سلسلة المذكرات الإرشادية

مسؤولية البيانات في العمل الإنساني

المذكرة الإرشادية حول تداعيات التهديدات السيبرانية للعاملين في المجال الإنساني

النقاط الرئيسية:

- تُعد التهديدات السيبرانية من أكثر القضايا إلحاحًا التي تواجه القطاع الإنساني اليوم. التحول الرقمي والاعتماد المتزايد على تكنولوجيا المعلومات والاتصالات وانتشار التهديدات السيبرانية تخلق مجموعة جديدة من المخاطر للوكالات الإنسانية والأشخاص الذين تخدمهم.
- تشمل التهديدات السيبرانية مجموعة متنوعة من الأنشطة والسلوكيات التي يمكن تمييزها بأنواع الجهات الفاعلة وراءها ودوافعها، وكذلك نوع التهديد.
- تشمل نقاط الضعف الشائعة في القطاع الإنساني عيوب البنية التحتية، وعدم كفاية الأمن السيبراني الأساسي ومحو الأمية الرقمية، والخطأ البشري، وغياب النهج المنسقة.
- يمكن أن تؤدي التهديدات السيبرانية إلى تقويض قدرة العاملين في المجال الإنساني على تقديم المساعدة وحماية السكان المتأثرين. تؤثر مباشرة على عدد من المجالات البرمجية الإنسانية الرئيسية، بما في ذلك الحماية، والوصول، والمساءلة تجاه السكان المتأثرين والتواصل مع المجتمعات.
- من أجل تحسين المرونة السيبرانية، يجب على المنظمات الاستثمار في الأمن السيبراني كقضية عبر تنظيمية، وتعزيز الاستعداد المؤسسي، وزيادة محو الأمية الرقمية للموظفين، وتحسين التنسيق والتعاون.

المقدمة

تعتمد المنظمات الإنسانية أكثر من أي وقت مضى على التقنيات الرقمية لمساعدة وحماية الناس في الأزمات.[1] تمكّن هذه التقنيات العاملين في المجال الإنساني من جمع البيانات لفهم احتياجات الأشخاص المتأثرين والاستجابة لها، وتوفر قنوات جديدة لتقديم المساعدات من خلال القرب الرقمي غير المسبوق.[2] ومع ذلك، فإن هذا التحول الرقمي المتزايد ليس بدون مخاطر - أبرزها هو تزايد خطر التهديدات السيبرانية.[3]

تُعد التهديدات السيبرانية واحدة من أكثر القضايا إلحاحًا التي تواجه القطاع الإنساني اليوم.[4] يخلق التحول الرقمي والاعتماد المتزايد على تكنولوجيا المعلومات والاتصالات (ICT) وانتشار التهديدات السيبرانية مجموعة جديدة من المخاطر للوكالات الإنسانية والأشخاص الذين يخدمونهم. تشمل بعض الأمثلة:

- في أبريل ٢٠٢٠، في بداية جائحة COVID-١٩، أبلغت منظمة ميرسي كور والمجتمع الدولي للصليب الأحمر والهلال الأحمر (IFRC) عن ارتفاع حاد في انتهاكات حماية البيانات،[5] ولاحظت منظمة الصحة العالمية (WHO) زيادة بمقدار خمسة أضعاف في عدد التهديدات السيبرانية ضد المنظمة.[6]

[1] NetHope (2022). **Humanitarians (and data) #NotATarget**.

[2] Massimo Marelli and Adrian Perrig (2020). **Hacking Humanitarians: Mapping The Cyber Environment And Threat Landscape**, International Committee of the Red Cross, 7 May.

[3] UNOCHA GHPF (2022). **Virtual Risk, Tangible Harm: The Humanitarian Implications of Cyber Threats**.

[4] World Economic Forum (2022). **The Global Risks Report 2022 17th Edition**. Geneva.

[5] Rebecca Root (2020). **COVID-19 Brings Wave of Cyberattacks Against NGOs**, Devex, 13 April.

[6] World Health Organization (2020). **WHO Reports Fivefold Increase in Cyberattacks, Urges Vigilance**, 23 April.

- Iفي مايو ٢٠٢١، تمكن القراصنة من الوصول إلى حساب التسويق عبر البريد الإلكتروني للوكالة الأمريكية للتنمية الدولية (USAID)، وأرسلوا رسائل إلكترونية لأكثر من ١٥٠ منظمة في محاولة واضحة لاختراقها.[٧]
- في فبراير ٢٠٢٢، تم اكتشاف عملية سيبرانية مستهدفة بشدة ضد خوادم اللجنة الدولية للصليب الأحمر (ICRC) مما أدى إلى اختراق بيانات حساسة لأكثر من ٥١٥،٠٠٠ فرد.[٨]

قد تسبب هذه الهجمات أضرارًا جسيمة. إنها تنتهك خصوصية الأشخاص الذين تم اختراق بياناتهم، وتعرض المعلومات الحساسة عنهم للخطر وتؤدي إلى تآكل الثقة في قدرات المنظمات الإنسانية.

