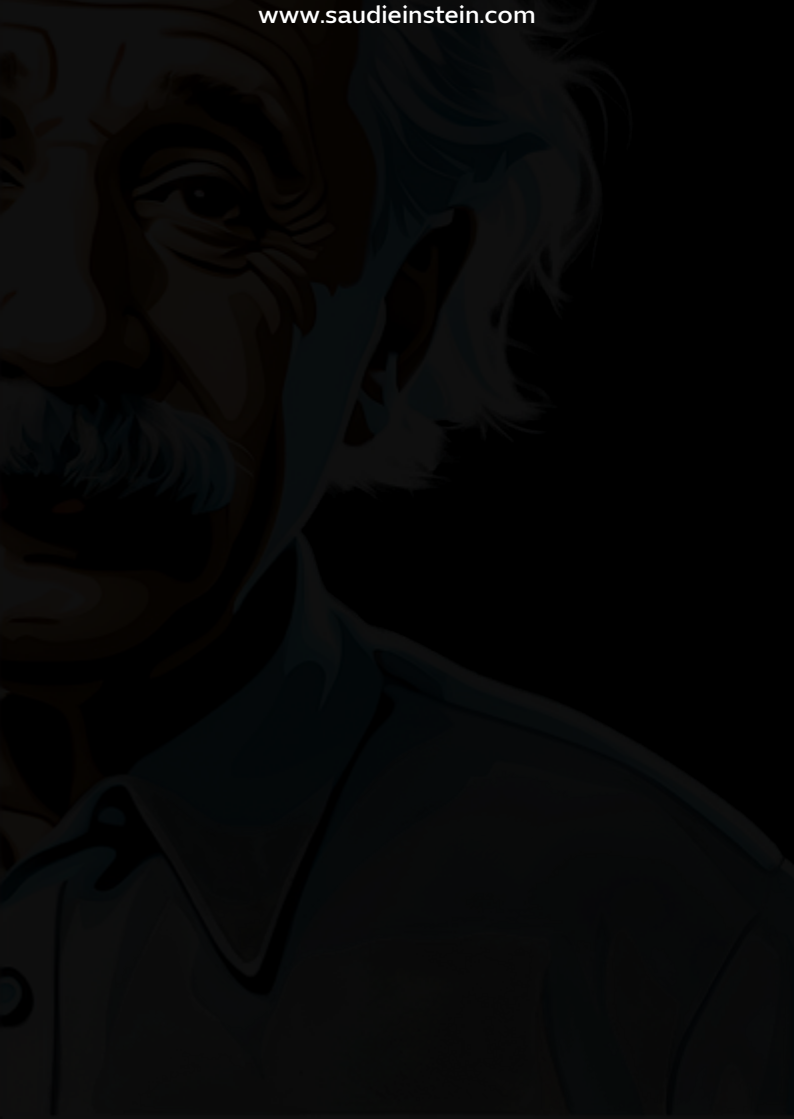
ثلاثية "ثغرات السيادة" 2من يكتب اكوادك يرسم مصيرك:خريطة الاختراق الناعم في زمن السيادة المبرمجة

21 يونيو 2025

تقنية وذكاء اصطناعي

27 دقيقة قراءة



ثلاثية "ثغرات السيادة" 2من يكتب اكوادك يرسم مصيرك:خريطة الاختراق الناعم في زمن السيادة المبرمجة



من يصل إلى شبكتك... يكتب سطور تاريخك بيدك، لا بيدهِ.. كيف زرعت إسرائيل والهند - مثالًا- ثغراتها في قلب أنظمتنا... على هيئة عقد صيانة وتحديث منتصف الليل.

في زمنٍ صارت فيه السيادة تُباع بعقود الصيانة، والأوطان تُخترق بتحديثات منتصف الليل، يبرز التحالف الاستخباراتي بين الهند وإسرائيل مثالًا كأحد أخطر التحالفات الهجينة في العصر الرقمي. تحالف غير معلن، لكنّ بصماته واضحة في الكود، والبنية، والقرارات الفنية التي لا تُراجَع؛ أو بالأحرى، التي نخشى مراجعتها كي لا نكتشف أنّنا نكتب نشيد السيادة بأقلام مستوردة، ونوقّع استقلالنا بحبر مغشوش.

في 17 يونيو 2025، أي بعد أربعة أيام فقط من "عملية Rising Lion" الإسرائيلية الدموية ضد إيران، نشر الباحث توماس كيث تغريدة مثيرة زعم فيها أن الهجوم فضح شبكة تجسس مشتركة امتدت 25 عامًا، جمعت بين الموساد وRAW، واستغلّت الجاليات والشركات الهندية كحصان طروادة ناعم داخل الخليج. التغريدة، وإن كانت غير مؤكدة رسميًا ومصدرها مشكوك فيه، لامست أحداثًا واقعية لم تعد قابلة للإنكار، على رأسها: قضية الجواسيس الهنود في قطر، 2023.

