مركز الخليج للأبحاث
المعرفة للجميع

دراسة تحليلية في تحولات الأمن البحري والدبلوماسية السيبرانية البحرية

اللواء البحري الركن (م) / عبدالله بن جابر الزايدي

مستشار أول دراسات دفاعية وأمنية

مركز الخليج للأبحاث

الرياض – يناير ٢٠٢٦

المحتويات

أولا: المقدمة.

١,١ خلفية الدراسة.

- **تطور مفهوم الأمن البحري في العصر الرقمي.**

تُعد البحار ركناً بنيويا في هيكل الاقتصاد العالمي، إذ يمر عبرها ما يقارب ٨٠٪ [١] من حجم التجارة الدولية، ونحو ٦١٪[٢] من امدادات النفط العالمية. هذه الأهمية لم تعد البحار مقتصرة على دورها التقليدي كممرات ملاحية لنقل السلع والطاقة. بل تعاظمت مكانتها الاستراتيجية مع تسارع الرقمنة وتطور التقنيات والاعتماد على البُنى التحتية البحرية بوصفها مكونات حيوية لتشغيل الاقتصاد الرقمي العالمي. هذا التحول اعاد تعريف المجال البحري كفضاء استراتيجي معقد تتقاطع فيه الأبعاد المادية والرقمية والاقتصادية والسياسية.

ونتيجة لهذا التحول البنيوي تطور مفهوم الأمن البحري نوعياً، إذ انتقل من ارتباطه التاريخي بالقوة البحرية لحماية خطوط الملاحة ومواجهة التهديدات التقليدية إلى إطار أكثر شمولية وتعقيد يدمج بين التقنية والأمن والاقتصاد والقانون الدولي. ومع التوسع في الأنظمة الرقمية والذكاء الصناعي العسكري البحري أصبح التداخل والتشابك بين الأمن البحري والأمن السيبراني أمراً واقعاً لا يمكن فصله.

- **التحول من التهديدات التقليدية إلى التهديدات السيبرانية والهجينة.**

نظراً لتسارع التقنية والاعتماد على النظم الرقمية المعاصرة. فإن التحليل الأمني البحري لم يعد مرتبط فقط بأنماط التهديد التقليدية، فقد ظهر على السطح تهديدات هجينة وسيبرانية بحرية تتسم بخصائص مختلفة كليا من حيث طبيعتها وفاعليها وآليات تنفيذها وآثارها الاستراتيجية. هذه التهديدات الجديدة لها أهداف مختلفة لأنها تستهدف تدمير وتعطيل الوظائف التشغيلية واحداث تأثيرات استراتيجية قد تفوق في خطورتها نتائج المواجهات البحرية التقليدية. وتشكل التهديدات الهجينة والسيبرانية نمط جديد ومعقد يعمل في المنطقة الرمادية بين السلم والحرب. هذا النمط يجمع بين أدوات تقنية حديثة ووسائل غير عسكرية وأنشطة متعددة يصعب اسنادها قانونياً أو سياسياً. ويؤدي هذا النمط إلى إضعاف فعالية الاستجابة العسكرية المباشرة نظرا لعدة أسباب منها الغموض وتعدد الفاعلين واستغلال الفجوات التنظيمية والمؤسسية. وذلك يعطي مفهوم جديد بأن الأمن البحري لا يقاس فقط بمدى السيطرة على المجال البحري المادي، بل بقدرة الدولة على مواجهة وإدارة المخاطر السيبرانية وتعزيز مرونة البُنى التحتية البحرية ودمج أدوات الأمن والدبلوماسية في إطار متكامل قادر على مواجهة التهديدات الجديدة.

١,٢ إشكالية الدراسة.

- **قصور الأطر التقليدية في التعامل مع الأمن السيبراني البحري.**

على الرغم من التحولات البنيوية التي أعادت تشكيل المجال البحري في ظل تسارع تقني ورقمي.

لاتزال الأطر النظرية والتنظيمية السائدة في الأمن البحري عاجزة عن استيعاب الأبعاد السيبرانية والهجينة بوصفها مكون بنيوي جديد ورئيسي في منظومة الأمن البحري، وليست مجال تقني مستقل أو تهديد ثانوي غير مرتبط بالمجال البحري.

1. https://unctad.org/news/shipping-data-unctad-releases-new-seaborne-trade-statistics
2. https://www.irena.org/Decarbonising-hard-to-abate-sectors-with-renewables-Enablers-and-recommendations/Transport-sector/Shipping

ويتجلى هذا القصور في استمرار التركيز على حماية الأصول المادية والسيطرة البحرية المكانية فقط مقابل محدودية التحليلات التي تتعلق بالمخاطر السيبرانية والهجينة في المجال البحري. ويلاحظ اتساع الفجوة بين طبيعة التهديدات السيبرانية والهجينة وبين الأدوات المفاهيمية والمؤسسية المصممة للتعامل مع تلك التهديدات، ووجود هذه الفجوة يحد من فعالية الاستجابة الأمنية المباشرة ويحد من القدرة على إدارة المخاطر بشكل استباقي.

- **غياب التكامل بين الأمن البحري والدبلوماسية السيبرانية.**

قصور الأطر التقليدية المذكورة في الفقرة السابقة تتفاقم في ظل غياب التكامل المفاهيمي والمؤسسي بين الأمن البحري والدبلوماسية السيبرانية.

وذلك لأن الدبلوماسية البحرية محكومة بأطر قانونية وسيادية تقليدية تركيزها فقط على حرية الملاحة، وترسيم الحدود البحرية، وتسوية النزاعات البحرية دون استيعاب وفهم كامل لخصوصيات الفضاء السيبراني البحري وما يفرضه من إشكاليات تتعلق بإجراءات بناء الثقة وتنظيم السلوك في البيئات الرمادية.

إن هذا القصور يؤدي إلى اضعاف قدرة الدولة على توظيف مفهوم الدبلوماسية السيبرانية كأداة وقائية وتنظيمية لإدارة التهديدات السيبرانية والهجينة في المجال البحري. وعدم معالجته يؤدي الى ارتفاع مستويات التعقيد والغموض والتشابك.

١,٣ أهمية الدراسة.

- **الأهمية الأمنية.**

تبرز الأهمية الأمنية لهذه الدراسة من التحول النوعي في طبيعة التهديدات التي تستهدف المجال البحري، حيث لم يعد يختزل هذا المجال في البعد العسكري فقط بل أصبح بنية تشغيلية رقمية مترابطة تشكل هدفا مباشرا للتهديدات السيبرانية والهجينة. فاستهداف أنظمة الملاحة الرقمية والموانئ الذكية والبُنى التحتية البحرية الحرجة وسلاسل الامداد لا يقتصر أثره على تعطيل النشاط البحري، بل يمتد إلى منظومات الأمن الوطني والاستقرار السياسي والاقتصادي، وتكمن أهمية الدراسة في مساهمتها لمعالجة الفجوة القائمة حاليا بين هذه التهديدات المعاصرة والأطر الأمنية والعسكرية التقليدية، وذلك عبر تقديم مقاربة تحليلية تسهم في بناء فهم أكثر تكاملاً للأمن السيبراني ويدعم تطوير سياسات وقائية وآليات استجابة اكثر مرونة وفاعلية على إدارة المخاطر في بيئات تتسم بالغموض والتشابك والتعقيد.

- **الأهمية الاقتصادية (سلاسل الامداد والتجارة العالمية).**

تكتسب الدراسة أهمية اقتصادية متزايدة في ظل الاعتماد البنيوي للاقتصاد العالمي على سلاسل امداد بحرية رقمية عالية الترابط، تدار عبر أنظمة معلوماتية عابرة للحدود، فأي خلل سيبراني يستهدف الموانئ أو أنظمة الشحن المؤتمتة أو منصات إدارة التجارة البحرية سوف يحدث اضطرابات متسلسلة في تدفقات التجارة والطاقة، ويرفع من تكاليف التأمين والشحن ويقوض موثوقية الأسواق العالمية. ومن هذا المنطلق فإن هذه الدراسة تسهم في توضيح الارتباط البنيوي بين الامن البحري السيبراني واستقرار سلاسل الامداد العالمية، وتُبين أن حماية البُنى التحتية البحرية الرقمية لم تعد مسألة تقنية أو تشغيلية، بل أساسا للحد من الهشاشة الاقتصادية وتعزيز القدرة على الصمود في مواجهة المخاطر السيبرانية.

- **الأهمية الاستراتيجية والدبلوماسية.**

على المستوى الاستراتيجي والدبلوماسي، تبرز أهمية هذه الدراسة من معالجتها للتحديات الناتجة من غياب التكامل بين الأمن البحري والدبلوماسية السيبرانية في بيئة بحرية رقمية تتسم بتشابك المصالح، وتعدد الفاعلين، وصعوبة الاسناد القانوني والسياسي. وأظهرت هذه التحولات محدودية الاعتماد على الأدوات الأمنية التقليدية في التعامل مع التهديدات المعاصرة، وهذا استدعى توظيف الدبلوماسية بوصفها أداة تنظيمية واستباقية لإدارة المخاطر، وبناء الثقة، وصياغة قواعد سلوك تستخدم في الفضاء البحري الرقمي، كما تسهم

في تطوير آليات وأدوار الدبلوماسية السيبرانية البحرية في ضبط التنافس وتقليص احتماليات التصعيد غير المقصود وتعزيز الاستقرار الرقمي في المجال البحري.

١,٤ أهداف الدراسة.

تهدف هذه الدراسة إلى تحليل التحول البنيوي في الأمن البحري في ظل تصاعد التهديدات السيبرانية والهجينة، عبر تقييم قصور الأطر المفاهيمية والتنظيمية التقليدية في استيعاب البعد السيبراني البحري. كما تسعى إلى توضيح الفجوات المطلوبة لتحقيق التكامل بين الأمن البحري والدبلوماسية السيبرانية البحرية ودور تلك الدبلوماسية كأداة وقائية وتنظيمية لإدارة المخاطر المعاصرة، وتعزيز الحوكمة، والحد من الهشاشة الأمنية والاقتصادية المرتبطة بسلاسل الامداد البحرية الرقمية والبُنى التحتية البحرية الرقمية.

١,٥ منهجية الدراسة.

تتبنى هذه الدراسة منهجية تحليلية تعتمد على الدمج بين التحليل المفاهيمي والتحليل المؤسسي وذلك بوصفهما مدخلين متكاملين لفهم واستيعاب التحولات البنيوية (**Structural Transformation**) التي يشهدها الأمن البحري في ظل تصاعد التهديدات السيبرانية والهجينة. وتستند الدراسة إلى مراجعة مستفيضة للأدبيات الأكاديمية المتخصصة في الأمن البحري والأمن السيبراني والدبلوماسية السيبرانية. مع التركيز على الأعمال التي تناولت التحول في طبيعة التهديد في المجال البحري، وتحليل نوعي للوثائق الاستراتيجية، والأطر التنظيمية، والتقارير الصادرة عن المنظمات الدولية والهيئات المعنية بحوكمة المجال البحري والبُنى التحتية البحرية الحرجة.

- **هيكل الدراسة.**

تُبنى هذه الدراسة على هيكل تحليلي متدرج يهدف إلى تفكيك الأمن البحري السيبراني بوصفه ظاهره أمنية معاصرة ومعقدة تتقاطع فيها الأبعاد التقنية والاستراتيجية والدبلوماسية. تبدأ الدراسة بتعريف منظومة الأمن البحري الأبعاد والخصائص الرئيسية ومفهوم الأمن البحري التقليدي وكذلك مفهوم منظومة الأمن البحري السيبراني والمكونات الرئيسية لهذه المنظومة والتي تتكون من المعلومات والتكنولوجيا والعنصر البشري والتحديات البنيوية التي تواجهها المنظومة ومن ثم نتطرق إلى كيفية إدارة المخاطر السيبرانية في المجال البحري.

وفي الفصل الثاني نبحث في تحليل الطبيعة التهديدية للأمن البحري السيبراني من خلال تأطير مفهوم التهديد البحري السيبراني ضمن التهديدات المعاصرة وغير التقليدية، وبيان العلاقة البنيوية بين الفضاء السيبراني والمجال البحري، مع تحليل عناصر التهديد الرئيسية.

والجهات الفاعلة، والمناطق البحرية الأكثر عرضة للمخاطر. ثم ننتقل إلى فحص تأثير هذه التهديدات على عناصر القوى الوطنية في المجال البحري، ولا سيما القوة العسكرية البحرية، والقدرة الاقتصادية المرتبطة بالشحن والتجارة والطاقة. والأمن القومي، والسمعة الدولية، مع إبراز دور التحول الرقمي والعامل البشري في تعزيز أو إضعاف هذه العناصر.

كما تعالج الدراسة بعد ذلك الانعكاسات الاستراتيجية لتحولات الأمن البحري السيبراني، من خلال تحليل موقعه ضمن الاستراتيجية الوطنية، واتساع نطاقه خارج الحدود الجغرافية التقليدية، ودوره المتنامي في الردع، وأهمية المرونة السيبرانية البحرية وما تفرضه من تحولات على العقيدة البحرية. كما تتناول الموقف الدولي المتطور تجاه هذا المجال عبر استعراض مقاربات الدول والمنظمات الدولية، وإشكاليات الحوكمة وتعدد أصحاب المصلحة. والهندسة الدفاعية السيبرانية كأداة استراتيجية لإدارة المخاطر ومنع التصعيد. وتختم الدراسة باستشراف المسارات المستقبلية للأمن البحري السيبراني حتى عام ٢٠٣٥، واستعراض التوصيات الاستراتيجية في هذا المجال. ومن ثم توقعات وآفاق البحث المستقبلية.

٢,١ الامن البحري. الأبعاد والخصائص الرئيسية.

يحظى الأمن البحري بإجماع تحليلي واسع في الأدبيات المتخصصة على أنه إطار متعدد الأبعاد، ويقوم على مجموعة من المكونات الجوهرية والرئيسية التي تعكس طبيعة التهديدات والوظائف المرتبطة بالمجال البحري. وفي هذا السياق، يُنظر إلى الأمن البحري بوصفه منظومة مركبة ومعقدة تتأسس على ثلاثة أبعاد رئيسية مترابطة [٣]، تشكل معاً البنية التحتية الأساسية لفهم تحدياته وخصائصه التشغيلية، **شكل رقم (١)**. وهذه الأبعاد هي:

- **الصراع على المصالح بين الدول. (Interstate Conflict).**

نمط من الصراع يرتبط بالقضايا التي تنشأ في إطار العلاقات البينية بين الدول، ويشمل النزاعات المرتبطة بالحدود أو السيادة على الأراضي، أو التنافس على الموارد. إضافة إلى حالات انتهاك قواعد القانون الدولي، وتندرج أنشطة العمليات الرمادية (**Grey Zone**) ضمن هذا الإطار بوصفها ممارسات تمارسها الدول أو أحد وكلائها، وتصاغ عمداً لتجنب الاستخدام المباشر للقوة العسكرية النظامية.

- **الإرهاب البحري والعنف المتطرف. (Extremism & Terrorism).**

يشير هذا البُعد إلى توظيف التنظيمات المتطرفة للمجال البحري كحيز تنفيذ وداعم مالي لأنشطتها الاجرامية، سواء عبر استهداف السفن التجارية وناقلات النفط، أو من خلال استغلال الجرائم البحرية لتمويل عملياتها وبناء قدراتها. ويتسم هذا النمط بمرونة جغرافية واضحة. إذ يمكن أن ينتقل العنف من البيئة الساحلية والبرية إلى البيئة البحرية، هذا البعُد يشمل شن هجمات على سفن الشحن في المناطق القريبة من الساحل.

- **الجريمة المنظمة (Blue Crime).**

أي نمط من أنماط الجريمة العابرة للحدود الوطنية التي تمارس في البحر أو من خلاله تعرف بمفهوم (**Blue Crime**). ويتبين هذا البُعد في ثلاثة أشكال رئيسية مترابطة: أولها الجرائم الموجهة ضد حرية وأمن الملاحة البحرية، منها هجمات القرصنة على السفن. وثانيها العمليات الاجرامية التي تشمل شبكات تهريب البشر والاتجار بالبضائع غير المشروعة عبر البحر. وآخرها الجرائم التي تلحق ضرر بالبيئة مثل الصيد غير المشروع وأنماط التلوث البحري بمختلف مصادرها، والذي يهدد البيئة البحرية واستدامتها.

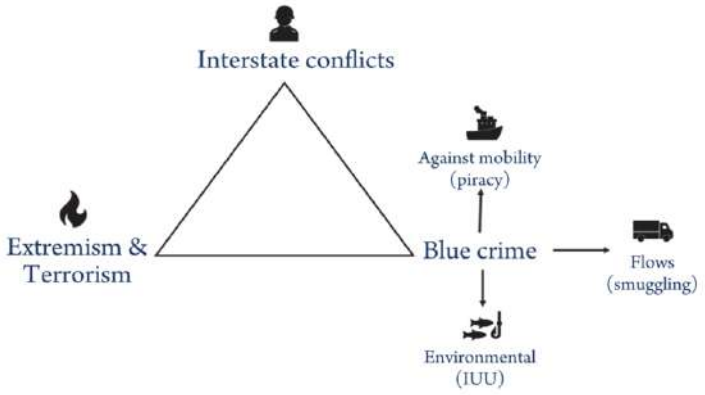


Figure 1.1 The three dimensions of maritime security

(شكل رقم ١) الأبعاد الرئيسية للأمن البحري.

الأبعاد الثلاثة تتميز عن بعضها البعض من خلال القواعد القانونية التي تحكمها والجهات الفاعلة المعنية. وهي مرتبطة بسلسلة من الخصائص والسمات التي تجمعها معاً في إطار الأمن البحري. مما يجعلها مشكله بارزه للأمن الدولي. وهذه السمات:

- **السمة المشتركة الأولى.**

تتميز البيئة البحرية بدرجة عالية من التعقيد العملياتي نظراً لاتساع نطاقها الجغرافي وتداخل أبعادها الطبيعية والقانونية. الأمر الذي يحد من فرض رقابة مستمرة وفعّالة عليها، ويُضعف آليات الرصد والإنقاذ، مما يخلق فجوات

3. Christian Buerger & Timothy Edmunds (2024) UNDERSTANDING MARITIME SECURITY.

أمنية قابلة للاستغلال من قبل الفاعلين غير الدوليين. هذه الظروف الجغرافية والأمنية تُسهم في تحويل المجال البحري الى بيئة مناسبة لتنفيذ أنشطة غير مشروعة وبعيدة عن الضبط الأمني المباشر لها.

- **السمة المشتركة الثانية.**

الأبعاد الثلاثة للأمن البحري تتسم بدرجة عالية من الترابط البنيوي (**Structural bonding**)، لاسيما العلاقة الوثيقة بين التطرف العنيف والجريمة المنظمة. حيث تلجأ الجماعات المتطرفة إلى توظيف أنماط من الجرائم البحرية المنظمة بوصفها أدوات تمويل ودعم لوجستي لأنشطتها.

- **السمة المشتركة الثالثة.**

يتسم الأمن البحري بتعقيد مؤسسي ناتج عن تعدد الجهات الفاعلة المسؤولة عن معالجة تحدياته، وفي مقدمتها القوات البحرية وحرس الحدود إلى جانب جهات حكومية وأمنية مساندة. لذلك هناك دول ومنظمات إقليمية تبنت استراتيجيات متخصصة وطورت ممارسات تنسيقية جديده مدعومة بمنظومات الوعي بالمجال البحري (**MDA**) لتعزيز الفهم المشترك والاستجابة السريعة للتهديدات.

٢,٢ مفهوم الامن البحري التقليدي.

يرى أستاذ العلاقات الدولية كريستيان بويغر في كتابه (**UNDERSTANDING MARITIME SECURITY**)[٤] بأن الأمن البحري لا يحظى حالياً بتعريف دولي موحد، وذلك ليس بوصفه قصوراً فهمياً ولكن بسبب طبيعته المركبة والمعقدة وتعدد الأجندات التي يستخدمها. والمفهوم السائد هو أنه عبارة عن مجموع السياسات والقدرات والإجراءات التي تعتمدها الدولة لحماية سيادتها البحرية وضمان السيطرة، وممارسة مفاهيم الحرمان البحري (**Sea Denial**)، وتأمين خطوط المواصلات البحرية الحيوية في أوقات السلم والحرب والأزمات.