استجابةً لهذه الهجمات، تشير عدد من المبادرات الجديدة إلى زيادة الاستثمار في هذا المجال. على سبيل المثال، تفكر اللجنة الدولية للصليب الأحمر (ICRC) في تطوير «رمز رقمي» وفتحت أيضًا وفدًا جديدًا للفضاء السيبراني في لوكسمبورغ. أنشأت NetHope مركز مشاركة وتحليل المعلومات الذي سيساعد في دعم احتياجات الأمن المعلوماتي للوكالات غير الربحية والمجتمعات الأكثر ضعفًا في العالم. ومع ذلك، يفتقر القطاع إلى نهج مشترك للتخفيف من المخاطر والتأثير المحتمل للتهديدات السيبرانية.

تهدف هذه المذكرة الإرشادية إلى المساعدة في بناء فهم مشترك ودعم العمل الاستراتيجي والجماعي داخل القطاع. توفر نظرة عامة على التهديدات السيبرانية ونقاط الضعف والتداعيات التي يواجهها العاملون في المجال الإنساني والأشخاص المتأثرون بالأزمات، وتقدم توصيات لزيادة المرونة السيبرانية داخل المنظمات وعبرها ومع شركائها.

التعريفات

الأمن السيبراني يشمل مزيجًا من الأدوات والسياسات والمفاهيم الأمنية وضمانات الأمان والإرشادات وطرق إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات والتأكيدات والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية وأصول المنظمة والمستخدمين ضد المخاطر الأمنية ذات الصلة في البيئة السيبرانية.

أمن المعلومات والبيانات يتضمن مجموعة من التدابير المادية والتكنولوجية والإجرائية التي تحمي سرية وسلامة وتوافر البيانات، وتمنع فقدانها أو تدميرها أو تعديلها أو اكتسابها أو الكشف عنها بشكل عرضي أو متعمد أو غير قانوني أو غير مصرح به بأي شكل من الأشكال.

التهديدات السيبرانية تشمل «الأنشطة التي تحدث على الأقل جزئيًا في المجال السيبراني، باستخدام و/أو استهداف تقنيات الاتصالات والمعلومات لتحقيق تأثير غير مصرح به من قبل المستخدم الشرعي للبيانات أو تكنولوجيا المعلومات والاتصالات و/أو له نية أو تأثير ضار على الضحية أو الضحايا».

المرونة السيبرانية تشير إلى قدرة المنظمة على تحديد التهديدات السيبرانية ومنعها واكتشافها، والاستجابة لها والتعافي منها.

التهديدات السيبرانية

لزيادة الأمن السيبراني داخل القطاع، يجب على المنظمات أولاً فهم التهديدات التي قد تواجهها في هذا المجال. تشمل التهديدات السيبرانية مجموعة واسعة من الأنشطة والسلوكيات التي يمكن تمييزها حسب أنواع الفاعلين وراءها ودوافعهم. تتراوح الفاعلون من دول قومية إلى منظمات إجرامية وأفراد خاصين أو مزيج منهم. يمكن أن توجه الانتماءات والأهداف الخاصة بالفاعلين كيفية تصرفهم بحدة، ومدى تعقيد الهجمات، والأساليب المستخدمة، ومن يتم استهدافه.

[7] Kelly Sheridan (2021). **US Seizes Attacker Domains Used in USAID Phishing Campaign**, DARKReading, 1 June; Adva Saldinger (2021). **USAID Hack is 'Wakeup Call' for Aid Industry on Cybersecurity**, Devex, 4 June.

[8] International Committee of the Red Cross (2022). **Cyber-Attack on ICRC: What We Know**, 16 February.

[9] ICRC (2022). **ICRC proposes digital red cross/crescent emblem to signal protection in cyberspace**, 3 November. Linked to this is the notion of the "sovereign cloud" – i.e., a cloud architecture in which data sovereignty can be respected and applied. See ICRC (2020). **Handbook on Data Protection in Humanitarian Action**.

[10] ICRC (2022). **The ICRC opens a new delegation for cyberspace in Luxembourg**, 17 November.

[11] NetHope (2022). **Digital Protection and Cybersecurity**.

يمكن أن تكون التهديدات السيبرانية مباشرة أو غير مباشرة، اعتمادًا على الهدف. التهديدات السيبرانية المباشرة، التي تستهدف المنظمات الإنسانية، زادت في السنوات الأخيرة. التهديدات السيبرانية غير المباشرة تستهدف البنية التحتية أو الخدمات التي يعتمد عليها الأشخاص المتأثرون بالأزمات الإنسانية أو المستجيبون لها للبقاء على قيد الحياة وتقديم المساعدات.

يمكن أيضًا تصنيف التهديدات السيبرانية وفقًا لنوعها أو طريقتها. تشمل هذه الهجمات هجمات حجب الخدمة (DoS) وهجمات حجب الخدمة الموزعة (DDoS)،[12] والبرمجيات الخبيثة (Malware)،[13] وبرمجيات الفدية (Ransomware)،[14] من بين أمور أخرى.