ثمانية ضباط في قطر: حين تُسرّب الأسرار بابتسامة الخبير البحري

في أكتوبر من ذاك العام، أصدرت محكمة

قطرية حكمًا بالإعدام على ثمانية ضباط هنود سابقين في البحرية، عملوا في شركة استشارات دفاعية محلية تُدعى "دهرهـ" تلك الشركة البريئة كحمامة نوح، والماكرة كثعلب الصحراء. التهمة: تسريب معلومات حساسة عن مشروع الغواصات القطرية إلى طرف ثالث، رجحت تقارير أنه إسرائيل. لم تُفصح الحكومة عن كل التفاصيل، لكن الرسالة وصلت: لا يمكن الوثوق التام حتى بالكوادر التقنية "المحايدة"؛ لئن كان ثمّة شيء اسمه الحياد في عصر الاستخبارات الناعمة، حيث الولاءات تُشترى بالعقود وتُباع بالأكواد.

والحال أنّ اكتشاف الأمر جاء عبر جهود استخبارية مكثفة راقبت أنشطة الشركة، واحتُجز

المتهمون انفرادياً لعدة أشهر. ورغم عدم إعلان روابط رسمية بين المتهمين وجهاز RAW، تُرجح تحليلات مستقلة أنهم تصرّفوا بتنسيق غير مباشر مع الموساد، وربما بدافع من جهات في الهند. وقد أسقطت قطر في نهاية المطاف أحكام الإعدام وأفرجت عن الضباط في مطلع 2024 بعفو أميري؛ بعد وساطات دبلوماسية طبعاً، وربما بعد صفقات نجهل تفاصيلها كما نجهل مفاتيح أنظمتنا الرقمية، ونظلّ نجهلها حتى تنفجر في وجوهنا.

لكنّ الحادثة لم تكن الأخيرة؛ ففي مطلع 2025، اعتُقل مهندس من شركة Tech Mahindra في قطر بتهمة سرقة بيانات حساسة، مما أكّد أنّ النمط مستمر كنبض

القلب: منتظم، ثابت، قاتل. يلوح، إذن، أنّ الاختراق صار نهجاً لا حادثة عابرة، صار عقيدة لا زلّة. أم أنّنا، كعادتنا، سنكتفي بالدهشة والاستنكار، ثمّ نعود لتوقيع عقود جديدة مع الشركات نفسها، مبرّرين ذلك بأنّ "الخطأ فرديّ والشركة بريئة"؟

حين نكتب سيادتنا بأكواد الآخرين: اعترافات مؤلمة عن واقع رقمي مُر

قبل أن نناقش التهديدات، علينا الاعتراف بما هو أعمق وأمرّ: أنّ كثيرًا من الأنظمة السيادية في الخليج لم تُصمّم محليًا، بل بُنيت من الخارج، وأُديرت بعقود تشغيل وصيانة أجنبية. أنظمة الجوازات، العدالة، التعليم، وحتى الهوية الوطنية، كثير منها بدأ تحت أيدٍ لا تتحدث

العربية، ولا تحلم بأحلامنا، ولا تخاف مخاوفنا. لم نكتب الكود. لم نراجع الشيفرات. ولم نكن نملك الخوادم. كأنّنا في غمرة السباق نحو الحداثة الرقمية، وقّعنا عقد ثقة أبدية مع من يملكون مفاتيح خزائننا الرقمية، ثمّ نمنا قريري العين.

بيد أنّ من يكتب الكود يملك القرار؛ ومن يُحدّث النظام يتحكّم في مصيره؛ ومن يملك البيانات يرسم المستقبل. وكأنّ السيادة عندنا تنتهي عند حدود العَلَم والنشيد الوطني، نرفع الأعلام نهاراً ونغنّي الأناشيد، ونُخترق رقمياً ليلاً ونصمت.

هذا التحالف الصامت بين الموساد وRAW ليس وليد اللحظة، ولا ابن الصدفة. ففي عام 2000، زار وزير الداخلية الهندي أدفاني إسرائيل، وشكر

الموساد على مساعدته في تعقّب مطلوبين داخل الخليج. منذها، ترسّخ التحالف: الموساد يملك التقنية والخبرة الاستخبارية، وRAW تملك النفاذ البشري والغطاء التجاري، عقد زواج مقدّس تُباركه مصالحنا المخترَقة وتشهد عليه ثغراتنا الأمنية. ومنذ 2008، بعد تفجيرات مومباي، بات التنسيق أكثر عمقًا، وأكثر حضورًا في الخليج، وأشدّ فتكاً بسيادتنا.

ذاك أنّ هذا التعاون يقوم على مصلحة مشتركة في مواجهة الإرهاب والجماعات المتطرفة - أو هكذا يقولون- بينما يتبادلون معلوماتنا كأوراق اللعب، ويتقاسمون أسرارنا كغنيمة حرب لم نشارك فيها. منذ الثمانينات تبادل الطرفان المعلومات حول أنشطة

باكستان النووية. واليوم، أصبحت الهند أكبر مستورد للسلاح الإسرائيلي، ووقّعا اتفاقيات في الأمن السيبراني منذ 2017. حلف مقدّس إذن، لكن قرابينه من لحمنا ودمنا الرقميّ.

