مؤسسة دبي للمستقبل
DUBAI FUTURE FOUNDATION

# الحياة بعد كوفيد-19

## اتجاهات المستقبل

# الأمن السيبراني

# الملخص

رصدت دولٌ عديدة حول العالم تزايد في الهجمات السيبرانية بالتزامن مع تفشي فيروس كورونا المستجد (كوفيد-19).

زادت الجرائم السيبرانية بسبب ضعف البنى التحتية الرقمية حالياً لأن أطقم أمن تقنية المعلومات يعملون من منازلهم دون وجود اتصالات بينهم، ولذا استغل المخترقون هذه الثغرة لاختراق الأنظمة الرقمية.

دفعت أزمة كوفيد-19 الدول إلى إعادة تقييم سياساتها الصارمة لخصوصية البيانات كي تستطيع تتبع المصابين والحد من انتشار الفيروس. لكن ذلك منح المخترقين فرصاً لاستهداف الأشخاص بالإضافة إلى أنه آثار تساؤلات عن مستقبل الرقابة الحكومية.

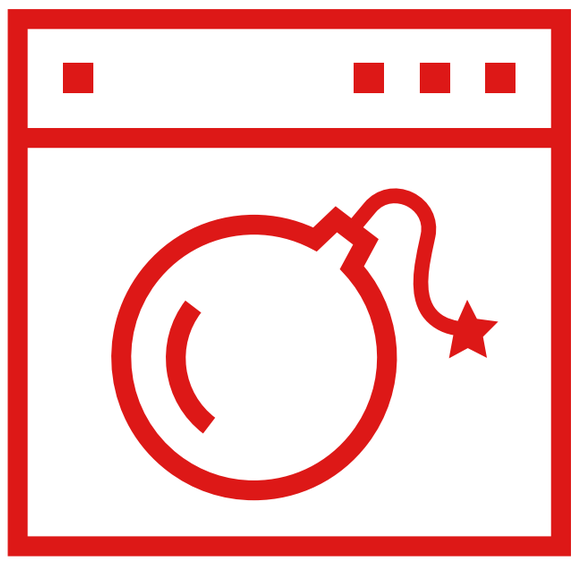
# الوضع الراهن

رصدت دولٌ عديدة حول العالم تزايد في الهجمات السيبرانية بالتزامن مع تفشي فيروس كورونا المستجد (كوفيد-19). إذ زادت رسائل البريد الإلكتروني المخادعة بأكثر من 600% منذ شهر فبراير 2020، واستهدف المخترقون الأشخاص والمؤسسات من خلال الروابط المشبوهة واختراق البريد الإلكتروني للحصول على بيانات الدخول إلى الحسابات والمعلومات المالية[1]. وحجبت جوجل 18 مليون رسالة بريد إلكتروني مخادعة على منصاتها[2]. وتعد هذه الرسائل إحدى أرخص وسائل الجريمة الإلكترونية وأسهلها، وتوجد أنواع أخرى من الهجمات السيبرانية. فمثلاً أنشأ هؤلاء المخترقون أكثر من 100 ألف نطاق جديد لمواقع إلكترونية عن كوفيد-19 في محاولة لخداع الأفراد كي يسجلوا بياناتهم الشخصية على هذه المواقع[3].

حجبت جوجل

**18 مليون رسالة بريد إلكتروني مخادعة**

على منصاتها



أنشأ المخترقون أكثر من

**100 ألف نطاق جديد لمواقع إلكترونية**

[1] Muncaster, P., "#COVID19 Drives Phishing Emails Up 667% in Under a Month", InfoSecurity, 2020.
[2] "Protecting businesses against cyber threats during COVID-19 and beyond", Google, 2020.
[3] Miles, R., "How to protect against cyberattacks when working from home during COVID-19", Intelligent CIO, 2020.

توجد أسباب عديدة وراء زيادة الهجمات السيبرانية. إذ ازداد ضعف البنى التحتية الرقمية حالياً لأن أطقم أمن تقنية المعلومات يعملون من منازلهم دون وجود اتصالات بينهم، ولذا لا يستطيعون اكتشاف هذه الهجمات سريعاً. ودفع التوتر الناجم عن أزمة كوفيد-19 الناس إلى النقر على روابط خطيرة ظناً منهم أنها تتضمن معلومات عن الفيروس. وبالإضافة إلى ذلك يسعى المخترقون إلى استغلال زيادة اعتماد الناس على الأنظمة الرقمية التي تستخدمها المستشفيات وجهات الخدمة العامة.

