

دور الأمن السيبراني في تعزيز الأمن الصحي للدول

The Role of Cybersecurity in Enhancing States Health Security



بوطبة عبد الله¹ ، بوستي توفيق²

¹ مخبر الدراسات القانونية البيئية، جامعة 08 ماي 1945-قائمة- الجزائر

Boutobba.abdallah@univ-guelma.dz

² مخبر الدراسات القانونية البيئية، جامعة 08 ماي 1945-قائمة- الجزائر

Bouctti.toufik@univ-guelma.dz

تاريخ الإرسال: 2024/09/05 تاريخ القبول: 2024/10/29 تاريخ النشر: 2024/12/01

ملخص: يعتبر الأمن السيبراني والأمن الصحي من المفاهيم الحديثة في الأدبيات السياسية والأمنية المعاصرة. نظرا لبروزهم نتيجة التحولات التي طرأت على بيئة وبنية النظام الدولي عقب الحرب الباردة، والتي أدت إلى بروز تهديدات لا تماثلية هددت أمن الدول والمجتمعات من بينها التهديدات الصحية والسيبرانية، حيث أثرت هذه التهديدات المستجدة على منظومة الأمن القومي للدول.

وتهدف هذه الدراسة إلى إبراز الإطار النظري لمفهوم الأمن السيبراني والأمن الصحي، وكذلك مكانتهم ضمن منظومة الأمن القومي للدول، مع تسليط الضوء على العلاقة التي تربطهما ببعض والإشارة إلى دور الأمن السيبراني في تعزيز الأمن الصحي للدول، إضافة إلى التطرق لأهم التحديات والحلول التي تواجه تطبيق الأمن السيبراني في القطاع الصحي. وخلصت الدراسة إلى أن الأمن السيبراني يعتبر دعامة أساسية لصد التهديدات التي تؤثر على منظومة الأمن الصحي للدول لضمان سيورتها، كما أن الأمن السيبراني له تأثير كبير على القطاع الصحي.

الكلمات المفتاحية: الأمن السيبراني، الأمن الصحي، التهديدات السيبرانية، البيانات الصحية

Abstract:

Cybersecurity and health security are modern concepts in contemporary political and security literature, due to their emergence as a result of the transformations that took place in the environment and structure of the international system after the Cold War, which led to the emergence of asymmetric threats that threatened the security of countries and societies, including health and cyber threats, as these new threats affected the national security system of countries. This study aims to highlight the theoretical framework of the concepts of cybersecurity and health security, as well as their status within the national security system of countries, while highlighting the relationship between them and referring to the role of cybersecurity in enhancing health security of countries, in addition to addressing the most important challenges and solutions facing the application of cybersecurity in the health sector. The study concluded that cybersecurity is an essential pillar to repel threats that affect the health security system of countries to ensure its functioning, and cybersecurity has a significant impact on the health sector.

Key words: Cybersecurity, Health security, Cyber Threats, Health data

مقدمة:

شهد العالم تطورا كبيرا في مجال التكنولوجيا الرقمية اتجهت من خلاله الكثير من الدول نحو مواكبة الثورة الرقمية وتبنيها في مختلف القطاعات الحيوية كالتعليم والاقتصاد والصحة، وهذا لتسهيل الخدمات وربح الوقت، وقد رافق هذه التطورات الرقمية تهديدات سيبرانية أثرت على مختلف القطاعات، ما افرز ضرورة حماية أمن المعلومات التي تعتبر من اهم قضايا العصر، ويعتبر الأمن السيبراني اليوم أحد التحديات التي تواجه الدول في القرن 21، بسبب تداعياته الخطيرة على امن الدول والمجتمعات، خاصة من جانبه الانساني الذي يعتبر الامن الصحي أحد أبعاده، إذ يحتل الملف الصحي اليوم مكانة هامة في استراتيجيات الدول، نظرا لارتباطه بحياة الشعوب ومستقبلها، من خلال تقديم الرعاية الصحية وخدمات العلاجات، وقد انتقلت هذه الخدمات في ظل الالفية الجديدة نحو التقدم وإدخال المتغير التكنولوجي عليها أصبحت أكثر ارتباطا بالتكنولوجيا الرقمية، حيث أن أي قصور أو خلل في أنظمة حماية المعلوماتية الخاصة بها تؤدي إلى تداعيات خطيرة على الامن الصحي وتلحق ضرر بالأفراد والمجتمعات، وقد شهد القطاع الصحي عدة هجمات سيبرانية أثرت على منظومات الأمن الصحي للدول .

تسعى الدراسة الى التعريف بالمفاهيم: الأمن السيبراني والأمن الصحي للدول، مع كشف العلاقة التأثيرية بينهما والوقوف على اهم التحديات والحلول التي تواجه تطبيق الأمن السيبراني ضمن القطاع الصحي. وذلك من خلال الإشكالية الاتية: كيف يؤثر الأمن السيبراني في تعزيز قدرة الأمن الصحي للدول؟ وتتفرع عن الإشكالية مجموعة تساؤلات فرعية التالية:

-ما المقصود بالأمن السيبراني؟ وما هي أبعاده؟ والتهديدات المرتبطة به؟

-ما مفهوم الأمن الصحي؟ وماهي أهميته في حماية استقرار الدول؟

تنطلق هذه الدراسة من فرضية تشير الى أن الهجمات السيبرانية تؤثر بشكل بالغ في البنية التحتية للصحة العامة وتزداد تلك الهجمات بشكل كبير خلال الازمات الصحية.

أما منهجية الدراسة فتم الاعتماد على المنهج الوصفي التحليلي لمعرفة ماهية التهديدات السيبرانية وعلاقتها بالأمن القومي مع إبراز أهم التحديات التي تعترض البنية الصحية للدول. وللإجابة على الإشكالية السابقة قسمت الورقة البحثية على النحو الاتي:

المبحث الأول: مفهوم الأمن السيبراني

المبحث الثاني: مفهوم الأمن الصحي

المبحث الثالث: تقاطع الأمن السيبراني بالأمن الصحي

المبحث الرابع: دور الأمن السيبراني في تعزيز الأمن الصحي

المبحث الخامس: تطبيق الامن السيبراني في القطاع الصحي (التحديات والحلول)

المبحث الأول

مفهوم الامن السيبراني

تعد تكنولوجيا الانترنت اليوم من أكثر المسائل أهمية في حياتنا المعاصرة، نظرا لعلاقتها المباشرة بجميع مناحي الحياة سواء الافراد او الدول، حيث تستخدم العديد من الدول التكنولوجيا الرقمية في بنيتها التحتية لإدارة مختلف الخدمات الرقمية، وهذا ربحا للوقت ولتقديم خدمة أفضل من خلال توظيف شبكات الحاسوب وأنظمة الاتصالات في معاملتها الرقمية.

وسنتطرق في هذا المبحث الى مفهوم الأمن السيبراني وتحديد أبعاده وأهم التهديدات المرتبطة به وأهميته ضمن منظومة الأمن القومي للدول.

المطلب الأول: تعريف الامن السيبراني

قبل التطرق لمفهوم الامن السيبراني يجب أن نعرّج على مفهوم رئيسي مرتبط بالأمن السيبراني وهو الفضاء السيبراني

الفرع الأول: الفضاء السيبراني

لقد أصبحت حروب اليوم تدار عن بعد ووراء شاشة الكترونية سلاحها كبسة زر ومعادلة خوارزمية ومقاتل افتراضي الكتروني، وتدار هذه المعارك عبر ساحة افتراضية يطلق عليها اسم "الفضاء السيبراني"، ويعتبر "ويليام غيبسون" William Gibson الكاتب المتخصص في الخيال العلمي أول من استخدم هذا المصطلح "الفضاء الالكتروني" لذاع صيت هذا المصطلح في تسعينيات القرن الماضي بعد تنامي استخدام الانترنت وشبكات والاتصال بشكل واسع.¹

كما يعد مصطلح "الفضاء السيبراني" من المفاهيم الحديثة في العلوم الاجتماعية الذي يفتقد لتعريف قار، حيث أشار كل من الباحثان "بيتر سينغر" Peter w singer و "الان فريدمان" Allan friedman الى أن "الفضاء السيبراني" عبارة عن عالم شبكي يحوي كمبيوترات ومستخدمين يتم من خلالها نقل ومشاركة وتخزين المعلومات عبر شبكة الانترنت.²

الفرع الثاني: تعريف الأمن السيبراني

يتكون مصطلح "الامن السيبراني " من لفظتين "الامن" و "السيبراني"، حيث يشير المعنى اللغوي " للأمن " الى نقيض الخوف او بمعنى السلامة والاطمئنان وزوال الخوف، بينما يعود لفظ "السيبراني" Cyber

¹ محمد مسيكة، الفضاء السيبراني وتحديات الامن القومي للدول، مجلة العلوم القانونية والاجتماعية، المجلد 07، العدد 04، جوان، 2022، ص454.

² فاتح حارك، الدولة بين الهيمنة وتحقيق الأمن في الفضاء السيبراني، المجلة الجزائرية للأمن الإنساني، المجلد 7، العدد 01، 2022، ص133.

إلى اللغة يونانية ، حيث اشتق من كلمة Kybernetes بمعنى الشخص الذي يدير دفة السفينة، ويستخدم مجازا للمتحكم Governor، وقد أشار بعض المؤرخين إلى أن أصلها يعود إلى عالم الرياضيات الأمريكي Wiener Norbert والتي استخدمها للدلالة على التحكم الآلي، أما مصطلح الأمن السيبراني Cybersecurity فيعتبر أحد فروع العلوم التكنولوجية، والذي يعنى بحماية الأنظمة والشبكات والبرامج من الهجمات الرقمية التخريبية، والتي تهدف إلى الوصول غير المرخص إلى المعلومات الحساسة بغرض تغييرها أو تعطيلها أو اتلافها، من جانب آخر يعرفه "ادوارد اومورسو" Edward Amorso صاحب كتاب "الأمن السيبراني" الصادر سنة 2007 بأنه "مجموع الوسائل التي تحد من خطر الهجوم على البرمجيات أو الشبكات" بواسطة وسائل وأدوات لمواجهة القرصنة وكشف الفيروسات الرقمية ووقفها وتوفير الاتصالات المشفرة والأمنة.¹

ويعرفه أيضا "ريتشارد كمرر" Richard a. Kemmerer بأنه عبارة عن وسائل دفاعية من شأنها كشف وصد محاولات التي يقوم بها القراصنة.²

وتعرفه وزارة الأمن الداخلي الأمريكية بأنه " القدرة وامكانية يتم بموجها حماية نظم المعلومات والاتصالات ضد الضرر او الاستخدام او تعديل الغير المصرح به".³

واستنادا إلى التعاريف السابقة يمكن القول أن الأمن السيبراني في نهاية المطاف هي القدرة على حماية أنظمة شبكات المعلومات المتصلة بالإنترنت وصد المخاطر المرتبطة باستخدام التكنولوجيا الرقمية.