لقد ارتبط هذا المفهوم تاريخيا بالقوة البحرية النظامية، حيث شكلت القوة البحرية الأداة الرئيسية لتنفيذه عبر الردع العسكري التقليدي، والدفاع عن المياه الإقليمية، وحماية الممرات البحرية الاستراتيجية ومواجهة التهديدات المادية المباشرة المتمثلة في الأساطيل البحرية المعادية والقرصنة.

وفي هذا السياق، ظل الأمن البحري يُفهم بوصفه امتدادا مباشرا للأمن الوطني وتحدده اعتبارات السيادة والقوة الصلبة للدولة أكثر من الأبعاد غير التقليدية أو العابرة للحدود.

٢,٣ مفهوم منظومة الامن البحري السيبراني.

منظومة متعددة المستويات تشمل مستويات متعددة الاستراتيجي والتقني والعملياتي والقانوني والمؤسسي، وتختص بحماية البنية الرقمية الداعمة للمجال البحري مثل أنظمة الاتصالات والملاحة والتحكم والموانئ الذكية وسلاسل الإمداد المؤتمتة والكابلات البحرية. وتعمل المنظومة على الربط بين الأبعاد التقنية والعملياتية والقانونية، بهدف منع الهجمات السيبرانية، وضمان استمرار الوظائف البحرية الحيوية في بيئة تشغيلية عابره للحدود.

٢,٤ المكونات الرئيسية لمنظومة الامن البحري السيبراني .

- **المعلومات.**

تُعد المعلومات الركيزة المعرفية الأساسية لمنظومة الأمن السيبراني. إذ تُساهم في بناء الوعي بالمجال البحري الرقمي (**Maritime Cyber Situational Awareness**)، وفهم أنماط التهديد السيبراني وتأثيراته التشغيلية، وجمع البيانات الصادرة من الأنظمة البحرية والموانئ وسلاسل الإمداد، ومن ثم تحليلها ودمجها بصورة واحدة تتيح الإنذار المبكر، ودعم صناعة القرار، وتعزيز الاستجابة للحوادث السيبرانية.

٤. Christian Bueger بروفيسور وزميل باحث في معهد الأمم المتحدة. مؤلف كتاب UNDERSTANDING MARITIME SECURITY- مع الكاتب Timothy Edmunds ٢٠٢٤

- **التكنولوجيا.**

تُمثل التكنولوجيا البنية التحتية التشغيلية للمنظومة. وتشمل أنظمة حماية الشبكات البحرية. وأمن أنظمة التحكم الصناعية التشغيلية، وتقنيات الاستشعار والمراقبة الرقمية، ومنصات ومراكز تبادل المعلومات. وتكمن أهميتها في كشفها عن الهجمات السيبرانية واحتواءها وإحباطها، وضمان استمرارية الوظائف البحرية الحيوية في بيئة بحرية تتسم بالتعقيد والترابط العابر للحدود. وهناك طبقتين للتكنولوجيا:

(**أ أ**). **طبقة البرمجيات** (**Software Layer**).

تضم هذه الطبقة الأنظمة والتطبيقات والمنصات التي تدير وظائف السفن والموانئ رقمياً، مثل برمجيات الملاحة وأنظمة إدارة الميناء ومنصات الاتصالات وأدوات المراقبة والكشف والاستجابة. وتعتبر هذه الطبقة محور الضبط الأمني عبر سياسات التهيئة الآمنة، وإدارة التحديثات، والتقسيم الشبكي، وتفعيل الرصد المستمر والاستجابة للحوادث.

(**ب ب**). **الطبقة الفيزيائية** (**Hardware Layer**).

تغطي الطبقة الفيزيائية البُنية المادية التي تُشغِّل وتمكّن الطبقة البرمجية داخل السفن والموانئ، وتمثل أشباه الموصلات (Semi-Conductor) وكذلك ال Firmware أساس الاعتمادية والثقة التشغيلية لهذه الطبقة، نظراً لارتباطهما المباشر بسلامة الإشارات ودقة التزامن. لذا يرتكز أمن هذه الطبقة على حوكمة العتاد وإدارة ال **Firmware**.

- **العنصر البشري.**

يُعد العنصر البشري عاملاً حاسماً في فاعلية منظومة الأمن البحري السيبراني سواء بوصفه خط الدفاع الأول أو أحد أبرز المخاطر. هذا العنصر يشمل الكفاءات التقنية، والقيادات العملياتية، والعاملين في المرافق البحرية. إن العنصر البشري يتطلب برامج تدريب وتأهيل مستمرة، وثقافة وعي سيبراني، وإجراءات واضحة لتوزيع المهام والمسؤوليات واتخاذ القرار أثناء الازمات الطارئة.

- **التحديات الرئيسية.**

تواجه منظومة الأمن البحري السيبراني جملة من التحديات البنيوية والتشغيلية التي تعيق فاعليتها، وتحد من قدرتها على مواكبة طبيعة التهديدات الرقمية المتسارعة. وتبرز هذه التحديات في أربعة محاور رئيسية تمس العنصر التقني والعنصر البشري، وكذلك مستوى الوعي بالمجال البحري، والإطار المؤسسي.

- **الأنظمة القديمة.**

إن الاعتماد على الأنظمة البحرية القديمة هو أحد أبرز التحديات في الأمن البحري السيبراني. وذلك لأن هذه الأنظمة صممت في الأساس لتحقيق الاستمرارية التشغيلية وليس لمواجهة التهديدات الرقمية المعاصرة والمتجددة. وهي أنظمة قديمة تفتقر إلى خصائص التحديث المنتظم والتشفير والعزل الشبكي. كما يصعب دمجها وتوافقها مع حلول الحماية الحديثة، وهذا يجعلها نقاط ضعف هيكلية رئيسية قابلة للاختراق السيبراني.

- **نقص الكفاءات المتخصصة.**

تعاني منظومة الأمن البحري السيبراني من فجوة واضحة ونقص في الكفاءات والكوادر القادرة على الجمع بين الفهم التقني العميق وبين الخبرة العملياتية البحرية. ويؤدي هذا النقص إلى ضعف في تقييم المخاطر، وتأخر في اكتشاف الهجمات، وصعوبة في إدارة الحوادث السيبرانية ذات البعد البحري، لاسيما في البيئات المعقدة التي تتطلب تنسيقا فوريا بين الجهات التقنية والتشغيلية.

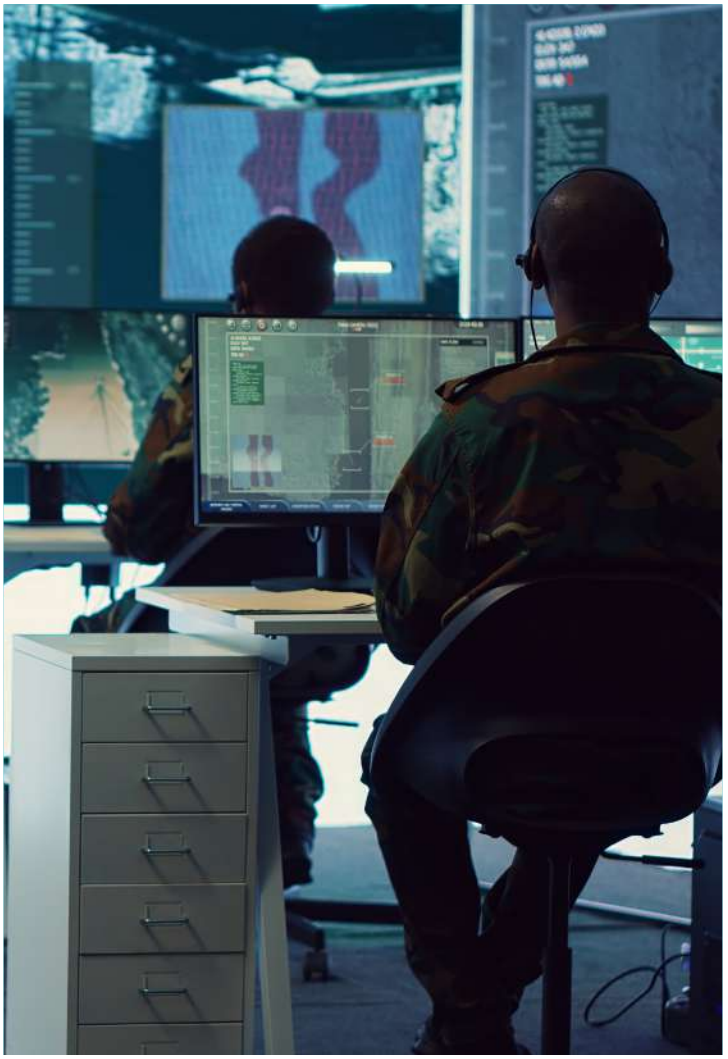
- **ضعف الوعي السيبراني.**

يُعد انخفاض الأمن البحري السيبراني لدى العاملين في السفن والموانئ والمنصات والجهات البحرية عامل مضاعف للمخاطر. اذ تسهم الممارسات غير الآمنة، وسوء استخدام التقنية والأنظمة، والاعتماد الدائم على الإجراءات التقليدية وغير المحدّثة في توسيع نطاق الهجوم السيبراني. كما يؤدي القصور في الوعي السيبراني إلى

تطبيع المخاطر الرقمية والتقليل من دلالاتها العملياتية، وهو ما يؤدي إلى التأخر في الإبلاغ والاستجابة، الأمر الذي يؤدي إلى انتقال الأثر إلى مستويات تمس السلامة البحرية واستمرار العمليات.

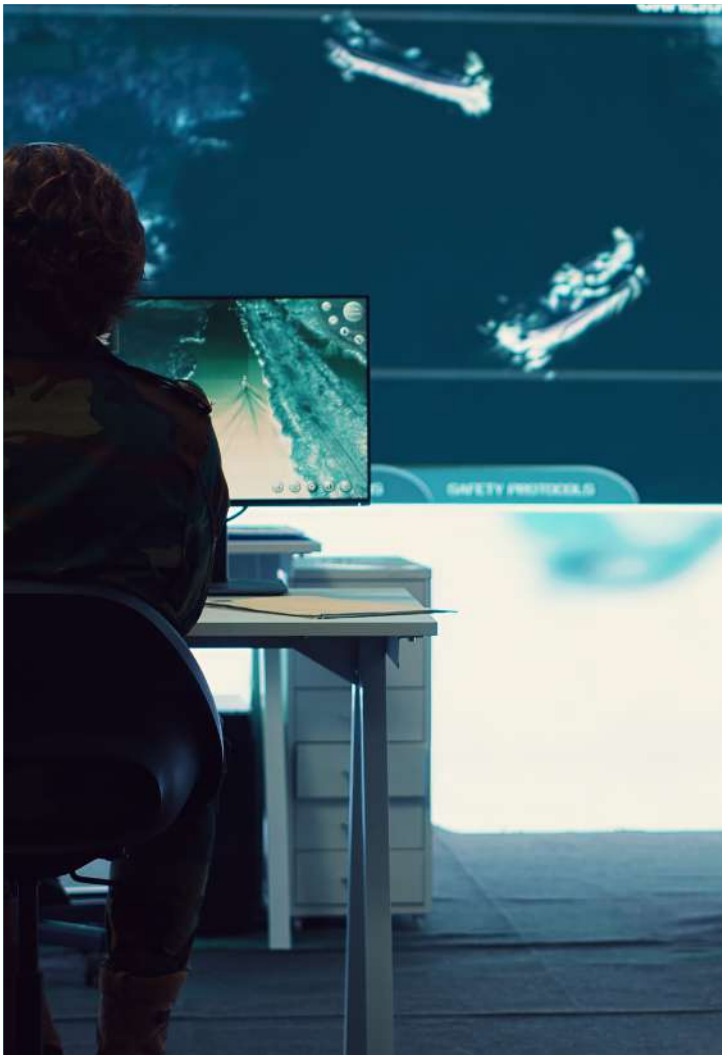
- **تشابك المسؤوليات المؤسسية.**

هناك تحدٍ جوهري في الأمن البحري السيبراني نتيجة تداخل وتشابك المسؤوليات بين الجهات البحرية والأمنية والتقنية سواء على المستوى الوطني أو الإقليمي أو الدولي. ويؤدي غياب وضوح الأدوار وسلاسل القيادة أثناء الحوادث السيبرانية إلى تأخر الاستجابة، وتضارب الإجراءات وضعف المساءلة. وهو ما يقلل من قدرة المنظومة على التعامل مع التهديدات السيبرانية العابرة للحدود.



٢.٤ إدارة المخاطر السيبرانية في المجال البحري. (Maritime Cyber Risk Management).

تؤكد الأدبيات المتخصصة أن إدارة المخاطر السيبرانية في المجال البحري تمثل مقاربة تحليلية ومنهجية تهدف إلى ضبط العلاقة بين التهديدات الرقمية والهشاشة التشغيلية للمنظومات البحرية. وتنطلق هذه الإدارة من تحديد الأصول البحرية الرقمية ذات الأهمية الاستراتيجية الحرجة، وتقييم احتمالات التعرّض السيبراني وآثاره المحتملة على السلامة والملاحة وسلاسل الامداد، وصولاً إلى تصميم استجابات وقائية وتصحيحية متدرجة. كذلك تقوم على دمج البعد التقني مع الابعاد العملياتية والمؤسسية والقانونية وبما يضمن موائمة قرارات إدارة المخاطر مع طبيعة البيئة البحرية، ويعزز القدرة على الصمود السيبراني واستمرارية الوظائف البحرية الحيوية.



ثالثا: التهديد البحري التقليدي.

يُقصد بالتهديد البحري التقليدي مجموعة الأفعال العدائية أو غير المشروعة التي تحدث في المجال البحري وتعتمد أساساً على وسائل مادية مباشرة (القوة البحرية المسلحة، نشاط القرصنة والسطو المسلح، الجريمة المنظمة من تهريب بأنواعه) بما يستهدف أمن السفن والأطقم والموانئ وخطوط الملاحة والسيادة البحرية وحرية العبور. وينطلق مفهوم التهديد البحري التقليدي من النظر إلى البحر بوصفه مسار اقتصادي يجب تأمينه ومجال للسيادة وفرض القانون، وبيئة لنشاط الجريمة المنظمة، وعند تصاعد التنافس بين الدول يصبح مسرح لصراع مسلح. وهناك نمطين لهذة التهديدات (تهديدات ذات طابع دولي–عسكري & وتهديدات الجريمة البحرية المنظمة).

٣,١ تهديدات ذات طابع دولي– عسكري.

التهديدات البحرية التقليدية ذات الطابع الدولي–العسكري تتمثل في استخدام الدولة للقوة البحرية أو التلويح باستخدامها وذلك لتحقيق غايات سياسية وعسكرية عبر التحكم في المجال البحري وحرمان الخصم من المناورة. ويشمل ذلك الاشتباك البحري بين القوات النظامية لدولتين أو أكثر، وعمليات استعراض القوة بما تحمله من رسائل ردع. إضافة إلى عمليات الحصار البحري والتحريم البحري (**Sea Denial**) لقطع الامدادات وتعطيل خطوط المواصلات البحرية ذات القيمة الاستراتيجية. ويأتي من ضمن التهديدات عمليات زراعة الألغام أو التهديد بها لرفع كلفة المرور، والاعتداء على السفن أثناء النزاع المسلح والأزمات الذي يرفع مخاطر التصعيد ويؤثر مباشرة في أمن التجارة الدولية.

٣,٢ الجريمة المنظمة (Blue Crime).

البحر بيئة مفضلة للجريمة المنظمة وذلك لثلاثة أسباب أولها اتساع وعمق المجال البحري (عبارة عن مساحة ضخمة مقابل قدرة مراقبة محدودة). وثانيها يتمثل في تجزئة الاختصاصات، حيث ان جزء منه يتبع الدولة المشاطئة مثل المياه الداخلية والإقليمية بينما المنطقة الاقتصادية وأعالي البحار لا تتبع لأي دولة، السبب الثالث هو كثافة التجارة والحركة الهائلة للسفن والتي تخلق ضجيج يخفي أنشطة غير مشروعة.

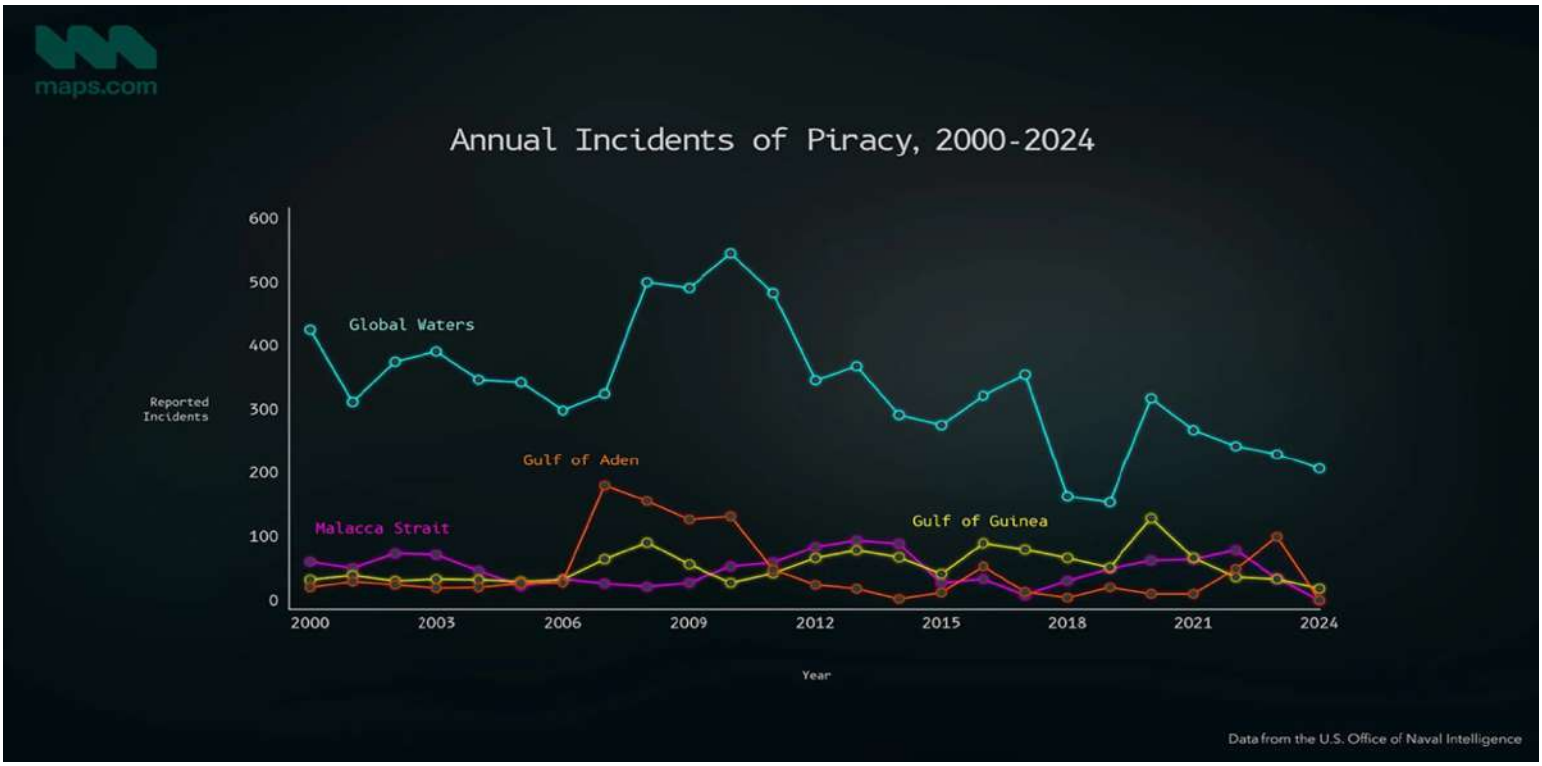
إن الجريمة المنظمة في المجال البحري (**Blue Crime**) تُعد تجسيداً لاقتصاد غير مشروع يعمل عبر البحر، وتوظف شبكات عابرة للحدود الممرات البحرية والموانئ وسلاسل الإمداد لتمرير السلع والأشخاص لتحقيق أرباح غير مشروعة. وتكمن خطورتها في أنها تربط الفعل الإجرامي بالحوكمة والفساد والقدرة على تعطيل الملاحة والأمن الاقتصادي. وتفرض مقاربة تكاملية بين إنفاذ القانون والتعاون الدولي. إن الجريمة المنظمة تشمل ثلاثة أنماط رئيسية:

- **جرائم ضد الحركة البحرية (أنشطة القرصنة البحرية والسطو المسلح ضد السفن).**

القرصنة البحرية والسطو المسلح يشتركان في كونهما نفس النشاط الإجرامي المتمثل في الاعتداء على السفن، لكن الفارق بينهما هو نطاق المكان والاختصاص. حيث أنه وفق اتفاقية الأمم المتحدة لقانون البحار، فإن نشاط القرصنة يكون في أعالي البحار وخارج الولاية القضائية لأي دولة، بينما نشاط السطو المسلح ضد السفن وفق تعريف (**IMO**) فهو يقع في المياه الداخلية أو المياه الإقليمية للدولة.

