المجلة العراقية للبحوث الإنسانية والإجتماعية والعلمية
Iraqi Journal of Humanitarian, Social and Scientific Research
Print ISSN 2710-0952 Electronic ISSN 2790-1254
العـــــدد 17S حزيران 2025
No.17S JUNE 2025

التهديدات السيبرانية على الهواتف النقالة وسياسة الحكومة العراقية لمواجهتها

م.م انوار جواد داخل
جامعة الكوفة/كلية الاثار
anwarj.alhafadhi@uokufa.edu.iq

الملخص: ان تهديدات الأمن السيبراني على الهواتف النقالة تشكل تحديات متزايدة تستدعي استراتيجيات وأدوات فعالة للتصدي لها،وبهذا يعتبر الهاتف النقال اليوم جزءًا حيويًا من حياة الأفراد والشركات، مما يجعله هدفًا مغريًا للهجمات السيبرانية التي تستهدف البيانات الحساسة والمعلومات الشخصية. وتعد أحد التهديدات الرئيسة هو البرمجيات الخبيثة التي يمكن أن تُثبت على الهواتف دون علم المستخدم وتقوم بسرقة البيانات أو تعطيل الجهاز ، وتطوير استراتيجيات فعالة يشمل التركيز على التحكم في الوصول إلى التطبيقات والبيانات، وتعزيز الوعي الأمني للمستخدمين لتجنب تنزيل البرامج الضارة. بالإضافة إلى ذلك، يجب استخدام أدوات فعالة لحماية الهواتف مثل برامج مكافحة الفيروسات وجدران الحماية وتحديث الأنظمة بانتظام، كما ينبغي تنفيذ إجراءات النسخ الاحتياطي للبيانات واستخدام التشفير لحماية المعلومات الحساسة. وبهذا فيتطلب التصدي للتهديدات السيبرانية المتزايدة على الهواتف المحمولة جهودًا متعددة الأوجه تشمل التحسين المستمر للأمان التقني وتعزيز الوعي الأمني واعتماد إجراءات وأدوات فعالة لحماية الأجهزة والبيانات.

الكلمات المفتاحية: الهاتف،التهديدات السيبرانية، الامن السيبراني ،الفضاء السيبراني ، الاستراتيجية

Cyber threats to mobile phones and the Iraqi government's policy to confront them

Anwar Jawad Dakhil

Abstract: Cybersecurity threats to mobile phones pose increasing challenges that require effective strategies and tools to address them. Today, the mobile phone is considered a vital part of the lives of individuals and companies, making it a tempting target for cyber attacks targeting sensitive data and personal information. One of the main threats is malware that can be installed on phones without the user's knowledge and steal data or disable the device. Developing effective strategies includes focusing on controlling access to applications and data, and enhancing the security awareness of users to avoid downloading malware.In addition, you should use effective tools to protect phones such as antivirus software and firewalls and update systems regularly. Data backup procedures should also be implemented and encryption used to protect sensitive information.Thus, addressing the increasing cyber threats to mobile phones requires multifaceted efforts that include continuous improvement of technical security, enhancing security awareness, and adopting effective procedures and tools to protect devices and data.

Keywords: (Phone, Cyber Threats, Cyber Security, Cyberspace, Strategy).

المقدمة

في عصرنا الحديث المعتمد على التكنولوجيا أصبحت الهواتف النقالة ليست مجرد أداة اتصال، بل أصبحت شريكًا حيويًا في حياة الأفراد، والمؤسسات على حد سواء، ومع تزايد انتشار استخدام الهواتف النقالة، تزايدت أيضًا التهديدات السيبرانية التي تستهدفها، مما يتطلب التفكير بجدية في تبني استراتيجيات واعية واستخدام أدوات فعالة لمواجهة هذه التحديات. تعد التهديدات السيبرانية الموجهة نحو الهواتف النقالة من بين أكثر التحديات التي تواجه المستخدمين والمؤسسات في العصر الرقمي الحالي، فمن خلال

استغلال الثغرات في أنظمة التشغيل والتطبيقات، يمكن للمهاجمين الوصول إلى معلومات حساسة مثل البيانات الشخصية والمالية وحتى التحكم في الجهاز بشكل غير مصرح به،لمواجهة هذه التهديدات بفعالية، يجب أن تكون الاستراتيجيات المتبعة شاملة ومتعددة الأوجه، فضلاً عن ذلك، يتطلب الأمر أدوات فعالة ومتطورة لتحديد ومكافحة التهديدات بشكل فعال.

هدف البحث:. ان هدف البحث يكمن في دراسة وتحليل التهديدات الأمنية التي تواجه الهواتف النقالة في الوقت الحالي، وتقديم استراتيجيات وأدوات فعالة لمكافحة هذه التهديدات وحماية الأجهزة والبيانات الحساسة المخزنة عليها.

أشكالية البحث:. الإشكالية التي تثار في هذا البحث هي كيفية التعامل مع التهديدات السيبرانية المتزايدة التي تستهدف الهواتف النقالة ؟

وينبثق من هذا السؤال اسئلة فرعية منها :

١_ ماهي التهديدات السيبرانية التي تستهدف الهواتف النقالة في الوقت الحالي؟ وكيف يمكن للمستخدمين حماية أنفسهم من هذه التهديدات؟

٢_ ما هي الاستراتيجيات الفعّالة التي يمكن اتباعها للتصدي للتهديدات السيبرانية على الهواتف النقالة؟ هل هناك أساليب محددة أو تقنيات مبتكرة يمكن استخدامها للحماية؟

٣_كيف يمكن للشركات المصنعة للهواتف النقالة تطوير منتجات أكثر أمانًا لمواجهة التهديدات السيبرانية؟ وما هي الخطوات التي يمكنها المستهلكون اتخاذها لتحسين أمان هواتفهم النقالة؟

الفرضية :.تفترض الدراسة أن زيادة الاعتماد على الهواتف النقالة في حياة الأفراد والشركات يجعلها عرضة لتهديدات سيبرانية متزايدة، وبالتالي فإن وضع استراتيجيات فعّالة واستخدام أدوات تقنية مبتكرة يمكن أن يلعب دورًا حاسمًا في حماية الأجهزة والبيانات الحساسة المخزنة عليها.

هيكلية البحث:.يتكون البحث الموسوم (التهديدات السيبرانية على الهواتف النقالة وسياسة الحكومة العراقية لمواجهتها) : من مقدمة ومبحثين رئيسين : الاول: حمل عنوان الاطار المفاهيمي للتهديدات السيبرانية ، وبدوره أنقسم إلى ثلاث مطالب : الاول : أختص في مفهوم التهديدات السيبرانية والمفاهيم المقاربة ، أما الثاني فكان نطاقات التهديدات السيبرانية، والثالث أختص بعنوان مصادر التهديدات السيبرانية . وتناغما مع مامضى جاء عنوان المبحث الثاني : تحليل التهديدات السيبرانية للهواتف النقالة وسبل مواجهتها ، لينشطر إلى انواع التهديدات السيبرانية التي تستهدف الهواتف النقالة ، والثاني ركز على استعراض سبل مواجهة التهديدات السيبرانية على الهواتف النقالة ، والثالث على سياسة الحكومة العراقية في مواجهة التهديدات السيبرانية، لنختم البحث بعد ذلك بجملة من النتائج والتوصيات.

المبحث الاول/ الاطار المفاهيمي للتهديدات السيبرانية

تعد التهديدات السيبرانية من المواضيع الحيوية في عصرنا الحالي حيث باتت تشغل اهتمامات الباحثين في هذا الشأن الى حد كبيراذ تشهد تكنولوجيا المعلومات والاتصالات تطورًا مستمرًا ينعكس على واقع الامن القومي للدول في ظل تنامي اخطار تلك التهديدات وتزايد اعتماد الدول على تطوير بنيتها التكنولجية التي تعكس مدى قوتها ومسايرتها للحداثوية ، لذا تناولنا في هذا السياق مفهوم التهديدات السيبرانية والمفاهيم المقاربة لها بالاضافة الى فهم النطاقات المختلفة التي تشملها ومصادر هذه التهديدات المتنوعة.

المطلب الاول : في مفهوم التهديدات السيبرانية والمفاهيم المقاربة

ان الوقوف على المفهوم العام للتهديدات السيبرانية والبحث في المفاهيم المقاربة لهذا المفهوم فضلا عن تناول نطاقات تلك التهديدات ومصادرها يعد مدخل منطقي لفهم ابعاد هذا المفهوم ولهذا نتناول كل ذالك في سياق اطار مفاهيمي باديء ذي بدء.

