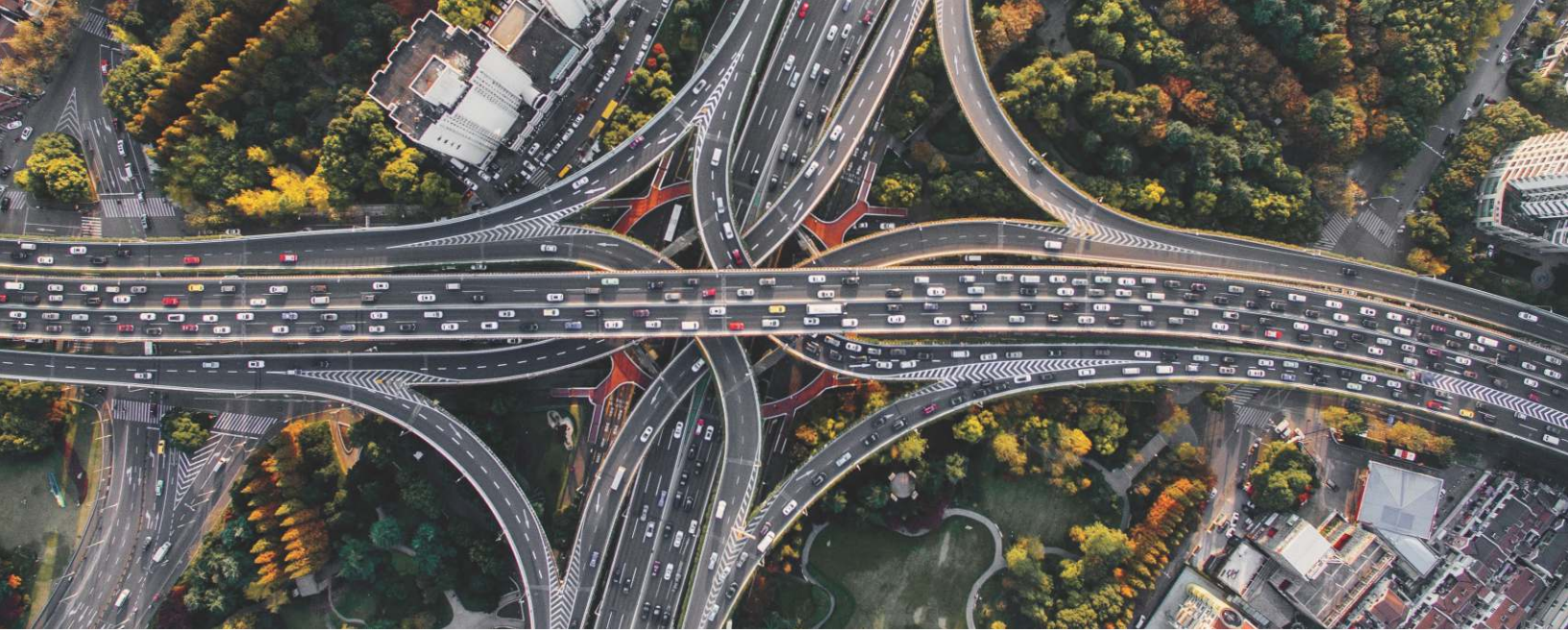
LOS DESAFÍOS DE LA VIGILANCIA Y CONTROL

COMO IMPULSAR EL CAMBIO A TRAVÉS DE LA TECNOLOGÍA

Conclusiones Tercera mesa redonda de Cityforum
BT Centre, Newgate Street, Londres

MOTOROLA SOLUTIONS



Prólogo

La comunidad que conforma la seguridad pública debe afrontar cada vez más desafíos: hacer más con menos, administrar la transición tecnológica y tener la capacidad de convertir grandes volúmenes de datos en inteligencia, una mayor eficiencia operativa y mejores resultados.

De la transformación tecnológica pueden surgir soluciones que ayuden a ahorrar tiempo, optimizar la eficiencia y proporcionar importantes beneficios para distintas áreas.