أظهرت أنشطة القرصنة والسطو المسلح خلال الفترة (٢٠٠٠–٢٠٢٤) عن تمركز ملحوظ في عدد من الممرات البحرية ذات الأهمية الاستراتيجية العالية **شكل رقم** (٢)، على سبيل المثال، مضيق ملقا جنوب شرق آسيا لفترة (٢٠٠٠–٢٠٠٥) تعتبر بؤرة رئيسية للقرصنة، وفيه تمت ٤٠٪ من إجمالي أنشطة القرصنة (١٣٠ من أصل ٣٢٥ عالميا)، كما برز خليج عدن قبالة سواحل الصومال خلال (٢٠٠٨–٢٠١٧) كنموذج لتهديد القرصنة وخطف السفن. أما خليج غينيا (٢٠١٠–٢٠١٥) تصاعدت عمليات الخطف والتي شكلت أكثر

من ٩٥٪ من خطف البحارة عالميا في ٢٠٢٠ وهو ما دفع الدنمارك إلى إعادة هيكلة استراتيجياتها واستحداث منصب بمسمى سفير للأمن البحري. كما أن الهجمات التي نفذها الحوثيين على السفن التجارية في جنوب البحر الأحمر (٢٠٢٤-٢٠٢٥) أحدثت تحولاً في طبيعة التهديدات التقليدية ذات الأبعاد الجيوسياسية المباشرة.



شكل رقم (٢) **حوادث القرصنة خلال الفترة** (٢٠٠٠-٢٠٢٤)

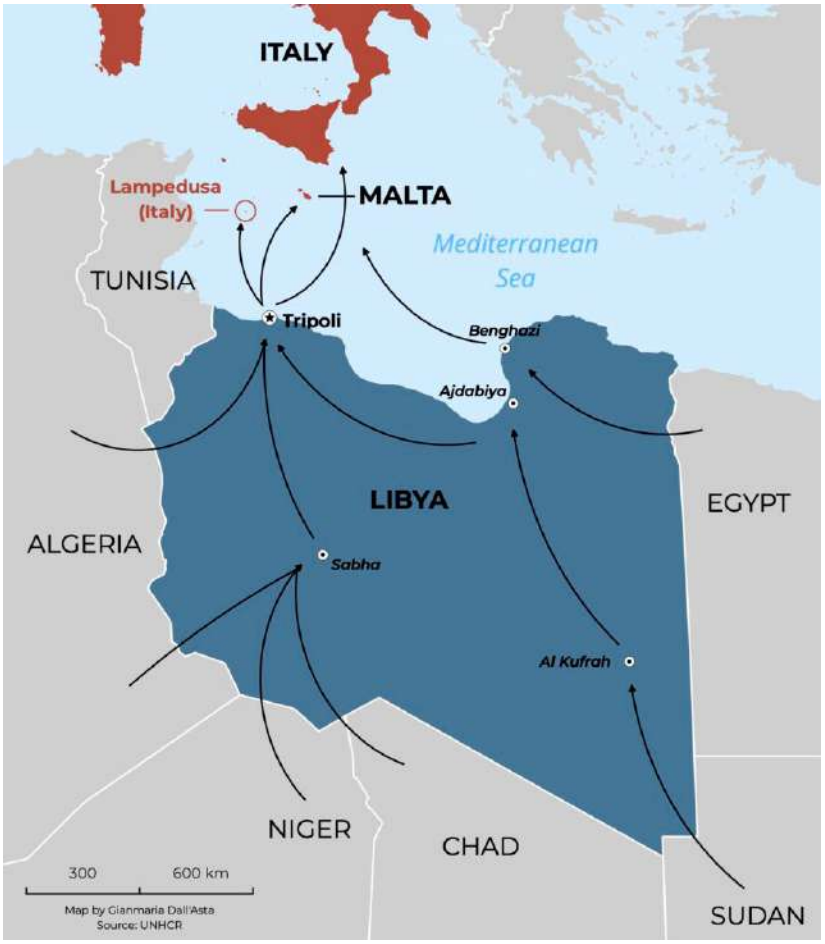
- **التدفقات الإجرامية عبر البحر (Criminal flows).**

نمط غير تقليدي من أنشطة الجريمة المنظمة البحرية تشمل أنشطة التهريب بمختلف صورها (مخدرات، أسلحة، وقود، مهاجرين)،و تعمل على تحويل البحر من مسرح اعتداء مباشر إلى قناة لوجستية لتمرير أشخاص أو سلع أو أموال عبر شبكات متعددة العُقد. جوهر هذا النمط ليس الاشتباك مع السفن بقدر ما هو استغلال سلاسل الإمداد البحرية لإخفاء الشحنات داخل تجارة مشروعة، أو نقلها بين سفن في عرض البحر ثم إعادة إدخالها للأسواق.

تُظهر مؤشرات تم تدوينها عن طريق وكالة المخدرات الأوربية (**EUDA**) بأنه تم ضبط ٤١٩ طن من الكوكايين (٥) خلال عام ٢٠٢٣. وفيما يتعلق بعمليات الاتجار بالبشر عبر البحر فأحدث رقم عالمي موجود لدى مكتب الأمم المتحدة المعني بالمخدرات والجريمة (**UNODC**) يشير إلى وجود ٦٩٦٢٧ ضحية مكتشفة (٦) في عام ٢٠٢٢. كما يُقدر مكتب (**UNODC**) أن القيمة المالية لنشاط تهريب المهاجرين بحرا عبر مسار وسط البحر الأبيض المتوسط من شمال أفريقيا إلى جنوب أوروبا **شكل رقم** (٣) يتراوح بين ٢٩٠-٣٧٠ مليون دولار خلال عام ٢٠٢٣.

5. https://www.euda.europa.eu/publications/european-drug-report/2025/cocaine_en

6. https://www.unodc.org/documents/data-and-analysis/glotip/2024/GLOTIP2024_BOOK.pdf



شكل رقم (٣). تهريب المهاجرين عبر مسار وسط البحر الأبيض المتوسط

- **الجرائم البيئية البحرية.**

يمثل هذا النمط مجمل الأفعال الاجرامية التي تستهدف المحيطات والبحار ومواردها بوصفها مصدراً للربح غير المشروع، ويتم ذلك عبر شبكات منظمة تستفيد من ضعف الرقابة والفساد وتباين ولايات الاختصاص في المجال البحري. ويأتي في مقدمة هذه الأفعال الصيد غير القانوني وغير المبلّغ عنه وغير المنظم (**IUU** **Unreported and Unregulated Fishing**) وهو ما تصفه منظمة الأغذية والزراعة (**FAO**) بأنه مفهوم واسع يشمل أنشطة صيد مخالفة للقوانين والمعايير، ويمكن أن يقع في أعالي البحار أو ضمن الولايات الوطنية. وقد يتداخل مع أنماط الجريمة المنظمة. ويُعد هذا النمط أكثر هذه الجرائم تأثيراً على الاقتصاد الأزرق – وفق التعريف الشائع في أدبيات البنك الدولي أنه منظومة اقتصادية تقوم على الاستخدام المستدام لموارد البحار والمحيطات لتحقيق نمو اقتصادي وفرص عمل وتحسين سبل العيش مع الحفاظ على صحة النظم البيئية البحرية– [٧]. وتشير تقديرات مرجعية أن خسائر الصيد غير القانوني وغير المُبلغ قد يتراوح بين ١٠–٢٣,٥ مليار دولار سنويا [٨]. وجرائم التلوث البحري تشمل مثل الألقاء والتسريب المتعمد لمواد سامة أو نفايات في البيئة البحرية، وتشير **INTERPOL** إلى أن جماعات إجرامية عابر للحدود تتجه بصوره متزايدة إلى الصيد غير المشروع بما يهدد الأمن الغذائي والاستقرار في الدول الساحلية [٩].

7. https://www.worldbank.org/en/news/infographic/2017/06/06/blue-economy
8. /https://pubmed.ncbi.nlm.nih.gov/19240812
9. https://www.interpol.int/en/Crimes/Environmental-crime/Fisheries-related-crimes

٤,١ مفهوم التهديد البحري السيبراني.

- **التهديدات السيبرانية كجزء من التهديدات غير التقليدية.**

التهديدات غير التقليدية (**Non-Traditional Security Threats**) هي أنماط تهديد غير متناظرة (**Asymmetric Threat**) تعمل خارج إطار المواجهة العسكرية المباشرة، وتعتمد على أدوات غير عسكرية أو هجينة، وتتسم بالغموض، وانخفاض مستوى التصعيد، والقدرة على إحداث آثار أمنية وإستراتيجية واسعة عبر استغلال نقاط الضعف البنيوية في الأنظمة الرقمية والعمل ضمن بيئات رمادية (**GREY ZONE**).

هذه التهديدات غير التقليدية لها أشكال متعددة منها التهديدات السيبرانية، والتهديدات الهجينة. ويُعرّف التهديد البحري السيبراني بأنه مجموعة الأنشطة العدائية التي تستهدف الأنظمة الرقمية والبُنى التحتية المعلوماتية المرتبطة بالمجال البحري، بما في ذلك السفن والموانئ الذكية، وأنظمة الملاحة والاتصالات، وسلاسل الامداد البحرية المؤتمتة. ويُصنّف هذا النوع من التهديدات ضمن التهديدات غير التقليدية لاعتماده على أدوات غير عسكرية، وفاعلين متعددي الأنماط، وقدرته على العمل في بيئات رمادية تتسم بصعوبة الإسناد وانخفاض التصعيد. وتستدعي تلك التهديدات تبني منطق وقائي قائم على إدارة المخاطر والمرونة في بيئة بحرية رقمية عالية الترابط.

- **العلاقة بين الفضاء السيبراني والمجال البحري.**

أصبح المجال البحري جزء من منظومة تشغيلية سيبرانية مترابطة تعتمد على أنظمة المعلومات والاتصالات في إدارة الملاحة البحرية، وتشغيل السفن والموانئ الذكية، وتأمين سلاسل الامداد البحرية. وأدى هذا الاندماج البنيوي بين الفضاء السيبراني والمجال البحري إلى تحول جوهري في الطبيعة التهديدية، حيث بات الاستهداف يتركز على الطبقة الرقمية بوصفها نقطة الضعف الأكثر تأثيراً في الأمن البحري المعاصر.

ويُفهم التهديد البحري السيبراني كنتيجة مباشرة للتداخل الوظيفي بين المجالين، بما يُتيح التأثر عن بُعد وبكلفة منخفضة ودون استخدام القوة العسكرية التقليدية. ويؤدي هذا النمط من التهديد إلى تعقيد الإسناد القانوني والسياسي، وتقويض أدوات الردع التقليدية، ويجعل منه مؤشراً مركزياً على التحول في طبيعة المخاطر البحرية، ومرتكزاً أساسياً لتحليل الأمن البحري السيبراني.

٤,٢ عناصر التهديد البحري السيبراني.

يُعرف التهديد بأنه كل العوامل التي تُضعف قدرة الدولة أو النظام الدولي على استخدام البحر بأمان وكفاءة، أو تمنع حرية الحركة، أو تستهدف البنى البحرية الحرجة[١٠]. والتهديدات السيبرانية البحرية هي عبارة عن مجموعة من العناصر المترابطة وتعمل ضمن منظومة واحدة، تستهدف الوظائف التشغيلية والاقتصادية والاستراتيجية للمجال البحري، وتستغل الاعتماد المتزايد على الرقمنة والترابط الشبكي. ولا تنبع خطورة هذه التهديدات من عنصر واحد منفصل، بل من تفاعل عناصرها وقدرتها على احداث تأثيرات متسلسلة تتجاوز حدود المجال البحري الى مجالات تتعلق بالأمن القومي والاقتصاد العالمي. وهذه العناصر تتمثل فيما يلي:

- **الهجمات السيبرانية على السفن الذكية.**

أدى التوسع المتسارع في اعتماد السفن على الأنظمة الرقمية إلى إحداث تحول نوعي في طبيعة التهديدات والمخاطر التي تواجه الأمن البحري، حيث أصبح الفضاء السيبراني جزءاً مكوناً من بيئة التشغيل البحري. وتتمثل الهجمات السيبرانية على السفن الذكية في استهداف أنظمة الملاحة والتحكم والاتصالات، وينتج عنه تعطيل

١٠. Geoffery Till (sea power. A Guide for the Twenty-First Century (ry

العمليات التشغيلية أو التلاعب بالمسار الملاحي والسرعة أو التأثير في أنظمة السلامة وهو ما يزيد من احتمالات الحوادث البحرية التي من الممكن كذلك تحدث في الممرات البحرية الحيوية والحرجة أو التعطيل المتعمد لحركة الشحن. وتتفاقم خطورة هذه التهديدات نتيجة تعقيد البُنى الرقمية على متن السفن، وضعف الفصل بين الشبكات التشغيلية (**OT**) وتقنية المعلومات (**IT**). وتمتد آثار هذه الهجمات إلى سلاسل الامداد البحرية وتؤثر على تكاليف التأمين والشحن ومستوى الثقة في أمن الملاحة. وهو ما يمنحها أبعاداً تشغيلية واستراتيجية تستدعي مقاربات شاملة قائمة على إدارة المخاطر وتعزيز المرونة السيبرانية.

- **البُنى التحتية البحرية الحرجة (Critical Maritime Infrastructure CMI).**

البُنى التحتية البحرية الحرجة هي مجموعة الأصول والأنظمة والشبكات (المادية والرقمية والخدمية) المرتبطة بالمجال البحري، والتي يُعد تعطيلها أو تدميرها أو اختراقها ذا أثر منهك على سلامة الملاحة والتجارة والطاقة والأمن القومي للدولة وقد يمتد أثره عبر الحدود[11]. وبالنظر إلى التأثير السيبراني المباشر عليها يمكن تصنيفها في ثلاث مجالات رئيسية:

(أ) البنية التحتية للنقل (الموانئ الرقمية – الممرات المائية الحيوية – سفن الشحن).

تُعد البنية التحتية البحرية الحرجة المرتبطة بالنقل هدف رئيسي للتهديدات غير التقليدية، نظرا لدورها المركزي في استمرارية التجارة العالمية وسلاسل الامداد. ولم تعد المخاطر التي تواجهها مقتصرة على التهديدات الأمنية المباشرة، بل امتدت لتشمل استهداف الوظائف التشغيلية والرقمية التي يقوم عليها النظام البحري المعاصر وهذا يضاعف أثر أي اضطراب ويمنحه بعداً استراتيجياً يتجاوز النطاق المحلي.

11. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/resilience-services/infrastructure-dependency-primer/learn/critical-infrastructure-systems

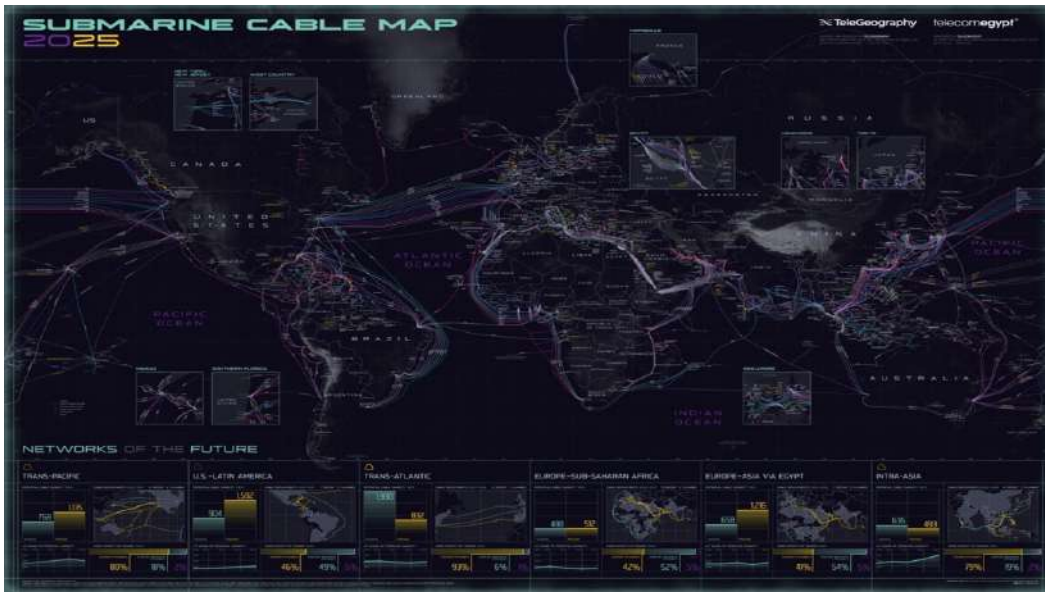
ان استهداف الموانئ الرقمية يؤدي إلى تعطيل التدفقات التجارية وانعدام الثقة اللوجستية، بينما يؤدي تهديد الممرات البحرية إلى خلق بيئة عدم يقين ذات أثر فوري على الأسواق العالمية نظرا لمحدودية البدائل، كما أنه يصنف تلك الممرات كممرات ذات هشاشة عالية. وبخصوص سفن الشحن فإن اعتمادها المتزايد على الأنظمة الرقمية يجعلها عرضة للاختراق آو التلاعب بالمعلومات الملاحية، والذي يؤدي بالتالي إلى حوادث أو تعطيل متعمد. كل ذلك يستدعي مقاربة تكاملية ترتكز على المرونة وإدارة المخاطر بشكل استباقي.

(ب ب) البنية التحتية للطاقة (منصات النفط والغاز البحرية – خطوط الانابيب تحت الماء – مزارع الرياح والطاقة المتجددة البحرية).

تعتبر من أكثر الأصول البحرية حساسية من الناحية الأمنية والاستراتيجية نظراً لدورها المحوري في أمن الطاقة واستقرار الاقتصادات الوطنية والأسواق العالمية. وهذا الثقل الاستراتيجي جعل المنشآت هدفاً مباشراً لتهديدات غير تقليدية تتسم بالغموض، والعمل في البيئات الرمادية، واستغلال التعقيد التقني والتشابك البنيوي لمنظومات الطاقة البحرية. تتجلى هذه التهديدات في استهداف أنظمة التشغيل والتحكم لمنصات النفط والغاز. وكذلك التخريب أو التعطيل المتعمد لخطوط الأنابيب تحت الماء. إضافة إلى الهجمات السيبرانية التي تستهدف مزارع الطاقة المتجددة البحرية والتي تعتمد على الأنظمة الرقمية. وخطورة تلك التهديدات هو في قدرتها على احداث انقطاعات طويلة الأمد في امدادات الطاقة، وخلق مشاكل اقتصادية تتجاوز النطاق المحلي إلى مستوى إقليمي ودولي. كل ذلك يستدعي مقاربة تكاملية لمعالجة تحديات أمن الطاقة البحرية بوصفه جزء رئيسي من منظومة الأمن البحري والأمن الوطني.

