الدو افع الأمنية للتعاون السيبر اني بين دول البحر الأبيض المتوسط في ظل تصاعد الحروب والجر ائم السيبر انية (2020–2025)

عبد الصماد باحفيض

باحث بسلك الدكتورة

الكلية متعددة التخصصات، جامعة محمد الاول - الناظور

يشهد العصر الرقمي تحولاً جذرياً في البنى الاجتماعية والسياسية والاقتصادية للدول، حيث لم يعد الفضاء السيبراني مجرد امتداد تقني مكمل، بل أصبح يشكّل جزءاً حيوياً لا يتجزأ من البنية التحتية الوطنية الحيوية. ومع تعاظم الاعتماد على التكنولوجيا في شتى المجالات، تتنامى بالمقابل التهديدات المرتبطة بالأمن السيبراني، ما يفرض على الدول تحديات جديدة ومعقدة تتجاوز الأطر التقليدية للحماية والردع.

أضحت البنى التحتية الحيوية مثل شبكات الطاقة والمياه، وأنظمة النقل، والاتصالات، والخدمات الصحية هدفاً مباشراً للهجمات السيبرانية، التي لم تعد تقتصر على الإرباك أو التخريب، بل قد تمتد إلى المساس بأمن الدولة واستقرارها الداخلي. وفي هذا الإطار، ظهرت "الحرب السيبرانية" كواقع جديد يعيد تشكيل مفهوم الصراع، حيث تؤدي المعلومات دوراً محورياً كسلاح ناعم يستعمل للتأثير السياسي والاقتصادي وحتى العسكري، سواء من قبل دول أم فواعل غير دولية.

وفي ضوء هذا الواقع المعقد، يبرز الفضاء السيبراني في منطقة البحر الأبيض المتوسط كمساحة استراتيجية للتفاعل الأمني، إذ تواجه دول هذه المنطقة تهديدات مشتركة عابرة للحدود، ما يجعل من التعاون الإقليمي في المجال السيبراني ضرورة أمنية لا خياراً. ومع ذلك، تظل جهود التعاون بين هذه الدول محدودة، إما بسبب تفاوت القدرات التقنية والمؤسساتية، وإما نتيجة غياب إطار تنسيقي فعّال قادر على مواكبة حجم التهديدات وتعقيداتها.

وعليه، **فما الدوافع الأمنية الحتمية التي تفرض على دول المتوسط ضرورة تعزيز التعاون الأمني السيبراني فيما بينها؟ وما أبرز التحديات التي تعرقل تحقيق هذا التعاون بشكل فعّال في مواجهة التهديدات السيبرانية المتزايدة؟**

للإجابة عن هذه الإشكالية سنقسم هذه الدراسة على مطلبين:

المطلب الأول: الحروب السيبرانية كتهديد مشترك يستوجب تعاوناً سيبرانياً إقليمياً في منطقة المتوسط

المطلب الثاني: تصاعد الجرائم السيبرانية بين الدول المتوسطية: دافع نحو التعاون الأمني السيبراني

المطلب الأول: الحروب السيبرانية كتهديد مشترك يستوجب تعاوناً سيبرانياً إقليمياً في منطقة المتوسط

في السنوات الأخيرة، تطورت الحروب السيبرانية لتصبح جزءاً لا يتجزأ من الصراعات الدولية، حيث تستعمل الهجمات السيبرانية كأداة استراتيجية في النزاعات بين الدول. في منطقة البحر الأبيض المتوسط، التي تعد مسرحاً للعديد من الأزمات الجيوسياسية، لا تقتصر الهجمات السيبرانية على الهجمات العشوائية، بل تتخذ أبعاداً استراتيجية تهدف إلى إضعاف الخصم، وتجميع المعلومات الاستخباراتية، أو حتى التأثير في العمليات العسكرية. هذه الهجمات قد تشمل استهداف أنظمة الدفاع والطاقة أو مهاجمة أنظمة الاتصال العسكرية؛ لشل قدرة الدولة على اتخاذ قرارات سريعة أو التواصل مع قواتها. مما يُظهر الدور المتزايد الذي تؤديه الحروب السيبرانية في التنافس الإقليمي. هذه التطورات تستدعي توحيد الجهود الأمنية بين دول البحر الأبيض المتوسط لصد الهجمات المعقدة، ومواجهة التهديدات السيبرانية التي تتسم بالسرعة والقدرة على الانتشار العابر للحدود.

كما أن هناك خصوصية رئيسة لهذا الشكل الجديد من الحروب متمثلة في أن الحرب السيبرانية تحدث في الفضاء السيبراني، وبالرغم من عدم تحقيقها في منطقة جغرافية محددة، ولكن يمكن أن تحدث عدم الاستقرار الجيوسياسي. ففي هذا النوع من الحرب تعد السيطرة على المعلومات

ذات أهمية كبرى. وعليه فتميل الدول المتقدمة تكنولوجيا إلى السيطرة على الفضاء السيبراني. لذلك مع تزايد نقاط ضعف الدول أمام الحرب السيبرانية فإن التدابير ضرورية لصد مختلف الهجمات[1].

في العصر الحديث، حيث تتسارع التطورات التقنية وتزداد الاعتمادية على الفضاء السيبراني، أصبحت "الحرب السيبرانية" أحد أبرز وأهم أدوات الصراع بين الدول. حيث لم تعد الحروب تقتصر على المواجهات العسكرية التقليدية، بل دخلت المعلومات في قلب الصراعات العالمية، لتصبح سلاحاً ذا تأثير بالغ في الاستراتيجيات السياسية والأمنية. وتحولت المعلومات إلى قوة حقيقية يمكن استعمالها لتحقيق مكاسب استراتيجية أو لزعزعة استقرار الدول.

على الصعيد ذاته، أصبحت "سرقة المعلومات والبيانات العسكرية" أو التلاعب بها من أخطر الأساليب المستعملة في الحروب الحديثة. في هذا السياق، لم يعد الحديث عن الحرب التقليدية أو عن الصراع في ميادين القتال فقط، بل أصبح من الممكن أن تؤدي عملية اختراق واحدة إلى تسريب معلومات حيوية قد تؤثر بشكل مباشر في خطط الدفاع أو التوازن العسكري بين الدول. ويمكن للمتسللين في هذه الحالة التلاعب بالمعلومات بشكل يزيد من قوة طرف على حساب الآخر، أو حتى تغيير مجريات الصراع عن طريق ضرب نقاط ضعف غير مرئية **(الفقرة الأولى)**.

وفي هذا الإطار، أصبحت "جمع المعلومات الاقتصادية الاستخباراتية" أحد الأبعاد الأساسية في الحروب الحديثة، لا سيما في الأوقات التي يتقاطع فيها الاقتصاد مع الأمن القومي. فالمعلومات الاقتصادية أصبحت جزءا لا يتجزأ من استراتيجيات الدول في سعيها إلى الحفاظ على قوتها ونفوذها العالمي. واستعمال الاستخبارات الاقتصادية يشمل التلاعب بالأسواق، أو الوصول إلى معلومات حساسة حول الموارد الطبيعية، والشركات الكبرى، أو حتى استراتيجيات التنسيق بين الدول. هذه البيانات تُعد بمنزلة ثروة حيوية يمكن أن تُسهم في بناء مواقف اقتصادية قوية أو إضعاف الدول المنافسة **(الفقرة الثانية)**.