الأمثلة التالية توضح كيف قد تبدو التهديدات السيبرانية في الممارسة العملية:

- الحرب السيبرانية تشير إلى «العمليات ضد جهاز كمبيوتر أو نظام كمبيوتر أو شبكة أو جهاز متصل آخر، من خلال تدفق البيانات، عندما تُستخدم كوسائل أو أساليب حرب في سياق نزاع مسلح».[15] في أوكرانيا، قوضت الهجمات السيبرانية توزيع الأدوية والطعام وإمدادات الإغاثة منذ فبراير ٢٠٢٢.[16] تراوحت تأثيراتها من منع الوصول إلى الخدمات الأساسية إلى سرقة البيانات ونشر المعلومات المضللة.

- المعلومات الخاطئة والمضللة وخطاب الكراهية (MDH) تشير إلى النشر المنظم (المتعمد أو غير المتعمد) للمعلومات الخاطئة عبر وسائل تكنولوجيا المعلومات والاتصالات التي تسيء إلى الفاعلين السياسيين أو العسكريين أو المجتمع المدني، أو تنشر أو تحرض أو تروج أو تبرر الكراهية والعنف على أساس التعصب. في ميانمار، تم ربط حملة MDH بلغة مهينة ومجردة من الإنسانية ضد أقلية الروهينجا المسلمة بارتكاب انتهاكات جسيمة لحقوق الإنسان.[17]

- الجريمة السيبرانية تشير إلى الجرائم التي تعتمد على الوسائل السيبرانية (التي ترتكب من خلال تكنولوجيا المعلومات والاتصالات) أو تعتمد على تكنولوجيا المعلومات والاتصالات (التي لا يمكن تحقيقها إلا بفضل تكنولوجيا المعلومات والاتصالات).

- التخريب السيبراني يشير إلى الأنشطة التي تهدف إلى تعطيل أو تدمير التشغيل الموثوق والخالي من الأخطاء لتكنولوجيا المعلومات والاتصالات. إذا تم تنفيذ عمل تخريبي من قبل مرتكبين بدوافع إرهابية، يشار إليه بالإرهاب السيبراني.

نقاط الضعف الشائعة في القطاع الإنساني

يجب على العاملين في المجال الإنساني التحقيق في وفهم نقاط الضعف المحتملة التي قد تؤثر على مرونتهم السيبرانية وتجعلهم أكثر عرضة لأن يصبحوا ضحايا للتهديدات السيبرانية.[18] تشمل هذه النقاط عيوب البنية التحتية، وعدم كفاية الأمن السيبراني الأساسي ومحو الأمية الرقمية، والخطأ البشري، وغياب النهج المنسق.

١. عيوب البنية التحتية

التهديدات السيبرانية عادة ما ترتبط بالعمليات التقنية المتقدمة التي تستهدف نقاط الضعف في البنية التحتية للمعلومات. تشمل نقاط الضعف الشائعة من هذا النوع في القطاع الإنساني:

- **أنظمة قديمة:** برامج أو أجهزة حوسبة قديمة غير قادرة على مقاومة أشكال الهجوم الحديثة، وتمثل خطرًا على التطبيقات والبيانات الأخرى التي قد تشارك في نفس البنية التحتية.[19]

[12] Denial-of-service (DoS) and Distributed denial-of-service (DDoS) attacks flood a system's resources, overwhelming them and preventing responses to service requests, which reduces the system's ability to perform. (**Source: IBM**).

[13] Malware is malicious software that can render infected systems inoperable. Most malware variants destroy data by deleting or wiping files critical to the operating system's ability to run. (**Source: IBM**).

[14] Ransomware is sophisticated malware that takes advantage of system weaknesses, using strong encryption to hold data or system functionality hostage. Cybercriminals use ransomware to demand payment in exchange for releasing the system. A recent development with ransomware is the add-on of extortion tactics. (**Source: IBM**).

[15] International Committee of the Red Cross (November 2019). **International Humanitarian Law and the Challenges of Contemporary Armed Conflicts: Recommitting to Protection in Armed Conflict on the 70th Anniversary of the Geneva Conventions**.

[16] European Parliamentary Research Service (June 2022). **Russia's war on Ukraine: Timeline of cyber-attacks**.

[17] UN. **Hate speech and real harm**; Human Rights Council (2018). **Report of the Independent International Fact-finding Mission on Myanmar** (A/HRC/39/64).

[18] UN (2021). **Cybersecurity in the United Nations system organizations: Report of the Joint Inspection Unit**.

[19] UN (2021). **Cybersecurity in the United Nations system organizations: Report of the Joint Inspection Unit**.