الشركات الهندية في الخليج: حمائم نوح التي تحمل رسائل الموت

ففي قطر، يبلغ عدد الهنود نحو 700 ألف نسمة — أي ربع السكان تقريبًا- وكأنّك تمشي في شوارع الدوحة فتسمع الأوردو أكثر مما تسمع العربية. وفي الإمارات، يتجاوز عددهم 3.4 مليون، أي نحو 35 إلى 38٪ من السكان؛ ما يعني أن الهند حاضرة هناك ليس كسوق تصدير، بل كقوة سكانية موازية. أما في السعودية، فالأرقام أكثر خفاءً، لكنّها لا تقلّ

دلالة: قرابة 2.6 مليون هندي، أي نحو 8٪ من إجمالي السكان، أو ما يعادل 14٪ من كامل الوافدين لم تعد الحاجة لإرسال عملاء سرّيين قائمة. فقط مهندس برمجيات يحمل في لوحة مفاتيحه مفاتيح وطن وفي ابتسامته براءة قابيل، أو موظف صيانة بقميص نظيف وضمير مُباع بثمن بخس، أو محلل بيانات بشهادة دولية وولاء مزدوج كعملة نادرة، كلّهم يملكون صلاحية الوصول إلى ما لا نملكه نحن، أصحاب الأرض والسيادة.

والشركات الكبرى - TCS وWipro وأخواتهما المباركات - تدير مشاريع حيوية تمسّ صميم وجودنا: في السعودية، نفّذت TCS مشروع التحوّل الرقمي للتأمينات الاجتماعية، ولها حضور

فـي الاتصـالات والمصـارف؛ فـي قطـر، أدارت مبادرة نظم المعلومات الجغرافية؛ أما Wipro، فهي الشريك التقني لبوابة حكومة دبي، وتدير أنظمة مصرف الإمارات الوطني. شركة Tech Mahindra الهنديـة تـولّت بنـاء نظـم "المراقبـة القانونيــة" فــي البحريــن - نعــم، المراقبــة القانونية!- كأنّنا نسلّم مفاتيح السجن لمن قد يصبح سجّاناً، ونعطـي سـوط الجلاّد لمـن قـد يجلدنا غداً.

ومع هذا، لا تُطرح أسئلة حول الأكواد التي تُزرع كألغام صامتة، أو البيانات التي تُنسخ كلصوص الليـل، أو التحـديثات التـي تُفعّـل فـي منتصـف الليل كقنابل موقوتة. كأنّ الثقة صارت عمياء والبصيرة انطفأت، والرقابة غدت ترفاً لا نملكه

فـي زمـن السـرعة والإنجـاز؛ أو لعلّنـا نخشـى أن نكتشف أنّنا نُكتب أكثر مما نكتب، نُراقَب أكثر مما نراقِب، نُختزَق أكثر مما نحمي.

مـن PROMIS إلـى Pegasus: تـاريخ الاختـراق الرقمي يتكرر بأدوات أحدث

لا شيء يربط هذه الحوادث ظاهريًا، لكنّ ما بينها خيط استراتيجي واضح كخيط العنكبوت: دقيق، شفّاف، قاتل. اختراق سيادي مقنّع بقناع الخدمة؛ استخبارات ناعمة متقنّعة بزيّ التقنية. مـن Pegasus إلـى Stuxnet، ومـن AppCloud إلـى البيجر المتفجّـر، العـدو لا يـدخل مـن البـاب المحصّـن، بـل مـن تحـديث بسـيط نضغـط عليـه بإصبع الثقة، أو عقد خدمة نوقّعه بقلم الغفلة، أو اتفاقية روتينية نمرّرها بختم اللامبالاة. أو من

ابتسامة مهندس هندي يقول: "صباح الخير، جئت لأصلح النظام" وهو يعني في سرّه: جئت لأملك النظام، لأسرق البيانات، لأرسم خرائط الضعف.

تذكّروا جيّداً: PROMIS، النظام الذي اخترق مئات الأنظمة السيادية عبر نسخة "محسّنة" كحصان طروادة العصريّ؛ Stuxnet الذي دمّر أجهزة الطرد المركزي في "مفاعل نطنز النووي" بإيران بكود برمجي فقط، دون طلقة واحدة؛ Pegasus الذي تم تثبيته على هواتف شخصيات خليجية بارزة، وبعض خوادمه كانت تمر عبر البنية التحتية الإقليمية، نعم، بنيتنا نحن كانت الممر والمعبر والجسر! كأنّنا نوفّر الطريق السريع للصوص كي يسرقونا براحة، ونضيء

لهم المصابيح كي يروا الغنائم بوضوح.

