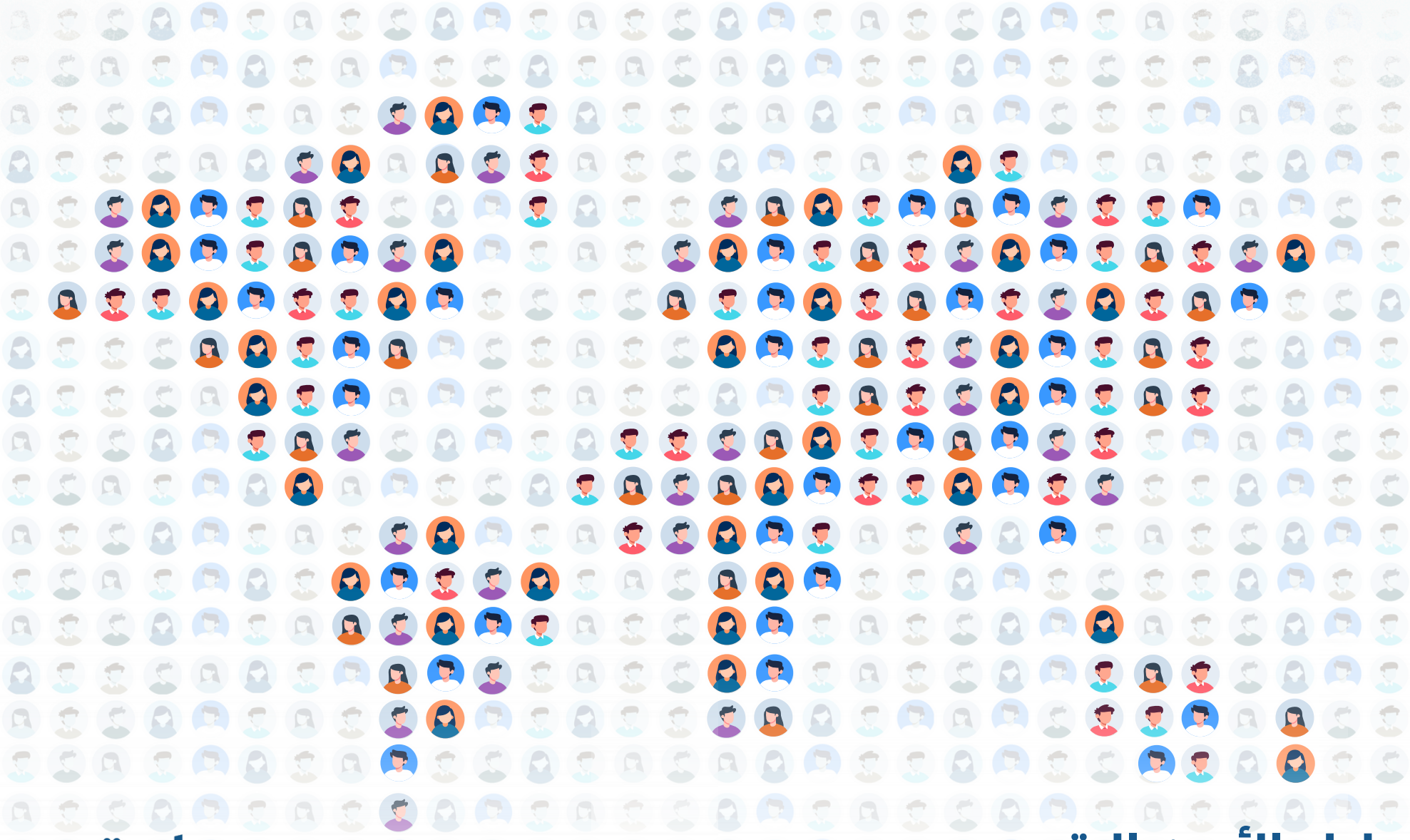


دليل الأمن الرقمي

خارطة الطريق للحماية عبر الإنترنت

مهارات
Maharat

دليل الأمن الرقمي

خارطة الطريق للحماية عبر الإنترنت

تم إعداد هذا الدليل من قبل مؤسسة مهارات، بدعم من هيئة الأمم المتحدة للمرأة والسفارة الفرنسية في بيروت.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

