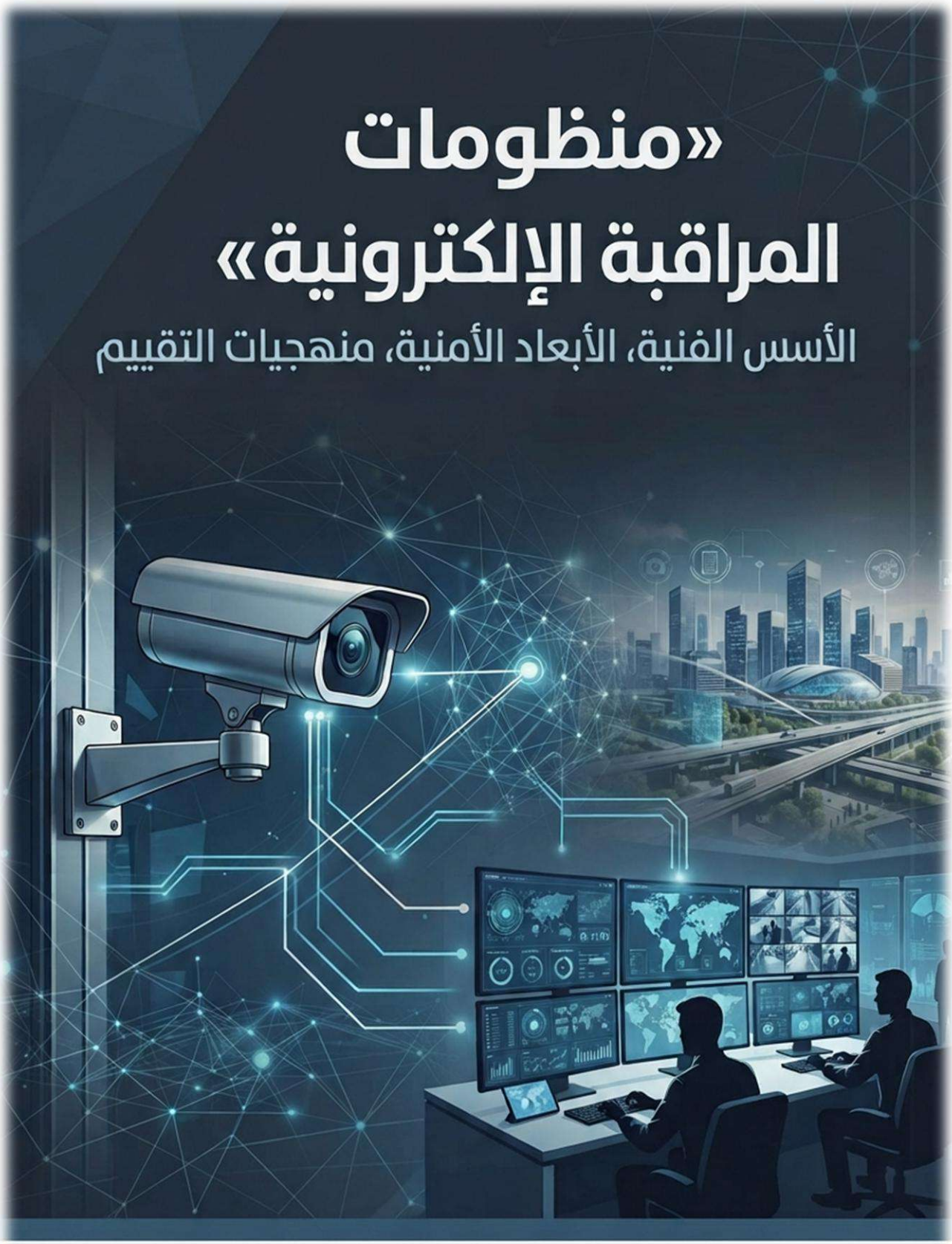
«منظومات المراقبة الإلكترونية»

الأسس الفنية، الأبعاد الأمنية، منهجيات التقييم



Compiled and Prepared by

Colonel Faisal Murjan

إهداء

إلى المخلصين الذين يعملون في غرف الرقابة،
حيث لا يلتفت أحدٌ إلى ما تفعلون.

إلى العيون الساهرة خلف الشاشات، التي ترى
ما يغفل عنه الآخرون، وتحرس بصمت.

إلى من يحملون الأمانة دون ضجيج،
ويؤدون واجبهم دون انتظار ثناء.

إلى المجهولين في المشهد، الذين لا تُرى
جهودهم، لكن يُرى غيابها.

إليكم هذا الكتاب؛ تقديرًا لمن جعلوا من
اليقظة أمانة، ومن الصمت إخلاصًا.