الفقرة الأولى: سرقة المعلومات والبيانات العسكرية أو التلاعب بها في دول البحر الأبيض المتوسط

---

[1] حسن قوادرة ، منى كحلوش، "التداعيات الاقتصادية لحرب المعلومات السيبرانية"، مقال منشور بمجلة الناقد للدراسات السياسية، العدد 1، 2021/04/30، ص 210.

تُعد سرقة المعلومات والبيانات العسكرية أو التلاعب بها أحد أبرز صور الحروب السيبرانية التي تُهدد الأمن الإقليمي لدول البحر الأبيض المتوسط. وتتمثل خطورة هذا النمط من الهجمات في كونه لا يستهدف مجرد التجسس أو جمع المعلومات، بل يتجاوز ذلك إلى التلاعب بالبيانات أو تدميرها إلكترونياً، ما قد يؤدي إلى شلل الأنظمة الدفاعية والعسكرية، وإحداث حالة من الفوضى الاستراتيجية.

كما يكون توظيف قراصنة محترفين أو جيوش نظامية إلكترونية ووكلاء سيبرانيين للقيام بشن هجمات سيبرانية بغرض السيطرة على نظم القيادة والسيطرة عن بعد، الأمر الذي يؤدي إلى إخراج بعض منظومات الأسلحة عن سيطرة القيادة المركزية، وإعادة توجيهها نحو أطراف داخلية أو ضد دول صديقة، كما يمكن أيضا السيطرة على الطائرات من دون طيار أو الغواصات النووية في أعماق البحار، أو السيطرة على الأقمار الصناعية العسكرية في الفضاء الخارجي وإخراجها عن سيطرة الدولة التابعة لها هذه الأسلحة والمعدات، إذ تزداد خطورة مثل هذه الهجمات إثر التطور التكنولوجي واعتماد اللوجستيات ونظم القيادة والتحكم وتحديد الأهداف، وإصابتها على برامج الكمبيوتر وشبكات الاتصال[2].

كما تقوم الهجمات السيبرانية بتدمير أنظمة إلكترونية لمنشآت حيوية عسكرية، وتعطيل شبكات الدفاع العسكرية أو إتلافها عن بعد، والاختراق أو التعطيل أو التدمير لشبكات القطاع الخاص ذي الصلة بالقطاع العسكري، وكذا التدخل في سلامة البيانات العسكرية الداخلية لدول أخرى، والقيام بمحاولات الإرباك والتشويش على أجهزتها[3].

في هذا السياق، شهدت تركيا في العقد الأخير محاولات مستمرة لاختراق شبكاتها الدفاعية، وهو ما دفعها إلى إنشاء وحدة سيبرانية خاصة تحت مظلة القوات المسلحة. كما أن الهجوم الذي تعرضت له منشآت الجيش الإيطالي في عام 2021 أدى إلى فقدان مؤقت للسيطرة على بعض أنظمة

---

[2] **إيهاب خليفة**، "تنامي التهديدات السيبرانية للمؤسسات العسكرية"، مجلة اتجاهات الأحداث، ع. 22 جويلية/ أوت 2017، ص. 3.

[3] **أميرة عبد العظيم محمد عبد الجواد**، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة الإسلامية، العدد 35، الجزء 3، 2020، ص373- 374.

الاتصالات الداخلية، وهو ما أبرز ضعف التنسيق الإقليمي في مواجهة هذه النوعية من الهجمات[4].

كما أن الهجمات السيبرانية لا تستهدف الأنظمة العسكرية المباشرة فقط، بل تمتد إلى البنية التحتية الحيوية ذات الصلة بالأمن القومي، مثل شبكات الطاقة، والاتصالات، والنقل، وحتى المنشآت الصحية والمصرفية. وتظهر خطورة هذه الهجمات في قدرتها على شلّ حركة الدولة بالكامل دون إطلاق رصاصة واحدة، كما حدث في الهجوم السيبراني الذي ضرب شبكة الطاقة الكهربائية في أوكرانيا في 2015، والذي يُعد نموذجاً تسترشد به وحدات إلكترونية في منطقة المتوسط[5].

وتستعمل هذه الهجمات في أحيان كثيرة لتوجيه عمليات عسكرية خاطئة، أو لتسريب معلومات مضللة بهدف تشتيت القيادة العسكرية، أو حتى إرباك نظم الردع والدفاع المبكر .وقد وثقت حالات في دول مثل اليونان وتونس، حيث جرى تسريب بيانات عسكرية دقيقة على الإنترنت بعد اختراق خوادم رسمية، ما شكل خطراً كبيراً على أمن القوات المنتشرة في مناطق نزاع أو حدودية.

وقد أظهرت التجارب أن خطورة هذه الهجمات تزداد بسبب اعتماد الأنظمة الحديثة على برمجيات معقدة مرتبطة بشبكات الاتصال والذكاء الاصطناعي، مما يجعل التحكم الكامل في الأنظمة العسكرية مهدداً في أي لحظة عبر هجوم تقني منسق. إذ يمكن لقراصنة التحكم عن بُعد في طائرات بدون طيار أو تعطيل الأقمار الصناعية أو التلاعب بأنظمة الملاحة العسكرية، كما حدث في هجوم سيبراني استهدف شبكة الأقمار الصناعية KA-SAT التابعة لشركة Viasat ، والذي أثر حتى في عمليات عسكرية في أوروبا الشرقية[6].

بالنظر إلى تنامي التهديدات السيبرانية في منطقة البحر الأبيض المتوسط، بات من الضروري على دول الإقليم تعزيز التعاون الأمني السيبراني المشترك، عن طريق إرساء آليات فعالة لتبادل المعلومات الاستخباراتية ذات الصلة، وتوحيد المعايير والبروتوكولات التقنية، إلى جانب اعتماد برامج تدريب وتكوين متبادل بين الكفاءات الوطنية. فهذه التهديدات العابرة للحدود لا يمكن مواجهتها بواسطة استراتيجيات وطنية منفردة، نظراً إلى طبيعتها المعقدة وسرعة انتشارها.

---

(4) European Union Agency for Cybersecurity (ENISA). (2021). *ENISA Threat Landscape Report 2021*. Retrieved from: https://www.enisa.europa.eu date of access march 20, 2025, on the watch 16:55.

(5) NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). (2021). *Cyber Threats and Responses in Europe*. Retrieved from: https://ccdcoe.org date of access June 13, 2025, on the watch 10:30.