ويعد قطاع الرعاية الصحية من أكثر القطاعات تعرضاً للهجمات السيبرانية حالياً. إذ تستهدف المستشفيات والمراكز الطبية والمؤسسات العامة في مختلف أنحاء العالم من خلال هجمات برامج الفدية بصورةٍ أساسية. وتحتاج أطقم الرعاية الصحية إلى بنية تحتية رقمية لمواجهة أزمة كوفيد-19، واستغل المخترقون هذه الثغرة، ظناً منهم أن المؤسسات الصحية ستضطر إلى الدفع لاستعادة أنظمتها[4]. وتعرضت أيضاً منظمة الصحة العالمية إلى هجمات استهدفت المعلومات الشخصية لموظفيها[5].

يستغل المخترقون أيضاً أزمة الرعاية الصحية لبيع الأدوات الطبية المزيفة. ويشمل ذلك عمليات احتيال عديدة تورط فيها أفراد وكيانات تنتحل صفة المسؤولين الحكوميين، وتدعي هذه الكيانات توصلها إلى اكتشافات جديدة عن فيروس كورونا المستجد (كوفيد-19)، وتروج لمبيعات أو منتجات طبية وهمية[6]. وأبلغ المكتب الوطني للاستخبارات الاحتيالية في المملكة المتحدة عن خسائر بقيمة 1.6 مليون جنيه إسترليني بسبب الاحتيال المرتبط بكوفيد-19[7]. إذ دفعت ضحيةٌ واحدة 15000 جنيه استرليني لشراء أقنعة وهمية.[8]

4 “COVID-19 cyberthreats”, Interpol, 2020.
5 Warrell, H. & Manson, K., “State-backed hackers using virus to increase spying, UK and US warn”, Financial Times, 2020.
6 “Jackson Jr., J., “COVID-19 Raises Financial Crime Risks, Report Says”, Law 360, 2020.
7 Townsend, M., “Fraudsters exploiting Covid-19 fears have scammed £1.6m.” The Guardian, 2020
8 Sattler, J., “Latest Covid-19-related cyber security news: Hospitals under attack”, F-Secure, 2020.

وتضرر أيضاً القطاعان المالي والنفطي بشدة. إذ حذر مصرف الإمارات العربية المتحدة المركزي العملاء من المحتالين الذين يسعون إلى اختراق الحسابات المصرفية. وأصبح الأمن السيبراني أكثر أهمية نظراً لأن الدول في مختلف أنحاء العالم تسعى إلى رقمنة عملاتها وجميع معاملاتها المالية. ونشرت مجموعة العمل المعنية بالإجراءات المالية بين الحكومات تقريراً يوجز المخاطر المختلفة التي تواجهها الشركات نتيجةً أزمة تفشي فيروس كورونا المستجد (كوفيد-19)، وهي تشمل تزايد عمليات الاحتيال من خلال المجرمين الذين ينتحلون صفة المسؤولين و/أو يستخدمون الأصول الافتراضية لنقل الأموال غير القانونية[9].

خسائر بقيمة

**£1.6 مليون**

في المملكة المتحدة بسبب الاحتيال المرتبط بكوفيد-19

[9] Jackson Jr., J., "COVID-19 Raises Financial Crime Risks, Report Says", Law 360, 2020.

ولم يكن قطاع النفط أقل عرضةً للخطر، فهو أحد أكثر القطاعات تضرراً في منطقة الشرق الأوسط وشمال إفريقيا. إذ تعرضت شركاتٌ عديدة في كثيرٍ من الدول، مثل الولايات المتحدة الأمريكية وماليزيا وإيران وسلطنة عُمان ودولة الإمارات والمملكة العربية السعودية، إلى رسائل بريد إلكتروني مخادعة لإيهام مستقبليها أنها مرسلة من شركة نفط وغاز حقيقية في مصر، وهي شركة حكومية تسمى الشركة الهندسية للصناعات البترولية والكيماوية «إنبي.» وسعى المخترقون إلى الحصول على تفاصيل حساسة عن الأفراد وإنتاج النفط، كي يبيعوها بعد ذلك على الإنترنت المظلم[10].

