الدارك ويب كمنصة للجرائم السيبرانية: دراسة حالة في الأمن السيبراني

الأستاذ: ياسر عامر عبدالرضا
القسم: هندسة تقنيات الامن السيبراني

جدول المحتويات

1.المقدمة

يشهد العالم في العصر الرقمي توسعًا متسارعًا في استخدام الإنترنت والتقنيات الحديثة في مختلف مجالات الحياة، بدءًا من التعليم والخدمات الحكومية، ووصولًا إلى القطاعات المالية والصحية والصناعية. ومع هذا التوسع الكبير، برزت تحديات أمنية متزايدة تتعلق بحماية البيانات، وضمان سرية المعلومات، والحفاظ على سلامة الأنظمة الرقمية من التهديدات والهجمات السيبرانية. وفي هذا السياق، أصبح من الضروري دراسة البيئات الرقمية التي تشكل مصدرًا مباشرًا أو غير مباشر لتلك التهديدات، ويأتي الدارك ويب في مقدمة هذه البيئات بسبب ارتباطه المتكرر بالأنشطة غير القانونية والجرائم السيبرانية المنظمة (Patsakis et al., 2024)

ولا يُنظر إلى الدارك ويب بوصفه مجرد جزء مخفي من الإنترنت فقط، بل باعتباره فضاءً رقميًا معقدًا يتداخل فيه الجانب التقني مع الجانب الإجرامي والتنظيمي. فهذه البيئة لا تُستخدم حصريًا للأغراض الإجرامية، إذ توجد لها استخدامات قانونية تتعلق بحماية الخصوصية وحرية التعبير في بعض البيئات المقيدة، إلا أن كثيرًا من الدراسات والتقارير الأمنية تشير إلى أنه أصبح أيضًا ملاذًا مناسبًا للمجرمين الإلكترونيين لتبادل الأدوات، وبيع البيانات المسروقة، وتقديم خدمات الاختراق والاحتيال، مستفيدين من صعوبة التتبع وارتفاع مستوى إخفاء الهوية (Jardine, 2015; Liggett et al., 2020)

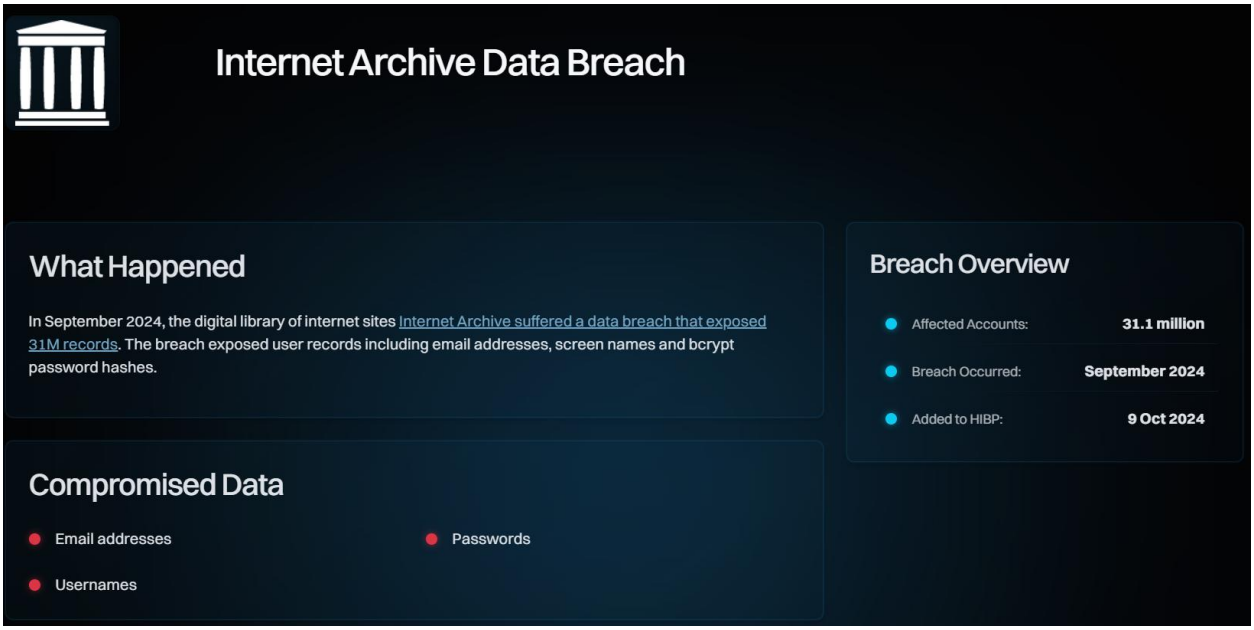
ومن هنا تكتسب دراسة الدارك ويب أهمية خاصة في مجال الأمن السيبراني، لأن فهم طبيعته وطرق استغلاله يسهم في كشف جانب مهم من سلسلة التهديدات الرقمية التي تواجه الأفراد والمؤسسات. كما أن تحليل هذا الفضاء يساعد في فهم كيفية انتقال الجريمة السيبرانية من كونها نشاطًا فرديًا محدودًا إلى نشاط منظم قائم على أسواق وخدمات وشبكات تواصل، الأمر الذي يزيد من تعقيد مشهد التهديدات ويجعل مواجهته أكثر صعوبة (Lusthaus, 2019)