(6) Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

ومن هذا المنطلق، يتعين إدراك أن أي دولة بمفردها، مهما بلغت قدراتها، لن تكون قادرة على التصدي الفعال لهذه التحديات دون الانخراط في تنسيق إقليمي محكم؛ لذا يصبح من الضروري إرساء منظومة جماعية للأمن السيبراني تشمل تبادل المعطيات في الوقت الحقيقي، وتوحيد إجراءات التصدي للهجمات، وتطوير ردود فعل سريعة وفعالة. وتشير تقارير مراكز بحثية مرموقة، مثل مركز التميز للدفاع السيبراني التعاوني التابع لحلف شمال الأطلسي (NATO CCDCOE, 2021)، إلى أن التعاون الإقليمي بين دول المتوسط يُسهم في تقليص الثغرات الأمنية، ويزيد من القدرة على اكتشاف الهجمات في مراحلها المبكرة، مما يحد من تأثيراتها السلبية ويوفر استجابة أكثر نجاعة[7].

الفقرة الثانية: جمع معلومات اقتصادية استخباراتية

ويتحقق عن طريق اختراق قواعد البيانات المالية والمصرفية وقواعد بيانات الشركات والبنوك وجمع المعلومات التي قد تؤثر في الأمن الوطني للدول، وكذلك عن طريق التجسس على المسؤولين الماليين ووزراء المالية ورؤساء الشركات الكبرى.

على سبيل المثال، تعرضت بعض الموانئ الأوروبية في المتوسط لهجمات سيبرانية تسببت في تعطيل حركة الشحن وزعزعة استقرار التجارة الدولية. كذلك، أظهرت التقارير أن العديد من الأنظمة المالية في دول البحر الأبيض المتوسط كانت هدفاً لهجمات تهدف إلى سرقة البيانات المالية أو تعطيل عمليات التحويلات المصرفية. هذه الجرائم السيبرانية العابرة للحدود تُظهر الحاجة الملحة إلى التعاون الأمني المشترك بين دول المنطقة، حيث لا يمكن لدولة واحدة مواجهة هذه التهديدات بمفردها. التعاون الأمني السيبراني بين دول البحر الأبيض المتوسط يصبح ضرورة ليس للتصدي لهذه الهجمات فقط، بل أيضاً لتبادل المعلومات الاستخباراتية، والوقاية من التهديدات المستقبلية، وترسيخ قدرة الدول على الاستجابة السريعة والفعّالة في حال وقوع الهجمات.

ومن ثم فالحروب السيبرانية صراع يستخدم معاملات أو هجمات معادية غير قانونية على الحواسيب والشبكات في محاولة لتعطيل الاتصالات، وغيرها من البنى التحتية، كإلحاق الضرر الاقتصادي، والسياسي وكذا العسكري، حيث تشمل الأسلحة السيبرانية المستعملة من أجل

---

[7] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). (2021). *Cyber Threats and Responses in Europe*. Retrieved from: https://ccdcoe.org date of access Juillet 10, 2025, on the watch 11:15.

تحقيق الأهداف الجيوسياسية مجموعة كبيرة من الأدوات، مثل تلك المتعلقة بالمراقبة، أو التجسس، أو التضليل، أو الهجمات المدمرة[8].

وعلى هذا فيمكن عد تحدي الأمن السيبراني[9] أعلى تحديات الأمن الوطني في القرن الواحد والعشرين، مع الإشارة إلى أن المفهوم الحديث للأمن لا يقتصر على الجوانب العسكرية فقط، بل يواكب كل التهديدات والتحديات التي يمكن أن تشكل حجر عثرة أمام الاقتصاد الرقمي وتدفق المعرفة، فقد أسقطت تكنولوجيا المعلومات والاتصالات مفهوم الحدود الجغرافية بين الدول مما يضع السيادة الوطنية على المحك، لاسيما مع اختراق المواقع الحكومية الرسمية والتجسس المعلوماتي على الدول[10].

ومما سبق ذكره، يمكن القول إن المجال السيبراني قد دخل ضمن المحددات الجديدة للقوة وأبعادها من حيث طبيعتها وأنماط استعمالها، بل وأيضا طبيعة الفاعلين وهو ما كان له انعكاس على قدرات الدول وعلاقاتها الخارجية، وأضفى خصائص جديدة للقوة والتي تمتد لتشمل الوسائل والطاقات والإمكانات المادية وغير المادية كافة، المنظورة وغير المنظورة التي بحوزة الدول، ويستعملها صانع القرار في فعل مؤثر يحقق مصالح الدولة، بما سيؤثر به في سلوك الوحدات السياسية الأخرى، فالعلاقة بين الأمن السيبراني والأمن الوطني تزداد كلما زاد نقل المحتوى المعلوماتي والعسكري، والأمني، والسياسي، والاقتصادي، والاجتماعي، والفكري، والخدمي العلمي والبحثي إلى الفضاء السيبراني، لاسيما مع تسارع الدول في تبني الحكومات الإلكترونية والمدن الذكية في العديد منها، واتساع نطاق وعدد مستخدمي الأنترنت في العالم، مما أدى إلى أن تكون قواعد البيانات الوطنية في حالة انكشاف خارجي، فضلاً عن حملات الدعاية والمعلومات المضللة ونشر الشائعات أو الدعوة لأعمال تحريضية أو دعم المعارضة أو الأقليات، مما يسهم في تلاشي سيادة الدولة ويشكك في قدرتها على الحفاظ على أمنها الوطني[11].

---

[8] **علاء الدين فرحات**، "الفضاء السيبراني: تشكيل ساحة المعركة في القرن الحادي والعشرين" مجلة العلوم القانونية والسياسية، 2019، ص 98.

[9] **مصطفى إبراهيم سلمان الشمري**، الأمن السيبراني وأثره في الأمن الوطني العراقي، مجلة العلوم القانونية والسياسية، العدد الأول، المجلد العاشر، 2021، ص: 158 – 159.

[10] **أميرة عبد العظيم محمد عبد الجواد**، مرجع سابق، ص: 374-375.

[11] **أميرة عبد العظيم محمد عبد الجواد**، مرجع سابق، ص ص. 434 – 435.

ومما سبق ذكره، يمكن القول إن المجال السيبراني قد أصبح أحد المحددات الجديدة للقوة والنفوذ في العلاقات الدولية، لاسيما في منطقة البحر الأبيض المتوسط التي تشهد تداخلاً كثيفاً في المصالح والنزاعات الجيوسياسية. هذا الفضاء، غير الخاضع لحدود جغرافية، أفرز نمطاً جديداً من الصراعات بين دول المتوسط، يعرف بالحروب السيبرانية، حيث يكون استهداف البنى التحتية الحيوية وقواعد البيانات السيادية، ونشر الشائعات والدعاية الموجهة، والتدخل في الشؤون الداخلية عبر الأدوات الرقمية. ومع ازدياد رقمنة المحتوى العسكري والأمني والسياسي، تصبح السيادة الوطنية مهددة بالاختراق، والتآكل في حال غياب أنظمة دفاع إلكترونية قوية.