المقدمة

أصبحت أنظمة كاميرات المراقبة خلال العقود الأخيرة أحد المكونات الأساسية في منظومات الأمن الحديثة، ولم تعد وظيفتها مقتصرة على تسجيل الصور ومتابعة ما يجري في المواقع والمنشآت، بل تطورت لتصبح جزءًا من منظومة أوسع لإدارة المخاطر، ودعم الوعي بالموقف الأمني، واكتشاف الأحداث، وتوثيق الوقائع، والمساهمة في سرعة الاستجابة، وتوفير معلومات يمكن الاستفادة منها في أعمال الاستدلال والتحقيق.

أسهم التطور المتسارع في تقنيات التصوير الرقمي والشبكات والتخزين ومعالجة البيانات والتحليلات الذكية في توسيع إمكانات هذه الأنظمة وتنوع تطبيقاتها الأمنية.

غير أن هذا التطور التقني أوجد، في المقابل، تحديًا مهمًا يتمثل في ضرورة الانتقال من النظر إلى كاميرات المراقبة باعتبارها أجهزة منفردة إلى النظر إليها باعتبارها منظومة أمنية متكاملة، تتفاعل فيها عناصر التخطيط والتصميم والاختيار والتنفيذ والتشغيل والتسجيل والتخزين والصيانة والحماية والعنصر البشري. فالكاميرا ذات المواصفات الفنية المرتفعة قد لا تحقق الغرض الأمني المطلوب إذا وُضعت في موقع غير مناسب، أو كانت زاوية رؤيتها غير ملائمة، أو أثرت الإضاءة في جودة الصورة، أو لم يكن التسجيل متاحًا عند الحاجة، أو لم تتوافر آليات مناسبة لإدارة النظام وتشغيله وصيانته.

ومن هنا تنطلق فكرة هذا الكتاب من مبدأ أساسي مفاده أن فاعلية منظومة المراقبة لا تُقاس بعدد الكاميرات ولا بارتفاع مواصفاتها التقنية وحدها، وإنما بقدرتها على تحقيق الهدف الأمني الذي صُممت من أجله. فالتقنية في المجال الأمني ليست غاية مستقلة، وإنما وسيلة ينبغي أن ترتبط باحتياج أمني واضح، وتحليل مناسب للمخاطر، وتصميم ملائم لطبيعة الموقع، وتشغيل منظم، وتقييم مستمر للأداء والنتائج.

❖ أولًا: دوافع تأليف الكتاب

جاء تأليف هذا الكتاب استجابة لعدد من الملاحظات المرتبطة بالتوسع الكبير في استخدام أنظمة كاميرات المراقبة في المنشآت والمؤسسات والمرافق المختلفة. فمن جهة، أصبحت هذه الأنظمة أكثر انتشارًا وتنوعًا من الناحية التقنية، ومن جهة أخرى لا

تزال الحاجة قائمة إلى محتوى عربي متخصص يجمع بصورة متوازنة بين المعرفة الفنية والمنظور الأمني والتطبيق العملي.

وقد دفعتني إلى إعداد هذا الكتاب ملاحظة أن تناول كاميرات المراقبة غالبًا ما يأتي من أحد اتجاهين منفصلين؛ اتجاه تقني يركز على مكونات الكاميرات ومواصفاتها وأنواعها، واتجاه أمني يتناول دورها في الحماية والرقابة والوقاية بصورة عامة. وبين الاتجاهين مساحة مهمة تحتاج إلى معالجة أكثر تكاملًا، تتمثل في الإجابة عن السؤال الآتي:

كيف نحدد ما إذا كانت منظومة كاميرات المراقبة فعالة أمنيًا بالفعل؟

ومن هذا السؤال نشأت الحاجة إلى كتاب لا يكتفي بتعريف القارئ بالتقنيات، ولا يكتفي بإبراز أهمية المراقبة، وإنما يحاول بناء فهم متكامل يبدأ من تحديد الهدف الأمني، ويمر بتحليل المخاطر وتصميم المنظومة واختيار مكوناتها وتشغيلها وصيانتها وحمايتها، وينتهي بتقييم قدرتها الفعلية على إنتاج قيمة أمنية.

كما يأتي هذا الكتاب في ظل التحول المستمر من أنظمة المراقبة التقليدية إلى الأنظمة الرقمية والشبكية، وما صاحبه من توسع في إمكانات التسجيل والتخزين والتحليل والربط والتكامل مع أنظمة أمنية أخرى، الأمر الذي يجعل الإلمام بالأسس الفنية والتشغيلية ضرورة للعاملين في المجال الأمني، وليس اختصاصًا فنيًا منفصلًا عن العمل الأمني.

❖ ثانيًا: أهمية الموضوع

تنبع أهمية موضوع الكتاب من المكانة التي أصبحت تحتلها أنظمة المراقبة في منظومات أمن المنشآت، ومن تعدد الوظائف التي يمكن أن تؤديها عندما يتم تصميمها وتشغيلها بصورة صحيحة .فهي قد تسهم في مراقبة المداخل والمخارج، ومتابعة المناطق الحساسة، ورصد الحركة، واكتشاف بعض الأحداث، ودعم سرعة الاستجابة، وتوثيق الوقائع، وتوفير معلومات بصرية يمكن الرجوع إليها عند الحاجة.

