جامعة الزعيم الازهري
المجلة العلمية المركزية

إطار عمل مقترح لتأسيس مبادرة سفراء الأمن السيبراني في السودان: نحو نموذج مستدام للتدريب التخصصي والخدمات الاستشارية الرقمية

1 د. طه الفضل طه https://orcid.org/0000-0003-1906-0110 tahapilot13@gmail.com	
2 مبارك الامين المبارك دليل mubarakdaleel99@gmail.com	3 خالد عثمان العالم khaildosman@gmail.com
4 د. عوض الكريم حسن محمد سعيد، shultif@gmail.com	5 عادل بشري يحيي يوسف، Adilbushra188@gmail.com
6 أمين طلحة حسن طلحة aminko2002@gmail.com	7 د. محمد عوض حمد Dr.mohammed.571@gmail.com
8 عثمان الفضل طه ، osmanFadul2030@gmail.com	9 مروة التجاني ابوبكر علي marwategani@gmail.com

1,2,6,5,4 كلية علوم الحاسوب وتقانة المعلومات، جامعة الزعيم الازهري،الخرطوم

3 كلية علوم الحاسوب وتقانة المعلومات، جامعة بحري،الخرطوم

7 جامعة الملك خالد المملكة العربية السعودية

8 المدير الاداري، مركز جيوفايف للتدريب

9 جامعة العلوم و التكنولوجيا اليمن

المستخلص

تُعد البنية التحتية الحيوية (العصب المحرك للدولة) في السودان، بما تشمله من قطاعات الطاقة، الصحة، الاتصالات، والمصارف، هدفاً استراتيجياً للتهديدات السيبرانية المتزايدة التي قد تؤدي إلى شلل خدمات الدولة الحيوية. تهدف هذه الورقة العلمية إلى تقديم إطار عمل مقترح لتأسيس "مبادرة سفراء الأمن السيبراني في السودان"، وهي مبادرة وطنية رائدة تسعى إلى سد الفجوة الرقمية والتقنية من خلال محورين أساسيين: التدريب التخصصي والخدمات الاستشارية الميدانية.

تعتمد المنهجية المقترحة على فلسفة تحويل العنصر البشري من "نقطة ضعف" وسهلة الاختراق عبر الهندسة الاجتماعية، إلى "خط دفاع" استباقي وجدار حماية بشري (Human Firewall). تتناول الورقة الأهمية الاستراتيجية للمبادرة في تعزيز السيادة الرقمية الوطنية، وتقدم هيكلاً تشغيلياً يضمن توزيع "السفراء" كخبراء

ومستشارين تقنيين عبر ولايات السودان المختلفة لضمان سرعة الاستجابة للحوادث السيبرانية وتقييم مخاطر البنية التحتية ميدانياً.

تخلص الورقة إلى أن الاستثمار في هذا الكادر الوطني يمثل جدوى اقتصادية واجتماعية عالية، حيث يقلل من تكاليف الخسائر الناتجة عن الهجمات الرقمية ويحد من الاعتماد على الخبرات الأجنبية. كما تقترح الورقة مجموعة من مؤشرات الأداء (KPIs) لضمان استدامة المبادرة كبيت خبرة وطني يدعم أهداف التنمية المستدامة ويحمي الأمن القومي المعلوماتي للدولة السودانية.

الكلمات المفتاحية: الأمن السيبراني، السودان، البنية التحتية الحيوية، سفراء الأمن، الاستشارات الرقمية، السيادة الرقمية، التدريب التقني.

Abstract

A Proposed Framework for Establishing the Cyber security Ambassadors Initiative in Sudan: Towards a Sustainable Model for Specialized Training and Digital Consultancy Services

Abstract

Critical infrastructure, the "driving engine of the state" in Sudan—encompassing energy, healthcare, telecommunications, and banking sectors—represents a strategic target for increasing cyber threats that could paralyze vital state services. This paper proposes a comprehensive framework for establishing the "Cyber security Ambassadors Initiative in Sudan." This pioneering national initiative seeks to bridge the digital and technical gap through two primary pillars: Specialized Training and Field Consultancy Services.

The proposed methodology is based on a transformative philosophy: shifting the human element from being a "point of weakness" vulnerable to social engineering into a proactive "line of defense" and a human firewall. The paper discusses the strategic importance of the initiative in enhancing national digital sovereignty and presents an operational structure that ensures the distribution of "Ambassadors" as technical experts and consultants across various Sudanese states. This distribution aims to ensure rapid incident response and on-site risk assessment of critical infrastructure.