وقد شهدت المنطقة في السنوات الأخيرة مؤشرات واضحة على هذا النوع من الصراع، عن طريق محاولات اختراق منصات حكومية في دول مثل اليونان، وقبرص، والمغرب، والجزائر، وإيطاليا، واتهامات متبادلة بين أطراف إقليمية بتدبير أو تمويل عمليات تجسس سيبراني وهجمات سيبرانية. وهو ما يجعل التعاون الأمني السيبراني بين دول المتوسط أمراً حتمياً لا خياراً، سواء عن طريق تبادل المعلومات الاستخباراتية حول الهجمات، أو تنسيق الردود، أو حتى وضع قواعد إقليمية لضبط هذا النوع من الحروب، التي إن تُركت دون تنظيم، قد تؤدي إلى توترات سياسية حادة أو صراعات مفتوحة يصعب احتواؤها.

المطلب الثاني: تصاعد الجرائم السيبرانية بين الدول المتوسطية: دافع نحو التعاون الأمني السيبراني

تواجه دول البحر الأبيض المتوسط في السنوات الأخيرة تصاعداً ملحوظاً في الجرائم السيبرانية، حيث أصبحت هذه الدول عرضة لهجمات تستهدف قطاعاتها الحيوية مثل الموانئ، والبنوك، وشبكات الطاقة، والاتصالات. هذا التصاعد يعود جزئياً إلى النمو السريع في الاعتماد على الأنظمة الرقمية في جميع المجالات، مما يزيد من فرص تعرض هذه الأنظمة للهجمات الإلكترونية. وتأتي الجرائم السيبرانية في أشكال متعددة، مثل الاختراقات الأمنية، والبرمجيات الخبيثة، والتصيد الاحتيالي، والهجمات باستعمال برامج الفدية، التي تُعطل الأعمال وتضر بالاقتصاد الوطني.

في هذا الإطار، أشارت التقارير الحديثة إلى تصاعد ملحوظ في الجرائم السيبرانية في منطقة البحر الأبيض المتوسط في السنوات الخمس الأخيرة (2020–2025)، لاسيما في دول ذات مواقع جيوسياسية حساسة مثل تركيا، اليونان، والمغرب. وعلى وفق تقرير صادر عن شركة "جروب-آي

بي"، تمثل تركيا 9.9% من إجمالي الهجمات السيبرانية في المنطقة، في حين يُستهدف المغرب بشكل متزايد، وبخاصة في مجالات الاحتيال الوظيفي، حيث يُستدرج الباحثون عن عمل بعروض توظيف وهمية عبر الإنترنت[12].

يُعزى هذا التصاعد إلى عوامل عديدة، أبرزها تسارع التحول الرقمي في المنطقة، مما يزيد من تعرض البنية التحتية الرقمية للهجمات. علاوة على ذلك، يُلاحظ أن الجماعات الإجرامية والإرهابية تستغل الفضاء السيبراني كوسيلة فعالة لتحقيق أهدافها، مثل استقطاب الشباب عبر المنصات الرقمية أو تمويل أنشطتها باستعمال العملات المشفرة[13].

كما جاء أيضا في بعض التقارير إلى تصاعد كبير لهذه الظاهرة الإجرامية على مستوى العالم، حيث أصبحت تُعد من أخطر وأعلى التهديدات تكلفة في العصر الرقمي. وبحسب تقرير رسمي للجرائم السيبرانية لعام 2022، فإن حجم التهديد السيبراني قد تضاعف بشكل كبير في السنوات القليلة الماضية، مما يعكس تزايد تعقيد هذه الجرائم وانتشارها عبر الحدود.

حيث تشير الإحصائيات إلى أن تكلفة مكافحة الجريمة السيبرانية تصل إلى ما يقارب 8 تريليونات دولار سنوياً، أي ما يعادل 667 مليار دولار شهرياً، و154 مليار دولار أسبوعياً، و21.9 مليار دولار يومياً، وحوالي 913 مليون دولار في الساعة، و15.2 مليون دولار في الدقيقة، و255 ألف دولار في الثانية[14]. في هذا السياق، يصبح التعاون الأمني السيبراني بين الدول ضرورة ملحة لمواجهة هذه التحديات المشتركة.

في المحصلة، فإن تصاعد الجرائم السيبرانية في البحر الأبيض المتوسط يشكل تحدياً مشتركاً أمام دول المنطقة، لا سيما في ظل تنامي التهديدات المرتبطة بالإرهاب السيبراني **(الفقرة الأولى)**، والجريمة المنظمة العابرة للحدود **(الفقرة الثانية)**. وبناء على ما سبق تعد هذه الأفعال الإجرامية

---

[12] **ياسين التازي**، " تقرير يكشف عن تزايد الاحتيال الرقمي والهجمات السيبرانية في المغرب"، مقال منشور بموقع بلبيريس، بتاريخ 19 ديسمبر 2024، على الساعة 00:23، متاح على الرابط التالي، https://www.belpresse.com، تاريخ الاطلاع 10 ماي 2025، على الساعة 14:45.

[13] **عادل عبد الصادق**، "التعاون الرقمي في المتوسط بين الفرص والتحديات وافاق المستقبل"، مقال منشور بالموقع الرسمي للمركز العربي لأبحاث الفضاء الالكتروني، بتاريخ 19 أكتوبر 2024، على الساعة 09:06. متاح على الرابط التالي: https://accronline.com، تاريخ الاطلاع 10 ماي 2025، على الساعة 15.34.

[14] **خالد محمود**، " عن الجرائم الالكترونية ظاهرة عالمية"، مقال منشور بموقع العربي الجديد، تاريخ 5 أكتوبر 2023، بدون ذكر الساعة، متاح على الرابط التالي: https://www.alaraby.co.uk، تاريخ الاطلاع 10 ماي 2025، على الساعة 16: 00.

من أهم الدوافع الموضوعية التي دفعت بدول البحر الأبيض المتوسط إلى الاعتماد على التعاون الأمني السيبراني كآلية لتحقيق الأمن السيبراني.

الفقرة الأولى: جرائم الإرهاب السيبراني كدافع للتعاون الأمني السيبراني

يعرف الإرهاب السيبراني **Cyberterrorism** بأنه أحد المفاهيم الحديثة في ميدان الأمن السيبراني، وهو ما دفع بالمهتمين بهذا المجال لمحاولة وضع تعريف لمصطلح ما زال غير محدد في شكله التقليدي، ومن التعريفات القابلة للتوافق، نذكر ما جاء به جيمس لويس James Leuiss، خبير في مركز الدراسات الاستراتيجية والدولية بالولايات المتحدة الأمريكية الذي يعرفه بأنه **"استخدام أدوات شبكات الحاسوب في تدمير أو تعطيل البنى التحتية الوطنية المهمة مثل الطاقة والنقل، أو بهدف ترهيب الحكومة والمدنيين"**[15]. كما عرفت وكالة المخابرات المركزية الأمريكية جريمة الإرهاب السيبراني بأنه **" أي هجوم تحضيري ذي دوافع سياسية موجهة ضد نظم معلومات الكمبيوتر، والبيانات والمعلومات التي تنتج من عنف ضد الأهداف المدنية عن طريق جماعات دون قومية أو عملاء سريين"**[16].