إلا أن أهمية الموضوع لا تكمن في إثبات أن كاميرات المراقبة مفيدة فحسب؛ فهذه الحقيقة أصبحت معروفة على نطاق واسع، وإنما تكمن في فهم الشروط التي تجعلها مفيدة وفعالة.

فالمنظومة الأمنية الناجحة لا تقوم على شراء معدات متقدمة فحسب، وإنما تبدأ من فهم طبيعة المخاطر والأهداف المطلوب تحقيقها .ومن ثم فإن اختيار الكاميرا، والعدسة، وموقع التركيب، وزاوية الرؤية، ومستوى الإضاءة، وجودة التسجيل، وسعة التخزين، واستقرار الشبكة والطاقة، وكفاءة التشغيل والصيانة، وحماية النظام والتسجيلات، كلها عناصر ينبغي النظر إليها ضمن منظومة واحدة مترابطة.

وتزداد أهمية الموضوع مع انتقال أنظمة المراقبة إلى بيئات رقمية وشبكية أكثر تعقيدًا؛ إذ لم يعد التحدي متعلقًا بجودة الصورة وحدها، وإنما أصبح يشمل كذلك موثوقية النظام، واستمرارية عمله، وحماية بياناته، وإدارة صلاحيات الوصول إليه، وقدرته على التكامل مع بقية مكونات البيئة الأمنية.

ولا يقتصر الأمر على البعد التقني والأمني فحسب، بل يمتد ليشمل البعد القانوني والأخلاقي المرتبط بحماية الخصوصية، وضوابط استخدام التسجيلات، والامتثال للتشريعات المنظمة للمراقبة .فالأمن لا يُبنى على حساب الحقوق والحريات، والمراقبة لا تكون فعالة إلا إذا كانت مسؤولة ومشروعة. وقد حرص الكتاب على معالجة هذه الإشكاليات ضمن إطارها المهني والأخلاقي.

ومن ثم يسعى الكتاب إلى تقديم معالجة تساعد القارئ على الانتقال من السؤال:

ما أفضل كاميرا؟

إلى سؤال أكثر أهمية من الناحية الأمنية:

ما أفضل منظومة لتحقيق الهدف الأمني المحدد؟

ثالثًا: الفئة المستهدفة

صُمم هذا الكتاب ليكون مناسبًا لمجموعة واسعة من القراء الذين يجمعهم الاهتمام بالأمن والتقنية وتطبيقاتهما، ومن أبرزهم:

١. مسؤولو ومديرو أمن المنشآت.

٢. العاملون في إدارات الأمن والحماية.

٣. مشغلو مراكز المراقبة والتحكم.

٤. المختصون في تصميم وتركيب وإدارة أنظمة المراقبة.

٥. المختصون في تقنية المعلومات والشبكات المرتبطة بالأنظمة الأمنية.

٦. مسؤولو الأمن والسلامة وإدارة المخاطر.
٧. العاملون في المؤسسات الحكومية والخاصة التي تعتمد على أنظمة المراقبة.
٨. الباحثون وطلبة الدراسات الأمنية والتقنية.
٩. المهتمون بتطوير وتقييم منظومات الحماية والمراقبة.

وقد روعي في إعداد الكتاب ألا يفترض امتلاك القارئ معرفة هندسية متقدمة؛ إذ يقدم المفاهيم الفنية في سياقها الأمني، مع المحافظة في الوقت نفسه على المستوى العلمي والتخصصي الذي يجعل الكتاب مفيدًا للمتخصصين.

رابعًا: منهج إعداد الكتاب

١. اعتمد إعداد الكتاب على منهج يجمع بين الوصف والتحليل والتطبيق، مع التركيز على الربط بين المكونات الفنية والوظائف الأمنية.
٢. فلم يُتعامل مع الكاميرا باعتبارها منتجًا تقنيًا مستقلًا، وإنما باعتبارها جزءًا من منظومة تبدأ باحتياج أمني وتنتهي بنتيجة أمنية. ولذلك يتدرج الكتاب من المفاهيم الأساسية ومكونات المنظومة إلى أسس التصميم والاختيار والتنفيذ والتشغيل، ثم ينتقل إلى الوظائف الأمنية وطرق تقييم الفاعلية.
٣. كما يقوم الكتاب على مبدأ مهم في معالجة الموضوع، وهو التمييز بين:
٤. المواصفات الفنية، والأداء الفعلي، والكفاءة التشغيلية، والفاعلية الأمنية.
٥. فارتفاع مواصفة تقنية معينة لا يعني بالضرورة أن المنظومة تحقق أفضل أداء، كما أن جودة الأداء الفني لا تعني تلقائيًا تحقق النتيجة الأمنية المطلوبة. ومن هنا فإن التحليل في هذا الكتاب يركز على العلاقة بين الهدف الأمني والمتطلب الفني والأداء الفعلي والنتيجة الأمنية.
٦. وقد استفاد إعداد الكتاب من الأدبيات العلمية والمراجع المتخصصة والمعايير والممارسات المهنية ذات الصلة، مع الحرص على التمييز بين المعلومات العلمية الموثقة وبين الآراء أو التقديرات الفنية، وعلى إسناد المعلومات والأفكار إلى مصادرها وفق نظام التوثيق المعتمد في الكتاب.
٧. كما يتضمن الكتاب نماذج وجداول وأدوات تطبيقية تساعد القارئ على تحويل المعرفة النظرية إلى إجراءات عملية، وعلى تقييم منظومات المراقبة بصورة أكثر