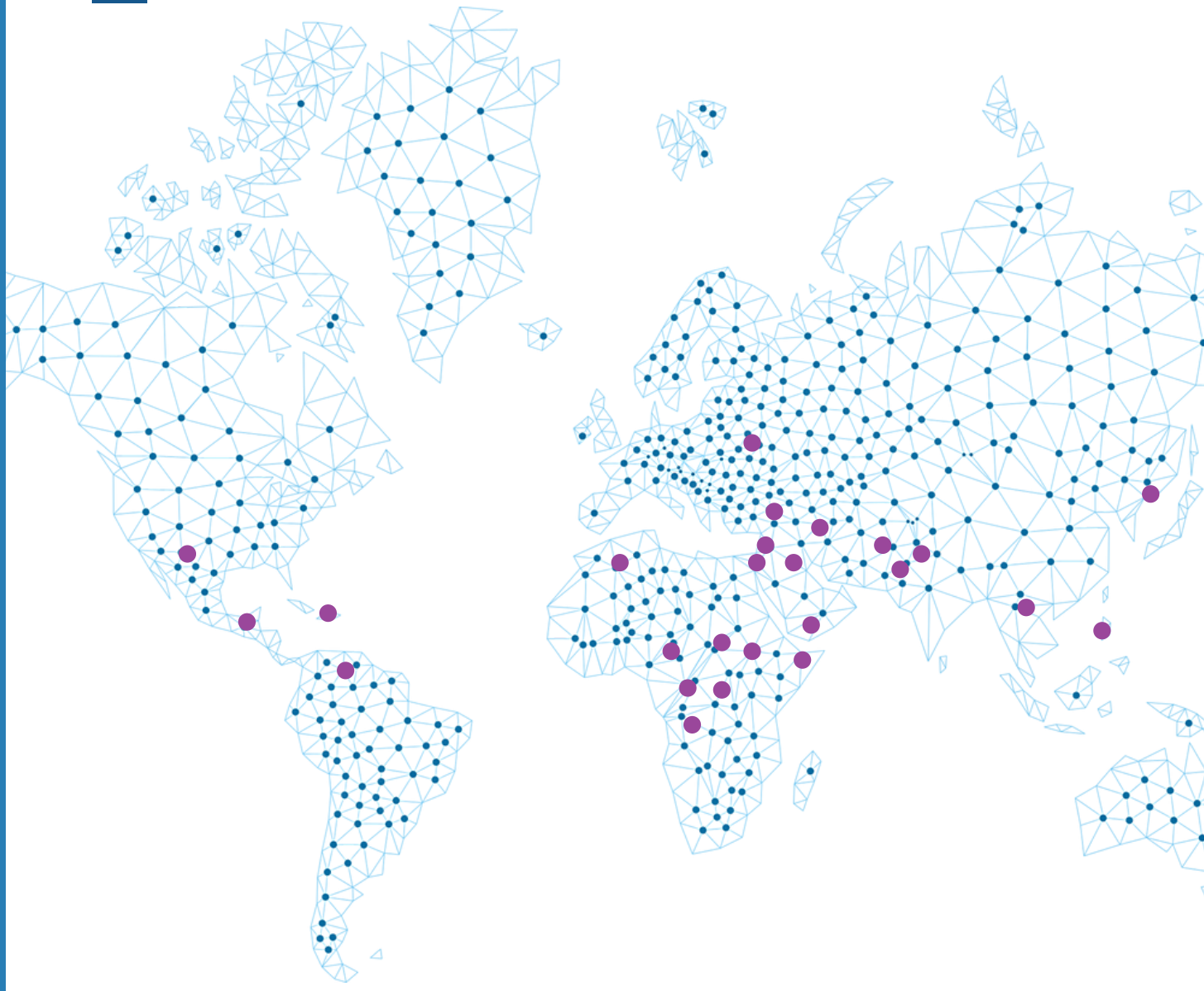
مهارات
Maharat

UN WOMEN

الجزء

فهم التهديدات السيبرانية :