وفي الصدد نفسه يرى بعض الباحثين أن جريمة الإرهاب السيبراني هي **" تلك الجريمة التي تقوم بالأساس على استعمال الموارد المعلوماتية، المتمثلة في شبكات المعلومات وأجهزة الكمبيوتر وشبكة الانترنت، فبدون هذه المواد لا يمكن للمجرم الإرهابي السيبراني أن يحقق غايته، كما لا يمكننا الحديث عن جريمة إرهابية سيبرانية، إلا إذا كانت تتجه هذه الغاية إلى شن هجمات ضد نظم معلوماتية أو الاعتماد على الشبكات والمعلومات وتخزينها من أجل استغلال وتخويف أو إكراه حكومة معينة أو فئة محددة، كما ينبغي أن يهدف هذا الهجوم للمس بالنظام العام"**[17].

ولقد عرفت السنوات الأخيرة، منطقة البحر الأبيض المتوسط تصاعداً ملحوظاً في الهجمات الإرهابية السيبرانية، حيث استهدفت جماعات متطرفة دولاً عديدة في المنطقة، مما أبرز الحاجة

---

[15] **Alix Desforges :** « cyber terrorisme : quel périmètre ? », fiche de l'Irsem n° 11, 2011, p. 03.

[16] **عادل صادق:** "استخدام الإرهاب الالكتروني في الصراع الدولي"، دار الحديث، القاهرة، 2015، ص 104.

[17] **صفية لكطيطي**، "الامن السيبراني دراسة مقارنة"، مطبعة دار السلام للنشر، الطبعة الأولى 2025، ص: 61-62.

الملحة إلى تعزيز التعاون الأمني السيبراني بين هذه الدول. فيما يلي أبرز الوقائع المتعلقة بهذه الهجمات:

في هذا الصدد، ألقت الشرطة الإسبانية القبض على ثلاثة قراصنة إلكترونيين يُشتبه في ولائهم لروسيا، بتهمة تنفيذ هجمات إلكترونية استهدفت إسبانيا وعدداً من الدول الأعضاء في حلف شمال الأطلسي (الناتو). وقد مست هذه الهجمات مؤسسات حكومية وبنى تحتية حيوية، من بينها مواقع إلكترونية تابعة لوزارات وهيئات عامة، وذلك باستعمال تقنيات من بينها هجمات حجب الخدمة الموزعة (DDoS)[18].

كما شنّت مجموعة قراصنة موالية لروسيا تُدعى "NoName057(16)" هجوماً إلكترونياً على قرابة عشرة مواقع رسمية في إيطاليا، بما في ذلك مواقع وزارة الخارجية ومطارات ميلانو. تمكنت الوكالة الوطنية للأمن السيبراني الإيطالية من الحد من تأثير الهجوم في ساعتين، دون التأثير في حركة الطيران. أما في يناير 2025، استهدفت المجموعة نفسها مواقع إلكترونية لبنوك وشركات إيطالية، بما في ذلك "إنتيسا سان باولو" و"مونتي دي باشي"، علاوة على موانئ تارانتو وتريستي، مما أدى إلى تعطيل مؤقت لبعض الخدمات[19].

بينما تعرضت ألبانيا لهجوم إلكتروني واسع النطاق من مجموعة تُدعى"HomeLand Justice" ، يُعتقد أنها مرتبطة بإيران. أدى الهجوم إلى تعطيل مواقع وخدمات حكومية، مما دفع ألبانيا إلى قطع علاقاتها الدبلوماسية مع إيران في سبتمبر من العام نفسه[20]. وفي أبريل 2015، تعرضت قناة "TV5Monde"الفرنسية لهجوم إلكتروني من مجموعة تُدعى"CyberCaliphate" ، المرتبطة بتنظيم الدولة الإسلامية .أدى الهجوم إلى تعطيل البث التلفزيوني لمدة تجاوزت ثلاث ساعات، واختراق حسابات وسائل التواصل الاجتماعي للقناة، ونشر رسائل مناهضة للسياسات الفرنسية في الشرق الأوسط[21].

---

[18] https://www.reuters.com/technology/cybersecurity/three-pro-russian-hackers-arrested-spain-over-cyberattacks-

[19] New cyber attacks target Italian banks, companies, https://www.ansa.it date of access April 12, 2025, on the watch 16:00.

[20] **أنظمة الخدمات الحكومية في ألبانيا تتعرض لهجوم إلكتروني جديد وتير انا تتهم إيران بالوقوف وراءه**، مقال منشور بموقع فرانس 24، بتاريخ 10/09/2022، على الساعة 21:34، متاح على الرابط التالي: https://www.france24.com/ar تاريخ الاطلاع 17/03/2025، على الساعة، 00:56.

[21] **Don Melvin and Greg Botelho**, Cyberattack disables 11 French TV channels, takes over social media sites, Updated 3:56 PM EDT, Thu April 9, 2015. https://edition.cnn.com. date of access June 28, 2025, on the watch 10.00.

وفي هذا الصدد، تعتمد الجماعات الإرهابية على تقنيات رقمية لغسل الأموال وتمويل أنشطتها. تشمل هذه التقنيات استعمال العملات الرقمية، وتحويل الأموال عبر الإنترنت، وإنشاء شبكات مالية غير رسمية. في عام 2018، كشفت تقارير عن استعمال تنظيم داعش لعملات رقمية مثل "بيتكوين" في تمويل عملياته، مما صعّب من تتبع الأموال وتحويلها عبر الحدود.[22]

وعليه تُظهر هذه الوقائع أهمية تعزيز التعاون الأمني السيبراني بين دول البحر الأبيض المتوسط، لمواجهة الجرائم الإرهابية السيبرانية التي تستهدف البنية التحتية الحيوية والمؤسسات الحكومية والأفراد. كما يُعد تبادل المعلومات والتنسيق بين الدول أمراً حيوياً للحد من تأثير هذه الظاهرة الإجرامية وضمان استقرار المنطقة.

الفقرة الثانية: الجريمة السيبرانية المنظمة كدافع حتمي للتعاون الأمني السيبراني في دول المتوسطية

تُعد الجريمة السيبرانية المنظمة من أخطر التهديدات التي تواجه المجتمعات الرقمية الحديثة، لاسيما في المناطق ذات الاتصال المتزايد بالعالم الرقمي، مثل منطقة البحر الأبيض المتوسط. يُقصد بها تلك الأنشطة الإجرامية التي تُمارَس بواسطة الفضاء السيبراني، وتكون منظمة بشكل هيكلي، يُشبه العصابات التقليدية، ولكن بأدوات رقمية وتقنيات معقدة. وغالباً ما تتسم هذه الجرائم بالطابع العابر للحدود، حيث يكون تنفيذها من دولة، وتستهدف أفراداً أو مؤسسات في دولة أخرى، مما يجعل ملاحقتها قضائياً وتقنياً أكثر تعقيداً.

