أثر الحرب السيبرانية الإسرائيلية – الإيرانية على الأمن الإقليمي العربي

The Impact of the Israeli-Iranian Cyberwar on Arab Regional Security

أحمد محى محمد أحمد علي [1]

ahmadmohee@gmail.com

إهداء

الي أمي، السيدة/ نادية خلف عبدالحافظ: الفتاة المصرية التي نشأت في طما، واحدة من أفقر مدن صعيد مصر، وعاشت طفولة بائسة تعاني من الجهل والفقر والتفكك الأسري. وبعد أن مُنعت من إكمال تعليمها الأساسي بسبب الفقر، تحدت كل قيود المجتمع والظروف، واقترضت خمسون قرشا لتكمل تعليمها الأساسي وتلتحق بتدريب مساعدات المولدات في مستشفي قنا المركزي فتتفوق وتكون الأولى على فصلها. وبالرغم من قسوة القيود الاجتماعية، نجحت في الاستقلال بحياتها، وتكوين اسرتنا الصغيرة، و إكمال ما فاتها من التعليم، وفي أن يكون لديها سجل مهني ناجح كممرضة لأكثر من 42 عامًا.

لقد قررت أن تغير من واقعها الأليم متسلحة بالعلم والاصرار لتشق طريقها في الحياة بين جبال عالية من صخور الجهل والفقر والتخلف. تجاهلت الانهزامية والحقد والتنمر وخاضت في رحلة حياتها معارك كثيرة مليئة بالتضحية والتفاني فقط لتنجو بسفينة اسرتنا الصغيرة إلى بر الأمان.

إلى السيدة الفاضلة/ رد الروح، ناظرة المدرسة الابتدائية بطما، التي أقرضت أمي تلك الخمسون قرشا عام 1960.

1. باحث ماجستير بمعهد البحوث والدراسات العربية

ملخص البحث

تهدف هذه الدراسة إلى قياس وتحليل أثر الحرب السيبرانية الإسرائيلية – الإيرانية على الأمن الإقليمي العربي، باستخدام مقولات نظرية مجمع الأمن الإقليمي لـــبوزان وفر و دي وايلد. فبناء على ذلك تم تحليل أنماط العلاقات الدولية بين دول الإقليم العربي، و رصد التغيرات في كل من: أنماط الصداقة والعداوة، والاعتماد الأمني المتبادل، وتوزيع القوى بين دول الاقليم. بهدف قياس أثر الحرب السيبرانية الإسرائيلية–الإيرانية على تلك العوامل وصولا إلى استنتاج عن الأثر الكلي لتلك الحرب على الأمن الإقليمي العربي.

أثبتت الدراسة أن الحرب السيبرانية الإسرائيلية – الإيرانية، كان لها تأثيراً واضحاً على الأمن الإقليمي العربي، حيث أدت تداعيات تلك الحرب وما خلفته من أخطار وتهديدات، إلى إحداث تغيرات جوهرية في أنماط العلاقات الدولية بالإقليم، وعلى وجه الخصوص فقد أدت إلى:

- زيادة الاعتماد الأمني السيبراني المتبادل
- تغير في أنماط الصداقة والعداوة
- وتغير في توازنات القوى السيبرانية بين دول الإقليم.

مما أدى إلى تكوين مجمعا إقليمياً عربياً للأمن السيبراني بمبادرة من المملكة العربية السعودية ومشاركة دول مجلس التعاون الخليجي.

الكلمات المفتاحية: الحرب السيبرانية، الأمن الإقليمي العربي، مجمع الأمن الإقليمي السيبراني، المملكة العربية السعودية،إسرائيل،إيران.

Abstract:

In this study, we aim to measure the overall impact of the Israeli-Iranian cyberwar on the Arab regional security using the regional security complex theory of Buzan, Wæver, and de Wilde. To this end, we analyzed international relations in the Arab world, including changes in patterns of amity-enmity, mutual security dependence, and distribution of powers.

This study proved that Israeli-Iranian cyberwar had a measurable impact on Arab regional security. The repercussions, dangers and threats of this cyberwar have led to fundamental changes to patterns of international relations in the Arab region, including:

- Increasing mutual Cybersecurity dependence
- Changing the patterns of amity-enmity
- Changing the balance of cyber power among the countries of the region.

This finally resulted in forming an Arab regional Cybersecurity complex, at the initiative of the Kingdom of Saudi Arabia with participation from the Gulf Cooperation Council countries.

Keywords: *cyberwar, Arab regional security, regional cybersecurity complex, Saudi Arabia, Israel, Iran.*

Author: *Ahmad Mohee*
ORCI: *0000-0003-3440-5199*
Email: *ahmadmohee@gmail.com*

المقدمة

بسبب وضعها الجيوبوليتيكي، أصبحت منطقتنا العربية مؤخرا مسرحا للعديد من الهجمات السيبرانية، بواسطة العديد من الفاعلين، ما بين دول ومنظمات. استهدفت تلك الهجمات شبكات مرافق، ومقدرات وشركات عربية، وسببت خسائر مادية هائلة وتهديد مباشر للأمن الإقليمي العربي[1]. وفي ظل غياب استراتيجية واضحة للعمل العربي المشترك في مجال الأمن السيبراني[2]، تزداد مساعي الفاعلين الدوليين في استغلال الفضاء السيبراني العربي لتحقيق أهدافهم عن طريق الهجمات السيبرانية. وأيضا في ظل غياب آليات الدفاع والردع السيبراني وغياب تفعيل الاعتماد الأمني المتبادل بين الدول العربية في الفضاء السيبراني[3]، يمكن أن يصبح الفضاء السيبراني العربي بمثابة مسرحا لافتراس إحدى الدول العربية سيبرانيا، تأخذ فيه باقي الدول العربية مقاعد المتفرجين.

مشكلة البحث وأهميتها

إن التهديدات الإيرانية والإسرائيلية للأمن الإقليمي العربي في الفضاء السياسي والاستراتيجي التقليدي معروفة للعيان. وبعد هجوم ستوكسنت أصبح انتقال تلك التهديدات إلى الفضاء السيبراني العربي واقع لا يمكن تجاهله.

[1] Nermeen Abbas, 2018, “Arab Countries Facing The Highest Number Of Cyber Attacks”. Forbes Middle East, Mar 28, accessed May 5, 2021, https://bit.ly/3doronD

[2] المنظمة العربية لتكنولوجيات المعلومات والاتصال، 2021: التزام استراتيجي بالأمن السيبراني في العالم العربي، المنتدى العربي للأمن السيبراني 21-22 أكتوبر – تونس، متاح بالرابط: https://bit.ly/3pChJ2r، تاريخ الدخول: 5 مايو 2021

[3] أمينة خيري وآخرون، 2020، "أين العرب من الأمن السيبراني؟" إندبندنت عربية، 18 يونيو، متاح بالرابط: https://bit.ly/3pyZ0EP، تاريخ الدخول: 5 مايو 2021

فقد كان من أبرز علامات هذا الانتقال، الهجوم السيبراني الذي تعرضت له شركة النفط السعودية أرامكو في 15 أغسطس 2012م، وكان أحد أكثر الهجمات السيبرانية تعطيلًا وإتلافاً لمقدرات الشركة. حيث أصاب الفيروس "شمعون" قرابة ثلاثين ألف محطة عمل وقضى على الأقراص الصلبة لها وعلى كل ما احتوته من بيانات بشركة أرامكو[1].

وتبع ذلك بأيام الهجوم السيبراني على شركة الغاز القطرية راس غاز في 27 أغسطس 2012م، والذي أعتُبِرَ من أكبر الهجمات التي شهدها القطاع الخاص تدميرا حتى ذلك الحين[2]. وقد أشارت أصابع الاتهام إلى إيران على أنها تقف وراء الهجومين[3].

ومنذ ذلك الحين تبادل الجانبين الإيراني والسعودي الهجمات والاتهامات السيبرانية، حتى أن كبير مسؤولي الدفاع المدني الإيراني، الجنرال غلام رضا جلالي، صرح في منتصف مايو 2016: "أن بلاده تستعد لهجمات سيبرانية كبرى من المملكة العربية السعودية، وأنه يعتبر المملكة ذات الأغلبية السنية تهديده الرئيسي في العام المقبل"[4].

يشير هذا التطور في اتجاه الهجوم، إلى اقتناع إيران بأن قدراتها السيبرانية يمكن أن تكون مفيدة في جبهات أخرى من صراعاتها الإقليمية بعيدا عن حربها مع إسرائيل، وبالتالى لم تتردد في توظيف تلك القدرات للهجوم على ألد أعدائها الإقليميين، المملكة العربية السعودية. وإذا كان الأمر كذلك فلا ينبغي

[1] Afp, 2012, US thinks Iran behind cyberattack in Saudi: ex-official, The Express Tribune, October 13, accessed Dec 9, 2021, https://bit.ly/3dy2rWM
[2] Patrick Osgood, 2012, Cyber attack takes Qatar's RasGas offline, Arabian Business, Aug 30, accessed Dec 9, 2021, https://bit.ly/30dz4Gi
[3] Afp, 2012, op. cit.
[4] Shayan Sardarizadeh, 2016, Iran-Saudi tensions erupt in 'cyberwar', BBC, Jun 3, accesses Dec 9, 2021, https://bbc.in/3dxaSBP

أن نستبعد أبدا، أن إسرائيل لن تتردد هى الأخرى في استخدام قدراتها السيبرانية للهجوم على أهداف عربية إذا ما دعتها الظروف للإقدام على ذلك.
وبالتالى من المهم لصانع القرار العربي تقييم القدرات الإيرانية والإسرائيلية في مجال الحرب السيبرانية وحصر التهديدات المحتملة على الأمن الإقليمي العربي، وفرص التعاون في إجراءات الدفاع والردع والإعتماد الأمني المتبادل بين الدول العربية في مجال الأمن السيبراني. من خلال دراسة أبعاد الحرب السيبرانية الإسرائيلية – الإيرانية وانعكاساتها على الأمن الإقليمي العربي.

مما يفتح مجالا واسعا أمام دراسة ظاهرة "**الحرب السيبرانية الإسرائيلية – الإيرانية**" وقياس أثرها على الأمن الإقليمي العربي، منذ عام 2010م. وبالتالي تتمثل إشكالية الدراسة في الإجابة على التساؤل الرئيسي: "**كيف تؤثر الحرب السيبرانية الإسرائيلية – الإيرانية على الأمن الإقليمي العربي؟**"

ويتفرع من هذا التساؤل الرئيسي عدة أسئلة فرعية:

- ما هو أثر الحرب السيبرانية الإسرائيلية – الإيرانية على الاعتماد الأمني المتبادل بين الدول العربية؟
- ما هو أثر الحرب السيبرانية الإسرائيلية – الإيرانية على أنماط الصداقة و العداوة فى المنطقة العربية؟
- ما هو أثر الحرب السيبرانية الإسرائيلية – الإيرانية على توزيع القوى في المنطقة العربية؟

أهداف وفروض البحث:

يهدف هذا البحث إلى:

1- قياس وتحليل أثر ظاهرة " الحرب السيبرانية الإسرائيلية – الإيرانية " على الأمن الإقليمي العربي منذ 2010م.

2- اختبار الفروض التالية:

- فرض وجود علاقة بين الحرب السيبرانية الإسرائيلية – الإيرانية والاعتماد الأمني المتبادل بين الدول العربية
- فرض وجود علاقة بين الحرب السيبرانية الإسرائيلية – الإيرانية وأنماط الصداقة و العداوة فى المنطقة العربية
- فرض وجود علاقة بين الحرب السيبرانية الإسرائيلية – الإيرانية وتوزيع القوى في المنطقة العربية

3- الوصول إلى استنتاجات وتوصيات بشأن التعامل مع تهديدات الحرب السيبرانية الإسرائيلية – الإيرانية على الأمن الإقليمي العربي

متغيرات البحث:

المتغير المستقل: *الحرب السيبرانية الإسرائيلية – الإيرانية*

المتغير التابع: *تفترض هذه الدراسة أن الدول الأعضاء في جامعة الدول العربية تكون نموذجا لمجمع الأمن الإقليمي، وبالتالي يكون المتغير التابع هو الأمن الإقليمي العربي.*

ويتكون نموذج مجمع الأمن الإقليمي المطبق في هذه الدراسة من ثلاثة مكونات تمثل عوامل المتغير التابع في هذه الدراسة:

1. مدى الاعتماد الأمني المتبادل بين الدول الأعضاء المرتبطة ببعضها البعض بواسطة الهدف الأمني المشترك وتقع داخل نطاق مكاني محدد.
2. نمط الصداقة والعداوة المحدد من خلال العلاقات التاريخية.
3. توزيع القوى الذي تحدده القدرات السيبرانية.