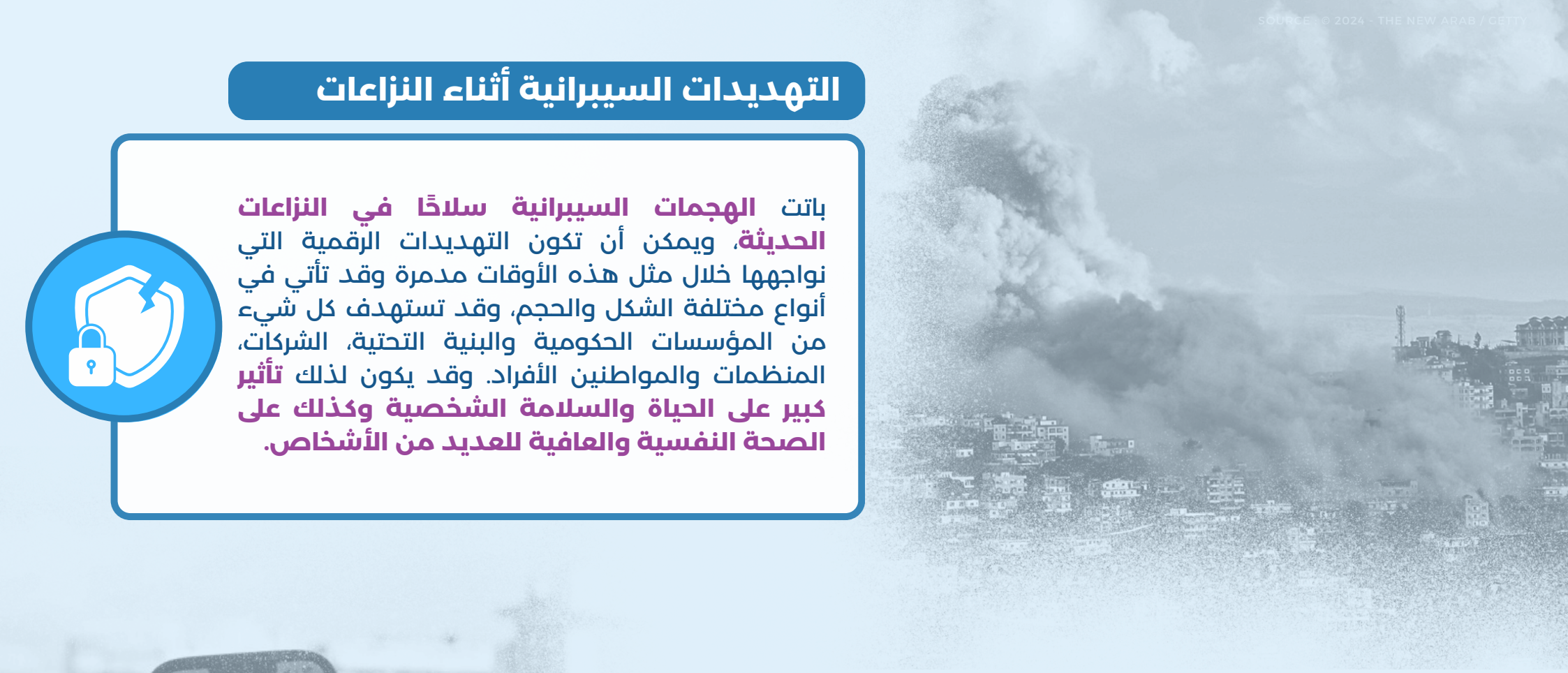
نظرة عامة على التهديدات السيبرانية الشائعة خلال **النزاعات** (مثل الاختراق، والتصيد، والمراقبة الإلكترونية).