اولا - مفهوم التهديدات السيبرانية : قامت الدول بتطوير إمكانياتها على كل الأصعدة السياسية والاقتصادية والاجتماعية والعسكرية لتواكب التحديات التي تفرضها البيئة الدولية، وبهذا فأن القوة السيبرانية لم تقتصر على الدولة الاقوى في البيئة الدولية وأنما أصبحت الدولة الضعيفة تمتلك هذه القوة السيبرانية ايضا ، وبهذا يلاحظ أن أي فاعل في البيئة الدولية مهما كانت قوته ومهما كانت الصفة القانونية التي يحملها سواء أكان رسميا أو غير رسمي أصبح يمتلك القدرة على استخدام القوة السيبرانية لتحقيق المصالح او تهديد الخصوم وهو مايفسر سعي الدول الدائم لأمتلاك تلك القدرات التي باتت في مقدمة المقاييس التي يمكن النظر اليها لقياس مدى قوة الدولة وفاعليتها على مختلف الصعد ([1]).

ان التهديدات السيبرانية في الواقع تشير إلى أي خطر أو هجوم الكتروني قد يهدد امن المجتمع وامن الاقتصاد والجانب الامني والعسكري للدول ، وعليه يجب على الدول المعرضة للتهديد وضع خطط استراتيجية من اجل مكافحتها والتخلص منها ([2]).

كما يشير المفهوم العام للتهديد السيبراني الى أي محاولة غير مصرح بها للأستفادة من ضعف أمان في نظام معلوماتي لتكون هناك نتائج ضارة ، يمكن أن يشمل ذلك الهجمات على الأنظمة الحاسوبية وشبكات الاتصالات والبرمجيات بهدف الوصول غير المصرح به أو التلاعب بالبيانات أو التسبب في توقف الخدمات ، وأبرز أنواع الأسلحة السيبرانية على البيئة الدولية هو سلاح الحرمان من الخدمة القادرة على شل حركة الأنظمة الإلكترونية وتعطيل مصالح الدول والافراد والجماعات والشركات ([3]).

لقد أصبح أي تهديد أو هجوم سيبراني على مستوى واسع ضد مصالح الدول الاستراتيجية يؤدي بشكل او بأخر إلى حدوث عدم توازن استراتيجي او الاخلال في توازنات القوى الدولية القائمة ، وهذا أسلوب جديد من التهديد للأمن القومي العالمي خاصة وان الحروب سيبرانية تكون أقل كلفة من الحروب التقليدية ([4]).

وعليه فأن العالم اليوم يواجه ثورة جديدة في التكنولوجيا العسكرية تجعل الحروب اسهل لان القادة يستطيعون الاشراف والتدخل بالعمليات العسكرية الميدانية من مسافات بعيدة وبدقة غير متناهية لم تكن ممكنة من ذي قبل ([5]).

ثانيا : المفاهيم المقاربة:

([1])عبد الغاني شرقي ،التهديدات السيبرانية واشكالية السيادة :اعادة قراءة لسيادة واستفاليا ،جامعة امحمد بوقرة بومرداس ،الجزائر، مجلة السياسة العالمية،المجلد7،العدد2 ، 2023 ، ص272-273

([2])د.فرح يحيى زعاترة، التهديدات السيبرانية على الامن القومي الامريكي ، العربي للنشر والتوزيع ، القاهرة ،2023،ص35

([3]) نوران شفيق،اشكال التهديدات الالكترونية ومصادرها،المركزالاوربي لدراسات مكافحة الارهاب ،متاح على هذا الرابط:https://www.europarabct.com/?=34807،تاريخ الدخول2024/1/17

([4]) جاسم محمد طه، التهديدات السيبرانية وانعكاساتها على الامن الوطني الامريكي ، المجلات الاكاديمية العلمية العراقية ، جامعة الموصل ، كلية العلوم السياسية ،2024/6/30 ، ص184

([5])احمد عبيس الفتلاوي ،الهجمات السيبرانية مفهومها والمسؤولية الدولية الناتجة عنها في ضوء التنظيم الدولي المعاصر ، مجلة المحقق الحلي للعلوم القانونية والسياسية ، مجلد 8، العدد 4، جامعة بابل ،2016، ،ص615

١_ **الفضاء السيبراني cyber space** : هو مصطلح يعبر عن البيئة الرقمية التي تتكون من أنظمة الحاسوب وشبكات الاتصالات والبرمجيات ، حيث يتفاعل فيها الأفراد والمؤسسات ، ويشتمل هذا الفضاء السيبراني على جوانب متعددة من التكنولوجيا والأمان ، حيث يتم تبادل المعلومات والبيانات بشكل رقمي ، ويهدف فهم الفضاء السيبراني إلى حماية الأنظمة والمعلومات من التهديدات السيبرانية ([1]).

٢_ **الأمن السيبراني cyber secuity:** هو ظاهرة عالمية وتحدي اجتماعي تقني معقد للحكومات وايضا يتطلب مشاركة الأفراد ، حيث يعتبر اليوم أهم التحديات التي تواجه الحكومات لان الرؤية والوعي العام لازالو محددين بأزاء تلك التهديدات التي تشكل خطر داهم لمصالح الدول والشعوب على حد سواء([2]).

وبهذا فإن الأمن السيبراني هو مجال يركز على حماية الأنظمة الرقمية والبيانات من التهديدات السيبرانية، مما يشمل الهجمات الإلكترونية وسرقة البيانات ، ويتضمن هذا المفهوم تنفيذ استراتيجيات وسياسات للكشف عن الهجمات المحتملة وتقويضها واستعادة النظم بعد وقوعها ، ويهدف الامان السيبراني إلى تعزيز الثقة في استخدام التكنولوجيا الرقمية([3]).

٣_ **الهجمات السيبرانية cyber attacks :** هي تلك الجهود الألكترونية الضارة التي تستهدف استغلال ثغرات في الأمان الرقمي لأنظمة الحاسوب والشبكات أو التطبيقات بهدف الوصول غير المصرح به أو التسبب في أضرار ، وتتضمن هذه الهجمات عدة أشكال مثل البرمجيات والتسلل(phishing) الخبيثة وهجمات التصيد (unauthorized Access) غير المصرح به والهجمات الضارة spoofing والحجب حيث يسعى محترفي الامان السيبراني بشكل مستمر الى أتخاذ تدابير لتحسين الأمان والحماية ضد هذه التهديدات المحتملة ([4]).

المطلب الثاني : نطاقات التهديدات السيبرانية

ان نطاقات التهديدات السيبرانية تمثل مجموعة واسعة من الأخطار والتحديات التي تواجه الأنظمة الإلكترونية والشبكات والبيانات في الفضاء السيبراني،وتتنوع هذه التهديدات في مصادرها وأشكالها وأهدافها، ويمكن تصنيفها إلى عدة نطاقات رئيسة يتعلق كل منها بجانب معين من الأمن السيبراني.

أولا/ الدول : تشير التهديدات السيبرانية التي تستهدف الدول إلى الهجمات الإلكترونية التي تستهدف البنية التحتية الحيوية والحساسة للدول مثل الشبكات الحكومية والمؤسسات والقطاعات الحيوية مثل قطاعات الطاقة والمياه، والقطاعات العسكرية بهدف التجسس أو التخريب أو الاستيلاء على المعلومات الحساسة، ولعل ابرز مضامين تلك التهديدات السيبرانية للدول تتلخص فيما يأتي ([5]):

1_ **الهجمات على البنية التحتية الحيوية :** اي الهجمات التي تستهدف قطاعات مهمة في الدولة مثل الطاقة والمياه والنقل بهدف تعطيل الخدمات فيها أو لغرض التجسس على البيانات الحساسة أو التخريب ،

([1]) cybersecurity:manaying systems,conducting managing systems, conducting Testing,and lnvestigating lntrusions . jones&Bartlett learning.

*اذ يختلف الفضاء الخارجي عن الفضاء السيبراني كون الاول هو الفراغ الموجود بين الاجرام السماوية بما في ذلك الارض.