Modernizar los servicios de emergencia con los datos adecuados, los equipos indicados e innovaciones inteligentes puede ayudar a aliviar parte de la carga. La automatización podría activar una serie de acciones para agilizar los tiempos de respuesta e identificar tendencias y comportamientos analizando los grandes volúmenes de datos comúnmente compartidos abiertamente por la comunidad a fin de detectar las amenazas más significativas y prioritarias. Siempre que el proceso de transformación incluya un nivel de Inteligencia Artificial (IA), podríamos incluso ser capaces de prever incidentes antes de que ocurran.

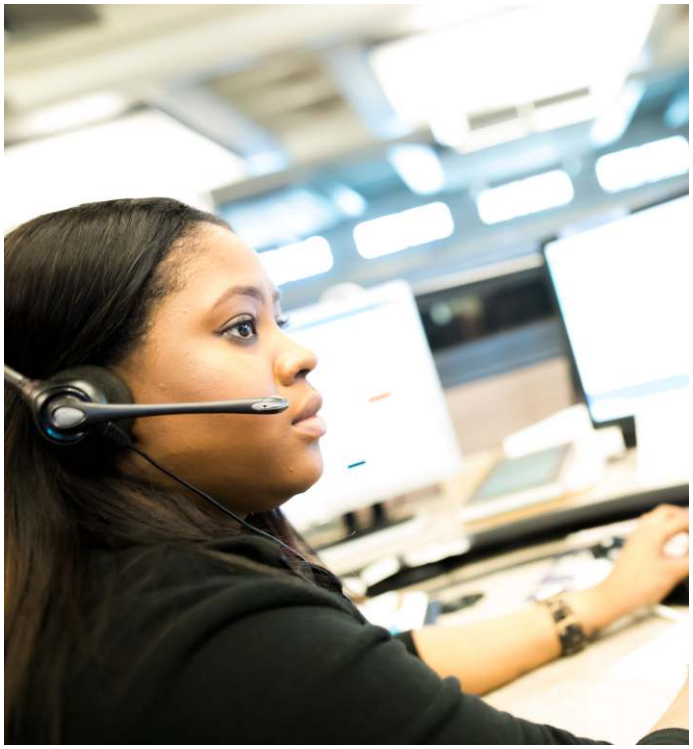
Para que esto suceda, las organizaciones de seguridad pública no solo deben contar con las mejores herramientas y los datos que les permitan satisfacer sus necesidades en constante cambio, sino que también necesitan un socio con los conocimientos y la experiencia suficientes para capacitar gente en el uso de dichas herramientas y en la identificación de maneras de trabajar inimaginables hasta ahora. Y ayudar a las fuerzas a abordar las necesidades de vigilancia y control de sus comunidades, sin desatender las amenazas a nivel nacional.

Por David Robinson, Motorola Solutions.

UN DÍA DE DEBATE, DIÁLOGO Y DECISIONES

La tercera Conferencia sobre Vigilancia y Control Digital de Cityforum logró reunir oficiales de policía, CIO de policía, proveedores de tecnología y especialistas del mundo de la vigilancia y empresarial. La discusión se llevó a cabo bajo la regla de Chatham House, dando lugar a la libre expresión de opiniones, expectativas y preocupaciones. Este resumen del evento intenta reflejar los temas tratados y el clima que se vivió en un día de debate intenso.

La tecnología avanza rápidamente, así como el servicio ante oportunidades o amenazas repentinas. La realidad es que, desde aquella primera conferencia sobre Vigilancia y Control Digital, las fuerzas han logrado mucho, especialmente en lo que respecta a la movilización del flujo de trabajo y a la captura de imágenes. No obstante, los desafíos que deben afrontar las fuerzas policiales y las barreras que impiden la transformación podrían parecer insuperables. Tal como remarcara uno de los participantes, el riesgo es querer "sacarle brillo" a un mismo problema una y otra vez, en lugar de buscar soluciones.



Los desafíos que deben afrontar las fuerzas policiales y las barreras que impiden la transformación podrían parecer insuperables.

¿CÓMO COMPROMETER AL PÚBLICO, CENTRÁNDOSE EN LA VÍCTIMA?