المطلب الثاني: أبعاد الأمن السيبراني

يمكن تقسيم ابعاد الامن السيبراني الى ما يلي:

الفرع الأول: البعد المتصل بأمن الدولة بشكل مباشر

يتجلى ذلك من خلال الهجوم السيبراني المباشر Cyber Attack ضمن الفضاء الالكتروني الذي يهدف الى المساس بالأنظمة الالكترونية والذي يؤدي الى تقويض شبكة الكمبيوتر لغرض سياسي والذي يؤدي بدوره الى اضرار مادية ،سواء كان الهجوم ضمن صراع الدول أو كهجوم إرهابي غرضه اجرامي ،لذلك تسعى الكثير من الدول الى تعزيز بنيتها في المجال السيبراني على غرار روسيا والولايات المتحدة الامريكية والصين، كما تتمتع الكثير من الجيوش نحو 30 جيشا من بينها تاوان استراليا، ايران، الهند ،باكستان على قدرات الحرب

¹ وفاء مطروح، تداعيات جائحة كوفيد 19 وتأثيره على تحقيق الامن السيبراني في الجزائر، المجلة الدولية للاتصال الاجتماعي، المجلد 02، العدد 09، 2022ص222.

² لامية طالة، الإرهاب السيبراني والامن القومي: قراءة في تحولات الاستراتيجية الدفاعية، حويلات جامعة الجزائر 01، المجلد 35، العدد 04، ص355.

³ حبيب عوفي، الفضاء الرقمي تحدي أمني جديد استراتيجيات الدول في تحقيق الامن السيبراني العالمي، المجلة الجزائرية للعلوم الانسانية والاجتماعية، المجلد 06، العدد 01، ص113.

الإلكترونية في طليعتها الولايات المتحدة الأمريكية والصين، وحسب كل من كلارك Clarke وكنيك Knake فإن القوة السيبرانية للدول تؤخذ على: قدرة الدول على الاعتماد على الشبكات السيبرانية-الإلكترونية الوطنية وتوظيفها ضمن بنيتها التحتية، إضافة إلى قدرتها على تنفيذ وصد الهجمات السيبرانية وفق تدابير مدروسة¹.

لذلك نجد الولايات المتحدة الأمريكية تتمتع بقدرات هجومية كبيرة مقابل قدرات دفاعية ضعيفة مقارنة بالصين ناهيك عن سيطرة القطاع الخاص على شبكتها السيبرانية.

الفرع الثاني: البعد المتصل بأمن الأفراد والمجتمعات

تهدف بعض الهجمات الإلكترونية إلى استهداف الأفراد والمجتمعات، وذلك من خلال التأثير على هوية الأفراد وتركيباتهم الثقافية وقناعاتهم الفكرية من خلال برامج الكترونية محددة، أين يتم توجيه المجتمعات نحو ثقافة معينة من خلال وسائط التواصل الاجتماعي هدفها خلق البلبلة والانشقاقات وتصعيد التوترات سواء داخل الدولة الواحدة أو بين الدول، وظهر ذلك من خلال حركة " حياة السود مهمة " الأمريكية سنة 2020 التي استقطبت الرأي العام الدولي وأدت إلى انكشاف العلاقات الاجتماعية داخل الولايات المتحدة الأمريكية وهذا من خلال نشاطها الرقمي².

المطلب الثالث: تهديدات الأمن السيبراني

ارتبطت التهديدات السيبرانية بظهور الانترنت، وقد عرفت القيادة الاستراتيجية الأمريكية التهديدات السيبرانية "بأنها تطوير عمليات القرصنة والتسلل لاستهداف نظام الكمبيوتر، بهدف منع الاستخدام الفعال لها والسيطرة على البيانات التي تحتويها"³.

والتهديدات السيبرانية عبارة عن برامج ضارة نابعة من الفضاء السيبراني، تهدف إلى المساس بأمن الميكرو كمبيوترات والهواتف الذكية والأجهزة اللوحية والشبكات المتصلة بالإنترنت، وقد يكون مصدر التهديد نابع من شخص أو دولة أو مجموعة قراصنة أو أطراف منظمة ذات أهداف جيوسياسية⁴.

¹مراد شحات، لبنى جصاص، الأمن السيبراني للدول: بعد افتراضي لواقع مادي، مجلة الناقد للدراسات السياسية، المجلد 07، العدد 02، السنة 2023، ص106.

²فايز الشهري، شبكات التواصل وتأثيرها على العلاقات الدولية، العربية نت، متاح الموقع : <https://shorturl.at/mKvuf> ، تاريخ الاطلاع: 2024/10/17

³عبد الله جعفري، التهديدات السيبرانية وتأثيرها على الأمن القومي للجزائر، المجلة الأفريقية للدراسات القانونية والسياسية، المجلد 06، العدد 02، السنة 2022، ص247.

⁴ساعد بوقرص، الأمن السيبراني: مخاطر وتهديدات وتحديات ممارسات توصيات استراتيجيات خاصة، مجلة الأبحاث في الحماية الاجتماعية، المجلد 3 العدد 1، ص65.

وتختلف حدة الهجمات السيبرانية التي تستهدف أنظمة وشبكة المعلومات والاتصالات من دولة إلى أخرى بحسب درجة التطور التكنولوجي السائد في البلاد، لذلك يمكن تقسيمها إلى ما يلي:

الفرع الأول: أنواع الهجمات السيبرانية

يتمحور هدف الهجمات الإلكترونية في المجلد إما لسرقة الهويات الرقمية أو اتلاف وتخريب البيانات والمعطيات الرقمية وتعطيلها أو التجسس والابتزاز والتحايل والتصيد والتأثير السلبي على الرأي العام، وهناك عدة طرق يتم استخدامها للوصول إلى هذه الأهداف المذكورة آنفا ومنها:

أولاً: برامج دفع الفدية: الذي يعمل على تشفير البيانات على النظام المستهدف ويطلب من خلاله الفدية مقابل السماح للمستخدم بالوصول إلى البيانات مرة أخرى، وتتراوح حدة هذه الهجمات من الازعاج المنخفض المستوى إلى الحوادث الخطيرة، حيث أصبح هذا النوع من الهجمات أكثر انتشاراً ويمثل تهديد كبير للشركات والأفراد نظراً لطابع الابتزاز.¹

إضافة إلى أسلحة سيبرانية أخرى تستخدم في الهجوم كالفيروسات الكمبيوتر والأجهزة الكهرومغناطيسية العابرة، إضافة إلى البرمجيات الملوثة وبرامج الهاكر برامج Rootkit الديدان Worms، ومفاتيح التشفير والقنابل المنطقية Logic Bombs والأبواب الخلفية Back Doors الانتحال وهجمات الحرمان من الخدمات الموزعة وغيرها.²

ثانياً: هجمات التصيد Phishing: تعتمد على أسلوب الهندسة الاجتماعية Engineering Social يتم خلالها تحفيز الضحية لفتح رابط يحتوي على برمجيات خبيثة تصيب الجهاز مباشرة، بينما هجمات وقف الخدمة DDOS تهدف إلى اغراق الضحية بآلاف الرسائل والطلبات، التي تؤدي في نهاية المطاف إلى قطع الخدمة ووقفها سواء كان ذلك عبر موقع الأنترنت أو خدمة الكترونية حكومية، أما الابواب الخلفية Back Doors هي ثغرات مقصودة توضع على أجهزة الضحايا بهدف التجسس والمراقبة او جمع المعلومات.³

كما يعتبر امكانية الرد على مثل هذه الهجمات معقدة للغاية لصعوبة تعقب مصدر الهجمات وتحديد هوية المهاجم، إضافة إلى أن القانون الدولي أغفل على هذا الجانب، حيث لم يرد هناك نصوص قانونية واضحة وقاطعة لمواجهة مثل هذه العمليات السيبرانية العابرة للحدود التي تعتبر حروب لا تناظرية Asymmetric.⁴

¹ ضحى لعبي، البعد الجيوسياسي للأمن السيبراني، مجلة العلوم الانسانية، المجلد 05، العدد 01، 2021، ص 207.

² علاء الدين فرحات، الحرب السيبرانية ومستقبل الامن العالمي، مجلة الناقد للدراسات السياسية، المجلد 6 العدد 02، 2022، ص 683

³ محمد مسيكة، مرجع سابق، ص 455.

⁴ علاء الدين فرحات، مرجع سابق، ص 683.

المطلب الرابع: مكانة الأمن السيبراني ضمن اهتمامات الأمن القومي وتأثيره على أمن الدول

يتسم مفهوم الأمن القومي للدول بالعمومية والشمولية، نظرا لنسبته من جهة وتأثره بعدة متغيرات نابعة من عوامل داخلية وخارجية من جهة أخرى، لكن يعد الأمن القومي قمة الضرورة والهدف الأعلى التي تسعى اليه كل دولة لضمان بقائها، لذلك تتجه الكثير من الدول إلى صياغة العديد من الاستراتيجيات والاجراءات التي تكفل سلامة أمنها الوطني ضد التهديدات الداخلية والخارجية، ويدور محور الأمن بشكل أساسي على التحرر والانعقاد من كل تهديد يشكل خطرا على الأمن القومي، وقد تغير مفهوم الأمن القومي للدول بمرور الزمن نتيجة عدة تحولات التي طرأت على المشهد الدولي أثرت على طبيعة مفهوم الأمن، أين انتقل من الأمن الصلب إلى الأمن اللين ومن أمن الدولة الى أمن الأفراد " الأمن الإنساني"، إضافة إلى ظهور فواعل جديدة أثرت على المنظومة الامنية العالمية، خاصة في ظل بروز تهديدات مستجدة كالأوبئة والإرهاب البيولوجي والسيبراني أثرت بشكل كبير على أمن الدول، أين أصبح أمن الدولة متعلق بعدة أبعاد خلافا للبعد التقليدي القائم على القوة الصلبة، حيث فرضت الثورة المعلوماتية والتكنولوجية الجديدة تغير في منظومة الأمن القومي للدول، نتيجة لتنامي الثورة المعلوماتية واستخدامها ضمن القطاعات الحيوية للدولة وما رافقها من تهديدات، أين أضى الأمن الوطني للدول تحت رحمة التطور التكنولوجي، خاصة مع التطور الكبير في الأقمار الصناعية ووسائل التجسس والاختراقات، أين أضحت السيادة الوطنية مختزلة بمفهوم التكنولوجي الحديث .