([2]) مصطفى ابراهيم سلمان الشمري ، الامن السيبراني واثره في الامن الوطني العراقي ،مجلة العلوم القانونية والسياسية ،مجلد 10،العدد الاول، جامعة ديالى ،2021،ص153

([3])ايهاب خليفة ، الحرب السيبرانية الاستعداد لقيادة المعارك العسكرية في الميدان الخامس ، العربي للنشر ، القاهرة ، 2021، ص35

([4]) Vacca ,computer and lnformation security Hand book, Morgan kaufmann,2014

([5]) نورة شلوش ،القرصنة الالكترونية في الفضاء السيبراني التهديد المتصاعد من الدول ، مجلة مركز بابل للدراسات الانسانية ، مجلد 8، العدد 2 ، 2018، ص200

مثل الهجوم السيبراني على شركة ارامكو السعودية في عام 2012والذي استهدف اكبر شركة لأنتاج النفط في العالم بهدف ايقاف تصدير النفط حيث ادى هذا الهجوم الى تعطيل 35000 جهاز كمبيوتر تابع للشركة وتم استبدالها فورا ([1]).

٢- **التجسس السيبراني :** حيث ان هذا الشكل من التهديد يستهدف جمع معلومات سرية وحساسة عن الدول ومؤسساتها الحكومية والعسكرية والاقتصادية بهدف الاستفادة من هذه المعلومات للمكاسب الجيوسياسية أو الاقتصادية والعسكرية،وهناك أمثلة على التجسس السيبراني للدول منها التسلل إلى شبكات الحكومة والمؤسسات الحيوية وسرقة المعلومات السرية والتلاعب بالأنظمة الحكومية والانتخابية ([2]).

٣- **الاختراقات العسكرية:** تستهدف البنية العسكرية والأنظمة العسكرية للدول سواء كانت ذات طابع دفاعي أو هجومي، هدفه التجسس على القدرات العسكرية والاستخباراتية، وإعاقة العمليات، وتعطيل النظم العسكرية، وتأثير على القرارات الاستراتيجية للدول،وهناك أمثلة على الاختراقات العسكرية للدول منها تعطيل الأنظمة العسكرية وتسريب المعلومات السرية وتعطيل البنية التحتية الحيوية([3]).

ثانيا/ الأفراد : تعتبر الهجمات السيبرانية التي تستهدف الأفراد واحدة من أكثر أنواع الهجمات شيوعًا في الوقت الحاضر ، ويمكن أن تتضمن تهديدات تنطوي على مايأتي: ([4]).

1-**الاحتيال الإلكتروني للافراد:**تستخدم ادوات الكترونية مختلفة للتلاعب والخداع وللاستيلاء على معلومات شخصية أو مالية من الأفراد عبر الإنترنت، ويتم ذلك غالبًا عبر استخدام البريد الإلكتروني المزور، الرسائل النصية، مواقع الويب المزيفة كأدوات لتنفيذ هذا النوع من الهجمات ([5]).

2-التطفل على خصوصية الافراد :يستهدف جمع معلومات شخصية عن الأفراد دون موافقتهم ودون علمهم ، حيث يؤدي ذلك الى انتهاك خصوصيتهم، من خلال اختراق الهواتف الذكية والأجهزة المحمولة والتجسس عبر الكاميرات الرقمية وأجهزة الويب وتتبع النشاط عبر الإنترنت ([6]).

([1]) The National Strategy for Critical Infrastructure Security and Resilience" , The White House,oct 31/2023 ،متاح على هذا الرابط:
https://www.google.com/search?q=The+National+Strategy+for+Critical+Infrastructure+Security+and+Resilience%22+%2C+The+White+House%2Coct+31%2F2023&rlz=1C1YTUH_arIQ1080IQ1082&oq=The+National+Strat

([2]) Mason Rice, Sujeet Shenoi, Critical Infrastructure Protection X: 10th IFIP WG 11.10 International Conference, ICCIP 2016, Arlington, VA, USA, March 14-16, 2016, Revised Selected Papers. AICT-485, 2016, IFIP Advances in Information and Communication ، متاح على هذا الرابط: https://dl.ifip.org/IFIP-TC11/hal-01614866v1

([3]) Marco Roscini, Cyber Operations and the Use of Force in International Law, OXFORD UNIVERSITY PRESS,2014,P87

([4]) TZIPORA HALEVI,NASIR D.MEMON,ODED NOV,SPEAR-PHISHING IN THE WILD :Areal-world Study Of Personality, Phishing self –Efficacy and Vuluerability to spear-Phishing Attacks, SSRN Electronic journal ,NEWYOURK,128, January 2015

([5]) Yifei Wang,Asurvey of phishing detection:from an intelligent countermeasures View,IEEE XPlore,11 DEC 2022, متاح على هذا الرابط:
https://ieeexplore.ieee.org/document/10016193/authors#authors

([6]) المصدر نفسه

3-**التصيد الاحتيالي(الفيشنج):**يستهدف الأفراد عبر إرسال رسائل بريد إلكتروني أو رسائل نصية مزيفة تدعي أنها من مؤسسات موثوق بها مثل البنوك أو الشركات أو الحكومة بهدف استخراج معلومات حساسة وتهديد الافراد بها من اجل الحصول على مقابل مالي ([1]).

المطلب الثالث: مصادر التهديدات السيبرانية

تنطوي مصادر التهديدات السيبرانية على انماط مختلفة تنطلق منها تلك التهديدات السيبرانية بدوافع مختلفة حيث تصنف هذه المصادر الى فئات رئيسة وعلى النحو الآتي ([2]):

١_ **المهاجمون الفرديون والمجموعات القرصانية**:هم أفراد أو قل مجموعات من الأشخاص منضمين او غير منضمين احياناً يقومون بهجمات سيبرانية على أنظمة المعلومات والشبكات بغرض تحقيق أهداف معينة مسبقا وتشتمل تلك الهجمات على اختراق الخصوصية لأغراض الابتزاز والتخريب أو التجسس ، وتشكل هذه المجموعات تحديات كبيرة لأمان المعلومات والأنظمة الالكترونية وابرز مصادر التهديدات السيبرانية ، وتتطلب جهود مستمرة لتعزيز الأمان والوقاية ([3]).

2_ **الحكومات والمؤسسات الاستخباراتية**:هي الجهات التي تعمل في مجال جمع المعلومات الاستخباراتية وتحليلها لصالح الدولة، تتضمن هذه الجهات وكالات الاستخبارات الوطنية واجهزة المخابرات والأجهزة الأمنية المتخصصة في جميع أنحاء العالم، اما اهداف هذه الاطراف تكمن في تحقيق مستوى عال من الامن القومي والاستقرار السياسي ومكافحة الارهاب وحماية المقدرات الاقتصادية ([4]).

3-**الموظفون السابقون أو الحاليون** : يعتبرون واحدة من المصادر المحتملة للتهديدات السيبرانية نظراً للوصول الذي يمكن أن يكون لديهم أنظمة وبيانات المؤسسة حيث يمكن لهؤلاء الموظفين الاستفادة من معرفتهم وصلاحياتهم الداخلية لتنفيذ هجمات أو تسريب المعلومات أو التسبب في تعطيل الخدمات، ومن أجل التصدي للتهديدات السيبرانية الناجمة عن الموظفين السابقين أو الحاليين، يجب على المؤسسات تبني إجراءات أمنية داخلية صارمة مثل تقييد الوصول والمراقبة الداخلية وتعزيز التدريب على الوعي الأمني للموظفين ([5]).

٤_ **الهجمات الحكومية والعسكرية :** تعد أحد أهم مصادر التهديدات السيبرانية نظرًا للقدرات والموارد الهائلة التي تتمتع بها الحكومات والقوات العسكرية، وتتمثل الهجمات الحكومية والعسكرية في الجهود التي تبذلها الدول والجيوش للقيام بأنشطة سيبرانية تستهدف الأنظمة الحيوية والبنية التحتية للدول الأخرى، ويتطلب التعامل مع الهجمات الحكومية والعسكرية

([1]) Gargi Sakar and Sandeep K.Shukla,Behaviorsal anaglysis of Cybercrime:paving the way for effective policing strategies ,Journal of Economic criminology,December2023, متاح على هذا الرابط:https://www.sciencedirect.com/science/article/pii/S2949791423000349

([2])فاطمة الزهراء بو شملة ،التهديدات السيبرانية واثرها على الامن القومي في ظل التحول الرقمي ،مجلة العلوم القانونية والسياسية ،جامعة محمد خيضر، بسكرة، العدد20، 2019

([3]) نورة شلوش ، القرصنة الالكترونية في الفضاء السيبراني التهديد المتصاعد من الدول ، مصدر سابق،ص200

([4]) بلعسل بنت بني ياسمين و عمروش الحسين ،التهديدات الالكترونية والامن السيبراني في الوطن العربي ،مجلة نوميروس الاكاديمية ، المجلد الثاني ،جامعة الدكتور يحيى فارس المدية ، الجزائر ،2021،ص167

([5]) حسن بن احمد الشهري ، الانظمة الالكترونية الرقمية المطورة لحفظ وحماية سرية المعلومات من التجسس ،المجلة العربية للدراسات الامنية والتدريب، المجلد(28)، العدد(56)،الرياض،2012،ص11

استراتيجيات دفاعية واحترافية قائمة على تحليل الأمان وتعزيز البنية التحتية السيبرانية وتعزيز التعاون الدولي في مجال أمن المعلومات والسيبرانية ([1]).