**ولم يكن قطاع النفط أقل عرضةً للخطر، فهو أحد أكثر القطاعات تضرراً في منطقة الشرق الأوسط وشمال إفريقيا.**

ولا تقتصر عمليات الاختراق على الحكومات أو المنظمات فحسب، بل تتعرض منصات مؤتمرات الفيديو أيضاً للخطر. إذ تعرضت هذه الأدوات مؤخراً إلى بعض الهجمات باستغلال وجود كثير من الأشخاص على هذه المنصات لحضور الاجتماعات والفصول الدراسية والمحادثات العائلية والأغراض التجارية. وأبلغ المستخدمون عما يسمى قصف منصة زوم من خلال بعض الأشخاص الذين ينضمون عشوائياً إلى اجتماع الفيديو ويعطلونه بمحتوى غير قانوني. وظهرت تقارير تفيد أيضاً بأن تسجيلات مقاطع الفيديو على منصة زوم لم تحفظ في مساحة تخزين سحابية آمنة، ونشرت بعد ذلك

[10] Paraskova, T., "Hackers Have Ailing Oil Industry In Their Crosshair", Oil Price.Com, 2020.

على شبكة الإنترنت. وشمل ذلك اجتماعات عمل خاصة، ومحادثات شخصية بين عائلاتٍ وأصدقاء[11]. وعلى الرغم من أن تطبيق زوم يستخدم حاليًا خطوات تحقق متعددة، تتضمن إضافة كلمات مرور إلزامية للاجتماعات وخيارات قبول أو رفض الانضمام للاجتماعات، لكن الخطر ما زال يحيط باستخدام تطبيقات الاجتماعات.

وتعرضت أيضاً منصاتٌ أخرى مثل منصات الألعاب عبر الإنترنت إلى هجماتٍ سيبرانية. إذ سعى المخترقون إلى اختراق شبكة نينتندو للحصول على معلومات مالية شخصية، مستغلين زيادة عدد الحسابات عليها، بسبب شعبية بعض ألعابها الجماعية، مثل لعبة أنيمال كروسينج التي تتيح للأشخاص الاتصال ببعضهم افتراضياً[12]. ولذا عطلت الشبكة القدرة على تسجيل الدخول إلى الحسابات من خلال معرف شبكة نينتندو[13].

[11] O'Flaherty, K., "Zoom Security: Here's What Zoom Is Doing To Make Its Service Safer", Forbes, 2020.
[12] Basu, T., "Why games like Animal Crossing are the new social media of the coronavirus era", MIT Technology Review, 2020.
[13] Warren, T., "Nintendo confirms 160,000 Nintendo Accounts accessed in hacking attempts", The Verge, 2020.

# الفـــرصـــة

سيزداد اعتمادنا على البنية التحتية الرقمية خلال أزمة كوفيد-19 وبعدها. ما يعني زيادة التهديدات السيبرانية. ولذا وضعت الدول استراتيجيات للأمن السيبراني وسياسات لأمن شبكة الإنترنت لمواجهة هذه المخاطر المتزايدة. وفي دولة الإمارات مثلًا، قادت تطوير هذه الاستراتيجيات الهيئة العامة لتنظيم قطاع الاتصالات ومركز دبي للأمن الإلكتروني. أما عالمياً فاتخذت تدابير لحماية الخصوصية على شبكة الإنترنت، مثل النظام الأوروبي العام لحماية البيانات وقانون خصوصية المستهلك لعام 2018 في كاليفورنيا. لكن أزمة كوفيد-19 دفعت الدول إلى إعادة تقييم سياسات الخصوصية الصارمة للبيانات كي تستطيع تتبع المصابين مع الحد من انتشار الفيروس. إذ طبقت دول متعددة منها جنوب إفريقيا إعفاءات من إجراءات خصوصية البيانات للسماح بتجميعها خلال هذه الأزمة[14]. وعلى الرغم من ذلك توجد مخاوف من أن تخفيف قوانين خصوصية البيانات قد يمنح المخترقين فرصاً إضافية لاستهداف الأفراد من خلال استخدام تطبيقات تتتبع جهات الاتصال لتتبع مواقع الأشخاص واختراق هواتفهم.

[14] Daniel Visser, Research Call, C4IR South Africa, 2020.