كما أصبح الفضاء السيبراني اليوم ساحة معركة خامسة بعد البر، الجو، البحر، الفضاء، و له تأثيرات قوية على أمن الدول والعالم نظرا لتداعياته الكبيرة، حيث يمكن الحاق ضرر بالاقتصاد لدولة ما من خلال كبسة زر، ناهيك عن التسلل الى القطاعات العسكرية والمدنية وتعطيلها¹، واستهداف البنية التحتية الحيوية والحاق اضرار تريبية بها، مثل استهداف الذي تعرضت له شركة الكهرباء البرازيلية سنة 2008 التي أدت الى انقطاع الكهرباء من خلال تسلل القراصنة للموقع والسيطرة عليه لمدة أسبوع كامل، اين توقفت الإضاءة وحركة القطارات وتأثر نحو 60 مليون شخص جراء الانقطاعات المتكررة للكهرباء²

إضافة إلى الهجمات التي وقعت على أوكرانيا سنة 2017 استهدفت محطات الطاقة والأنظمة المالية والمصرفية، والهجوم السيبراني على محطات النووية في إيران بواسطة فيروس Stuxnet الذي عطل أجهزة

¹ باسكال بونيفاس، الجيوبولتيك، مقارنة لفهم العالم، مقارنة لفهم العالم 48 مقالا، (تر: اياد عيسى)، دمشق، منشورات الهيئة العامة السورية للكتاب، وزارة الثقافة، 2020، ص 81.

² شريفة كلاع، الأمن السيبراني وتحديات الجوسسة والاختراقات الالكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الإنسانية، المجلد 15، العدد 01، 2022، ص 301.

الطرد المركزي لتخصيب اليورانيوم سنة 2010، ناهيك عن تعرض الشركة الكورية الجنوبية للطاقة النووية والمائية الى هجمات الكترونية سنة 2014¹، كما تعرضت الولايات المتحدة الامريكية لهجمات على شبكات الكهرباء عام 2009 والتي تعتبر أهم البنى التحتية في البلاد، كما تعرضت أيضا المرشحة السابقة للرئاسة الامريكية "هيلاري كلينتون" عن الحزب الديمقراطي الامريكي لتسريب معلومات خطيرة من بريد ها الالكتروني أدت في نهاية المطاف الى خسارتها في الاستحقاقات الرئاسية الاخيرة امام نظيرها "دونالد ترامب".²

أما من الناحية الاقتصادية فإن تكلفة الهجمات السيبرانية على أنظمة تكنولوجيا المعلومات والاتصالات له تداعيات مالية ضخمة جدا على الدول، وتشير بعض التقارير الى أن الخسائر العالمية المقدرة جراء جرائم الانترنت تتجاوز 400 مليار دولار امريكي سنويا، هذا ما دفع الرئيس الامريكي "باراك اوباما" يصف الأمن السيبراني بأنه واحد من أخطر تحديات الأمن الاقتصادي والوطني التي نواجهها.³

هذا ما جعل الانفاق العالمي على أمن المعلومات يبلغ أكثر من 114 مليار دولار في عام 2018 بزيادة قدرها 4.12% عن العام 2017 وارتفع الى 124 مليار دولار في العام 2019 أي بزيادة قدرها 7.8 %⁴.

كما أن وسائل التواصل الاجتماعي لها تأثير كبير على الجماهير، حيث أصبحت اليوم تحظى باهتمام بالغ ومتنامي لدى معظم شعوب العالم، وقد تشكل تهديد للأمن القومي ومخاوف كبيرة من توجيه الرأي العام والتأثير عليه من خلال الدعايات المغرضة، وقد شهد العالم مدى تأثير وسائل التواصل الاجتماعي على منظومة الأمن الوطني، وظهر ذلك بشكل جلي خلال الحراك الشعبي العربي أو الاحتجاجات الجماهيرية سنة 2011 والتي كانت أولى شرارتها الفايسبوك، والتي أخذت فيما بعد شكل ثورات مسلحة دمرت الاوطان⁵، هذا ما جعل الكثير من الدول تهتم بالأمن السيبراني وجعلته ضمن اهتمامات أمنها القومي ليس في بعده التقني فقط بل يشمل مختلف الابعاد السياسية والاقتصادية والثقافية والاجتماعية والعسكرية، وتبنت عدة دول مقترح الأمن السيبراني ضمن استراتيجيتها الأمنية واعتباره جزء لا يتجزأ من منظومة الأمن الوطني للدولة، حيث أنشأت الولايات المتحدة الامريكية قيادة متخصصة تعنى بالأمن السيبراني وأعلنت من خلالها أن الفضاء السيبراني مجال جديد للحرب، كما يعتبر من بين الأولويات الثلاثة الأولى لمكتب التحقيقات الفيدرالية FBI هي مكافحة الارهاب والتجسس والهجمات السيبرانية، كما أضحت سرعة الهجوم وحجمه وقوته متاح للدول

¹ إيهاب خليفة، تنامي التهديدات السيبرانية للمؤسسات العسكرية، مجلة اتجاهات الاحداث، العدد 22، 2017، ص56.

² هاني مطر ابو سعود، ارتباطات الامن المعلوماتي بالأمن القومي، مجلة الدراسات الحقوقية، المجلد 07، العدد 02، جوان 2020، ص209.

³ مصطفى ابراهيم سلمان الشمري، الأمن السيبراني وأثره في الامن الوطني العراقي، مجلة العلوم القانونية والسياسية، المجلد 10، العدد الأول، 2021، ص167.

⁴ نفس المرجع، ص169.

⁵ نفس المرجع، ص161.

الكبرى والصغرى على حد سواء، فالدول القوية تستغل قوتها التكنولوجية والسيبرانية لمهاجمة الدول الضعيفة واختراقها والتجسس عليها مقابل ذلك تستغل الدول الصغرى الفضاء السيبراني لمهاجمة الدول القوية والعامل الحاسم هنا يكمن في الذكاء والابتكار.¹

المبحث الثاني

مفهوم الأمن الصحي

المطلب الأول: تعريف الأمن الصحي وأهميته في استقرار المجتمعات

الفرع الأول: تعريف الأمن الصحي

يعتبر الأمن الصحي أحد أبعاد الأمن الإنساني، وقد ظهر المصطلح لأول مرة في تقرير التنمية البشرية لسنة 1994، والذي يشير حسب التقرير الأمم المتحدة إلى "ضمان الحد الأدنى من انتشار الأمراض واتخاذ تدابير للوقاية منها"، كما عرفته لجنة أمن الانسان في تقريرها الصادر سنة 2003 على أنها الحماية من المرض والعجز من جانب آخر عرفته منظمة الصحة العالمية على أنه " حالة سلامة الجسم من الأمراض والأسقام البدنية والذهنية"²، كما عرف الأمن الصحي أيضا على أنه " مجموعة الأنشطة الاستباقية التي تؤدي الى تقليل التعرض لأحداث الصحة العامة بين السكان "³.

الفرع الثاني: أهمية الصحة في استقرار المجتمعات

تعتبر الصحة و الأمن الصحي عنصرا هاما في أداء وفعالية دور المؤسسات الدولة من خلال مخرجات للسياسة الرشيدة والتي تضع الفرد ضمن اهتمامه لضمان صحة جيدة لجميع أفرادها، ما يجعل صناع السياسية في وضع المرضي عليه من قبل المجتمع وسبيل نحو الاستقرار واستباب الأمن للدولة، خاصة في ظل مؤسسات تسهر على التصدي لمختلف التهديدات المحدقة بالأمن الصحي للبلاد، أين يشعر الفرد فيها بالأمن والصحة الجيدة والتي انعكاس للأمن السياسي للدولة، كما يعتبر أيضا الأمن الصحي عامل مهم في دفع عجلة التنمية الاقتصادية من خلال توفير عامل ماهرة تتمتع بصحة جيدة قادرة على الإنتاجية، كما تنعكس أيضا حالة اللا أمن الصحي على أمن الأفراد والدول، إذ يؤدي انتشار التهديدات الصحية وصعوبة وصول الأفراد للرعاية الصحية اللازمة الى تفاقم الوضع الأمني ويؤدي الى إحباط جماعي أين تتجه الأوضاع العنف

¹ نفس المرجع، ص 165.

² زوبر محمد خيثر، واقع الامن الصحي بالجزائر: دراسة تحليلية للمؤشرات الصحية لولاية عين الدفلى، مجلة نماء للاقتصاد والتجارة، المجلد 03، العدد 01، 2019، ص 05.

³ دستور منظمة الصحة العالمية، منظمة الصحة العالمية، متوفر على الرابط:

<https://www.who.int/governance/eb/constitution/ar>، تاريخ الاطلاع : 2024/10/17.

وانتقال الوضع الأمني من حالة الاستقرار الى حالة الفوضى، نظرا لارتباط الأمن الصحي بالأفراد وارتباط الأمن الصحي والفرد بالأمن القومي.¹

كما شهد الأمن الصحي تحولا كبيرا نظرا لتنامي تفشي الأمراض والأوبئة ليصبح ذات بعد عالمي ودولي في ظل العولمة ولتصبح التهديدات الصحية عابرة للقارات، خاصة في ظل انتشار الأمراض المعدية، لذلك سعت كثير من دول العالم للعناية بصحة مواطنها وجعلها ضمن أولى الأولويات، كونها قضية لا تتحمل أي جدال باعتبارها تتجاوز طاقة وحدود المواطن وقدرته على مواجهة عوارض الأوبئة بمفرده.²

لذلك فإن توفير الأمن الصحي للأفراد والمجتمعات من خلال مجموعة من الإجراءات المتعلقة بتوفير الأدوية ومرافق الرعاية الصحية وسهولة الوصول إليها وهي مرتبطة بعدة مقومات أساسية منها: سلامة البنية التحتية الصحية، فواعل صحية على قدر عال من الكفاءة الصحية، بنية البحث والتطوير متقدمة، إضافة إلى كفاءة منظومة الطوارئ للدول، وجود منظومة تكنولوجية متطورة قادرة على صد مختلف التهديدات الالكترونية، وقد جاء في ذات السياق توصيات مؤشر الأمن الصحي لسنة 2020 وفق هذه المقومات يتطلب على الدول بذل المزيد للتصدي لمخاطر الأمن الصحي.³

المبحث الثالث

تقاطع الأمن السيبراني بالأمن الصحي

الفرع الاول: إدخال الأنظمة التكنولوجية والرقمية في المجال الصحي

مع التطور التكنولوجي المتقدم تبنت الكثير من الدول إدخال المتغير التكنولوجي في معظم قطاعاتها الحيوية ومنها قطاع الصحة، أين اتجهت معظم الدول العالم نحو الصحة الرقمية أو ما يصطلح عليها بالصحة الذكية، وهو مشروع دعت إليه منظمة الصحة العالمية في الكثير من المناسبات، من خلال ضرورة الانتقال إلى الصحة الرقمية لمواكبة التطورات التكنولوجية الحديثة، حيث شهدت الأنظمة الصحية عقب ذلك تحولا كبيرا بفضل التكنولوجيا الرقمية التي ساهمت في خفض التكاليف الرعاية الصحية من جهة وتحسين جودة الخدمات وكفاءتها فاعليتها من جهة أخرى، وهذا بفضل إدخال الأجهزة الطبية المتطورة

¹وليد العويمر، اء كنعان جميل، الأمن الصحي وأثره على العلاقات الدولية، تريندز للبحوث والاستشارات، متاح على الموقع: <https://shorturl.at/X4fpQ>، تاريخ الاطلاع: 2024/10/17.