El crecimiento de los delitos informáticos y el surgimiento de nuevas amenazas digitales constituyen factores impulsores determinantes para la demanda inédita de una verdadera transformación de los procesos de vigilancia y control basados en tecnología.

Los oficiales veteranos ya están en la cuerda floja tratando de encontrar el equilibrio ideal entre atender la demanda de vigilancia y control por parte de la comunidad y abordar las amenazas del terrorismo y el crimen organizado. Están decididos a que el servicio policial debe mantenerse a la altura de las principales preocupaciones de la ciudadanía abordando los nuevos vectores de amenazas en línea que van surgiendo. No abordar eficientemente estas nuevas formas de victimismo implicaría desafiar la confianza ciudadana, quizás hasta llegar a erosionar las percepciones de legitimidad. Los delegados propusieron ciertas preguntas fundamentales acerca del rol que podría cumplir el servicio. Se acordó que nuestro modelo reactivo de vigilancia y control es claramente insuficiente ante el uso de imágenes utilizadas para fines de acoso y chantaje, la magnitud del grooming vía Web y la industrialización del delito económico.

¿ACASO LA SOLUCIÓN SERÍA UN ENFOQUE PROACTIVO PARA IMPEDIR LA ACTIVIDAD MALICIOSA?

La definición de nuevas medidas legislativas y operativas implica una mayor comprensión de la vulnerabilidad digital por parte de la política y del público en general. Es decir, el enfoque de vigilancia y control que se adopte debe comunicar un mensaje claro y coherente sobre las amenazas en línea, las posibilidades que se tienen de abordarlas, y las implicaciones éticas de todo este proceso. El mensaje y el enfoque deben estar formulados en términos claros y relevantes, lo que puede resultar complejo para un servicio centrado en tareas, y sumido siempre en los conceptos tradicionales de criminalidad y victimismo. Ninguno de los oradores subestimó la dificultad de diseñar nuevos modelos de vigilancia y control digital bajo el escrutinio de políticos y socios; todos estuvieron de acuerdo en que sería esencial contar con el consentimiento de estos.

DEMANDA Y CONTROL

El tema claramente dominante en la discusión sobre el cambio en la naturaleza de la demanda fue lo relacionado con las salas de control. Se remarcó que las amenazas y los riesgos más recientes –estén o no asociados al ciberdelito– pueden afectar considerablemente el tiempo que lleva procesar y clasificar incidentes. A los delegados se les advirtió que no deberían esperar que las iniciativas de cambio de canal ayuden a reducir la carga de la sala de control. La innovación en la generación de informes de incidentes no necesariamente debería estar ligada a proyecciones de eficiencia optimistas.

LA NECESIDAD DE CREDIBILIDAD FINANCIERA

Es imposible no hablar de dinero al discutir la transformación del proceso de vigilancia y control.
Es cierto que los argumentos bien fundados pueden llegar a influenciar clases políticas y analistas, lo que hace aún más evidente la necesidad de tener siempre un discurso coherente en lo referente a modelos operativos digitales. Pero para argumentar eficientemente a favor de la inversión digital en tiempos de austeridad, debe mejorarse la manera de articular los beneficios económicos asociados a los procesos de vigilancia y control.

Si bien los objetivos de cambio cultural constituyen un componente clave de la digitalización policial, el impacto financiero es sumamente difícil de evaluar. Muchos de los programas son esencialmente preventivos, y es difícil presentar prueba de beneficios cuando no hay ningún otro escenario simulado alternativo. Los casos de beneficios suelen formularse en base a suposiciones acerca del impacto sobre la dotación de personal, que luego quedan sin efecto.

El servicio es razonablemente bueno a la hora de definir objetivos de inicio, pero no tanto a la hora de evaluar los avances, los logros y el contexto más amplio, lo que significa que el potencial y el alcance de los beneficios pueden diferir considerablemente de las suposiciones iniciales, aun cuando los programas arrojaran resultados viables.

Son desafíos complejos, y esta cuestión más amplia de la profesionalización o tercerización del desarrollo de proyectos podría proporcionar algunas de las respuestas. Un participante de otra área de gobierno les recordó a los delegados que es mucho más probable alcanzar los resultados financieros fijados con proyectos más pequeños que con planes grandiosos y a largo plazo. Es un consejo útil. Pero el norte debe ser la consolidación de un sinfín de iniciativas. En vigilancia y control digital se debe poder hablar con sensatez de números grandes.