إعداد:
خبير في الأمن الرقمي بهاء نصر

التهديدات السيبرانية أثناء النزاعات

باتت **الهجمات السيبرانية سلاحًا في النزاعات الحديثة**، ويمكن أن تكون التهديدات الرقمية التي نواجهها خلال مثل هذه الأوقات مدمرة وقد تأتي في أنواع مختلفة الشكل والحجم، وقد تستهدف كل شيء من المؤسسات الحكومية والبنية التحتية، الشركات، المنظمات والمواطنين الأفراد. وقد يكون لذلك **تأثير كبير على الحياة والسلامة الشخصية وكذلك على الصحة النفسية والعافية للعديد من الأشخاص.**



SOURCE : © 2024 - THE NEW ARAB / GETTY

تشمل التهديدات السيبرانية الأكثر شيوعًا **الاختراقات والتصيد الإلكتروني والمراقبة.** يمكن استخدام هذه التقنيات من قبل جهات ترعاها الدول، أو مجموعات من مجرمي الإنترنت (الهاكرز)، أو الأفراد ذوي النوايا الخبيثة. لكل تهديد ميزاته الخاصة، لكن جميعها تهدف إلى استغلال نقاط الضعف في الأنظمة الرقمية وسلوك البشر.

SOURCE : © 2024 - JOSEPH EID/AFP

الاختراق: اختراق الخطوط الأمامية الرقمية

الاختراق هو احد التهديدات السيبرانية الأكثر شهرة. وفي سياق الحرب السيبرانية، يتضمن الاختراق **الوصول غير المصرح به** إلى أنظمة الكمبيوتر أو الشبكات، وغالبًا ما يكون ذلك لسرقة البيانات أو التلاعب بها أو تدميرها. **تختلف الأهداف** الكامنة وراء عمليات الاختراق بشكل كبير، **بدءًا من التجسس والتخريب إلى المكاسب المالية أو الحرب النفسية.**

تشويه مواقع الكترونية Defacement

يتضمن تشويه الموقع الالكتروني **سيطرة المقرصنين على الموقع** وتغيير مظهره أو محتواه، غالبًا **لنشر الدعاية أو المعلومات الخاطئة**، ويُستخدم هذا التكتيك لتقويض الثقة في حكومة أو منظمة ما، وإثارة الارتباك، أو الاستهزاء بالمعارضة.

اختراق البيانات

قد يستهدف القراصنة قواعد البيانات التي تحتوي على معلومات حساسة، مثل البيانات الشخصية (الأسماء، العناوين، أرقام الهواتف...) والخطط العسكرية، أو الاستراتيجيات الحكومية. ومن خلال الوصول إلى قواعد بيانات مثل هذه، يمكن للمهاجمين استهداف مجموعات محددة، ابتزاز الأفراد، بيع البيانات إلى كيانات معادية، وتسريب المعلومات. ويمكن لمثل هذه الهجمات أن تُسبب حالة من الذعر على نطاق واسع.

هجمات برامج الفدية (Ransomware)

تقوم برامج الفدية بتشفير ملفات الضحية، والمطالبة بدفع فدية (عادةً بالعملة المشفرة) مقابل مفتاح فك التشفير. ويمكن أن تستهدف برامج الفدية القطاعين العام والخاص، مؤسسات او افراد، ما يمكن ان يؤدي الى شلّ الخدمات الأساسية مثل المستشفيات وشبكات الاتصالات.

هجمات الحرمان من الخدمة (DoS)

تقوم هذه الهجمات بإغراق الشبكات أو المواقع الإلكترونية بحركة مرور مفرطة، مما يؤدي إلى استنفاد مواردها وجعلها غير متاحة للمستخدمين.

