم الابتزاز، وذلك لا يعكس فشل الأجهزة الأمنية بقدر ما يعكس نجاح الجاني في عزل الضحية عن الحارس الكفاء سوسيولوجيًا من خلال المراهنة على رد فعل المجتمع تجاه الضحية.

- **الربط بنموذج مثلث الاستهداف السوسيورقمي:** هنا يتقاطع ضعف الجاني المتحفز مع غياب الحارس الكفاء، فالوصمة تبني جدارًا يعطل ميكانيزمات الحماية الرسمية. الجاني هنا يزداد تحفزًا عندما يدرك أن النظام القيمي للمجتمع سيوجه لومه للضحية بدلًا من ملاحقة المجرم. مما يغلق أضلاع المثلث الثلاثة بإحكام.

التوصيات المقترحة لكسر مثلث الاستهداف السوسيورقمي :

1- **توصيات موجهة لكسر ضعف الإنكشاف الرقمي (إدارة الروتين الرقمي) :**

- عقلنة الروتين الرقمي : ضرورة الانتقال من التوعية التقنية الجافة إلى برامج تربية سوسيورقمية تهدف إلى توعية المستخدمين حول الخصوصية في الفضاء الافتراضي وكيفية حمايتها كفعل مقاوم للانكشاف الإرادي.

- مبدأ الحد الأدنى من البيانات : تشجيع الأفراد على تعديل أنماطهم السلوكية اليومية لتقليص كمية البيانات السوسيولوجية المتاحة رقميًا ، مما يصعب عملية "الرصد" التي يقوم بها الجاني لبناء بروفايل الضحية.

2- **توصيات موجهة لكسر ضعف الإستغلال الرقمي (مواجهة الوصمة والهشاشة) :**

- تفكيك ثقافة الوصمة : إطلاق حملات وطنية تهدف إلى تغيير التمثيلات الاجتماعية السلبية تجاه الضحية ، و التركيز على أن الضحية (مجني عليها) و (ليست منذبة) . لكسر جدار الصمت الذي يغذي الرقم الأسود.

- ردم فجوة الهشاشة المعرفية : بإدراج المواطنة الرقمية في المناهج التعليمية منذ الصغر ، ليس كمهارة تقنية فحسب بل كمنظومة قيمية بمنح الفرد الحصانة المعرفية لمواجهة الابتزاز دون الخوف من الوصمة.

3- **توصيات موجهة لتعزيز ضعف الحارس الكفاء (الحد من مناورة الجاني) :**

المحددات السوسيولوجية للضحية في الفضاء السيبراني ————— د. / حمزة الدامي

- ثقافة التبليغ : استحداث منصات تبليغ رقمية تتميز بالسرية المطلقة لتقليل خوف الضحية من الفضيحة مما يحول الحارس الكفاء إلى قوة رادعة وفاعلة.

- تفعيل دور الحارس الإجتماعي : تعزيز دور الأسرة ومؤسسات التنشئة الاجتماعية كحارس "داعم" و ليس "معاقب" لخلق بيئة تتيح للضحية اللجوء للمساعدة في المراحل الأولى للاستهداف قبل مرحلة "شل الإرادة".

4- على المستوى البحثي والأكاديمي :

- اعتماد "نموذج مثلث الإستهداف السوسيورقمي" كأداة تحليلية في الدراسات السوسيولوجية، ودراسات علم الجريمة وكذلك الدراسات الجنائية المستقبلية وتطويره ليشمل متغيرات أخرى قد تظهر مع تطور الذكاء الإصطناعي والواقع الافتراضي.

الخاتمة

إن نموذج مثلث الإستهداف السوسيورقمي يفسر بوضوح أن الجريمة السيبرانية ليست مجرد اختراق تقني. بل هي تفاعل ديناميكي داخل الفضاء السوسيورقمي. فهي تبدأ بالإستهداف بناء على البروفایل الإجتماعي، وتتغذى على الإنكشاف الناتج عن الروتين الرقمي، وتنتهي بالإستغلال عبر تفعيل آليات الوصم وشل إرادة الضحية.

حيث أن "الوصمة الإجتماعية" هي الضلع الأخطر، فهي تغذي الجاني وتكشف الضحية وتعطل الحارس في آن واحد. مما يجعل كسر حلقة الضحية رهينا بتغيير أساليب التنشئة الإجتماعية الرقمية وليس فقط بتعزيز الترسانة التقنية.

وبناء عليه تستنتج الدراسة أن المقاربات الأمنية والتقنية الصرفة تظل قاصرة عن احتواء ظاهرة الإجرام السيبراني ما لم يقترن ذلك بترميم سوسيولوجي لمنظومة القيم المجتمعية. فكسر مثلث الإستهداف السوسيورقمي يبدأ بتجريد الجاني من أقوى أسلحته النفسية وهي المناورة بالوصمة الإجتماعية التي تقتات على خوف الضحية وتمنعها من طلب الحماية، مما يحول الخوف من مجرد الشعور بالتهديد إلى عامل ميسر لعمية التحول إلى ضحية.