Debe mejorarse la manera de articular los beneficios económicos asociados a los procesos de vigilancia y control.

EXISTE LA COLABORACIÓN, AUNQUE PUEDE SER DESIGUAL

El concepto de departamentos de ICT (Tecnologías de la Información y la Comunicación) compartidos no es nuevo, como tampoco lo es el de grupos de fuerzas definidos por sus preferencias de aplicaciones. Lo que ha mejorado es la capacidad general de conducir alianzas, identificar un número razonable de interesados y tomar decisiones en consecuencia, especialmente por parte de los oficiales veteranos con responsabilidades a nivel nacional.

EL CONSENSO TECNOLÓGICO Y EL FIN DEL LEGADO

Existe un optimismo perceptible respecto de la capacidad de los líderes de ICT a proporcionar la tecnología requerida para los procesos de vigilancia y control digital, y de optimizar al máximo los presupuestos para ICT asignados al servicio. El nivel de frustración por la proporción del gasto asociado al mantenimiento de sistemas sigue siendo alto, pero la discusión acerca de la meta fijada parece haber sido ganada.

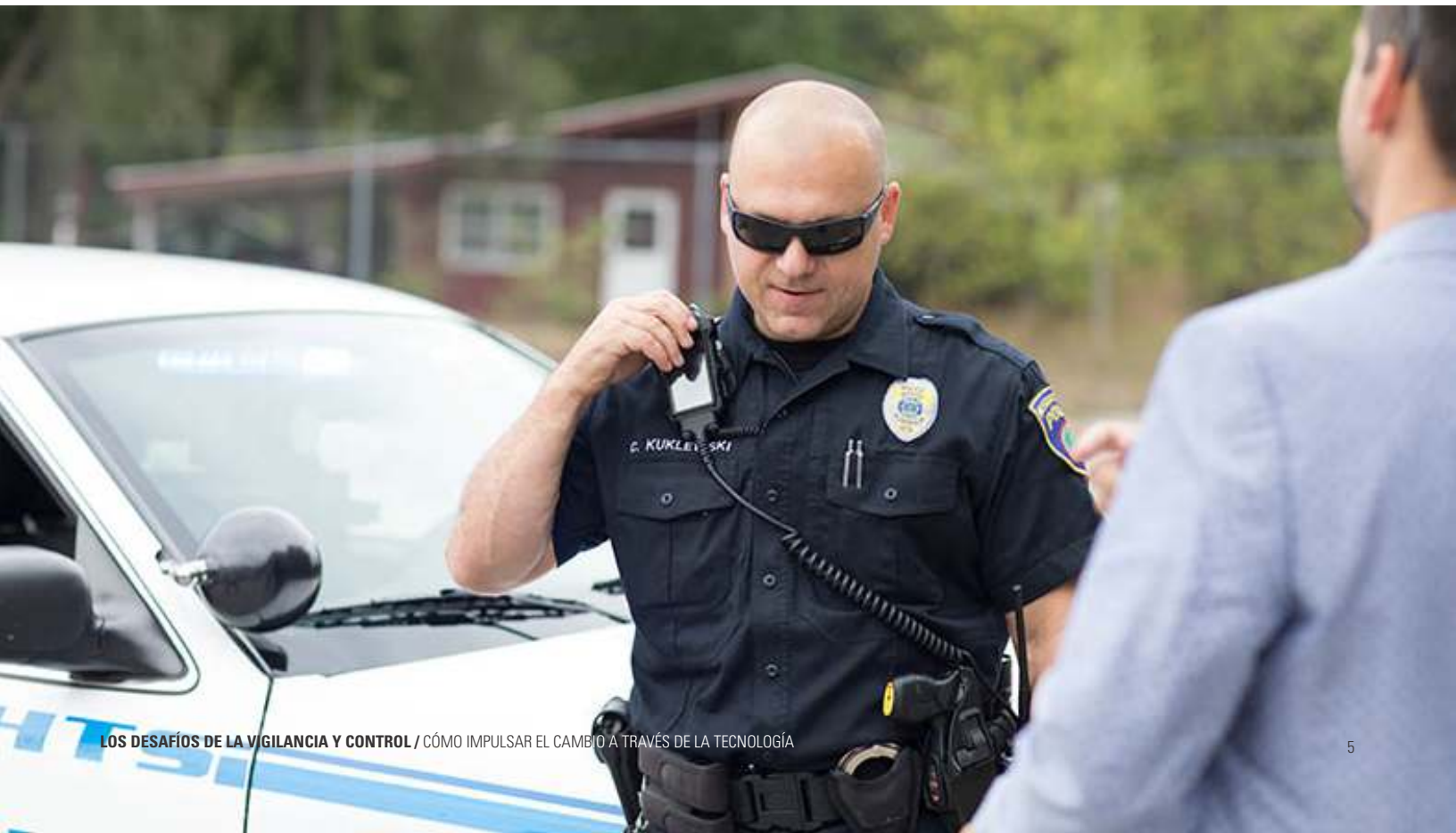
Algunas fuerzas ya hace tiempo se han embarcado en este viaje a una tecnología basada en la nube y entrega de aplicaciones rápida y con capacidad de respuesta. Están conformes con su estrategia, pero advierten que los costos iniciales de la transición al modelo de nube son altos. Los pares del sector público algo más adelantados en el camino aportaron cierto grado de tranquilidad.