٥_ **الهجمات الإرهابية**: قد تشمل أي نوع من الهجمات التي تستهدف الحياة البشرية أو الممتلكات باستخدام العنف أو التهديد بالعنف، ويمكن أن تكون هذه الهجمات مصدراً للتهديدات السيبرانية عبر استخدام التكنولوجيا والإنترنت في تنفيذها أو تعزيزها ([2]).

٦_ **التهديدات الناشئة والتقنيات الجديدة**: تشكل مصدرًا مهمًا للتهديدات السيبرانية بسبب تطورها المستمر وتأثيرها المحتمل على الأنظمة والبنى التحتية الرقمية ومن بين هذه التهديدات والتقنيات هي الذكاء الاصطناعي والتعلم الآلي وإنترنت الأشياء (IoT) وتقنيات التشفير والحوسبة الكمية وهجمات الفدية (Ransomware) والهجمات الموجهة (Targeted Attacks) ،وتفهم هذه التهديدات والتقنيات الجديدة يساعد في تطوير استراتيجيات الدفاع السيبراني وتعزيز الوعي حول أهمية حماية البنى التحتية الرقمية والبيانات من الهجمات السيبرانية المستقبلية ([3]).

وعلى هذا فأن التهديدات السيبرانية بدآ بجذورها المفاهيمية مرورًا بنطاقاتها، وانتهاءً بمصادرها المتعددة، تبيّن أن التهديدات السيبرانية تمثل ظاهرة معقدة ومتطورة تتقاطع مع مفاهيم أمنية ومعلوماتية متعددة وتتسع لتشمل أفرادًا ومؤسسات وبنى تحتية حيوية، كما أظهرت الدراسة تنوع مصادر هذه التهديدات بين جهات فاعلة منظمة ومهاجمين مستقلين وأخطاء بشرية وتقنية ، وتؤكد هذه الرحلة التحليلية على ضرورة الإحاطة الشاملة بطبيعة التهديدات ونطاقاتها ومصادرها كمدخل أساسي لبناء استراتيجيات فعالة للوقاية والاستجابة.

المبحث الثاني: تحليل التهديدات السيبرانية للهواتف النقالة وسبل مواجهتها

ان تحليل التهديدات السيبرانية التي تواجه الهواتف النقالة لايقتصر على دراسة اساليب الهجوم فقط وانما يتطلب فهماً معمقاً للبنية التقنية لهذه الاجهزة والانماط السلوكية للمستخدمين والممارسات الامنية المتبعة ، وفي هذا المبحث سيتم تسليط الضوء على انواع التهديدات السيبرانية للهواتف النقالة بالاضافة الى سبل مواجهة التهديدات السيبرانية على الهواتف النقالة مع الاخذ بعين الاعتبار سياسة الحكومة العراقية في مواجهة تلك التهديدات .

المطلب الأول : أنواع التهديدات السيبرانية التي تستهدف الهواتف النقالة

بشكل عام تشير التهديدات السيبرانية إلى أي خطأ ينشأ عن استخدام التكنولوجيا لا سيما في مجال الإنترنت وشبكات الكمبيوتر، ويمكن أن تشمل هذه التهديدات العديد من الأنشطة الضارة مثل القرصنة والتصيد الاحتيالي اوهجمات البرامج الضارة وبرامج الفدية وغيرها، يمكن أن تستهدف التهديدات السيبرانية افراداً أو منظمات أو حتى الحكومات، وغالبا ما تؤدي إلى خسائر مالية وسرقة البيانات او انتهاكات للخصوصية او تعطيل الخدمات الحيوية، وقبل ان نتعرف على أنواع التهديدات التي تواجه هواتفنا الذكية يجب ان نعرف ماذا يريد المهاجم الحصول عليه من خلال هذه الهجمات، يمكن ان يحاول الحصول على الصور والفيديوهات الشخصية وذلك لابتزاز الضحية مقابل الحصول على مبالغ مالية او لأغراض اخرى، او سرقة بيانات البطاقات المالية، او محاولة الحصول على كلمات المرور للحسابات

([1]) محمد عبد القادر الداغستاني، النظرية العسكرية والمذهب العسكري والعقيدة العسكرية : دراسة تحليلية بضمنها تطور النظريات العسكرية عبر تاريخ فن الحرب ، الاكاديميون للنشر والتوزيع ،الاردن ،2019،ص108

([2])امير فرج يوسف، مكافحة الارهاب الالكتروني :الارهاب الرقمي في ظل الاتفاقية دول مجلس التعاون الخليجي ،دار الكتب والدراسات العربية ،2016،مصر ، ص253

([3]) عادل جارش، مقاربة معرفية حول التهديدات الامنية الجديدة ، مجلة العلوم السياسية والقانون ،العدد(1)، المركز الديمقراطي العربي للبحوث والدراسات الاستراتيجية، برلين 2017، ص259

الشخصية في مواقع التواصل الاجتماعي فيس بوك انستكرام واتساب وتليكرام وغيرها، او الحصول على اي معلومات شخصية تمكنه من انتحال شخصية الضحية لاستخدامها لأغراض تهديد او غيرها([1]).

ان هناك أنواع من التهديدات السيبرانية التي يمكن أن تستهدف الهواتف النقالة وهي ([2]) :

1. **هجمات التصيد الاحتيالي phishing:** وهو من اكثر الطرق استخداما وتتضمن هجمات التصيد الاحتيالي خداع الضحية لتقديم معلومات حساسة مثل كلمات المرور الخاصة أو تفاصيل بطاقة الائتمان وذلك من خلال التظاهر بأنهم كيان رسمي، ويمكن أن يحدث التصيد الاحتيالي من خلال الرسائل النصية الاحتيالية أو رسائل البريد الإلكتروني أو روابط مواقع ويب مزيفة مصممة لتبدو وكأنها مصادر موثوقة([3]).

2. **البرمجيات الخبيثة malwar:** تعتبر من اخطر التهديدات التي تواجه الهواتف النقالة، وتشمل هذه البرمجيات الفيروسات ، الديدان، والتي يمكن ان تتسبب في سرقة البيانات او تعطيل الهاتف، ويمكن ان تنتقل هذه البرمجيات الخبيثة من خلال التطبيقات الضارة وهذه *التطبيقات* برامج تجسسية تم تصميمها لتسبب ضررًا للأجهزة الإلكترونية مثل الهواتف النقالة، تهدف هذه البرامج إلى سرقة المعلومات الشخصية أو المالية، ويمكن أن تنتقل إلى الهواتف النقالة عن طريق تحميل تطبيقات غير موثوقة أو فتح رسائل غير معروفة أو زيارة مواقع ويب مشبوهةومن الممكن تقسيم هذه البرامج الضارة بالشكل الاتي([4]) :

أ- برامج الهجمات الضارة Malicious Attacks: وهي تطبيقات تستخدم لتنفيذ هجمات سيبرانية على الأجهزة الأخرى أو شبكات الاتصال، مثل هجمات الاختراق والتصيد الاحتيالي.

ب - برامج التجسس Spyware : وهي تطبيقات تستخدم للتجسس على المستخدمين وسرقة معلوماتهم الشخصية مثل الرسائل والصور وكلمات المرور.

ج - برامج الاحتيال Malware : وهي تطبيقات تستخدم أساليب احتيالية لخداع المستخدمين وسرقة معلوماتهم المالية أو الشخصية، مثل التطبيقات المزيفة للبنوك أو الشركات التجارية.