(ج ج) البنية التحتية للاتصالات والمعلومات (كابلات الاتصالات البحرية –أنظمة الملاحة والاقمار الصناعية–الشبكات والتحكم).

هذه البنية تشمل كابلات الاتصالات البحرية وأنظمة الملاحة والأقمار الصناعية وشبكات المراقبة والتحكم. وتُعد عنصرا بنيويا في تشغيل المجال البحري والاقتصاد الرقمي العالمي. وتعتبر هدفا مباشراً للتهديدات، ولأهمية وحساسية مكونات هذه البنية سوف نفصل قليلا في ذلك. الكابلات البحرية تعتبر عنصر رئيسي في الاقتصاد الرقمي حالياً، وهي أهم مصدر لنقل البيانات والاتصالات. حيث إنها تنقل٩٨-٩٧ ٪ من حركة البيانات الدولية عبر شبكة تمتد بين القارات .كما أن لها أهمية اقتصادية وأمنية عالية، حيث تعتبر الشريان الرئيسي للاقتصاد الرقمي في الوقت الحالي. وتقدر عدد الكابلات البحرية ب (٥٩٧) كيبل بحري حسب موقع **Submarine Cable Map 2025** [١٢]. **شكل رقم (٤).**



شكل رقم (٤) مسار الكابلات البحرية في البحار

وتشير الأدبيات إلى أن أي تقاطع عدة كابلات اتصالات بحرية في نقطة أو نطاق جغرافي محدد يعرف اصطلاحاً ب (Submarine Cable Hub) وهي نقاط تشكل عقداً مركزية في بنية الاتصالات العالمية. ولهذا سوف نعتمد في هذه الدراسة مصطلح (**المناطق الحرجة لتقاطع الكابلات البحرية Critical Submarine Cable Convergence Zone**) للإشارة إلى الأقاليم الجغرافية البحرية أو الساحلية التي تتجمع فيها عدة أنظمة من الكابلات الدولية ضمن حيز مكاني ضيق، وتكتسب هذه المناطق حساسية استراتيجية عالية نظراً لحجم تدفقات البيانات والاتصالات التي تمر عبرها، وما تمثله من نقاط ارتكاز حيوية للاقتصاد الرقمي والأمن الوطني. **ويؤدي فقدان السيطرة أو الحماية لهذه الكابلات إلى تقويض السيادة الرقمية للدولة. ما يجعل أي انقطاع أو عبث بها مسألة أمن قومي ذو ابعاد أمنية واستراتيجية وليس مجرد خلل تقني.**

وما يتعلق بأنظمة الملاحة والأقمار الصناعية فهي تمثل العمود الفقري للملاحة البحرية المعاصرة وإدارة الحركة البحرية والسلامة في البحار. هذه الأنظمة تواجه تهديدات تشمل التشويش والتضليل والذي قد يؤدي إلى فقدان الدقّة الملاحية وخلق بيئة عالية المخاطر في الممرات البحرية الحيوية. هذا التهديد له بعد استراتيجي عالي نظراً لاعتماد القطاعات المدنية والعسكرية معاً على هذه الأنظمة، مما يجعل أي اضطراب فيها وخاصة خدمات (Positioning, Navigation, and Timing PNT) له آثار مزدوجة تتجاوز المجال البحري إلى النقل الجوي والبري، والاقتصاد، وسلاسل الامداد، والاتصالات والطاقة.

12. https://submarine-cable-map-2025.telegeography.com

وفيما يخص شبكات المراقبة والتحكم البحرية سواء تلك المرتبطة بإدارة الموانئ أو مراقبة السواحل أو تشغيل البنية التحتية البحرية الحرجة، فإن التهديد يتمثل في استهداف أنظمة الاستشعار، ومنصات دمج البيانات، وشبكات القيادة والسيطرة. ويؤدي اختراق هذه الشبكات أو تعطيلها إلى إضعاف الوعي بالمجال البحري (Maritime Domin Awareness)، وتقليص قدرة الاستجابة المبكرة، وخلق فجوات تشغيليه يمكن استغلالها لأغراض امنية أو اقتصادية أو استخباراتية.

- **الذكاء الاصطناعي العسكري البحري.**

يُمثّل الذكاء الاصطناعي العسكري البحري تحول بنيوي في طبيعة العمليات البحرية. إذ ينقلها من منطق الاستجابة وردة الفعل إلى منطق التوسع الاستباقي القائم على تحليل البيانات الضخمة وتسريع عملية صناعة القرار وتمكين القيادة من اتخاذ قرارات حاسمة في فترة زمنية قصيرة. ولا يُعد الذكاء الاصطناعي تهديداً بحد ذاته بل قدرة عملياتية (**Operational Capability**) تعزز الوعي بالمجال البحري (**MDA**) والكفاءة التشغيلية وإدارة المخاطر. وخطورته تكمن في كونه تقنية مزدوجة الاستخدام (**Daul-Use Technology**). اذ يمكن توظيفه سواء لتعزيز الأمن البحري أو استخدامه ضمن التهديدات الهجينة عبر أتمتة الاستهداف وتسريع التصعيد وإضعاف الاستقرار في البيئات البحرية المتنازع عليها. إن الذكاء الاصطناعي يعتبر عاملاً حاسماً في معادلات الردع والتنافس المستقبلي في البحر.

- **التهديدات الهجينة (سيبرانية-سياسية-اقتصادية).**

يُعد التهديد الهجين (**Hybrid Threat**) من أخطر أنماط التهديدات في المجال البحري. إذ يقوم على توظيف متكامل لأدوات متعددة منها العسكرية والسيبرانية والسياسية والاقتصادية، وذلك لاستهداف الملاحة البحرية والبنية التحت بحرية الحرجة وسلاسل الامداد وكابلات الاتصالات. ويهدف هذا النمط إلى احداث تأثير استراتيجي في مناطق عمليات محددة دون الوصول إلى حرب مباشرة. يعتمد هذا التهديد على وسائل مادية مُسيّرة مثل الزوارق والطائرات والغواصات والصواريخ بعيدة المدى، ووسائل غير مادية تشمل الهجمات السيبرانية والتشويش الملاحي. ويساهم الضغط السياسي والأدوات الاقتصادية في هذا النمط. وتتمثل نتائجه في تصعيد مستمر وتقييد حركة الملاحة واضطراب سلاسل الامداد وارتفاع أسعار الطاقة. كما أنه يسهم بشكل رئيسي في إعادة تشكيل موازين القوى البحرية.

- **القرصنة الرقمية لسلاسل الإمداد.**

تتسم سلاسل الامداد البحرية بترابط بنيوي عال وتعدد الفاعلين وتداخل الأنظمة الرقمية والتشغيلية، وهذا يجعلها بيئة مثالية لهجمات القرصنة الرقمية لسلاسل الامداد بوصفها استراتيجية متعددة الطبقات ومركبة لا تستهدف جهة واحدة، ولكن المنظومة بأكملها عبر استغلال نقطة ثانوية أو طرف ثالث. تتجلى خطورة هذا النمط في إحداث تداعيات جيوستراتيجية مباشرة لتشمل تعطيل قطاعات اقتصادية حيوية أو احداث خلل في تشغيل الموانئ الذكية. حيث يؤدي اختراق هدف واحد إلى الحاق الضرر بعدة شركات في مناطق مختلفة كما حدث في هجوم (**Notpetya**) على شركة (**Maersk**) [١٣] **شكل رقم** (٥) . يتيح هذا النمط الوصول العميق إلى الأنظمة الداخلية دون اختراق الواجهات الأمامية. وتتميز بصعوبة الاكتشاف وسرعة الانتشار لوجوده خارج نطاق الهدف. **ويصنف في مراحله الأولى كخلل تقني مما يؤخر الاستجابة ويضاعف الخسائر.**

شكل رقم (٥)

هجوم سيبراني (Notpetya) على شركة (Maersk) تضررت منه فروع كثيرة للشركة ٢٠١٧

13. https://observablehq.com/@massonn-js-ws/malware-notpetya-attack-on-maersk-in-2017-incident

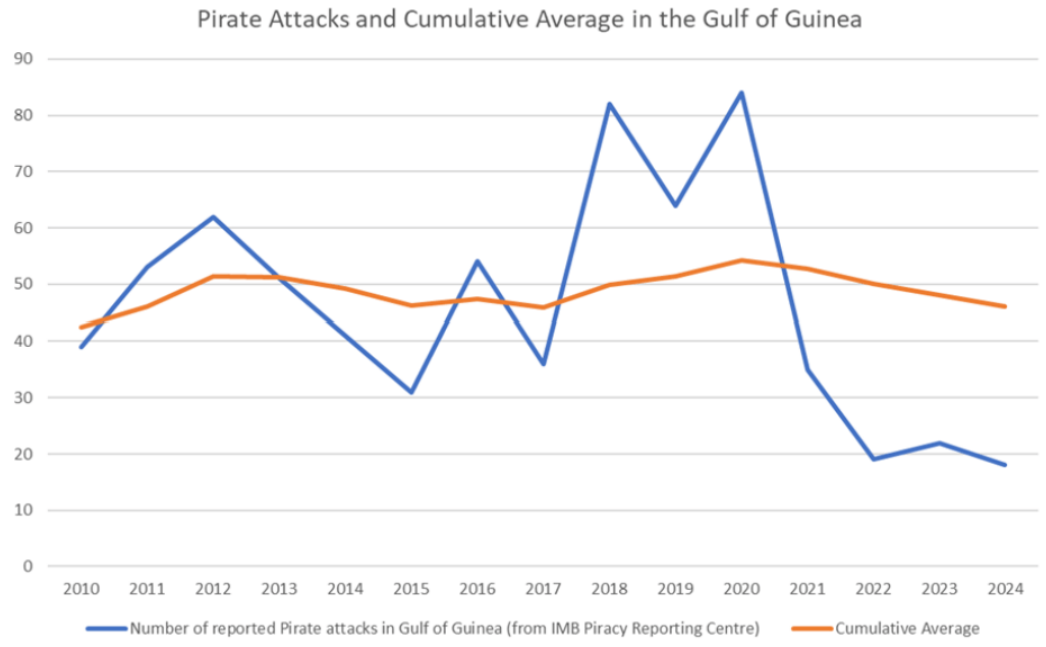
٤,٣ الجهات الفاعلة.

- **الدول.**

تُعد الدول فاعلاً رئيسياً في التهديدات البحرية غير التقليدية وذلك لما تملكه من موارد سيادية وقدرات تقنية وعسكرية وأدوات قانونية ودبلوماسية، تمكنها من التأثير في المجال البحري دون اللجوء إلى مواجهة مباشرة. وتوظف بعض الدول مقاربات هجينة تشمل أدوات سياسية واقتصادية وسيبرانية، إلى جانب عمليات بحرية محدودة أو غير معلنة وتستهدف عناصر من البنية التحتية البحرية الحرجة مثل الموانئ وكابلات الاتصالات والمناطق الحرجة لتقاطع لتلك الكابلات ومنشآت الطاقة. تُدار هذه الأنشطة ضمن أُطر تتسم بالغموض وهذا مما يُعقد عمليات الاسناد القانوني والسياسي. هذا النمط من السلوك يحقق اهداف استراتيجية تدريجية مثل التأثير في حرية الملاحة أو تعديل موازين النفوذ البحري.

- **الجماعات غير الحكومية.**

تعتبر الجماعات غير الحكومية من الفاعلين المؤثرين في التهديدات غير التقليدية وبالذات في المناطق الساحلية ذات الهشاشة العالية (الساحل الغربي لليمن وخليج غينيا **شكل رقم (٦)**. أو المناطق المتنازع عليها أو تلك التي ضعيفة الحوكمة. تستفيد هذه الجماعات من الانتشار الواسع للتقنيات منخفضة التكلفة. مثل المنصات غير المأهولة أو القدرات السيبرانية المحدودة والتي يتيح لها تنفيذ أنشطة تهديدية تستهدف الملاحة البحرية أو الموانئ أو سفن الشحن أو البنية التحتية البحرية للطاقة. وقد تعمل هذه الجماعات بشكل مستقل أو في إطار علاقات غير مباشرة أو أدوات لأطراف دولية، وهذا يعقد عملية الاسناد والاستجابة. وأهمية هذه الجماعات هو في قدرتها على احداث اضطرابات تشغيلية واقتصادية ذات اثر عالي وعابر للحدود رغم الموارد المحدودة.



شكل رقم (٦) هجمات الجماعات غير الحكومية في خليج غينيا الفترة (٢٠١٠-٢٠٢٤)

- **القراصنة السيبرانيون.**

القراصنة السيبرانيون هم من أكثر الفاعلين تأثيراً في التهديدات البحرية غير التقليدية، وذلك نظراً لاعتماد المجال البحري بشكل متزايد على الأنظمة الرقمية في تشغيل السفن والموانئ الذكية وسلاسل الامداد وأنظمة الملاحة والاتصالات. وهذه الأنشطة تستهدف البنى الرقمية البحرية عبر اختراق أنظمة تقنية المعلومات أو الانظمة التشغيلية ومن خلال طرف ثالث او نقاط ضعف في سلاسل الامداد التقنية. هذا النمط يتصف بصعوبة الاسناد والطابع العابر للحدود وانخفاض كلفة التهديد مقارنة بالأثر المحتمل. وهذه الأنشطة تتم بدوافع إجرامية، وتكمن أهميتها في قدرتها على تعطيل وظائف بحرية حيوية دون وجود مادي مباشر.

- **الشركات العابرة للحدود.**

تمثل الشركات العابرة للحدود فاعلاً غير تقيدي ولها دور مركب في البيئة الأمنية البحرية وذلك بحكم سيطرتها أو مشاركتها في تشغيل عناصر أساسية من البنية التحتية البحرية الحرجة مثل الموانئ وكابلات الاتصالات وسلاسل الشحن والطاقة. وأمنيا فإن هذه الشركات ليست مصدر تهديد مباشر بالضرورة، لكنها تتحول إلى عنصر مؤثر في منظومة التهديدات نتيجة قرارات تشغيلية أو استثمارية أ، تفاوت في طبقات ومستويات الحماية السيبرانية، كما يمكن استغلالها كمقاط دخول غير مباشرة في الهجمات السيبرانية أو الهجينة. وتبرز أهميتها التحليلية في طبعها العابر للسيادة الوطنية. وذلك يخلق فجوات حوكمة وتحديات تنسيقية بين الدول والقطاع الخاص في تأمين المجال البحري وإدارة مخاطر غير تقليدية.

٤,٤ المناطق البحرية الأكثر تهديداً.

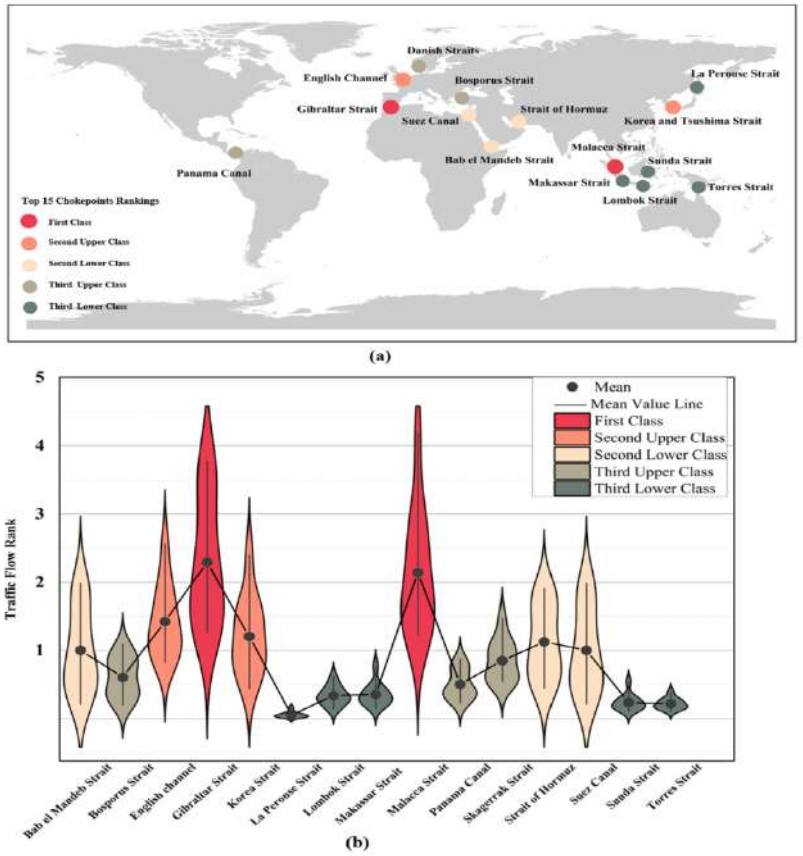
التهديدات البحرية لا تتوزع بصورة متساوية عبر المحيطات والبحار، بل ترتكز بدرجات متفاوتة في مناطق ذات قيمة استراتيجية وتشغيلية عالية مما يجعلها أكثر عرضة للتهديدات. هذه المناطق تعتبر نقاط ارتكاز حيوية للملاحة وتدفقات التجارة والطاقة والبيانات. وهذه المناطق :

- **الممرات البحرية الاستراتيجية. (Strategic Maritime Routes).**

مسارات بحرية واسعة نسبيا تمتد عبر مسافات طويلة وتربط بين مناطق انتاج ومناطق استهلاك او مراكز اقتصادية وجيوسياسية كبرى والتهديدات فيها تؤثر على كفاءة وسرعة وتكلفة النقل لكن لا يؤدي ذلك الى شلل كامل في سلاسل الامداد. وتعد من أكثر المناطق البحرية تعرضاً للتهديد وذلك بدورها الحيوي في ربط سلاسل الامداد العالمية، وتعتبر شريان حركة رئيسي للاقتصاد الدولي. وهو ما يجعل أي اضطراب فيها له آثار قوية. والتهديدات التي تستهدفها تتمثل في اعمال تخريبية وهجمات سيبرانية وضغوط سياسية وأمنية يتم تنفيذها في إطار المنطقة الرمادية.

- **نقاط الاختناق البحرية. (Maritime Chokepoints).**

مواقع بحرية ضيقة ومحددة جغرافيا، تُجبر حركة الملاحة على المرور عبرها دون بدائل عملية وقريبة وحساسيتها شديدة لأي اضطراب. تُصنّف بأنها بُؤر عالية الحساسية في منظومة الأمن البحري وذلك لأنه يرتكز فيها حجم كبير من الحركة الملاحية ضمن نطاق جغرافي ضيق، وهو ما يضاعف قابليتها للتأثر بالتهديدات غير التقليدية. ويؤدي استهداف نقاط الاختناق الى نتائج استراتيجية غير متناسبة مع حجم الفعل. مما يجعلها أدوات ضغط فعالة في التنافس البحري المعاصر. وأي تعطيل فيها يؤدي الى شلل فوري في تدفقات الطاقة والتجارة. **شكل رقم** (٧).



شكل توضيحي يبين ١٥ نقطة اختناق استراتيجية ... (b) تصنيف نقاط الاختناق استراتيجيا حسب حركة الملاحة البحرية.

شكل رقم (٧)

- **البيانات عالية الاعتماد على الرقمنة.**

تعتمد البنية التحتية البحرية الحديثة بصورة متزايدة على الأنظمة الرقمية في تشغيل عناصر حيوية مثل الملاحة البحرية والاتصالات وإدارة الحركة وربط سلاسل الامداد بالمنظومات اللوجستية والاقتصادية العالمية. وهو ما جعل البيانات بُعداً تشغيلياً حاسماً ومركز ثقل جديد في الأمن البحري. وقد أفرزت هذه الرقمنة العميقة قابلية عالية للاستهداف، إذ ان تعطيل الأنظمة الرقمية أو تدفقات البيانات يمكن أن يُحدث شللاً تشغيلياً واسعاً دون حضور مادي مباشر. وتبرز هنا أهمية كابلات الاتصالات البحرية والتي تنقل نحو (٩٩٪)[١٤] من حركة البيانات العالمية، وتمر عبر مناطق بحرية تُعرف اصطلاحاً ب(**المناطق الحرجة لتقاطع الكابلات البحرية Critical Submarine Cable Convergence Zone**). ويؤدي تداخل البنية المادية للكابلات مع الأنظمة الرقمية الساحلية إلى تضخيم المخاطر السيبرانية والهجينة، بحيث تتجاوز آثار أي اضطراب في المجال البحري لتطال منظومات الدولة الحساسة، والسيادة الرقمية واستقرار الاقتصاد الرقمي العالمي. وهو ما يُكرس هذه المناطق بوصفها مراكز ثقل استراتيجية في الأمن البحري المعاصر.