2.مشكلة الدراسة

تتمثل مشكلة هذه الدراسة في أن الدارك ويب بات يشكل بيئة خصبة لنمو الجرائم السيبرانية وتطورها، وذلك بسبب ما يتيحه من خصائص مثل إخفاء الهوية، وصعوبة التتبع، وتوفير أسواق ومنتديات متخصصة في تداول السلع والخدمات غير المشروعة. ولم تعد هذه الجرائم تقتصر على أفراد يمتلكون مهارات تقنية عالية، بل أصبح بالإمكان شراء الأدوات والخدمات الجاهزة من خلال هذه المنصات، بما يجعل تنفيذ الجرائم الرقمية أكثر سهولة واتساعًا وانتشارًا (Lusthaus, 2019; Patsakis et al., 2024)

وتزداد خطورة هذه المشكلة عندما نأخذ بعين الاعتبار أن كثيرًا من الأصول الرقمية التي تُباع أو تُتداول في الدارك ويب ترتبط بشكل مباشر بأمن المعلومات، مثل كلمات المرور، وحسابات البريد الإلكتروني، وملفات تعريف المستخدمين، وبيانات البطاقات المصرفية، وأدوات البرمجيات الخبيثة، وخدمات الوصول إلى الشبكات المخترقة. وهذا يعني أن الدارك ويب لا يشكل مجرد تهديد نظري، بل يمثل خطرًا عمليًا ومستمرًا على الأفراد والمؤسسات والبنى التحتية الرقمية (Brau et al., 2025)

وعليه، فإن المشكلة الحقيقية لا تكمن فقط في وجود هذا الفضاء الرقمي، بل في تحوله إلى منصة تمكينية تدعم الاقتصاد الإجرامي السيبراني، وتربط بين الفاعلين المختلفين داخل سلسلة الجريمة، من مطوري البرمجيات الخبيثة إلى بائعي البيانات المسروقة والمشترين الذين يستخدمونها في الاحتيال والابتزاز وهجمات الفدية.