3. **استغلال ثغرات النظام والتطبيقات :** يكون هذا الاستغلال في نظام التشغيل مثل Androidاو ios، استغلال صلاحيات rootاو jailbreak للوصول الى ملفات النظام ، وهجمات Zero_day التي تنفذ عبر نقاط ضعف غير معروفة سابقا .

4. **هجمات الشبكة :** تكون من خلال هجمات الوسيط باستخدام شبكات الواي فاي عامة ، وانتحال الشبكات يتم من خلال انشاء نقطة اتصال مزيفة لخداع الضحية ، وتتبع الموقع الجغرافي عبر الشبكة .

5. **سرقة الهوية والبيانات :** حيث يتم فيها سرقة جهات الاتصال والصور والرسائل واستخراج بيانات الاعتماد المصرفي والدخول الى الحسابات الاجتماعية او المهنية المرتبطة بالجهاز.

6. **التهديدات عبر البلوتوث و NFC:** هذه التهديدات تتم من خلال نقل البرمجيات الخبيثة او روابط خبيثة عند فتح الاتصال وتنفيذ اوامر عن بعد على الجهاز اذا كان غير محمي .

7. **التهديدات الناتجة عن اهمال المستخدم :** وذلك يكون بتنزيل تطبيقات من مصادر غير موثوقة ، واستخدام كلمات مرور ضعيفة ، وعدم تفعيل التحديثات الامنية ([5]).

([1])حسين باسم عبد الامير ،تحديات الامن السيبراني ، مركز الدراسات الاستراتيجية ، جامعة كربلاء ، ايار 2018، متاح على هذا الرابط : https://kerbalacss.uokerbala.edu.iq/wp/blog/category/politic/husain-basim/?utm_source=chatgpt.com

([2]) سفيان العامري ، الامن السيبراني والهواتف الذكية : التهديدات واساليب الحماية ، مجلة دراسات امنية ، المجلد 8، العدد2، 2022، ص112_135

([3]) Markus Jakobsson and Steven Myers, Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft,New Jersey, Wiley-Interscience, 2006).

([4])حسين باسم عبد الامير ، مصدر سابق

([5])Cisco Networking Academy, Introduction to Cybersecurity, accessed June 5, 2025, https://prelogin-authoring.netacad.com/ar/courses/cybersecurity/introduction-cybersecurity.

أضافة الى ماتقدم فأن الهواتف الذكية أصبحت هدفًا رئيسيًا للهجمات السيبرانية وذلك لاحتوائها على كم هائل من المعلومات الحساسة لذا يتطلب تأمينها فهمًا دقيقًا لأنواع التهديدات وآليات الحماية الخاصة بها، سواء على مستوى المستخدم أو المؤسسة.

المطلب الثاني : سبل مواجهة التهديدات السيبرانية على الهواتف النقالة

إن الهواتف النقالة تمتاز بمميزات تجعلها أكثر عرضة للهجمات السيبرانية مقارنة بالأجهزة التقليدية الاخرى كالحواسيب بسبب الاتصال الدائم بالإنترنت وتعدد أنظمة التشغيل واعتمادها على تطبيقات مختلفة بالإضافة إلى ضعف الوعي الأمني لدى الاشخاص المستخدمين، ومن هنا تبرز الحاجة الأكاديمية والعلمية إلى دراسة الأسباب التي تدفع إلى ضرورة مواجهة هذه التهديدات ليس فقط لحماية خصوصية الأفراد وأمن معلوماتهم بل أيضاً لاستقرار المنظومات الرقمية الحديثة لذا فإن التصدي لهذه المخاطر بات مسؤولية جماعية تستلزم تعاوناً بين الأطر القانونية والتقنية والتوعوية ومن هنا نتناول مسألة تجنب تلك التهديدات من خلال منطلقين هما ([1]):

اولاً- اليات الحماية من الاختراق السيبراني للهواتف النقالة

1- عند اختيار رقم السري لحساب شخصي او للبطاقة الائتمانية يجب ان نتجنب الرموز سهلة التنبؤ مثل تواريخ الميلاد ورقم الهاتف، واستعمال كلمات سر قوية للغاية تحتوي على ارقام وحروف ورموز كبيرة وصغيرة ومشكّلة أي يجب ان لا تكون كلمة المرور سهلة وبسيطة.

2- عدم تدوين الرقم السري داخل المحفظة الشخصية او خلف البطاقة.

3- عدم مشاركة بيانات بطاقتك مع أي شخص آخر، ولا تكشف عن رقمها السري لأحد

الاتصال بشبكات Wi-Fi الموثوقة ، و تجنب الاتصال بشبكات Wi-Fi العامة أو المجهولة المصدر حيث يمكن للمهاجمين استخدام هذه الشبكات للوصول غير المصرح به إلى هاتفك ويمكن عند الضرورة استخدام شبكة VPN عند الاتصال بشبكات Wi-Fi العامة لتشفير اتصالك مما يجعل من الصعب على المتسللين تتبع وسرقة بياناتك ([2]).

4- تثبيت تحديثات النظام: يجب تثبيت أحدث تحديثات النظام المتاحة لهاتفك الذكي كون هذه التحديثات تحتوي على تصحيحات أمان مهمة لسد الثغرات الأمنية.

5- تنزيل التطبيقات من مصادر موثوقة: يجب تنزيل التطبيقات فقط من متاجر التطبيقات الرسمية مثل Google Playأو App Store وفحص التطبيقات قبل تنزيلها للتأكد من خلوها من البرامج الضارة، كذلك تفعيل الحماية من الفيروسات من خلال تثبيت برنامج مكافحة الفيروسات على هاتفك للكشف عن البرامج الضارة والحماية منها.

6- الحذر من الرسائل الاحتيالية وتجنب فتح رسائل أو ملفات مرفقة غير معروفة، وتجنب النقر على روابط غير موثوقة في الرسائل الإلكترونية أو الرسائل النصية و *عدم الاستجابة لاي* اعلانات تطلب معلومات شخصية او معلومات عن البطاقة الائتمانية مثل الرقم السري او كلمة المرور وتذكر ان المصرف لا يطلب هذه المعلومات برسالة نصية ولا عبر البريد الالكتروني ، ويمكن التحقق من ان

([1])راشد محمد حمد المري ، الامن السيبراني وحماية الانظمة الالكترونية : دراسة تحليلية تأصيلية، مجلة الدراسات القانونية والاقتصادية ، المجلد 9، العدد1، 31مارس 2023

([2]) مركز الاعلام الرقمي يحمل شركات الهاتف النقال مسؤولية حماية مستخدميها من انتحال ارقامهم الهاتفية ، مركز الاعلام الرقمي ، 29يوليو 2022، متاح على هذا الرابط : https://dmc-iq.com/2022/07/29/%D9%85%D8%B1%D9%83%D8%B2-%D8%A7%D9%84%D8%A5%D8%B9%D9%84%D8%A7%D9%85-%D8%A7%D9%84%D8%B1%D9%82%D9%85%D9%8A-%D9%8A%D8%AD%D9%85%D9%91%D9%84-%D8%B4%D8%B1%D9%83%D8%A7%D8%AA-/%D8%A7%D9%84%D9%87%D8%A7%D8%AA

الموقع موثوق من وجود" قفل "أو "https://" في بداية عنوان الموقع، وهذا يشير إلى أن الموقع آمن .

7- في حال استبدال البطاقة او الغائها ، يجب التأكد من التخلص منها ،وقص الشريحة المغناطيسية الموجودة عليها.

8-*يجب تعيين قفل الشاشة لحماية* الهاتف من الوصول غير المصرح به، *ويمكن استخدام رمز PIN أو نمط أو بصمة الأصبع أو التعرف على الوجه*.

9- تنزيل التطبيق الخاص بالمصرف والتاكد من انه موثوق من متجر التطبيقات المناسب لنظام التشغيل الخاص بجهازك الذكي مثل App Store لنظام iOS أو Google Play لنظام Android ،و مراقبة الحسابات المالية عبر الإنترنت من خلال هذا التطبيق بانتظام للتحقق من الأنشطة والمعاملات، و عند إجراء المعاملات يجب التأكد من أنك تتعامل مع موزع (منفذ) موثوق به وآمن وتجنب تزويد البطاقة لأشخاص غير موثوق بهم.

10- قم بتمزيق الإيصالات التي تحتوي على معلومات بطاقة الائتمان الخاصة بك إلى قطع صغيرة قبل التخلص منها،لا ترمي الإيصالات في سلة المهملات العامة.