١٤. https://blog.telegeography.com/cybersecurity-submarine-cable-systems

التهديدات السيبرانية تُؤثر على عناصر القوى الوطنية. وذلك من خلال المخاطر التي تستهدف وظائف الدولة الحيوية ومنظوماتها التشغيلية بما يؤدي إلى ضعف ووهن القدرة الفعلية على السيطرة والحوكمة والاستجابة، حتى مع بقاء عناصر القوة التقليدية قائم شكليا.

٥.١ مفهوم القوى الوطنية في المجال البحري.

مفهوم القوى الوطنية في المجال البحري هو القدرات والموارد التي تمكن الدولة من تحقيق السيادة البحرية على مجالها البحري وضمان استمرارية وظائفها الحيوية. ويشمل ذلك تأمين الملاحة وحماية البُنى التحتية البحرية الحرجة، وإدارة سلاسل الامداد، وضمان أمن البيانات والاتصالات عبر الكابلات البحرية في مواجهة التهديدات التقليدية والسيبرانية والهجينة. ليشمل ليس فقط السيطرة الإقليمية ولكن أيضاً السيطرة الوظيفية. حيث تقاس فاعلية القوى الوطنية بقدرة الدولة على التكامل المؤسسي وبناء المرونة السيبرانية والصمود والتعافي في ظل بيئة بحرية معقدة وذات مستويات متعددة.

٥,٢ تأثير التهديدات السيبرانية البحرية على:

- **القوة العسكرية البحرية.**

تؤثر التهديدات السيبرانية على القوة العسكرية البحرية وذلك عبر استهداف منظومات القيادة والسيطرة والملاحة والاستشعار التي تقوم عليها العمليات البحرية الحديثة، وذلك يؤدي إلى تقويض الوعي البحري وإرباك صنع القرار على المستوى العملياتي لكي لا يصل إلى مواجهه عسكرية مباشرة، ويحد هذا النمط من التهديد من فعالية الردع التقليدي، ويحوّل التفوق التقني إلى نقطة ضعف محتملة في بيئات تشغيلية عالية الرقمنة.

لم تعد فعالية القوة البحرية تُقاس بحجم الأسطول أو التسليح فقط، بل بمدى اندماج الأمن السيبراني في العقيدة البحرية، وقدرة المنظومة العسكرية على الصمود واستمرارية القيادة والسيطرة، والتكامل بين الأبعاد العملياتية والتقنية في مواجهة التهديدات غير التقليدية.

- **القوة الاقتصادية (الشحن – التجارة – الطاقة).**

تؤثر التهديدات السيبرانية بصورة مباشرة في القوة الاقتصادية للدولة عبر استهداف المنظومات الرقمية التي تقوم عليها أنشطة الشحن البحري والتجارة الدولية وتدفقات الطاقة. ويؤدي تعطيل أنظمة إدارة الموانئ وسلاسل الامداد المؤتمتة، وأنظمة تتبع السفن والطاقة إلى ارباك حركة التجارة ورفع تكاليف النقل والتأمين وتعطيل تدفقات النفط والغاز دون الحاجة إلى استهداف مباشر.

هذا النمط من التهديد يقوض الثقة في البنية التحتية الاقتصادية البحرية، ويحوّل الاعتماد الرقمي إلى مصدر هشاشة استراتيجي، ويحد من قدرة الدولة على ضمان الاستقرار الاقتصادي واستمرار التدفقات التجارية والطاقة. لم تعد القوة الاقتصادية البحرية تقاس بحجم التجارة أو الطاقة بل بقدرة المنظومات اللوجستية ومنظومات الطاقة على الصمود السيبراني، والتعافي السريع والتكامل بين الأمن الاقتصادي والأمن البحري.

- **الأمن الوطني.**

التهديدات السيبرانية لها تأثير مباشر على الأمن الوطني عبر استهداف الوظائف الحيوية للدولة ومنظوماتها التشغيلية. وهذا يحد من قدرتها على التحكم والاستجابة وضمان الاستمرارية دون مواجهة عسكرية مباشرة. ويمتد أثرها ليشمل مكونات القوى

الوطنية العسكرية والاقتصادية والسياسية، وذلك من خلال تعطيل أنظمة القيادة والسيطرة وسلاسل الامداد والطاقة. كما أن طابع التهديدات المتمثل في كونه عابر للحدود يُعقِّد أدوات الاسناد والردع.

- **السمعة الدولية للدولة.**

تؤثر التهديدات في السمعة الدولية للدولة من خلال تقوّيض الثقة في قدرتها على حماية بنيتها التحتية البحرية الحيوية وكذلك المحافظة على السيادة الرقمية. ويؤدي تكرار الحوادث السيبرانية أو ضعف الاستجابة لها الى الاضرار بمصداقية الدولة كشريك اقتصادي وأمني موثوق. وانعكاس ذلك على تصنيفات المخاطر وجاذبية الاستثمار ومستوى التعاون الدولي والإقليمي. لذلك فإن السمعة الدولية الجيدة هي الامتداد الطبيعي للأمن الوطني المستقر. حيث يعد الصمود السيبراني وإدارة الأزمات الرقمية عنصراً حاسماً في الحفاظ على المكانة الدولية للدولة في بيئة أمنية رقمية عالية الترابط.

٥,٣ دور التحول الرقمي في تعزيز أو اضعاف القوة الوطنية.

يؤدي التحول الرقمي دوراً مركزياً في إعادة تشكيل القوى الوطنية في المجال البحري وذلك لكونه مضاعفا

للكفاءة والسيطرة الوظيفية من جهة، ومصدراً محتملاً للهشاشة من جهة أخرى. فعندما يُدمج ضمن اطار استراتيجي محكوم فإنه يعزز قدرة الدولة على إدارة الملاحة، وتشغيل الموانئ، وتأمين سلاسل الإمداد البحرية، بما يدعم الأمن البحري والسيادة الرقمية. غير أن التحول الرقمي غير المؤمن ينقل نقاط الضعف إلى الطبقة السيبرانية، ويقوض السيطرة الفعلية، مما يجعل السيادة البحرية مرهونة بقدرة الدولة على تحقيق صمود وسيادة رقمية مستدامة.

٥,٤ العنصر البشري كعنصر قوة أو ضعف.

العنصر البشري هو عنصر حاسم ضمن عناصر القوى الوطنية في بيئة التهديدات السيبرانية. إذ يمكن أن يمثل مصدر قوة أو نقطة ضعف بنيوية وذلك اعتمادا على مستوى الوعي والكفاءة والانضباط المؤسسي. فعلى الرغم من تطور التقنيات الرقمية، تظل الأخطاء البشرية وضعف الثقافة السيبرانية وسوء إدارة الصلاحيات من أبرز مداخل الاختراق السيبراني. وفي المقابل يُسهِم الاستثمار في رأس المال البشري وبناء القدرات السيبرانية وتعزيز الوعي المؤسسي في رفع مرونة الدولة السيبرانية وقدرتها على الصمود والاستجابة. وهو ما يجعل العنصر البشري مكون مركزي في الأمن الوطني والسيادة الرقمية وليس فقط مجرد عنصر داعم للتقنية.

٦.١ الامن البحري في الاستراتيجية الوطنية.

التحول السريع في الأمن البحري السيبراني أدّى إلى إعادة تشكيل البيئة الاستراتيجية البحرية. وذلك لأن المجال البحري لم يعد مجالاً مادياً تحكمه القوة البحرية التقليدية فقط. بل أصبح فضاء مركب ومُعقّد تتداخل فيه الأبعاد السيبرانية والاقتصادية والأمنية واللوجستية. هذا التحول نقل نعه مراكز الثقل التهديدية من استهداف المناطق الحيوية والمنصات البحرية إلى استهداف الوظائف البحرية الحيوية، مثل الملاحة، وإدارة الموانئ، وسلاسل الامداد، والبُنى التحتية البحرية الحرجة وكيابل الاتصالات البحرية.

وهذه التهديدات السيبرانية والهجينة أحدثت آثار استراتيجية تفوق حجمها المادي، من خلال تعطيل القيادة والسيطرة أو إرباك الملاحة في الممرات البحرية الحيوية ونقاط الاختناق البحرية المرتبطة بالطاقة والتجارة الدولية. ونتيجة لذلك لم تعد القوة البحرية تقاس بالقدرات القتالية فقط، بل بقدرة الدولة على حماية الأنظمة والمعلومات والبُنى التحتية البحرية الرقمية. **مما جعل الأمن البحري السيبراني مكوناً بنيوياً من مكونات الأمن الوطني واحتياجا رئيسيا لاستدامة السيادة والمصالح الوطنية.**

٦.٢ التوسع في مفهوم الأمن البحري خارج حدود المياه الإقليمية للدولة.

ان التحول في الأمن البحري السيبراني أسهم في إعادة تشكيل نطاق الأمن البحري بحيث لم يعد مقصوراً على الحدود الجغرافية للدولة الساحلية، بل أصبح مرتبطاً بفضاء وظيفي عابر للحدود تحكمه تدفقات البيانات والبُنى التحتية البحرية الرقمية وفي مقدمتها الكابلات البحرية. هذا التوسع له سند معياري في اتفاقية الأمم المتحدة لقانون البحار لاسيما للمواد (١١٢ إلى ١١٥) المتعلقة بحرية أعالي البحار ونظام حماية الكابلات البحرية. ونتيجة لذلك، باتت الدول معنية بأمن منظومات حيوية قد تقع خارج ولايتها الإقليمية المباشرة، لكنها تمارس أثر مباشر على أمنها الوطني واستمرارية وظائفها الاقتصادية. ويعكس هذا الواقع **انتقال مفهوم الأمن البحري من منطق السيادة الإقليمية إلى منطق السيادة الوظيفية**. حيث أصبحت حماية الكابلات البحرية والأنظمة الرقمية شرطاً تشغيلياً لاستمرارية التجارة والطاقة والاتصالات، وركيزة بنيوية ضمن منظومة الأمن الوطني المعاصر حتى عندما تقع هذّ البُنى خارج المياه الإقليمية للدولة.

٦.٣ الأمن السيبراني البحري كعامل ردع.

إن توظيف الأمن البحري السيبراني كعامل ردع يتم من خلال تحويله من إطار الحماية التقنية الرقمية إلى إطار الحرمان الوظيفي للعدو. وهذا يقلص قدرة العدو على تحقيق مكاسبه التشغيلية في المجال البحري، ويتحقق ذلك من خلال التحصينات التقنية للمنصات البحرية وأنظمة الموانئ والكابلات البحرية، وذلك لأنها تعتبر مراكز ثقل وظيفية ولضمان استمرارية الملاحة وسلاسل الامداد حتى في حال التعرض لهجوم. وبهذا المعنى، يصبح الأمن السيبراني مكوناً بنيوياً في منظومة الردع البحري الحديثة، وهو قائم على تقليص الجدوى الاستراتيجية لهجوم العدو.

٦.٤ المرونة السيبرانية البحرية (Maritime Cyber Resilience).

المرونة السيبرانية البحرية لم تعد مقتصرة على منع الهجمات أو تحييدها. بل انتقل الى بناء قدرة تعتمد على الصمود والتعافي وضمان الاستمرارية، ويتم ذلك في بيئة بحرية رقمية عالية الترابط. أدى الاعتماد المتزايد على الأنظمة الرقمية في المجال البحري إلى كون التعطيل السيبراني أمراً واقع الحدوث، وهذا الذي

أعاد توجيه التفكير الاستراتيجي من منطق الحماية الكاملة إلى منطق إدارة التعرض للمخاطر

- **الصمود (Endurance).**

المرونة السيبرانية هناك حالتين تتمثل لها وهي إما الصمود السيبراني (**Cyber Endurance**) وهو القدرة على امتصاص الهجوم وتقليص أثره المباشر على الوظائف البحرية الحيوية. أو المقاومة السيبرانية (**Cyber Resistance**) وهي قدرة الأنظمة البحرية الرقمية على منع أو تقليل احتمالية نجاح الهجمات السيبرانية للعدو من خلال التحصين التقني وتقليل الثغرات ومنع الاختراق قدر الامكان.

- **التعافي (Recovery).**

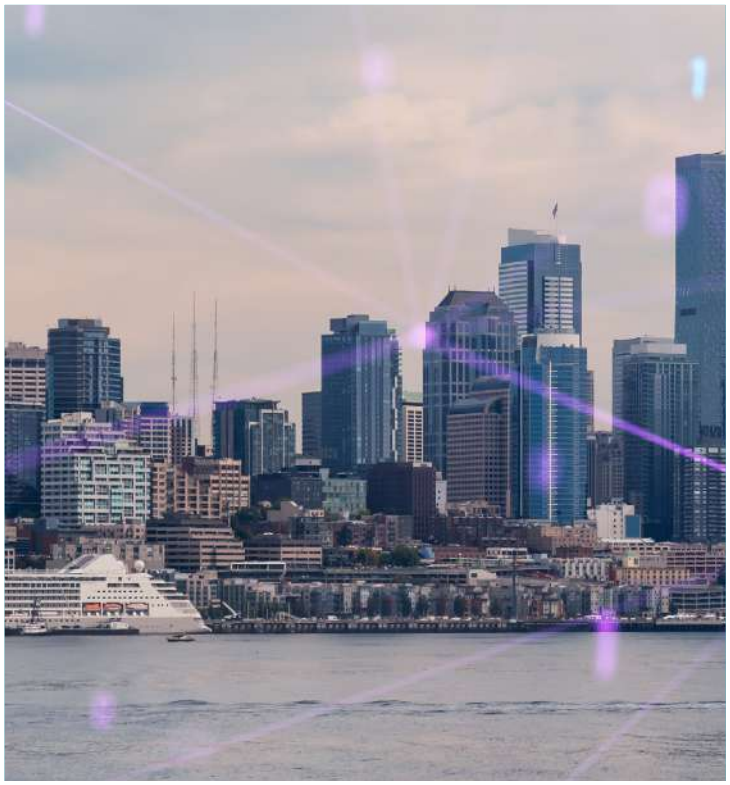
التعافي هو قدرة المنظومة البحرية على استعادة الوظائف البحرية الحيوية والأنظمة الرقمية والتشغيلية بعد أي الحوادث السيبرانية ضمن إطار زمني مقبول وبطريقة تمنع تكرار المشكلة.

- **الاستمرارية (Continuity).**

هي قدرة المنظومة البحرية على الحفاظ على الحد الأدنى من الوظائف البحرية الحيوية أثناء الاضطرابات السيبرانية، وذلك عبر تشغيل بدائل وإجراءات تعويضية وبديلة تضمن التدفقات الأساسية للملاحة والموانئ وسلاسل الإمداد. وتكمن أهميتها إستراتيجيا في كون توقف هذه الوظائف ينتج عنه ضغط اقتصادي وسياسي عالي. إن الاستمرارية تُعد بُعداً مركزياً للمرونة السيبرانية البحرية.

٦.٥ التحولات في العقيدة البحرية نتيجة التهديدات السيبرانية.

ان العقيدة البحرية كانت ترتكز على التفوق المادي والسيطرة عبر الوحدات القتالية بوصفهما الأساس لتحقيق السيطرة البحرية وحماية المصالح الوطنية. ولا تشهد العقائد البحرية تحولاً جوهرياً إلا عند حدوث تغير بنيوي في طبيعة البيئة العملياتية، أو انتقال في مراكز الثقل على المستويين الاستراتيجي أو العملياتي، أو إعادة تشكيل العلاقة بين القوة التقليدية والوظيفة التي المفترض يؤديها. غير أن التحول المتسارع في الأمن السيبراني البحري أفضى إلى تغيير عميق في هذه المحددات، حيث تغيرت الطبيعة العملياتية من طابعها المادي إلى الرقمي، وأعيد تعريف مراكز الثقل. كما تم فصل القوة المادية عن قدرتها على تنفيذ الوظيفة المحددة بسبب التدخل السيبراني. إلى جانب ذلك، أسهم الطابع العابر للحدود والذي هو أحد سمات التهديدات السيبرانية البحرية في توسيع نطاق العقيدة البحرية ليشمل أدوار غير عسكرية.



٧.١ الامن البحري السيبراني في العلاقات الدولية.

يُنظر للأمن البحري السيبراني في العلاقات الدولية بوصفة امتداداً مباشراً لتحوّل البحر من مجال مادي تقليدي إلى فضاء هجين تتقاطع فيه المصالح السيادية والاقتصادية والرقمية. إن اعتماد الملاحة والموانئ وسلاسل الامداد البحرية على الأنظمة الرقمية أعاد تعريف مصادر التهديد ومراكز الثقل الاستراتيجي. وأصبحت الدول ملزمة بإدماج البُعد السيبراني ضمن مفاهيم الردع وإدارة المخاطر. ويتسم الموقف الدولي بالتدرج لا بالتوافق الكامل. وهناك مقاربات حوكمية ومعيارية عبر أُطُر حكومية وهيئات عالمية مثل الأمم المتحدة والمنظمة البحرية الدولية وكذلك تحالفات عالمية مثل حلف شمال الأطلسي.

٧,٢ ردود الفعل الدولية على التهديدات السيبرانية البحرية.

تتسم ردود الفعل الدولية على التهديدات السيبرانية بطابع تراكمي وتدريجي. يعكس حداثة المجال وتباين إدراك الدول لمصادر الخطر وحدوده. لقد انتقلت الاستجابات من التركيز على الحماية التقنية وبناء القدرات الوطنية الرقمية إلى تبنّي مقاربات حكومية ومعيارية هدفها الأساسي ضبط السلوك السيبراني. وهذا التوجه يتم صياغته عبر أطر دولية تقودها الأمم المتحدة وتحالفات مثل حلف شمال الأطلسي، ومع ذلك لاتزال هناك فجوه بين التوافق السياسي الدولي وغياب آليات تنفيذ ملزمة للأطراف الفاعلة، كما أن هناك استمرار في الخلافات حول الإسناد والسيادة وحدود الردع السيبراني.

٧,٣ دور المنظمات الدولية.

يُعد الأمن البحري السيبراني مجالاً مركباً ومتعدد الوظائف، تتداخل فيه الأبعاد التقنية والتنظيمية والقانونية والأمنية والاقتصادية، إلى جانب متطلبات بناء القدرات المؤسسية والبشرية. وهذا يجعله عابر للحدود نتيجة اعتماد الأنشطة البحرية الرقمية على شبكات وبُنى تحتية تتجاوز نطاق السيادة الإقليمية للدول. هذا التداخل جعل مجال الأمن البحري السيبراني مُجزأ وظيفياً، وتتوزع بموجبه الأدوار والمسؤوليات بين هيئات حكومية متعددة وليس منظومة قيادة موحدة تضبط الحوكمة أو ترسم الإجراءات التنفيذية. وبناء عليه لا يوجد كيان مستقل مخصص للأمن البحري السيبراني ضمن منظومة الأمم المتحدة. بل تتولاه هيئات أممية تمارس أدواراً مباشرة وغير مباشرة عبر فرق خبراء حكوميين ومجموعات عمل مفتوحة، تُعنى بتطوير الأُطُر القانونية والمعيارية، وتنسيق التعاون وبناء القدرات، مع التركيز على مبادئ السلوك السيبراني المسؤول واحترام السيادة الرقمية والعمل على إجراءات بناء الثقة، دون الانخراط في التفاصيل التشغيلية. وجميع هذه الهيئات الأممية تفتقر للسلطة التنفيذية المباشرة.