يمكن أن يكون تأثير الاختراق في النزاعات مدمرًا.

حيث يمكن لحملة اختراق منسقة جيدًا أن تؤدي إلى شلّ اقتصاد بأكمله، نشر الخوف بين المواطنين، واضعاف قدرة الدولة على الاستجابة بفعالية للصراع العسكري.

التصيد: استغلال نقاط الضعف البشرية

التصيد هو شكل من أشكال الهجوم السيبراني الذي يستخدم الهندسة الاجتماعية **لخداع الأفراد للكشف عن معلومات حساسة.** يمكن أن تكون هجمات التصيد معقدة، وقد يحاول المهاجمون الاستفادة من التوتر المتزايد والارتباك والخوف الذي يرافق الأزمات. ويركز التصيد على **التلاعب بالسلوك البشري لتحقيق أهدافه.**

كيف يعمل التصيد

تتضمن هجمات التصيد عادةً إرسال **رسائل بريد إلكتروني احتيالية، او رسائل عبر وسائل التواصل الاجتماعي، أو مواقع الكترونية تبدو مشروعة** ولكنها مصممة لخداع المستخدمين واستدراجهم لتقديم معلومات شخصية، مثل بيانات تسجيل الدخول أو التفاصيل المالية أو غيرها من البيانات الحساسة.

غالبًا ما **ينتحل المهاجمون صفة مؤسسات موثوقة**، مثل البنوك، أو شركات التواصل الاجتماعي، أو الوكالات الحكومية، أو أصحاب العمل، لزيادة احتمالية النجاح.

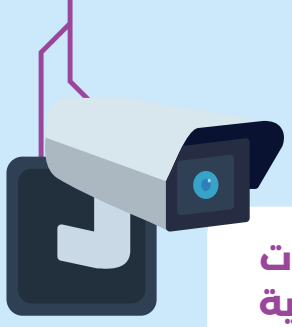
هجمات التصيّد الاحتيالي (Spear Phishing): هو شكل من أشكال التصيد الموجه بدقة حيث يقوم المهاجمون باستهداف اشخاص او مؤسسات محددين ويقومون بتوجيه هجومهم وبتخصيص رسائلهم لهؤلاء الأفراد أو المؤسسات. تُعدّ حملات التصيّد الاحتيالي أمرًا شائعًا أثناء النزاعات، حيث قد يستهدف المهاجمون شخصيات سياسية أو صحفيين أو عسكريين للوصول إلى معلومات مهمة وحساسة. على سبيل المثال، قد تقوم الجهات المخترقة التي ترعاها الدولة بصياغة رسائل بريد إلكتروني تحاكي الاتصالات الحكومية الرسمية، مما يستدرج المستهدفون إلى مشاركة البيانات السرية.

عادةً ما تستغل هجمات **التصيد الفوضى وعدم اليقين الذي يحيط بالوضع أثناء الحرب.**

EXAMPLE

على سبيل المثال، قد يتظاهر المهاجمون **بأنهم منظمات إنسانية تطلب التبرعات أو كوكالات حكومية تقدم معلومات عاجلة** تتعلق بالسلامة او عدد واسماء الجرحى والوفيات.

غالبًا ما تتضمن هذه الرسائل مرفقات ضارة أو توجه المستخدمين إلى مواقع إلكترونية مزيفة مصممة لجمع بيانات تسجيل الدخول أو لتحميل وتثبيت برامج ضارة على أجهزتهم.

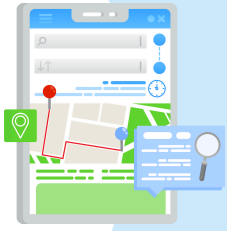


المراقبة الإلكترونية: المراقبة والسيطرة على ساحة المعركة الرقمية

تعد **المراقبة** تهديدًا رقميًا رئيسيًا، خاصة عندما يتعلق الأمر **بتتبع ومراقبة والتحكم في اتصالات وأنشطة الأفراد أو الجماعات.** يمكن استخدام تقنيات المراقبة من قبل **الحكومات أو القوات العسكرية أو الجهات المعادية** لجمع المعلومات الاستخباراتية والسيطرة على السكان وقمع المعارضة.