- **التكوين الافتراضي أو غير الصحيح:** الأنظمة التي تخرج من العلبة، أي مع كلمات مرور افتراضية أو بسيطة وتكوينات مفرطة في السماح، تكون أسهل على المهاجمين لاختراقها.[٢٠]

- **عدم وجود تشفير:** في غياب التشفير، يمكن للمهاجمين استخدام برامج لاكتشاف أسماء المستخدمين وكلمات المرور. يعني نقص التشفير أن المهاجم يمكنه الوصول إلى البيانات على الأجهزة المخترقة. البيانات التي يتم نقلها عبر قنوات غير مشفرة تكون أيضًا عرضة للوصول غير المصرح به.

- **بنية تحتية تابعة لجهات خارجية:** يمكن للمهاجمين التسلل إلى أنظمة تكنولوجيا المعلومات والاتصالات من خلال شريك خارجي أو بائع عن طريق استغلال نقاط الضعف المختلفة. قد يتمكن المهاجمون أيضًا من الوصول إلى البيانات المخزنة من قبل المزودين. يمكن أن يؤدي تعطيل البنية التحتية الحيوية من خلال العمليات السيبرانية إلى إيقاف الخدمات الأساسية، مما يمكن أن تكون له عواقب وخيمة على الأشخاص المحتاجين ويعطل العمليات الإنسانية. كما يعتبر التعلق بالبائع بسبب عدم توافق المنتجات، أو انخفاض مستويات التوافقية أو قابلية النقل، أو قلة البدائل في السوق مصدر قلق كبير أيضًاs

٢. عدم كفاية الأمن السيبراني الأساسي ومحو الأمية الرقمية

تظل الجاهزية السيبرانية، الاستعداد التنظيمي، ومحو الأمية الرقمية محدودة في القطاع الإنساني.[٢٤] عدم كفاية محو الأمية البياناتية ونقص الممارسات والأدوات المتسقة لضمان الأمن السيبراني منتشرة بين المنظمات الإنسانية. لا يزال يُنظر إلى الأمن السيبراني على أنه قضية تقنية بشكل رئيسي، مما يؤدي إلى قلة المشاركة من الموظفين أو القيادة لزيادة الوعي بالتهديدات وتزويد الأشخاص في جميع أنحاء المنظمات بالمهارات والأدوات اللازمة لتقليل المخاطر. يترجم هذا النقص في المشاركة والتركيز أيضًا إلى نقص في الموارد والتمويل للأمن السيبراني.[٢٥] حتى عندما يقوم العاملون في المجال الإنساني برقمنة عملياتهم، تظل الفجوات قائمة بين الاستثمار في الواجهة الأمامية للتكنولوجيا (بنائها، نشرها، وإغلاق المشروع)، والواجهة الخلفية (الحفاظ على الخدمات والحفاظ على المعلومات آمنة ومحمية على مر الزمن).[٢٦]

٣. الخطأ البشري

في السنوات الأخيرة، كان هناك تحول ملحوظ من مهاجمة المتسللين للخوادم والشبكات والأجهزة إلى «اختراق الأشخاص».[٢٧] الآن، ٩٥٪ من انتهاكات الأمن السيبراني ناتجة عن خطأ بشري.[٢٨] تقنيات الهندسة الاجتماعية (مثل التصيد الاحتيالي، والانتحال) التي تهدف إلى التلاعب بالأفراد للكشف عن معلومات حساسة هي الوسيلة الأكثر شيوعًا لاستغلال هذا الضعف. معظم هذه التقنيات مصممة للوصول إلى عدد كبير من المستخدمين في وقت واحد، مما يزيد من احتمالية حدوث اختراق. يمكن أن تمر هذه التطفلات دون أن تُكتشف لفترات طويلة، مما يمنح المهاجمين الوصول إلى بنية الأمان الداخلية والمعلومات السرية، مما يوفر فرصًا إضافية للهجوم.

الأخطاء البشرية التي تزيد من التعرض للتهديدات السيبرانية قد تشمل:

- إساءة استخدام عرضية من قبل المستخدمين الذين لديهم وصول معتمد وشرعي إلى أنظمة الكمبيوتر;
- الاستخدام غير المصرح به من قبل المهاجمين المدعومين بمستخدم تم اختراقه;
- تجاهل الموظفين للسياسات والإجراءات الأمنية;
- أخطاء في تكوين أو تشغيل الأنظمة;

[20] Checkpoint (2020). **Critical Infrastructure and SCADA/ICS Cybersecurity Vulnerabilities and Threats**.

[21] Massimo Marelli (2021). **The SolarWinds hack: lessons for humanitarians**. International Committee of the Red Cross, 18 May.