هذا النمط يتكرّر بإصرار المجرم العائد: شركة برمجيات تبيعك منتجًا ملوّثًا ملفوفًا بورق الثقة الذهبيّ، موظف تقني يملك مفاتيح الخوادم وربما مفاتيح المصير الوطنيّ، منصة أجنبية تدمج في بنيتك الوطنية بلا مراجعة أو محاسبة أو حتى تساؤل. إذا لم تُفكك هذه النماذج كمشروع استخباراتي واحد متكامل الأركان، فسنظل نواجه كل حادثة على أنها مفاجأة من السماء. أغلب الظنّ أنّنا سنستمر في دفن رؤوسنا في الرمال، فهذه رياضتنا الوطنية العربية المفضّلة، نمارسها بإتقان الأبطال الأولمبيّين منذ عقود.

البيجر المتفجّر: تسع سنوات من الصبر

الاستخباراتي تنفجر في لحظة

في سبتمبر 2024، فجّرت إسرائيل آلاف أجهزة البيجر في أيدي عناصر حزب الله. الأجهزة كانت صُمّمت في إسرائيل، وبِيعت عبر واجهات تجارية بريئة المظهر. التفعيل تمّ برسالة مشفّرة واحدة. عشرات القتلى، وآلاف الجرحى، وسؤال وحيد يصرخ في الفضاء: من أين جاء هذا الاختراق؟ من سلسلة التوريد؛ تلك السلسلة التي نثق بها ثقة العاشق الأعمى، ونسلّمها مقاليد حياتنا وموتنا.

تسع سنوات من التخطيط والتنفيذ الصبور؛ تسع سنوات زرعت فيها إسرائيل الثقة كبذرة، ورعتها بماء الخداع، ثم فجّرتها في لحظة واحدة كقنبلة عنقوديّة. راهناً، ما يُخشى أن يكون قد

حُقن في بيئة "حزب الله" قد يُحقن - بأدوات أكثر دقة وحرفيّة - في أنظمة دول الخليج. إلاّ إذا كنّا نظنّ أنّنا محصّنون بقوّة خارقة لا يملكها الآخرون، أو أنّ السماء تحمينا دون سواها، أو أنّ حظّنا أفضل من حظّ غيرنا.

عمليــة Rising Lion: حيــن تتحــول البيانــات المسروقة إلى خرائط موت

وإذ كـان البيجر درساً فـي الصـبر الاستخباراتي الطويـل، فـإنّ مـا حـدث فـي إيـران درس فـي التطوّر النوعي للاختراق المعاصر. ففي 13 يونيو 2025، وبينمـا كنّـا نكتـب عـن ثغـرات السـيادة الرقميـة ونحـذّر مـن مخاطرهـا، جـاءت "عمليـة Rising Lion" الإسـرائيلية لتؤكّـد أنّ الاختـراق الاستخباراتي لـم يعـد يكتفـي بسـرقة البيانـات

والمعلومات. تسعة علماء نوويين إيرانيين بارزين اغتيلوا في يوم واحد - بينهم فريدون عباسي ومحسن فخري زادة - إلى جانب كبار قادة الحرس الثوري: القائد الجديد حسن سلامي، وقائد قوات الجو الفضائي علي حاجي زادة، ورئيس الأركان محمد باقري، وقادة المخابرات العسكرية واحداً تلو الآخر.

والسؤال الذي لا يُطرح - أو الذي نخشى طرحه- كما نخشى النظر في المرآة صباحاً: كيف عرفت إسرائيل مواقعهم الدقيقة، تحرّكاتهم اللحظيّة، أماكن تواجدهم في تلك اللحظة بالذات، بالثانية والدقيقة؟

الإجابة تكمن في سنوات من الاختراق الصامت الدؤوب. معلومات جُمعت قطرة قطرة كماء

المطر في الصهريج، من هاتف مخترَق هنا، ونظام مراقبة مُباع هناك، وموظف مُجنّد في مكان ثالث، وشركة صيانة في مكان رابع. وربما - وهذا احتمال لا يمكن استبعاده مهما بدا مؤلماً - عبر شبكات التعاون الاستخباراتي بين الموساد وRAW، التي قد تكون وفّرت معلومات حساسة من مصادر غير متوقعة. ولعلّ بعض هذه المعلومات مرّت عبر خوادمنا دون أن ندري؛ كضيف عابر لا يترك أثراً إلا الدمار والموت!

هذا هو التطوّر الطبيعي للاختراق الرقمي في عصرنا: يبدأ بسرقة بيانات تبدو عاديّة، وينتهي بسرقة أرواح ثمينة. السيادة الرقمية كالعذرية؛ تُفقد مرة واحدة، ولا تُستعاد بعقود الصيانة أو وعود التحديث.