11- النسخ الاحتياطي للبيانات: قم بعمل نسخ احتياطية للبيانات المهمة على هاتفك بشكل منتظم، لحمايتها في حالة حدوث أي خلل أو هجوم سيبراني([1]) .

***ثانياً*- سبل مواجهة الاختراق السيبراني للهواتف النقالة**

أول خطوة يجب اتخاذها هي التأكد من أن الهاتف قد تعرض فعلاً لهجوم سيبراني، في حال ملاحظة أي سلوك غير طبيعي مثل بطء غير مبرر في الجهاز، أو استهلاك مفرط للبيانات أو البطارية، أو ظهور تطبيقات غير معروفة، يجب التفكير في احتمالية تعرض الجهاز لهجوم ، بعد التأكد من الهجوم يجب اتباع الاتي ([2]) :

1- قطع الاتصال بالأنترنت على الفور: يجب وضع الهاتف في وضع الطيران هذا سيمنع المخترق من الوصول عن بعد لجهازك.

2- تغيير كلمات المرور للحسابات الشخصية على الفور: من جهاز اخر امن قم بتغيير كلمات المرور للحسابات الحرجة مثل البريد الالكتروني و البطاقة المصرفية وحسابات التواصل الاجتماعي، يجب عليك استخدام كلمات قوية وفريدة لكل حساب.

3- تحديد أي نشاط غير عادي في الجهاز مثل التطبيقات غير المألوفة المثبتة او الرسائل غير المتوقعة او أي معاملات غير مصرح بها وقم بازالتها من الجهاز.

4- برامج الأمان: يجب تنصيب تطبيق موثوق لمكافحة الفيروسات او البرامج الضارة ثم قم باجراء فحص شامل للجهاز.

5- تحديث برمجيات الجهاز: تاكد من ان نظام تشغيل الهاتف و التطبيقات محدثة لانه في حالة وجود ثغرات أمنية في نظام التشغيل يتم معالجتها من خلال التحديث المستمر للهاتف.

6-*تغيير إعدادات الخصوصية: يجب مراجعة إعدادات الخصوصية على هاتفك والتأكد من تحديد الإعدادات التي تحمي بياناتك الشخصية.*

7- يجب الحذر عند استعادة البيانات من النسخ الاحتياطي حيث قد تحتوي بعض النسخ الاحتياطية على البرمجيات الخبيثة، لذلك من الأفضل استعادة البيانات بشكل تلقائي([3]) .

([1]) راشد محمد حمد المري ، الامن السيبراني وحماية الانظمة لالكترونية : دراسة تحليلية تأصيلية ،مصدر سابق ، ص960

([2])كاسبرسكي، كيف تحمي نفسك من المهاجمين: الوقاية من الهجمات الإلكترونية، مركز موارد كاسبرسكي، بدون تاريخ، متاح على هذا الرابط: https://me.kaspersky.com/resource-center/preemptive-safety/protect-yourself-from-cyberattack .

([3])Cisco Networking Academy, Introduction to Cybersecurity, accessed June 5, 2025, https://prelogin-authoring.netacad.com/ar/courses/cybersecurity/introduction-cybersecurity

8- اذا كان الاختراق يتضمن التلاعب ببطاقة SIM يجب ابلاغ شركة الاتصال الخاصة بك لكي يقدمون لك نصائح او دعم إضافي.
9- إعادة ضبط المصنع: كحل أخير في حال عدم نجاح الطرق السابقة يمكن لعملية إعادة ضبط المصنع ان تزيل معظم أنواع البرامج الضارة، يجب الانتباه ان هذا الاجراء يؤدي الى محو جميع البيانات الموجودة على الجهاز لذا من الضروري وجود نسخة .
10- اذا تم اختراق هاتفك بالفعل وتعرضت الى تهديد من المهاجمين يجب عليك ابلاغ الجهات المسؤولة على الفور وهي فريق الاستجابة للأحداث السيبرانية CERT العراقي على رقمهم الخاص 166 او البريد الالكتروني info@cert.gov.iq ([2]).
أضافة إلى ماتقدم إن التهديدات السيبرانية للهواتف النقالة تتطلب استجابة شاملة متعددة الأبعاد، تبدأ من وعي المستخدم وتنتهي عند التشريعات الدولية، وإن تعزيز خط الحماية الأول للهاتف باعتباره بوابة الدخول للبيانات يظل عاملاً مركزياً في تقليص المخاطر وتوفير بيئة سيبرانية أكثر أماناً، ومن هنا فإن مواجهة هذه التهديدات تتطلب تعاوناً تكاملياً بين الفرد، والمؤسسة، والدولة، وصولاً إلى المجتمع الدولي.

المطلب الثالث: سياسة الحكومة العراقية في مواجهة التهديدات السيبرانية

أصبحت التهديدات السيبرانية أحد أبرز التحديات الأمنية التي تواجه الدول في العصر الحداثوي الرقمي، لا سيما مع التحول المتسارع في الخدمات الإلكترونية في مختلف القطاعات الحيوية، ويعد العراق من بين الدول التي بدأت تدرك حجم هذه المخاطر وتأثيراتها المحتملة على الأمن القومي والبنى التحتية الحيوية، وأمام هذا الواقع بدأت الحكومة العراقية بوضع سياسات واستراتيجيات لمواجهة هذه التهديدات، في إطار سعيها لحماية الفضاء السيبراني الوطني وتعزيز قدراتها الدفاعية الرقمية ([3]).
بدأ مفهوم الأمن السيبراني بالظهور في الخطاب السياسي العراقي مع تصاعد الهجمات التي استهدفت البنى التحتية الحيوية (كالكهرباء، والمطارات، ومواقع الوزارات) بعد عام 2014، وهو العام الذي شهد تصاعد نفوذ الجماعات الإرهابية الرقمية في المنطقة، لا سيما تنظيم داعش، الذي استخدم الفضاء السيبراني لأغراض دعائية وعملياتية،ويلاحظ أن المقاربة العراقية تجاه الأمن السيبراني ظلت حتى وقت قريب مقاربة دفاعية، تركز على رد الفعل بعد حدوث الاختراق، بدلًا من بناء منظومة وقائية واستباقية شاملة، وذلك نتيجة ضعف الإدراك المؤسساتي لمخاطر الفضاء الرقمي في البدايات([4]).
وعلى هذا فالعراق يفتقر الى قانون متكامل للامن السيبراني ،حيث ان الجهد التشريعي الابرز تمثل في مشروع قانون الجرائم المعلوماتية الذي وضع لاول مرة عام 2011 واعيدت مناقشته في 2020 ، وقد اثار جدلا واسعا بسبب ما اعتبره البعض مساسا بالحريات الرقمية مما أخر قراره ، ومع ذلك فإن بعض القوانين الجزئية تحاول معالجة الجرائم الرقمية مثل قانون العقوبات العراقي رقم (111) لسنة 1969 المعدل، وقانون مكافحة الإرهاب رقم (13) لسنة 2005، لكنها غير كافية لمواجهة التهديدات السيبرانية المعقدة ذات الطبيعة التقنية العالية([5]) .
وبهذا قامت الحكومة العراقية بتشكيل عدة كيانات في العقد الاخير بهدف ادارة الفضاء السيبراني ومنها مركز الامن السيبراني في وزارة الداخلية الذي يختص برصد التهديدات وتوجيه التحذيرات الامنية ومراقبة الهجمات الالكترونية لاسيما في المؤسسات الحكومية ،ووحدة امن المعلومات في جهاز الامن

([1]) مركز الامن السيبراني العراقي ،مهام مديرية الامن السيبراني في نشر الوعي الامني ، وزارة الداخلية العراقية ، 22/كانون الاول /2024، متاح على هذا الرابط : https://www.moi.gov.iq/?page=6295
([2]) مركز الامن السيبراني العراقي ،مهام مديرية الامن السيبراني في نشر الوعي الامني ، وزارة الداخلية العراقية ، 22/كانون الاول /2024، متاح على هذا الرابط : https://www.moi.gov.iq/?page=6295
([3]) علاء عبيس راضي ، الهجمات السيبرانية والامن الوطني العراقي بين المواجهة والادارة ، مركز البيان للدراسات والتخطيط ، 2025/2/17، متاح على هذا الرابط : https://www.bayancenter.org/2025/02/13311/
([4])مصطفى ابراهيم سلمان ، الامن السيبراني وأثره في الامن الوطني العراقي ، مجلة العلوم السياسية والقانونية ، جامعة ديالى ، كلية القانون والعلوم السياسية ، المجلد 10 ، العدد 1، 2021، ص153-180
([5])علاء عبيس راضي ، الهجمات السيبرانية والامن الوطني العراقي : بين المواجهة والادارة، مصدر سابق

الوطني والذي يعنى بتحليل التهديدات السيبرانية ذات الطابع الاستخباراتي ومتابعة الانشطة الرقمية الضارة ، وايضا هيئة الاعلام والاتصالات والتي تشمل مراقبة المحتوى الرقمي وشبكات الاتصالات ولها دور في حماية البنى التحتية للاتصالات ، واخيرا قسام تكنولوجيا المعلومات في الوزارات رغم وجوده بشكل متفاوت في الوزارات الا انه يعاني من ضعف الامكانيات التقنية والبشرية ، الا ان المشكلة المركزية تكمن في غياب مركز وطني موحد للقيادات السيبرانية ينسق جهود هذه الجهات تحت اطار استراتيجي واحد ([1]).