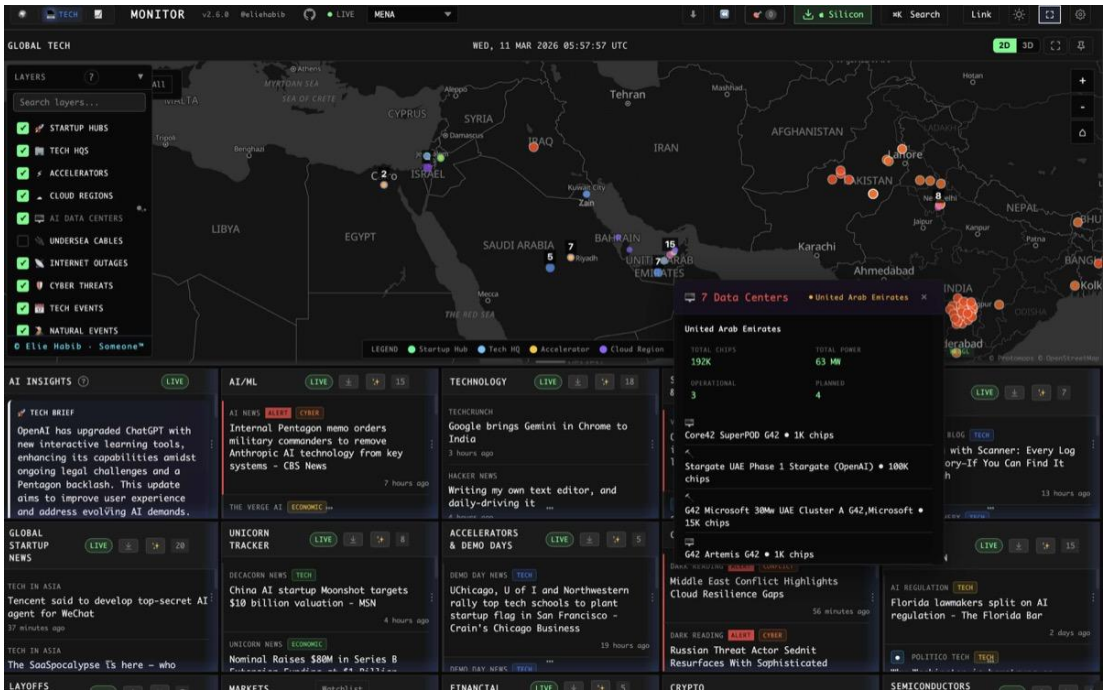


3.أهمية الدراسة

تستمد هذه الدراسة أهميتها من عدة جوانب مترابطة. أولًا، إنها تسلط الضوء على واحد من أخطر المسارات الحديثة في تطور الجريمة السيبرانية، وهو اعتماد المجرمين على بيئات خفية ومنظمة لتسويق الأنشطة غير القانونية وتبادل الأدوات والخدمات. ثانيًا، تساعد هذه الدراسة في توضيح العلاقة بين الدارك ويب وأمن المعلومات، وبيان كيف يمكن للأنشطة التي تجري في هذه البيئة أن تنعكس بشكل مباشر على المؤسسات من خلال تسريب البيانات، أو تمكين الاختراقات، أو تسهيل الوصول غير المصرح به إلى الأنظمة الحساسة (Liggett et al., 2020)

ثالثًا، توفر هذه الدراسة بعدًا توعويًا مهمًا، لأنها لا تكتفي بعرض الجانب التقني للدارك ويب، بل توضّح أيضًا أثره التنظيمي والأمني والاستراتيجي. فالمؤسسات التي لا تدرك طبيعة هذه البيئة قد تنظر إلى الهجمات السيبرانية باعتبارها حوادث معزولة، بينما تكشف الأدبيات أن كثيرًا من هذه الهجمات ترتبط بمنظومات أوسع من التبادل والخدمات الإجرامية التي تبدأ أو تتوسع عبر الدارك ويب (Samtani et al., 2021)

رابعًا، تساعد الدراسة في دعم التفكير الوقائي والاستباقي داخل المؤسسات الأكاديمية والإدارية، من خلال إبراز أهمية الاستخبارات السيبرانية، ومراقبة مؤشرات التسريب، وفهم التهديدات قبل أن تتحول إلى اختراقات فعلية. وهذا يجعل الدراسة ذات قيمة علمية وعملية في الوقت نفسه، خصوصًا في ظل التزايد المستمر في اعتماد المجتمعات على الأنظمة الرقمية والخدمات الإلكترونية (Patsakis et al., 2024)



4.أهداف الدراسة

تهدف هذه الدراسة إلى تحقيق مجموعة من الأهداف العلمية والعملية، ويمكن تلخيصها في النقاط الآتية. أولًا، التعريف بمفهوم الدارك ويب وبيان طبيعته التقنية وخصائصه التي تميزه عن الشبكة السطحية والويب العميق. ثانيًا، توضيح كيف أصبح الدارك ويب منصة تستخدم في تسهيل الجرائم السيبرانية ودعمها. ثالثًا، عرض دراسة حالة حقيقية تبيّن كيفية استغلال هذا الفضاء في بيع البيانات المسروقة وتمكين الهجمات الإلكترونية. رابعًا، تحليل الآثار المباشرة وغير المباشرة لهذه الأنشطة على أمن المعلومات والمؤسسات الرقمية. خامسًا، اقتراح مجموعة من التدابير والتوصيات التي يمكن أن تساعد على تقليل المخاطر المرتبطة بالدارك ويب والحد من تأثيره على الأمن السيبراني.

