التشفير ما بعد الكم

(Post-Quantum Cryptography) وحماية الاتصالات الحكومية

الإمارات العربية المتحدة - دبي

26 – 30/ 04 / 2026

مقدمة:

في عام 2026، ومع اقتراب "اليوم صفر لـ كيو" (Q-Day)، لم يعد التشفير التقليدي كافياً لحماية أسرار الدولة. إن التشفير ما بعد الكم (PQC) هو الدرع السيادي الذي يضمن بقاء الاتصالات الحكومية محصنة ضد القوة الحسابية الخارقة للحواسيب الكمومية. يهدف هذا البرنامج إلى تمكين القادة من قيادة "التحول الكمي" وتوظيف الخوارزميات المقاومة للكم لتصفير البيروقراطية في إجراءات التحديث الأمني، مما يضمن النزاهة المطلقة والريادة العالمية في حماية الأصول المعلوماتية الوطنية.

أهداف الدورة:

- استيعاب مفاهيم "الحوسبة الكمومية" وعلاقتها بانهيار أنظمة التشفير التقليدية.(RSA/ECC)
- تطوير مهارات هندسة "المرونة التشفيرية (Crypto-agility) "في البنى التحتية الحكومية.
- إتقان فن اختيار وتطبيق خوارزميات PQC المعتمدة عالمياً.(NIST Standards)
- حوكمة ممارسات الانتقال للهياكل الهجينة (Hybrid Approaches) لضمان استمرارية الأعمال.
- تعزيز السيادة المعلوماتية عبر بناء "معايير تشفير وطنية" مستقلة ومقاومة للكم.
- تطبيق استراتيجيات القيادة في إدارة "مخاطر البيانات المخزنة (Harvest Now, " Decrypt Later).

محتويات الورشة:

اليوم الأول :

فلسفة "الأمن الكمي" والرشاقة في مواجهة تهديدات المستقبل

هندسة الجاهزية السيادية وتصفير البيروقراطية في تقييم المخاطر

- مفهوم التهديد الكمي 2026: تحليل استراتيجية "احصد الآن وفك التشفير لاحقاً" وأثرها على السيادة.
- مواءمة استراتيجيات التشفير مع مبدأ تصفير البيروقراطية عبر أتمتة جرد الأصول التشفيرية (Inventory).
- تحليل العلاقة بين "الحصانة الكمية" وبين بناء الثقة والمصداقية الدولية في النموذج الرقمي للدولة.
- تمرين هندسة الاستباقية لتصميم خارطة طريق تصفّر زمن الانتقال للخوارزميات الجديدة بنزاهة وشفافية.

قيادة النزاهة في حوكمة "الأسرار الوطنية" والريادة العالمية الشاملة

- تعزيز السيادة على مفاتيح التشفير الوطنية لضمان استقلاليتها وتوافقها مع القيم والهوية والتميز.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في اختيار مزودي تقنيات PQC.
- بناء ثقافة "الأمان المستدام" وعلاقتها بجودة الحياة والولاء المؤسسي والأمن القومي الشامل والنمو.
- صياغة ميثاق أخلاقيات قائد التحول الكمي لدعم النزاهة والقدوة في كافة المستويات القيادية والوطنية.

اليوم الثاني :

السيادة التقنية وهندسة الخوارزميات المقاومة للكم(PQC Algorithms)

تصفير مخاطر الاختراق عبر التشفير القائم على الشبكات (Lattice-based) والذكاء الاصطناعي

- استعراض خوارزميات NIST المعتمدة) مثل CRYSTALS-Kyber) وتصفير احتمالات الضعف التقني بنزاهة.
- حماية "القنوات الاتصالية السيادية" عبر تقنيات التوقيع الرقمي المقاوم للكم) مثل.Dilithium)
- تطبيق الهوية الرقمية للمفاتيح التشفيرية لتصفير الهدر البيروقراطي في إجراءات التجديد والتدقيق.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي لحالة "المرونة التشفيرية."

حوكمة الأنظمة الخوارزمية والنزاهة في "المرونة التشفيرية(Crypto-agility) "

- إدارة المسؤولية البشرية القيادية عند استخدام أنظمة التحليل الآلي في تبديل البروتوكولات الأمنية.
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في تقدير مستويات الأمان.
- ترسيخ مفهوم الأمانة في اختيار المعايير التقنية لضمان المصداقية أمام صانع القرار والسيادة والتميز.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات التشفير بنزاهة تامة والنمو.

اليوم الثالث :

هندسة الانتقال والحياد في إدارة الأنظمة الهجينة والشمولية

تصفير البيروقراطية في "البروتوكولات الهجينة (Hybrid Protocols) "والشمولية الرقمية

- هندسة الأنظمة التي تجمع بين التشفير التقليدي والكمي لتصفير مخاطر الانتقال المفاجئ بنزاهة وشفافية.
- تفعيل الرقابة الأخلاقية على منصات تبادل المفاتيح لضمان حياد النظم الرقمية والتميز والنمو الشامل.
- تطبيق تقنيات "توزيع المفاتيح الكمية (QKD) "لتصفير فجوات التنصت على الألياف البصرية السيادية.
- حساب معامل الثقة في مؤشرات الإنجاز الأمني لتقليل احتمالات الخطأ الناتج عن الفجوات التقنية.

المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية الشاملة

- حوكمة الشراكات مع مراكز الأبحاث العالمية لضمان توافقها مع معايير جودة الحياة والسيادة والنزاهة.
- تطوير آليات رصد الأثر الاجتماعي والاقتصادي للتحول الكمي لضمان النزاهة والعدالة والتميز والنمو.
- بناء سجلات نزاهة رقمية لكل تحديث في خوارزميات التشفير الحكومية لضمان الشفافية والوضوح والريادة.
- تمرين محاكاة لإدارة حوار استراتيجي حول "السيادة التشفيرية" بأسلوب قيادي واثق وملهم للشركاء.