# أزمة كوفيد-19 دفعت الدول إلى إعادة تقييم سياسات الخصوصية الصارمة للبيانات كي تستطيع تتبع المصابين مع الحد من انتشار الفيروس.

وتعالج بعض الشركات هذه المشكلة من خلال تعزيز أنظمتها الحالية. فمثلاً أصدرت كلٌ من جوجل وآبل بياناً يؤكد للمستخدمين أن نظامهم لتتبع الاتصال سيشفر وأن اتصال بلوتوث المستخدم لتتبع الموقع سيكون قوياً إلى درجة كافية كي لا يخترق لتحديد الموقع والحصول على تفاصيل الجهاز[15] .

وتسعى مجموعة من أعضاء مجلس الشيوخ الأمريكي الجمهوريين إلى تقديم مشروع قانون للخصوصية ينظم البيانات التي جمعتها التطبيقات الخاصة بتتبع التلاقي بين الأشخاص خلال أزمة كوفيد-19. وبموجب قانون حماية بيانات المستهلك خلال أزمة كوفيد-19، سيوفر القانون المطروح الأمريكيين بمزيد من الشفافية حول مكان وكيفية استخدام بياناتهم[16].
وعلى الرغم من أن التفاصيل ما زالت غير واضحة، فإن اللوائح المحتملة تطرح تساؤلاً عن مسؤولية الأمن السيبراني. هل هو مسؤولية مزود النظام أم دور الجهات التنظيمية؟ فمن منظور جوجل وآبل، يعد الأمن السيبراني مسؤولية الشركة ما يضمن عدم إمكانية اختراق النظام. وكذلك ترى الحكومات أن التعقب والأمن يقع ضمن نطاق مسؤوليتها، وقد أدى هذا إلى نقاش أوسع حول ما إن كنا نحتاج إلى تطبيق نظام المركزية الحكومية، لأن البلدان ذات البنى التحتية الرقمية المركزية مثل الصين وكوريا الجنوبية تتعامل مع الأزمة بشكل أفضل من البلدان ذات البنى التحتية الأكثر تنوعًا مثل الولايات المتحدة الأمريكية والمملكة المتحدة[17].

[15] McGee, P. & Murphy, H., "Apple and Google boost privacy and accuracy of contact tracing system", Financial Times, 2020.
[16] Lyons, K., "Senators' plan for reining in contact tracing apps doesn't make a lot of sense", The Verge, 2020.
[17] Goldsmith, J., "Internet Speech Will Never Go Back To Normal", The Atlantic, 2020.

وفي الدول العربية دفع كوفيد-19 الشركات إلى إعادة تقييم أنظمة الأمن السيبراني الخاصة بها. ورصدت تريند مايكرو، وهي شركة متعددة الجنسيات لها مقر في المنطقة، 8434 تهديداً لشركات البرمجيات على مدار الأشهر القليلة الماضية. وتمثل دول مجلس التعاون الخليجي من أكثر الدول عرضة للخطر من ناحية هجمات البرمجيات الخبيثة، إذ سجلت ما يقرب من 5.5 مليون محاولة خلال العام الماضي. وأبلغت المملكة العربية السعودية وحدها عن 2.4 مليون هجوم خلال العام 2019[18]. ولسد هذه الثغرات الأمنية، تسعى الشركات إلى تفعيل طبقات متعددة من الأمن السيبراني، ويشمل ذلك إضافة مزيد من جدران الحماية للأنظمة والشبكات الخاصة الافتراضية. (وخضع هذا الموضوع للنقاش بتوسع أكبر في تقرير مؤسسة دبي للمستقبل عن مستقبل الاتصالات)[19].