² عبد الله جعفر عزيز، الأمن الإنساني في ظل فيروس كورونا، متاح على الموقع: <https://feji.us/q1twra>، تاريخ التصفح: 2022/09/12.

³ احمد طليب، الأمن الصحي في الظروف الاستثنائية بين تكريس الحق وصناعة الوعي، مجلة دفاتر البحوث العلمية، المجلد 08، العدد 02، 2020، ص 65.

والمتصلة بشبكة الانترنت إضافة لرقمنة السجلات الالكترونية للمرضى ومراقبتهم عن بعد مع إجراء عمليات جراحية وتقديم استشارات طبية عن بعد، مع استخدام أجهزة الذكاء الصناعي في التشخيص الطبي، وهنا أضحت معظم تفاصيل صحتنا رهينة ملفات الكترونية وأنظمة معلوماتية ومزودي خدمات إلكترونية الذين يملكون معلومات شخصية عن الكثير من الناس بدءا بتفاصيل الهوية الشخصية مروراً بالبيانات الديموغرافية والمعلومات الصحية الشخصية أو العائلية كالسجل الطبي والوصفات الطبية الالكترونية والحالة الصحية الراهنة والعلاجات التي نخضع لها وغيرها .

كما زادت وتيرة الاعتماد على الصحة الرقمية أو الذكية بشكل كبير خلال جائحة كورونا، إذ فرض الوضع الصحي الاستثنائي ضرورة التطبيب عن بعد، حيث كشفت دراسات تشير الى أن نحو 49% من الأشخاص خلال سنة 2021 اعتمدوا على الرعاية الصحية عن بعد، وهذا زيادة تقدر بأربعة أضعاف عن سنة 2018 التي لم تتعدى فيها النسبة 12%، وقد ساعدت هذه الخطوات في تسهيل عمليات الرعاية الصحية وتوفير الوقت والجهد.¹

وعقب انتشار فيروس كورونا - covid19 أعلنت منظمة الصحة العالمية في 11 مارس 2020 عن تصنيف الوباء على أنه جائحة، وهذا بعد اتساع نطاق انتشاره على المستوى العالمي، وأدخل الدول والمؤسسات المحلية والدولية في حالة استنفار قصوى، وأعدت من خلالها الدول والحكومات استراتيجيات مختلفة للحد من هذا الوباء القاتل، ومن بين تلك الآليات المستخدمة في مكافحة الوباء المستجد توظيف التكنولوجيا الرقمية سعياً لاحتواء الفيروس والتقليل من حدته، ومن بين الدول السبّاقة في ذلك الصين التي استخدمت الروبوتات الألية لمساعدة الطواقم الطبية في التشخيص وذلك بسبب محدودية الطواقم الطبية مقارنة بعدد الاصابات المتزايدة بشكل يومي، حيث تقوم الروبوتات بالكشف على المرضى، وتسجيل حالاتهم الطبية وتصنيف درجة خطورتهم وحفظ البيانات الصحية مثل العمر ودرجة الحرارة والأمراض الأخرى التي يعانون منها، ثم يرفع التقرير للطواقم الطبية التي تحدد نوعية العلاج والجرعة اللازمة، كما تقوم روبوتات أخرى بتوصيل العلاجات والمواد الطبية المقررة إلى المرضى، دون أن يحدث احتكاك مباشر بينهم وبين الطاقم الطبي، وذلك لمنع اتساع دائرة انتشار المرض وتقليل من درجة الاحتكاك بالمرضى، كما وظفت أيضاً سيارات إسعاف ذكية دون سائق تقوم بنقل الحالات المصابة إلى المستشفيات، حيث تستطيع هذه السيارات حمل 6 أشخاص مصابين دفعة واحدة، كما استخدمت أيضاً طائرات "الدرونز" في عمليات المسح السريع للمارة في الشوارع وتقديم الإرشادات والتعليمات الطبية والتوعوية مع الكشف العشوائي عن الحالات التي يمكن أن تكون مصابة، من خلال قياس درجة حرارتها بالاعتماد على كاميرات حرارية تحملها هذه

¹ ما هو دور التكنولوجيا في الرعاية الصحية؟ وكيف تلحق بركبها؟، ميسر للخدمات الطبية، متاح على الموقع: <https://shorturl.at/ioTPF>، تاريخ التصفح: 2024/10/17.

الطائرات، ويتم تشخيص الحالة المصابة عبر المختصين في غرف التحكم المركزية، ترافقها طائرات أخرى بدون طيار استخدمت في عمليات التعقيم عبر رش المواد المطهرة في الشوارع المزدحمة¹.

كما وضفت اليابان أيضا روبوتا يحمل اسم Robear يعمل كممرض داخل المستشفيات ويؤدي مهام متعددة، من بينها الحد من التعامل المباشر مع المرضى المصابين، كما استخدمت كوريا الجنوبية وتايوان برامج ترصد مسار المريض والأماكن التي زارها قبل ظهور أعراض المرض، وبالمثل استخدمت موسكو شبكة الكاميرات المنتشرة في الأماكن العامة، والتي تضم حوالي 170 ألف كاميرا، تتمتع بتقنية التعرف على الوجوه، بحيث تسجل السلطات صور المرضى، وتراقب أيضا مدى التزام المرضى بأوامر الحجر الصحي وعدم مخالفة تعليمات العزل ومغادرة المنزل نحو الشوارع دون إستشارة طبية².

واستخدمت أيضا الشركة الأمريكية لتوصيل الأدوية Zipline طائرات بدون طيار في خضم أزمة كوفيد-19 لنقل اللقاحات ما بين المدن وهذه الشركة لها خبرة وتجربة رائدة في نقل لقاحات شلل الاطفال والحمى الصفراء في روندا وغانا وغيرها من البلدان الافريقية³.

من جانب آخر وظفت أيضا تكنولوجيا الأقمار الصناعية من قبل الولايات المتحدة الأمريكية في عمليات التجسس على المواقع الطبية وأماكن الدفن لإحصاء عدد الضحايا في الصين بعد التكتّم الشديد للصين حول العدد الحقيقي للمصابين والوفيات، كما وظفت أيضا دول أخرى تكنولوجيا السياج الالكتروني لإخطار السلطات المعنية عندما ينتقل المواطنون من مناطق الحجر الصحي، وفي ذات السياق تم استغلال بيانات الهواتف الخلوية لتعقيب المصابين بفيروس كورونا⁴.

وهذا وقد ساهم توظيف التكنولوجيا الرقمية في خضم أزمة كوفيد في إنقاذ الكثير من الارواح وسهلت أيضا من مهمة الطواقم الطبية والأمنية في عملية المراقبة والعزل الصحي في وقت قصير، كما قللت أيضا من حدة انتشار فيروس كورونا على نطاق واسع.

¹ ايهاب خليفة، كيف توظف الصين التكنولوجيا لمكافحة الفيروس، مركز المستقبل للأبحاث والدراسات المتقدمة، تم التصفح يوم متاح على الموقع: <https://shorturl.at/548Ms>، تاريخ التصفح: 2020/09/11.

² طه الراوي، كيف تعزز التكنولوجيا الرقابة الصحية ضد الامراض؟، متاح على الموقع:

<https://www.noonpost.com/content/36540>، تاريخ التصفح: 2022/03/22.

³ متاح على الموقع: <https://shorturl.at/2G0yn>، تاريخ التصفح 2022/12/10.

⁴Gordon Corera, Coronavirus: How will it change national security and spying?,available at : <https://shorturl.at/y5mJh> ,accecced at:12/03/2022.

الفرع الثاني: مخاطر الهجمات السيبرانية على القطاع الصحي

وبالرغم من الانتشار الواسع والكبير لهذه التكنولوجيا الناشئة في مجال الرعاية الصحية، إلا أنها لم تسلم هي الأخرى من مختلف المخاطر والتهديدات الالكترونية والهجمات السيبرانية كالقرصنة الالكترونية على المستشفيات والمخابر البيولوجية التابعة لها وسرقة السجلات الالكترونية للمرضى وبيعها عبر النت.¹

ووفقا لبعض الإحصائيات الصادرة عن معهد Cyber Peace Institute الذي يشير الى سرقة نحو 10 ملايين سجل طبي للمرضى مع نتائج اختبارات فيروس نقص المناعة البشرية وصولا لبعض تفاصيل الخاصة بالمتبرعين ،كما تشير احصائيات أخرى إلى قرصنة نحو 03 ملايين سجل طبي عبر شبكات المستشفيات ومؤسسات الرعاية الصحية، إضافة لهجمات أسفرت عن تعطيل مؤسسات الطبية بشكل كبير، ما عرضها لخسارة مالية فادحة، ناهيك عن تعرض صحة وسلامة المرضى للخطر نتيجة توقف الخدمات الصحية الحيوية وتعرضها للقرصنة والهجمات السيبرانية، ومن بين هذه الهجمات الهجوم الذي شنه القراصنة والمتسللين على هيئة الخدمات الصحة الوطنية البريطانية في ماي سنة 2017 التي أدت الى حظر الوصول للأنظمة المعلوماتية ومنع الموظفون من الوصول إلى بيانات المرضى والخدمات الصحية الحساسة، أين أجبر على الغاء آلاف المواعيد الطبية والعمليات الجراحية، إضافة إلى هجوم ثاني وقع سنة 2018 على مجموعة "سنغافورة للخدمات الصحية" الذي يعتبر أكبر مؤسسة للرعاية الصحية في دولة سنغافورة، حيث أدى الهجوم إلى سرقة البيانات الشخصية لحوالي 1.5 مليون مريض بما في ذلك الوصفات الطبية لرئيس وزراء سنغافورة "لي هسين لونغ"، كما شهدت استراليا هي الأخرى حوادث مماثلة من بينها إستهداف مستشفيات تابعة للتحالف الصحي بأستراليا الذي أدى إلى تأخر العمليات الجراحية وخدمات المرضى كون العطب والاختراق أدى إلى منع الوصول لعدة أنظمة معلوماتية صحية بما فيها نظم الادارة والمالية، وشهدت الولايات المتحدة الامريكية هي الأخرى حوادث مماثلة في اكتوبر 2019 أين تم استهداف النظام الصحي لمجمع مستشفيات "درويد" والمراكز الطبية الاقليمية، والذي أدى الى توقف رعاية المرضى بسبب ظهور شفرة الفدية ودعوة القراصنة لدفع الفدية مقابل استئناف خدمات الرعاية الصحية، وتعرضت أيضا مجموعة "لايف هيلث كير" Life Healthcare أيضا بجنوب افريقيا في يونيو 2020 لهجوم الكتروني على أنظمة التشغيل المتعلقة بتقديم الخدمات الطبية للمرضى.²

¹ احمد البيكاوي، تهديدات الامن السيبراني وقطاع الرعاية الصحية في زمن الازمة، مجلة القبس، متاح على الموقع: <https://shorturl.at/xFIOP>، تاريخ التصفح 2023/01/10.