اليوم الرابع :

المسؤولية المهنية وإدارة السمعة والنزاهة في عصر الحواسيب الكمومية

القيادة الاتصالية وحماية السمعة الرقمية للجاهزية الوطنية الشاملة

- أخلاقيات التواصل عند الكشف عن "ثغرات كمية" في الأنظمة القديمة والموازنة بين الإبهار والوقار والنزاهة.
- الرقابة على البصمة الرقمية للأنظمة التشفيرية لتعزيز مصداقية القرار السيادي عالمياً والريادة والتميز.
- بناء أنظمة الإفصاح الاستباقي عن كفاءة "الحصانة الكمية" لتصفير فرص انتشار الشائعات والنزاهة والشفافية.
- التدقيق الأخلاقي على سلاسل توريد البرمجيات التشفيرية لضمان خلوها من الممارسات الضارة والسيادة.

حصانة المنظومة السيادية ضد الانتهاكات المعلوماتية والتلاعب بالنتائج

- المسؤولية القيادية في التبليغ عن الثغرات التي قد تهدد أمن بنك معلومات التشفير والسيادة والريادة.
- مهارات التواصل الأخلاقي عند حدوث خطأ في "ترقية التشفير" لضمان استعادة الثقة ببيانات صادقة ونزيهة.
- إدارة التعافي المؤسسي وإعادة بناء الصورة الذهنية بعد رصد أي انحراف في قيم العمل الرقمي والتميز.
- بناء خطة الحصانة المنظومية الشاملة لتحصين نتائج الرصد ضد التلاعب الممنهج بالبيانات والواقع الرقمي.

اليوم الخامس :

خارطة الطريق وصناعة القائد الرقمي "Quantum-Ready" القدوة: من تأمين الأسرار إلى هندسة السيادة التشفيرية الشاملة

هندسة "النبض الاستراتيجي" والرشاقة السيادية في الأمن الكمي

- مصفوفة "النبض اللحظي" للجاهزية الكمية: تصميم نظام رصد سيادي يعتمد على الذكاء الاصطناعي لتحويل بيانات "المرونة التشفيرية" (Crypto-agility) إلى نبضات استراتيجية تظهر للقائد فوراً. يهدف النظام إلى تصفير زمن الكشف عن الخوارزميات الضعيفة وضمان الترقية التلقائية للمفاتيح بنزاهة ومصداقية تامة لمواجهة استراتيجية "احصد الآن وفك التشفير لاحقاً".
- بروتوكول "الرشاقة السيادية" للتحول التشفيري اللحظي: هندسة مسار قرار "صفري الإجراءات" يسمح للمنظومة بتبديل الخوارزميات الكلاسيكية بأخرى مقاومة للكم (مثل Lattice-based) فور رصد النبضة الاستراتيجية للتهديد. يضمن هذا البروتوكول استمرارية حماية الأسرار الوطنية دون قيود بيروقراطية أو انتظار للاعتمادات الإدارية التقليدية التي قد تستغرق سنوات.
- حوكمة "الصدق التشفيري" والنزاهة السيادية: وضع ضوابط أخلاقية تضمن خلو المعايير الوطنية للتشفير من "الثغرات المتعمدة" أو الانحيازات الرقمية، وتفعيل ميثاق "النزاهة في إدارة المفاتيح" لضمان استقلال القرار الأمني القومي والوضوح التام أمام صانع القرار.
- مختبر "هندسة الحصانة ضد اليوم صفر للكم": تمرين محاكاة متقدم لاختبار قدرة القائد على إدارة "نبضة أزمة" ناتجة عن كسر مفاجئ لمعايير التشفير الحالية، وكيفية تفعيل "التوزيع الكمي للمفاتيح" (QKD) لحماية القنوات السيادية الحساسة.

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية حصانة كمية تضمن نزاهة التعامل مع البيانات والبيئات الوطنية بنسبة %.100
- القدرة على هندسة منظومات تشفير رشيقة وسيادية تتوافق مع معايير الريادة والتميز العالمية الشاملة.
- إتقان أدوات الرقابة الأخلاقية على الأنظمة الذكية لضمان الشفافية وتصفير مخاطر الانحياز الرقمي في النتائج.
- بناء سجل ممارسات فضلى في إدارة الذكاء الاستراتيجي للتحول الكمي يدعم اتخاذ القرار القيادي الآمن والمستدام.

الفئة المستهدفة:

- القيادات العليا ومدراء الأمن السيبراني، وتقنية المعلومات، والاتصالات الحكومية والسيادية.
- مسؤولو التميز المؤسسي وفرق تصفير البيروقراطية والتحول الرقمي في القطاعات الاستراتيجية.
- خبراء الحوكمة والنزاهة والرقابة التقنية المعنيون بضبط جودة الأمن القومي الرقمي.
- مهندسو التشفير ومحللو المخاطر السيبرانية في الهيئات الاتحادية والمحلية.

أساليب التدريب:

يتم استخدام بعض من الأساليب التالية أو الكل حسب المتطلبات لكل تخصص :

- دراسة الحالة المعقدة (Complex Case Studies)
- المحاكاة والألعاب الاستراتيجية (Simulation and War Gaming)
- ورش العمل القائمة على التفكير التصميمي (Design Thinking Workshops)
- حلقات النقاش مع خبير من القطاعين العام أوالخاص.(Expert Panels)
- المختبرات التقنية التفاعلية (Interactive Technology Labs)
- التعلم من الأقران عبر الجهات الحكومية (Inter-Agency Peer Learning)
- نهج التعلم المدمج والمستمر (Blended & Continuous Learning Approach)