Se requieren estrategias de administración de datos independientes de la aplicación, quizás reguladas por el principio que afirma que "los nuevos datos son los metadatos".

El ahorro que representa la transición de aplicaciones ligadas a servicios basados en la nube se verá mejor cuando se logren eliminar por completo los sistemas anteriores. Las nuevas plataformas serán mucho más efímeras que los gigantes que vienen a reemplazar. No obstante, son los datos propiamente dichos los que pueden ser de utilidad a largo plazo, a medida que van surgiendo oportunidades de estudios analíticos. Esto significa que se requieren estrategias de administración de datos independientes de la aplicación, quizás reguladas por el principio que afirma que "los nuevos datos son los metadatos".

PRESUPUESTOS EN LA ERA DIGITAL

Lógicamente, ni los representantes de la industria ni los líderes de ICT aplicadas a las fuerzas policiales admitirían la idea de reducir el gasto en tecnología a fin de liberar fondos para inversión en primera línea. Tampoco considerarían el presupuesto total de tecnología asignado a la fuerza como un sustituto valioso para lograr la eficiencia que necesitan. Sería



una idea insostenible en el tiempo, a medida que los costos de la tecnología se van desplazando de inversión de capital a gastos operativos, cada vez más asociados a los individuos y las herramientas que emplean. Tanto políticos como oficiales expertos parecen coincidir en esto. Pero si bien la inversión en tecnología parece segura, queda claro que el camino más simple para el financiamiento de las nuevas iniciativas de vigilancia y control digital yace en poder ahorrar parte del presupuesto actual asignado a las ICT.

Esta cuestión presupone un problema práctico para los líderes tecnológicos. Para los procesos de vigilancia y control digital se requieren nuevos enfoques tecnológicos, que pueden tomarse de las arquitecturas ágiles y flexibles del mundo digital. Esta clase de desarrollo de aplicaciones evita gran parte del costo inicial, y está vista como una alternativa sensata y austera a los programas complejos y poco flexibles con mucho riesgo político asociado. No obstante, hay ciertos costos significativos asociados a la transición a los modelos de infraestructura y dotación de personal implícitos en el nuevo escenario, costos cuya recuperación puede llevar tiempo. Sin un nuevo financiamiento –o aumento considerable en los preceptos– a muchos de los jefes de área de ICT se les hará muy difícil cumplir con los requerimientos de inversión en tecnología que los programas nacionales exigirán para los próximos años.