5.الإطار النظري

يشير الإطار النظري للدراسة إلى أن الدارك ويب يمثل جزءًا من الإنترنت لا يظهر في محركات البحث التقليدية، ويُتاح الوصول إليه غالبًا عبر شبكات خاصة مثلTor ، التي توفر طبقات من إخفاء الهوية لكل من المستخدم والمضيف. وقد نشأت هذه التقنية في الأصل لأغراض تتعلق بالخصوصية والأمان، إلا أن توظيفها في بيئات غير قانونية أدى إلى تحولها إلى بنية تحتية يستفيد منها مجرمو الإنترنت في ممارسة أنشطتهم بعيدًا عن الرصد التقليدي (Jardine, 2015)

ومن منظور علم الإجرام السيبراني، لا يمكن اختزال الدارك ويب في فكرة "الموقع المخفي" فقط، لأن الدراسات الحديثة تصفه بوصفه بيئة اقتصادية واجتماعية إجرامية لها قواعدها وآلياتها. فهناك أسواق متخصصة، ومنتديات مغلقة، وآليات تقييم للبائعين، وأنظمة سمعة، ووسطاء، وحتى خدمات دعم فني في بعض الأحيان. وهذا يعكس مستوى من التنظيم يجعل التعاملات داخل هذه البيئة شبيهة نسبيًا بالأسواق الإلكترونية الشرعية، مع اختلاف جوهري يتمثل في طبيعة السلع والخدمات المتداولة فيها (Liggett et al., 2020)

كما يوضح (Lusthaus, 2019) أن الاقتصاد الإجرامي المرتبط بالدارك ويب لا يعمل بصورة عشوائية أو بدائية، بل يستند إلى تقسيم أدوار واضح بين جهات متعددة، مثل مزودي الوصول، ومطوري البرمجيات الخبيثة، وسماسرة البيانات، والمشترين النهائيين. وهذا التقسيم أدى إلى نشوء ما يُعرف بمفهوم
Cybercrime-as-a-Service، أي الجريمة السيبرانية كخدمة، حيث يمكن لأي شخص تقريبًا شراء خدمة اختراق أو حزمة بيانات أو أدوات احتيال، حتى إن لم يكن يمتلك خلفية تقنية متقدمة.

وعلى المستوى الأمني، تؤكد الدراسات أن مراقبة الدارك ويب أصبحت عنصرًا مهمًا في بناء الاستخبارات السيبرانية، لأن كثيرًا من مؤشرات التهديد تظهر في تلك البيئة قبل أن تظهر آثارها داخل الشبكات المستهدفة. فقد تُعرض بيانات اعتماد موظفين، أو تُناقش ثغرات معينة، أو تُعلن خدمات مرتبطة بجهة مستهدفة، وهو ما يتيح للمؤسسات التي تمتلك أدوات رصد مناسبة أن تتخذ إجراءات وقائية مبكرة (Samtani et al., 2021)

6.دراسة الحالة: سوق Genesis Market

تم اختيار Genesis Market بوصفه نموذجًا واقعيًا بارزًا يوضح كيف يمكن للدارك ويب أن يعمل كمنصة مركزية لتسهيل الجريمة السيبرانية. وتشير البيانات الرسمية الصادرة عن وزارة العدل الأمريكية إلى أن هذا السوق كان متخصصًا في بيع حزم من بيانات الوصول المسروقة، تضمنت أسماء المستخدمين، وكلمات المرور، وملفات تعريف الارتباط، وبصمات المتصفح، وغيرها من البيانات الرقمية التي تُمكّن المشترين من انتحال هوية الضحايا والوصول إلى حساباتهم أو خدماتهم الإلكترونية (Brau et al., 2025)