وعلى ذلك تم انتخاب عوامل المتغير التابع التالية لقياس أثر المتغير المستقل عليها:

- الاعتماد الأمني المتبادل
- نمط الصداقة والعداوة
- توزيع القوى

الإطار النظري: نظرية مجمع الأمن الإقليمي

في كتاب الناس والدول والخوف، يُعرف باري بوزان[1] المركب الأمني بأنه "مجموعة من الدول التي ترتبط اهتماماتها الأمنية الأساسية ببعضها البعض بشكل وثيق بحيث لا يمكن اعتبار الأمن الوطني لكل دولة منها واقعا بمعزل عن الأمن الوطني للدول الأخري". يشمل المصطلح كلاً من سمة الأمن ومفهوم الترابط بين الجيران سواء في شكل تنافس أو في شكل مصالح مشتركة. يساعد هذا الإطار في بناء "نهج شامل متعدد المستويات لتحليل مشاكل الأمن...مخصص لإدراج مستوى متوسط من التحليل بين مستوى النظام العالمي... ومستوى الدولة الفردي"[2]. ويوضح كذلك أن كل مستوى يحتفظ بطابعه المميز وديناميكيته لإجراء تحليل منفصل بينما من الممكن أيضاً فحص التفاعلات مع الآخرين من أجل فهم أكثر شمولاً[3].

تم تطوير نظرية مجمع الأمن الإقليمي في اتجاهات مختلفة. كان أحد الاتجاهات هو تحليل المجمعات المتجانسة (تسمى أيضاً المجمعات الخاصة

[1] Barry Buzan, 2007, People, states & fear: An agenda for international security studies in the post-cold war era (2nd ed.), Colchester, UK: ECPR Press

[2] Barry Buzan, 1988, The Southeast Asian security complex. Contemporary Southeast Asia, 10(1), 1–16.

[3] Patrick M. Morgan, 1997, Regional security complexes and regional orders. Regional orders: Building security in a new world, pp.20-42

بقطاع معين لأنها تقدم تحليلاً "لديناميكيات الأمن الخاصة بقطاع معين معزول"[1]، مثل مجمعات أمن الطاقة الإقليمية أو المجمعات الأمنية المائية. تؤكد هذه الأمثلة على أن المجمعات الأمنية الإقليمية الخاصة بقطاعات معينة لها ارتباطها الأساسي بمفهوم الأمن. وبالرغم من أنه تاريخياً، قد ارتبط الأمن في العلاقات بين الدول بشكل أساسي بالتهديدات العسكرية، وبالتالي، فُهم بشكل أساسي على أنه أمن عسكري. تحت "الأجندة الأمنية الموسعة"، الا أن بوزان و وفر ودي وايلد قاموا بتحليل الأمن ليس فقط في نطاق الجيش، ولكن أيضاً في قطاعات الأمن السياسي والاقتصادي والبيئي والمجتمعي[2].

وبناءً على ذلك، يمكن اعتبار التهديدات السيبرانية كجزء من النزاعات العسكرية على أنها قضية أمن قومي رئيسية، وبالتالي يمكن اعتبار القطاع السيبراني أيضاً قطاعاً أمنياً متميزاً ويمكن تكوين مجمعات الأمن السيبراني الإقليمية (مجمعات خاصة بقطاع معين) و تحديدها وفقا لهذا النهج في التحليل. قد تتشكل مثل هذه المجمعات عندما تكون التفاعلات الأمنية الإقليمية المتميزة مرئية بوضوح في الفضاء السيبراني. وبشكل عام، قد لا يختلف تكوينها عن الأنواع الأخرى من المجمعات الخاصة بقطاع معين. وقد تتماشى وقد لا تتوافق مع المجمعات الأمنية الإقليمية في الفضاء المادي. ومع الاعتماد المتزايد على استخدام تقنيات المعلومات، قد يتشكل المزيد من مجمعات الأمن السيبراني الإقليمية، والتي لها أيضاً ديناميكيات أمنية مختلفة عن المجمعات المادية[3].

---

[1] B. Buzan, O. Wæver, & J. de Wilde, 1998, Security: A new framework for analysis. Boulder, CO.: Lynne Rienner, p. 17

[2] B. Buzan, O. Wæver, & J. de Wilde, 1998, op.cit p 168.

[3] Māris Andžāns, 2015, Prospects of Regionalization of Security in the Cyberspace: Case of the Baltic States, Proceedings of the Conference of Turiba University, XIV International Scientific Conference “Creating the Future: Communication, Education, Business". p.p.20-21

الإطار المفاهيمي: التعريف الإجرائي للأمن الإقليمي العربي

في ضوء نظرية مجمع الأمن الإقليمي لبوزان و ويفر ودي وايلد، يمكن تعريف الأمن الإقليمي العربي على أنه: مجموعة المصالح و/أو الشواغل الأمنية المشتركة بين كل أو بعض الدول الأعضاء في جامعة الدول العربية، أو بينها وبين دول الجوار والقوى المؤثرة في الإقليم العربي.

وعليه تكون جامعة الدول العربية، بمثابة المجمع الأمني الإقليمي العربي الرئيس، الذي يمكن أن تتفرع منه مجمعات أمنية إقليمية فرعية تهدف إلي تحقيق مصالح أو التعامل مع شواغل أمنية مشتركة بين كل أو بعض الدول الأعضاء في جامعة الدول العربية عن طريق إحداث تغيرات في أنماط العلاقات الدولية فيما بينها وبين دول الجوار والقوى المؤثرة في الإقليم العربي، خصوصا في أنماط الصداقة والعداوة، والإعتماد الأمني المتبادل، وتوازنات القوى.

وبالنظر إلى ذلك يمكن تعريف مجمع الأمن الإقليمي العربي على أنه مجموعة من كل أو بعض الدول الأعضاء في جامعة الدول العربية، تهدف إلى تحقيق المصالح أو التعامل مع الشواغل الأمنية المشتركة بينها وبين بعضها البعض أو بينها وبين دول الجوار والقوى المؤثرة إقليميا، عن طريق إحداث تغيرات في العلاقات الدولية فيما بينها، خصوصا في أنماط الصداقة والعداوة، والإعتماد الأمني المتبادل، وتوازنات القوى.

الأدبيات السابقة: أثر الحرب السيبرانية على الأمن الإقليمي

أولا: أثر الحرب السيبرانية على الاعتماد الأمني المتبادل

دراسة حالة الحرب السيبرانية الإندونيسية – الأسترالية

تؤثر الحرب السيبرانية تأثيرا مباشرا على الاعتماد الأمني المتبادل للدول، خصوصا تلك الدول المتجاورة أو التي تقع في نفس الإقليم الجغرافي. ولا أدل

على ذلك من حالة الحرب السيبرانية بين الدولتين المتجاورتين إندونيسيا وأستراليا. فخلال عام 2013 وقعت حادثة التنصت على شبكة اتصالات الرئيس الأندونيسي يودويونو من قِبَل أستراليا، والتي كانت بمثابة هجوم سيبراني[1]. ونتج عن تلك الحادثة، ظهور تهديدات أمنية جديدة للجانبين. حيث كان لها تأثيرا مباشرا على الفضاء السيبراني، وسرعان ما أدت إلى اندلاع حرب سيبرانية بين أستراليا واندونيسيا وقعت خلالها العديد من الضحايا بين مواقع حكومية وتجارية من الجانبين [2] .

على إثر ذلك، بدأت أستراليا تهتم بأنظمة الأمن السيبراني كأولوية أساسية في أمنها الدولي. وعلى الجانب الآخر، استقبلت إندونيسيا ذلك الاهتمام على أنه يمثل خطورة على أمنها السيبراني[3]. مما دفع إندونيسيا في عام 2018، إلى توقيع مذكرة تفاهم للتعاون في مجال الأمن السيبراني مع أستراليا خصوصا في مجال الاستجابة للجرائم السيبرانية [4].

وهكذا تسببت ديناميكيات العلاقات الدولية في خلق علاقة ندية وتعاون بين إندونيسيا وأستراليا من رحم الحرب السيبرانية بينهما. حيث أصبح تطوير تكنولوجيا المعلومات أحد مجالات تركيز كلا من إندونيسيا وأستراليا في الحفاظ على الأمن الإقليمي. أثر هذا التطور فى النزاع السيبراني بين

[1] L. Rainie, J. Anderson, & J. Connolly, 2014, Cyber Attacks Likely to Increase, Pew Research Center, Oct 29, accessed Apr 24, 2022, https://pewrsr.ch/3JJbIt8

[2] E. Lukman, 2013, Tech in Asia - Connecting Asia's Startup Ecosystem, www.techinasia.com, Nov 11, accessed Apr 25, 2022, https://bit.ly/36JJZKY

[3] R. Dwinanda, 2018, BSSN to Team up with Australia to Deal with Cyber Attacks, Republika Online, Feb 1, accessed Apr 25, 2022, https://bit.ly/3MrIRLh

[4] Department of Foreign Affairs and Trade, 2018, Memorandum of Understanding between the Government of the Republic of Indonesia and the Government of Australia on Cyber Cooperation, accessed Apr 25, 2022, https://bit.ly/3Lnp6Ve

إندونيسيا وأستراليا، على الاعتماد الأمني المتبادل بين الجانبين. إذ أنه وضح أن إندونيسيا كانت بحاجة إلى أستراليا لتطوير نظام الأمن السيبراني ومواصلة علاقة التعاون والاعتماد الأمني المتبادل فيما بينهما[1].

دراسة حالة الحرب السيبرانية الروسية الإستونية ودول البلطيق

اشتهرت إستونيا على نطاق واسع بـــ "أول هجوم سيبراني منسق على الإطلاق ضد دولة بأكملها"[2] شملت الهجمات التي كان مصدرها روسيا، هجمات ضد موارد الإدارة العامة والشركات الخاصة بما في ذلك البنوك ووسائل الإعلام وشركات الاتصالات والموارد في كل من إستونيا وليتوانيا.

بُعيد تلك الهجمات كرست دول البلطيق اهتماماً كبيراً بالأمن السيبراني، مع التركيز بشكل خاص على النزاعات المحتملة بين الدول في الفضاء السيبراني. حيث نفذت إستونيا العديد من الأنشطة المرتبطة بالصراعات المحتملة بين الدول في الفضاء السيبراني، من أجل تحسين استعدادها للاستجابة للتهديدات السيبرانية. كان أبرزها إنشاء مركز الامتياز للدفاع السيبراني التعاوني NATO CCD COE التابع لحلف شمال الأطلنطي في العاصمة تالين [3].

وعلى الرغم من أن لاتفيا لم تواجه آنذاك حوادث كبرى معروفة علناً في الفضاء السيبراني، لم تستبعد حكومتها حدوث مثل هذه الهجمات في

[1] E.A.P. Lestari, 2021, Complex Interdependence Between Indonesia-Australia Through Cybersecurity Cooperation Post-Indonesia-Australia Cyberwar in 2013, Jurnal Hubungan Internasional, 9(2), pp.178-188. https://doi.org/10.18196/hi.v9i21.10522

[2] Government of Estonia, 2008, Cyber Security Strategy, Ministry of Defence, p. 6, accessed Apr 24, 2022, https://bit.ly/3MC5M6v

[3] Government of Estonia, 2008, op.cit. pp. 10-21

المستقبل[1]. كما كرست ليتوانيا أيضًا اهتمامًا كبيرًا للتهديدات في الفضاء السيبراني على غرار إستونيا ولاتفيا[2].