[٢٢] بين يونيو ٢٠٢٠ وأبريل ٢٠٢٢، قام معهد CyberPeace بتحليل بيانات حول ٣٧٩ هجومًا سيبرانيًا ضد قطاع الرعاية الصحية في ٣٦ دولة، مع متوسط اختراق يبلغ ١٦٥،٠٠٠ سجل لكل حادثة – وهذا مجرد جزء بسيط من مدى المشكلة الكامل. في عام ٢٠١٥، تركت عملية برامج خبيثة متطورة تستهدف شبكة الكهرباء في أوكرانيا ٢٣٠،٠٠٠ مقيم بدون كهرباء لمدة تصل إلى ست ساعات في منتصف الشتاء، في أول اختراق مؤكد لإسقاط شبكة طاقة. أفاد مزود المياه الوطني في إسرائيل، مكوروت، في عام ٢٠٢١ أن شبكات المياه الخاصة به تتعرض لـ»عدة مئات من آلاف محاولات القرصنة» سنويًا. في فبراير ٢٠٢٢، أفادت شركة الاتصالات الفضائية فياسات عن هجوم سيبراني مشتبه به أدى إلى انقطاع جزئي لخدمات النطاق العريض السكنية في أوكرانيا ودول أوروبية أخرى.

[23] Massimo Marelli (2021). **The SolarWinds hack: lessons for humanitarians**. International Committee of the Red Cross, 18 May.

[24] UN GHPF (2021). **The Humanitarian Implications of Cyber Threats**.

[25] WEF (2022). **Why the humanitarian sector needs to make cybersecurity a priority**, 17 January.

[26] Catherine Cheney (2022). **Delivering digital aid when the internet becomes a weapon of war**, DevEx, 28 January.

[27] UN (2021). Cybersecurity in the United Nations system organizations: Report of the Joint Inspection Unit.

[28] WEF (2020). After reading, writing and arithmetic, the 4th 'r' of literacy is cyber-risk.

٤. غياب النهج المنسق

هناك فجوة حادة في التنسيق بشأن القضايا المتعلقة بالسيبرانية في القطاع الإنساني. هذه الفجوة موجودة داخل وبين المنظمات. قلة من المنظمات لديها فرق مخصصة للأمن السيبراني أو مكلفة بالكشف عن المخاطر السيبرانية وتقييمها والتخفيف منها. لا توجد جهة واحدة مكلفة رسميًا بتنسيق نهج موحد للأمن السيبراني في القطاع، على الرغم من وجود مبادرات مثل تلك الموصوفة أعلاه، وتطوير الموارد والإرادة السياسية الظاهرة.[٢٩]

يعني نقص التنسيق أن المنظمات تفتقر إلى الرؤية حول الهجمات التي يتعرض لها نظراؤها، أو أنها غير قادرة أو لا توجد لديها سياسات لمشاركة المعلومات حول التهديدات السيبرانية التي تعرضت لها أو الدروس المستفادة بشكل متسق، ولا تستثمر في نهج جماعي لتقليل نقاط الضعف والتخفيف من المخاطر.[٣٠]

الآثار الإنسانية للتهديدات السيبرانية

الآثار الإنسانية للتهديدات السيبرانية كبيرة. يمكن أن تقوض القدرة على تقديم المساعدة والحماية، وكذلك تفاقم الاحتياجات الإنسانية من خلال تعطيل الخدمات الأساسية للبقاء على قيد الحياة. يمكن أن تؤدي التهديدات السيبرانية إلى المراقبة، والتمييز، والاضطهاد وعواقب ضارة أخرى للسكان المتأثرين، وتفاقم انعدام الأمن لدى الفئات والأفراد الضعفاء بالفعل، وتآكل الثقة وتقويض تقديم المساعدة الإنسانية على أساس المبادئ.[٣١]

يعني تقديم المساعدة المبدئية أن تكون الخدمات والمساعدات الإنسانية متوافقة مع مبادئ الإنسانية، والحياد، وعدم التحيز، والاستقلالية.[٣٢] للعمل بالحياد في المجال الرقمي، يجب على العاملين في المجال الإنساني «ضمان أن البيانات والأنظمة التي يستخدمونها لا توفر أي ميزة عسكرية أو تشغيلية تكتيكية للأطراف المشاركة في الأعمال العدائية».[٣٣] قد يتعارض مبدأ الاستقلالية الإنسانية مع الاعتماد على العمل الإنساني المدعوم بتكنولوجيا المعلومات والاتصالات على البنية التحتية المملوكة والمدارة من قبل شركات خاصة مرتبطة بدول مختلفة. المبدأ الشامل «عدم الإضرار» يلزم جميع العاملين في المجال الإنساني بتجنب تعريض الناس لمخاطر إضافية من خلال العمل الإنساني، مما يتطلب منهم اتخاذ خطوة للوراء من التدخل للنظر في السياق الأوسع وتخفيف الآثار السلبية المحتملة.[٣٤]

التهديدات السيبرانية تؤثر بشكل مباشر على عدد من المجالات الإنسانية الرئيسية، مثل:

- **الحماية**
- **الوصول**
- **المساءلة تجاه المتأثرين (AAP)**
- **التواصل مع المجتمعات (CwC)**

بما أن الأدوات التقنية لإدارة البيانات في هذه المجالات المختلفة قد تطورت بشكل أسرع من الأدوات السياسة التي تحكم استخدامها، يجب على المنظمات توخي الحذر عند تصميم ونشر التقنيات الرقمية. تقدم الأقسام أدناه اعتبارات لمساعدة المنظمات على فهم ومعالجة الآثار الإنسانية للتهديدات السيبرانية في هذه المجالات.