دول مجلس التعاون الخليجي
سجلت ما يقرب من

**5.5 مليون محاولة هجمات البرمجيات الخبيثة (malware)**

خلال العام 2019

**2.4 مليون هجمة في المملكة العربية السعودية**

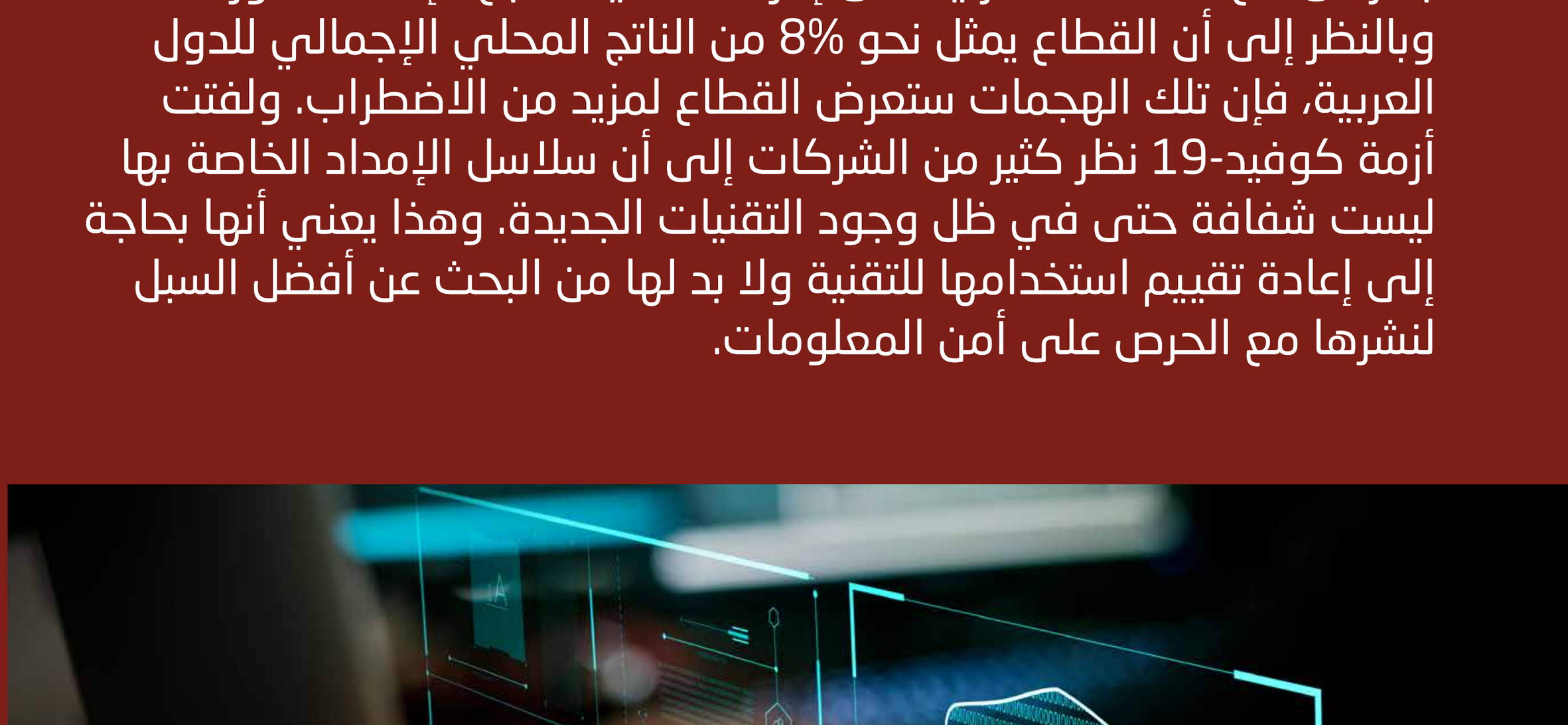
خلال العام 2019

[18] Binali, M., "Remote working calls for regional organisations to overhaul their cybersecurity postures", Arabian Business, 2020.
[19] Telecommunications, Dubai Future Foundation, April 15 2020.

وفي مجال التجارة الإلكترونية التي سيصل حجم سوقها إلى 28.5 مليار دولار في المنطقة العربية بحلول العام 2022[20]، تحاول الشركات التصدي لزيادة الهجمات الإلكترونية وعمليات التحايل. فمثلاً شركة أمازون التي طبقت سابقاً إجراءات تحقق شخصية من البائعين، بدأت بتجربة مكالمات الفيديو للتأكد من مطابقة وثائق الهوية لمقدم الطلب.[21]

وتستخدم أيضاً تقنيات جديدة لتحديث منصات الأمن السيبراني الحالية، إذ تبحث العديد من وكالات الاستخبارات العالمية في كيفية استخدام الذكاء الاصطناعي لمواجهة التهديدات السيبرانية. ويمكن استخدام تعلم الآلة لتحليل مجموعات البيانات وتحديد الأنماط والصلات الخاصة بالهجمات بسرعة أكبر مما يمكن أن يفعله المحققون باستخدام الوسائل التقليدية.[22]