The paper concludes that investing in this national cadre offers high economic and social feasibility by reducing costs associated with cyber-attack losses and minimizing reliance on foreign expertise. Furthermore, the study suggests a set of Key Performance Indicators (KPIs) to ensure the initiative's sustainability as a national center of excellence that supports Sustainable Development Goals (SDGs) and protects the state's national information security.

Keywords: Cyber security, Sudan, Critical Infrastructure, Cyber Ambassadors, Digital Consultancy, Digital Sovereignty, Technical Training.

1. المقدمة(Introduction)

يشهد السودان تحولاً رقمياً متسارعاً في مختلف مؤسسات الدولة، حيث أصبحت الأنظمة الرقمية هي العصب المحرك للخدمات الأساسية مثل الإدارة الحكومية، الصحة، التعليم، والكهرباء. ومع هذا الاعتماد المتزايد على التكنولوجيا، برزت تحديات أمنية معقدة تهدد استقرار هذه البنية التحتية الحيوية.

تُشير الإحصائيات العالمية إلى أن العنصر البشري يظل الحلقة الأضعف في منظومة الأمن السيبراني، حيث تعود أغلب الاختراقات الناجحة إلى ضعف الوعي أو نقص الخبرة الفنية في التعامل مع التهديدات المتطورة. في السياق السوداني، يزداد هذا التحدي حدةً بسبب الفجوة الرقمية ونقص الكوادر المتخصصة القادرة على تقديم الدعم الفني والاستشاري السريع[i].

1.1. المبادرة

تأتي مبادرة "سفراء الأمن السيبراني "كإطار عمل استراتيجي يهدف إلى معالجة هذه الفجوة عبر محورين متوازيين:[ii]

1. المحور التدريبي :بناء قدرات وطنية شابة وموزعة جغرافياً لضمان وجود "خط دفاع أول" في كل ولاية ومؤسسة.
2. المحور الاستشاري :تقديم الدعم الفني والخبرة المتخصصة للمؤسسات الحيوية لتمكينها من تقييم المخاطر وبناء أنظمة صمود (Resilience)رقمية.

إن مبادرة سفراء الأمن السيبراني هي استثمار في "المرونة الوطنية". فالدولة التي تمتلك جيشاً من المستشارين التقنيين الميدانيين هي دولة قادرة على امتصاص الصدمات الرقمية والتعافي منها بسرعة، مما يضمن استمرارية "العصب المحرك" تحت أي ظرف.

تستعرض هذه الورقة منهجية تأسيس المبادرة، وكيف يمكن لنموذج "السفراء" أن يتحول إلى آلية مستدامة للتدريب والاستشارات، تضمن حماية السيادة الرقمية للدولة وتدعم أهداف التنمية المستدامة من خلال بيئة تقنية آمنة وموثوق.

1.2.أهداف المبادرة (Initiative Objectives)

تتمحور الأهداف الاستراتيجية لمبادرة "سفراء الأمن السيبراني في السودان" حول بناء منظومة دفاعية مرنة تعتمد على الكادر البشري المؤهل، ويمكن تلخيص هذه الأهداف في النقاط التالية:

1. بناء قدرات استشارية وطنية: تأهيل نخبة من الخبراء (السفراء) ليكونوا مستشارين ميدانيين قادرين على إجراء عمليات تقييم المخاطر (Risk Assessment) للمؤسسات الحيوية في الولايات المختلفة، مما يقلل الاعتماد على الاستشارات الخارجية.
2. تعزيز صمود البنية التحتية الحيوية (Infrastructure Resilience): تطوير خطط استباقية وتدريبية لحماية القطاعات التي تمثل "عصب الدولة" (مثل شبكات الكهرباء، أنظمة المستشفيات، والمصارف)

من الهجمات السيبرانية المعقدة وضمان استمرارية الأعمال.

3. توطين ثقافة الأمن السيبراني: تحويل المفاهيم التقنية المعقدة إلى ممارسات يومية مفهومة للموظفين والمواطنين، وبناء "جدار حماية بشري" قادر على اكتشاف هجمات الهندسة الاجتماعية وإفشالها قبل وقوع الضرر.
4. تأسيس منصة استشارية وتدريبية مستدامة: خلق نموذج عمل (Business Model) يتيح للمبادرة تقديم خدمات استشارية وتدريبية مدفوعة أو مدعومة للمؤسسات، مما يضمن استدامة المبادرة مالياً وتقنياً على المدى الطويل.
5. الاستجابة الجغرافية السريعة للحوادث: توزيع السفراء جغرافياً عبر ولايات السودان لضمان وجود "مستجيب أول" (First Responder) يمتلك الخبرة اللازمة للتعامل الفوري مع أي خرق أمني في أي نقطة جغرافية، وتقليل زمن الاستجابة للأزمات.
6. دعم التحول الرقمي الآمن: مواكبة توجه الدولة نحو "الحكومة الإلكترونية" من خلال توفير الدعم الاستشاري اللازم للمشاريع الرقمية الجديدة لضمان بنائها على أسس أمنية متينة منذ مراحلها الأولى (Security by Design).
7. المساهمة في السيادة الرقمية الوطنية: تقليل الفجوة الرقمية السيادية عبر امتلاك أدوات تحليل وتأمين "سودانية" بأيدي خبراء محليين، مما يعزز أمن المعلومات القومي في مواجهة التحديات الدولية.