² نيكي اوبراين، جاي مارتن وآخرون، تقرير حول حماية نظم الرعاية الصحية، مؤتمر القمة العالمي الابتكار في الرعاية الصحية، 2020، ص13.

ولم تقتصر الهجمات السيبرانية على المستشفيات والمراكز الصحية فقط، بل امتدت الى استهداف المراكز البحثية المتعلقة بالتكنولوجيا الحيوية بسبب القصور في حماية الأنظمة المعلوماتية لتلك المراكز، حيث تعرضت شركات الأدوية لسرقة الملكية الفكرية وكذلك المراكز العلمية المخصصة للبحوث في مجال الفيروسات سواء من ناحية التهجين أو التخزين، مثل تقنية كريسبر CRISPR التي تستخدم للأغراض العلاجية والشفاء من بعض الامراض، إلا أن هذه التقنية الطبية سلاح ذو حدين وتحمل الداء والدواء في نفس الوقت، حيث برزت هناك مخاوف من التلاعب الجيني بواسطة هذه التقنية لإنتاج سلالات منقرضة من الفيروسات ووقوعها بين أيدي المحتالين والقراصنة البيولوجيين عبر الانترنت واستغلالها لأغراض إجرامية، ما تطلب حماية أمنية كبيرة نظرا لجسامة خطورتها¹، حيث برزت هناك مخاوف كبيرة في مجال التكنولوجيا الحيوية من جراء تسرب ونقل بعض الشفرات الجينية واستخدامها لأغراض إرهابية كخلق مرض شديد العدوى معدل وراثيا في المخابر البيولوجية من خلال التلاعب بترتيب تسلسل الجينوم بواسطة البيولوجيا التركيبية وتوصل بعض الخبراء البيولوجيين في كندا لخلق فيروس الجدري مختبريا²، ونجح أيضا مجموعة من الباحثين الأستراليين سنة 2001 بهندسة سلالة من فيروس الفئران جديدة لأغراض علاجية ، كما يمكن استخدام هذه السلالة الجديدة لهندسة سلالات من فيروس الجدري أكثر فتكا ورعبا³.

وفي أغلب الأحيان يتم تبادل المعلومات البيولوجية التي تمت قرصنتها أو ما يسمى بالإرهاب البيولوجي عبر الشبكة المظلمة مثل Silk Road وAlphaba وقد عرضت سنة 2017 السجلات الصحية للأستراليين للبيع عبر مواقع الويب المظلم⁴، خاصة في ظل توفر المصادر المفتوحة للتكنولوجيا الحيوية في العصر الرقمي، حيث أصبحت متاحة للجميع ودون رقابة، أين يمكن الولوج الى الأبحاث العلمية والاطلاع على تجارب حول البيولوجيا التركيبية، كما يمكن أيضا شراء الحمض النووي المركب من الشركات التجارية ومصنعي الحمض النووي عبر الانترنت كون العديد من الأبحاث العلمية توفر المجال الأمن الوصول المفتوح الى المقالات التي تقدم تفاصيل حول كيفية إجراء تجارب البيولوجيا التركيبية⁵.

¹ SMITH, Marcus et WALSH, Patrick. Improving health security and intelligence capabilities to mitigate biological threats. The International Journal of Intelligence, Security, and Public Affairs, vol. 23, no 2, 2021, p 04.

² RAINA MACINTYRE, C., ENGELLS, Thomas Edward, SCOTCH, Matthew, et al. Converging and emerging threats to health security. Environment Systems and Decisions, vol. 38, no 2, 2018, p199 .

³ JIN, Andrew et LINKOV, Igor. Synthetic Biology Brings New Challenges to Managing Biosecurity and Biosafety. Emerging Threats of Synthetic Biology and Biotechnology, 2021, p.124

⁴ RAINA MACINTYRE,op ,cit , p.199

⁵ JEFFERSON, Catherine, LENTZOS, Filippa, et MARRIS, Claire. Synthetic Biology and Biosecurity: How scared should we be?. 2014., p25.

وفي خضم جائحة كورونا ارتفعت عدد الهجمات السيبرانية الموجهة ضد مؤسسات الرعاية الصحية بشكل كبير مقارنة من ذي قبل ، حيث استهدفت المؤسسات الصحية في الوقت الذي حشدت فيه المؤسسات الصحية جهودها لمواجهة فيروس كورونا، والبداية كانت تعرض منظمة الصحة العالمية وعدد من المستشفيات والمؤسسات الطبية لقرصنة واختراق وهجمات سيبرانية متتالية بحثا عن معلومات متعلقة بعلاجات واختبارات ولقاحات لفيروس كورونا، وقد تعددت آليات وصور القرصنة، حيث ادعى القراصنة والمتسللين بأنهم مسؤولين كبار في منظمة الصحة العالمية، أين يقومون بنشر روابط وهمية لصناديق التبرع بإسم منظمة الصحة العالمية مستخدمين بذلك شعارات لمنظمة الصحة العالمي ، كما تم اختراق العديد من مواقع وزارات الصحة، واستهدف الأطباء والعاملين في المؤسسات الرعاية الصحية عبر رسائل الكترونية وهمية تحمل بعضها برامج ضارة لغرض الصيد الاحتيالي، كما استهدفت أيضا أنظمة المستشفيات الخاصة والحكومية بهجمات الفدية، حيث شهد شهر سبتمبر من عام 2020 تسجيل حالة وفاة بشرية جراء هجوم الفيروس الالكتروني "الفدية" الذي سبب عطل في أنظمة تكنولوجيا المعلومات في المستشفى بجامعة "دوسلدورف" الألمانية ما أدى لوفاة امرأة¹، كما تعرضت بعض الدول لهجمات سيبرانية على قطاعاتها وهيكلها الصحية على غرار كندا التي رصدت العديد من التهديدات السيبرانية خلال أزمة كورونا من قبل جهازها الاستخباري، ما أدى إلى إطلاق حملة تحذيرات من قبل مؤسسة أمن الاتصالات الكندية لقطاع الصحة بشأن احتمال استهداف المستشفيات والمؤسسات الصحية العاملة في البلاد، حيث أسدت إليها توصيات بضرورة اتخاذ الاحتياطات بشأن انتشار المعلومات المضللة المنتشرة عبر الانترنت².

وفي ذات السياق شهدت جمهورية التشيك هي الأخرى هجمات إلكترونية على نظام الحواسيب لأحد المستشفيات الجامعية في مدينة "برنو"، ما تسبب في تعطيل أحد أكبر مختبرات فحص فيروس كورونا في الجمهورية، وتسبب أيضا فيروس "الفدية" في تعطيل نظام الصحة العامة المستخدم لإدارة المعلومات المتعلقة بجائحة كورونا في مدينة "تشمبين" بمقاطعة إلينوي بالولايات المتحدة الأمريكية³.

وبحسب وكالة الأمن السيبراني التابع للاتحاد الأوروبي (Enisa) فإنه في خضم أزمة كورونا ارتفعت الهجمات الإلكترونية على المستشفيات وشبكات الرعاية الصحية بنسبة 47%، شلت الهجمات الإلكترونية من خلالها مستشفيات "داكس" و"فيلفرانش"، "سورساو" لدرجة أن العاملين الصحيين اضطروا للعودة

¹ محمود محمد حامد، الهجمات الالكترونية في عصر فيروس كورونا (Covid-19)، متاح على الموقع: <https://rb.gy/ujen14>، تاريخ التصفح: 2022/03/22.

² Stéphanie carvin, National Security and pandemics the limits of early warning, available at : <https://rb.gy/0xnum6>, accessed at: 12/03/2022.

³ ذو الهدى سني، كورونا وانتشار الهجمات السيبرانية الارهابية، متاح على الموقع: <https://shorturl.at/b6Dsh>، تاريخ التصفح: 2022/05/22.

إلى استخدام الوسائل التقليدية مثل القلم والورق، كما أسفر هجوم إلكتروني آخر إلى تدمير شبكة تكنولوجيا المعلومات التابعة للخدمات الصحية الأيرلندية بواسطة فيروس "فدية" من قبل فرقة قراصنة تدعى Wizard Spider، وهي مجموعة مجرمين إلكترونيين¹.

ويشير خبراء الأمن السيبراني إلى أن قطاع الرعاية الصحية كان في مقدمة القطاعات التي تعرضت للهجمات الإلكترونية من خلال هجمات برامج "الفدية"، كون المؤسسات الصحية ستضطر إلى دفع الأموال لاستعادة أنظمتها التي تعتمد عليها في مواجهة انتشار الفيروس، فضلاً عن أعداداً كبيرة من المخترقين يستغلون أزمة فيروس كورونا لبيع الأدوات الطبية المزيفة، وانتحال شخصيات لمسؤولين حكوميين ونشر ادعاءات بالتوصل إلى علاجات جديدة لفيروس كورونا والترويج لمنتجات طبية وهمية بملايين الدولارات².

الفرع الثالث: حماية البنى التحتية الصحية

في ظل التدفق الهائل للمعلومات واستخدامها على نطاق واسع خاصة في البنى التحتية الحيوية، أصبح من الضروري حماية أمن المعلومات والشبكات من مختلف الهجمات السيبرانية المتعددة التي تلحق ضرر بالأفراد وتعطل الخدمات الأساسية، لذلك وجب حماية المنشآت الرئيسية لضمان سيرورة عملها خاصة المنشآت الصحية التي لها ارتباط وثيق بحياة الأفراد، باعتبارها أكثر القطاعات استهدافاً من قبل مجرمي الانترنت بسبب وفرة المعلومات والطابع الاستعجالي للقطاع في دفع الفدية في حالة تعطله، حيث كشفت بعض التقارير لسنة 2022 عن وجود 1463 هجوم أسبوعياً³، وتؤدي طول فترة الإغلاق بسبب الهجمات السيبرانية على القطاعات الصحية إلى عواقب وخيمة مثل تعطل الأجهزة الطبية المرتبطة بالشبكات وتعثر فترة الاستشفاء، حيث تعرضت مستشفيات كندا لهجمات سيبرانية سنة 2019 كلفها دفع فدية كبيرة مقابل استعادة بيانات نحو 15 مليون مريض⁴.