بالنظر إلى دول البلطيق الثلاث باعتبارها تشكيلًا إقليميا متميزًا في الفضاء السيبراني، من المهم أن نلاحظ أيضًا أوجه الاعتماد الأمني المتبادل فيما بينها. حيث كانت دول البلطيق الثلاث من بين الدول المؤسسة لمركز الامتياز للدفاع السيبراني التعاوني التابع لحلف شمال الأطلسي CCDCOE في تالين. ومنذ عام 2009 أيضا تم تنظيم اجتماعات ثلاثية متخصصة منتظمة تهدف إلى تنسيق سياسات أمن تكنولوجيا المعلومات. تكللت تلك الاجتماعات بتوقيع مذكرة تفاهم بين الأطراف الثلاثة في 4 نوفمبر 2015، لتنسيق سياسات وجهود الدفاع السيبراني الخاصة بهم[3].

وبالنظر إلى أن الدول الثلاث، بشكل عام، تشترك في الاعتماد الكبير على استخدام تقنيات المعلومات، وتتعرض لتهديدات سيبرانية مماثلة، كما أنهم يشاركون سياسات مماثلة تجاه التهديدات السيبرانية، يتم تنسيقها إلى حد معين. فيمكن القول أن دول البلطيق الثلاث تشكل مجمعا إقليميا منفصلاً للأمن السيبراني يمكن اعتباره منطقة فرعية أو مجمعًا فرعيًا لمجمع أمني إقليمي سيبراني أوسع للاتحاد الأوروبي، فمن الواضح من جميع ما سبق أن التهديدات السيبرانية التي فرضتها الهجمات السيبرانية الروسية منذ 2008 قد

[1] European Union Agency for Cybersecurity, 2014, Cyber Security Strategy Of Latvia 2014-2018, enisa.europa.eu, European Union Agency for Cybersecurity, p. 2, accessed Apr 27, 2022, https://bit.ly/3ydaPqr

[2] Government of Lithuania, 2011, the Programme for the Development of Electronic Information Security (Cyber-Security) for 2011–2019. enisa.europa.eu, European Union Agency for Cybersecurity, p. 1, accessed Apr 27, 2022, https://bit.ly/3OIGIwM

[3] Per Concordiam, 2016, Baltic Cyber Cooperation: Estonia, Latvia and Lithuania Sign a Historic Document to Align Their Cyber Defense Policies, Jul 14, accessed Apr27, 2022, https://bit.ly/3xRnmj0

أثرت بشكل واضح وكبير في تعزيز الاعتماد الأمني المتبادل بين استونيا وليتوانيا ولاتفيا[1].

ثانيا: أثر الحرب السيبرانية على أنماط الصداقة والعداوة

دراسة حالة الحرب السيبرانية الإندونيسية – الأسترالية

نعود مجددا إلى حالة الحرب السيبرانية الإندونيسية – الأسترالية، وبالنظر إلى العلاقة بين البلدين نجد أنها شهدت تقلبات ديناميكية من وقت لآخر. في فترة معينة، بدت العلاقات بين البلدين ودية للغاية وتعاونية وداعمة لبعضها البعض. وفي فترات أخرى، أصبحت العلاقة متوترة ومريبة وأقل ودية. ليس من النادر أن تتغير طبيعة العلاقة بين البلدين بسرعة كبيرة وفي فترة زمنية قصيرة جداً. عندما تبنت إندونيسيا سياسة المواجهة مع الغرب، مثلما حدث عندما عارضت إندونيسيا اتحاد ماليزيا مع بريطانيا عام 1963، بدأت العلاقات بين إندونيسيا وأستراليا تشهد توتراً. ازدادت التوترات عندما ضمت إندونيسيا تيمور الشرقية باعتبارها المقاطعة السابعة والعشرين في عام 1976. ومنذ ذلك الحين وحتى الآن، كانت ديناميكيات العلاقات بين إندونيسيا وأستراليا شديدة التقلب. أحياناً ما يكون البلدان قريبين و ودودين للغاية، كما كان الحال في عهد الرئيس سوهارتو ورئيس الوزراء بول كيتنغ في 1992–1995. وغالباً ما تشتد الخلافات بسرعة مثل أوقات رئيس الوزراء جون هوارد والرئيس حبيبي، أو في عهد الرئيس يودويونو و رئيس الوزراء توني أبوت في 2013–2014، وبوجه عام كان نمط الصداقة والعداوة بين البلدين يهيمن عليه جانب العداء أكثر من الصداقة[2].

[1] Māris Andžāns, 2015, op. cit. p-p 14-24

[2] S. M. A. Setyawati, & D. Agussalim, 2015, security Complex Indonesia-Australia dan Pengaruhnya terhadap Dinamika Hubungan Kedua Negara, Jurnal Ilmu Sosial dan Ilmu Politik, 19(2), p-p 111-124

وبسبب الحرب السيبرانية التي وقعت بين الجانبين في نهاية عهد الرئيس يودويونو 2013–2014، رأت اندونيسيا تغليب جانب الصداقة في علاقتها مع أستراليا، لعدة أسباب واقعية، أهمها:

- وجود فارق كبير في تطور القدرات السيبرانية لصالح أستراليا
- الاستفادة من التطور الاسترالي في مجال الأمن السيبراني لتطوير القدرات السيبرانية الإندونيسية
- ضمان تحييد القوى السيبرانية الأسترالية التي نمت بشكل كبير
- تجنب الأخطار السيبرانية حال استخدام تلك القوى في ادارة علاقة العداء بين البلدين
- وللتعاون في مجال الاستجابة للجرائم السيبرانية الخارجية.

مما دفع إندونيسيا في عام 2018، إلى توقيع مذكرة تفاهم للتعاون في مجال الأمن السيبراني مع أستراليا خصوصا في مجال الاستجابة للجرائم السيبرانية[1].[2]

ومنذ ذلك الحين أصبح جانب الصداقة يهيمن بشكل واضح على جانب العداء في نمط الصداقة والعداوة الإندونيسي – الأسترالي. حتى أن رئيس الوزراء الأسترالي سكوت موريسون أعلن خلال عام 2020 أن البلدين يتمتعان بمستوى من "الثقة التي تدعم فقط الصداقات الحقيقية"، كما وصف الرئيس الإندونيسي جوكو ويدودو أستراليا بأنها "أصدق صديق لإندونيسيا". وإن كانت تلك التصريحات لا تخلو من المبالغة إلا أنها ربما تمهد لبناء نوع من الشراكة الإستراتيجية التي سيستفيد منها كلا البلدين خلال العقود القادمة.[3].

[1] R. Dwinanda, 2018, op. cit.
[2] Department of Foreign Affairs and Trade, 2018, op. cit.
[3] D. Engel, 2021, Australia–Indonesia relations: Keeping It Real, The Strategist, Feb 23, accessed Apr 28, 2022, https://bit.ly/3kn425i

دراسة حالة الحرب السيبرانية الروسية الإستونية ودول البلطيق

في حالة دول البلطيق، كان هناك نمط صداقة واضح فيما بينها للتعامل مع التهديدات التي من المحتمل أن تكون صادرة من روسيا – فقد برز دور الأمننة المتعلق بتلك التهديدات في تطوير سياسات الأمن السيبراني لدول البلطيق. واشتركت الثلاث دول في تصور أمني مماثل قائم على أمننة التهديدات السيبرانية الصادرة من روسيا خصوصا بعد الهجمات السيبرانية التي وقعت على استونيا منذ عام 2007[1].

تاريخيا يمكن ترتيب دول البلطيق كجزء من مجمع أمني إقليمي يرتكز على روسيا، وبالرغم من ذلك، فإن الروابط الاستراتيجية والسياسية، وكذلك الخبرة التاريخية، والروابط الثقافية والاقتصادية لا تسمح بفصل دول البلطيق عن بولندا، والدول الأعضاء في الاتحاد الأوروبي والناتو بشكل عام[2].

عندما أشار بوزان و ويفر Buzan وWæver إلى دول البلطيق باعتبارها جزءاً من مجمع الأمن الإقليمي "ما بعد السوفياتي"[3]، لم تكن هذه الدول جزءاً من الناتو والاتحاد الأوروبي وكانت الصداقة تغلب على نمط الصداقة والعداوة بينها وبين روسيا حيث كان لها "علاقات تأمين" متبادلة مع روسيا. حاليا، وبعد توسعها في أمننة الأخطار الروسية وخصوصا السيبرانية منها، هيمن جانب العداء على نمط الصداقة والعداوة بين روسيا ودول البلطيق، وأصبحت دول البلطيق جزءاً من الناتو والاتحاد الأوروبي.

[1] Per Concordiam, 2016, op. cit.
[2] Māris Andžāns, 2014, Securitization in Defining Regional Security Complexes: the Case of the Baltic States (2004–2013), Summary of the Doctoral Thesis
[3] Barry Buzan and Ole Wæver, 2003, Regions and powers, Cambridge, UK: Cambridge University Press, p. 435

ثالثا: أثر الحرب السيبرانية على توزيع القوى

تشير العديد من الدراسات إلى وجود تغير ملحوظ في توازنات القوى نتج عن إعادة توزيع القوى في منطقة البلطيق، فيما بين دول البلطيق وروسيا من ناحية خلال ما يعرف بمجمع الأمن الإقليمي "ما بعد السوفياتي"، وفيما بين دول البلطيق والاتحاد الأوروبي من ناحية أخرى. وقد اتضح ذلك التغير بقوة بعد الحرب السيبرانية الروسية – الإستونية خلال عام 2007[1].

كانت تجربة الحرب السيبرانية الروسية – الإستونية بمثابة "جرس إنذار" لحلف الناتو وأطلقت أنشطة الحلف السيبرانية الموجهة[2]. ففي عام 2008 تمت الموافقة على السياسة الأولى لحلف شمال الأطلسي بشأن الدفاع السيبراني. وفي عام 2010، تبنى الناتو مفهوماً استراتيجياً جديداً تضمن جدول الأعمال السيبراني لأول مرة. اعتباراً من ذلك العام، أصبح الإنترنت جزءاً كاملاً من أجندات الناتو، وأصبح لاحقًا جزءاً من مهمة الدفاع الجماعي الأساسية[3].

في دراسة لادوارد رودس بعنوان:"الرؤية الأمريكية لهيكل الأمن البلطيقي: فهم مبادرة أوروبا الشمالية" أكد أن اندماج المناطق الحدودية في شمال غرب روسيا في مجموعة متنوعة من الروابط الاقتصادية والسياسية والاجتماعية

[1] M. Prucková, a 2022, Regional Security Complex Theory and the Baltic states. How Have Their Relations with the Russian Federation Changed after the Bronze Year 2007 incident? Security Outlines, Mar 23, accessed May 11, 2022, https://bit.ly/3L5qjzr

[2] Ondřej Rojčík, 2019, "Achievements and Failures of NATO Cyber Policies", In NATO at 70: Outline of the Alliance Today and Tomorrow, edited by R. Ondrejcsák, T. H. Lippert, 179-192. Bratislava: STRATPOL

[3] M. Prucková b, 2022, Cyber Attacks and Article 5 – a Note on a Blurry but Consistent Position of NATO, ccdcoe.org, accessed May 11, 2022, https://bit.ly/3FJ6qgr

والثقافية سيقلل حتماً من قوة ونفوذ موسكو، مما يزيد من إضعاف سلطة وشرعية الدولة الروسية المتوترة بشدة[1].

منذ استقلالها وزيادة اندماجها في الناتو والاتحاد الأوروبي، كانت روسيا تفقد نفوذها باستمرار على دول البلطيق. ومما لاشك فيه فان إستونيا ولاتفيا وليتوانيا مندمجة بعمق في الهياكل الأوروبية الأطلسية اليوم[2]، وبالتالى تبتعد سياسياً وثقافياً عن النفوذ الروسي. وبالتالي، لم تعد روسيا تعتبر دول البلطيق جزءاً من فضاء ما بعد الاتحاد السوفيتي ولكن على أنهم "شمال أوروبا"[3] .

من الواضح أن ذلك التغير في توازنات القوى قد بدأ قبل الهجمات السيبرانية عام 2007. تسارع الانجراف بعد هجمات عام 2007 السيبرانية وخلال الحرب في جورجيا وتصاعد مرة أخرى في عام 2014 عندما ضمت روسيا شبه جزيرة القرم[4].