تمثل هذه الأنشطة جزءاً من ما يسمى بـ"الإجرام المنظم السيبراني"، إذ تعمل مجموعات إجرامية محترفة على تنفيذ خطط ممنهجة لاختراق الأنظمة وجني الأرباح، سواء عن طريق الابتزاز أم الاحتيال أم سرقة البيانات. وتعتمد هذه العصابات غالباً على الشبكة المظلمة(Dark Web) ، وخوادم مشفّرة، والعملات الرقمية، ما يزيد من صعوبة تتبعها أو الإيقاع بها .**أبرز أنواع الجرائم السيبرانية المنظمة ما يلي:**

أولا: الابتزاز السيبراني

---

[22] ISIS and other terrorist groups increase the use of Bitcoin after the losses on the battlefield, https://www.gfatf.org date of access June 13, 2025, on the watch 9:25.

يُعد الابتزاز السيبراني من أكثر الجرائم السيبرانية المنظمة انتشاراً في منطقة البحر الأبيض المتوسط. تقوم هذه الجرائم على اختراق بيانات حساسة تخص أفراداً أو مؤسسات، مثل الصور الشخصية، والمعلومات المالية، أو المراسلات الخاصة، ثم يكون تهديد الضحية بنشرها ما لم يدفع مبلغاً مالياً معيناً .وغالباً ما يكون الدفع بعملة رقمية مثل "البيتكوين"، نظراً إلى صعوبة تتبعها.

وبحسب تقرير يوروبول لعام 2024، فإن الهجمات السيبرانية التي تستهدف الأفراد والشركات الصغيرة والمتوسطة قد ازدادت بشكل ملحوظ، مما يجعلها أكثر عرضة للابتزاز السيبراني. تستغل هذه الهجمات تقنيات مثل الهندسة الاجتماعية والتصيد الاحتيالي للوصول إلى البيانات الحساسة. كما أن استعمال أدوات الذكاء الاصطناعي مثل "deepfakes" قد سهل من تنفيذ هذه الجرائم، مما يزيد من تعقيد مكافحتها[23].

وفي هذا الصدد، تمكنت السلطات الإيطالية من تفكيك شبكة متخصصة في الابتزاز الإلكتروني، كانت تستهدف موظفين داخل شركات باستعمال وسائل تقنية متقدمة. وقد تمثلت الخطة الإجرامية في إرسال رسائل بريد إلكتروني تحتوي على برمجيات خبيثة(malware) ، يكون بواسطتها اختراق أجهزة الحاسوب الخاصة بالضحايا. بعد الدخول إلى هذه الأجهزة، يقوم الجناة بجمع ملفات شخصية وصور حساسة، ثم يشرعون في تهديد الضحايا بنشر هذه البيانات ما لم يدفع مبالغ مالية بعملة البيتكوين. وعلى وفق تحقيقات الشرطة، سجلت أكثر من 250 حالة موثقة لهذا النوع من الابتزاز، وكانت الغالبية العظمى من الضحايا تقيم في مدينتي روما وميلانو. هذا المثال يعكس مدى تطور الجرائم الإلكترونية العابرة للحدود، وصعوبة تتبع مرتكبيها نظراً إلى استعمالهم تقنيات تشفير متقدمة والعملات الرقمية غير القابلة للتتبع.

شهد المغرب في السنوات الأخيرة تصاعداً في جرائم الابتزاز الإلكتروني، لاسيما تلك المرتكبة ضد النساء على مواقع التواصل الاجتماعي. ففي مدينة فاس سنة 2023، ألقت السلطات الأمنية القبض على شاب تورط في ابتزاز عدد من الفتيات بعد أن تمكن من اختراق هواتفهن الذكية. استعمل الجاني برامج تجسس (spyware) مكنته من الوصول إلى الصور والمحتويات الخاصة، مستغلاً منصات مثل "إنستغرام" و"واتساب" للتواصل مع ضحاياه. وقد عمد إلى إخفاء هويته الرقمية باستعمال الشبكات الخاصة الافتراضية(VPN) ، وطالب ضحاياه بدفع مبالغ مالية

---

(23) Europol: Immer mehr Cybercrime und KI-Nutzung von dpa | 23.Jul 2024 | Europe in brief, sur le site : https://europeannewsroom, date entrée : 20/01/2025, à l'heure 22 :17.

تراوحت بين 3000 و8000 درهم مغربي مقابل عدم نشر الصور الخاصة بهن. تعكس هذه الواقعة تعقيدات التحقيق في مثل هذه القضايا، لاسيما في ظل استعمال أدوات إخفاء الهوية الرقمية، وضرورة التوعية المجتمعية بمخاطر مشاركة البيانات الشخصية على الإنترنت.[24]

ثانياً: غسل الأموال عبر العملات المشفرة

تُمثل العملات الرقمية بيئة مثالية لغسل الأموال، نظراً إلى طبيعتها اللامركزية وصعوبة تعقب العمليات التي تكون عبرها .تقوم الشبكات الإجرامية بتحويل أموال غير مشروعة إلى عملات رقمية، ثم إعادة توزيعها أو استثمارها في أنشطة تبدو قانونية .في ظل غياب نظام رقابي إقليمي موحد، باتت دول المتوسط عرضة لاستعمال أنظمتها المالية كبوابات لتمرير هذه العمليات.

في تقرير صادر عن وكالة الشرطة الأوروبية (يوروبول) لعام 2024، كان تسليط الضوء على تزايد اعتماد الشبكات الإجرامية على العملات المشفّرة في عمليات غسل الأموال، لا سيما عن طريق منصات مثل"ChipMixer" ، التي صادرت السلطات أصولاً مرتبطة بها تقدّر بـ44.2 مليون يورو. وأشار التقرير إلى أن هذه الشبكات تستغل الثغرات في التشريعات الوطنية والتباينات القانونية بين الدول الأوروبية لتسهيل عملياتها غير المشروعة[25].

كما أعلنت الشرطة الإسبانية في عام 2022 عن تفكيك شبكة دولية لغسل الأموال، قامت بتحويل ملايين اليوروهات الناتجة عن الاتجار بالمخدرات إلى عملات رقمية، قبل إعادة ضخّها في استثمارات بمجال العقارات والفنادق. استعملت هذه الشبكة محافظ رقمية وهمية وتقنيات تمويه الهوية عبر خدمات "Mixers"، التي تدمج المعاملات لجعل تتبّعها أمراً بالغ الصعوبة[26].