- **المنظمة البحرية الدولية (IMO).**

هي أحد الوكالات التابعة للأمم المتحدة (١٧٥ دولة عضو)، ويتمثل دورها في دمج البُعد السيبراني ضمن منظومة السلامة البحرية، وذلك عبر توجيهات إدارة المخاطر السيبرانية (**MCRM**) للسفن والموانئ. والمنظمة تتعامل مع الهجمات السيبرانية كأحداث قد تؤدي إلى حوادث بحرية، أو فقدان السيطرة على أنظمة الملاحة، أو تعطّل العمليات في السفن والموانئ، لا كمسألة صراع ونفوذ استراتيجي .مهمتها العمل على تقليل احتمالات الحوادث البحرية الناتجة عن الاختراق الرقمي والهجمات السيبرانية، من خلال وضع اتفاقيات ومعايير دولية.

- **الإتحاد الدولي للاتصالات (ITU).**

أحد الوكالات المتخصصة والتابعة للأمم المتحدة (١٩٣ دولة عضو)، ويُسهم الاتحاد في تعزيز أمن البنية التحتية الرقمية العابرة للحدود والتي يرتكز عليها الأمن البحري السيبراني، وذلك من خلال وضع معايير تقنية ودعم

الجاهزية السيبرانية، وبناء القدرات. يكون التركيز على مرونة الشبكات أكثر من الأبعاد الأمنية أو السياسية. هذه المنظومة تعمل كجهة تنظيمية – تقنية لها معايير ثابتة وتؤثر بصورة غير مباشرة في الأمن البحري السيبراني عبر حماية واستدامة البنية الرقمية العالمية. وثيقة مشتركة بين (**IMO**) و (**ITU**) تتناول حماية أنظمة الاتصالات البحرية.[١٥]

- **اللجنة الدولية لحماية الكابلات البحرية (ICPC).**

منظمة دولية غير حكومية وغير ربحية (١٩٠اجهة عضو)، ذات طابع فني – تنسيقي، يُعنى بحماية كابلات الاتصالات البحرية وضمان استمرارها على المستوى العالمي. لاتُعد منظمة دولية حكومية بالمعنى القانوني للأمم المتحدة، لكنها تُصنّف كمنظمة دولية متخصصة بحكم عضويتها العابرة للحدود ودورها العالمي.

- **التحالفات العسكرية.**

تتعامل التحالفات العسكرية مع الأمن السيبراني بما فيه البُعد البحري باعتباره مجال عملياتي وأداة ضمن منظومة الردع والدفاع الجماعي. وينصب تركيز التحالفات على رفع الجاهزية العملياتية لقوات التحالف عبر التمارين والمحاكاة التشغيلية، وتعزيز تبادل المعلومات الاستخبارية حول التهديدات، وسلاسل الإمداد التقنية المرتبطة بالأنظمة البحرية. كما تطور هذه التحالفات استراتيجياتها وعقائدها المشتركة. ان هذه التحالفات تساعد في تطوير عقائد استجابة تربط الحوادث السيبرانية بتداعيات ميدانية مباشرة. وهذا هو الاختلاف الجوهري بينها وبين المنظمات الدولية. حيث إن التحالفات تنفذ خطة الأمن السيبراني، بينما المنظمات الدولية تُحكّم وتنظم الأمن السيبراني.

- **الأطر متعددة الأطراف.**

الأطر متعددة الأطراف تتناول الأمن السيبراني البحري من زاوية الحوكمة والمعيارية الدولية، وليست من منطق الردع أو المواجهة. وهذه الأطر تحكم وتنسق وتبني قدرات ولا تنفذ عمليات، وتأثيرها على الأمن البحري السيبراني تأثير معياري وغير مباشر. وهذه الأطر تتمثل في:

(أ أ). أُطر السلوك والمعايير(Norms & Rules of Behavior).

يتكون من إطارين، الإطار السياسي المعيار للسلوك المسؤول وبناء الثقة، وكذلك الإطار القانوني لتطبيق القانون الدولي على الهجمات السيبرانية ذات الآثار البحرية، دون أي أدوار تنفيذية أو تشغيلية.

(ب ب). إجراءات بناء الثقة (CBMs).

تُعد إجراءات بناء الثقة السيبرانية التي تعمل على تطويرها منظمة الأمن والتعاون في أوروبا إطارا متعدد الأطراف يركز على الشفافية، وقنوات الاتصال بهدف تقليل المخاطر وسوء التقدير والتصعيد أثناء الحوادث السيبرانية. وذلك دون أي صلاحيات تنفيذية أو تشغيلية.

(ج ج). بناء القدرات السيبرانية (Cyber Capacity Building).

تركز برامج بناء القدرات السيبرانية على رفع الجاهزية التقنية والرقمية للدول عبر التدريب، ونقل المعرفة، وتطوير الاستراتيجيات.

(د د). الأُطر القانونية.

توفر اتفاقية بودابست[١٦] إطار قانوني دولي لم كافحة الجرائم السيبرانية عبر توحيد التجريم، وتسهيل التعاون القضائي، وتبادل الأدلة، بما يشمل الهجمات السيبرانية التي تستهدف الموانئ وسلاسل الإمداد البحرية. ويتم ذلك دون معالجة أبعاد الردع أو العمليات الأمنية.

١٥. https://www.itu.int/harmful-interference-to-rnss/wp-content/uploads/sites/74/2025/07/Joint-Declaration-ITU-ICAO-IMO-on-RNSS1303_DBM.pdf

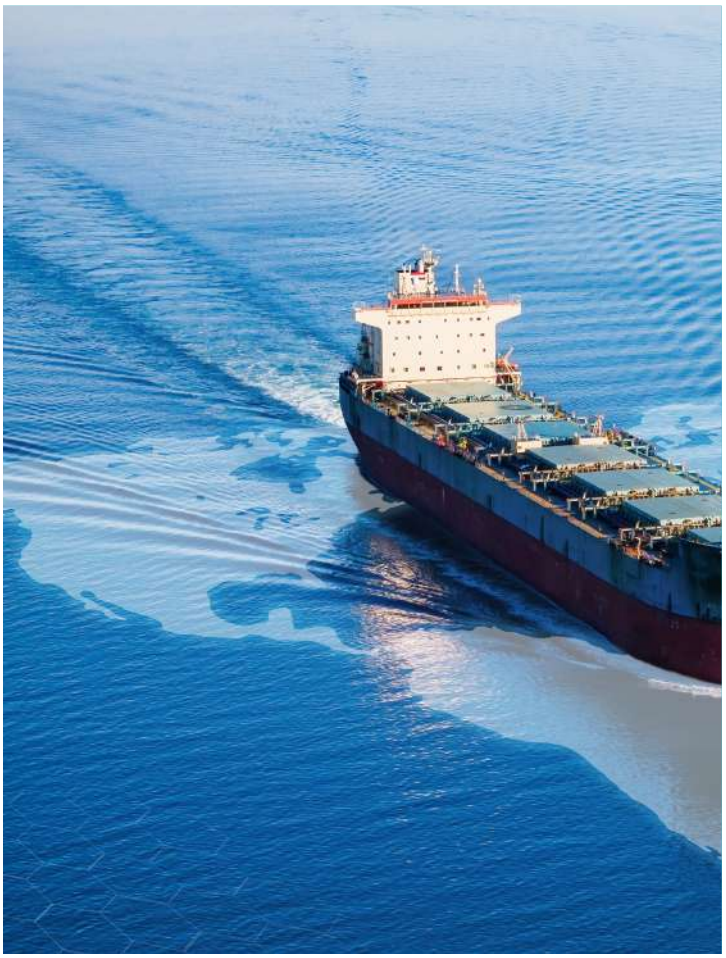
١٦. https://www.coe.int/en/web/cybercrime/the-budapest-convention

٧,٤ الحوكمة الدولية للأمن السيبراني البحري.

تتسم الحوكمة الدولية للأمن السيبراني بطابع شبكي متعدد الطبقات، يعكس الطبيعة العابرة للحدود للفضاء الرقمي وتداخل وظائفه التقنية والقانونية والأمنية والاقتصادية. ولا ترتكز هذه الحوكمة على سلطة مركزية موحدة أو مرجعية ثابتة، بل تقوم على منظومة متداخلة من القواعد والمعايير والمبادئ والإجراءات التي تطورها الدول ضمن أطر متعددة الأطراف، يأتي في مقدمتها الأمم المتحدة. وذلك عبر مجموعات خبراء حكوميين ومنصات حوار مفتوحة. وتركز هذه الأطر على ترسيخ مبادئ السلوك المسؤول، واحترام السيادة الرقمية، وحماية البُنى التحتية البحرية الحرجة، إلى جانب إجراءات بناء الثقة وتنسيق التعاون وبناء القدرات، مع الابتعاد المتعمد عن الأدوار التنفيذية والتشغيلية. هذا النموذج يعكس التوازن البنيوي بين الحفاظ على السيادة الرقمية للدول من جهة، والحاجة إلى إدارة مخاطر سيبرانية ذات آثار استراتيجية واقتصادية عابرة للحدود من جهة أخرى.

٧,٥ تعدد أصحاب المصلحة وتحديات التنسيق الدولي.

يتسم الأمن البحري السيبراني بتعدد واضح في أصحاب المصالح يشمل الدول، والهيئات التنظيمية، والتحالفات الأمنية، وشركات الشحن والموانئ، ومشغلي الاتصالات والكابلات، وشركات التأمين. هذا التعدد يُعقّد عملية التنسيق الدولي بسبب تباين الأولويات والولايات القانونية والقضائية، وتفاوت مستويات الجاهزية والمسؤولية. كما أن الطبيعة العابرة للحدود التي تتميز بها الأنشطة البحرية الرقمية تزيد من إشكاليات الاسناد، وتبادل المعلومات، وتوحيد إجراءات الاستجابة. وفي ظل عدم وجود سلطة مركزية، تعتمد الجهود الدولية على آليات توافقية معيارية وإجراءات بناء ثقة، وذلك يحقق شمولية سياسية لكنه يترك فجوه تنفيذية تعتبر التحدي الرئيسي أمام حوكمة فعّالة ومنسّقة.



ثامنا: الهندسة الدفاعية السيبرانية البحرية.

مع تسارع وتيرة الرقمنة في المجال البحري وتزايد تعقيد التهديدات السيبرانية ذات التأثيرات المادية المباشرة، لم تعد المقاربات الأمنية التقليدية قادرة على توفير مستوى الحماية المطلوب للأنظمة البحرية الحديثة. وقد أسهم هذا التحول في بروز توجه هندسي جديد يُعنى بتصميم وتأمين الأنظمة البحرية الرقمية من منظور دفاعي متكامل. يراعي خصوصيات البيئة البحرية وتشابك أنظمتها التشغيلية. ورغم أن مصطلح الهندسة الدفاعية السيبرانية البحرية لا يُعد مصطلحاً معتمداً أو متداولاً رسمياً في الأدبيات الأكاديمية أو الأُطر التنظيمية ، فإن المفهوم الذي يُعبّر عنه قائم ومُطبّق فعليا ضمن الدراسات والممارسات العلمية تحت مسميات متعددة تعكس جوهر التوجه ذاته. وفي هذا السياق يمكن النظر إلى مختلف الإجراءات الدفاعية السيبرانية البحرية المطبقة حاليا في المجال البحري بوصفها تندرج ضمن هذا الإطار الهندسي الدفاعي، والذي يهدف إلى تصميم وبناء وتأمين الأنظمة البحرية الرقمية في مواجهة التهديدات البحرية السيبرانية المتنامية. وعليه فإن استخدام هذا المصطلح يُعد صياغة تحليلية ومفهومية تهدف إلى تجميع ممارسات قائمة ومتفرقة ضمن إطار نظري واحد.

شكل توضيحي رقم (٨).

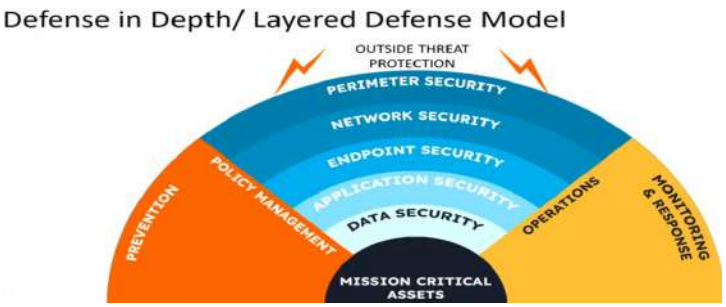
٨,١ مفهوم الهندسة الدفاعية السيبرانية البحرية.

تُظهر الأدبيات المرتبطة بالعلوم التطبيقية، لا سيما في مجالي الهندسة والأمن، أن وجود المفهوم لا يُقاس بالضرورة بمدى شيوع تسميته أو اعتماده رسميا، بقدر ما يُقاس بمدى تجسده العملي وتطبيقه الفعلي ضمن الأُطر التشغيلية والتنظيمية. وهو ينطبق على مفهوم الهندسة الدفاعية السيبرانية البحرية، الذي يُمارس عمليا ضمن عدد من المقاربات الهندسية والأمنية المعاصرة. وفي هذا السياق يمكن القول بأن مفهوم الهندسة الدفاعية السيبرانية البحرية بأنها إطار هندسي تطبيقي يهدف إلى تصميم وبناء معيارية أمنية متكاملة للأنظمة البحرية الرقمية، تشمل السفن والموانئ والبُنى التحتية البحرية الحرجة، والكابلات البحرية، بما يضمن تحقيق مستويات فعّالة من الوقاية والكشف والاستجابة والصمود والتعافي من التهديدات والهجمات البحرية السيبرانية في ظل بيئة بحرية تتسم بالتعقيد والديناميكية وتداخل الأبعاد التقنية والتشغيلية على مختلف الطبقات.

٨,٢ النماذج الدفاعية المستخدمة.

في ظل التحولات العميقة التي يشهدها المجال البحري بسبب الاعتماد المتزايد على الأنظمة الرقمية، برزت الحاجة إلى تطوير نماذج دفاعية متقدمة، تتجاوز الحلول التقنية الجزئية لضمان استمرار الوظائف البحرية الحيوية. ضمن هذا الإطار تتبلور النماذج الدفاعية المستخدمة في الأمن البحري السيبراني بوصفها منظومة متكاملة، وتقوم على الدمج بين الدفاع متعدد الطبقات، والأمن السيبراني بالتصميم، و حماية الأنظمة البحرية–الفيزيائية، وذلك لمعالجة طبيعة التهديدات المعاصرة.

- **الدفاع متعدد الطبقات. (Multi–Layered Defense).**



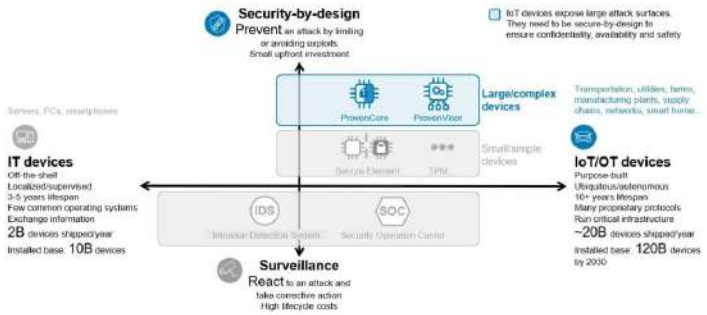
شكل رقم (٩). الدفاع متعدد الطبقات.

يعتمد هذا النموذج على توزيع وظائف الحماية وذلك عبر طبقات متدرجة تشمل الطبقة الفيزيائية، والرقمية، والتشغيلية، والبشرية. بما يضمن عدم اعتماد الأمن على نقطة فشل واحدة. وتتم عن طريق دمج أمن السفن والموانئ، وأنظمة الملاحة والتحكم، وشبكات الاتصالات، مع آليات رصد مبكر واستجابة مرحلية. والهدف من هذا النموذج من الدفاع ليس فقط منع الاختراق، بل احتواءه وتقليص أثره التشغيلي عند حدوثه بما يحافظ على استمرارية العمليات البحرية الحيوية.

- **شكل توضيحي رقم (٩).**

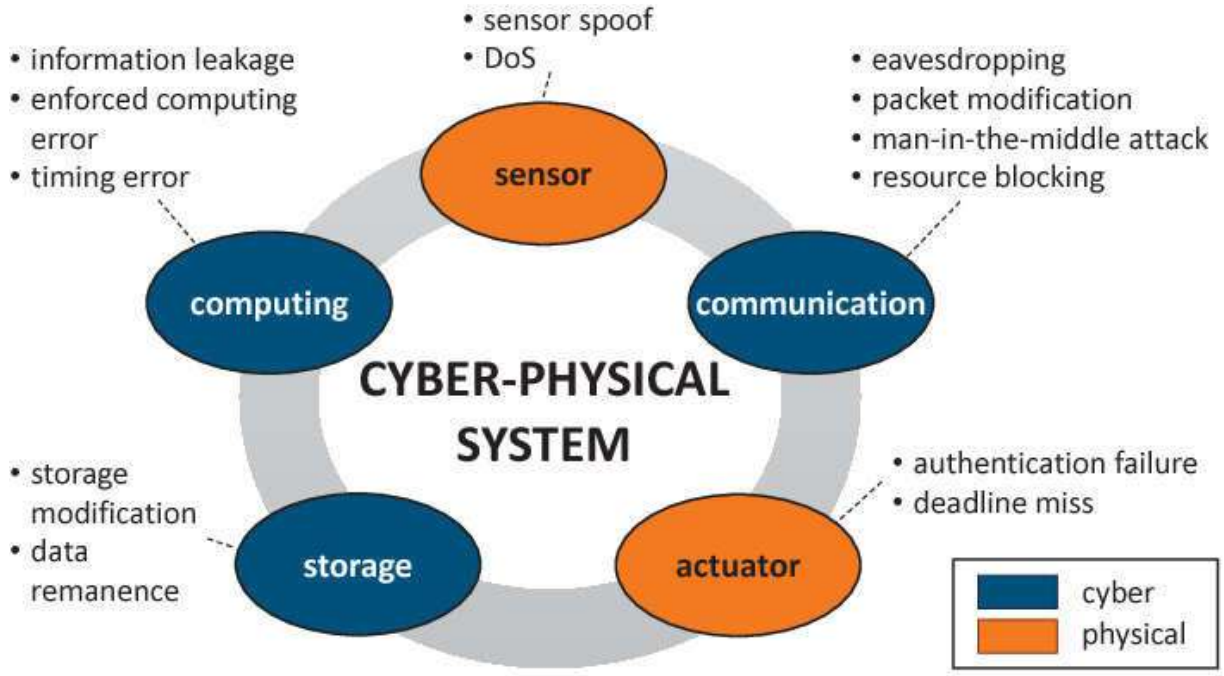
هناك عدة نماذج دولية يظهر فيها الدفاع متعدد الطبقات بشكل واضح مثل النموذج الأمريكي (**US Coast Guard / Department of Homeland Security**) وهو نموذج تشغيلي–أمني، يركز على الفيزيائي والتشغيلي أولا، ثم الرقمي والبشري كطبقات مساندة، أما نموذج (**European Union**) الأوربي فهو نموذج حوكمي–رقمي يركز على الرقمي والبشري. ويُؤطّر التشغيلي والفيزيائي دون إدارة مباشرة.

- **الامن السيبراني بالتصميم. (Cybersecurity by Design).**



يرتكز هذا النهج على إدماج متطلبات الأمن منذ المراحل الأولى لتصميم الأنظمة البحرية الرقمية، وذلك يشمل اعتماد معيارية آمنة افتراضياً، ومبدأ أقل صلاحيات، والفصل الوظيفي بين الأنظمة الحرجة. إضافة إلى اختبارات أمان منهجية قبل التشغيل في البيئة البحرية. هذا النموذج له أهمية مضاعفة نظراً لطول عمر المنصات البحرية وصعوبة تحديثها أثناء الخدمة. وهذا يجعل قرار التصميم المبكر حاسم في مستوى الصمود السيبراني على المدى الطويل . **شكل توضيحي رقم (١٠).**

النماذج الدولية التي يبرز فيها الأمن السيبراني بالتصميم بشكل خاص هو النموذج الأوربي (**EU Maritime Cybersecurity Architecture**) من خلال إدماج الأمن في تصميم الموانئ الذكية والسفن الجديدة. وكذلك النموذج الياباني (**Cyber–Physical System–Based Model**) حيث يُدمج الأمن ضمن تصميم الأنظمة السيبرانية–الفيزيائية منذ مرحلة الهندسة.