اما الاستراتيجيات الوطنية التي اطلقتها الحكومة العراقية بالتعاون مع شركاء دوليين عام 2022(مسودة الاستراتيجية الوطنية للامن السيبراني 2022_2026) والتي تضمنت الاهداف الاتية ([2]):

1- بناء القدرات التقنية والبشرية من خلال التدريب والتعليم وتطوير فرق الاستجابة الرقمية.

2- تعزيز الحوكمة السيبرانية عبر تطوير أطر تنظيمية وادارية تحكم العمل السيبراني بين الجهات الحكومية .

3- نشر ثقافة الوعي السيبراني عبر حملات مجتمعية وتعليمية .

4- تعزيز التعاون الدولي خصوصا مع المنظمات الاممية والاتحاد الاوروبي والويات المتحدة .

ورغم أهمية هذه الاستراتيجية الا انها ماتزال في مرحلة التنفيذ الاولى وتفتقر الى مؤشرات قياس الاداء والتمويل المستدام كما أن تنفيذها على المستوى الاقليمي والمحلي محدود .

اما التحديات البنيوية في السياسة السيبرانية العراقية تكون محددة بعدة نقاط منها ([3]):

1_ ضعف البنية التحتية الرقمية ، حيث تعتمد العديد من المؤسسات على شبكات وأجهزة متهالكة غير محدثة مايجعلها عرضة للاختراقات .

2_ نقص الكوادر المؤهلة ، حيث يعاني العراق من ندرة الخبراء المتخصصين في الامن السيبراني لاسيما في المحافظات .

3_ غياب الاطار القانوني الموحد وعدم وضوح الصلاحيات بين المؤسسات .

4_ تهديدات متقدمة تقنيا من جهات دولية وميليشيات رقمية تستخدم ادوات هجومية معقدة تتجاوز قدرات الدفاع التقليدي .

أضافة الى ماتقدم فأن الحكومة العراقية تواجه تحديًا استراتيجيًا في بناء سياسة سيبرانية فعالة تتسم بالشمولية، والمرونة، والمهنية، ورغم ما تحقق من خطوات تنظيمية واستراتيجية، إلا أن الطريق لا يزال طويلاً في ظل التحديات البنيوية والتقنية القائمة، إن ضمان الأمن السيبراني للعراق لا يتطلب فقط بنى مؤسسية وتشريعية، بل يتطلب تحولًا ثقافيًا في فهم طبيعة التهديدات الرقمية وتحديث مقاربة الدولة تجاهها، وفق إطار تشاركي يشمل الحكومة، والمؤسسات الأكاديمية، والقطاع الخاص، والمجتمع المدني.

الخاتمة

لقد باتت التهديدات السيبرانية التي تستهدف الهواتف النقالة تمثل إحدى أبرز التحديات الأمنية في العصر الرقمي، لاسيما في ظل الاعتماد المتزايد على هذه الأجهزة في مختلف مفاصل الحياة الشخصية والمهنية، ويواجه العراق كغيره من الدول مخاطر متصاعدة ناتجة عن ضعف البنى التحتية الرقمية، وغياب الوعي المجتمعي الكافي، إضافة إلى الاستغلال المتنامي للثغرات التقنية من قبل جهات مخربة داخلية وخارجية.

أنَّ السياسات الحالية ما تزال تعاني من ضعف في التنفيذ، وتفتقر إلى استراتيجية وطنية موحدة، شاملة ومحدثة، تأخذ في الحسبان تطور التهديدات وخصوصية البيئة التكنولوجية والاجتماعية العراقية .

([1])نسرين رياض شنشول ود. انور حامد حمد ، الامن السيبراني وحماية الاقتصاد العراقي : التهديدات السيبرانية واستراتيجيات المواجهة ، مركز البيان للدراسات والتخطيط ،2025/4/23 ، متاح على هذا الرابط :
https://www.bayancenter.org/2025/04/13599/

([2])المصدر نفسه

([3])مصطفى ابراهيم سلمان ، الامن السيبراني واثره في الامن الوطني العراقي ، مصدر سابق

استنتاجات

لا يمكن تجاهل أهمية حماية الهواتف النقالة من التهديدات السيبرانية، حيث تشكل هذه التهديدات خطراً حقيقياً على الخصوصية والأمان الشخصي، ويتطلب تأمين الهواتف النقالة استخدام استراتيجيات متعددة الطبقات تشمل التحديثات الدورية للأنظمة والتطبيقات، واستخدام كلمات مرور قوية، وتفعيل خدمات الحماية والتعقب المدمجة في الأجهزة، وينبغي على المستخدمين التحسين في التوعية السيبرانية وتعلم السلوكيات الآمنة على الإنترنت، بما في ذلك عدم فتح روابط مشبوهة أو تحميل ملفات من مصادر غير موثوق بها.

توصيات

هذه بعض التوصيات التي يمكن للحكومة اتباعها لمواجهة التهديدات السيبرانية للهواتف النقالة، ومن المهم أن تكون هذه التوصيات مستمرة ومحدثة لمواجهة التهديدات المتطورة في عالم التكنولوجيا.
1- تعزيز التوعية والتثقيف: يجب على الحكومة تعزيز التوعية بأمان الهواتف النقالة وتثقيف المستخدمين حول التهديدات السيبرانية المحتملة وكيفية حماية أنفسهم.
2- تطوير القوانين والتشريعات: وضع قوانين وتشريعات صارمة لحماية الهواتف النقالة ومعاقبة المتسببين في الهجمات السيبرانية.
3- تطوير التكنولوجيا الأمنية: دعم البحث والتطوير في مجال التكنولوجيا الأمنية للهواتف النقالة وتطوير حلول فعالة لمكافحة التهديدات السيبرانية.
توفير الدعم والمساعدة: توفير الدعم والمساعدة للأفراد والشركات التي تتعرض للهجمات السيبرانية، بما في ذلك توفير الخدمات القانونية والتقنية اللازمة.
3. تعزيز البنية التحتية السيبرانية: تعزيز البنية التحتية السيبرانية لضمان أمان الهواتف النقالة وحماية البيانات الحساسة.
4. التعاون الدولي: التعاون مع الدول الأخرى والمنظمات الدولية لمكافحة التهديدات السيبرانية وتبادل المعلومات والخبرات.
6. تعزيز التعاون مع القطاع الخاص: التعاون مع الشركات المصنعة للهواتف النقالة ومزودي الخدمات لتعزيز أمان الأجهزة وتحسين الحماية من التهديدات السيبرانية.