فاستناداً إلى علاقاتها عبر الأطلسي، أصبحت دول البلطيق تمتلك القدرة على الردع الاستراتيجي، لاسيما في المجال السيبراني[5].

أثر الحرب السيبرانية الإسرائيلية – الإيرانية على الأمن الإقليمي العربي

تمهيد

باستقراء محصلة الخبرات السابقة للدول التي شكلت فيما بينها مجمعات للأمن الإقليمي، والتي أوردنا بعضها في الدراسات السابقة، يمكن رصد عدة تغيرات

[1] E. Rhodes, 2000, The American Vision of Baltic Security Architecture: Understanding the Northern Europe Initiative, Baltic Defence Review, 4, pp.91-112, accessed May 11, 2022, https://bit.ly/3w6jnOl

[2] Una Bergmane, 2020, Fading Russian Influence in the Baltic States, Orbis 64(3), p-p 479-488

[3] Dmitry Gorenburg, 2019, Russian Strategic Culture in a Baltic Crisis, George C. Marshall European Center for Security Studies, Mar 2019 , accessed May 11, 2022, https://bit.ly/39cgySy

[4] Una Bergmane, 2020, op. cit.

[5] M. Prucková, a 2022, op. cit.

في العلاقات الخارجية تمثل نمطا مشتركا لسلوك تلك الدول نابع من تأثير الحروب السيبرانية على الأمن الإقليمي لتلك الدول.

فبمجرد أن تلوح الحرب السيبرانية في الأفق أو تزداد أخطار الهجمات السيبرانية في المحيط الإقليمي، تشرع الدول، التي تشغل ذلك المحيط الإقليمي، في إحداث تَغَيُرات في علاقاتها الخارجية عن طريق انتهاج كل أو بعض السلوكيات التالية:-

- تسعى إلى تعزيز وتطوير قدراتها السيبرانية الذاتية، خصوصا فيما يتعلق بقدرات الرصد والدفاع والردع السيبراني.
- تسعى إلى تعزيز القدرات السيبرانية على المستوى الإقليمي، فتحرص على إبرام الاتفاقيات ومذكرات التعاون وتنخرط في الجهود والفعاليات والكيانات الإقليمية والدولية في مجال الأمن السيبراني، مثل كيانات العمل السيبراني المشترك خصوصا في مجالات الرصد والدفاع والردع السيبراني.
- تعيد ترتيب أنماط الصداقة والعداوة في محيطها الإقليمي بناءا على مستوى التعاون أو التنافس فيما بينها في مجال الدفاع والأمن السيبراني، أو بناءا على ما تتعرض له من أخطار سيبرانية.

و بانتهاج الدول مثل هذه السلوكيات في محيطها الإقليمي، فهي تُحدث تغيرا في نمط علاقاتها الخارجية ينتج عنه ازديادا في الاعتماد الأمني المتبادل، و تغيرات في أنماط الصداقة والعداوة، وفي توازنات القوى، بما يؤدي إلى تكوين مجمعا للأمن الإقليمي السيبراني فيما بينها.

وبالنظر إلى الأخطار والمخاطر التي خلفتها الحرب السيبرانية الإسرائيلية – الإيرانية على دول الدول العربية، كان من الطبيعي أن تكون استجابة الدول العربية لتلك الأخطار والمخاطر متفاوتة، وذلك لتفاوت درجة تعرض وتأثر وأمننة كل من الدول العربية لتلك الأخطار. وحيث أن أغلب الهجمات السيبرانية الإيرانية استهدفت منطقة الخليج العربي، مثل الهجوم على أرامكو السعودية عام 2012، والهجوم الذي استهدف راس غاز القطرية عام 2012، كانت دول الخليج العربي الأكثر استجابة من بين الدول العربية للأخطار والمخاطر التي خلفتها الحرب السيبرانية الإسرائيلية – الإيرانية.

في دراستهما التى نشرت عام 2018[1]، جادل كل من Russell Seeger & Dania Thafer أنه: "من خلال تحليل مؤشرات متعددة للتأهب السيبراني العام مثل التشريعات الوطنية، والتصنيفات من قبل المنظمات الدولية، والتعاون بين الدول، وُجِد أن قطر والإمارات العربية المتحدة وسلطنة عمان هي القوى السيبرانية الرائدة في منطقة الخليج بينما كانت الكويت، البحرين والمملكة العربية السعودية متأخران نسبيًا.

وحيث أن المملكة العربية السعودية تعد أكثر الدول العربية تعرضا للهجمات السيبرانية، وتأثرا بالحرب السيبرانية الإسرائيلية – الإيرانية، فمن الطبيعي أن تكون أكثر الدول استجابة لأخطار ومخاطر تلك الحرب. لذلك يركز هذا

[1] Russell Seeger & Dania Thafer, 2018, “The New Battlefront: Cyber Security across the GCC – Gulf International Forum.” Gulfif.org, Oct 29, accessed Nov 30, 2022, https://bit.ly/3XNimWW

الفصل على دراسة حالة المملكة العربية السعودية لبيان الإجراءات التي اتخذتها علي وجه التفصيل استجابة للمخاطر التي تعرضت لها جراء الحرب السيبرانية الإسرائيلية–الإيرانية.

أولا: أثر الحرب السيبرانية الإسرائيلية – الإيرانية على الاعتماد الأمني المتبادل بين الدول العربية

تعزيز وتطوير القدرات السيبرانية الذاتية

تعتمد القدرات السيبرانية الذاتية للدول على مدى تطور وانتشار تقنيات الاتصال وتكنولوجيا المعلومات بين شعوبها. وخلال العقد الأول من الألفية الثانية، عانت شعوب المنطقة العربية من تأخر شديد في انتشار تقنيات الاتصال وتكنولوجيا المعلومات فيما بينها. وهي حقيقة أكدتها جميع التقارير الدولية الصادرة في هذا المجال، حيث أشار معظمها إلى انخفاض مؤشر مهارة استخدام التقنية في جميع الدول العربية، وإلى وجود فجوة بين الدول العربية ودول العالم المتقدم من حيث المهارة التكنولوجية[1]. وربما كان ذلك هو السبب الرئيسي وراء اختيار المنطقة العربية كساحة لأحد أكبر الحروب

[1] ITU, 2013, MEASURING THE INFORMATION SOCIETY 2013, op.cit. And
B. Bilbao-Osorio, S. Dutta & B. Lanvin, 2014, Insight Report: the Global Information Technology Report 2014, Rewards and Risks of Big Data, World Economic Forum, accessed Feb 22, 2022, https://bit.ly/3verZ5v. And
ABI Research, 2014, GLOBAL CYBERSECURITY INDEX. ITU, op.cit.

السيبرانية وأكثرها تأثيرا في مجال العلاقات الدولية، وجعلها قبلة ومنصة وساحة مهيأة للهجمات والجرائم السيبرانية[1].

وبمجرد أن لاحت الحرب السيبرانية الإسرائيلية – الإيرانية في أفق الإقليم العربي، وتكشفت أبعادها وأهدافها، بدأت الدول العربية تنتبه إلى أهمية تطوير قدراتها السيبرانية الذاتية خصوصا المملكة العربية السعودية، لكونها أكبر الدول العربية تعرضا للهجمات السيبرانية[2]. حيث شرعت كل دولة في تطوير البنية التشريعية وبنية الاتصال وتكنولوجيا المعلومات الخاصة بها، وذلك تمهيدا لإحداث تطور ملموس في قدراتها السيبرانية الذاتية.

باعتبارها حليفا مهما للولايات المتحدة الأمريكية وراعيا لمصالحها الاستراتيجية في المنطقة، وبسبب نمط العداء التاريخي بينها وبين إيران، تم استهداف البنية التحتية الوطنية الحيوية للمملكة العربية السعودية عدة مرات خلال الحرب السيبرانية الإسرائيلية – الإيرانية[3]. ومنذ عام 2017 أصبحت المملكة العربية السعودية هدفًا لأكبر عدد من الهجمات السيبرانية في الشرق الأوسط. حيث تعرضت المملكة إلى ما يقرب من 60 مليون هجوم سيبرانيا يومياً تستهدف مؤسسات القطاعين العام والخاص بهدف زعزعة استقرار الاقتصاد[4].

---

[1] S. Ghernaouti-Hélie, 2008, From risk management to information security policies and practices: a multi perspective framework for ICT security effectiveness. Geneva: International Telecommunication Union, Apr 14, accessed Feb 22, 2022, https://bit.ly/3vdfWoO

[2] Nermeen Abbas, 2018, op. cit.

[3] Kate Fazzini, 2019, "The Saudi Oil Attacks Could Be a Precursor to Widespread Cyberwarfare — with Collateral Damage for Companies in the Region." CNBC, Sep 21, accessed Nov 5, 2022, https://cnb.cx/3U8JWfj

[4] Ibrahim al-Hussein, 2017, "60 Million Cyber Attacks Targeted Saudi Arabia in One Year." Al Arabiya English, May 2, accessed, Nov 5, 2022, https://bit.ly/3UnOs9k

أظهر استطلاع حديث أجرته Tenable أن 95٪ من الشركات السعودية واجهت تهديدات سيبرانية تؤثر على عملياتها خلال عام 2019. وكشف الاستطلاع أيضاً أن 85٪ من المشاركين السعوديين أشاروا إلى ارتفاع كبير في التهديدات السيبرانية في العامين 2018 و2019 مما أدى إلى فقدان البيانات أو مدفوعات الفدية أو الخسائر المالية[1]. علاوة على ذلك، خلص تقرير المعهد الإسرائيلي لدراسات الأمن القومي إلى أن المملكة العربية السعودية من بين الدول الأكثر استهدافاً عبر الإنترنت في العالم، ويعتقد أن إيران هى المصدر الرئيسي لهذه الهجمات. على سبيل المثال، 42٪ من الهجمات السيبرانية التي نفذتها مجموعة APT33 الإيرانية كانت موجهة ضد المملكة. كما سلط التقرير الضوء على أن المملكة العربية السعودية لا تزال معرضة بشدة للهجمات السيبرانية حيث أوضحت دراسة حديثة أن أربعة فقط من أصل 10 من قادة الأعمال السعوديين ذكروا أن كياناتهم مستعدة للتعامل مع التهديدات السيبرانية[2].كما كشف تقرير حديث لـــ Bitdefender أن مجموعة APT الإيرانية استهدفت وسائل النقل الجوي والهيئات العامة في الكويت وفي المملكة العربية السعودية[3].

وقد لعبت هذه الأحداث دوراً حاسماً في تجديد المخاوف المتعلقة بالأمن السيبراني في المملكة. وجعلت المملكة العربية السعودية عازمة على تحسين

[1] Hala Tashkandy, 2020, Cyberattacks hit 95% of Saudi businesses last year, says study, Arab News, Aug 12, accessed Nov 5, 2022, https://arab.news/j4pt5

[2] Yoel Guzansky & Ron Deutch, 2019, How Prepared is Saudi Arabia for a Cyber War? INSS Insight No. 1190, July 10, accessed Nov 5, 2022, https://bit.ly/3icsOHl

[3] Liviu Arsene, 2020, Iranian Chafer APT Targeted Air Transportation and Government in Kuwait and Saudi Arabia, bitdefender.com, May 21, accessed Nov 5, 2022, http://bit.ly/3u4SHvv

وضع الأمن السيبراني في المستقبل. ونتيجة لذلك، أصبح جاهزية الأمن السيبراني أحد مؤشرات الأداء الرئيسية لمبادرات التحول في جميع أنحاء المملكة. واتخذت المملكة خطوات رئيسية في التخفيف من التعرض المستقبلي للتهديدات السيبرانية[1]، وفي مجال تعزيز وتطوير القدرات السيبرانية الذاتية. مما مكن المملكة العربية السعودية من تحقيق المرتبة الثانية عالمياً في مؤشر الأمن السيبراني وفقا لتقرير الكتاب السنوي للتنافسية العالمية لعام 2022 الصادر عن مركز التنافسية العالمي.