1.3.الأهمية الاستراتيجية(Strategic Significance)

تتجاوز مبادرة "سفراء الأمن السيبراني" كونها برنامجاً تدريبياً لتصبح ضرورة استراتيجية تفرضها متطلبات الأمن القومي السوداني. وتبرز أهميتها من خلال ثلاثة أبعاد رئيسية:

أولاً: حماية الأصول السيادية والعصب المحرك للدولة : تمثل قطاعات الكهرباء، المياه، الصحة، والاتصالات في السودان "أهدافاً ناعمة" ومرغوبة للمهاجمين. إن تأمين هذه القطاعات عبر "سفراء" متخصصين يضمن: الاستقرار الخدمي: منع انقطاع الخدمات الأساسية الذي قد يؤدي إلى اضطرابات اجتماعية. تأمين البيانات الوطنية: حماية السجلات المدنية والمالية والصحية من السرقة أو التلاعب، مما يحفظ خصوصية المواطن وهيبة الدولة.

ثانياً: تعزيز السيادة الرقمية والاستقلال التقني : في ظل المتغيرات الجيوسياسية، يصبح الاعتماد على الشركات الأجنبية أو المستشارين الخارجيين لتأمين الأنظمة الحساسة مخاطرة استراتيجية. تساهم المبادرة في: توطين المعرفة: بناء "قاعدة بيانات بشرية" من الخبراء السودانيين القادرين على إدارة الأزمات محلياً. القرار الأمني المستقل: امتلاك

القدرة على تحليل التهديدات واتخاذ قرارات المواجهة بناءً على المصالح الوطنية العليا دون تدخل خارجي.

ثالثاً: الجدوى الاقتصادية وخفض التكلفة الإجمالية للمخاطر : الهجمات السيبرانية لا تدمر الأنظمة فحسب، بل تستنزف ميزانية الدولة. تساهم المبادرة في: الوقاية من الخسائر المليارية: تكلفة تدريب "سفير" تُمثل جزءاً ضئيلاً جداً من تكلفة استعادة نظام بنكي أو شبكة كهرباء بعد تعرضها لهجوم "برمجيات الفدية" (Ransomware). خلق سوق عمل استشاري: تحويل السودان من مستهلك لخدمات الأمن السيبراني إلى مصدّر للخبرات والكفاءات، مما يدعم الاقتصاد الرقمي.

رابعاً: دعم التحول الرقمي الموثوق (Trust–Based Digital Transformation) *:* لا يمكن نجاح أي مبادرة للتحول الرقمي (مثل الدفع الإلكتروني أو الهوية الرقمية) دون وجود "ثقة" لدى المستخدم. وجود سفراء منتشرين ميدانياً يعزز ثقة الجمهور والمؤسسات في الأنظمة الحكومية، مما يسرع من وتيرة التنمية المستدامة.

2. الاطار العام

2.1. استعراض حالة الأمن السيبراني في السودان (Cybersecurity Landscape in Sudan)

يمر السودان بمرحلة انتقالية نحو الرقمنة الشاملة، حيث اعتمدت الدولة استراتيجيات طموحة للحكومة الإلكترونية والشمول المالي، مما جعل القطاعات الحيوية (مثل المصارف، الاتصالات، والطاقة) تعتمد بشكل كلي على الشبكات المفتوحة. ومع ذلك، هذا التحول السريع لم يواكبه تطور مماثل في استراتيجيات الدفاع السيبراني، ويمكن تلخيص الحالة الراهنة في النقاط التالية:

1. تزايد التهديدات النوعية: واجه السودان في الآونة الأخيرة هجمات إلكترونية استهدفت مواقع حكومية رسمية ومنصات بنكية، تراوحت بين هجمات حجب الخدمة (DDoS) وبرمجيات الفدية، مما أدى في بعض الأحيان إلى شلل مؤقت في تقديم الخدمات الحيوية[iii].
2. التحديات التشريعية والتنظيمية: على الرغم من وجود "قانون مكافحة جرائم المعلوماتية"، إلا أن هناك حاجة ملحة لتحديث الأطر القانونية لتشمل معايير حماية البنية التحتية الحيوية، وإلزام المؤسسات بتبني سياسات أمنية صارمة[iv].
3. النقص الحاد في الكوادر المتخصصة: يعاني القطاعين العام والخاص من هجرة العقول التقنية، مما خلق فجوة كبيرة في القدرة على الاستجابة الفورية للحوادث السيبرانية (Incident Response) وإجراء عمليات التدقيق والاستشارات الأمنية الدورية.

4. غياب الوعي المجتمعي والمؤسسي: لا يزال "الهندسة الاجتماعية" (Social Engineering) تمثل التهديد الأكبر، حيث يتم استغلال ضعف الوعي السيبراني لدى الموظفين والمواطنين للوصول إلى بيانات حساسة، مما يجعل الحاجة إلى مبادرة مثل "سفراء الأمن السيبراني" ضرورة قصوى وليست ترفاً.
5. الاعتماد على التقنيات المستوردة: يمثل الاعتماد الكبير على حلول أمنية أجنبية تحدياً للسيادة الرقمية، خاصة في ظل الظروف السياسية المتغيرة، مما يستوجب بناء خبرات وطنية قادرة على تقديم استشارات وتدريبات نابعة من فهم عميق للبيئة المحلية[v].

2.2. تعريف سفير الأمن السيبراني (Cyber security Ambassador):

في إطار هذه المبادرة، يتم إعادة صياغة دور "السفير" ليتجاوز المفهوم التقليدي للتمثيل، ليصبح دوراً محورياً يجمع بين الكفاءة التقنية والقدرة الاستشارية. ويمكن تعريف "سفير الأمن السيبراني" في هذا السياق على النحو التالي: هو كادر وطني مؤهل تأهيلاً عالياً، يتم اختياره وتدريبه ليكون "نقطة الارتكاز الرقمية" في بيئته المهنية أو الجغرافية. لا يقتصر دوره على نشر الوعي فحسب، بل يعمل كذراع تقنية واستشارية ميدانية تساهم في حماية الأصول الرقمية للدولة[vi].هذا التعريف ينقل المبادرة من مجرد "حملة توعوية" إلى "شبكة استشارية وطنية". فبدلاً من اعتماد الدولة على مستشارين أجانب بتكاليف عالية، تتيح المبادرة وجود مستشار ميداني في كل وحدة إدارية أو جغرافية في السودان، مما يضمن سرعة الاستجابة ودقة الاستشارة النابعة من فهم الواقع المحلي. ويمكن تفصيل هذا المفهوم عبر بعدين أساسيين:

1. السفير كخبير تقني (Technical Expert): الدرع الواقي: يمتلك المهارات الفنية اللازمة لتحديد الثغرات البرمجية والتقنية داخل الأنظمة والمؤسسات. المستجيب الأول: يعمل كخط دفاع أول في حال حدوث اختراقات، حيث يمتلك القدرة على عزل الأنظمة المتضررة وتقليل حجم الخسائر قبل وصول فرق الاستجابة المركزية. المواكب للتطور: هو الشخص الذي يتابع أحدث أنماط الهجمات السيبرانية وبرمجيات الفدية ويقوم بتطبيق التحديثات والتحصينات اللازمة بشكل استباقي.
2. السفير كاستشاري ميداني (Field Consultant): مقيم المخاطر: يقوم بإجراء عمليات تدقيق (Auditing) أولية للمؤسسات الحيوية في السودان (مثل محطات الكهرباء أو المستشفيات) لتقديم تقارير استشارية حول نقاط الضعف البشرية والتقنية. وسيط المعرفة: يعمل كحلقة وصل استشارية بين "المركز القومي للمعلومات" والجهات الميدانية، حيث يترجم السياسات الأمنية المعقدة إلى إجراءات عملية بسيطة ومفهومة للموظفين. مخطط استمرارية

الأعمال: يقدم استشارات حول كيفية ضمان استمرار "العصب المحرك للدولة" في العمل أثناء وبعد وقوع الهجمات السيبرانية، واضعاً خطط الطوارئ المناسبة لكل بيئة عمل.