والحال أنّ ما حدث في إيران ليس استثناءً لن يتكرّر، ولا حادثة معزولة في سجلّ التاريخ، بل نموذج لما يمكن أن يحدث حين تتحوّل المعلومات المسروقة إلى خرائط اغتيال دقيقة كدقّة ساعة برج مكة. في الخليج، حيث الشخصيات الاعتبارية تتحرّك في بيئة مفتوحة نسبياً، وحيث أنظمة المراقبة والاتصالات تديرها شركات أجنبية بعقود طويلة الأمد، السؤال ليس "هل يمكن أن يحدث هذا؟" بل "متى سيحدث؟" وهل سنكتفي حينها بإصدار بيان شجب واستنكار نكتبه بالحبر نفسه الذي وقّعنا به عقود اختراقنا، أم سنبحث عن شركة أخرى لتكتب لنا البيان بلغة أجمل؟

ذاك أنّ الموظف الذي يزرع برنامج تتبّع في برج

اتصالات لا يجمع فقط بيانات عامة عابرة؛ إنّه يرسم خريطة دقيقة لحركة كل شخصية مهمة: متى تدخل مكتبها، أين تتناول غداءها، مع من تجتمع، أي طريق تسلك، متى تنام ومتى تستيقظ. معلومات تبدو بريئة كوجه طفل رضيع، لكنّها في يد الخصم تتحوّل إلى أدوات قتل أدقّ من رصاصة قنّاص، وأخطر من صاروخ موجّه.

مشاهد من الاختراق اليومي: حين يملك الضيف مفاتيح البيت

في إحدى الوزارات السيادية، يعمل موظف أجنبي في الدعم الفني، بعقد مع شركة صيانة دولية مرموقة. يملك صلاحيات الوصول إلى السيرفر الرئيسيّ. خلال صيانة ليلية روتينيّة،

ينسخ نسخة احتياطية من قواعد البيانات على وحدة تخزين مؤقتة. خلال دقائق معدودة، تكون معلومات ملايين المواطنين - أسماؤهم، عناوينهم، أرقامهم، مواقعهم، ارتباطاتهم، تحرّكاتهم - في متناول جهة أجنبية. والمسؤول عن الأمن السيبراني؟ نائم في بيته، مطمئن البال إلى أنّ "الشركة عالمية ولديها شهادات أمنية معتمدة" كمن يحرس خزنة بقفل ذهبي لامع بينما اللص يملك المفتاح الأصلي، بل يملك مصنع المفاتيح!

وفي شركة اتصالات كبرى، يزرع موظف آخر برنامج تتبّع صامت في برج رئيسي يغطّي منطقة حيويّة. خلال أسبوع واحد، تُبنى قاعدة بيانات شاملة تُظهر حركة كل شخصية اعتبارية

بدقّـة مذهلـة. مـن هنـا تبـدأ القـدرة علـى الاستهداف الدقيق، الاغتيال المحسوب، الابتزاز المدروس، أو التجنيد الناعم. وكلّ هذا يحدث بينما نحن منشغلون بمناقشة ميزانية الأمن السيبراني التي ترفعنا بالمؤشرات للعام القادم، دون مناقشة مخاطر الاستيراد والأجانب وكيفية التوطين، لم نناقش ذلك العام الماضي، ولن نناقشه العام المقبل، فالهدف خبر بوكالة الأنباء وانفوجرافيك لتصنيفات إعلامية لا واقعية، والثغرة تتّسع يوماً بعد يوم كجرح لا يندمل!

حتى لو خزّنت بياناتك محليًا في خوادم وطنيّة، فإن شركة أميركية تُخضَع بموجب قوانين مثل Cloud Act أو Patriot Act، ويمكن أن تُجبر قانونياً على تسليم البيانات لحكومتها. ينطبق

الشيء نفسه بحذافيره على الشركات الصينية التي تخضع لـ Data Security Law الصارم.

السيادة الحقيقيّة لا تتحقق فقط بموقع الخادم الجغرافيّ، بل بمن يملكه فعليّاً، ومن يكتب له الكود الأساسيّ، ومن يتحكم في تحديثاته اليوميّة، ومن يملك مفاتيح تشغيله. وإلاّ، فأنت كمن ينقل السجن من بلد إلى آخر ويظنّ أنّه تحرّر؛ ثم يحتفل بافتتاح السجن الجديد ويدعو السجّان لقصّ الشريط، ويصفّق له الجمهور!

القانون هناك يفرض نفسه هنا بقوّة السيف؛ والاختراق اليوم لم يعد فعلًا عسكريًا استثنائيّاً، بل ممارسة تجارية روتينية يوميّة. يتسلّل في شكل خدمة تقنية بريئة، تحديث ضروريّ، شراكة برمجية مثمرة.

في قطر، لم تُطلق رصاصة واحدة؛ فقط لوحة مفاتيح صامتة في يد خبير بحري ماهر. ولعلّه كان يبتسم ابتسامة الرضا وهو يسرّب الأسرار، ابتسامة المنتصر الذي يعرف أنّه لن يُحاسَب، وأنّ ضحاياه لن يعرفوا حتى أنّهم ضحايا!