ووفقا للتقرير كانت أبرز العوامل التي أسهمت في تحقيق هذا الإنجاز:

- إنشاء الأكاديمية الوطنية للأمن السيبراني
- تنفيذ البرامج التدريبية والتمارين السيبرانية
- إطلاق مسرع أعمال لدعم الشركات الناشئة في مجال الأمن السيبراني
- إصدار الأطر التنظيمية لدعم بناء الكوادر السيبرانية
- وجود حوكمة فاعلة لمنظومة الأمن السيبراني
- توفير بيئة تشريعية متينة لقطاع الأمن السيبراني[2]

تعزيز وتطوير القدرات السيبرانية على المستوى الإقليمي

يعتمد تطوير القدرات السيبرانية على المستوى الإقليمي في الأساس على المشاركة في الفعاليات والتكتلات الدولية وإبرام إتفاقيات الشراكة والاستثمار ومذكرات التعاون فيما بين دول الإقليم وبينها وبين دول العالم في مجال تبادل الخبرات والمعلومات ومكافحة ورصد الهجمات السيبرانية.

---

[1] IDC, 2020. "Cybersecurity and its impact on digital Saudi" idc.com, accessed Nov 5, 2022, https://bit.ly/3E4A68y

[2] وكالة الأنباء السعودية، 2022، عام / المملكة تُحقق المرتبة الثانية عالمياً في مؤشر الأمن السيبراني وفق تقرير «الكتاب السنوي للتنافسية العالمية لعام 2022، 15 يونيو، متاح بالرابط: https://www.spa.gov.sa/2362614، تاريخ الدخول: 28 أكتوبر 2022

وفيما يلي أهم الخطوات التي اتخذت في مجال تعزيز وتطوير القدرات السيبرانية للمملكة العربية السعودية على المستوى الإقليمي:

- خلال شهر سبتمبر من العام 2013، أقر مجلس الوزراء السعودي تطبيق النظام "القانون" الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون الخليجي[1].
- وفي التاسع من فبراير عام 2017، شاركت المملكة العربية السعودية في الاجتماع الأول للجنة الدائمة للأمن السيبراني بدول مجلس التعاون الخليجي[2].
- في الثلاثاء 29 مارس 2022، وقع الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز مذكرة تفاهم مع المنظمة العربية للتربية والثقافة والعلوم "الألكسو"، حيث اتفق الطرفان على التعاون في مجال الأمن السيبراني[3].
- خلال أبريل من العام 2022، وقّعت الهيئة الوطنية للأمن السيبراني مذكّرة تفاهم مع الأمانة العامة لمجلس التعاون لدول الخليج العربية، بهدف تعزيز التعاون بين الطرفين في مختلف الموضوعات ذات الصلة بمجال الأمن السيبراني، وتوظيف إمكانياتهما وخبراتهما بما يحقق المصلحة المشتركة[4].

---

[1] مشعل الحميدان، 2013، 39 مادة قانونية لمكافحة الجرائم المعلوماتية الخليجية، الاقتصادية، 11 سبتمبر، متاح بالرابط: http://bit.ly/3hqLwur، تاريخ الدخول: 9 نوفمبر 2022

[2] الخليج أونلاين، 2017، انعقاد أول اجتماع للجنة الخليجية للأمن السيبراني بالإمارات، 10 فبراير، متاح بالرابط: https://perma.cc/TZL3-XDEQ، تاريخ الدخول: 19 نوفمبر 2022

[3] موقع الاتحاد السعودي للأمن السيبراني، 2022، الأمن السيبراني السعودي و"الألكسو" يواجهان المخاطر المعلوماتية في العالم العربي، 29 مارس، متاح بالرابط: https://safcsp.org.sa/news-elexo، تاريخ الدخول: 8 نوفمبر 2022

[4] موقع الهيئة الوطنية للأمن السيبراني، 2022، الهيئة الوطنية للأمن السيبراني توقع مذكّرة تفاهم مع الأمانة العامة لمجلس التعاون لدول الخليج العربية، 12 أبريل، متاح بالرابط: https://nca.gov.sa/news?item=6، تاريخ الدخول: 7 نوفمبر 2022

- في 26 يوليو 2022، ترأست المملكة ممثلة في الهيئة الوطنية للأمن السيبراني أعمال الدورة السابعة للجنة الدائمة للأمن السيبراني بمجلس التعاون لدول الخليج العربية، التي عُقدت افتراضياً يومي الثلاثاء والأربعاء 26 – 27 يوليو 2022م[1].
- في 23 من أكتوبر 2022، نفذت المملكة العربية السعودية بمشاركة الجهات المختصة بمجال الأمن السيبراني في دول مجلس التعاون لدول الخليج العربية والأمانة العامة للمجلس «التمرين الخليجي للأمن السيبراني». وذلك على هامش الاجتماع الأول للجنة الوزارية للأمن السيبراني في مجلس التعاون الذي تستضيفه المملكة ممثلة بالهيئة الوطنية للأمن السيبراني، والمنعقد في مقر الأمانة العامة لمجلس التعاون لدول الخليج العربية بالرياض[2].

ثانيا: أثر الحرب السيبرانية الإسرائيلية – الإيرانية على أنماط الصداقة و العداوة فى الإقليم العربي

حتى مطلع الألفية الجديدة كان نمط العلاقات الدولية السائد تاريخيا بين الدول العربية وإسرائيل يغلب عليه طابع العداء. وذلك بسبب نكبة 1948 وما تبعها من تداعيات إنشاء الدولة الإسرائيلية على الأراضي الفلسطينية المحتلة. وبالرغم من تفاوت حدة العداء بين إسرائيل وبين الدول العربية منفردة، إلا أن الموقف العربي الرسمي الموحد قد بدا واضحا في هذا المجال، حيث ربط السلام وتطبيع العلاقات مع إسرائيل بعدة شروط حاسمة اعتبرت إسرائيل

[1] موقع الهيئة الوطنية للأمن السيبراني، 2022، المملكة ترأس اجتماع اللجنة الدائمة للأمن السيبراني في مجلس التعاون لدول الخليج العربية، 28 يوليو، متاح بالرابط:
https://nca.gov.sa/news?item=227، تاريخ الدخول: 6 نوفمبر 2022

[2] موقع الهيئة الوطنية للأمن السيبراني، 2022، بمشاركة الجهات المختصة بدول مجلس التعاون انطلاق «التمرين الخليجي للأمن السيبراني» في الرياض، 23 أكتوبر، متاح بالرابط:
https://nca.gov.sa/news?item=341، تاريخ الدخول: 6 نوفمبر 2022

أغلبها مستحيل التنفيذ، و على رأسها الانسحاب الكامل من الأراضي العربية المحتلة وعودة اللاجئين. وتجلي ذلك في أكثر المبادرات العربية مرونة على الإطلاق، وهي مبادرة السلام التي أطلقها العاهل السعودي الملك عبدالله بن عبدالعزيز، وأقرتها القمة العربية التي عقدت في بيروت عام 2002 بالإجماع[1].

من ناحية اخرى، من المرجح أن نمط العداء التاريخي بين إيران والمملكة، وكون المملكة أهم الحلفاء الاستراتيجيين للولايات المتحدة الأمريكية بالمنطقة، كان أحد أسباب توسيع جبهة الحرب السيبرانية الإسرائيلية الإيرانية لتشمل أهداف حيوية سعودية[2] .

أصدقاء اليوم أعداء الأمس

في دراسة نشرت عام 2019 [3] بعنوان "تسهيل شروط التطبيع بين المملكة السعودية وإسرائيل، خلال الفترة من 2015–2018" للباحثين: مريم جميلة، حافظ عليا فكرة، و ذو الكفل حرزة، رصدوا فيها أنه تم خلق مجموعة من الظروف التي من شأنها تسهيل جهود التطبيع بين المملكة العربية السعودية وإسرائيل خلال الفترة ما بين عامي 2015–2018. وكان من أهم تلك الظروف:

[1] سي ان ان، 2020، السعودية تتمسك بها.. ما هي بنود المبادرة العربية للسلام مع إسرائيل؟ سي ان ان العربية، 20 أغسطس، متاح بالرابط: https://cnn.it/3VsmppN، تاريخ الدخول: 8 نوفمبر 2022

[2] BBC Monitoring, 2017, Iran and Saudi Arabia: Friends and foes in the region, BBC News, Nov 10, accessed Nov 26, 2022, http://bit.ly/3U5jIcF.
And
Yoel Guzansky & Ron Deutch, 2019, op. cit.

[3] M .Jamilah, H.U. Fikra, & Z. Harza, 2019, Facilitating Conditions of Saudi Arabia–Israel Normalization in 2015-2018, Journal of Diplomacy and International Studies, 2(01), pp.38-51

- تطبيق نظرية **تفكيك الأمننة** Desecuritisation و حدوث تغير في لغة ولي العهد السعودي الأمير/ محمد بن سلمان، يوحي بتفكيك أمننة الأخطار الإسرائيلية على الأمن الإقليمي العربي.
- و زيادة النفوذ الجيوسياسي لإيران الذي جعل الظروف اللازمة للتطبيع مهمة للغاية.

وجادل الباحثون بأنه خلال تلك الفترة كانت السعودية هي الطرف الذي لم يتوقف عن التعبير عن إمكانية تحقيق تطبيع العلاقات بين العالم العربي وإسرائيل. حيث أنه لا يمكن للسعوديين أن ينكروا الإسهام الهائل للمشاركة الإسرائيلية المتفوقة في تطوير تكنولوجيا الإنترنت وفي مجال الفضاء السيبراني. وبأن السعوديين يحتاجون إلى هذين الأمرين لنجاح مشروع نيوم، وهذا يدل على أن إنجاز مشروع نيوم يتطلب علاقة جيدة مع إسرائيل بسبب الموقع الجغرافي للمشروع وأيضاً بسبب احتياج السعودية للتكنولوجيا التي تملكها إسرائيل.

من ناحية أخرى، لم يتم إخماد الموقف العدائي للمملكة العربية السعودية مع إيران منذ الثورة الإيرانية عام 1979. حيث أدى تراجع صدام حسين في العراق، وظهور الربيع العربي إلى زيادة الصدام بين البلدين. من ناحية أخرى، كان عداء إسرائيل لإيران سببه تورطها في الحرب الإسرائيلية في لبنان، لكن كلاً من السعودية وإسرائيل، لديهما هدف واحد لقمع نفوذ إيران في الشرق الأوسط. وبالتالي، فإن التهديد الأمني الذي تريد السعودية وإسرائيل توقعه هو تهديد أمني واحد بسبب النفوذ الجيوسياسي لإيران، ومقاومة إسرائيل لإيران التي ظهرت منذ الربيع العربي جعلت المصالح الأمنية للمملكة العربية السعودية تتشابه مع المصالح الأمنية لإسرائيل.

الاتفاق الإبراهيمي Abraham Accords

في 15 سبتمبر 2020، شهد العالم حقبة جديدة من العلاقات الإسرائيلية-العربية، حيث فتحت الإمارات والبحرين علاقات دبلوماسية مع إسرائيل، فيما يعرف بالاتفاق الإبراهيميAbraham Accords الذي يهدف إلى تعظيم المصالح المشتركة ومعالجة القضايا الأمنية لتشكيل جبهة جديدة ضد التهديدات الإيرانية. وبالتالي أصبح التعاون المشترك بين إسرائيل ودول الخليج أكثر وضوحًا من أي وقت مضى، لا سيما في الفضاء السيبراني، حيث يشتركان في عدو مشترك واحد. من خلال الشراكة الجديدة ستستفيد دول الخليج من القدرات السيبرانية الإسرائيلية المتقدمة والتكنولوجيا في تأمين بنيتها التحتية الحيوية ضد التهديدات الإيرانية بينما ستفتح دول الخليج أسواقها المربحة لشركات الأمن السيبراني والمستثمرين الإسرائيليين. وبالتالي، فإن التعاون التقني المشترك وتبادل المعلومات سيمكن كلا الجانبين من معالجة الأنشطة السيبرانية الإيرانية بشكل أفضل.