لذلك يتوجب حماية دور الرعاية الصحية من الهجمات السيبرانية لضمان سيرورة عملها، وذلك من خلال الاستثمار في تكنولوجيا الدفاع السيبراني وتنفيذ تدابير أمنية خاصة بتكنولوجيا المعلومات كتشفير البيانات والمراقبة المستمرة لنشاط الشبكة وحمايتها، إضافة إلى إجراء اختبارات منتظمة للكشف عن الثغرات الأمنية وتحديد نقاط الضعف ومنع استغلالها من قبل مجرمي الانترنت، وتدريب العاملين والموظفين

¹ ملف امن سيبراني - مخاطر الهجمات السيبرانية، التظليل الاعلامي وانتهاك الخصوصية، المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات، متاح على الموقع: <https://shorturl.at/HdHrz>، تاريخ التصفح: 2022/05/12.

² احمد داليا السيد، لماذا تصاعد خطر الهجمات الالكترونية في خضم أزمة كورونا، متاح على الموقع: <https://shorturl.at/16Lap>، تاريخ التصفح: 2022/03/02.

³ Elena Canorea, Protecting critical infrastructure from cyber-attacks, available at : <https://shorturl.at/QULoP>, accessed at: 17/10/2024.

⁴ Owens, Brian. "How hospitals can protect themselves from cyber attack." (2020): p03.

على ممارسات تكنولوجيا أمنة بمعنى يجب على الموظفين دراية بمخاطر الهجمات الالكترونية¹، إضافة إلى تقيد الوصول العشوائي إلى الشبكات الالكترونية الخاصة بالصحة إلى من طرف طبيب، مع تأمين البريد الالكتروني الذي يتم تبادل المعلومات الطبية عبره، مع تطبيق مبدأ الثقة الصفرية في مجال الأمن السيبراني وهي استراتيجية أساسية لحماية القطاع الصحي من الهجمات السيبرانية ومنع الوصول لها². إضافة إلى نقاط أخرى يمكن اجمالها فيما يلي:

- تخزين المعلومات والبيانات الأنظمة التشغيلية على وسيط خارجي.
- الإلتزام بالتشفير العالي أثناء نقل البيانات عبر الشبكة، وحمايتها من كل أشكال التجسس والاستخدام غير المصرح به.
- نسخ المعلومات والبيانات بشكل احتياطي لإستعادتها في حال فقدانها.
- تحسين أمن التطبيقات ورفع مستوى الحماية البرمجية.
- تحديث البرامج والأنظمة المعلوماتية لسد الثغرات.
- الرصد الأمني لمختلف الأنشطة السيبرانية وضمان الاستجابة السريعة³.

المبحث الرابع

دور الأمن السيبراني في تعزيز الامن الصحي

المطلب الأول: تأمين البيانات الصحية

يشير أمن البيانات إلى مجموعة من التدابير التي يتم تنفيذها لحماية بيانات المرضى داخل مؤسسات الرعاية الصحية ويشمل مجموعة واسعة من الضمانات وبروتوكولات الأمان التي تهدف إلى منع الوصول غير المصرح به للبيانات، حيث تخزن المراكز الرعاية الصحية والمستشفيات كميات هائلة من المعلومات والبيانات الصحية للمرضى ما يجعلها هدف مغرى للقراصنة والمحتالين، فمع ارتفاع حجم المعلومات المخزنة ترتفع معها التهديدات الخصوصية والأمان، لذلك فإن تأمين البيانات الصحية يتطلب جملة من الإجراءات الفنية والإدارية من بينها

- تثقيف موظفي الرعاية الصحية بضرورة الحفاظ على الأمن المعلوماتي للمرضى باعتبار العنصر البشري أحد أكبر التهديدات في مجال الرعاية الصحية، حيث يمكن أن يؤدي الخطأ البشري بسبب الإهمال أو التواطئ الى عواقب وخيمة ومكلفة.

¹ Recommendations to prevent a cyber attack in the health sector, available at : <https://shorturl.at/JgP1W>, accessed at:17/10/2024.

² What is Healthcare Cybersecurity?,available at : <https://shorturl.at/3Jvyo>, accessed at:17/10/2024.

³ الأمن السيبراني مفهومه وتاريخه، الجزيرة نت، متاح على الموقع: <https://shorturl.at/VlkY5> ، تاريخ التصفح:2024/10/17.

- تقيد الوصول الى البيانات ووضع ضوابط صارمة من شأنها ان يؤدي تعزيز حماية البيانات الطبية¹
- التقليل من مخاطر الأجهزة المتصلة بأنترنت الأشياء والمراقبة الدورية لها لصد أي اختراق.
- تشفير البيانات المخزنة والمرسلة وجعلها غير قابلة للقراءة باستثناء المستخدمين.²
- التحكم الجيد في استخدام البيانات الصحية وتأمينها كحظر التحميل عبر الويب ونسخ البيانات على الأقراص الصلبة الخارجية هذا ما يؤدي الى تقليل الهجمات السيبرانية.
- التخلص من المعدات القديمة التي تعتبر أكثر الأجهزة عرضة للاختراقات واستبدالها بمعدات جديدة ذات تقنيات حديثة، إضافة الى الابتعاد عن الأجهزة ذات الاتصال اللاسلكي التي نعتبر هدف سهل للاختراقات.
- تعزيز الأمن الكافي للأجهزة الطبية التي تعمل بنظام اللاسلكي مثل أجهزة الأشعة السنية وأجهزة التصوير بالرنين المغناطيسي³.

المطلب الثاني: حماية الأنظمة الصحية والاستجابة للهجمات السيبرانية

لقد بلغ مستوى الاختراقات في مجال القطاع الصحي ذروته في سنة 2021، أين تعرضت العديد من المؤسسات الصحية الى اختراقات عديدة بغية الحصول على المعلومات الصحية لغرض الابتزاز أو بيعها، حيث يعادل بيانات السجل الطبي نحو 40 ضعفا بيانات بطاقات الائتمان المسروقة بسبب أن السجلات الطبية تحتوي على الكثير من المعلومات من أرقام الضمان الإجتماعي الى المعلومات الشخصية وحتى المالية⁴

وقد أشار تقرير للشرطة الدولية (الإنتربول) الصادر سنة 2020 إلى أن وباء كورونا "كوفيد-19" شجع على تصاعد الهجمات الإلكترونية في حوالي 50 دولة، استهدفت بشكل متزايد المؤسسات الصحية، أين رصدت الشرطة الدولية خلال الأربعة الأشهر الأولى من سنة 2020 نحو 907 آلاف رسالة إلكترونية غير مرغوب فيها و737 حادثة ناجمة عن برامج خبيثة و48 ألف رابط لعناوين مواقع إلكترونية ضارة، كلها تتعلق بفيروس كورونا المستجد وكشف أيضا تقرير صادرة عن شركة "مايم كاست"، بعنوان "100 يوم من فيروس كورونا" عن إرتفاع عدد الجرائم الإلكترونية بنسبة 33 % منذ مطلع العام 2020 حتى نهاية مارس من العام نفسه، مع زيادة في عدد زيارات الروابط غير الآمنة أكثر مما كان قبل تفشي الوباء، كما زادت عدد رسائل البريد الإلكتروني المخادعة أكثر من 600% منذ شهر فبراير 2020، حيث استهدف المخترقون الأشخاص والمؤسسات

¹ Nate Lord, Healthcare Cybersecurity: Tips for Securing Private Health Data, available at : <https://shorturl.at/fHXuI>, accessed at: 17/10/2024.

² Aline Liu, 6 steps to protect your healthcare data, available at : <https://shorturl.at/Gau6P>, accessed at: 18/10/2024.

³ Healthcare data security: safeguarding patient information in the digital age, available at : <https://shorturl.at/eAFvO>, accessed at: 18/10/2024.

⁴ How To Prevent Security Breaches In Healthcare, available at : <https://shorturl.at/rmRgr>, accessed at : 18/10/2024.

من خلال روابط مشبوهة واختراق البريد الإلكتروني للحصول على بيانات الدخول إلى الحسابات المالية، وأنشأوا بذلك قرابة من 100 ألف موقع جديد عن فيروس كورونا "كوفيد-19" بغرض سرقة المعلومات والبيانات الخاصة وبيعها، وبحسب تقرير صادر عن شركة حلول الأمن السيبراني Check Point أنه تم إنشاء أكثر من 4 آلاف موقع إلكتروني خاص بكورونا لغرض الاحتيال¹.

هذا ما أفرز تحدي كبير حول كيفية الحفاظ على سلامة الأنظمة الصحية وأمنها بما يضمن استمرار عمل المؤسسات الرعاية الصحية وتحقيق الأمن الصحي في البلاد، وذلك من خلال السعي نحو تأمين النظم الصحية الإلكترونية وضمان تبادل المعلومات والوصول إليها بشكل آمن، وقد بذلت العديد من المؤسسات الصحية جهود كبيرة في مجال الحفاظ على الأنظمة الصحية لمؤسساتها من خلال التصدي للتهديدات الخارجية التي تأتي من قبل المتسللين ومجرمي الأنترنت ومن الداخل نتيجة سوء استغلال المعطيات البيانية الصحية، والتقليل من الهجمات السيبرانية إلى أقصى مستوى ممكن وحماية أنظمة الحاسوب والشبكات والبيانات من السرقة أو الوصول الغير المصرح به، وهذا بواسطة مجموعة من التدابير مثل برامج مكافحة الفيروسات جدران الحماية وتقنيات التشفير العالية².

كما فعلت الكثير من الدول منظوماتها فيما يخص الأمن السيبراني للتصدي للهجمات السيبرانية، منها ألمانيا التي فعلت مركز الدفاع السيبراني، وأعادت فرنسا تشكيل وحدة لمكافحة القرصنة الإلكترونية التي نجحت خلال فيروس كورونا في صد أكثر 800.000 هجوم حول العالم³، كما تعاونت كل من الولايات المتحدة الأمريكية وبريطانيا من خلال المركزين وكالة الأمن السيبراني CISA الأميركية والمركز الوطني البريطاني للأمن السيبراني على التصدي لمختلف الهجمات السيبرانية خاصة تلك المتعلقة بالقطاع الصحي⁴.

إلى جانب ذلك بذلت الشركات جهود كبيرة على غرار شركة "مايكروسوفت" وشركة "مكافي" لحماية البيانات ومحاربة برمجيات الفدية والتصدي لتهديدات البرمجيات الخبيثة في صورة تحالف سمي Ransomware Task Force، حيث وظفت أيضا بريطانيا وحدة هجومية المعروفة باسم القوة السيبرانية الوطنية National Cyber Force وهي وحدة تابعة لوكالة الاستخبارات البريطانية التابعة لوزارة الدفاع

¹ أحمد داليا السيد، لماذا تصاعد خطر الهجمات الإلكترونية في خضم أزمة كورونا، متاح على الموقع: <https://shorturl.at/16Lap>، تاريخ التصفح: 2022/03/02.