لماذا الآن؟ التوقيت ليس صدفة والصمت ليس حكمة

ليس صدفة أن تطفو هذه القضايا الشائكة في 2025 بالذات. فبعد حرب غزة 2023، حين انحازت الهند علنًا لإسرائيل بلا مواربة، أُثيرت حساسيات عميقة في الرأي العام الخليجي، ذلك الرأي العام الذي نتجاهله عادة كطفل مشاغب حتى ينفجر كبركان نائم استيقظ فجأة. إقليمياً، انخراط دول الخليج في اتفاقيات

إبراهيم وتقارب بعضها مع إسرائيل ولّد مخاوف مشروعة من اختراقات استخبارية مرافقة ومخاوف صامتة، طبعاً، مكتومة في الصدور، فنحن لا نجرؤ على التصريح بها كأنّها عورة وطنية يجب سترها. وبعد أن كان التركيز لعقود طويلة على تهديدات الإرهاب التقليديّ، بدأ الاهتمام ينتقل تدريجيّاً إلى أمن المعلومات والسيادة الرقمية. وجاءت عملية Rising Lion في يونيو 2025 لتؤكد بما لا يدع مجالاً للشكّ أنّ المخاوف لم تكن من فراغ، بل من واقع أمرّ من الحنظل، وأخطر من السمّ.

بيد أنّ التركيز على التهديد الهندي الإسرائيلي لا ينبغي أن يحجب الصورة الأوسع والأشمل. فالصين، عبر مجموعات قرصنة محترفة مثل

APT27، استهدفت مؤسسات حكومية وشركات اتصالات في الشرق الأوسط بهجمات منسّقة؛ روسيا وإيران لهما سوابق موثّقة في اختراق منشآت خليجية حسّاسة؛ أمّا الولايات المتحدة، فرغم كونها حليفًا استراتيجيّاً، كشفت تسريبات سنودن الشهيرة أن وكالة NSA راقبت اتصالات في الشرق الأوسط بشكل مكثف ومنهجيّ. ومشروع Raven الإماراتي الذي نفّذه عملاء أمريكيون سابقون دليل ساطع على أنّ حتى الحلفاء يتجسّسون، حلفاء بالنهار المشرق، جواسيس بالليل المظلم! الصداقة في النهار لا تمنع التجسّس في الليل.

التجسس، إذن، بات "لعبة الجميع ضد الجميع" في عصر المعلومات الرقميّة؛ والتهديد الهندي

الإسرائيلي، وإن كان خطيرًا ومتناميًا، يبقى جزءًا من صورة أكبر وأعقد. صورة نرفض النظر إليها مباشرة لأنّها تُظهر حقيقة مؤلمة كالجرح النازف: أنّنا عراة رقمياً كآدم في الجنّة، لكن بلا براءته الأولى، وبلا أوراق التوت!

البراغماتية المُرّة: لماذا نستمر في احتضان من يخترقنا؟

رغم المخاوف الأمنية المتصاعدة، تستمر دول الخليج في الاعتماد الكثيف على الخبرات الهندية. لماذا؟ لأنّ البدائل مكلفة ماليّاً وغير متوافرة بشريّاً. العمالة الهندية مؤهلة تقنيّاً ومنخفضة التكلفة نسبياً، واستبدالها سريعًا سيضرّ بالنمو الاقتصادي المنشود - ونحن نعشق النمو الاقتصادي أكثر من عشقنا

للسيادة الوطنيّة- نعبد الأرقام الخضراء ونهمل الحقائق الحمراء، نطارد المؤشّرات ونتجاهل المخاطر. الهند مستورد رئيسي للنفط والغاز الخليجي، والعلاقات الاستراتيجية -عبر بريكس ومشاريع الممر الاقتصادي الطموحة - تفوق في أهميتها الآنيّة المخاطر الأمنية "المحدودة" أو "المحتملة".

لهذا اختارت قطر سياسة الاحتواء الهادئ الحكيم: حاكمت المتهمين بصمت دبلوماسيّ، ثم أطلقتهم بعفو أميري كريم، وأبقت على صفقات بمليارات الدولارات مع الهند سارية المفعول. البراغماتية السياسية تقتضي إدارة المخاطر بحكمة، لا قطع العلاقات بحماقة. يلوح أنّنا محكومون بالواقعية المُرّة أكثر من المثاليات

الأمنية أو ربما نحن ببساطة جبناء رقميون نخاف المواجهة الصريحة أكثر من خوفنا من الاختراق الصامت.

لم تعد إسرائيل أو الهند بحاجة ماسّة إلى اختراق عبر الجدران المحصّنة؛ فقط عبر واجهات التطبيقات البريئة، والكوابل الضوئيّة السريعة، والواجهات الخلفية المنسيّة. هذا هو التطبيع التقني الاستخباراتي الجديد: حين تصبح الخدمات نافذة مشرّعة، والكود عميلًا نائمًا ينتظر الإيقاظ، والعقد الموقّع صكّ استسلام مؤجّل. الاختراق اليوم يأتي مغلّفًا بورق هدايا جميل: عقد استشاري مربح، أو شراكة تقنية واعدة، أو برنامج تدريبي متقدّم. يدخل من الباب الأمامي الواسع، بابتسامة عريضة صادقة،

وشهادات دولية معتمدة - ونحن نصفّق له بحرارة ونمنحه مفاتيح المملكة الرقميّة!