على مدى العقد الماضي، تعاونت دول الخليج بهدوء مع إسرائيل في مجال الأمن السيبراني. على سبيل المثال، وفقًا لعضو الكنيست الإسرائيلي السابق إريل مارغاليت، ساعدت شركات الأمن السيبراني الإسرائيلية المملكة العربية السعودية في إصلاح الضرر الناجم عن الهجوم السيبراني على أرامكو السعودية الذي دمر حوالي 30 ألف محطة عمل وشكل أكبر هجوم سيبراني تجاري في ذلك الوقت[1]. وفي عام 2019، دعت البحرين مسؤولاً إسرائيلياً

[1] Orr Hirschauge, 2017, Former Israeli Parliamentarian Says Homegrown Companies Can Help Build Saudi Future City Neom, calcalistech.com, Nov 21, accessed Nov 26, 2022, http://bit.ly/3GW7dx0

رفيعاً لحضور مؤتمر أمني لمناقشة السبل الممكنة لتشكيل تحالف ضد تدخلات طِهران في المنطقة[1].

ووفقًا لصحيفة جيروزاليم بوست، تتفاوض الشركات الإسرائيلية سراً مع صندوق الاستثمارات العامة السعودي بشأن السبل الممكنة لتبادل الخبرات والمهارات التقنية اللازمة لإكمال مدينة نيوم السعودية الذكية[2].

مما سبق، يمكن استنتاج أن ارتفاع الهجمات السيبرانية ضد أهداف دول مجلس التعاون الخليجي والمملكة العربية السعودية على وجه الخصوص، أدى إلى تسريع عملية إنشاء إطار عمل تعاوني بينها وبين إسرائيل، بهدف تعزيز المواءمة والتنسيق لمواجهة التهديدات السيبرانية المحتملة من خلال تبادل المعلومات والتقنيات والخبرات التكنولوجية في مجال الأمن السيبراني. وبالتالي شكل ذلك تغيرا ملحوظا في نمط الصداقة والعداوة بين دول مجلس التعاون الخليجي والمملكة من ناحية وإسرائيل من ناحية أخرى، حيث كونوا جميعا جبهة واحدة في مواجهة إيران.

وفي المقابل تم تشكيل تحالف سيبراني آخر في المنطقة بين إيران وروسيا. في 26 يناير 2021، وقعت إيران وروسيا اتفاقية تعاون مشتركة في مجال الأمن السيبراني تشمل نقل التكنولوجيا والتدريب وتبادل المعلومات والتعاون الثنائي خلال الأحداث الدولية[3]. فمن خلال الاتفاق يمكن لروسيا تزويد إيران بأنظمة الدفاع السيبراني والتدريب لمعالجة أوجه القصور الدفاعية لديها، مما

[1] Reuters Staff, 2019, Senior Israeli official attends Bahrain security meeting focusing on Iran, Reuters, Oct 21, accessed Nov 26, 2022, http://bit.ly/3iem1gq

[2] M. Schindler, 2017, Israeli companies working with Saudi Arabia? The Jerusalem Post, Oct 26, accessed Nov 26, 2022, http://bit.ly/3EIdlGy

[3] Russian News Agency, 2021, Russia, Iran sign agreement on cyber security cooperation, TASS, Jan 26, accessed Nov 26, 2022, https://tass.com/politics/1248963

سيجعل الهجمات السيبرانية المحتملة ضد الأهداف الإيرانية أكثر تكلفة وصعوبة في المستقبل. علاوة على ذلك، يمكن لإيران بدورها توفير التقنيات الروسية لوكلائها في المنطقة، مثل حزب الله وميليشيا الحوثي، والتي يمكن استخدامها ضد أهداف خليجية أو إسرائيلية. أخيراً، يمكن إرسال فرق سيبرانية روسية إلى إيران لمراقبة الشبكات الإيرانية وفحص البرامج الضارة الأمريكية أو الإسرائيلية المستخدمة ضد إيران، مما يساعد كلا البلدين على تعزيز قدراتهما الدفاعية ضد الهجمات المستقبلية[1].

ثالثا: أثر الحرب السيبرانية الإسرائيلية – الإيرانية على توزيع القوى في الإقليم العربي

بعد هجوم ستوكسنت، الذي كشف عن ضعف وهشاشة منظومة الأمن السيبراني الإيرانية، طورت إيران من قدراتها السيبرانية، وخلال العقد التالي، ردت على الولايات المتحدة وإسرائيل[2]. ومع تحسين أنظمة الأمن السيبراني الخاصة بهم، استهدف المتسللون الإيرانيون بشكل متزايد دول الخليج الأقل حماية. كذلك قام خبراء الإنترنت الإيرانيون بتدريب المتسللين الموجودين بين وكلائهم و شجعوهم على شن هجمات ضد أعدائهم. وفي عام 2015، استهدف الجيش السيبراني اليمني وزير الخارجية السعودي وسرب وثائق سرية على

[1] O. Wechsler, 2021, The Iran-Russia Cyber Agreement and U.S. Strategy in the Middle East, Council on Foreign Relations. Mar 21, accessed Nov 26, 2022, https://bit.ly/3XwZJXf

[2] J. Work & R. Harknett, 2020, Troubled vision: Understanding recent Israeli–Iranian offensive cyber exchanges. Atlantic Council, Jul 22, accessed Nov 26, 2022, http://bit.ly/3XAtXZl

وسائل الإعلام الإيرانية[1]. مما يشير إلى تغير في توازنات القوى السيبرانية في منطقة الشرق الأوسط لصالح إيران.

لطالما كان الفضاء السيبراني العربي مسرحا مفتوحا للهجمات السيبرانية، فظهور القدرات التكنولوجية والرقمية في دول الخليج العربي فتح ثغرات جديدة دفعت الكثير إلى استهدافها بالهجمات السيبرانية. وبالرغم من الخطوات الحثيثة التي اتخذتها في مجال تطوير القدرات السيبرانية، إلا أن دول الخليج لم تكن قادرة حتى وقت قريب على تطوير نظام شامل للأمن السيبراني لحماية الهياكل الحكومية والمرافق الحيوية والشركات والأفراد من مثل هذه التهديدات. على سبيل المثال، وفقًا لمعهد بوتوماك في تقريره الصادر عام 2017، كانت المملكة العربية السعودية "لا تزال غير مستعدة بشكل كاف في جميع العناصر الأساسية للجاهزية السيبرانية"[2]. حيث فشلت الاستراتيجية الوطنية السعودية لأمن المعلومات في تقديم إرشادات محددة وبنية متسقة للأمن السيبراني. في كثير من الأحيان، كانت العديد من الوزارات والشركات والكيانات الأخرى تقوم بتطوير استراتيجياتها السيبرانية الخاصة بها بشكل مستقل، مما يؤدي إلى خلق فجوات خطيرة في الأمن السيبراني الوطني. علاوة على ذلك، مع أزمة فيروس كورونا، زادت التهديدات السيبرانية مع تكاثر هجمات التصيد الاحتيالي والبرامج الضارة. في مثل هذه البيئة، احتاجت دول الخليج إلى شركاء ذوي خبرة لتعزيز أنظمة الأمن السيبراني لديها[3].

[1] Sputnik International, 2015, Yemeni Hackers Reveal Top Secret Docs in Saudi Government Cyber Attack, May 22, accessed Nov 26, 2022, https://sputniknews.com/20150522/1022475567.html

[2] M. Hathaway, F. Spidalieri, & F. Alsowailm, 2017, Kingdom of Saudi Arabia cyber readiness at a glance, Potomac Institute for Policy Studies, accessed Nov 30, 2022, https://bit.ly/3VmrK2b

[3] Kristian Alexander, 2020, “Israeli-Gulf Cyber Cooperation.” Modern Diplomacy, Dec 23, accessed Nov30, 2022, https://bit.ly/3UluVpu

من ناحية أخرى أدركت دول الخليج أن إسرائيل هى الدولة الأكثر تقدماً في الشرق الأوسط من حيث الأمن السيبراني. حيث صرح الرئيس التنفيذي لشركة الأمن السيبراني الإماراتية DarkMatter أن "الدولة الوحيدة في المنطقة التي تتمتع بقوة في مجال الأمن السيبراني هى إسرائيل[1].

وبالتالي، لاحداث تغير ايجابي في توازنات القوى السيبرانية في منطقة الخليج العربي والتخفيف من حدة نقاط الضعف السيبراني لدول الخليج، كان الحصول على الخبرة الإسرائيلية في الاستخبارات والحرب السيبرانية (حتى قبل الاتفاق الإبراهيمي Abraham accords) عاملا هاما. حيث ادعت إسرائيل ودول الخليج رسمياً أن تعاونهما يهدف إلى صد التهديدات الإيرانية في الفضاء السيبراني. إلا أن دول مجلس التعاون الخليجي كانت ولازالت تهدف إلى الإستفادة من الخبرة الإسرائيلية لتعزيز قدراتها التقنية الخاصة بالأمن السيبراني[2].

وفي النهاية من المرجح أن يؤدي التعاون الإسرائيلي مع دول الخليج في مجال الأمن السيبراني إلى تغير ملحوظ في توازنات القوى السيبرانية في الإقليم العربي.

[1] Jonathan Fenton-Harvey, 2019, "UAE-Israel Cyber-Spying Aids Emirati Influence, Repression." Inside Arabia, Dec 27, accessed Nov 30, 2022, https://bit.ly/3uehUn7

[2] Kristian Alexander, 2020, op. cit.

الخاتمة:

النتائج: المملكة العربية السعودية ودول الخليج تشكل مجمعا إقليميا للأمن السيبراني

وفقًا لـــ "نظرية مجمع الأمن الإقليمي"، والتي تنص على أن ديناميكيات الأمننة، بما في ذلك بناء التهديدات، يمكن أن تعمل على المستوى الإقليمي بين مجموعات معينة من الدول. في هذه الحالات، يجادل بوزان وويفر بأن تلك الدول تشكل "مجمعًا أمنيًا إقليميا"، حيث تكون تصوراتها للأمن مترابطة حتى لو لم يتفق جميع أعضاء مجمع الأمن الإقليمي على التهديدات الأمنية[1]. أثبتت هذه الدراسة أنه من الممكن تطبيق هذا النهج في الأمن السيبراني من خلال تكوين "مجمع للأمن السيبراني الإقليمي". من شأن الرسم الأولي لمثل هذا

[1] Barry Buzan & Ole Wæver, 2003, op.cit. p. 435

المجمع أن يرى أن المملكة العربية السعودية ودول مجلس التعاون الخليجي يشكلون مجمع إقليميا للأمن السيبراني، حيث تعرض كل منهم لعمليات سيبرانية كبيرة داخل وخارج حدوده، ويمتلك مجموعة من هياكل وقدرات الأمن السيبراني. كما أن لديهم عدو مشترك يمثل لهم تهديدا مستمرا في الفضاء السيبراني، وهو إيران، وحليف استراتيجي مشترك يقدم لهم الدعم، وهو إسرائيل.

وبالنظر للعوامل التي حددتها نظرية مجمع الأمن الإقليمي كشروط لتحقق مثل هذا النمط من العلاقات الدولية بين عدد من الدول، نجد أن الحرب السيبرانية الإسرائيلية – الإيرانية، قد ساهمت بما لا يدع مجالا للشك، في تكوين مجمعا إقليميا للأمن السيبراني بين المملكة العربية السعودية ودول مجلس التعاون الخليجي، حيث:

أولا: دفعت أمننة الأخطار السيبرانية الناتجة عن الهجمات المتكررة على مقدرات دول الخليج والمملكة العربية السعودية إلى تطوير قدراتها السيبرانية داخليا كما فسرنا في الفصل السابق. وبعد أن كانت تعاني المملكة من التأخر في التصنيفات الدولية في مجال الأمن السيبراني، أصبحت تحتل المركز الثاني عالميا طبقا لأحدث التقارير الدولية في هذا المجال.

كذلك قامت المملكة العربية السعودية بتعزيز قدراتها السيبرانية على المستوى الإقليمي، وابرمت العديد من اتفاقيات التعاون المشترك بينها وبين دول الإقليم ودول العالم، وأدارت وشاركت في العديد من الفعاليات الدولية والإقليمية في مجال الأمن السيبراني، وقادت دول مجلس التعاون الخليجي في تكتل سيبراني تحت مسمى "اللجنة الدائمة للأمن السيبراني بمجلس التعاون لدول الخليج العربية".

وبذلك يتحقق تغيرا ايجابيا في الاعتماد الأمني المتبادل بين المملكة العربية السعودية ودول مجلس التعاون الخليجي. وكان الدافع الأساسي لإحداث مثل هذا التغير هو الهجمات السيبرانية التي تعرضت لها المملكة العربية السعودية خلال الحرب السيبرانية الإسرائيلية – الإيرانية ومن قِبَل طرف من أطراف تلك الحرب وهو إيران.