² محمد عبد الله الشيبة، الأمن السيبراني.. استراتيجيات التصدي والحماية، صحيفة الاتحاد، متاح على الموقع: <https://www.aletihad.ae>، تاريخ التصفح: 2024/10/17.

³ بسمة فايد، حروب السيبرانية ... ترسانات رقمية وتهديدات دولية، متاح على الموقع: <https://rb.gy/yixw2v>، تاريخ التصفح: 2022/03/22.

⁴ "هجوم خبيث" يستهدف المؤسسات العاملة في التصدي لكورونا، متاح على الموقع: <https://rb.gy/qpp27q>، تاريخ التصفح: 2022/05/03.

الملكي، وبدأت عملها بشكل سري منذ مطلع 2020 ويتمحور هدفها الأساسي في تعطيل الاتصالات التي تمثل تهديدا للمملكة¹، كما أعلنت "الشبكة الأوروبية الاستجابة لحوادث أمن الكمبيوتر" رفع درجة التأهب والاستعداد للتصدي للهجمات الإلكترونية التي تستهدف الخدمات الصحية ومراكز البحوث².

المبحث الخامس

تطبيق الأمن السيبراني في القطاع الصحي (التحديات والحلول)

المطلب الأول: التحديات

لقد خضع القطاع الصحي لتحول رقمي كبير أين تم إدخال أنظمة رقمية متطورة سهلت من سيرورة القطاعات الصحية، لكن صاحب ذلك عدة تهديدات وتحديات يمكن اجمالها فيما يلي:

- تزايد الأجهزة الطبية المتصلة بالإنترنت: يتصل بالمستشفيات عدد هائل من الأجهزة الطبية في شبكة واحدة ما يجعلها هدف محتمل للمهاجمين للتسلل لتلك الشبكة من خلال اختراق جهاز واحد فقط للسيطرة على كامل الشبكة واختراق الأجهزة الطبية³.
- تزايد الهجمات على القطاعات الصحية: لقد شهد القطاع الصحي تزايد كبير في الهجمات الإلكترونية من قبل مجرمي الإنترنت كون القطاع الصحي مربح نظرا للملفات الطبية الهائلة التي تحتوي على المعلومات المربحة، وأصبح برامج التحايل الفدية أكثر البرامج المنتشرة في القطاعات الصحية أين يقوم المهاجمين على تشفير البيانات الطبية مقابل دفع أموال لاستعادة الملفات، وعادة ما يتم الهجوم على الأجهزة القديمة التي تفتقد إلى ميزة الأمان وهذه الأجهزة في تزايد كبير نظرا للتكلفة الباهظة للأجهزة الحديثة.
- القيود المالية والبشرية: تعاني الكثير من المؤسسات الصحية من نقص في الموارد المالية والميزانيات المرصودة في اقتناء الأجهزة المتطورة ذات الأمان العالي من جهة والقيام بتدابير الحماية للأجهزة القديمة من جهة أخرى، ما يجعل الأنظمة الصحية عرضة للهجمات والاختراقات الإلكترونية، إضافة إلى نقص موظفي الأمن السيبراني

¹ رعد البيبي، الأمن السيبراني في 2020: بين الفرص والتحديات والحماية، متاح على الموقع: <https://shorturl.at/4BdYF>، تاريخ التصفح: 2023/05/08.

² أسماء قنديل، طرق حماية الأمن الرقمي ضد هجمات الهاكرز أثناء فترات الأوبئة والكوارث، متاح على الموقع: <https://rb.gy/ytr5ab>، تاريخ التصفح: 2022/03/22.

³ Cybersécurité dans le secteur de la santé : le scénario, les risques et les défis futurs, safecore, available at : <https://shorturl.at/hpHI3>, accessed at: 17/10/2024.

المتخصصين في دور الرعاية الصحية والمستشفيات ما يعقد من صعوبة معالجة التهديدات السيبرانية بشكل فعال.¹

- مخاطر مرتبطة بعوامل خارجية: تعمل مؤسسات الرعاية الصحية مع العديد من المؤسسات الخارجية مثل مصنعي الأجهزة الطبية وبائعي المعدات، حيث يمكن لهؤلاء تشكيل مخاطر سيبرانية.²

- الخطأ البشري: يشكل الأخطاء البشرية أحد التحديات الكبيرة للأمن السيبراني في القطاع الصحي، وقد يكون الخطأ البشري عن قصد أو غير متعمد من خلال سوء استعمال البيانات أو تسريبها بالإغراء، وهذا ما يلحق ضرر كبير بالقطاع الصحي.³

المطلب الثاني: الحلول

إن حماية القطاع الصحي من الهجمات السيبرانية يتطلب عدة تدابير منها:

- سن قوانين وتشريعات صارمة كالمساءلة في حالة وقوع هجمات سيبرانية، إضافة إلى اللوائح والارشادات المتعلقة بتحسين عمل الامن السيبراني في المراكز الصحية والهدف منها وضع معايير دنيا للأمن السيبراني في مجال الرعاية الصحية مثلما هو معمول به في الولايات المتحدة ودول الاتحاد الأوروبي.⁴
- إجراء تقييمات منتظمة ودورية لصد أي هجوم، وهذا كإجراء استباقي، حيث تؤدي هذه العملية إلى تحديد نقاط ضعف في أمن المؤسسات الصحية وتدارك الثغرات والتقليل من الاخطار المحتملة.⁵
- تدريب الكوادر الطبية والإدارية على مخاطر الامن السيبراني وتجنب الهجمات السيبرانية، كون الخطأ البشري يعتبر الأكثر شيوعا والذي يصعب الحد منه.
- تحديث الأنظمة الالكترونية بشكل دوري لسد الثغرات الأمنية ومنع تسلل المحتالين ومجرمي الانترنت.
- التعاون والتواصل اثناء الهجوم السيبراني كون التعاون المتعدد الأطراف يساهم في تنسيق الاستجابة والتصدي للهجمات السيبرانية خاصة مع خبراء الامن السيبراني والهيئات الأمنية والقضائية، إضافة إلى الاستفادة من الحوادث السابقة وتحليل أسبابها بغرض تحسين خطط الاستجابة مستقبلا.⁶

¹ Cyber Security Challenges in the Healthcare Industry, available at : <https://shorturl.at/o5tV1> ,accessed at:17/10/2024.

² Healthcare Cybersecurity, available at : <https://shorturl.at/mjIDV> ,accessed at:17/10/2024.

³ Altay Ataman, Cybersecurity in Healthcare: 7 Challenges & 10 Best Practices in '23,available at : <https://shorturl.at/jm1mW> ,accessed at:18/10/2024.

⁴ The Claroty Team, Healthcare Cybersecurity: Key Strategies for Safeguarding Your Environment, available at ; <https://shorturl.at/hYyMb> ,accessed at:17/10/2024.

⁵ Nate Lord, Healthcare Cybersecurity: Tips for Securing Private Health Data,available at : <https://shorturl.at/6eUCZ> ,accessed at:18/10/2024.

⁶ Peter Hall, Healthcare Cyber Security Challenges: Protecting Patient Data,available at : <https://shorturl.at/0adNo> ,accessed at:17/10/2024.

- نشر الوعي والتثقيف الصحي بدءاً من المريض مروراً بالعاملين في القطاع الصحي انتهاءً بوضعي الاستراتيجيات والخطط للأمن السيبراني للمؤسسات الصحية، مع ضرورة توظيف الأمن السيبراني في المناهج الدراسية والبرامج الوطنية فيما يتعلق بدور الرعاية الصحية¹
- تصميم إطار عالمي موحد للأمن السيبراني في القطاع الصحي يستوعب الدول ذات الدخل المرتفع والدول ذات الدخل المنخفض.
- توفير الموارد البشرية والمالية لتطوير القدرات الفنية لأن التهديدات السيبرانية في تطور مستمر وأصبحت أكثر تعقيداً خاصة بعد استخدام الذكاء الاصطناعي، ما يستوجب تأهيل اليد العاملة البشرية في المجال الصحي بالوعي الأمني الضروري وتعليمهم كيفية اكتشاف الأخطار السيبرانية وتفاديها.
- تنوع خوادم الكمبيوترات لتفادي التعطيل الكامل لأنه غالباً ما يتم ربط شبكات الكمبيوترات بخادم واحد في المستشفيات والعيادات، مع فرض المصادقة المتعددة للوصول إلى البيانات الصحية وذلك حفاظاً على السلامة الرقمية.²

خاتمة:

لقد ساهم التطور التكنولوجي بشكل كبير في إنقاذ الأرواح، نتيجة استخدام المعدات الطبية الذكية والمتطورة، وربط المنظومات الصحية بالتكنولوجيات الحديثة لتحسين جودة الخدمات الصحية، إلا أنه برزت تهديدات مرتبطة بالتكنولوجيا الصحية شكلت تهديداً للأمن الصحي، خاصة فيما يتعلق بحماية المعطيات البيانية للمرضى والأجهزة الطبية، حيث أضحت التكنولوجيا الطبية نتيجة لتزايد انتشارها عرضة للاختراقات والتلاعب والابتزاز من قبل القراصنة ومحتالي الإنترنت، ما تطلب تفعيل منظومة الأمن السيبراني للحفاظ وحماية أمن المعلومات والبيانات والمعدات أيضاً سواء وقت السلم أو الأزمات، وذلك وفق الإجراءات التالية:

- وضع اطر للاستجابة للحوادث السيبرانية والاختراقات في المجال الصحي من خلال التشفير عالي المستوى.
- حماية الأجهزة الطبية والمعلومات الصحية الرقمية المتصلة بالإنترنت لمنع القراصنة الوصول إليها والعبث بها وذلك بإنشاء وحدات أمنية سيبرانية تعنى بالأمن التكنولوجي في القطاع الصحي "الأمن الإلكتروني".
- التنسيق الدوري مع مختلف الجهات الفاعلة لحماية منظومة الصحي والاستعداد للعمليات الإستباقية.
- ضرورة الاستغلال الأمثل لكل الطاقات المادية والبشرية لتحقيق السيادة الصحية.
- وضع برامج تدريبية ووقائية للحد من القرصنة البيولوجية.

¹ نيكى اوبراين وآخرون، حماية نظم الرعاية الصحية "إطار عالمي للأمن السيبراني"، مؤسسة قطر، 2020، ص 08.

² Cybersecurity Challenges in Healthcare Industry, available at : <https://shorturl.at/wbNHP>, accessed at: 17/10/2024.

قائمة المصادر والمراجع:

الكتب

- 01- بونيفاس باسكال، الجيوبولتيك، مقارنة لفهم العالم، مقارنة لفهم العالم 48 مقالا، (تر: اياد عيسى)، دمشق، منشورات الهيئة العامة السورية للكتاب، وزارة الثقافة، 2020.