١. الحماية

بالنسبة للمنظمات الإنسانية، تعني الحماية الدعوة ودعم الإجراءات التي تهدف إلى تقليل ومنع تعرض الناس للمخاطر وضمان احترام حقوق الأفراد من قبل المسؤولين. يجب على العاملين في المجال الإنساني النظر في كيفية تأثير التهديدات السيبرانية ونقاط الضعف ذات الصلة على مسؤولياتهم في الحماية، وما هي تأثيرات التكنولوجيا على توزيع الموارد، وكيفية إعادة تعريف العلاقات بناءً على الاعتماد على البنية التحتية السيبرانية والبائعين.[٣٦]

[29] UN (2021). Cybersecurity in the United Nations system organizations: Report of the Joint Inspection Unit.

[٣٠] مثال بارز على التواصل حول الانتهاكات السيبرانية كان رد فعل اللجنة الدولية للصليب الأحمر (ICRC) على الهجوم السيبراني في عام ٢٠٢٢، حيث تواصلت المنظمة بطريقة شفافة وفي الوقت المناسب، وأبقت الشركاء والمستفيدين على اطلاع بأقصى قدر ممكن من المعلومات.

[31] UNOCHA GHPF (2022). Virtual Risk, Tangible Harm: The Humanitarian Implications of Cyber Threats.

[32] UNOCHA on Message: Humanitarian Principles.

[33] Brittany Card. (2015). Applying Humanitarian Principles To Current Uses Of Information Communication Technologies: Gaps In Doctrine And Challenges To Practice.Signal Program on Human Security and Technology, Harvard Humanitarian Initiative.

[34] ALNAP (2018). **Incorporating the principle of "Do No Harm": How to take action without causing harm - Reflections on a review of Humanity & Inclusion's practices**.

[35] UNOCHA, **Themes: Protection**.

المعلومات حول موقع الأشخاص الضعفاء، وكذلك البيانات التي تسمح بإعادة تحديد هوية ضحايا العنف القائم على النوع الاجتماعي هي مثالان على القضايا المحددة للحماية التي قد تتفاقم باستخدام تكنولوجيا المعلومات والاتصالات حيث يمكن أن تجعل هذه المعلومات أكثر سهولة للجهات الفاعلة الخبيثة.[٣٧] قلق آخر يتعلق بحماية البيانات الإنسانية. على سبيل المثال، أصبح استخدام وسائل التواصل الاجتماعي أكثر شيوعًا في تقديم الخدمات، لكن هذا يجلب معه عددًا من مخاطر حماية البيانات مثل التصنيف الشخصي.[٣٨]

٢. الوصول

يشير الوصول الإنساني إلى قدرة العاملين في المجال الإنساني على الوصول إلى السكان المحتاجين وقدرة السكان المتأثرين على الوصول إلى المساعدة والخدمات.[٣٩]

يمكن أن تساعد تكنولوجيا المعلومات والاتصالات في زيادة وتبسيط وصول المستفيدين إلى الخدمات الإنسانية مثل المساعدة النقدية، والخدمات الإحالة، أو الرعاية الصحية. ومع ذلك، يمكن أن يؤدي الاعتماد المتزايد من العاملين في المجال الإنساني على التقنيات الرقمية والاعتماد المتعلق بالبنية التحتية والخدمات الخارجية والداخلية إلى تحديات جديدة.
يمكن أن تعوق الوصول إلى الخدمات نقاط الضعف الكامنة في القطاعات التي تعتمد عليها المنظمات والمستفيدون (مثل الرعاية الصحية، والخدمات اللوجستية، والبنوك، وغيرها).[٤٠] استمرارية الخدمات في الفضاء الرقمي ليست دائمًا مضمونة - يمكن أن تؤدي انقطاعات الإنترنت وفشل الشبكات إلى اضطرابات كبيرة في تقديم الخدمات الأساسية.[٤١] في كينيا، أدى فشل الشبكة إلى «تأخيرات عرضية، وتعطيل أو إلغاء توزيع الغذاء في المخيمات، مما ساهم في حدوث طوابير طويلة وتحديات في السيطرة على الحشود».[٤٢]

٣. المساءلة تجاه المتأثرين والتواصل مع المجتمعات

تشير المساءلة تجاه المتأثرين إلى التزام نشط باستخدام السلطة بشكل مسؤول من خلال أخذ الحساب، وتقديم الحساب، والمساءلة من قبل الأشخاص الذين تسعى المنظمات الإنسانية إلى مساعدتهم.[٤٣] يهدف التواصل مع المجتمعات إلى تلبية احتياجات المعلومات والاتصالات للأشخاص المتأثرين بالأزمات.[٤٤]

ضمان الوصول في الوقت المناسب والمستخدم الموثوق للمعلومات هو أمر بالغ الأهمية لـ AAP وCwC. بشكل متزايد، يقدم العاملون في المجال الإنساني هذه المعلومات جزئيًا على الأقل من خلال القنوات الرقمية، إما لتكملة الخدمات المباشرة أو عندما لا تكون القرب الجسدي من المجتمعات ممكنًا. يعتمد هذا الاعتماد على الخدمات الرقمية على أن العمليات السيبرانية يمكن أن يكون لها تداعيات إنسانية خطيرة.