وتكمن خطورة هذه الحالة في أن السوق لم يكن يبيع معلومات أولية فقط، بل كان يبيع ما يمكن وصفه بـ "الهوية الرقمية الجاهزة"، أي مجموعة بيانات تسمح للمهاجم بتجاوز كثير من ضوابط الحماية التي تعتمد على التحقق من الجهاز أو سلوك المستخدم. وقد أشارت الجهات الرسمية إلى أن المنصة احتوت على بيانات مستخرجة من أكثر من 1.5 مليون جهاز مخترق، وأكثر من 80 مليون بيانات اعتماد، ما يوضح الحجم الكبير لهذا النشاط ومدى تأثيره المحتمل على الأفراد والمؤسسات في مختلف الدول (Brau et al., 2025)

كما أن أهمية هذه الحالة لا تتعلق بحجم البيانات فقط، بل بطريقة تنظيم الخدمة. فوجود سوق منظم يتيح البحث عن البيانات وتصنيفها وشرائها بسهولة يدل على أن الجريمة السيبرانية أصبحت في هذه البيئات أكثر احترافية ومأسسة. وهذا ما يجعل Genesis Market مثالًا واضحًا على انتقال الدارك ويب من كونه مجرد مكان لتبادل الملفات أو التواصل السري إلى كونه سوقًا فعّالًا لتدوير العوائد الإجرامية وتمكين هجمات لاحقة مثل الاستيلاء على الحسابات، والاحتيال المالي، وهجمات الفدية(Patsakis et al., 2024)

7.تحليل دراسة الحالة

تكشف دراسة حالة Genesis Market عن عدة مؤشرات مهمة. أولها أن الدارك ويب يؤدي دورًا محوريًا في ربط مراحل الجريمة السيبرانية ببعضها؛ فالبرمجيات الخبيثة تُستخدم أولًا لسرقة البيانات من الأجهزة، ثم تُنقل هذه البيانات إلى السوق، ثم تُباع لطرف آخر قد يستخدمها في تنفيذ هجوم جديد. وهذه السلسلة توضح أن الجريمة السيبرانية الحديثة لا تُدار دائمًا بواسطة جهة واحدة، بل كثيرًا ما تكون نتيجة تعاون غير مباشر بين عدة أطراف متخصصة داخل الاقتصاد الإجرامي الرقمي (Lusthaus, 2019)

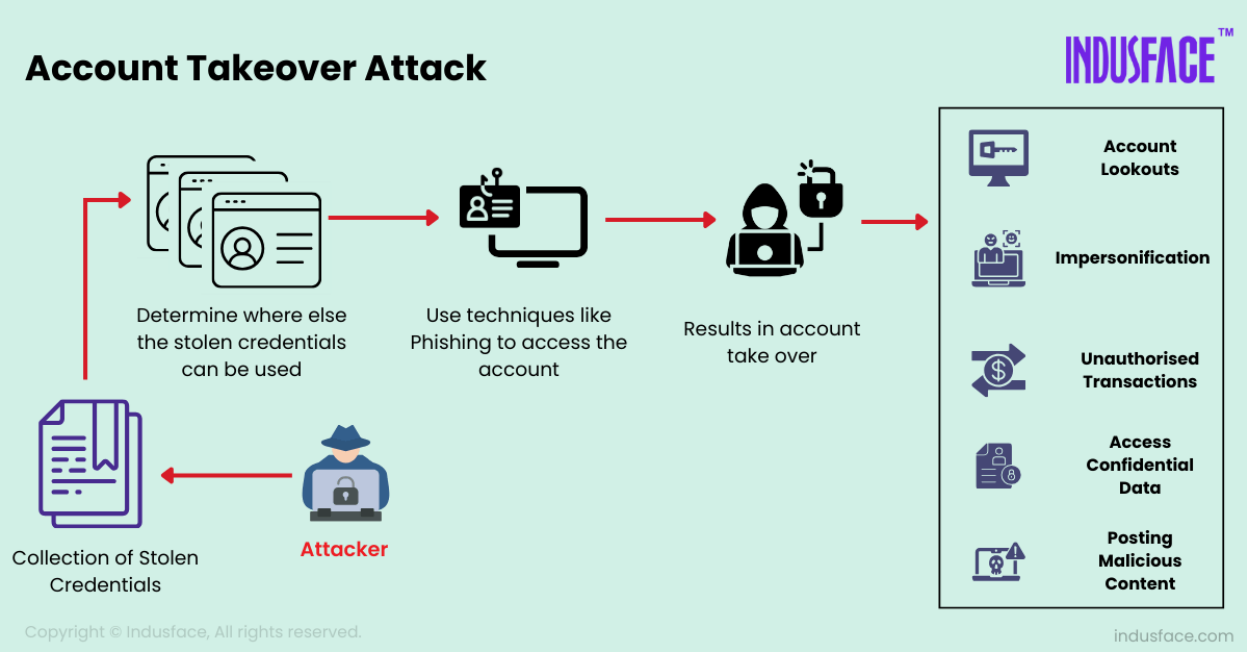
وثانيها أن هذه البيئة تقلل من حاجز الدخول إلى عالم الجريمة السيبرانية، لأن من يريد تنفيذ الاحتيال أو اختراق حسابات لم يعد مضطرًا لتطوير البرمجيات الخبيثة بنفسه أو جمع البيانات ذاتيًا، بل يكفيه شراء ما يحتاجه من أسواق مثل Genesis وهذا يعني أن الدارك ويب لا يزيد فقط من قوة المهاجمين المحترفين، بل يسهم أيضًا في توسيع قاعدة المشاركين في الأنشطة الإجرامية عبر تبسيط الأدوات وتسهيل الوصول إليها (Liggett et al., 2020)