وفي السياق نفسه، شهدت تركيا واحدة من أبرز قضايا الاحتيال المرتبطة بالعملات المشفّرة، تمثّلت في فضيحة منصة ."Thodex" ففي أبريل 2021، أوقفت المنصة نشاطها بشكل مفاجئ، فيما اختفى مؤسسها، فاروق فاتيح أوزر، حاملاً معه نحو ملياري دولار من أموال المستثمرين. كانت "Thodex" تضم ما يقارب 391,000 مستخدم نشط، وكانت تُجري تداولات يومية بمبالغ كبيرة. عقب فراره، تبيّن أن أوزر لجأ إلى ألبانيا، حيث ألقي القبض عليه في أغسطس 2022، وسلم لاحقاً إلى السلطات

---

[24] Casablanca: Police arrest cyber extortion suspect threatening of public order, November 28, 2023, sur le site https://en.hespress.com, date entrée: 01/03/2025, à l'heure 15 :30.

[25] Europol. (2024). *Crypto assets a growing money laundering risk, says Europol*. Investment International

[26] CriptoNoticias. (2022). *Policía de España desmantela red de narcotráfico que lavaba dinero con criptomonedas*.

التركية. وفي سبتمبر 2023، أصدرت محكمة تركية حكماً عليه بالسجن لمدة 11,196 سنة، بعد إدانته بتهم تتضمن الاحتيال، وغسل الأموال، وتأسيس وإدارة منظمة إجرامية[27].

ثالثا: الاحتيال الإلكتروني كتهديد متصاعد في منطقة جنوب وشرق المتوسط

يأخذ الاحتيال الإلكتروني أشكالاً متعددة، منها الاحتيال عبر البريد الإلكتروني، وإنشاء مواقع إلكترونية زائفة، والتصيد الاحتيالي .(phishing) غالباً ما تستهدف هذه العمليات الشركات الصغيرة أو المستخدمين الأفراد، مما يؤدي إلى خسائر مالية جسيمة.

لقد أشار تقرير يوروبول (Europol) المعنون بـInternet Organise" Crime Threat Assessment "2024 (IOCTA) إلى أن الاحتيال الإلكتروني يُعد من أبرز أشكال الجرائم السيبرانية التي تعرف تزايداً ملحوظاً في دول جنوب وشرق البحر الأبيض المتوسط .ويُعزى هذا التزايد إلى عوامل عديدة، من أبرزها ضعف الوعي الرقمي لدى بعض الفئات المجتمعية، وقصور الأنظمة الأمنية الإلكترونية المعتمدة من قبل الأفراد والمؤسسات، ما يفتح المجال أمام مجرمي الإنترنت لاستغلال هذه الثغرات وتحقيق مكاسب غير مشروعة[28].

وتشكل الثغرات الأمنية وضعف التوعية مدخلاً رئيساً للهجمات الإلكترونية، حيث برز التقرير المشار إليه أعلاه أن الفئات المستهدفة غالباً ما تفتقر إلى الوعي الكافي بأساليب الاحتيال الإلكتروني، لاسيما في ظل الانتشار المتزايد للخدمات الرقمية والبنكية على الإنترنت. ومع غياب برامج التوعية الأمنية، تصبح هذه الفئات هدفاً سهلاً لهجمات التصيّد الإلكتروني(Phishing) ، وهجمات الاحتيال المالي عبر المنصات الرقمية، حيث يُخدع الضحايا عبر رسائل أو مواقع إلكترونية مزيفة تطلب منهم تقديم معلومات شخصية أو مالية حساسة.

وفي هذا الصدد، شهدت تونس سنة 2023 واحدة من أبرز حملات التصيّد الإلكتروني التي استهدفت مستخدمي البنوك الرقمية، حيث أصدرت الوكالة الوطنية للسلامة المعلوماتية بلاغاً يُحذر من مواقع إلكترونية مزيفة صممت لتُطابق تصميم البنوك المعروفة محلياً. وطُلب من الضحايا، عبر رسائل بريد إلكتروني احتيالية، "تحديث بياناتهم البنكية"، مما أدى إلى اختراق

---

(27) Home Incidents Attack Vectors Market Health Synthetic Data, An article published on the following website: https://dn.institute/research/cyberattacks/incidents/ , Date of access: 23/11/2024, On the hour 23:57.

(28) Europol. (2024). *Internet Organised Crime Threat Assessment (IOCTA) 2024*. European Union Agency for Law Enforcement Cooperation. Retrieved from: https://www.europol.europa.eu date of access April 17, 2025, on the watch 15:00.

حساباتهم المالية وسرقة الأموال. وقد سجلت أكثر من 400 حالة احتيال في مدة لا تتجاوز الشهر، ما يعكس حجم التحديات الأمنية التي تواجهها البنية التحتية الرقمية في البلاد[29].

وفي مثال آخر يوضح امتداد الجريمة السيبرانية إلى بعد دولي، تمكنت السلطات الفرنسية في مدينة ليون سنة 2024 من تفكيك شبكة احتيال دولية كانت تدير عملياتها من رومانيا، والجزائر. تخصصت هذه الشبكة في الاحتيال عبر مواقع بيع السيارات المستعملة، حيث عرضت سيارات وهمية بأسعار منخفضة لجذب الضحايا، ثم طالبتهم بتحويل دفعات مالية مقدّمة عبر خدمات مثل PayPal. وبعد استلام الأموال، كان أفراد الشبكة يختفون دون أي أثر. هذا المثال يوضح مدى التنظيم العالي لهذه العصابات، واستغلالها للبنية الرقمية عبر الحدود في تنفيذ عملياتها الاحتيالية[30].

وفي هذا الصدد نجد الحكم الصادر عن المحكمة الابتدائية بالرباط، وذلك بخصوص شكاية تقدمت بها وزارة الطاقة والمعادن والبيئة إلى وكيل الملك مفادها أن النظام الالكتروني الخاص بها تعرض لاختراق معلوماتي، وبعد الأبحاث التمهيدية توصلت الشرطة القضائية إلى أن المدير العام لشركة «ميكائيل» واثنين من المستخدمين قاموا باختراق الأنظمة المعلوماتية للوزارة وتثبيت البرامج المعلوماتية TEAMVIWE وERSE التي تسمح بالتحكم عن بعد، وتتيح إمكانية مسح، وحذف الملفات، والبيانات من النظام المعلوماتي[31].

وبناء على ما سبق، يؤكد تقرير يوروبول على ضرورة تطوير التعاون بين الدول المعنية، لاسيما في المناطق التي تشهد نشاطاً متزايداً للجريمة الإلكترونية. ويوصي التقرير بإنشاء آليات تنسيق بين الجهات الأمنية، وتبادل المعلومات في الوقت الفعلي، فضلاً عن إطلاق برامج توعية رقمية موجهة للفئات الأكثر عرضة للاستهداف .كما شدد التقرير على أهمية الاستثمار في تحديث البنية التحتية للأمن السيبراني داخل المؤسسات العامة والخاصة، بما يتماشى مع تطور أساليب الجريمة الرقمية.

رابعا: هجمات برامج الفدية تهديد متصاعد للبنى التحتية الحيوية

---

[29] Europol. (2024). *Internet Organised Crime Threat Assessment (IOCTA) 2024*? OP. CIT.