انتظامًا وموضوعية. وقد أُدرجت دراسات حالة تطبيقية من قطاعات متنوعة (صناعية، وحكومية، وتعليمية، وصحية) لاستخلاص الدروس والعبر من التجارب الواقعية، وربط المحتوى النظري بالممارسة الميدانية.

خامسًا: حدود موضوع الكتاب

يركز الكتاب بصورة أساسية على أنظمة كاميرات المراقبة المستخدمة في تعزيز أمن المنشآت، من منظور فني وأمني وتطبيقي.

ويتناول لذلك:

١. التخطيط لمنظومة المراقبة.
٢. تحليل الاحتياجات والمخاطر المرتبطة بها.
٣. اختيار أنواع الكاميرات والمكونات المناسبة.
٤. تصميم مواقع التركيب والتغطية.
٥. جودة الصورة والإضاءة.
٦. التسجيل والتخزين وإدارة التسجيلات.
٧. الشبكات والطاقة واستمرارية التشغيل.
٨. مراكز المراقبة والعامل البشري.
٩. التشغيل والصيانة.
١٠. حماية النظام والتسجيلات.
١١. التكامل مع بعض الأنظمة الأمنية.
١٢. تقييم الأداء والكفاءة والفاعلية الأمنية للمنظومة.
١٣. الاتجاهات التقنية الحديثة ذات الصلة.

ولا يهدف الكتاب إلى أن يكون مرجعًا هندسيًا متخصصًا في تصنيع الكاميرات أو تصميم الدوائر الإلكترونية أو تطوير البرمجيات، كما لا يتناول الجوانب القانونية والتنظيمية بصورة موسعة، إلا بالقدر الذي يرتبط مباشرة بالاستخدام الأمني المسؤول للأنظمة وإدارة التسجيلات وحمايتها.

كذلك لا يفترض الكتاب أن كاميرات المراقبة تمثل حلًا منفردًا لجميع المخاطر الأمنية؛ فهي عنصر ضمن منظومة أمنية متكاملة، وتزداد فاعليتها عندما تتكامل مع إجراءات الحماية البشرية والتنظيمية والتقنية الأخرى.

سادسًا: كيفية الاستفادة من الكتاب

يمكن قراءة الكتاب قراءة متسلسلة تبدأ من المفاهيم الأساسية وتنتهي بالتقييم والتطبيق، وهي الطريقة المناسبة للقارئ الذي يريد تكوين فهم متكامل للموضوع.

كما يمكن استخدامه بصورة مرجعية متخصصة؛ إذ يستطيع مسؤول الأمن، مثلًا، الرجوع إلى الفصول المتعلقة بالتخطيط والتوزيع والتقييم، بينما يستطيع المختص الفني التركيز على الفصول المتعلقة بالكاميرات وجودة الصورة والتسجيل والشبكات، ويستطيع الباحث الاستفادة من الإطار التحليلي والمراجع والنماذج التطبيقية.

ولتحقيق أكبر فائدة عملية، يُنصح بعدم الاكتفاء بقراءة المعلومات الفنية، وإنما بمحاولة تطبيق الأسئلة والمعايير الواردة في الكتاب على منظومة مراقبة حقيقية؛ فالغرض من المعرفة الفنية في النهاية ليس زيادة عدد المصطلحات التي يعرفها القارئ، وإنما رفع قدرته على اتخاذ قرار أمني وفني أكثر دقة.

وقد أُعدت الجداول والنماذج وأدوات التقييم بحيث يمكن الاستفادة منها في الفحص الأولي للمنظومات، وفي تحديد مواطن القوة والقصور، وفي إعداد خطط التطوير والتحسين.

سابعًا: البنية المنهجية للفصول

اعتمد الكتاب بنية منهجية موحدة في جميع فصوله، تسهّل على القارئ المتابعة والاستفادة، وتتكون من: تمهيد الفصل، ثم المفاهيم الأساسية، ثم التحليل الفني والأمني، ثم التطبيقات الأمنية، ثم خلاصة الفصل، ثم أهم النتائج، ثم أسئلة التفكير والتقييم، وأخيرًا المراجع الخاصة بالفصل. وقد أُعدت هذه البنية لتخدم هدفين: تحقيق التكامل بين النظرية والتطبيق، وتمكين القارئ من الانتقال السلس بين مستويات المعرفة المختلفة.