ثانيا: كان التغير في أنماط الصداقة والعداوة في المنطقة حتميا، خصوصا مع وجود القدرات السيبرانية التي يتمتع بها أحد أطراف الحرب السيبرانية الإسرائيلية – الإيرانية وهو إسرائيل. كانت إسرائيل، ولا تزال، لا تشكل تهديدا أمنيا مباشرا للمملكة العربية السعودية ولدول الخليج العربي، بل إن الكثير من مياة التعاون قد جرت بين الجانبين على مدى السنوات السابقة للحرب السيبرانية الإسرائيلية – الإيرانية، خصوصا في مجال الأمن السيبراني.

وبالرغم من ما خلفه الصراع الفلسطيني – الإسرائيلي من عقبات حالت دون تطبيع العلاقات الكامل بين الدول العربية وإسرائيل، إلا أن المملكة العربية السعودية رأت أنه من الممكن **تفكيك أمننة** الأخطار أو الهواجس الأمنية التي خلفتها المشكلة الفلسطينية، في سبيل التقارب بينها وبين إسرائيل على الأقل في مجال الأمن السيبراني. وأخذت بعض دول الخليج طريقا أكثر تقدما لتعزيز التعاون بينها وبين إسرائيل عن طريق إبرام الاتفاق الإبراهيمي.

مما أحدث تغيرا ملحوظا في أنماط الصداقة والعداوة بين دول الإقليم العربي.

ثالثا: أدى التغير الإيجابي في قدرات الدفاع والردع السيبراني لدى المملكة العربية السعودية إلى إحداث تغيرا ملحوظا في توازنات القوى السيبرانية في الإقليم العربي. فبعد أن كانت المنطقة العربية مرتعا للمهاجمين السيبرانيين من الأفراد والدول، وربما كانت تلك الحالة من التأخر والضعف هى ما أغرت

إيران بالقيام بالهجمات السيبرانية على المقدرات السعودية لإحداث أضرار بالمصالح الاستراتيجية للولايات المتحدة الأمريكية وهي أحد أطراف الحرب السيبرانية الإسرائيلية – الإيرانية، عن طريق مهاجمة أحد أهم حلفائها الاستراتيجيين في المنطقة.

تتمتع دول الخليج العربي حاليا، و على رأسها المملكة العربية السعودية بقدرات للدفاع والردع السيبراني، صنفتها المؤسسات الدولية بالمرتبة الثانية عالميا. كما أنها تتمتع بروابط تعاون وتنسيق أمني سيبراني مع الولايات المتحدة الأمريكية وإسرائيل وهما يشكلان الطرف المعادي لإيران في الحرب السيبرانية الإسرائيلية – الإيرانية.

هذا التغير الملموس في توازنات القوى السيبرانية في المنطقة العربية، مثل رادعا قويا لإيران وغيرها من الدول والجماعات التي ربما تفكر في الهجوم سيبرانيا على المملكة العربية السعودية و/ أو دول الخليج. حتى أن التقارير الحديثة رصدت تراجعا ملحوظا في الهجمات السيبرانية على منطقة الخليج وعلى المملكة العربية السعودية على وجه الخصوص[1].

وبذلك يمكن القول بأن الحرب السيبرانية الإسرائيلية – الإيرانية، كان لها تأثيرا واضحا على الأمن الإقليمي العربي، حيث أدت تداعيات تلك الحرب وما خلفته من أخطار وتهديدات، إلى إحداث تغيرات جوهرية في أنماط العلاقات الدولية بالإقليم، و على وجه الخصوص فقد أدت الي:

- زيادة الاعتماد الأمني السيبراني المتبادل
- تغير في أنماط الصداقة والعداوة
- وتغير في توازنات القوى السيبرانية بين دول الإقليم.

[1] Manda Banda, 2022, "Latest Data Shows Saudi Arabian Organisations Making Gains in Building Greater Cyber Resilience." Intelligent CIO Middle East, Jul 20, accessed Dec 3, 2022, https://bit.ly/3uphQkJ

مما أدى إلى تكوين مجمعا إقليميا عربيا للأمن السيبراني بمبادرة من المملكة العربية السعودية وبمشاركة دول مجلس التعاون الخليجي.

التوصيات:

بناءً على النتائج السابقة يوصي الباحث بالآتي:

1- تمكنت المملكة العربية السعودية من تحقيق قفزات سريعة في مجال الجاهزية السيبرانية، إلا أنه من الملاحظ التفاوت الشديد في جهود باقي دول مجلس التعاون الخليجي في مجال الجاهزية السيبرانية. وبالتالي يجب أن تلتزم حكومات دول مجلس التعاون الخليجي بالتزام مستدام بالمرونة السيبرانية التي توفر إرشادات واضحة للمنظمات والأعمال وتحقق أفضل استخدام لهياكل الأمن السيبراني الناشئة بها. قد يتطلب ذلك المزيد من المشاركة في المبادرات مع الشركاء الإقليمين الدوليين لتعزيز الجاهزية السيبرانية[1].

[1] James Shires & Joyce Hakmeh, 2020, International Security Programme, Is the GCC Cyber Resilient? March, accessed Nov 30, 2022, https://bit.ly/3GWlN7Z

2- يجب ألا يقتصر نشاط مجمع الأمن الإقليمي السيبراني الذي كونته المملكة العربية السعودية مع دول مجلس التعاون الخليجي، على التعامل مع الأخطار السيبرانية في نطاقه الجغرافي الضيق فحسب، بل يجب أن تمتد مظلته الأمنية لتشمل الأقليم العربي كله من المحيط إلى الخليج. من خلال انضمام جميع الدول الأعضاء بجامعة الدول العربية إلى أنشطته وفعالياته واتفاقيته المنظِمة.

3- يجب أن تنضم جميع الدول العربية أيضاً في إطار منصة مشتركة تهدف إلى وضع كل دولة على مستوى مماثل من الجاهزية السيبرانية وفقًا لمعايير موحدة. ولا أجدر بلعب ذلك الدور من المنظمة العربية لتكنولوجيا الاتصال والمعلومات. وهي إحدى المنظمات العربية المتخصصة المنبثقة عن جامعة الدول العربية[1].

4- يجب أن تتوخى الدول العربية قدرا كبيرا من الحيطة والحذر في التعامل مع إسرائيل في مجال الأمن السيبراني. ويجب أن لا تنخدع بالتضخيم الزائد عن حده في قدرات إسرائيل السيبرانية. فقد كشفت الحرب السيبرانية الإسرائيلية – الإيرانية عن نقاط ضعف واضحة في منظومة الأمن السيبراني الإسرائيلي، تمكنت إيران من خلالها من القيام بهجمات سيبرانية مؤلمة لإسرائيل.

5- يجب أن يدرك صناع القرار السياسي العربي أن فتح الأسواق العربية على مصراعيها لشركات الأمن السيبراني الإسرائيلية يعني بالضرورة تسليم إسرائيل نسخة من مفاتيح خزائن البيانات العربية. فالتاريخ يعلمنا أنه لاشيء بلا ثمن خصوصا في التعامل مع مُحتل أبدى شراسة

[1] المنظمة العربية لتكنولوجيات المعلومات والاتصال، 2021، مرجع سابق

بالغة وتصلبا منقطع النظير على مدى أكثر من 50 عام من الصراع العربي الإسرائيلي.

6- في مجال التعليم والبحث العلمي: يجب على الدول العربية التوسع في إنشاء المدن الذكية ومنتزهات التكنولوجيا Technology Parks، والتي تخلق مساحة مشتركة علمية وبحثية واستثمارية تُمَكن المسؤولين الحكوميين والأكاديميين ورجال الأعمال من التعاون في الأبحاث والمشاريع السيبرانية و تبادل البيانات علي نحو يرتقي بمستوى الجاهزية السيبرانية للمجتمع ككل.

7- يجب تصميم برامج تعليمية تهدف الي تدريب الطلاب العرب في كافة المراحل التعليمية على مهارات سيبرانية استثنائية، لضمان إمداد الشركات والمراكز العلمية والبحثية السيبرانية العربية بالكوادر والموارد البشرية المؤهلة.

8- في المجال التقني: يجب على جميع الدول العربية أن تضمن لشعوبها مستوى معقول من انتشار التكنولوجيا، لا يقل عن المتوسط العالمي، عن طريق الاستثمار في مد خطوط الانترنت فائقة السرعة، وتزويد المدارس والجامعات بأجهزة ومعامل الحواسب المتقدمة، و التوسع في برامج رقمنة الخدمات الحكومية، مع عدم اغفال ما يتطلبه كل ذلك من رفع لمستوى الجاهزية السيبرانية.

9- في المجال السياسي: يجب أن تضع جامعة الدول العربية إطار ملزم لكافة الدول العربية ينظم اتفاقيات الشراكة والتعاون في مجال الأمن السيبراني بين الدول العربية وبعضها، وبينها وبين الدول غير العربية، على أن يضمن هذا الإطار تأمين تبادل البيانات العربية بما

لا يعرض الأمن الإقليمي العربي لأخطار التجسس والاختراق والتخريب.

10- يجب أن تدرك الدول العربية التي تشرع في تطوير قدراتها السيبرانية الذاتية، أن الشفافية وضمان حرية الرأي و التعبير، وضمان حرية تبادل البيانات والمعلومات لأفراد الشعوب العربية، هي عوامل أساسية حاسمة توفر الدافع لجميع فئات المجتمع للاشتراك بفعالية في عملية تطوير القدرات السيبرانية الذاتية، وتضمن توعية جميع فئات المجتمع بالمخاطر السيبرانية وكيفية التعامل معها على كافة المستويات.

قائمة المراجع:

أولا: المراجع باللغة العربية:

1. الحميدان، مشعل، 2013، 39 مادة قانونية لمكافحة الجرائم المعلوماتية الخليجية، الاقتصادية، 11 سبتمبر، متاح بالرابط: http://bit.ly/3hqLwur، تاريخ الدخول: 9 نوفمبر 2022
2. الخليج أونلاين، 2017، انعقاد أول اجتماع للجنة الخليجية للأمن السيبراني بالإمارات، 10 فبراير، متاح بالرابط: https://perma.cc/TZL3-XDEQ، تاريخ الدخول: 19 نوفمبر 2022
3. المنظمة العربية لتكنولوجيات المعلومات والاتصال، 2021: التزام استراتيجي بالأمن السيبراني في العالم العربي، المنتدى العربي للأمن

السيبراني 21-22 أكتوبر- تونس، متاح بالرابط: https://bit.ly/3pChJ2r، تاريخ الدخول: 5 مايو 2021

4. خيري، أمينة وآخرون، 2020، "أين العرب من الأمن السيبراني؟" إندبندنت عربية، 18 يونيو، متاح بالرابط: https://bit.ly/3pyZ0EP، تاريخ الدخول: 5 مايو 2021

5. سي ان ان، 2020، السعودية تتمسك بها.. ما هي بنود المبادرة العربية للسلام مع إسرائيل؟ سي ان ان العربية، 20 أغسطس، متاح بالرابط: https://cnn.it/3VsmppN، تاريخ الدخول: 8 نوفمبر 2022

6. موقع الاتحاد السعودي للأمن السيبراني، 2022، الأمن السيبراني السعودي و"الألكسو" يواجهان المخاطر المعلوماتية في العالم العربي، 29 مارس، متاح بالرابط: https://safcsp.org.sa/news-elexo، تاريخ الدخول: 8 نوفمبر 2022

7. موقع الهيئة الوطنية للأمن السيبراني، 2020، المملكة الثانية عالمياً في التحسن المستمر في مؤشر الأمن السيبراني للشركات ضمن تقرير التنافسية العالمية 2020م، 22 يونيو، متاح بالرابط: https://nca.gov.sa/news?item=40، تاريخ الدخول: 7 نوفمبر 2022

8. موقع الهيئة الوطنية للأمن السيبراني، 2022، المملكة ترأس اجتماع اللجنة الدائمة للأمن السيبراني في مجلس التعاون لدول الخليج العربية، 28 يوليو، متاح بالرابط: https://nca.gov.sa/news?item=227، تاريخ الدخول: 6 نوفمبر 2022

9. موقع الهيئة الوطنية للأمن السيبراني، 2022، الهيئة الوطنية للأمن السيبراني توقع مذكّرة تفاهم مع الأمانة العامة لمجلس التعاون لدول الخليج العربية، 12 أبريل، متاح بالرابط: https://nca.gov.sa/news?item=6، تاريخ الدخول: 7 نوفمبر 2022

10. موقع الهيئة الوطنية للأمن السيبراني، 2022، بمشاركة الجهات المختصة بدول مجلس التعاون انطلاق «التمرين الخليجي للأمن السيبراني» في الرياض، 23 أكتوبر، متاح بالرابط: https://nca.gov.sa/news?item=341، تاريخ الدخول: 6 نوفمبر 2022

11. وكالة الأنباء السعودية، 2022، عام / المملكة تُحقق المرتبة الثانية عالمياً في مؤشر الأمن السيبراني وفق تقرير «الكتاب السنوي للتنافسية العالمية لعام 2022، 15 يونيو، متاح بالرابط: https://www.spa.gov.sa/2362614، تاريخ الدخول: 28 أكتوبر 2022

ثانيا: المراجع باللغة الانجليزية

Books:

1. Buzan, B., & Wæver, O., 2003, Regions and powers, Cambridge, UK: Cambridge University Press
2. Buzan, B., 2007, People, states & fear: An agenda for international security studies in the post-cold war era (2nd ed.), Colchester, UK: ECPR Press
3. Buzan, B., Wæver, O., & de Wilde, J., 1998, Security: A new framework for analysis. Boulder, CO.: Lynne Rienner.

