استراتيجيات مكافحة الجريمة المنظمة العابرة للحدود والتهديدات الهجينة

الإمارات العربية المتحدة - دبي

2026 / 04 /30 – 26

مقدمة:

في عالم مترابط ومعقد، لم تعد الجريمة مجرد فعل محلي، بل تحولت إلى شبكات عابرة للحدود تدمج بين الجرائم التقليدية والتهديدات الهجينة التي تستهدف استقرار الدول. يهدف هذا البرنامج إلى تمكين القادة من أدوات "الأمن الاستباقي" وتوظيف الذكاء الاصطناعي لتصفير البيروقراطية في ملاحقة الشبكات الإجرامية، مع ضمان أعلى معايير النزاهة والشفافية في حماية السيادة الرقمية والوطنية، مما يعزز ريادة الدولة كواحة للأمن والأمان العالمي في عام 2026.

أهداف الدورة:

- استيعاب المفاهيم الحديثة للتهديدات الهجينة (Hybrid Threats) وعلاقتها بالسيادة الرقمية.
- تطوير مهارات هندسة العمليات الاستخباراتية المشتركة لتفكيك شبكات الجريمة المنظمة.
- إتقان فن توظيف الذكاء الاصطناعي في رصد أنماط غسل الأموال والجرائم السيبرانية العابرة للحدود.
- حوكمة العمليات الأمنية لضمان التوازن بين سرعة الاستجابة وبين المتطلبات القانونية السيادية.
- تعزيز السيادة المعلوماتية عبر بناء منظومات رصد وطنية ذكية تصفّر زمن الكشف عن التهديدات.
- تطبيق استراتيجيات القيادة في إدارة الأزمات الأمنية المعقدة وضمان الشفافية والمصداقية الدولية.

محتويات الورشة:

اليوم الأول :

فلسفة الأمن السيادي والرشاقة في مواجهة الجريمة المنظمة

هندسة الحصانة الوطنية وتصفير البيروقراطية في الملاحقة

- مفهوم الجريمة المنظمة 2.0 وأثر التهديدات الهجينة على السيادة الرقمية والوطنية.
- مواءمة استراتيجيات المكافحة مع مبدأ تصفير البيروقراطية عبر أتمتة تبادل المعلومات بين الأجهزة.
- تحليل العلاقة بين "الأمن الرشيق" وبين بناء الثقة والمصداقية الدولية في النموذج الأمني للدولة.
- تمرين هندسة الاستجابة الاستباقية لتصميم دورة عمل أمنية تصفّر زمن تفكيك الشبكات بنزاهة وشفافية.

قيادة النزاهة في حوكمة التعاون الأمني الدولي والريادة

- تعزيز السيادة على القرارات الأمنية لضمان استقلاليتها وتوافقها مع القيم والهوية والنمو.
- دور القائد في حماية صورة المؤسسة عبر ممارسات النزاهة في ملاحقة الجرائم العابرة للحدود.
- بناء ثقافة "الأمن كمحرك للتنافسية" وعلاقتها بجودة الحياة والريادة العالمية الشاملة.
- صياغة ميثاق أخلاقيات قائد مكافحة الجريمة المنظمة لدعم النزاهة والتميز في كافة المستويات.

اليوم الثاني :

السيادة التقنية وهندسة الاستخبارات الرقمية التنبؤية

تصفير التهديدات عبر التحليلات الذكية والربط المنظومي

- توظيف الذكاء الاصطناعي في رصد التدفقات المالية المشبوهة وتصفير مخاطر غسل الأموال بنزاهة.
- حماية "البيانات الأمنية السيادية" عبر أنظمة تشفير وطنية لضمان موثوقية المعلومات والنتائج.
- تطبيق الهوية الرقمية في تتبع الأنشطة الإجرامية لتصفير الهدر البيروقراطي في إجراءات التدقيق والتحري.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي للتهديدات العابرة للحدود.

حوكمة الأنظمة الخوارزمية والنزاهة في التحليل الجنائي

- إدارة المسؤولية البشرية القيادية عند استخدام أنظمة التحليل الآلي في تحديد بؤر الجريمة.
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في تقدير التهديدات.
- ترسيخ مفهوم الأمانة في البيانات المستقاة من الذكاء الاصطناعي لضمان المصداقية أمام صانع القرار.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات الأمن القومي بنزاهة تامة.