تهديد معين يتعلق بـ AAP وCwC هو المعلومات المضللة، والمعلومات الخاطئة، وخطاب الكراهية، الذي أصبح أكثر انتشارًا مع الاستخدام المتزايد لتكنولوجيا المعلومات والاتصالات.[٤٥] يمكن أن تعرض MDH المجتمعات المتأثرة والعاملين في المجال الإنساني للخطر من خلال زعزعة استقرار البيئات الهشة، وزيادة الضعف، والتأثير على سمعة المنظمات الإنسانية.[٤٦]

[36] Sandvik, Jacobsen and McDonald (2017). **Do no harm: A taxonomy of the challenges of humanitarian experimentation**, International Review of the Red Cross (2017), 99 (1), 319–344.

[37] ICRC (2020). **Handbook on Data Protection in Humanitarian Action**.

[38] 'Incidents reported include social engineering attacks such as phishing employed via messaging apps (targeting of Tibetan diaspora via Whatsapp) profiling and targeting of the Tibetan Diaspora through WhatsApp); commercially available spyware used against political dissidents outside of country of origin and for targeting asylum seekers; as well as new vulnerabilities that are being regularly discovered and patched in major messaging services (eg. Whatsapp)' see UNHCR (2021). **Using Social Media in Community Based Protection: A Guide**.

[39] OCHA on Message (April 2017). **Humanitarian Access**.

[40] Fore more on these vulnerabilities and how they are exacerbated by emerging cyber threats, see: UNOCHA GHPF (2022). **Virtual Risk, Tangible Harm: The Humanitarian Implications of Cyber Threats**.

[41] KeepItOn (2019). **The State of Internet Shutdowns around the world. The 2018 #KeepItOn Report**, Access Now for the #KeepItOn coalition.

[42] World Food Programme (WFP)/UNHCR (2014). **Joint Assessment Mission: Kenya Refugee Operation**, Dadaab (23–25 June 2014) and Kakuma (30 June–1 July 2014) Refugee Camps, 2014.

[43] IASC: **Accountability to Affected Populations (AAP) : A brief overview**.

[44] OCHA (2014). **OCHA on Message: Communications with Communities**.

[45] CDAC (2021). **Digital Communication and Accountability: Insights from a year of discussions with CDAC Network**.

[46] International Review of the Red Cross (2020). **Q&A: Humanitarian operations, the spread of harmful information and data protection**. IRRC 102 (913), 27–41.

التوصيات

يجب على المنظمات الإنسانية النظر في التوصيات التالية لتحسين المرونة السيبرانية.

الاستثمار في الأمن السيبراني كقضية تنظيمية شاملة من خلال:

- دمج الأمن السيبراني في الأطر والاستراتيجيات التنظيمية الأوسع، بما في ذلك الضمانات القانونية والتقنية والتشغيلية ذات الصلة.
- تعزيز موقف نشط من الموظفين على جميع المستويات من خلال برامج التوعية وعرض أسلوب قيادة منخرط في مسائل الأمن السيبراني بشكل عام.[٤٧]
- تخصيص تمويل طويل الأجل ومرن للأمن السيبراني ومسؤولية البيانات كعنصر متكامل من برمجة العمل الإنساني.
- الدعوة إلى زيادة الاستثمار في تشغيل التقنيات الرقمية بمسؤولية لتقليل نقاط الضعف ذات الصلة.

تعزيز الاستعداد المؤسسي من خلال:

- تحديد وتحليل التحديات الشائعة للأمن السيبراني بما في ذلك تحديد التهديدات المحتملة والجهات الفاعلة الخاصة بها، وكذلك نقاط الضعف المحتملة في عملياتها وأنظمتها.
- إجراء تقييمات مخاطر دورية لتحديد التهديدات ونقاط الضعف، خاصة عند التخطيط لأنشطة جديدة تعتمد على التكنولوجيا السيبرانية أو استكشاف تقنيات جديدة لدعم الأنشطة.
- تنفيذ عدة تدابير للتخفيف من المخاطر، مثل وضع معايير أمان للأجهزة والبرامج، واعتماد نهج «الثقة المعدومة» الذي يفضل القيود مثل الوصول الأقل امتيازًا، والتجزئة الدقيقة، والمصادقة متعددة العوامل.
- تنويع سلاسل التوريد لإزالة الاعتماد القوي على الموردين، والنظر في البدائل المجانية والمفتوحة المصدر (طالما أنها معتمدة أو مفحوصة بشكل مناسب).
- تطوير وتكييف التقنيات الحالية لتناسب الأوضاع الإنسانية، وضمان التكييف السياقي، والاختبار، والفعالية، والسلامة قبل النشر.
- إنشاء نُهُج داخلية وعبر المنظمات لتحديد وحل وتتبع والتواصل حول حوادث البيانات.[٤٨]