حماية الأنظمة السيبرانية–الفيزيائية. (Cyber–Physical System Protection)

شكل توضيحي رقم (١١).

تُعالج هذه المقاربة التداخل المباشر بين البرمجيات والمكونات الفيزيائية في السفن والموانئ .وذلك لأن أي هجوم سيبراني سوف يُحدث أمراً مادياً مباشراً على الملاحة وسلاسل الإمداد والسلامة. وتتم هذه الحماية عبر آليات تكاملية تشمل العزل الوظيفي مثل العزل بين **IT & OT**. والمراقبة السلوكية للأنظمة، وربط الأمن البحري السيبراني بإجراءات السلامة التشغيلية.

تعتبر هذه المقاربة جوهرية في المجال البحري، وذلك لأن الخلل الرقمي لا يظل افتراضيا بل قد يتحول سريعا إلى حادث ملاحيأو تعطيل إستراتيجي للبُنى التحتية البحرية الحرجة.

٨,٣ التنفيذ العملي للهندسة الدفاعية.

إن نموذج حماية الأنظمة السيبرانية–الفيزيائية تمثل جوهر النموذج الياباني (**Cyber–Physical System–Based Model**)، ونظرا لأن النموذج السنغافوري (**Maritime Cybersecurity Operation Center**) يعمل كمنصة تنفيذ وتشغيل ولا يضيف نموذج هندسي جديد. لذلك فهذا النموذج يدار تشغيلياً بشكل واضح لديهم عبر مراكز الرصد والاستجابة.

ومع هذا التكامل فإنه لا تفهم النماذج الدفاعية بوصفها أدوات تقنية منفصلة. بل كمنظومة هندسية – تشغيلية واحدة تعكس التحول البنيوي للأمن البحري في عصر الرقمنة والتهديدات الهجينة.

٨,٤ التنفيذ العملي للهندسة الدفاعية.

قصد بالتنفيذ العملي للهندسة الدفاعية السيبرانية البحرية هو تحويل الإطار المفاهيمي إلى منظومة متكاملة تُدمج فيه الحوكمة، والتصميم الهندسي، والضوابط التقنية، والإجراءات التشغيلية عبر دورة حياة السفن والموانئ. ويشمل ذلك إدماج المخاطر السيبرانية في أنظمة السلامة، وتحديد المسؤوليات المؤسسية وآليات صناعة القرار التشغيلي خلال الحوادث السيبرانية البحرية، وحصر الأصول الرقمية والتشغيلية والسيبرانية–الفيزيائية ذات التأثير المباشر على السلامة البحرية وتدفقات البيانات. ثم تطبيق العزل والتقسيم الطبقي بين أنظمة **IT** و **OT**. ويُستكمل التنفيذ عبر اعتماد مبدأ الأمن بالتصميم، الذي يقوم على ادماج الضوابط السيبرانية ضمن البنية الهندسية للأنظمة منذ مرحلة التصميم. وضوابط التشغيل والكشف والاستجابة. مع تحقق وامتثال دوري يضمن الاستدامة التشغيلية.

٨,٥ دور التكنولوجيا في تعزيز الدفاع البحري السيبراني.

تلعب التكنولوجيا دوراً محورياً في تعزيز مفهوم الهندسة الدفاعية السيبرانية البحرية من خلال تمكين الرصد اللحظي، وتحليل السلوك غير الطبيعي، وبناء استجابات تلقائية للتهديدات السيبرانية. وتُسهم تقنيات مثل الذكاء الصناعي، وتحليل البيانات الضخمة، وتقسيم الشبكات في رفع مستوى الصمود التشغيلي للسفن والموانئ. وتُؤكد أطر المنظمة البحرية الدولية **IMO** و المعهد الوطني للمعايير والتقنية **NIST** على توظيف التكنولوجيا بوصفها عنصراً بنيوياً في الوقاية والكشف والاستجابة للتهديدات البحرية السيبرانية.

لا تُعد الديبلوماسية السيبرانية البحرية مصطلحاً معتمداً أكاديمياً أو قانونياً ، بل تمثل إطاراً تحليلاً ناتج عن تداخل أدبيات الدبلوماسية السيبرانية مع دراسات الأمن البحر السيبراني. وأسهم الاعتماد المتزايد على الرقمنة في تشغيل الموانئ والسفن الذكية وأنظمة الملاحة والكابلات البحرية في إحداث تحول بنيوي في طبيعة المجال البحري، وهو ما نقل التهديدات السيبرانية من الفضاء الرقمي المجرد إلى صميم منظومة الأمن البحري العالمي. وفي هذا السياق لا تُمثل الدبلوماسية السيبرانية البحرية أمناً سيبرانياً تقنياً خالصاً ولا دبلوماسية بحرية تقليدية. بل تشكل طبقة تكاملية بين المجالين، وتشير التقارير المتخصصة تشير إلى تصاعد الهجمات السيبرانية على منظومة النقل البحري (**MTS**) وما يُصاحب ذلك من حاجة مُلِحّة إلى تعاون عابر للحدود، في وقت تكتشف فيه الأدبيات القانونية عن فجوات في الحوكمة الدولية للعمليات السيبرانية البحرية. وهو ما أفضى الى بروز الحاجة لإطار دبلوماسي منظّم لإدارة المخاطر[IV].

٩,١ مفهوم الدبلوماسية السيبرانية البحرية.

يعتبر المفهوم الإطار التحليلي والسياسي والذي يُعنى بتوظيف أدوات السياسة الخارجية والعلاقات الدولية لتنظيم وإدارة المخاطر السيبرانية والهجينة التي تستهدف البنية التحتية البحرية الرقمية وسلاسل الامداد البحرية والكابلات وأنظمة الملاحة البحرية. ولا تُمثل هذه المقاربة بديلاً عن الأمن السيبراني التقني، بل إطارا تكامليا يركز على بناء قواعد سلوك، وتنسيق الاستجابة للحوادث، وتطوير ترتيبات تعاون دولية بين الدول والقطاع الخاص بما يقلل احتمالات التصعيد ويعزز استقرار التجارة العالمية. وتنسجم هذه المقاربة مع التوجيهات الدولية، ولا سيما إرشادات المنظمة البحرية الدولية (**IMO**) نحو تعزيز إدارة المخاطر السيبرانية في القطاع البحري وتحديث أُطُر الحوكمة الناظمة له.

٩,٢ اهداف الدبلوماسية السيبرانية البحرية.

تهدف الدبلوماسية السيبرانية البحرية إلى منع وتقليل التهديدات السيبرانية التي تستهدف البنية البحرية والبنية التحتية المرتبطة بها، بما في ذلك سلاسل الإمداد والكابلات البحرية، وذلك من خلال بناء قواعد سلوك دولية وتعزيز التعاون العابر للحدود. كما تسعى إلى إدارة الأزمات السيبرانية بين الدول وتنسيق الاستجابة للحوادث بما يحد من مخاطر التصعيد. كذلك تعمل على سد فجوات الحوكمة الدولية عبر الدفع نحو أُطُر قانونية وتنظيمية تحكم وتقنن استخدام القدرات السيبرانية في المجال البحري، وذلك بما يعزز استقرار التجارة العالمية وأمن الملاحة.

٩,٣ أدوات الدبلوماسية السيبرانية البحرية.

تعتمد الدبلوماسية السيبرانية البحرية على مجموعة من الأدوات الدبلوماسية والتنظيمية التي تهدف إلى تحويل التهديدات في البيئة البحرية من مصادر تصعيد وعدم استقرار إلى مجالات قابلة للإدارة والتنسيق الدولي. لا تقوم هذه الأدوات على الرد التقني أو العسكري، بل على توظيف آليات السياسة الخارجية، وبناء التفاهمات، ووضع ترتيبات تعاون رسمية وغير رسمية. بما يسمح بضبط السلوك، وتقليل المخاطر وتعزيز الاستقرار في المجال الرقمي.

- **الاتفاقيات الثنائية.**

تُعد الاتفاقيات الثنائية أداة عملية محورية في الدبلوماسية السيبرانية البحرية. إذ تُمكِّن الدول من إنشاء قنوات اتصال رسمية لإدارة الحوادث السيبرانية البحرية. وتبادل مؤشرات الاختراق، وتنفيذ تدريبات مشتركة، وتنسيق التحقيقات عند استهداف الموانئ أو

17. https://www.atlanticcouncil.org/in-depth-research-reports/report/raising-the-colors-signaling-for-cooperation-on-maritime-cybersecurity

السفن. وتكمن قيمتها الأساسية في تقليص فجوات الثقة وتسريع الاستجابة، خصوصا في بيئة تتوزع فيها البيانات الحساسة بين جهات حكومية ومشغلين تجاريين.

- **الأطر متعددة الأطراف.**

توفر الأُطُر متعددة الأطراف منصة لتنسيق السياسات وتوحيد المعايير في مجال الأمن البحري السيبراني، وربطه بالحوكمة البحرية والقانون الدولي. كما تُسهم في انتاج حد أدنى من قواعد السلوك المشتركة، وتسهيل تنسيق الاستجابات الإقليمية والدولية، لا سيما في ظل اتساع الفجوة بين قواعد القانون البحري التقليدي وطبيعة العمليات السيبرانية البحرية العابرة للحدود.

- **إجراءات بناء الثقة.**

تشمل إجراءات بناء الثقة السيبرانية البحرية إنشاء نقاط اتصال وطنية وبروتوكولات إخطار بالحوادث، وتنفيذ تمارين مشتركة، والتفاهم حول حماية بعض البُنى البحرية الحيوية. وتهدف هذه الإجراءات إلى تقليل سوء الفهم ومنع ردود الفعل المبالغ فيها عند وقوع حوادث سيبرانية بحرية، خاصة في ظل صعوبة الإسناد وإمكانية توظيف الهجمات كأدوات ضغط استراتيجي.

- **تبادل المعلومات.**

يمثل تبادل المعلومات الركيزة التشغيلية للدبلوماسية السيبرانية البحرية، ويشمل مشاركة بيانات التهديدات، وأنماط الهجمات، ونقاط الضعف في الأنظمة البحرية بين الحكومات والقطاع الخاص. وتؤكد الإرشادات الدولية الصادرة عن المنظمة البحرية الدولية (**IMO**) وغيرها من منظمات دولية وأمنية أن تحديد المخاطر وتقييمها ومعالجتها عملية مستمرة، ما يجعل تبادل المعلومات شرطاً أساسياً لفعالية حوكمة سيبرانية بحرية.

٩,٤ الدبلوماسية السيبرانية كأداة لمنع التصعيد.

تُستخدم الدبلوماسية السيبرانية البحرية كأداة للتصعيد المنضبط عبر آلية تدريجية تنقل الهجوم السيبراني البحري من كونه حادثاً تقنياً إلى كونه سلوكاً دولياً محال مساءلة سياسية. تبدأ هذه الآلية بعمليات الإسناد السياسي والدبلوماسي للهجمات، ثم إصدار بيانات إدانة رسمية وبناء سردية قانونية–سياسية حول التهديد الواقع على البُنى البحرية الحيوية، وفي المراحل اللاحقة يتم العمل على حشد مواقف جماعية وتحالفات ردع، ودمج الحادث ضمن أطر استجابة متعددة الأطراف، بما يسمح بفرض تدابير تقييدية أو عقوبات دولية عند تكرار الهجمات أو اتساع آثارها. ويُعد نهج الإتحاد الأوربي في (**Cyber Diplomacy Toolbox**)[١٨] نموذجاً واضحاً لهذا التصعيد المتدرج، إذ يوازن بين الردع السياسي وضبط التصعيد، ويرفع تكلفة الهجمات السيبرانية البحرية دون الانزلاق إلى مواجهة عسكرية مباشرة.

٩,٥ التحديات التي تواجه الدبلوماسية السيبرانية البحرية.

تواجه الدبلوماسية السيبرانية البحرية جملة من التحديات البنيوية والمعرفية، في مقدمتها صعوبة الإسناد الدقيق للهجمات السيبرانية وإثبات المسؤولية القانونية، وتعدد الفاعلين غير الحكوميين، وتداخل الاختصاصات بين القانون البحري والقانون الدولي السيبراني. كما يسهم تفاوت القدرات التقنية والمؤسسية بين الدول في إضعاف فاعلية التعاون وبناء الاستجابات الجماعية. وتُظهر الأدبيات القانونية فجوات واضحة في قدرة الأُطُر القائمة، بما في ذلك اتفاقية الأمم المتحدة لقانون البحار على استيعاب العمليات البحرية السيبرانية بصورة متّسقة. الأمر الذي يعيق تطوير قواعد سلوك ملزمة ويُبقي المجال البحري السيبراني ساحة مفتوحة للعمليات الرمادية منخفضة التكلفة.

18. https://data.consilium.europa.eu/doc/document/ST-10289-2023-INIT/en/pdf

ينطلق الاستشراف المستقبلي للأمن البحري السيبراني من إدراك متزايد بأن التحولات التقنية والرقمنة العميقة للمجال البحري وتداخل التهديدات السيبرانية مع التنافس الجيوسياسي سوف تعيد تشكيل بيئة الأمن البحري بصورة بنيوية، وهذا المحور لا يسعى إلى التنبؤ الحتمي بل إلى تحليل اتجاهات قابلة للتحقق وبناء تصورات واقعية لمسارات مخاطر الأمن السيبراني بما يتيح تطوير سياسات استباقية قادرة على التعامل مع عدم اليقين والتعقيد المستقبلي.

- **التخطيط بالسيناريوهات.**

يُعد التخطيط بالسيناريوهات من أكثر أدوات الاستشراف ملاءمة لتحليل الأمن البحر السيبراني وذلك نظراً لطبيعته المعقدة التي تتقاطع فيه المتغيرات التقنية والبيئية والسياسية والاقتصادية. ويرتكز هذا النهج على تحديد محركات التغيير الرئيسية، مثل تسارع الرقمنة البحرية، وتطور أدوات الهجوم السيبراني، وتحول أنماط الصراع الدولي، ثم اختبار تفاعلاتها ضمن مسارات مستقبلية متعددة. وتكمن قيمته العلمية في قدرته على كشف مظاهر الهشاشة البنيوية في المنظومات البحرية الرقمية، وتقييم الآثار طويلة المدى ومتوسطة المدى للقرارات الحالية، بما يدعم الانتقال من منطق إدارة الازمات إلى مقاربة إدارة المخاطر الاستباقية في بيئة تتسم بدرجة عالية من عدم اليقين. ولا يهدف التخطيط بالسيناريوهات في مجال الأمن البحري السيبراني إلى التنبؤ بما سيحدث بقدر ما يسعى إلى تحليل فرضيات (ماذا لو حدث) وكيف ستتفاعل المنظومات التقنية والمؤسسية والقانونية معها. وبهذا يصبح السيناريو أداة تحليلية لكشف نقاط الضعف الكامنة وليس مجرد تمرين افتراضي.

- **الاتجاهات المستقبلية للأمن البحري السيبراني.**

تشير الاتجاهات المستقبلية للأمن البحري السيبراني إلى انتقاله من نطاق تقني محدود إلى مجال استراتيجي متكامل يرتبط بالأمن الوطني واستقرار الاقتصاد العالمي، مدفوعاً بالتوسع المتسارع في الأتمتة البحرية وتكامل السفن والموانئ مع شبكات البيانات العالمية وسلاسل الإمداد الرقمية. ويقابل هذا التحول تصاعد التهديدات تكون أكثر تعقيداً وتكيفاً تشمل الهجمات الهجينة، والتلاعب بالبيانات، وتعطيل الخدمات والعمليات اللوجستية بما يوسع سطح الهجوم ويحوّل استدامة العمليات إلى هدف مركزي للهجمات. وفي هذا السياق **تبرز أشباه الموصلات وال Firmware** كطبقة فيزيائية حاكمة للثقة داخل الأنظمة، ويضيف مسار مخاطر مرتبط بسلسلة التوريد والتحقق من المصدر وإدارة تحديثات وال **Firmware**.

كما يتوقع أن يؤدي اتساع الفجوة التقنية بين الدول الى تكريس عدم التماثل في التهديدات. وهو ما يجعل التعاون الدولي وبناء الأُطر التنظيمية المشتركة عنصراً حاسماً في احتواء المخاطر المستقبلية.

وهناك حوادث حدثت مثل هجوم **NotPetya** على شركة الشحن **Maersk** في ٢٠١٧ أعطى مُؤشر اتجاه (**Trend Indicators**) على أن التهديدات المستقبلية أصبحت خطر استراتيجي عابر للحدود وهي تتجه لتكون أقل وضوحاً قانونياً وأعلى تأثيراً اقتصاديا وأكثر ارتباطا بالصراع الهجين وإدارة النفوذ.

١٠,١ سيناريوهات محتملة حتى عام ٢٠٣٥.

- **سيناريوهات محتملة على مستوى النظام الدولي.**

هذه السيناريوهات تضع تصور مستقبلي كيف يُدار الأمن البحري السيبراني، وكيف تتشكل العلاقة السيبرانية بين الدول، وكذلك منطق الصراع والتعاون السائد.

(أ أ). سيناريو التكيف التعاوني. (Cooperative Adaptation Scenario).

يفترض سيناريو التكيف التعاوني أنه حتى عام ٢٠٣٥ ستتجه الدول والفاعلون البحريون الرئيسيون إلى تطوير استجابة جماعية لتهديدات الأمن البحري السيبراني، مدفوعة بارتفاع كلفة الاضطرابات التشغيلية والاقتصادية الناتجة عن الرقمنة المتسارعة. ويقوم هذا السيناريو على إعادة تعريف الأمن البحري السيبراني كمنفعة جماعية تتطلب توافقاً وظيفياً على أُطُر الحوكمة والمعايير التشغيلية. حتى في ظل استمرار التنافس الجيوسياسي مع التركيز على\ى إدارة المخاطر واحتواء الأثر بدلا من منع الاختراق بشكل مطلق.

ويتوقع أن يؤدي هذا المسار إلى تعزيز المرونة التشغيلية واستمرارية الخدمة وتقليص احتمالات التعطل واسع النطاق، وذلك عبر توحيد خطوط الأساس لإدارة المخاطر وتبادل معلومات التهديدات وبناء آليات انذار مبكر، ولكن التحدي الوحيد في ذلك هو معالجة تباين القدرات بين الدول وحساسية مشاركة المعلومات وتجنب الاكتفاء بالامتثال الشكلي دون تطبيق مؤسسي فعال.

(ب ب). سيناريو التصعيد الهجين (Hybrid Escalation Scenario).

يفترض سيناريو التصعيد الهجين إن الأمن البحري السيبراني حتى عام ٢٠٣٥ سيشهد تصاعداً في استخدام الأدوات السيبرانية البحرية كوسائل ضغط سياسي واستراتيجي منخفضة الكلفة دون تجاوز عتبة الصراع العسكري التقليدي. ويقوم هذا المسار على استهداف انتقائي للمنظومات البحرية الرقمية بما يحقق اضطراباً تشغيلياً واقتصادياً محسوب مع الحفاظ على الغموض القانوني وصعوبة الاسناد. ويعكس هذا السيناريو تحول الصراع البحري نحو مناطق رمادية تُدار فيها المنافسة عبر التأثير على البيانات واستمرارية التشغيل مع مخاطر كامنة تتعلق بسوء التقدير والتصعيد غير المقصود.

(ج ج). سيناريو الانكشاف البنيوي (Scenario of Structural Exposure).

يفترض سيناريو الانكشاف البنيوي أنه حتى عام ٢٠٣٥ ستفشل بعض الدول أو التكتلات في مواكبة التحولات المتسارعة في الرقمنة البحرية والأمن السيبراني، وذلك نتيجة ضعف الحوكمة أو محدودية الموارد أو قصور الأُطُر التنظيمية. ولا يكمن الخطر في غياب التكنولوجيا بحد ذاتها، بل في عدم دمجها ضمن منظومات مؤسسية قادرة على إدارة المخاطر. ويؤدي ذلك إلى تراكم هشاشة هيكلية في البُنى التحتية البحرية الحرجة. وهو ما يجعلها عرضة لتعطيلات متكررة وآثار اقتصادية متسلسلة تمتد إلى سلاسل الامداد العالمية وتُحول الضعف المحلي إلى تهديد نظامي عابر للحدود.