Periodicals:

1. Buzan, B., 1988, The Southeast Asian security complex. Contemporary Southeast Asia, 10(1)
2. Jamilah, M., Fikra, H.U. & Harza, Z., 2019, Facilitating Conditions of Saudi Arabia–Israel Normalization in 2015-2018, Journal of Diplomacy and International Studies, 2(01)
3. Morgan, P.M., 1997, Regional security complexes and regional orders. Regional orders: Building security in a new world.

Working Papers:

1. Andžāns, Māris , 2015, Prospects of Regionalization of Security in the Cyberspace: Case of the Baltic States, Proceedings of the Conference of Turiba University, XIV International Scientific Conference “Creating the Future: Communication, Education, Business"
2. Andžāns, Māris, 2014, Securitization in Defining Regional Security Complexes: the Case of the Baltic States (2004–2013), Summary of the Doctoral Thesis
3. Bergmane, Una, 2020, Fading Russian Influence in the Baltic States, Orbis 64(3)
4. Lestari, E.A.P, 2021, Complex Interdependence Between Indonesia-Australia Through Cybersecurity Cooperation Post-Indonesia-Australia Cyberwar in 2013, Jurnal Hubungan Internasional, 9(2)
5. Rhodes, E., 2000, The American Vision of Baltic Security Architecture: Understanding the Northern Europe Initiative, Baltic Defence Review, 4, accessed May 11, 2022, https://bit.ly/3w6jnOl
6. Rojčík, Ondřej, 2019, “Achievements and Failures of NATO Cyber Policies“, In NATO at 70: Outline of the Alliance Today and Tomorrow, edited by R. Ondrejcsák, T. H. Lippert, 179-192. Bratislava: STRATPOL
7. Setyawati, S. M. A., & Agussalim, D., 2015, security Complex Indonesia-Australia dan Pengaruhnya terhadap

Dinamika Hubungan Kedua Negara, Jurnal Ilmu Sosial dan Ilmu Politik, 19(2).

Reports:

1. ABI Research, 2014, GLOBAL CYBERSECURITY INDEX. ITU, Dec 9, accessed Feb 23, 2022, https://bit.ly/353qkVB
2. Alexander, K., 2020, "Israeli-Gulf Cyber Cooperation." Modern Diplomacy, Dec 23, accessed Nov30, 2022, https://bit.ly/3UluVpu
3. Arsene, Liviu, 2020, Iranian Chafer APT Targeted Air Transportation and Government in Kuwait and Saudi Arabia, bitdefender.com, May 21, accessed Nov 5, 2022, http://bit.ly/3u4SHvv
4. Berman, Ilan, 2012, Cyberwar And Iranian Strategy, AFPC Defense Dossier, August, accessed Feb 7, 2022, https://bit.ly/3GsolH7
5. Bilbao-Osorio, B., Dutta, S. & Lanvin, B. , 2014, Insight Report: the Global Information Technology Report 2014, Rewards and Risks of Big Data, World Economic Forum, accessed Feb 22, 2022, https://bit.ly/3verZ5v
6. European Union Agency for Cybersecurity, 2014, Cyber Security Strategy Of Latvia 2014-2018, enisa.europa.eu, European Union Agency for Cybersecurity, accessed Apr 27, 2022, https://bit.ly/3ydaPqr
7. Ghernaouti-Hélie, S, 2008, From risk management to information security policies and practices: a multi perspective framework for ICT security effectiveness. Geneva: International Telecommunication Union, Apr 14, accessed Feb 22, 2022, https://bit.ly/3vdfWoO
8. Government of Estonia, 2008, Cyber Security Strategy, Ministry of Defence, accessed Apr 24, 2022, https://bit.ly/3MC5M6v
9. Government of Lithuania, 2011, the Programme for the Development of Electronic Information Security (Cyber-

Security) for 2011–2019. enisa.europa.eu, European Union Agency for Cybersecurity, accessed Apr 27, 2022, https://bit.ly/3OIGIwM
10. Guzansky, Yoel & Deutch, Ron, 2019, How Prepared is Saudi Arabia for a Cyber War? INSS Insight No. 1190, July 10, accessed Nov 5, 2022, https://bit.ly/3icsOHl
11. Hathaway, M., Spidalieri, F. & Alsowailm, F., 2017, Kingdom of Saudi Arabia cyber readiness at a glance, Potomac Institute for Policy Studies, accessed Nov 30, 2022, https://bit.ly/3VmrK2b
12. IDC, 2020, "Cybersecurity and its impact on digital Saudi" idc.com, accessed Nov 5, 2022, https://bit.ly/3E4A68y
13. Rainie, L., Anderson, J. & Connolly, J., 2014, Cyber Attacks Likely to Increase, Pew Research Center, Oct 29, accessed Apr 24, 2022, https://pewrsr.ch/3JJbIt8
14. Seeger, Russell & Thafer, Dania, 2018, "The New Battlefront: Cyber Security across the GCC – Gulf International Forum." Gulfif.org, Oct 29, accessed Nov 30, 2022, https://bit.ly/3XNimWW
15. Shires, James, & Hakmeh, Joyce, 2020, International Security Programme, Is the GCC Cyber Resilient? March, accessed Nov 30, 2022, https://bit.ly/3GWlN7Z.

Press:

1. Abbas, N., 2018, "Arab Countries Facing The Highest Number Of Cyber Attacks". Forbes Middle East, Mar 28, accessed May 5, 2021, https://bit.ly/3doronD
2. Afp, 2012, US thinks Iran behind cyberattack in Saudi: ex-official, The Express Tribune, October 13, accessed Dec 9, 2021, https://bit.ly/3dy2rWM
3. Banda, Manda, 2022, "Latest Data Shows Saudi Arabian Organisations Making Gains in Building Greater Cyber Resilience." Intelligent CIO Middle East, Jul 20, accessed Dec 3, 2022, https://bit.ly/3uphQkJ

4. BBC Monitoring, 2017, Iran and Saudi Arabia: Friends and foes in the region, BBC News, Nov 10, accessed Nov 26, 2022, http://bit.ly/3U5jIcF
5. Concordiam, P., 2016, Baltic Cyber Cooperation: Estonia, Latvia and Lithuania Sign a Historic Document to Align Their Cyber Defense Policies, Jul 14, accessed Apr27, 2022, https://bit.ly/3xRnmj0
6. Dwinanda, R., 2018, BSSN to Team up with Australia to Deal with Cyber Attacks, Republika Online, Feb 1, accessed Apr 25, 2022, https://bit.ly/3MrIRLh
7. Engel, D., 2021, Australia–Indonesia relations: Keeping It Real, The Strategist, Feb 23, accessed Apr 28, 2022, https://bit.ly/3kn425i
8. Fazzini, Kate, 2019, "The Saudi Oil Attacks Could Be a Precursor to Widespread Cyberwarfare — with Collateral Damage for Companies in the Region." CNBC, Sep 21, accessed Nov 5, 2022, https://cnb.cx/3U8JWfj
9. Fenton-Harvey, Jonathan, 2019, "UAE-Israel Cyber-Spying Aids Emirati Influence, Repression." Inside Arabia, Dec 27, accessed Nov 30, 2022, https://bit.ly/3uehUn7
10. Gorenburg, D., 2019, Russian Strategic Culture in a Baltic Crisis, George C. Marshall European Center for Security Studies, Mar, accessed May 11, 2022, https://bit.ly/39cgySy
11. Hirschauge, Orr, 2017, Former Israeli Parliamentarian Says Homegrown Companies Can Help Build Saudi Future City Neom, calcalistech.com, Nov 21, accessed Nov 26, 2022, http://bit.ly/3GW7dx0
12. Hussein, Ibrahim al-, 2017, "60 Million Cyber Attacks Targeted Saudi Arabia in One Year." Al Arabiya English, May 2, accessed, Nov 5, 2022, https://bit.ly/3UnOs9k
13. Lukman, E., 2013, Tech in Asia - Connecting Asia's Startup Ecosystem, www.techinasia.com, Nov 11, accessed Apr 25, 2022, https://bit.ly/36JJZKY

14. Osgood, Patrick, 2012, Cyber attack takes Qatar's RasGas offline, Arabian Business, Aug 30, accessed Dec 9, 2021, https://bit.ly/30dz4Gi
15. Prucková, M., a 2022, Regional Security Complex Theory and the Baltic states. How Have Their Relations with the Russian Federation Changed after the Bronze Year 2007 incident? Security Outlines, Mar 23, accessed May 11, 2022, https://bit.ly/3L5qjzr
16. Prucková, M., b, 2022, Cyber Attacks and Article 5 – a Note on a Blurry but Consistent Position of NATO, ccdcoe.org, accessed May 11, 2022, https://bit.ly/3FJ6qgr
17. Reuters Staff, 2019, Senior Israeli official attends Bahrain security meeting focusing on Iran, Reuters, Oct 21, accessed Nov 26, 2022, http://bit.ly/3iem1gq
18. Russian News Agency, 2021, Russia, Iran sign agreement on cyber security cooperation, TASS, Jan 26, accessed Nov 26, 2022, https://tass.com/politics/1248963
19. Sardarizadeh, S., 2016, Iran-Saudi tensions erupt in 'cyberwar', BBC, Jun 3, accesses Dec 9, 2021, https://bbc.in/3dxaSBP
20. Schindler, M., 2017, Israeli companies working with Saudi Arabia? The Jerusalem Post, Oct 26, accessed Nov 26, 2022, http://bit.ly/3EIdlGy
21. Sputnik International, 2015, Yemeni Hackers Reveal Top Secret Docs in Saudi Government Cyber Attack, May 22, accessed Nov 26, 2022, https://sputniknews.com/20150522/1022475567.html
22. Tashkandy, Hala, 2020, Cyberattacks hit 95% of Saudi businesses last year, says study, Arab News, Aug 12, accessed Nov 5, 2022, https://arab.news/j4pt5
23. Wechsler, O., 2021, The Iran-Russia Cyber Agreement and U.S. Strategy in the Middle East, Council on Foreign Relations. Mar 21, accessed Nov 26, 2022, https://bit.ly/3XwZJXf
24. Work, J. & Harknett, R., 2020, Troubled vision: Understanding recent Israeli–Iranian offensive cyber

exchanges. Atlantic Council, Jul 22, accessed Nov 26, 2022, http://bit.ly/3XAtXZl.

Websites:

1. Department of Foreign Affairs and Trade, 2018, Memorandum of Understanding between the Government of the Republic of Indonesia and the Government of Australia on Cyber Cooperation, accessed Apr 25, 2022, https://bit.ly/3Lnp6Ve