قائمة المصادر والمراجع :

أولا – الكتب العربية

1- د.فرح يحيى زعاترة، التهديدات السيبرانية على الامن القومي الامريكي ، العربي للنشر والتوزيع ، القاهرة ،2023،ص35
2- ايهاب خليفة ، الحرب السيبرانية الاستعداد لقيادة المعارك العسكرية في الميدان الخامس ، العربي للنشر ، القاهرة ، 2021، ص35
3- محمد عبد القادر الداغستاني، النظرية العسكرية والمذهب العسكري والعقيدة العسكرية : دراسة تحليلية بضمنها تطور النظريات العسكرية عبر تاريخ فن الحرب ، الاكاديميون للنشر والتوزيع ،الاردن ،2019،ص108
4- امير فرج يوسف، مكافحة الارهاب الالكتروني :الارهاب الرقمي في ظل الاتفاقية دول مجلس التعاون الخليجي ،دار الكتب والدراسات العربية ،2016،مصر ، ص253

ثانيا- التقارير والمجلات العلمية

1- عبد الغاني شرقي ،التهديدات السيبرانية واشكالية السيادة :اعادة قراءة لسيادة واستقاليا ،جامعة امحمد بوقرة بومرداس ،الجزائر، مجلة السياسة العالمية،المجلد7،العدد2 ، 2023 ، ص272-273

2ـجاسم محمد طه، التهديدات السيبرانية وانعكاساتها على الامن الوطني الامريكي ، المجلات الاكاديمية العلمية العراقية ، جامعة الموصل ، كلية العلوم السياسية ،2024/6/30 ، ص184

3ـ احمد عبيس الفتلاوي ،الهجمات السيبرانية مفهومها والمسؤولية الدولية الناتجة عنها في ضوء التنظيم الدولي المعاصر ، مجلة المحقق الحلي للعلوم القانونية والسياسية ، مجلد 8، العدد 4، جامعة بابل ،2016، ،ص615

4ـ مصطفى ابراهيم سلمان الشمري ، الامن السيبراني واثره في الامن الوطني العراقي ،مجلة العلوم القانونية والسياسية ،مجلد 10،العدد الاول، جامعة ديالى ،2021،ص153

5ـ نورة شلوش ،القرصنة الالكترونية في الفضاء السيبراني التهديد المتصاعد من الدول ، مجلة مركز بابل للدراسات الانسانية ، مجلد 8، العدد 2 ، 2018، ص200

6- فاطمة الزهراء بو شملة ،التهديدات السيبرانية واثرها على الامن القومي في ظل التحول الرقمي ،مجلة العلوم القانونية والسياسية ،جامعة محمد خيضر، بسكرة، العدد20، 2019

7- بلعسل بنت بني ياسمين و عمروش الحسين ،التهديدات الالكترونية والامن السيبراني في الوطن العربي ،مجلة نوميروس الاكاديمية ، المجلد الثاني ،جامعة الدكتور يحيى فارس المدية ، الجزائر ،2021،ص167

8- حسن بن احمد الشهري ، الانظمة الالكترونية الرقمية المطورة لحفظ وحماية سرية المعلومات من التجسس ،المجلة العربية للدراسات الامنية والتدريب، المجلد(28)، العدد(56)،الرياض،2012،ص11

9- عادل جارش، مقاربة معرفية حول التهديدات الامنية الجديدة ، مجلة العلوم السياسية والقانون ،العدد(1)، 2017، ص259

10- نوران شفيق،اشكال التهديدات الالكترونية ومصادرها،المركزالاوربي لدراسات مكافحة الارهاب ،متاح على هذا الرابط:https://www.europarabct.com/?=34807،تاريخ الدخول2024/1/17

11- حسين باسم عبد الامير ،تحديات الامن السيبراني ، مركز الدراسات الاستراتيجية ، جامعة كربلاء ، ايار 2018، متاح على هذا الرابط :
https://kerbalacss.uokerbala.edu.iq/wp/blog/category/politic/husain-basim/?utm_source=chatgpt.com

12- سفيان العامري ، الامن السيبراني والهواتف الذكية : التهديدات واساليب الحماية ، مجلة دراسات امنية ، المجلد 8، العدد2، 2022، ص112_135

13- راشد محمد حمد المري ، الامن السيبراني وحماية الانظمة الالكترونية : دراسة تحليلية تأصيلية، مجلة الدراسات القانونية والاقتصادية ، المجلد 9، العدد1، 31مارس 2023

14- كاسبرسكي، كيف تحمي نفسك من المهاجمين: الوقاية من الهجمات الإلكترونية، مركز موارد كاسبرسكي، بدون تاريخ، متاح على هذا الرابط: https://me.kaspersky.com/resource-center/preemptive-safety/protect-yourself-from-cyberattack .

15- علاء عبيس راضي ، الهجمات السيبرانية والامن الوطني العراقي بين المواجهة والادارة ، مركز البيان للدراسات والتخطيط ، 2025/2/17، متاح على هذا الرابط :
https://www.bayancenter.org/2025/02/13311/

16- مصطفى ابراهيم سلمان ، الامن السيبراني وأثره في الامن الوطني العراقي ، مجلة العلوم السياسية والقانونية ، جامعة ديالى ، كلية القانون والعلوم السياسية ، المجلد 10 ، العدد 1، 2021، ص153-180

17- نسرين رياض شنشول ود. انور حامد حمد ، الامن السيبراني وحماية الاقتصاد العراقي : التهديدات السيبرانية واستراتيجيات المواجهة ، مركز البيان للدراسات والتخطيط ،2025/4/23 ، متاح على هذا الرابط :https://www.bayancenter.org/2025/04/13599/

ثالثا : المواقع الالكترونية

1- مركز الاعلام الرقمي يحمل شركات الهاتف النقال مسؤولية حماية مستخدميها من انتحال ارقامهم الهاتفية ، مركز الاعلام الرقمي ، 29يوليو 2022، متاح على هذا الرابط : https://dmc-iq.com/2022/07/29/%D9%85%D8%B1%D9%83%D8%B2-%D8%A7%D9%84%D8%A5%D8%B9%D9%84%D8%A7%D9%85-%D8%A7%D9%84%D8%B1%D9%82%D9%85%D9%8A-%D9%8A%D8%AD%D9%85%D9%91%D9%84-%D8%B4%D8%B1%D9%83%D8%A7%D8%AA-/%D8%A7%D9%84%D9%87%D8%A7%D8%AA

2- مركز الامن السيبراني العراقي ،مهام مديرية الامن السيبراني في نشر الوعي الامني ، وزارة الداخلية العراقية ، 22/كانون الاول /2024، متاح على هذا الرابط :
https://www.moi.gov.iq/?page=6295

رابعا: المصادر الاجنبية

1_ cybersecurity:manaying systems,conducting manaying systems, conducting Testing,and lnvestigating lntrusions . jones&Bartlett learning.
2_ Vacca ,computer and lnformation security Hand book, Morgan kaufmann,2014
3_ The National Strategy for Critical Infrastructure Security and Resilience" , The White House,oct 31/2023 ،متاح على هذا الرابط:
https://www.google.com/search?q=The+National+Strategy+for+Critical+Infrastructure+Security+and+Resilience%22+%2C+The+White+House%2Coct+31%2F2023&rlz=1C1YTUH_arIQ1080IQ1082&oq=The+National+Strat

4_ Mason Rice, Sujeet Shenoi, Critical Infrastructure Protection X: 10th IFIP WG 11.10 International Conference, ICCIP 2016, Arlington, VA, USA, March 14-16, 2016, Revised Selected Papers. AICT-485, 2016, IFIP Advances in Information and Communication ، متاح على هذا الرابط: https://dl.ifip.org/IFIP-TC11/hal-01614866v1
5_ Marco Roscini, Cyber Operations and the Use of Force in International Law, OXFORD UNIVERSITY PRESS,2014,P87
6_ TZIPORA HALEVI,NASIR D.MEMON,ODED NOV,SPEAR-PHISHING IN THE WILD :Areal-world Study Of Personality, Phishing self –Efficacy and Vuluerability to spear-Phishing Attacks, SSRN Electronic journal ,NEWYOURK,128, January 2015
7_ Yifei Wang,Asurvey of phishing detection:from an intelligent countermeasures View,IEEE XPlore,11 DEC 2022, متاح على هذا الرابط:
https://ieeexplore.ieee.org/document/10016193/authors#authors

8_ Gargi Sakar and Sandeep K.Shukla,Behaviorsal anaglysis of Cybercrime:paving the way for effective policing strategies ,Journal of Economic criminology,December2023, متاح على هذا الرابط: https://www.sciencedirect.com/science/article/pii/S2949791423000349

9_ Markus Jakobsson and Steven Myers, Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft,New Jersey, Wiley-Interscience, 2006).

10_ Cisco Networking Academy, Introduction to Cybersecurity, accessed June 5, 2025, https://prelogin-authoring.netacad.com/ar/courses/cybersecurity/introduction-cybersecurity.

11_ Cisco Networking Academy, Introduction to Cybersecurity, accessed June 5, 2025, https://prelogin-authoring.netacad.com/ar/courses/cybersecurity/introduction-cybersecurity