[30] Eurojust, "Annual Report 2023: Cybercrime," 2023.

[31] قرار رقم 34.00 صادر عن غرفة الجنح الاستئنافية بالمحكمة الابتدائية بالرباط في ملف عدد 14/2010/2751، غير منشور.

تُعد هجمات برامج الفدية من أخطر أشكال الجرائم السيبرانية المعاصرة، إذ تقوم فيها جهات إجرامية بزراعة برمجيات خبيثة في أنظمة الضحية تؤدي إلى تشفير جميع البيانات المخزنة، ثم تطالب بفدية مالية - غالباً بالعملات المشفّرة مثل البيتكوين- مقابل تزويد الضحية بمفتاح فك التشفير الذي يمكنه من استعادة البيانات. وقد تطورت طبيعة هذه الهجمات في السنوات الأخيرة، حيث لم تعد تستهدف الأفراد أو الشركات الصغيرة فقط، بل أصبحت تركز على البنى التحتية الحيوية مثل المستشفيات، والمطارات، والمؤسسات الحكومية، مما يجعلها تهديداً مباشراً للأمن الوطني للدول. وقد رُصدت هذه الأنشطة في دول أوروبية وشرق متوسطية مثل إسبانيا، وفرنسا، واليونان، ما يعكس البعد الدولي لهذا التهديد.

وعلى وفق تقرير Eurojust لعام 2023، فقد شهدت هجمات برامج الفدية زيادة ملحوظة من حيث العدد والتأثير، حيث استهدفت مجموعات إجرامية منظمة، مثل مجموعة"Ragnar Locker" ، أكثر من 168 شركة ومؤسسة دولية منذ عام 2020. وقد أدت هذه الهجمات إلى خسائر مالية جسيمة واضطراب في أنظمة العمل، مما يجعل مكافحتها تمثل تحدياً كبيراً للسلطات القضائية والأمنية على المستوى الأوروبي والدولي. ويشير التقرير أيضاً إلى أن هذه الجماعات تعمل غالباً ضمن شبكات معقدة وعابرة للحدود، وتستعمل الإنترنت المظلم لتنسيق أنشطتها وتلقي المدفوعات[32].

وفي هذا السياق، استُهدفت وزارة الصحة في اليونان بهجوم ببرنامج الفدية المعروف بـ .LockBit تسبب الهجوم في شلل شبه كامل للنظام الصحي الرقمي، مما أثر في المستشفيات ومواعيد المرضى الإلكترونية لعدة أيام. المهاجمون طالبوا بدفع فدية قدرها ثلاثة ملايين يورو بالبيتكوين مقابل فك التشفير، واستعادة البيانات، الحكومة اليونانية رفضت الاستجابة لهذا الابتزاز، واعتمدت على فرق الاستجابة الوطنية للأمن السيبراني لاستعادة النظام بشكل تدريجي. تعكس هذه الحادثة خطورة التهديدات السيبرانية حينما تستهدف قطاعاً حيوياً مثل الصحة العامة[33].

كما تعرضت أحد البنوك المصرية الخاصة الكبرى في عام 2022 لهجوم عبر برمجية Conti .Ransomware أظهر التحقيق أن الجهة المهاجمة كانت جزءاً من شبكة إجرامية تعمل من شرق أوروبا، وقد استعانت بوسطاء في شمال إفريقيا لترتيب عملية دفع الفدية، وذلك عن طريق

---

[32] Eurojust. (2023). *Annual Report 2023*. European Union Agency for Criminal Justice Cooperation. Retrieved from: https://www.eurojust.europa.eu date of access June 16, 2025, on the watch 16:00.

[33] نفس المرجع السابق.

التواصل عبر الإنترنت المظلم. لم تُعلن الجهات الرسمية تفاصيل الاستجابة أو حجم الخسائر، لكن هذه الواقعة أثارت تساؤلات حول جاهزية القطاع المصرفي في المنطقة لمواجهة هجمات من هذا النوع[34].

وعليه، تُظهر هذه الحالات أن برامج الفدية أصبحت أداة ابتزاز رقمي فعالة بيد جماعات الجريمة المنظمة، مستفيدة من تطور تقنيات التشفير ووسائل الاتصال غير القانونية. ونظراً إلى استهدافها لوزارات ومؤسسات مالية وصحية، فإن التهديد يتجاوز الأبعاد التقنية، ليصبح عاملاً مؤثراً في الاستقرار الاقتصادي والسياسي للدول. ويوصي تقرير Eurojust بضرورة تعزيز قدرات التحقيق الرقمي، وتطوير أنظمة الأمن السيبراني في القطاعات الحيوية، علاوة على تكثيف التعاون القضائي الدولي لمواجهة الشبكات العابرة للحدود.

خاتمة

في ضوء ما تقدم، يتّضح أن التحديات الأمنية السيبرانية في منطقة البحر الأبيض المتوسط لم تعد مجرد تهديدات تقنية عابرة، بل تحولت إلى معضلات استراتيجية تمسّ الأمن القومي للدول، واستقرار المجتمعات، وسلامة البنى التحتية الحيوية. هذه التهديدات، التي تتخذ أشكالاً متعددة من هجمات سيبرانية منظمة إلى جرائم إلكترونية عابرة للحدود، لا يمكن مواجهتها ضمن الأطر التقليدية للأمن، بل تتطلب تحولاً في التفكير الأمني الإقليمي، يعتمد على التكامل، والتعاون متعدد الأطراف، وبناء الثقة بين دول المنطقة.

كما أن التعاون السيبراني لم يعد خياراً، بل بات ضرورة وجودية تفرضها طبيعة التهديدات السيبرانية التي لا تعترف بالحدود الجغرافية، ولا تميز بين دولة متقدمة وأخرى نامية. ومن هذا المنطلق، فإن دول المتوسط مدعوة إلى تأسيس آليات تنسيق إقليمية فعالة تشمل تبادل المعلومات في الوقت الفعلي، والتدريب المشترك، وتوحيد السياسات والتشريعات السيبرانية، وبناء بنية تحتية رقمية آمنة ومترابطة. كما يُعد انخراط المنظمات الإقليمية والدولية، والقطاع الخاص، والمؤسسات الأكاديمية، عنصراً حاسماً في تطوير منظومة أمنية متكاملة ومواكِبة للتطور التكنولوجي.

---

[34] Eurojust, "Annual Report 2023: Cybercrime," 2023.

علاوة على ذلك، فإن تعزيز هذا التعاون من شأنه أن يسهم في تعزيز الاستقرار السياسي والاقتصادي للمنطقة، وخلق بيئة آمنة للاستثمار الرقمي، وتحقيق تنمية مستدامة قائمة على الاقتصاد الرقمي. وبذلك، يصبح الأمن السيبراني ليس خط دفاع ضد الهجمات فقط، بل رافعة استراتيجية لبناء مستقبل رقمي مشترك، أكثر أمناً وتقدماً لدول المتوسط جميعاً.