الاستعداد لعصر ما بعد الكوانتم وتأمين المعلومات للمستقبل

الإمارات العربية المتحدة - دبي

26 – 30/ 07 / 2026

مقدمة:

في عام 2026، ومع القفزات الهائلة في الحوسبة الكمومية، لم يعد التهديد نظرياً بل أصبح واقعاً يمس عمق السيادة الوطنية. إن تقنيات التشفير التي نعتمد عليها اليوم قد تصبح هشة أمام "اليوم صفر للكم" (Q-Day). يهدف هذا البرنامج إلى تمكين القادة من أدوات استباق المستقبل، وتوظيف التشفير ما بعد الكوانتم (PQC) لتصفير البيروقراطية في تحديث الأنظمة، وضمان النزاهة المطلقة للأسرار الوطنية في وجه القوى الحسابية الخارقة، مما يرسخ ريادة الدولة كحصن رقمي منيع للمستقبل.

أهداف الدورة:

- استيعاب حجم التهديد الكمي على أنظمة التشفير الحالية ومفهوم "احصد الآن وفك التشفير لاحقاً."
- تطوير مهارات هندسة "المرونة التشفيرية (Crypto-agility) "لضمان التحديث التلقائي دون بيروقراطية.
- إتقان فن التحول نحو الخوارزميات المقاومة للكم (Lattice-based, Code-based) بنزاهة وشفافية.
- حوكمة ممارسات الأمن الكمي لضمان التوازن بين الانفتاح التقني وبين حماية الأصول السيادية.
- تعزيز السيادة المعلوماتية عبر بناء معايير وطنية مستقلة للتشفير المقاوم للكم.
- تطبيق استراتيجيات القيادة في إدارة "التحول الكبير" وضمان المصداقية والسمعة الدولية الشاملة.

محتويات الورشة:

اليوم الأول :

فلسفة الأمن في عصر الكوانتم والرشاقة الاستراتيجية

هندسة الحصانة المستقبلية وتصفير البيروقراطية في تقييم الجاهزية

- مفهوم "السيادة الكمية" 2026 وأثره على الأمن القومي وجودة الحياة والنمو والتميز العالمي.
- مواءمة استراتيجيات التشفير مع مبدأ تصفير البيروقراطية عبر الأتمتة الذكية لجرد الأصول التشفيرية.
- تحليل العلاقة بين "الأمن الكمي الاستباقي" وبين بناء الثقة والمصداقية الدولية في الاقتصاد الرقمي.
- تمرين هندسة الاستباقية لتصميم خارطة طريق تصفّر زمن الكشف عن نقاط الضعف بنزاهة وشفافية.

قيادة النزاهة في حوكمة "الأسرار السيادية" والريادة الوطنية الشاملة

- تعزيز السيادة على المفاتيح التشفيرية الوطنية لضمان استقلاليتها وتوافقها مع القيم والهوية.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في اختيار تقنيات التشفير الجديدة.
- بناء ثقافة "الأمان المستدام" وعلاقتها بالولاء المؤسسي والأمن القومي الشامل والنمو والريادة.
- صياغة ميثاق أخلاقيات قائد التحول الكمي لدعم النزاهة والقدوة في كافة المستويات القيادية.

اليوم الثاني :

السيادة التقنية وهندسة التشفير ما بعد الكوانتم(PQC)

تصفير مخاطر الاختراق عبر الخوارزميات المقاومة للكم والذكاء الاصطناعي

- توظيف خوارزميات التشفير القائم على "الشبكات (Lattice-based) "وتصفير احتمالات الضعف بنزاهة.
- حماية "البيانات السيادية" عبر أنظمة تشفير وطنية تضمن موثوقية المعلومات والنزاهة الرقمية.
- تطبيق الهوية الرقمية للمفاتيح (Key Identity) لتصفير الهدر البيروقراطي في إجراءات التحديث.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي لحالة "المرونة التشفيرية."

حوكمة الأنظمة الخوارزمية والنزاهة في "المرونة التشفيرية"

- إدارة المسؤولية البشرية القيادية عند استخدام الذكاء الاصطناعي في إدارة سلاسل التشفير المعقدة.
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في تقدير الأمان.
- ترسيخ مفهوم الأمانة في البيانات المستقاة من رصد التهديدات الكمية لضمان المصداقية والسيادة.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات التشفير بنزاهة تامة.

اليوم الثالث :

هندسة الانتقال الهجين والحياد في إدارة الأنظمة والشمولية

تصفير البيروقراطية في "بروتوكولات التشفير الهجين" والشمولية الرقمية

- هندسة الأنظمة التي تجمع بين التشفير الكلاسيكي والكمي لتصفير مخاطر الانتقال المفاجئ بنزاهة.
- تفعيل الرقابة الأخلاقية على منصات تبادل المفاتيح لضمان حياد النظم الرقمية والتميز والنمو.
- 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 المختبرات العالمية لضمان توافقها مع معايير جودة الحياة والسيادة والنزاهة.
- تطوير آليات رصد الأثر الاجتماعي والاقتصادي للتحول الكمي لضمان النزاهة والعدالة والنمو.
- بناء سجلات نزاهة رقمية لكل عملية تحديث للتشفير الحكومي لضمان الشفافية والوضوح والريادة.
- تمرين محاكاة لإدارة حوار استراتيجي حول "السيادة والكم" بأسلوب قيادي واثق وملهم للشركاء.

اليوم الرابع :

المسؤولية المهنية وإدارة السمعة والنزاهة في عصر الكم

القيادة الاتصالية وحماية السمعة الرقمية للجاهزية الوطنية الشاملة

- أخلاقيات التواصل عند الكشف عن "ثغرات كمية" في الأنظمة القديمة والموازنة بين الإبهار والوقار.
- الرقابة على البصمة الرقمية للأنظمة التشفيرية لتعزيز مصداقية القرار السيادي عالمياً والريادة والنمو.
- بناء أنظمة الإفصاح الاستباقي عن كفاءة "الحصانة الكمية" لتصفير فرص انتشار الشائعات والنزاهة.
- 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.
- إدارة التعافي المؤسسي وإعادة بناء الصورة الذهنية بعد رصد أي انحراف في قيم العمل والنزاهة.
- بناء خطة الحصانة المنظومية الشاملة لتحصين نتائج الرصد ضد التلاعب الممنهج بالبيانات والواقع.

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 للوطن.

الفئة المستهدفة:

- القيادات العليا ومدراء الأمن السيبراني، وتقنية المعلومات، والاتصالات في الهيئات الحكومية والسيادية.
- مسؤولو التخطيط الاستراتيجي والتميز المؤسسي وفرق تصفير البيروقراطية في القطاعات الحيوية.
- خبراء الحوكمة والنزاهة والرقابة التقنية المعنيون بحماية بنوك البيانات الوطنية والسيادة.
- رؤساء فرق المهام الخاصة ومحللو التهديدات المستقبلية في المؤسسات 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)