2.3. مفهوم "سفراء الأمن السيبراني": تحويل الأفراد من "نقطة ضعف" إلى "خط دفاع"

في أدبيات الأمن السيبراني التقليدية، غالباً ما يُشار إلى العنصر البشري بوصفه "الحلقة الأضعف" (The Weakest Link) في منظومة الحماية، حيث تُشير التقارير الدولية إلى أن أكثر من 90% من الاختراقات الناجحة تبدأ بخطأ بشري (مثل النقر على روابط مشبوهة أو ضعف إدارة كلمة المرور). تهدف مبادرة "سفراء الأمن السيبراني في السودان" إلى قلب هذه المعادلة جذرياً من خلال استراتيجية "التمكين والتحصين"، وذلك وفق الأسس التالية:

1. الفرد كنقطة ضعف (The Human as a Vulnerability): في غياب الوعي والتدريب، يمثل الموظف أو المواطن "ثغرة غير مرئية" تتجاوز أقوى جدران الحماية النارية (Firewalls). فالهندسة الاجتماعية تستهدف العاطفة أو قلة المعرفة لدى الفرد للوصول إلى بيانات "العصب المحرك للدولة". هنا، يكون الفرد هو المدخل الذي يُعرض البنية التحتية الحيوية للشلل.

2. الفرد كخط دفاع (The Human as a Shield): تسعى المبادرة إلى إعادة صياغة هذا الدور، بحيث يصبح السفير هو "جدار الحماية البشري" (Human Firewall). يتم ذلك من خلال:

الوعي الاستباقي: تحويل "رد الفعل" لدى الفرد إلى "استشعار استباقي"، حيث يصبح قادراً على تمييز محاولات التسلل قبل وقوعها. الاستجابة اللحظية: بدلاً من انتظار تدخل الفرق المركزية، يعمل السفير كخط دفاع أول يمتلك الأدوات التقنية لإيقاف التهديد في مهده.

3. آلية التحول (The Transformation Mechanism): يتم التحول من "الضعف" إلى "الدفاع" عبر ثلاث مراحل أساسية يتبناها الإطار المقترح للمبادرة: التفكيك: تفكيك السلوكيات الرقمية الخاطئة واستبدالها بممارسات أمنية منضبطة. البناء التقني: تزويد السفراء بمهارات استشارية وميدانية تمكنهم من تقديم حلول تقنية فورية لمؤسساتهم. التمكين القيادي: منح السفير السلطة العلمية والتقنية ليكون مرجعاً واستشارياً في محيطه، مما يعزز الثقة الوطنية في الكوادر المحلية.

4. الأثر على استدامة الدولة: إن تحويل المواطن السوداني إلى "سفير سيبراني" يعني توزيع مراكز الحماية جغرافياً ومؤسسياً. فبدلاً من حماية مركزية واحدة، يصبح للدولة آلاف الحصون البشرية الموزعة على قطاعات الكهرباء والصحة والتعليم، مما يضمن مرونة عالية وصموداً أمام الهجمات السيبرانية المعقدة.

5. لمنهجية

بما أن المبادرة تركز على التدريب والاستشارات، فإن هيكل المبادرة يجب أن يُصمم كمنظومة متكاملة تضمن تحويل المتدرب إلى مستشار فاعل. المبادرة تتبنى فلسفة "التدريب من أجل التنفيذ"؛ حيث يكون المشروع الختامي لكل متدرب هو إجراء دراسة حالة استشارية حقيقية لمؤسسة سودانية، مما يوفر قاعدة بيانات ضخمة من التقارير الاستشارية الأولية التي تخدم أمن الدولة القومي.

5.1. هيكل المبادرة (Initiative Framework) : يعتمد هيكل المبادرة على نموذج (TCC – Training, Consultancy, Community) الذي يربط بين بناء القدرات، تقديم الخدمة، واستمرارية الأثر، وذلك عبر المسارات التالية:

أولاً: مسار التدريب التخصصي (Specialized Training Track) : لا يهدف التدريب هنا إلى منح شهادات حضور، بل إلى "تمكين فني" مقسم إلى مستويات:

- المستوى التأسيسي (Cyber Literacy): يستهدف بناء الوعي العام وتأمين السلوك الرقمي الشخصي والمؤسسي.
- المستوى المتقدم (The Specialist): تدريب عملي على تقنيات فحص الثغرات، حماية الشبكات، والاستجابة للحوادث داخل بيئات البنية التحتية الحيوية.
- المستوى الاستشاري (The Consultant): تأهيل السفراء على مهارات "كتابة التقارير الفنية" و"تحليل المخاطر" وإدارة الامتثال للمعايير الدولية (مثل ISO 27001).