LA TERCERIZACIÓN COMO POSIBILIDAD: LA INDUSTRIA Y LOS CAMBIOS EN EL ÁREA

A los tecnólogos de las fuerzas policiales no sólo les preocupa cómo financiar el cambio en sus propias jurisdicciones. También les preocupa la capacidad del servicio para aprovechar los beneficios de las nuevas plataformas digitales. Los aportes que sugerían que las áreas de vigilancia y control necesitan cierta ayuda externa con el cambio y las tecnologías provinieron tanto de participantes abocados al área como de representantes de firmas de servicios empresariales.

¿Cuáles son las capacidades que la vigilancia y el control podrían no tener? Uno de los asistentes se refirió a la diferencia entre la manera en que los oficiales expertos administran los incidentes reales y la eficiencia con la que logran controlar el cambio en su organización. Hay líderes ejemplares que se toman muy en serio cada aspecto del riesgo siempre que está en juego la seguridad pública y que podrían mostrarse relativamente algo más comprensivos respecto del riesgo de falla en los programas de cambio. Parecen más dispuestos a recurrir a especialistas y aceptar los contratiempos de buena manera. ¿Requiere la transformación policial de un nuevo estilo de liderazgo, decidido y con determinación en la búsqueda de nuevos modelos operativos? ¿O acaso pueden importarse la energía y el enfoque requeridos para impulsar los programas de cambio?

El área de vigilancia y control digital debe ser igual de ágil y receptiva para adaptarse a nuevas amenazas y circunstancias, siempre con los anuncios respectivos para garantizar el apoyo sostenido del público en general y de todos los interesados.

La transferencia de estas capacidades no es nada sencilla. Las diferencias entre la gestión del cambio en vigilancia y control y en otras áreas son muy marcadas. No obstante, la posibilidad de articularlas demuestra la magnitud del desafío, y la escasez de capacidad interna. El control que se tiene en vigilancia y control sobre la demanda es muy limitado en comparación con áreas comerciales. Gran parte de la demanda deriva de la priorización por parte de otros servicios públicos locales. Esto no exime al área de vigilancia y control de la necesidad de analizar y abordar la cuestión de la productividad, pero sí indica que el rendimiento debe ser considerado como parte de un nexo de relaciones y del ecosistema local de servicios. Los pivotes organizacionales del mundo comercial requieren de un mercadeo ágil. El área de vigilancia y control digital debe ser igual de ágil y receptiva para adaptarse a nuevas amenazas y circunstancias, siempre con los anuncios respectivos para garantizar el apoyo sostenido del público en general y de todos los interesados. Es posible que la pericia y los recursos necesarios para cumplir con requerimientos como estos tengan que importarse.

La reforma que la industria exige sobre la fuerza de trabajo generalmente implica la tercerización de ciertas tareas, especialmente las asociadas a funciones de apoyo administrativo y servicios que podrían ser compartidos. La tercerización, tal como la conocemos hoy, se basa fundamentalmente en el arbitraje laboral. El trabajo va adonde la mano de obra es más barata. Aunque, en el futuro, la industria se encaminará rápidamente hacia un modelo basado en la automatización y el aprendizaje automático. El área de vigilancia y control deberá ser ahorrativa –y estar bien asesorada por abogados especializados– a fin de asegurarse de que el ahorro no sea para los proveedores.

Las dudas sobre el modelo de prestación adecuado siguen estando subordinadas al dilema de si los programas de cambio del área deberían ser gestionados a nivel de la fuerza o a nivel nacional. Los defensores de la idea de salir al mercado y conformar un consorcio lo suficientemente grande para que

asuma el riesgo de la transformación tenían la esperanza de que el servicio pudiera consolidar los procesos operativos antes de implementar nuevas plataformas tecnológicas. Este enfoque es consistente con la recomendación de un despliegue más gradual del portafolio de tecnología aplicada a vigilancia y control a nivel nacional.

Aunque un cambio de área a nivel nacional traería aparejadas ciertas complejidades. Un representante del gobierno central remarcó que no hay un buen equilibrio entre la estandarización y la innovación; lo que se exige a nivel nacional suele ser muy flexible, y evita la duplicación de esfuerzos, pero el lado triste de la cuestión es que las soluciones impuestas tienden a fallar. También se sugirió que el sector público como un todo no logra identificar las mejores prácticas y desarrollar los mecanismos adecuados para compartirlas con todo el sistema. Este tema de la vigilancia y el control se tomó como un caso paradigmático, con el proceso de Financiamiento para la Transformación Policial actual visto como una competencia en la que ganaba quien llegaba primero, y no el más apropiado a nivel nacional.