اليوم الثالث :

التهديدات الهجينة والحياد في إدارة الأمن المجتمعي

هندسة الحماية ضد التضليل والشمولية الرقمية في الوعي

- استخدام التحليلات الذكية لضمان عدالة حماية جميع فئات المجتمع من التهديدات الهجينة بنزاهة.
- تفعيل الرقابة الأخلاقية على منصات رصد الخطاب المتطرف لضمان الشفافية وحياد البيانات الرقمية.
- تطبيق قاعدة الإرادة البشرية القيادية للتدخل وتعديل مسارات المواجهة التي قد تغفل البعد الإنساني.
- حساب معامل الثقة في مؤشرات الإنجاز الأمني لتقليل احتمالات الخطأ الناتج عن الفجوات التقنية.

المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية

- حوكمة الشراكات مع القطاع الخاص لضمان توافق الأنظمة الأمنية مع معايير جودة الحياة والسيادة.
- تطوير آليات رصد الأثر الاجتماعي للسياسات الأمنية لضمان النزاهة والعدالة في حماية الأفراد.
- بناء سجلات نزاهة رقمية لكل عملية مكافحة كبرى لضمان الشفافية المطلقة والوضوح التام والتميز.
- تمرين محاكاة لإدارة حوار وطني رقمي حول "الأمن الهجين" بأسلوب قيادي واثق وملهم للجمهور.

اليوم الرابع :

المسؤولية المهنية وإدارة السمعة في الأزمات الأمنية

القيادة الاتصالية وحماية السمعة الرقمية للجاهزية الوطنية

- أخلاقيات التواصل في الأزمات الأمنية المتسارعة والموازنة بين الإبهار وبين الوقار السيادي الحكومي.
- الرقابة على البصمة الرقمية للالتزام الأمني وأثرها في تعزيز مصداقية القرار السيادي عالمياً والريادة.
- بناء أنظمة الإفصاح الاستباقي عن إحباط العمليات الإجرامية لضمان الشفافية وتصفير الشائعات.
- التدقيق الأخلاقي على سلاسل توريد التقنيات الأمنية لضمان خلوها من الممارسات الضارة أو التجسسية.

حصانة الأنظمة السيادية ضد الانتهاكات المعلوماتية والتلاعب

- المسؤولية القيادية في التبليغ عن الثغرات التقنية التي قد تهدد أمن بنك المعلومات الأمني والسيادة.
- مهارات التواصل الأخلاقي عند حدوث عطل في منظومات الرصد لضمان استعادة الثقة ببيانات صادقة.
- إدارة التعافي المؤسسي وإعادة بناء الصورة الذهنية بعد رصد أي انحراف في قيم العمل الرقمي والمهني.
- بناء خطة الحصانة المنظومية الشاملة لتحصين نتائج العمل الأمني ضد التلاعب الممنهج بالحقائق.

اليوم الخامس :

مختبر الابتكار المهني وصناعة نموذج "الأمن الاستباقي" الريادي

التطبيق العملي وتصفير البيروقراطية في أنظمة الملاحقة والتميز المؤسسي

- تطوير خارطة الطريق التنفيذية لدمج أدوات الاستخبارات التنبؤية في العمليات الأمنية اليومية بمرونة ورشاقة تضمن تفكيك الشبكات الإجرامية والتميز والنمو المستدام.
- تصميم بروتوكولات الحوكمة الذكية الخاصة بـ التعاون الأمني العابر للحدود لتصفير المسارات البيروقراطية وضمان النزاهة والشفافية والوضوح في تبادل البيانات اللحظية والريادة العالمية.
- منهجية صياغة ملفات التميز للمنافسة في الجوائز الوطنية (مثل جوائز وزير الداخلية للتميز، وجوائز الحوكمة الرقمية) مع التركيز على الابتكار في "تصفير الجريمة المنظمة" والرشاقة والوضوح.
- تمرين مختبر المحاكاة لإدارة التهديدات الهجينة المعقدة (مثل الهجمات السيبرانية المتزامنة مع عمليات غسل أموال رقمية) وصياغة الحلول الاستباقية الناجحة والتميز في الأداء والسيادة.

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية حصانة أمنية تضمن نزاهة التعامل مع البيانات والمشاريع الوطنية بنسبة 100%.
- القدرة على هندسة منظومات مكافحة رشيقة وسيادية تتوافق مع متطلبات 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 الأمني الاستراتيجي يدعم اتخاذ القرار القيادي الآمن والمستدام.

الفئة المستهدفة:

- القيادات العليا ومدراء الإدارات في أجهزة مكافحة الجريمة المنظمة والأمن الوطني.
- مسؤولو التحريات المالية والجمارك وفرق التميز المؤسسي في القطاعات الأمنية.
- خبراء التحول الرقمي والحوكمة والنزاهة المعنيون بتطوير منصات الرصد الأمني.
- رؤساء فرق المهام الخاصة ومحللو التهديدات الهجينة 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)