ثانياً: مسار الخدمات الاستشارية (Consultancy Services Track) : هذا هو القلب المحرك للمبادرة، حيث يتم تفعيل دور السفير لتقديم خدمات ملموسة للمؤسسات السودانية، وتشمل:

- استشارات تقييم الجاهزية: فحص مدى استعداد المؤسسة (مثل مستشفى أو محطة كهرباء) لمواجهة الهجمات.
- استشارات الامتثال الرقمي: مساعدة المؤسسات الحكومية والخاصة في مواءمة أنظمتها مع القوانين السودانية لجرائم المعلوماتية.
- بناء خطط التعافي (Disaster Recovery): تقديم استشارات ميدانية حول كيفية استعادة البيانات والخدمات في حال حدوث اختراق أو عطل تقني كبير.

ثالثاً: المختبر الاستشاري المتنقل (The Mobile Cyber Lab) : توفير أدوات تقنية محمولة للسفراء تمكنهم من إجراء عمليات المسح والاستشارة في المواقع البعيدة والولايات، مما يضمن وصول الخدمة الاستشارية إلى "أطراف" البنية التحتية للدولة وليس المركز فقط.

رابعاً: نظام العضوية والاعتماد (Accreditation System)

- يتم منح السفراء "رخصة سفير معتمد" بناءً على أدائهم في المهام الاستشارية الميدانية.
- يتم تصنيف السفراء في قاعدة بيانات وطنية تتيح للمؤسسات طلب "الاستشارة" من السفير الأقرب جغرافياً أو الأكثر تخصصاً.

5.2. المنهجية التشغيلية (Implementation Roadmap) : تنفذ المبادرة عبر أربع مراحل زمنية وتقنية، تضمن الانتقال السلس من التخطيط إلى الاستدامة الاستشارية:

المرحلة الأولى: مرحلة التأسيس والاعتماد (0 – 3 أشهر)

- صياغة المعايير: وضع المعايير الفنية والأخلاقية لاختيار "السفراء"، مع التركيز على الكفاءة التقنية والالتزام الوطني.
- بناء الشراكات الاستراتيجية: توقيع مذكرات تفاهم مع (المركز القومي للمعلومات، جهاز تنظيم الاتصالات، والجامعات السودانية) لتوفير الغطاء القانوني والاعتماد الأكاديمي للشهادات والاستشارات.
- تجهيز "الحقيبة الاستشارية": إعداد المناهج التدريبية والأدوات التقنية التي سيستخدمها السفراء في الميدان.

المرحلة الثانية: مرحلة "النواة" والتدريب المركزي (3 – 6 أشهر)

- برنامج (Train the Trainers): تدريب الدفعة الأولى (50–100 سفير) في الخرطوم أو مراكز الولايات المستقرة، ليكونوا قادة الفرق الاستشارية لاحقاً.
- إطلاق المنصة الرقمية: تدشين منصة "سفراء الأمن السيبراني" لتكون مستودعاً للتقارير الاستشارية ووسيلة لطلب الدعم الفني من قبل المؤسسات.

المرحلة الثالثة: الانتشار الجغرافي والتمكين الميداني (6 – 12 شهراً)

- نشر السفراء في الولايات: توزيع الفرق الاستشارية على الولايات (بدءاً بالولايات ذات الكثافة الحيوية للكهرباء والزراعة مثل ولاية الجزيرة، البحر الأحمر، والولاية الشمالية).
- المسح الاستشاري الشامل: تكليف السفراء بإجراء "مسح أولي" لنقاط الضعف في المؤسسات الحكومية الحيوية في كل ولاية ورفعها في شكل تقارير استشارية سرية لصناع القرار.

المرحلة الرابعة: الاستدامة والتحول لبيت خبرة (ما بعد السنة الأولى)

- تفعيل نموذج العمل (Business Model): البدء في تقديم استشارات مدفوعة للقطاع الخاص (البنوك، شركات

الاتصالات) لتمويل الأنشطة التدريبية المجانية للقطاع العام.

- التقييم والتطوير: تحديث المناهج بناءً على الهجمات السيبرانية الفعلية التي تم رصدها خلال العام الأول.
- التكامل الإقليمي: البحث عن فرص لتبادل الخبرات مع مبادرات مشابهة في دول حوض النيل لتعزيز الأمن السيبراني المشترك.

5.3. عوامل النجاح الحرجة (Critical Success Factors):

1. الدعم السياسي: تبني المبادرة من أعلى مستويات السلطة لتسهيل دخول السفراء للمؤسسات الحيوية.
2. المرونة الرقمية: استخدام خوادم محلية آمنة (Cloud) لضمان عدم تسرب التقارير الاستشارية خارج السودان.
3. الذكاء الاصطناعي الجغرافي (Geo-AI): استخدام خرائط رقمية لمتابعة انتشار السفراء وتحديد "المناطق الحمراء" تقنياً والتي تحتاج لتدخل استشاري عاجل.