سياسات السيادة الرقمية: بين الطموح والواقع المرير

تُظهر السياسات الخليجية وعيًا متزايدًا - أو هكذا نحبّ أن نوهم أنفسنا ونطمئن قلوبنا. سنت السعودية قانون حماية البيانات (PDPL) الطموح، ومنعت نقل البيانات خارج حدودها دون إذن سيادي صريح؛ ألزمت سدايا بتوطين استضافة البيانات الحكومية الحسّاسة؛ فرضت قطر والإمارات إقامة البيانات محليًا بقوانين صارمة، وقيّدت استخدام السحابات الدولية المشبوهة.

وأطلقت السعودية مشاريع ضخمة مثل: STC

Sovereign Cloud بالشراكة مع Oracle، نعم، شراكة مع شركة أمريكية عملاقة لبناء سيادة رقمية وطنيّة! كمن يستأجر حارساً أجنبيّاً ليحرسه من الحرّاس الأجانب، أو يستعين بلصّ محترف ليحميه من اللصوص. وسحابة SCCC بالتعاون الوثيق بين STC وAlibaba Cloud – الصينية هذه المرّة– لأنّ تنويع مصادر الاختراق المحتمل أفضل من احتكارها بيد واحدة! وأكاديمية طويق لتأهيل آلاف السعوديين الشباب في مجالات الأمن السيبراني وهندسة الأنظمة المتقدّمة، تصرخ: متى توطنون الوظائف التقنية؛ فشبابنا لا يقلون عن أفضل الموادر العالمية متى ماتوفر الدعم والإرادة.

ثم، أين التقييم الشامل والصريح بعد حادثة

قطر المدوّية؟ أين التحقيق السيادي العميق في عقود الشركات التقنية المشبوهة؟ الصمت الرسـمي مفهـوم سياسـيّاً، لكـن السـكوت التنظيمي غير مقبول أمنيّاً. أم أنّنا ننتظر فضيحة أكبر وأفدح لنستيقظ من سباتنا، فضيحة تُكتب فصولها الآن، فـي هـذه اللحظـة بـالذات، فـي خوادمنا المخترقة؟

الخليـج يحمـل خصـائص بنيويـة فريـدة تجعلـه هـدفًا مغريًـا للاختـراق: التركيبـة السـكانية المفتوحة كساحة مطار دولي مزدحم، الاعتماد الكثيف على الخبرات الأجنبية كطفل رضيع على أمّه، الطفرة التقنية السريعة المذهلة دون نمو مـوازٍ فـي الكـوادر المحليـة المؤهّلـة، الثـروة النفطيـة الهائلـة التـي تجـذب الذبـاب والنحـل

والدبابير معاً، والموقع الجيوسياسي الحساس كقلب نابض على مفترق شرايين العالم.

أضف إلى ذلك عاملاً تاريخيّاً مؤثّراً: الاعتماد التاريخي الطويل على الحماية الأمنية الغربية جعلنا أقل تطورًا في قدرات الاستخبارات المضادة المحلية الذاتيّة. كنّا نعتمد كليّاً على القواعد الأمريكية والبريطانية للرصد والحماية، لكن هذا قد يعني اختراقات خفية ماكرة من الحلفاء أيضًا. أغلب الظنّ أنّنا ندفع الآن ثمن عقود من الاتّكالية الأمنية المريحة - والفاتورة لم تكتمل بعد، بل لعلّها لم تبدأ حقّاً!- المستقبل قد يحمل مفاجآت أكثر إيلاماً.

التوصيات الواضحة التي ستبقى حبراً على ورق المملكة بدأت فعليّاً تبني سيادتها الرقمية

بخطوات واثقة، ووضعت اللبنات الصحيحة في البنية والخبرة والتشريع. لكن السيادة الحقيقيّة لا تـأتي بالاسـتثمارات الضخمـة وحـدها، بـل بالتدقيق الصارم، والمراجعة المستمرّة، وإحلال الكفاءة الوطنية محل الاعتمادية الأجنبيّة. ما لم نراجـع بدقّـة مـن يكتـب الكـود الأساسـيّ، ومـن يراجـع العقـود الحسّاسـة، ومـن يملـك مفاتيـح التحديث اليوميّ، فسنظل ننقل بنيتنا التحتية من "الاختراق المحتمل" إلى "الاحتلال الرقمي التدريجي" ونحتفل بكل نقلة كأنّها فتح مبين، ونصفّق لكلّ إنجاز كأنّه نصر عظيم!