أ أنواع المراقبة:

المراقبة الإلكترونية: يشمل ذلك مراقبة قنوات الاتصال مثل البريد الإلكتروني، المكالمات الهاتفية، والرسائل النصية. قد تقوم الحكومات أو وكالات الاستخبارات أو القراصنة باعتراض الاتصالات لجمع معلومات عن تحركات الأفراد او المجموعات المشاركة في النزاع أوعن خططهم أو تحالفاتهم.



تتبع الموقع: يمكن استخدام الأجهزة المحمولة (الهاتف والساعة الذكية) وأنظمة تحديد الموقع (GPS) والمعلومات المتوفرة عبر وسائل التواصل الاجتماعي لتتبع الموقع الفعلي للأفراد. في مناطق النزاع، يُمكن استخدام هذه التقنيات لمراقبة تحركات العسكريين أو النشطاء السياسيين أو الصحافيين. ويمكن أن يسهل تتبع الموقع أيضًا الهجمات الموجهة، مثل ضربات المسيّرات أو الغارات.

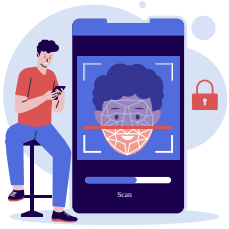
جمع البيانات الجماعية: قد تقوم الحكومات والمنظمات بجمع كميات هائلة من البيانات من المواطنين، مثل استخدام الإنترنت أو نشاط وسائل التواصل الاجتماعي أو عادات التصفح. ويمكن تحليل هذه البيانات لتحديد المعارضين، أو قمع المعارضة، أو تحييد التهديدات بشكل استباقي.

B المراقبة خلال الحرب

خلال النزاعات، يمكن أن تكون المراقبة **سيفًا ذو حدّين**، فمن جهة، يمكن استخدامها لحماية **الأمن القومي**، مما يُمكّن الحكومات من اكتشاف التهديدات والاستجابة لها بسرعة. كما يُمكن أيضًا استخدام المراقبة **لقمع المعارضة، وانتهاك حقوق الخصوصية، وقمع حرية التعبير**. في الأنظمة الاستبدادية، غالبًا ما يتم استخدام أدوات المراقبة **لقمع المتظاهرين، والناشطين، والصحافيين، مما يؤدي إلى اعتقالات جماعية وانتهاكات لحقوق الإنسان.**

إن ظهور أدوات المراقبة المتطورة، مثل:

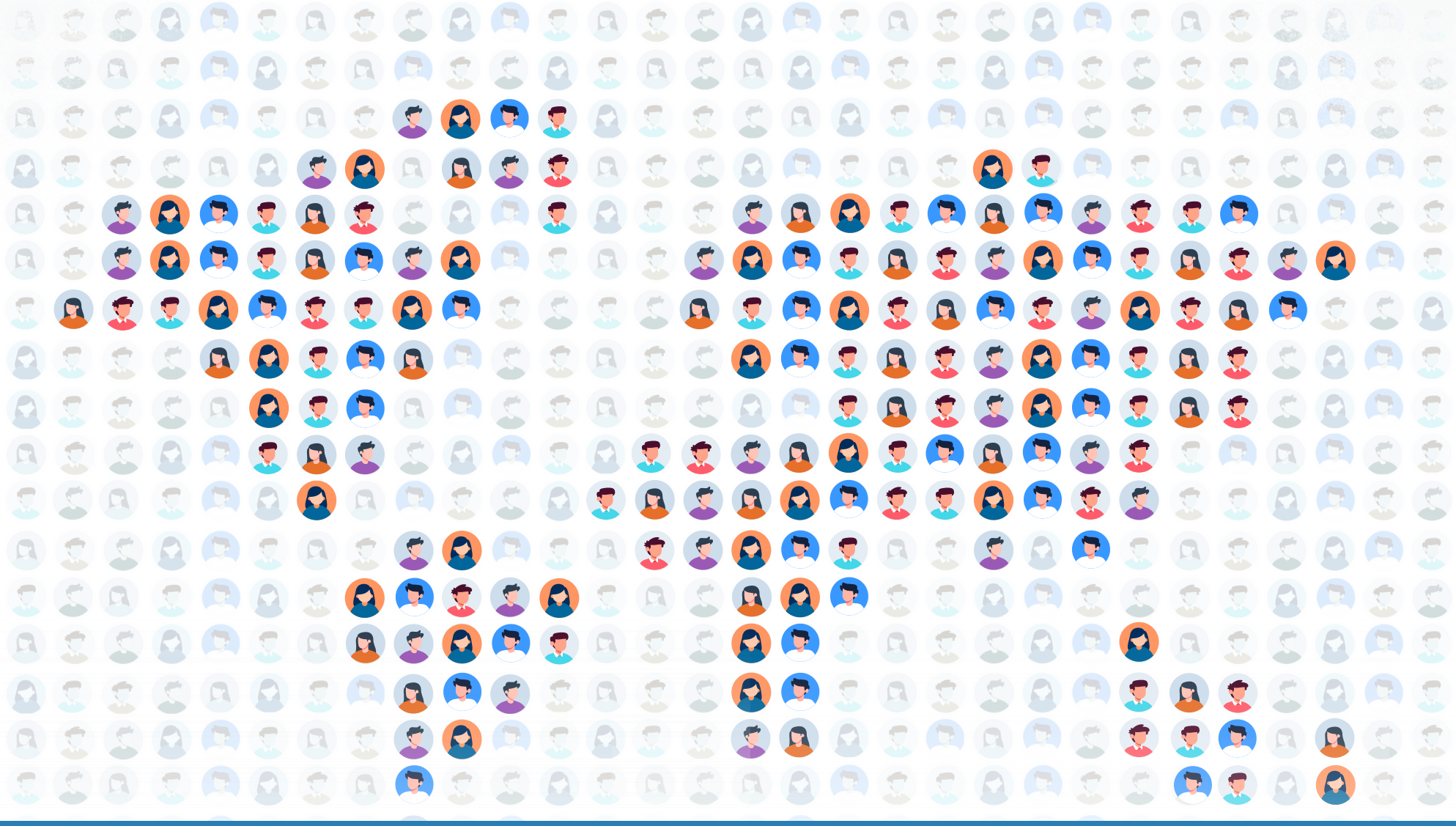
الذكاء الاصطناعي



تقنية التعرف على الوجه

كان له تأثير إضافي على الأمن والخصوصية، وفي سيناريوهات النزاع، يمكن استخدام هذه التقنيات من خلال كاميرات المراقبة والطائرات المسيرة وجميع وسائل التجسس **لمراقبة أعداد كبيرة من السكان** بدقة مثيرة للقلق، مما يطرح **تساؤلات أخلاقية حول استخدامها.**

الطريقة الوحيدة لحماية أنفسنا هي من خلال زيادة الوعي الرقمي وإعتماد ممارسات أمنية قوية، تمكننا من تقليل المخاطر التي تشكلها الهجمات السيبرانية مثل الاختراقات، التصيد والمراقبة. ولكن، مع استمرار تطور التهديدات الرقمية، يجب أيضًا تحديث استراتيجياتنا للتصدي لها في ظل مشهد الحرب السيبرانية المتغير باستمرار.



مؤسسة مهارات

العنوان:
جديدة، المتن
بيروت، لبنان

معلومات التواصل:
الموقع الإلكتروني: maharatfoundation.org
البريد الإلكتروني: info@maharatfoundation.org

مهارات
Maharat