كلمة أخيرة

هذا الكتاب لا ينطلق من افتراض أن التقنية هي الحل لكل مشكلة أمنية، ولا من الاعتقاد بأن كثرة الكاميرات تعني بالضرورة ارتفاع مستوى الحماية، وإنما ينطلق من قاعدة أكثر واقعية:

قيمة منظومة المراقبة لا تقاس بما تملكه من تقنيات فحسب، وإنما بما تستطيع أن تحققه من نتائج أمنية تتناسب مع المخاطر والأهداف والبيئة التي تعمل فيها.

ومن هذا المنطلق يأتي هذا الكتاب محاولة لبناء جسر معرفي بين الأمن والتقنية والتطبيق، بما يسهم في تطوير فهم أكثر نضجًا لأنظمة كاميرات المراقبة، والارتقاء بطريقة تصميمها وتشغيلها وتقييمها، وتحويلها من مجرد وسيلة للرؤية والتسجيل إلى مكون فعال ضمن منظومة أمنية متكاملة.

وما توفيقي إلا بالله، عليه توكلت، وإليه أنيب.

المؤلف

الباب الأول:
الإطار العام لمنظومات المراقبة

الفصل الأول: مدخل إلى كاميرات المراقبة في المجال الأمني

تمهيد الفصل

تمثل المراقبة أحد المكونات الأساسية في العمل الأمني؛ إذ ترتبط القدرة على الوقاية من المخاطر واكتشاف الأحداث والاستجابة لها بوجود معلومات مناسبة عن البيئة الأمنية وما يطرأ عليها من تغيرات. ومن هذا المنطلق، لا ينبغي فهم المراقبة الأمنية باعتبارها مجرد مشاهدة أو متابعة بصرية، وإنما باعتبارها عملية منظمة لجمع المعلومات ذات الصلة بالأمن، ومتابعة الأحداث والتغيرات، والاستفادة من المعلومات الناتجة عنها في الوقاية والكشف والاستجابة والتوثيق ودعم اتخاذ القرار.

وقد تطورت وسائل المراقبة مع تطور طبيعة المخاطر ووسائل مواجهتها؛ فبعد أن اعتمدت بدرجة كبيرة على الملاحظة البشرية المباشرة، أصبحت تستفيد من وسائل تقنية متعددة، من بينها أنظمة الدوائر التلفزيونية المغلقة(CCTV) ، ثم الأنظمة الرقمية والشبكية، وصولًا إلى الأنظمة التي تتضمن إمكانات متقدمة لمعالجة الصور وتحليل الفيديو والربط مع أنظمة أمنية أخرى.(1)

وتنطلق معالجة هذا الكتاب من فكرة محورية مفادها أن فاعلية المراقبة الأمنية لا تنتج من التقنية وحدها، وإنما من تكامل التقنية مع التخطيط والتشغيل والعنصر البشري والإجراءات الأمنية .وهذه الفكرة تمثل الخيط الناظم الذي يربط مباحث هذا الفصل وجميع فصول الكتاب، إذ إن الكاميرا لا تمثل المراقبة في معناها الكامل، وإنما تمثل وسيلة تقنية ضمن عملية أمنية أوسع. ويتناول هذا الفصل ثلاثة مباحث: مفهوم المراقبة الأمنية، ونشأة وتطور أنظمة المراقبة، وتطور كاميرات المراقبة.

المبحث الأول: مفهوم المراقبة الأمنية

أولاً: مفهوم المراقبة

تدل المراقبة في معناها العام على المتابعة المنظمة لشخص، أو مكان أو نشاط أو بيئة معينة بهدف الحصول على معلومات عنها. ويكتسب هذا النشاط طابعًا أمنيًا عندما يرتبط الغرض منه بحماية الأشخاص، أو الممتلكات أو المنشآت، أو باكتشاف الأحداث والسلوكيات والظروف التي قد تمثل خطرًا أو مخالفة أو تهديدًا أمنيًا.(2)

وعليه، يمكن النظر إلى المراقبة الأمنية في إطار هذا الكتاب باعتبارها نشاطًا منظمًا لجمع المعلومات ومتابعة الأحداث والتغيرات في بيئة محددة، باستخدام وسائل بشرية أو تقنية أو مزيج منهما، بهدف دعم الوقاية والكشف والاستجابة والتوثيق واتخاذ القرار الأمني.(3)

ويكشف هذا التعريف عن أن المراقبة الأمنية تتجاوز مجرد «الرؤية»؛ فالرؤية تمثل القدرة على الحصول على معلومات بصرية، في حين تتطلب المراقبة وجود غرض محدد، ومجال معلوم للملاحظة، وآلية للمتابعة، وقدرة على التعامل مع المعلومات الناتجة عنها (٤). فوجود كاميرا في موقع ما لا يعني بالضرورة أن الموقع يخضع لمراقبة أمنية فعالة. فقد تكون الكاميرا موجودة، ولكنها لا تغطي المنطقة ذات الأولوية، أو تنتج صورة لا تحقق الغرض المطلوب، أو لا تتوافر متابعة مناسبة لما تعرضه، أو لا توجد وسيلة ملائمة لتسجيل المعلومات واسترجاعها، أو لا توجد إجراءات واضحة للتعامل مع الأحداث التي تكشفها.(5)