Los especialistas en tecnología reconocen la vigilancia y el control como un proceso humano.

EL IDIOMA COMO PUENTE

La regulación de datos e información aún presenta múltiples desafíos para la armonización del proceso, la colaboración entre organismos y la actividad analítica. Pareció atinado el comentario de que "hay islas de buenas prácticas, pero no hay puentes que las unan".

Si bien hay muy buenas oportunidades para vigilancia y control a través de la armonización de datos que derivan de iniciativas locales, y dependen del apoyo de líderes locales de organismos asociados, hay ejemplos de uso compartido de información a gran escala, y de una comunidad tecnológica que está fomentando las alianzas bilaterales.
Las principales barreras para el uso compartido de información a escala aparecen cuando no se habla un mismo idioma. Las discrepancias en nomenclaturas pueden resolverse, pero las divergencias culturales son más difíciles de conciliar. Es clave el grado de convergencia entre las ideas y preocupaciones del personal experto de vigilancia y control y las de los representantes de la industria tecnológica.

Los especialistas en tecnología reconocen la vigilancia y el control como un proceso humano. Saben que las máquinas no pueden empatizar: que el aprendizaje automático nunca podrá reemplazar la inteligencia emocional del hombre a la hora de abordar a una víctima de violación o a una persona en completo estado de ebriedad y aflicción. La pregunta es cómo escalar lo esencial, lo humano, en vigilancia y control; cómo sacar lo mejor del servicio.

Y esto significa que las perspectivas del proceso, las perspectivas de los datos y las perspectivas de la tecnología exigen una terminología común, y todo en el contexto de un modelo operativo claro. Hay una jerarquía de servicios, capacidades y componentes que ofrece permitirá la articulación de cada uno de los componentes en términos de procedimiento, flujo de trabajo, tecnología y financiación. Esto representa un programa de desarrollo integral para la incorporación de nuevos componentes y capacidades en el entorno operativo y en la pila tecnológica.

Para vigilancia y control digital es fundamental que el servicio pueda articular lo que hace, lo que desea hacer, y lo que más valora para poder apuntar a la industrialización de parte de ello –pero no de todo, en absoluto. La mayor esperanza de lograr esto se basa en un modelo de referencia compartido que derive del servicio, y no impuesto por el centro, o ideado por un asesor, independientemente de la manera en la que eventualmente se aplicare.

Y en cuanto al desafío subyacente para quienes ocupan puestos de responsabilidad: “dejar de ver el desafío digital como un "problema digital", y aprovechar las oportunidades que se presenten para construir una nueva base de aptitudes, conocimiento y práctica para un futuro sumamente innovador en materia de vigilancia y control basado en aplicaciones digitales”. Stephen Kavanagh. Jefe de Policía de Essex y Presidente del Consejo de Vigilancia y Control Digital

CITYFORUM

- Cityforum viene apoyando el debate sobre políticas públicas desde 1990.

- Elabora y publica informes y planifica y organiza eventos en el Reino Unido y, en ciertos casos de invitación especial, en cualquier otra parte del mundo.

- A Cityforum le interesa particularmente el trabajo con las fuerzas policiales y organiza entre tres y cuatro mesas redondas al año para debatir sobre estrategias, tecnología, recursos humanos, el valor del dinero y comunicación estratégica. También asesora a nivel de especialista y monitorea el trabajo de comisionados y jefes de fuerzas policiales.

- La tercera mesa redonda sobre vigilancia y control digital estuvo presidida por: Stephen Kavanagh, Jefe de Policía de Essex y Presidente del Consejo de Vigilancia y Control Digital. El Orador por parte del gabinete fue Nick Hurd Diputado, Viceministro de Extinción de Incendios y Vigilancia y Control, Ministerio del Interior. Octubre 2017, Londres.

MOTOROLA SOLUTIONS