وثالثها أن المؤسسات قد تكون هدفًا غير مباشر حتى لو لم تُخترق أنظمتها مباشرة في البداية. فمثلًا، قد تبدأ المشكلة بتسريب جهاز مستخدم أو موظف، ثم تُباع بياناته عبر السوق، ثم تُستخدم لاحقًا لاختراق أنظمة المؤسسة أو خدماتها المرتبطة بذلك المستخدم. وهذا يبرز أهمية فهم التهديدات من منظور متكامل لا يقتصر على الجدار الناري أو مضاد الفيروسات، بل يشمل سلسلة التهديد بأكملها من نقطة الإصابة الأولى إلى مرحلة الاستغلال النهائي.

8.الانعكاسات على الأمن السيبراني وأمن المعلومات

إن أخطر ما في الدارك ويب من منظور أمن المعلومات هو أنه يحول البيانات المسروقة من مجرد نتائج اختراق إلى أصول قابلة للتداول والاستثمار الإجرامي .فعندما تُباع بيانات الاعتماد، أو تُؤجر أدوات الاختراق، أو يُعرض الوصول إلى الشبكات، تصبح المؤسسة معرضة لخطر متجدد لا ينتهي عند لحظة الاختراق الأولى. وهذا يفرض على المؤسسات تبني نهج أمني أكثر شمولًا يقوم على الافتراض بأن التهديد قد يبدأ خارج حدود الشبكة التقليدية، في منتدى أو سوق أو مجموعة تداول ضمن الدارك ويب (Samtani et al., 2021)

كذلك، فإن اعتماد المجرمين على هذا النوع من الأسواق يجعل الهجمات أكثر مرونة وسرعة. فالمهاجم يمكنه الحصول على بيانات أو أدوات جاهزة خلال وقت قصير، ومن ثم توظيفها في تنفيذ الاحتيال أو الابتزاز أو سرقة الحسابات أو دعم حملات التصيد. وهذا يفسر سبب ازدياد تعقيد مشهد التهديدات، ويؤكد أن التحدي الأمني لم يعد فقط في منع الاختراقات، بل أيضًا في مراقبة البيئة التهديدية الأوسع التي تُدار فيها هذه الأنشطة (Patsakis et al., 2024)



9.التوصيات

بناءً على ما تقدم، فإن من الضروري أن تعتمد المؤسسات على مجموعة من التدابير المتكاملة لمواجهة التهديدات المرتبطة بالدارك ويب. أولًا، ينبغي تعزيز قدرات الاستخبارات السيبرانية الاستباقية من خلال متابعة مؤشرات التسريب والأنشطة المرتبطة باسم المؤسسة أو موظفيها أو خدماتها في البيئات المشبوهة، لأن هذا قد يوفر فرصة للكشف المبكر وتقليل الأضرار قبل وقوعها (Samtani et al., 2021)

ثانيًا، يجب عدم الاكتفاء بكلمات المرور بوصفها وسيلة الحماية الأساسية، بل ينبغي تطبيق المصادقة متعددة العوامل على الأنظمة والحسابات الحساسة، لأن كثيرًا من الخدمات الإجرامية في الدارك ويب تعتمد على سرقة بيانات الدخول وإعادة استخدامها. ثالثًا، ينبغي رفع وعي المستخدمين وتدريبهم على تجنب الرسائل الاحتيالية، والبرمجيات الخبيثة، وممارسات الاستخدام غير الآمن، لأن العامل البشري ما يزال يمثل نقطة ضعف رئيسة في كثير من حوادث الاختراق.