ومن هنا يمكن التمييز بين ثلاثة مستويات مترابطة:

الرؤية ← المراقبة ← الفعل الأمني

فالرؤية تعني الحصول على المعلومات البصرية، والمراقبة تعني توظيف هذه المعلومات في متابعة البيئة والأحداث، أما الفعل الأمني فيتمثل في استخدام المعلومات الناتجة عن المراقبة لاتخاذ الإجراء المناسب وفق طبيعة الحدث.(6)

ثانياً: المراقبة الأمنية بوصفها عملية

من المنظور الأمني، يمكن فهم المراقبة باعتبارها عملية مترابطة تبدأ بتحديد الغرض الأمني، وتنتهي باستخدام المعلومات الناتجة عنها في اتخاذ إجراء أو دعم قرار أو توثيق

واقعة (٧). ويمكن تمثيل هذه العملية على النحو الآتي: تحديد الهدف الأمني ← تحديد البيئة محل المراقبة ← جمع المعلومات ← رصد الأحداث ← تحليل المعلومات وتفسيرها ← تقييم الحدث ← الاستجابة ← التوثيق والمراجعة

ولا يعني هذا التسلسل أن جميع أنظمة المراقبة تعمل بالطريقة نفسها أو أن كل مرحلة تتم بصورة آلية؛ وإنما يوضح المكونات الوظيفية التي تساعد على فهم المراقبة باعتبارها عملية تتجاوز مرحلة الحصول على الصورة.(8)

وعليه، فإن تقييم كفاءة نظام المراقبة لا ينبغي أن يقتصر على قدرته على جمع المعلومات، بل ينبغي أن يشمل مدى قدرة المنظومة على تحويل هذه المعلومات إلى قيمة أمنية قابلة للاستخدام. فقد توفر كاميرا صورة واضحة، إلا أن عدم وجود متابعة مناسبة أو إجراءات تشغيلية للتعامل مع الأحداث قد يحد من القيمة الأمنية لهذه الصورة. وفي المقابل، قد تكون منظومة ذات مواصفات فنية أقل تقدمًا أكثر ملاءمة لغرض معين إذا صُممت وفق احتياجات الموقع، ووُضعت في المواقع المناسبة، وتوافرت لها إجراءات تشغيل واستجابة واضحة.(9)

ومن هنا تبرز القاعدة الأساسية التي تحكم هذا الكتاب:

فاعلية المراقبة الأمنية لا تنتج من التقنية وحدها، وإنما من تكامل التقنية مع التخطيط والتشغيل والعنصر البشري والإجراءات الأمنية.

ثالثاً: المراقبة الأمنية والمراقبة بالكاميرات

المراقبة الأمنية مفهوم أوسع من المراقبة بالكاميرات؛ فالأولى تمثل الوظيفة الأمنية، بينما تمثل الثانية إحدى الوسائل التقنية التي يمكن استخدامها لتنفيذ هذه الوظيفة (١٠).

وقد تكون المراقبة الأمنية:

١. مراقبة بشرية مباشرة.
٢. مراقبة باستخدام كاميرات الفيديو.
٣. مراقبة باستخدام أجهزة الاستشعار.
٤. مراقبة تعتمد على أنظمة الإنذار.
٥. مراقبة تعتمد على بيانات الأنظمة الرقمية.
٦. أو مراقبة تجمع بين أكثر من وسيلة.

ومن ثم فإن كاميرات المراقبة ينبغي ألا تُدرس باعتبارها نظامًا منفصلًا عن البيئة الأمنية، وإنما باعتبارها أداة ضمن منظومة أوسع. وتوضح الأطر المهنية لأنظمة كاميرات المراقبة أن النظام لا يقتصر على الكاميرا ذاتها، وإنما يرتبط بمجموعة من المكونات والوظائف المتعلقة بالتقاط الصور والمعلومات ومعالجتها وتخزينها وإدارتها واستخدامها. كما يؤكد الإطار المهني البريطاني ضرورة أن يكون استخدام نظام المراقبة قائمًا على غرض محدد وحاجة واضحة، وأن تكون هناك مسؤوليات وإجراءات وضوابط واضحة لإدارته (11).