الهوامش و المراجع :

المراجع العربية :

- موسوعة النظرية الجنائية، (2010)، إعداد مجموعة من الخبراء، القاهرة، المركز القومي للبحوث الاجتماعية والجنائية.

- عبد الفتاح، أحمد فوزي، (2021)، تحليل تأثير جائحة كورونا (Covid-19) على ارتفاع معدلات الجرائم السيبرانية في مصر: دراسة تحليلية جنائية وسوسيولوجية، المجلة الجنائية القومية، المركز القومي للبحوث الاجتماعية والجنائية، المجلد 64، العدد 2.

- مجموعة الرواد للإدارة والتدريب (RMG) ، (2026) ، الفجوة الرقمية: فهم التحديات العالمية والحلول المبتكرة،
https://www.rmg-sa.com/الفجوة-الرقمية-فهم-التحديات-العالمية/ (تم التصفح يوم 27 / 03 / 2026 ، الساعة
13:15).

المراجع الأجنبية :

- Castells, Manuel, (2005), The Network Society: A Cross-cultural Perspective, United Kingdom, Edward Elgar Publishing, p. 07.
- DataReportal, (2025), Digital 2025: Algeria, <https://datareportal.com/reports/digital-2025-algeria> (Accessed: 14/02/2026, 21:10)
- NortonLifeLock, (2021), The Norton Cyber Safety Insights Report 2021: Global Results (FullPDFReport), <https://www.nortonlifelock.com/content/dam/nortonlifelock/docs/reports/norton-cyber-safety-insights-report-2021.pdf> (Accessed: 11/01/2026, 14:35)
- Federal Bureau of Investigation (FBI), (2024), Internet Crime Report 2023 (Full PDF Report), https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf (Accessed: 11/01/2026, 15:10)
- Verizon, (2024), 2024 Data Breach Investigations Report (DBIR) – Full PDF Report, <https://www.verizon.com/business/resources/reports/dbir/> (Accessed: 13/01/2026, 10:15).
- Kaspersky, (2024), Kaspersky Security Bulletin 2024: Consumer Threats and Statistics – Full PDF Report, <https://securelist.com/ksb-2024-statistics/114795/> (Accessed : 11/01/2026, 14:30).
- Kaspersky, (2024), What is Cybercrime: Risks and Prevention, <https://me.kaspersky.com/resource-center/threats/what-is-cybercrime> (Accessed: 11/01/2026, 14:30).
- Hadnagy, Christopher, (2018), Social Engineering: The Science of Human Hacking, 2nd Edition, Indianapolis, John Wiley & Sons, Inc.
- Zuboff, Shoshana, (2019), The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, New York, PublicAffairs.
- Silva, Fabricio Sales, (2015), Digital Eye: Surveillance, Power and Resistance in the Digital Age, London, Routledge.
- European Union Agency for Cybersecurity (ENISA), (2023), ENISA Threat Landscape 2023 – Full PDF Report, <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023> (Accessed: 13/01/2026, 10:45).

- Holt, Thomas J., (2023), Cybercrime and Digital Forensics: An Introduction, London, Routledge .
- McKee, Adam J., (2026), Cyber Victimization Definition: Criminal Justice Glossary, <https://docmckee.com/cj/docs-criminal-justice-glossary/cyber-victimization-definition> (Accessed: 12/01/2026, 09:40)
- Prensky, Marc, (2001), Digital Natives, Digital Immigrants, The Technology Source, Vol. 9, No. 5, https://www.technologysource.org/article/digital_natives_digital_immigrants/ (Accessed: 12/01/2026, 10:15).
- Abdullah, A. & Jahan, I., (2020), Cybercrime Victimization: A Systematic Review, International Journal of Research and Review (IJRR), Vol. 7, No. 5.
- Sarkki, Salla, (2025), Fear of Cybercrime in Europe: Examining the Role of Individual and Contextual Factors, Journal of Criminal Justice, Vol. 97, Article 102315, <https://doi.org/10.1016/j.jcrimjus.2025.102315>(Accessed: 15/02/2026, 11:45)
- Council of Europe, (2026), Operational Guide to Cybercrime: Investigation and International Cooperation, 2nd Edition, Strasbourg, Council of Europe Publishing.
- Felson, Marcus, (2002), Crime and Everyday Life, 3rd Edition, Thousand Oaks, CA: Sage Publications.
- Goffman, Erving, (1963), Stigma: Notes on the Management of Spoiled Identity, Englewood Cliffs, NJ: Prentice-Hall.
- Global Tech Council, (2025), Global Cybersecurity Awareness and Education Report: Closing the Human Gap, 2nd Edition.
- ITU, (2024), Global Cybersecurity Index (GCI) 2024: Regional Profile: Arab States, International Telecommunication Union.