6. النتائج ومناقشتها

يتم توضيح أن مبادرة سفراء الأمن السيبراني ليست مجرد مشروع تطوعي، بل هي استثمار استراتيجي يحقق عوائد مالية واجتماعية ملموسة للدولة والمجتمع.

6.1. الجدوى الاقتصادية والاجتماعية (Social Feasibility & Economic) :

تعتمد المبادرة نموذجاً يحقق التوازن بين تقديم الخدمة الوطنية وبين الاستدامة المالية، وذلك عبر الأبعاد التالية:

أولاً: الجدوى الاقتصادية (العائد على الاستثمار التقني)

- خفض تكلفة "الاستجابة للأزمات": إن تكلفة التدريب الاستباقي لسفير واحد تُمثل أقل من 1% من الخسائر المباشرة الناتجة عن هجوم "برمجيات فدية" (Ransomware) قد يشل القطاع المصرفي أو نظام التحصيل الإلكتروني.[vii]
- توفير العملة الصعبة: عبر توطين قطاع الاستشارات، يتم تقليل الحاجة للتعاقد مع شركات استشارية أجنبية تتقاضى مبالغ طائلة بالعملات الصعبة، والاعتماد بدلاً من ذلك على "بيت الخبرة الوطني" المتمثل في السفراء.
- نموذج "الخدمات المتقاطعة" (Cross-Subsidization): يمكن للمبادرة تمويل نفسها ذاتياً من خلال تقديم استشارات تخصصية مدفوعة الثمن للقطاع الخاص (البنوك، الشركات الكبرى) واستخدام تلك العوائد لتدريب الكوادر في القطاع الحكومي والتعليمي مجاناً.

ثانياً: الجدوى الاجتماعية والتنموية

- خلق فرص عمل نوعية: تساهم المبادرة في خلق مهن جديدة في السوق السوداني تحت مسمى "مستشار أمن سيبراني معتمد"، مما يحد من هجرة العقول التقنية عبر توفير بيئة عمل احترافية ومجزية محلياً.
- ردم الفجوة الرقمية بين الولايات: من خلال التوزيع الجغرافي للسفراء، تضمن المبادرة وصول المعرفة والاستشارات للمناطق النائية، مما يحقق عدالة تنموية في حماية "البنية التحتية" أينما وجدت في السودان.
- بناء "الثقة الرقمية": عندما يشعر المواطن أن بياناته في المستشفيات والمصارف محمية بأيدي خبراء وطنيين، تزداد معدلات استخدامه للخدمات الرقمية، مما يرفع من كفاءة الاقتصاد الكلي للدولة.

ثالثاً: الأثر على الأمن القومي : تحويل الأمن السيبراني من "عبء مالي" على ميزانية الدولة إلى "محرك للنمو" ودرع يحمي أصول الدولة الاقتصادية (مثل قطاع الذهب، النفط، والكهرباء) من التخريب الرقمي الذي قد يكلف الدولة خسائر لا تُقدر بثمن.

6.2.مؤشرات الأداء الرئيسية (Key Performance Indicators – KPIs)

لقياس نجاح مبادرة "سفراء الأمن السيبراني" وضمان تحقيق أهدافها في التدريب والاستشارات، يتم الاعتماد على المؤشرات التالية:

أولاً: مؤشرات المسار التدريبي (Training Metrics)

- معدل التأهيل السنوي: عدد السفراء الذين أتموا البرنامج التدريبي بنجاح وحصلوا على "رخصة سفير معتمد" في كل ولاية.
- جودة المخرجات: نسبة السفراء الذين اجتازوا الاختبارات التقنية الدولية أو المحلية بنسبة تفوق 80%.
- التغطية الجغرافية: النسبة المئوية للمناطق الحيوية في السودان التي يتوفر بها سفير واحد على الأقل (نحو تغطية 100% من الولايات).

ثانياً: مؤشرات المسار الاستشاري (Consultancy Metrics)

- عدد المسوحات الميدانية: عدد التقارير الاستشارية المرفوعة لتقييم ثغرات المؤسسات الحيوية (مثل المستشفيات ومحطات المياه).
- سرعة الاستجابة: متوسط الوقت المستغرق من قبل السفير للوصول لموقع الحادث السيبراني أو تقديم الاستشارة الطارئة (Target: أقل من ساعتين في المناطق الحضرية).
- معدل سد الثغرات: نسبة الثغرات التي تم إغلاقها أو معالجتها بناءً على التوصيات الاستشارية التي قدمها السفراء للمؤسسات.