زيادة الوعي الرقمي بين الموظفين من خلال:

- تخصيص الموارد والتمويل المناسب للتدريب وجهود التوعية.
- إشراك وتدريب الموظفين وأصحاب المصلحة بانتظام للمساعدة في بناء الأمن السيبراني في ممارسات العمل اليومية.
- بناء الوعي الرقمي للعاملين في المجال الإنساني من خلال التوظيف عبر القطاعات وتطوير المهارات.
- زيادة الوعي بالبيانات لتمكين الموظفين من اعتماد ممارسات مسؤولة وتحسين نظافتهم السيبرانية، بما في ذلك إدارة كلمات المرور الجيدة، واستخدام برامج مكافحة الفيروسات/البرامج الضارة، وتجنب هجمات التصيد الاحتيالي.[٤٩]

[47] UN (2021). **Cybersecurity in the United Nations system organizations: Report of the Joint Inspection Unit**.

[48] Centre for Humanitarian Data (2019). **Guidance Note on Data Incident Management**.

[49] Centre for Humanitarian Data (2022). **Guidance Note on Data Security in Operational Data Management**.

زيادة الوعي الرقمي بين الموظفين من خلال:

تخصيص الموارد والتمويل المناسب للتدريب وجهود التوعية.

- إشراك وتدريب الموظفين وأصحاب المصلحة بانتظام للمساعدة في بناء الأمن السيبراني في ممارسات العمل اليومية.
- بناء الوعي الرقمي للعاملين في المجال الإنساني من خلال التوظيف عبر القطاعات وتطوير المهارات.
- زيادة الوعي بالبيانات لتمكين الموظفين من اعتماد ممارسات مسؤولة وتحسين نظافتهم السيبرانية، بما في ذلك إدارة كلمات المرور الجيدة، واستخدام برامج مكافحة الفيروسات/البرامج الضارة، وتجنب هجمات التصيد الاحتيالي.[٤٩]

تحسين التنسيق والتعاون من خلال:

- خلق بيئة تعزز ثقافة التنسيق والتعاون ومشاركة المعلومات بين الفاعلين.
- الاندماج في مجتمعات الأمن السيبراني الأوسع في القطاعين العام والخاص، وضمان المشاركة في تحليل تهديدات المعلومات وقنوات مشاركة المعلومات، بما في ذلك الإفصاح.
- الشراكة مع أصحاب المصلحة المعنيين لتحسين الأمن السيبراني والوصول إلى مجالات جديدة من الخبرة والتقنيات للعاملين في المجال الإنساني.[٥٠]

دعم المبادرات والأنظمة والمشاريع القائمة، مثل تعزيز منصات مشاركة البيانات القابلة للتشغيل البيني مع حماية كافية للبيانات الشخصية والحساسة داخل المنظمات وعبر القطاعات.

التواصل حول المبادرات، وفحص التهديدات، والانتهاكات المحتملة لتسليط الضوء على قضية الأمن السيبراني ودعم تطوير قاعدة معرفية، مما يعزز نهجًا أكثر تنسيقًا لإدارة الحوادث بمرور الوقت.

ينشر مركز البيانات الإنسانية («المركز») بالتعاون مع شركاء رئيسيين مجموعة من المذكرات الإرشادية والنشرات التوجيهية حول مسؤولية البيانات في العمل الإنساني خلال عامي ٢٠٢٢ و ٢٠٢٣. تكمل هذه المنشورات سلسلة المذكرات الإرشادية والنشرات التوجيهية للمركز، بالإضافة إلى التوجيه التشغيلي للجنة الدائمة بين الوكالات حول مسؤولية البيانات في العمل الإنساني وإرشادات مسؤولية البيانات لمكتب تنسيق الشؤون الإنسانية (OCHA)، والتي نُشرت في فبراير ٢٠٢١ وأكتوبر ٢٠٢١ على التوالي. من خلال هذه السلسلة، يهدف المركز إلى دعم المشاركة المستمرة من مجموعات أصحاب المصلحة المختلفة حول الالتزامات رفيعة المستوى والعمل الجماعي على مسؤولية البيانات. أصبحت هذه المذكرات الإرشادية ممكنة بدعم من حكومة سويسرا.

تبني هذه المذكرة الإرشادية على منشورات مكتب تنسيق الشؤون الإنسانية (OCHA) حول القضايا المتعلقة بالسيبرانية في القطاع الإنساني، بما في ذلك الإنسانية في عصر الحرب السيبرانية: نحو الاستخدام المبدئي والآمن للمعلومات في حالات الطوارئ الإنسانية ونظرة عامة على المخاطر الافتراضية، والأضرار الملموسة: الآثار الإنسانية للتهديدات السيبرانية لعام ٢٠٢٢.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Foreign Affairs FDFA

[50] Centre for Humanitarian Data (2020). **Guidance Note on Data Responsibility in Public-Private Partnerships**.