رابعًا، من المهم أن تستثمر المؤسسات في مراقبة السجلات، وتحليل السلوك، وتفعيل خطط الاستجابة للحوادث، بحيث لا يقتصر الأمن على المنع فقط، بل يشمل أيضًا الكشف السريع والاحتواء والتعافي. خامسًا، ينبغي تشجيع التعاون مع الجهات المختصة وإنفاذ القانون، لأن مواجهة الأسواق الإجرامية الكبرى تتطلب تنسيقًا دوليًا وتقنيًا وقانونيًا معقدًا، كما أظهرت عمليات الإطاحة بعدد من المنصات الإجرامية الكبرى خلال السنوات الأخيرة (Brau et al., 2025; Patsakis et al., 2024)

10.الخاتمة

في ضوء ما تقدم، يتبين أن الدارك ويب يشكل تحديًا حقيقيًا ومتزايدًا في مجال الأمن السيبراني، لأنه لم يعد مجرد مساحة رقمية يصعب الوصول إليها، بل تحول إلى بيئة منظمة تدعم الجريمة السيبرانية بمختلف صورها. وقد أوضحت هذه الدراسة، من خلال العرض النظري ودراسة حالة Genesis Market ، أن الدارك ويب يوفر للمجرمين بنية تحتية مناسبة لبيع البيانات المسروقة، وتبادل الأدوات، وتسويق الوصول غير المشروع، وهو ما يجعله عنصرًا مؤثرًا في تصاعد التهديدات الرقمية ضد الأفراد والمؤسسات.

كما يتضح أن التعامل مع هذا التحدي لا يمكن أن يكون محدودًا بالإجراءات التقنية التقليدية فقط، بل يجب أن يقوم على رؤية شاملة تجمع بين الوعي، والحوكمة، والاستخبارات السيبرانية، والتدريب، والاستجابة، والتعاون الدولي. فكلما كان فهم المؤسسة لطبيعة الدارك ويب أعمق، كانت قدرتها أفضل على تقدير المخاطر واتخاذ التدابير الوقائية المناسبة. ومن ثم، فإن دراسة هذا الموضوع لا تمثل أهمية أكاديمية فقط، بل تحمل أيضًا قيمة عملية كبيرة في بناء بيئة رقمية أكثر أمانًا واستقرارًا، بما ينسجم مع متطلبات حماية المعلومات وتعزيز الثقة في المؤسسات الرقمية(Liggett et al., 2020; Patsakis et al., 2024)

المراجع

Brau, B., Itkonen, J., Jeong, J., Lang, M. H., & Niemela, M. (2025). The dark web and capital markets. *Available at SSRN 5288434* .

Jardine, E. (2015). The Dark Web dilemma: Tor, anonymity and online policing. *Global Commission on Internet Governance Paper Series* .(21)

Liggett, R., Lee, J. R., Roddy, A. L., & Wallin, M. A. (2020). The dark web as a platform for crime: An exploration of illicit drug, firearm, CSAM, and cybercrime markets. In *The Palgrave handbook of international cybercrime and cyberdeviance* (pp. 91–116). Springer .

Lusthaus, J. (2019). Beneath the dark web: Excavating the layers of cybercrime's underground economy. 2019 IEEE European symposium on security and privacy workshops (EuroS&PW) ,

Patsakis, C., Arroyo, D., & Casino, F. (2024). The malware as a service ecosystem. In *Malware: Handbook of Prevention and Detection* (pp. 371–394). Springer .

Samtani, S., Li, W., Benjamin, V., & Chen, H. (2021). Informing cyber threat intelligence through dark Web situational awareness: The AZSecure hacker assets portal. *Digital Threats: Research and Practice (DTRAP)*, *2*(4), 1–10 .