وهنا يظهر فارق جوهري بين وجود كاميرات للمراقبة ووجود منظومة مراقبة أمنية تستخدم الكاميرات بصورة فعالة .فالأول يصف وجودًا ماديًا لمعدات تقنية، أما الثاني فيصف قدرة تشغيلية وأمنية متكاملة.(12)

رابعاً: أهداف المراقبة الأمنية : تختلف أهداف المراقبة باختلاف طبيعة المنشأة والمخاطر والبيئة التشغيلية، إلا أن مجموعة من الوظائف الأساسية يمكن أن تشكل إطارًا عامًا للمراقبة الأمنية:(13)

١. الوقاية والردع

يمكن للمراقبة أن تسهم في الوقاية من بعض السلوكيات غير المرغوبة عندما يدرك الأفراد أن الموقع يخضع للمراقبة وأن احتمال اكتشاف المخالفات قائم. غير أن الردع لا ينبغي أن يُعامل باعتباره نتيجة مضمونة لمجرد تركيب الكاميرات؛ فنتائج الدراسات التجريبية والمراجعات المنهجية تشير إلى تفاوت أثر CCTV باختلاف المكان وطريقة التطبيق وطبيعة المشكلة الأمنية. فقد خلصت مراجعة منهجية شملت ٤٤ تقييمًا إلى أن لـ CCTVأثرًا متواضعًا في خفض الجريمة إجمالًا، مع اختلاف واضح في الفاعلية بين البيئات، وظهور نتائج أفضل في مواقف السيارات مقارنة ببعض البيئات الأخرى (١٤). كما خلصت مراجعة منهجية وتحليل تلوي لاحق إلى وجود انخفاض متواضع ودال في الجريمة، مع ظهور أقوى الآثار وأكثرها اتساقًا في مواقف السيارات (١٥). وعليه، فإن الردع يمثل أحد الآثار المحتملة للمراقبة، وليس معيارًا وحيدًا للحكم على فاعلية المنظومة.

٢. الكشف

تمثل القدرة على اكتشاف الأحداث أحد أهم أهداف المراقبة الأمنية، سواء تعلق الأمر بدخول غير مصـــرح به، أو حركة غير معتادة، أو حادث أمني، أو مخالفة للإجراءات. ولا ترتبط قدرة النظام على الكشـف بالكاميرا وحدها، وإنما تتأثر بعوامل متعددة، منها موقع الكاميرا، ومجال رؤيتها، والإضاءة، وجودة الصورة، واستمرارية التشغيل، وطريقة المتابعة، وكفاءة المشـغل، أو إمكانات التحليل الآلي عند اسـتخدامها (١٦). ومن ثم فإن «وجود صورة» لا يعني بالضرورة «القدرة على الكشف»، لأن الكشف يتطلب أن تكون المعلومات التي توفرها المنظومة مناسبة لطبيعة الحدث المراد اكتشافه.

٣. دعم الاستجابة

لا تقتصـر قيمة المراقبة على اكتشـاف الحدث، بل تمتد إلى توفير معلومات تسـاعد العاملين على تقدير الموقف واتخاذ الإجراء المناسـب. فالمعلومة المرئية قد تسـاعد، بحسـب طبيعة النظام والموقع، على تحديد مكان الحدث، وطبيعته، ومدى امتداده، وما إذا كان يتطلب تدخلًا فوريًا (١٧). وبذلك تصبح المراقبة جزءًا من دورة أمنية تبدأ بالملاحظة ولا تنتهي بمجرد اكتشـاف الحدث، وإنما تمتد إلى اسـتخدام المعلومات في دعم الاستجابة المناسبة.

٤. التوثيق: تمثل التسـجيلات المرئية مصـدرًا مهمًا للمعلومات التي يمكن الرجوع إليها بعد وقوع الحدث. وتختلف قيمة التسـجيل باختلاف جودة الصـورة، واسـتمرارية التسـجيل، وسـلامة البيانات، وإمكان الوصـول إليها واسـترجاعها، والضوابط المطبقة على حفظها واستخدامها (١٨). ولهذا فإن وجود التسجيل لا يكفي وحده؛ فالقيمة الأمنية للتسـجيل تعتمد على قابليته للاسـتخدام والاسترجاع والتحقق من سلامته.

٥. دعم التحقيق والاستدلال

يمكن أن توفر التسجيلات المرئية معلومات تساعد في إعادة بناء تسلسل الأحداث، وتحديد أوقات وقوعها، ومتابعة الحركة داخل الموقع، وربط بعض الأحداث ببعضـها. إلا أن قيمة هذه المعلومات تعتمد على جودة التسـجيل وسـياقه وسـلامته، وعلى الإجراءات المهنية المتبعة في التعامل معه (١٩). ومن ثم لا ينبغي النظر إلى كاميرات المراقبة على أنها بديل عن التحقيق، وإنما باعتبارها مصـدرًا من مصـادر المعلومات

المرئية التي يمكن أن تدعم أعمال الاستدلال والتحقيق متى كانت التسجيلات مناسبة للغرض المطلوب ومحفوظة بطريقة سليمة.