أما في القطاع الصناعي، فارتفعت معدلات الهجمات السيبرانية أيضاً بالتزامن مع الاعتماد المتزايد على إنترنت الأشياء لتتبع الإمدادات ورصدها. وبالنظر إلى أن القطاع يمثل نحو 8% من الناتج المحلي الإجمالي للدول العربية، فإن تلك الهجمات ستعرض القطاع لمزيد من الاضطراب. ولفتت أزمة كوفيد-19 نظر كثير من الشركات إلى أن سلاسل الإمداد الخاصة بها ليست شفافة حتى في ظل وجود التقنيات الجديدة. وهذا يعني أنها بحاجة إلى إعادة تقييم استخدامها للتقنية ولا بد لها من البحث عن أفضل السبل لنشرها مع الحرص على أمن المعلومات.



[20] "Ecommerce in MENA expected to reach $28.5 billion by 2022: report", MENA Bytes, 2019.
[21] ANI, "Amazon pilots using video call to verify third-party sellers", Gulf News, 2020.
[22] Warrell, H., "UK intelligence urged to step up AI use to counter cyber threats", Financial Times, 2020.

# التخطيط للمستقبل

## على المدى القصير
(خلال تفشي كوفيد-19)

**1**

نتيجة لعمل موظفي أمن تقنية المعلومات عن بُعد، وانخفاض قدرتهم على اكتشاف الهجمات الإلكترونية بكفاءة لأن الموظفين لا يستخدمون خوادم موحدة عند العمل من المنزل، قد يتطلب ذلك تطبيق تدابير جديدة، مثل مشاركة الشاشة ومراقبة شاشات الأجهزة لضمان تأمين الموظفين. ومن المحتمل أن يثير هذا الأمر التساؤلات بشأن خصوصية البيانات أثناء العمل عن بُعد.

## من المدى القصير إلى الطويل
(ما بعد فيروس كوفيد-19)

**1**

ستزداد الأتمتة في مجال الأمن السيبراني وتصبح سائدة. وستبدأ الهيئات الحكومية في دراسة استخدام أنظمة الأمن السيبراني التي تعتمد على الذكاء الاصطناعي لتوفير التحليل المستمر للتهديدات السيبرانية والهجمات المحتملة. وسيعني ذلك أن الأتمتة ستدخل أيضاً في عمليات المراجعة الافتراضية لأنظمة تقنية المعلومات باستخدام أدوات المصادقة الذاتية مثل البلوكتشين.

**2**

سيستمر نمو الطب عن بعد خلال وبعد أزمة كوفيد-19 ليصبح إحدى أساليب الرعاية الصحية في جميع أنحاء العالم. ويجب سريعاً إقرار إرشادات موحدة لكيفية إعداد الأجهزة الطبية وتشغيلها لضمان سلامتها، ويشمل ذلك مكوناتها الأمنية.

# على المدى البعيد

سيزداد ذكاء هجمات المخترقين وستزداد صعوبة مكافحتها كلما تطورا التقنية. وستصبح الحوسبة الكوانتية عنصراً مهماً في الأمن السيبراني وتحليل الهجمات وصدها في غضون ثوانٍ. ومن ناحية أخرى، قد تصبح المركبات ذاتية القيادة عرضة للتجسس السيبراني والهجمات الإرهابية وستحتاج إلى الاعتماد على أنظمة الذكاء الاصطناعي لتحديد التهديدات والأنماط المحتملة.

خلال نمو سوق الأمن السيبراني، قد يفقد العاملون على أرض الواقع وظائفهم ذات الطبيعة الأولة، فمع تعمق استخدام الأتمتة في المستقبل سيراقب المبرمجون ومطورو المنتجات الأنظمة وهي تعمل وتقاوم الهجمات دون تدخلٍ منهم.

وسيؤدي هذا إلى وجود قطاع أمن إلكتروني عالمي يقوده الذكاء الاصطناعي، وقد يؤدي هذا إلى خرق قوانين خصوصية البيانات إن تجاوز تعلم الآلة القيود المفروضة على استخدام المعلومات الشخصية. ولهذا يجب إجراء تعديلات مستمرة على الأنظمة المطبقة لضمان تحقيق الأمن والخصوصية للأفراد.