- **سيناريوهات محتملة تعل على مستوى الآليات والبُنى.**

هذه السيناريوهات تعمل على وضع تصور مستقبلي متعلق ب (**Structural & Mechanism–Level**) مثل مستوى التجزئة الرقمية والاعتماد المفرط على الأتمتة والصدمة النظامية.

(أ أ). سيناريو التجزئة الرقمية البحرية. (Maritime Cyber Fragmentation).

يفترض هذا السيناريو تشكُل فضاءات سيبرانية بحرية متباينة وذلك نتيجة اختلاف المعايير التقنية والتشريعات ونماذج الحوكمة بين التكتلات الدولية. وبدلاً من نظام بحري رقمي عالمي متكامل سوف ينشأ نظام مُجزأ تُدار فيه الموانئ وأنظمة الملاحة وتبادل البيانات وفق أطر إقليمية أو سياسية متنافسة. ويؤدي ذلك إلى تقليص قابلية التشغيل البيني وارتفاع كلفة الامتثال وزيادة مخاطر سوء التقدير والأخطاء التشغيلية وهو ما ينعكس سلبا على أمن الملاحة والتجارة الدولية.

لا يُعد سيناريو التجزئة الرقمية افتراضا مستقبلياً محضاً، بل يمثل امتداد منطقي لاتجاهات قائمة تتمثل في تباين معايير الأمن البحري السيبراني بين الدول، واختلاف الأطر التنظيمية ومستويات الامتثال إلى جانب تزايد تسييس البيانات والبُنى الرقمية البحرية. وفي ظل تصاعد التنافس الجيوسياسي في الفضاء الرقمي، يُرجّح أن تتجه الدول نحو بناء نظم بحرية رقمية ذات طابع إقليمي، والذي سيؤدي إلى تراجع قابلية التشغيل البيني، وارتفاع مخاطر سوء التنسيق والأخطاء التشغيلية. جميع المعطيات السابقة تجعل من سيناريو التجزئة الرقمية أكثر السيناريوهات احتمالا حتى عام ٢٠٣٥.

(ب ب). سيناريو خصخصة الأمن السيبراني (Cybersecurity Privatization Scenario).

يفترض هذا السيناريو تنامي دور الفاعلين غير الحكوميين – شركات التكنولوجيا ومشغلي الموانئ وشركات التأمين والأمن السيبراني – في تولي مهام الحماية والاستجابة، مقابل تراجع نسبي للدور الحكومي المباشر. ويحدث ذلك نتيجة تعقيد التهديدات وتسارع الابتكار وعدم قدرة الأطر الحكومية التقليدية على المواكبة الزمنية والتقنية. وينشأ عن هذا المسار تحديات تتعلق بالمساءلة وتضارب المصالح وتوزيع المسؤوليات القانونية عند وقوع حوادث سيبرانية كبرى.

لا يُعد سيناريو خصخصة الأمن البحري السيبراني افتراضاً مستقبليا بحتاً، بل مسار بدأ بالفعل بصورة تدريجية، يتجلى في اعتماد شركات الشحن والموانئ على مزودي خدمات أمن سيبراني من القطاع الخاص وفي اشتراطات التأمين السيبراني التي تفرض متطلبات تقنية محددة

، فضلا عن الدور المتزايد للحكومات في وضع أُطُر تنظيمية عامة تتولى الجهات الخاصة تنفيذها وتطبيقها عملياً. ومع التطلع إلى أفق ٢٠٣٥، يتوقع أن تتسارع وتيرة الابتكار التقني بدرجة تفوق قدرة البيروقراطيات الحكومية على المواكبة، بما يوسع الفجوة بين التنظيم والتنفيذ. وفي هذا السياق لا تمثل الخصخصة احتمالاً مستقبليا بقدر ما تشكل اتجاها متقدما يُعمّق إشكاليات السيادة والمساءلة.

(ج ج). سيناريو الاعتماد المفرط على الأتمتة (Scenario Automation of Dependency Risk).

يفترض هذا السيناريو أن يؤدي التوسع غير المنضبط في استخدام الذكاء الاصطناعي والأنظمة الذاتية في السفن والموانئ الى تقليص دور العنصر البشري في اتخاذ القرار التشغيلي والأمني. ورغم المكاسب التشغيلية، سينشأ خطر جديد يتمثل في فقدان القدرة على التدخل اليدوي الفعال عند فشل الأنظمة أو تعرضها لهجوم سيبراني معقد. وتتحول الأتمتة من عنصر قوة إلى نقطة هشاشة إذا لم تدمج ضمن إطار مرونة بشرية–مؤسسية.

بحلول عام ٢٠٣٥ فإن سيناريو الاعتماد المفرط سيكون مرشح تقنيا وحاضر جزئيا على الأقل في عدد من الموانئ والمسارات البحرية. وذلك لتزايد أعداد السفن الذكية والموانئ المؤتمتة وتزايد استخدام الذكاء الاصطناعي في إدارة الحركة واللوجستيات، ويمكن الخطر في تراجع المهارات البشرية وهشاشة أنظمة الرجوع اليدوي والثقة المفرطة بالخوارزميات.

(د د). سيناريو الصدمة النظامية البحرية (Scenario Systemic Shock).

الصدمة النظامية في الأمن البحري السيبراني يقصد بها الاضطراب الواسع الذي ينشأ نتيجة خلل أو هجوم سيبراني ويتجاوز أثره النطاق التقني ليحدث سلسلة تأثيرات متراكبة تطال سلاسل الامداد والاقتصاد والاستقرار المؤسسي ويحد من قدرة النظام على الاستجابة والاحتواء.

يفترض هذا السيناريو وقوع حادث سيبراني واسع النطاق ليس بالضرورة هجوم متعمد، ويؤدي إلى تعطيل متزامن لعدة عقد بحرية حرجة من موانئ وممرات ملاحية أو أنظمة وبيانات لوجستية، ويظهر هذا السيناريو كيف يمكن لحدث واحد أن يطلق سلسلة تأثيرات متراكبة تتجاوز القطاع البحري إلى الاقتصاد العالمي والأمن الغذائي والطاقة والاستقرار السياسي.

هذا السيناريو منخفض الاحتمال ولكن عالي التأثير وممكن وخطير استراتيجياً بسبب الترابط العميق بين سلاسل الإمداد، والاعتماد المتبادل بين الأنظمة وكذلك هشاشة العقد الحرجة. وقد ينشأ من فشل تقني في ظل ضعف الحوكمة وتأخر الاستجابة.

يُظهر تحليل السيناريوهات المحتملة للأمن البحري السيبراني حتى عام ٢٠٣٥ أن مستقبل هذا المجال لن يتحدد عبر مسار واحد أو نموذج خطّي، بل سيتشكل من تفاعل معقد بين أنماط التعاون الدولي والتنافس الجيوسياسي، والهشاشة البنيوية الناتجة عن الرقمنة المتسارعة للبيئة البحرية. وتكشف السيناريوهات المطروحة، سواء في صيغتها الأساسية أو المركبة أن التهديد السيبراني البحري يتجه ليكون أقل وضوحا من الناحية القانونية وأكثر تأثيراً من حيث التداعيات الاقتصادية، وأكثر اندماجاً في منطق الصراع الهجين وإدارة النفوذ دون الانزلاق إلى مواجهة عسكرية مباشرة.

كما تبرز هذه السيناريوهات أن التحدي المستقبلي لا يكمن في طبيعة الهجمات السيبرانية بحد ذاتها، بل في قدرة المنظومات البحرية على امتصاص الصدمات، والحفاظ على استمرارية التشغيل وإدارة المخاطر ضمن بيئة عالية من عدم اليقين. وعليه ستقاس فعالية الأمن البحري السيبراني مستقبلاً بمدى نضوجيه الحوكمة ومرونة البُنى التحتية الحرجة وكفاءة الموائمة بين القدرات التقنية والإطار المؤسسي والمسار الدبلوماسي بما يُعيد تعريف الأمن البحري ليس كحالة دفاعية جامدة بل كقدرة ديناميكية على التكيف والاستباق.

١،٢ أثر التطورات التكنولوجية المستقبلية.

من المتوقع أن تحدث التطورات التكنولوجية المستقبلية تحولا نوعيا في طبيعة الأمن البحري السيبراني، لا من حيث الأدوات فقط، بل من حيث منطق التهديد والاستجابة. فالانتشار المتزايد للذكاء الاصطناعي والأنظمة ذاتية التشغيل في السفن والموانئ وأنظمة إدارة الحركة البحرية سيعزز من كفاءة التشغيل، وسرعة اتخاذ القرار، والقدرة على المراقبة والتحليل التنبئي. غير أن هذا الاعتماد المتنامي على الأنظمة المؤتمتة سينتج في الوقت ذاته أنماطاً جديدة من الهشاشة تتمثل في تعقيد سلاسل البرمجيات، واتساع سطح الهجوم، وصعوبة التحقق من سلامة البيانات والخوارزميات.

ويتوقع أن تسهم تقنيات متقدمة مثل الحوسبة الكمية مستقبلاً في إعادة تشكيل موازين القوة السيبرانية، عبر تقويض بعض نماذج التشفير الحالية، وفرض تحديات غير مسبوقة على أمن الاتصالات البحرية. ونتيجة لذلك، لن يكون التحدي المستقبلي تقنياً لحتاً، بل مؤسسياً استراتيجياً، يرتبط بقدرة الدول على استيعاب هذه التقنيات ضمن أطر حوكمة وتشريعات وعقائد أمن بحري مرنه وقابلة للتكيف. وسيصبح التفوق في الأمن البحري السيبراني نتاجاً للتكامل بين الابتكار التقني، والنضج المؤسسي والرؤية الاستشرافية طويلة المدى، وليس مجرد امتلاك أدوات تقنية متقدمة.

تختتم هذه الدراسة بخلاصة مفادها أن التحولات في الأمن البحري لم تعد محصورة في تغير أنماط التهديد، بل تعكس تحولاً بنيوياً في المجال البحري نفسه مع تساع التحول الرقمي وتزايد الاعتماد على الأنظمة الشبكية في تشغيل السفن والموانئ وأنظمة الملاحة والاتصالات وسلاسل الامداد البحرية. وبناء على ذلك، لم تعد التهديدات البحرية السيبرانية والهجينة تُعامل كحوادث تقنية منفصلة، بل كتهديدات وظيفية قد تسبب تعطلاً متسلسلاً يمتد من المجال البحري إلى الاقتصاد والحوكمة والاستقرار.

وترتكز الخاتمة على مقاربة تكاملية تجمع مسارين مترابطين: مسار هندسي-تشغيلي يتمثل في الهندسة الدفاعية السيبرانية البحرية بوصفها إطاراً لرفع المرونة وتقليص قابلية التعطيل عبر التصميم الدفاعي للمنظومات وربط متطلبات الحماية باستمرار الاعمال، ومسار حوكمي-دبلوماسي يقوم على ترتيبات تعاون عابرة للحدود لتنسيق الاستجابة، وتبادل المعلومات، وبناء الثقة، وإدارة الحوادث المشتركة بما يحد من مخاطر التصعيد ويُسرع عملية الاحتواء والتعافي.

١١,١ النتائج الرئيسية.

أظهرت الدراسة أن مركز ثقل الأمن البحري (**CoG**) يشهد انتقالا من حماية المنصات والعتاد الى حماية الوظائف البحرية الحرجة مثل التشغيل والخدمات اللوجستية والملاحة والاتصالات، وذلك بوصفها نقاط الهشاشة الأكثر حساسية في بيئة بحرية رقمية عالية الاعتماد على الترابط الشبكي. وأوضحت الدراسة كذلك أن الهجمات السيبرانية التي تستهدف السفن والموانئ وأنظمة الملاحة والاتصالات وسلاسل الامداد لا تقتصر آثارها على الخلل التقني المباشر، بل تتسع لتُحدث تداعيات متسلسلة تشمل تعطل الخدمات، وارتفاع كلفة المخاطر، واختلال اليات التنسيق المؤسسي ضمن منظومة النقل البحري. وفي هذا السياق تبرز الهندسة الدفاعية السيبرانية البحرية كاستجابة بنيوية تُعيد مواءمة تصميم المنظومات البحرية مع متطلبات المرونة التشغيلية واستمرارية الأعمال. وبالتوازي تتسب الأطر الدبلوماسية والحوكمية أهمية متزايدة باعتبارها ركيزة أساسية لإدارة المخاطر حين تتجاوز الحوادث النطاق الإقليمي وتتعدد الأطراف المعنية وذلك عبر ترتيبات تنسيق وتبادل معلومات، وبناء ثقة تعمل على تحسين سرعة الاحتواء وتحد من احتماليات التصعيد وسوء التقدير.

١١,٢ الاستنتاجات التحليلية.

الأمن البحري لا يُدار بفاعلية عبر مقاربات استجابات تكتيكية قصيرة المدى، بل يتطلب اطار تكاملي يربط بين حماية الطبقة التقنية وبين إدارة الاعتماد المتبادل التي تفرضه طبيعة التشغيل البحري الحديثة وسلاسل التوريد العابرة للحدود. إن جوهر التهديد في البيئة البحرية الرقمية لا يتمثل في الاختراق كواقعة تقنية منعزلة، بقدر ما يتمثل في تعطيل الوظائف البحرية الحرجة كأثر تشغيلي ممتد ينعكس على السلامة البحرية، واستمرارية الخدمات، وفاعلية الحوكمة.

من هذا المنطلق، تبرز الهندسة الدفاعية السيبرانية البحرية كمسار بنيوي لتقليص قابلية التعطيل عبر تصميمات دفاعية للمنظومات يُرسّخ مبادئ الفصل بين البيئات التشغيلية والمعلوماتية، والتقسيم الشبكي، وتقييد الصلاحيات وفق مبدأ الحد الأدنى من الصلاحيات، وبناء قدرات رصد واستجابة وتعافي مرتبطة مباشرة بمتطلبات استمرارية الاعمال. وتؤدي هذه المقاربة عمليا إلى تعزيز الردع بالحرمان عبر رفع كلفة الهجوم وتقليل العائد المتوقع منه من خلال تقوية قدرة المنظومة على إحتواء أثر الهجوم السيبراني واستعادة الوظائف التشغيلية.

كما أن لأطُرُ الدبلوماسية والترتيبات التنظيمية تُعد مكوناً حاسماً لضبط المخاطر حين تتداخل مسؤوليات الدول والجهات المشغلة، وتتوزع البيانات والخدمات عبر ولايات فقضائية متعددة. إذ توظف الدبلوماسية السيبرانية البحرية بوصفها تنسيق لتأسيس قنوات اتصال دائمة، وبروتوكولات لتبادل الانذارات والمعلومات الفنية، وترتيبات مشتركة لإدارة الحوادث العابرة للحدود، وبما يقلص فجوات الإدراك ويحد من سوء التقدير والتصعيد، ويرفع سرعة الاحتواء واستعادة الخدمة. إن الفاعلية المستقبلية في حماية المجال البحري تتأسس على تكامل الصلابة الهندسية مع الحوكمة العابرة للحدود ضمن نموذج واحد لإدارة المخاطر وتعزيز المرونة التشغيلية.

١١,٣ التوصيات الاستراتيجية.

توصي الدراسة بتبني نموذج استراتيجي تكاملي يقوم على مسارين متوازيين ومتداخلين: مسار هندسي–تشغيلي يُعيد تشغيل منظومات العمل البحري على أساس المرونة التشغيلية، ومسار دبلوماسي–حوكمي يُحول التعاون العابر للحدود من صيغة إعلان نوايا إلى ترتيبات قابلة للتفعيل عند وقوع الحوادث.

فعلى المستوى الهندسي–التشغيلي، تنطلق المعالجة من تحديد الوظائف البحرية الحرجة (الملاحة، التحكم التشغيلي، الاتصالات، إدارة الحركة، الخدمات اللوجستية) بوصفها وحدات قياس للتهديد وليست الأنظمة بمعناها التقني. ثم يُبنى التصميم الدفاعي عبر ضوابط فصل وتقسيم شبكي بين نظم التشغيل ونظم تقنية المعلومات ، وتطبيق مبادئ الحد الأدنى من الصلاحيات وإدارة الهوية ، وتأمين الطرفيات وسلاسل التوريد الرقمية. ويستكمل ذلك بمنظومة قياس أداء تربط باستمرارية الاعمال، مثل زمن الاكتشاف، وزمن الاحتواء، وزمن الاستعادة، ومستوى الخدمة أثناء الطوارئ.

١١,٤ افاق البحث المستقبلي.

تتطلب آفاق البحث المستقبلي الانتقال من الطرح التكاملي الذي يجمع بين الهندسة الدفاعية السيبرانية البحرية والأُطر الدبلوماسية إلى نماذج تحليلية قابلة للقياس والمقارنة والتحقق التجريبي، ويبدأ ذلك بتطوير مؤشرات كمية للمرونة التشغيلية في الموانئ والسفن وسلاسل الامداد. هذه المؤشرات لا تقيس مستوى الأمن بصفه عامة، بل تقيس القدرة على استمرار الوظائف الحرجة خلال اضطراب سيبراني–تشغيلي، بما يشمل زمن الاكتشاف والاحتواء، وزمن الاستعادة، ومعدلات التدهور المقبول للخدمة أثناء الأزمات.

كما تُعد دراسة فعالية التصميم الدفاعي في البيئات البحرية عالية التعقيد أولوية بحثية، وذلك عبر تقييم مقاربات مثل التقسيم الشبكي، والثقة المعدومة (**Zero Trust**)، وهندسة التعافي (**Recovery Engineering**) ضمن سياقات تشغيلية حقيقية تتسم بتعدد الموردين، وطول دورة حياة الأنظمة. ويتوازى ذلك مع ضرورة تعميق البحث في الحوكمة القانونية والتنظيمية للحوادث العابرة للحدود، بما يشمل مسؤوليات الإبلاغ، وحدود مشاركة البيانات الفنية، واشكاليات الاختصاص القضائي، ودور التأمين البحري السيبراني في تشكيل الحوافز والسلوك المؤسسي.

ومن منظور التعاون الدولي، تحتاج أدوات إعادة بناء الثقة (**CBMs**) إلى تقييم منهجي عبر دراسات حالة مقارنة وتكارين محاكاة تقيس أثرها على تقليص فجوات الإدراك، وتسريع الاستجابة، وخفض احتمالات التصعيد وسوء التقدير.

ويستلزم الاستشراف حتى عام ٢٠٣٥ بناء سيناريوهات تُفحص فيها تداعيات الذكاء الاصطناعي والأتمتة وانترنت الأشياء (**IoT**) على توازن المخاطر بين الفاعلين، وعلى قابلية تشغيل الدبلوماسية السيبرانية كأداة للاستقرار وإدارة الأزمات.

Gulf Research Center
Knowledge for All

مركز الخليج للأبحاث
المعرفة للجميع

يعبر هذا المقال عن أفكار وآراء الكاتب، ولا يعبر بالضرورة عن رأي المركز

Gulf Research Center Jeddah (Main office)

19 Rayat Alitihad Street
P.O. Box 2134
Jeddah 21451
Saudi Arabia
Tel: +966 12 6511999
Fax: +966 12 6531375
Email: info@grc.net

Gulf Research Center Riyadh

Unit FN11A
King Faisal Foundation
North Tower
King Fahd Branch Rd
Al Olaya Riyadh 12212
Saudi Arabia
Tel: +966 112112567
Email: info@grc.net

Gulf Research Center Foundation

Avenue de France 23
1202 Geneva
Switzerland
Tel: +41227162730
Email: info@grc.net

Gulf Research Centre Cambridge

University of Cambridge
Sidgwick Avenue,
Cambridge CB3 9DA
United Kingdom
Tel:+44-1223-760758
Fax:+44-1223-335110

Gulf Research Center Foundation Brussels

4th Floor
Avenue de
Cortenbergh 89
1000 Brussels
Belgium
grcb@grc.net
+32 2 251 41 64