ثالثاً: مؤشرات الأثر الاستراتيجي (Strategic Impact Metrics)

- انخفاض معدل الاختراقات: قياس مدى انخفاض الهجمات السيبرانية الناجحة في

القطاعات التي يشرف عليها السفراء مقارنة بالأعوام السابقة.

- العائد المالي الموفر: تقدير حجم الأموال التي وفرتها الدولة من خلال تجنب دفع "الفدية الرقمية" أو تكاليف استعادة الأنظمة بفضل جهود السفراء.
- مؤشر الثقة الرقمية: استطلاعات رأي لقياس مدى شعور الموظفين والمواطنين بالأمان أثناء استخدام الخدمات الإلكترونية الحكومية.

7. التوصيات والخاتمة (Recommendations & Conclusion)

أولاً: التوصيات (Recommendations) : لضمان نجاح مبادرة "سفراء الأمن السيبراني" وتحويلها إلى واقع مستدام، تقترح الورقة العلمية الآتي:

1. الاعتراف الرسمي: إصدار قرار سيادي يتبنى المبادرة كجزء من "الاستراتيجية الوطنية للأمن السيبراني"، مما يمنح السفراء الصلاحيات القانونية لتقديم الاستشارات للمؤسسات.
2. التكامل المؤسسي: ربط المبادرة بالجامعات السودانية والمراكز البحثية لتكون حاضنة للمناهج التدريبية، وتوفير معامل محاكاة (Cyber Ranges) للتدريب العملي.
3. تحفيز القطاع الخاص: تشجيع البنوك وشركات الاتصالات على رعاية المبادرة كجزء من مسؤوليتها الاجتماعية، والاستفادة من خريجيها كمستشارين معتمدين.
4. منصة "المرصد السيبراني": إنشاء منصة رقمية مركزية تعمل بالذكاء الاصطناعي الجغرافي لربط السفراء ببعضهم، وتبادل التقارير الاستشارية حول أنماط التهديدات الجديدة في السودان.
5. الاستثمار في "التدريب المستمر": نظراً لطبيعة الأمن السيبراني المتغيرة، يجب تحديث "رخصة السفير" سنوياً بناءً على مواكبته لأحدث التطورات العالمية.

ثانياً: الخاتمة (Conclusion) : في ختام هذه الورقة، يتضح أن حماية البنية التحتية الحيوية في السودان لم تعد خياراً تقنياً، بل هي ضرورة وجودية لاستمرار "العصب المحرك للدولة". إن مبادرة "سفراء الأمن السيبراني" تقدم نموذجاً مبتكراً يتجاوز الحلول البرمجية التقليدية، ليركز على بناء "السيادة الرقمية" عبر العقول الوطنية.

من خلال دمج التدريب التخصصي بالخدمات الاستشارية الميدانية، ستتمكن الدولة من بناء جيش رقمي لا يكتفي برد الفعل، بل يمتلك المهارة الاستباقية لتأمين مستقبل السودان الرقمي. إن الاستثمار في هؤلاء السفراء هو الاستثمار الحقيقي في استقرار الدولة ونموها الاقتصادي، وضمان بقاء خدمات المواطن الحيوية بعيدة عن متناول التهديدات السيبرانية المتزايدة.

References

[i]Workshop for Launching the Cyber security Ambassadors Initiative , GeoFive Training, Sudan, 1/1/2026
[ii]Penniston, J., & Ettang, D. (2026). BRICS'Contribution to Addressing Youth Unemployment in South Africa. In *Expanded BRICS Nations: Peace, Security, Global Economy and Sustainable Development* (pp. 321-364). Singapore: Springer Nature Singapore.
[iii]Alcaide, J. C. N., & Greco, S. (2023). Online education, international cooperation and sustainable development in Sudan.
[iv] Osunji, O. (2022). *Government's role in building trust and confidence in the internet: A case study of Uganda in the implementation of cybersecurity capacity maturity model for nations*. Marymount University.
[v]Niyikora, E. (2025). *Cybersecurity Risk Assessment Methods for Digital Financial Services in Sub-Saharan Africa* (Doctoral dissertation, Walden University).
[vi]Smart Cities Security Workshop, Sudanese Smart Cities and Communities Initiative, Sudan, 1/10/2025
[vii]Buheji, M. (2025). Eliminating illiteracy in post-conflict Syria–Inspiration Economy Lab perspective. *Int J Res Publ Rev*, *6*(9), 2383-94.