II . المقالات:

1. أبو سعود هاني مطر، ارتباطات الامن المعلوماتي بالأمن القومي، مجلة الدراسات الحقوقية، المجلد 07، العدد 02، جوان 2020.
2. بوقرص ساعد، الأمن السيبراني: مخاطر وتهديدات وتحديات ممارسات توصيات استراتيجيات خاصة، مجلة الأبحاث في الحماية الاجتماعية، المجلد 3 العدد 1، 2020.
3. جعفري عبد الله، التهديدات السيبرانية وتأثيرها على الامن القومي للجزائر، المجلة الأفريقية للدراسات القانونية والسياسية، المجلد 06، العدد 02، السنة 2022.
4. حارك فاتح، الدولة بين الهيمنة وتحقيق الأمن في الفضاء السيبراني، المجلة الجزائرية للأمن الإنساني، المجلد 7، العدد 01، 2022.
5. زوبر محمد خير، واقع الامن الصحي بالجزائر: دراسة تحليلية للمؤشرات الصحية لولاية عين الدفلى، مجلة نماء للاقتصاد والتجارة، المجلد 03، العدد 01، 2019.
6. الشمري مصطفى ابراهيم سلمان، الأمن السيبراني وأثره في الامن الوطني العراقي، مجلة العلوم القانونية والسياسية، المجلد 10، العدد الأول، 2021.
7. طالة لامية، الإرهاب السيبراني والامن القومي: قراءة في تحولات الاستراتيجية الدفاعية، حوليات جامعة الجزائر 01، المجلد 35، العدد 04.
8. طليب احمد، الامن الصحي في الظروف الاستثنائية بين تكريس الحق وصناعة الوعي، مجلة دفاتر البحوث العلمية، المجلد 08، العدد 02، 2020.
9. عوفي حبيب، الفضاء الرقمي تحدي أمني جديد استراتيجيات الدول في تحقيق الامن السيبراني العالمي، المجلة الجزائرية للعلوم الانسانية والاجتماعية، المجلد 06، العدد 01.
10. فرحات علاء الدين، الحرب السيبرانية ومستقبل الامن العالمي ، مجلة الناقد للدراسات السياسية ، المجلد 6 ، العدد 02، 2020.
11. لعبي ضحى كاظم السدخان، البعد الجيوسياسي للأمن السيبراني، مجلة العلوم الانسانية، المجلد 05، العدد 01، 2021.
12. مسيكة محمد، الفضاء السيبراني وتحديات الامن القومي للدول، مجلة العلوم القانونية والاجتماعية، المجلد 07 ، العدد 04، جوان 2022.
13. مطروح وفاء، تداعيات جائحة كوفيد 19 وتأثيره على تحقيق الامن السيبراني في الجزائر، المجلة الدولية للاتصال الاجتماعي، المجلد 02، العدد 09، 2022.

14. نواروسار، الصحة الرقمية في ظل جائحة كوفيد 19 الهواتف الذكية أنموذجا، مجلة الدولية للاتصال الاجتماعي، جامعة عبد الحميد بن باديس، مستغانم، مجلد09، العدد 01، 2022.
- 15- شحات مراد، جصاص لبنى، الأمن السيبراني للدول: بعد افتراضي لواقع مادي، مجلة الناقد للدراسات السياسية، المجلد 07، العدد02، السنة 2023.
- 16- كلاع شريفة، الأمن السيبراني وتحديات الجوسسة والاختراقات الالكترونية للدول عبر الفضاء السيبراني،، مجلة الحقوق والعلوم الإنسانية، المجلد 15، العدد 01، 2022.
- 17- خليفة إيهاب، تنامي التهديدات السيبرانية للمؤسسات العسكرية، مجلة اتجاهات الاحداث، العدد22د، 2017.

III التقارير:

- 01- اوبراين نيكي، جاي مارتن وآخرون، تقرير حول حماية نظم الرعاية الصحية، مؤتمر القمة العالمي الابتكار في الرعاية الصحية، 2020.
- 02- نيكي اوبراين وآخرون، حماية نظم الرعاية الصحية " اطار عالمي للأمن السيبراني"، مؤسسة قطر، 2020،

IV. المواقع الالكترونية:

01. أسماء قنديل، طرق حماية الأمن الرقمي ضد هجمات الهاكرز أثناء فترات الأوبئة والكوارث، متاح على الموقع: <https://rb.gy/ytr5ab>
- 02- السيد احمد داليا، لماذا تصاعد خطر الهجمات الالكترونية في خضم ازمة كورونا، متاح على الموقع : <https://shorturl.at/16Lap>
03. البيكاوي احمد، تهديدات الامن السيبراني وقطاع الرعاية الصحية في زمن الازمة، مجلة القبس، متاح على الموقع: <https://shorturl.at/xFIOP>
04. الراوي طه، كيف تعزز التكنولوجيا الرقابة الصحية ضد الامراض؟، متاح على الموقع: <https://www.noonpost.com/content/36540>
05. البهي رغد، الأمن السيبراني في 2020: بين الفرص والتحديات والحماية، متاح على الموقع: <https://shorturl.at/4BdYF>
06. بسمه فايد، حروب السيبرانية ... ترسانات رقمية وتهديدات دولية، متاح على الموقع: <https://rb.gy/yixw2v>
07. خليفة ايهاب، كيف توظف الصين التكنولوجيا لمكافحة الفيروس، مركز المستقبل للأبحاث والدراسات المتقدمة، تم التصفح يوم متاح على الموقع <https://shorturl.at/548Ms>
08. عزيز عبد الله جعفر، الأمن الإنساني في ظل فيروس كورونا، متاح على الموقع <https://feji.us/q1twra> :
09. محمود محمد حامد، الهجمات الالكترونية في عصر فيروس كورونا (Covid-19)، متاح على الموقع: <https://rb.gy/ujen14>
10. سني ذو الهدى، كورونا وانتشار الهجمات السيبرانية الارهابية، متاح على الموقع <https://shorturl.at/b6Dsh>
11. ملف امن سيبراني - مخاطر الهجمات السيبرانية، التظليل الاعلامي وانتهاك الخصوصية، المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات، متاح على الموقع: <https://shorturl.at/HdHrz> .
12. " هجوم خبيث" يستهدف المؤسسات العاملة في التصدي لكورونا، متاح على الموقع <https://rb.gy/qpp27q>

دور الأمن السيبراني في تعزيز الأمن الصحي للدول

- 13- محمد عبد الله الشيبة، الأمن السيبراني.. استراتيجيات التصدي والحماية، صحيفة الاتحاد، متاح على الموقع: <https://www.aletihad.ae>
- 14- بسمة فايد، حروب السيبرانية ... ترسانات رقمية وتهديدات دولية، متاح على الموقع: <https://rb.gy/yixw2v>.
- 15- الأمن السيبراني مفهومه وتاريخه، الجزيرة نت، متاح على الموقع: <https://shorturl.at/VlkY5>
- 16- فايز الشهري، شبكات التواصل وتأثيرها على العلاقات الدولية، العربية نت، متاح الموقع: <https://shorturl.at/mKvuf>.
- 17- وليد العويمر، آلاء كنعان جميل، الأمن الصحي وأثره على العلاقات الدولية، تريندز للبحوث والاستشارات، متاح على الموقع: <https://shorturl.at/X4fpQ>
- 18- ما هو دور التكنولوجيا في الرعاية الصحية؟ وكيف تلحق بركبها؟، ميسر للخدمات الطبية، متاح على الموقع: <https://shorturl.at/ioTPF>.
- 19- دستور منظمة الصحة العالمية، منظمة الصحة العالمية، متوفر على الرابط: <https://www.who.int/governance/eb/constitution/ar>

I. المراجع باللغة الأجنبية:

1. JEFFERSON, Catherine, LENTZOS, Filippa, et MARRIS, Claire. Synthetic Biology and Biosecurity: How scared should we be?. 2014.
2. JIN, Andrew et LINKOV, Igor. Synthetic Biology Brings New Challenges to Managing Biosecurity and Biosafety. Emerging Threats of Synthetic Biology and Biotechnology, 2021.
3. RAINA MACINTYRE, C., ENGELLS, Thomas Edward, SCOTCH, Matthew, et al. Converging and emerging threats to health security. Environment Systems and Decisions, vol. 38, no 2, 2018.
4. SMITH, Marcus et WALSH, Patrick. Improving health security and intelligence capabilities to mitigate biological threats. The International Journal of Intelligence, Security, and Public Affairs, vol. 23, no 2, 2021.
5. Owens, Brian. "How hospitals can protect themselves from cyber attack." (2020).

II. المواقع الالكترونية باللغة الأجنبية:

1. Gordon Corera, Coronavirus: How will it change national security and spying?, available at : <https://shorturl.at/y5mJh>
2. Stéphanie carvin, National Security and pandemics the limits of early warning, available at : <https://rb.gy/0xnum6>.
3. Elena Canorea, Protecting critical infrastructure from cyber-attacks, available at : <https://shorturl.at/QULoP>.
4. Recommendations to prevent a cyber attack in the health sector, available at : <https://shorturl.at/JgP1W>.
5. What is Healthcare Cybersecurity?, available at : <https://shorturl.at/3Jvyo>
6. Nate Lord, Healthcare Cybersecurity: Tips for Securing Private Health Data, available at : <https://shorturl.at/fHXuI>
7. Aline Liu, 6 steps to protect your healthcare data, available at <https://shorturl.at/Gau6P>
8. Healthcare data security: safeguarding patient information in the digital age, available at : <https://shorturl.at/eAFvO>.

9. How To Prevent Security Breaches In Healthcare,available at : <https://shorturl.at/rmRgr>
10. Cybersécurité dans le secteur de la santé : le scénario, les risques et les défis futurs, safecore,available at : <https://shorturl.at/hpHI3>
11. Cyber Security Challenes in the Healthcare Industry,available at : <https://shorturl.at/o5tV1>
12. Healthcare Cybersecurity,available at : <https://shorturl.at/mjIDV>
13. Altay Ataman, Cybersecurity in Healthcare: 7 Challenges & 10 Best Practices in '23,available at : <https://shorturl.at/jm1mW>
14. The Claroty Team, Healthcare Cybersecurity: Key Strategies for Safeguarding Your Environment,available at ; <https://shorturl.at/hYyMb>
15. Nate Lord, Healthcare Cybersecurity: Tips for Securing Private Health Data,available at : <https://shorturl.at/6eUCZ>.
16. Peter Hall, Healthcare Cyber Security Challenges: Protecting Patient Data,available at : <https://shorturl.at/0adNo>
17. Cybersecurity Challenges in Healthcare Industry,available at : <https://shorturl.at/wbNHP>