التوصـيات واضحـة كشمـس الظهيـرة: وحـدة اسـتخبارات تقنيـة متخصّـصة لفحـص الأكـواد البرمجية - فكل كود يدخل بيئة حكومية يجب أن

يُراجع وطنيًا بدقّة كما يُراجع الطعام صحّياً والدواء كيميائيّاً؛ تدقيق أمني دوري صارم لموظفي الشركات المتعاقدة - خاصة في البنية التحتية الحيويّة والاتصالات والبيانات السياديّة؛ توطين مفاصل التشغيل الفعليّة، لا فقط الواجهة التجميليّة - فلا يكفي أن نُعيّن مديرًا سعوديًا للعلاقات العامّة والمهندس الأجنبي هو من يدير النظام من الخلف ويملك كلّ المفاتيح؛ بنك بيانات استخباراتي شامل عن العلاقات الخفية بين الشركات الكبرى وجهات خارجية مشبوهة؛ وأخيراً، وحدة حماية متخصّصة للشخصيات الاعتبارية رقمياً، تراقب البصمة الرقمية للقيادات والعلماء والشخصيات الحساسة على مدار الساعة، وتضمن عدم

تسـرّب معلومـات حركتهـم وأنشطتهـم عـبر الأنظمة المخترَقة.

لكـن مـن سـيطبّق هـذه التوصـيات الحيويّـة؟ وهل سنكتفي بوضعها في تقرير أنيق مجلّد ثم ننساها فـي الأدراج كما نسينا تقارير سابقة كثيـرة؟ أم سـننتظر حتـى يكتـب الذكـاء الاصطناعي نفسه تقرير اختراقنا النهائيّ؛ بخط جميل أنيق وتوقيع رقمي مصدّق، وربّما بختم رسميّ أيضاً؟

السيادة الرقمية الكاملة المطلقة وهم جميل فـي عصـر العولمـة التقنيـة الجارفـة. حتـى مـع تـوطين البيانـات الحسّاسـة وبنـاء السـحابات المحلية الضخمة، ستبقى المعالجات من شركات عالميـة محـدودة معـدودة، والخوارزميـات مـن

عمالقة التقنية المحتكرين. لكن يمكن تحقيق مستوى معقول ومقبول من الحصانة الرقميّة عبر: توطين البيانات الحساسة بصرامة، تنويع مصادر التقنية بذكاء، بناء الكوادر المحلية بإصرار، والأطر القانونية الصارمة الواضحة.

الاتحاد الأوروبي نفسه - بكلّ إمكانيّاته الهائلة - يسعى لـ"سيادة رقمية" نسبية متواضعة عبر قوانين مثل GDPR الصارمة. نموذج يمكن أن نحتذي به مع تكييفه لواقعنا الخاصّ - لئن كنّا جادّين فعلاً في حماية أنفسنا، لا مجرّد متفرّجين سلبيّين على مأساتنا الرقمية المتفاقمة.

السيادة الرقمية مسألة حياة أو موت

السيادة الرقمية، إذن، ليست ترفاً تقنياً للمترفين، أو هوساً أمنياً للموسوسين؛ إنّها،

بالمعنى الحرفي الصريح للكلمة، مسألة حياة أو موت، بقاء أو فناء. فالمعلومة البريئة التي تُسرّب اليوم قد تتحوّل غداً إلى إحداثية دقيقة في خريطة اغتيال محكمة؛ والنظام الذي يُخترَق لجمع البيانات العاديّة قد يُستخدم لاحقاً لتوجيه الصواريخ القاتلة. وما حدث في إيران ليس سوى مثال صارخ حيّ على قدرة الاستخبارات المعاصرة المذهلة على تحويل البيانات المسروقة إلى عمليات قتل دقيقة ومنسّقة؛ قتل بالمعلومة قبل الرصاصة، اغتيال بالبيانات قبل السكّين.

———-

في المقال القادم، لن نسأل فقط: من يملك البيانات؟ بل: من يكتب الأكواد الأساسيّة؟ من

يراجع العقود الحسّاسة؟ من يُنشئ المنصة من الصفر؟ ومن يُحمي "منصة الوطن" من أن تتحول إلى منصة خيانة غير مرئية؟ هل نريد الاكتفاء بتوطين الواجهة الجميلة... بينما نُسلّم مفاتيح النظام نفسه لعقود أجنبية مشبوهة؟ وفي عصر الذكاء الاصطناعي القادم بقوّة، هل سنكرّر أخطاءنا القديمة ذاتها بأدوات أكثر تطوّراً وخطورة؟ أم سننتظر بصبر حتى يكتب الذكاء الاصطناعي نفسه تقرير اختراقنا النهائيّ - ويوقّعه باسمنا، ويختمه بختمنا الرسميّ؟

التوطين الوظيفي لا يكفي أبداً. نحتاج إلى التوطين السيادي الحقيقيّ. وإلّا، فسنظلّ نكتب تاريخنا بأكواد الآخرين، ونرسم مستقبلنا بأقلامهم. أم أنّنا، ببساطة مؤلمة، صرنا نُكتب ولا

نكتب؟