خامساً: عناصر المراقبة الأمنية الفعالة

عناصر تحليل المراقبة الأمنية الفعالة :(20)

١. الهدف :ما الذي نريد معرفته أو اكتشافه أو متابعته؟

٢. المكان :أين ينبغي أن تتم المراقبة؟

٣. الوسيلة :ما الأداة المناسبة للحصول على المعلومات المطلوبة؟

٤. التشغيل :من يتابع المعلومات، وكيف يتم التعامل معها؟

٥. الإجراء :ماذا يحدث عندما تكشف المراقبة حدثًا أو مؤشر خطر؟

ومن خلال هذه العناصر يتضح أن اختيار الكاميرا لا يمكن أن يكون نقطة البداية الوحيدة. فاختيار التقنية ينبغي أن يأتي بعد تحديد الهدف الأمني والمتطلبات التشغيلية. فعندما يكون الهدف مراقبة حركة الأشخاص في مساحة واسعة، قد تختلف المتطلبات عن حالة يكون الهدف فيها الحصول على تفاصيل دقيقة عند نقطة دخول. وعندما تكون المراقبة مطلوبة ليلًا في بيئة ضعيفة الإضاءة، فإن متطلبات النظام ستختلف عن بيئة داخلية ذات إضاءة مستقرة.

ومن هنا يصبح السؤال المهني الصحيح :ما متطلبات المراقبة التي يفرضها الهدف الأمني؟ وليس :ما أعلى مواصفات الكاميرا المتاحة؟ وهذا المبدأ سيكون أساسًا في الفصول اللاحقة عند تناول تصميم المنظومة واختيار مكوناتها؛ إذ لا يكون الاختيار الفني صحيحًا إلا إذا ارتبط بالهدف الذي يفترض أن يخدمه.

سادساً: المراقبة الأمنية بين التقنية والعنصر البشري

على الرغم من التطور الكبير في تقنيات التصوير والتحليل الآلي، فإن العنصر البشري لا يزال يمثل مكونًا أساسيًا في كثير من منظومات المراقبة، ولا سيما فيما يتعلق بتفسير الأحداث، وتقدير مستوى الخطورة، واتخاذ القرار، وتنسيق الاستجابة.(21)

وقد تناولت الدراسات بصورة مباشرة دور العاملين في تشغيل أنظمةCCTV ، وأظهرت أهمية وظيفة أفراد الأمن وطريقة التشغيل في أداء منظومات المراقبة ونتائجها. وقد خصصت مراجعة منهجية لدراسة العلاقة بين أفراد الأمن الخاص وأنظمةCCTV ،

وبينت أن أداء النظام لا ينفصل عن كيفية تشغيله واستخدامه في السياق الأمني الذي يعمل فيه.(22)

وبناءً على ذلك، فإن تقييم منظومة المراقبة لا ينبغي أن يقتصر على الأجهزة والمواصفات، بل يجب أن يشمل كذلك: كفاءة المشغلين، والتدريب والتأهيل، وإجراءات العمل، وسرعة اكتشاف الأحداث، وآليات التصعيد، وإجراءات الاستجابة، والصيانة، واستمرارية التشغيل. وعليه، فقد تمتلك المنظومة معدات متقدمة، لكنها تظل محدودة من الناحية الأمنية إذا لم تكن البيئة التشغيلية قادرة على الاستفادة منها.

سابعاً: المراقبة الأمنية بوصفها جزءًا من منظومة إدارة المخاطر

لا ينبغي فصل المراقبة الأمنية عن مفهوم المخاطر؛ إذ إن الغرض من المراقبة في النهاية هو التعامل مع مخاطر أو تهديدات محددة، وتوفير المعلومات اللازمة للوقاية منها أو اكتشافها أو الاستجابة لها.(23)

أسئلة التخطيط السليم للمراقبة:

١. ما الأصول التي نريد حمايتها؟
٢. ما التهديدات والمخاطر المحتملة؟
٣. أين تتركز نقاط الضعف؟
٤. ما الأحداث التي نحتاج إلى اكتشافها؟
٥. ما المعلومات التي نحتاج إليها عند وقوع الحدث؟
٦. ما الزمن المطلوب لاكتشاف الحدث والاستجابة له؟
٧. ما مستوى التفاصيل المطلوب من الصورة؟
٨. من سيستخدم المعلومات الناتجة عن المراقبة؟

وتؤدي الإجابة عن هذه الأسئلة إلى تحديد المتطلبات الفنية والتشغيلية للمنظومة. ويتفق هذا الاتجاه مع المبادئ المهنية الحديثة التي تشدد على ضرورة أن يكون استخدام أنظمة المراقبة قائمًا على غرض محدد وحاجة واضحة، وأن تكون أهداف النظام قابلة للتحديد والمراجعة (٢٤). ومن ثم يمنع هذا المنهج الوقوع في أحد الأخطاء الشائعة، وهو شراء التقنية أولًا ثم البحث لاحقًا عن الاستخدام المناسب لها.

فالتخطيط الرشـيد يسـير في الاتجاه الآتي: المخاطر ← الأهداف الأمنية ← متطلبات المراقبة ← التصميم ← التقنية ← التشغيل ← التقييم

ثامناً: حدود المراقبة الأمنية

على الرغم من أهمية المراقبة، فإنها ليست حلًا مطلقًا للمشكلات الأمنية، ولا يمكن اعتبار وجود الكاميرات دليلًا بذاته على ارتفاع مستوى الحماية.(25)

وقد أظهرت المراجعات المنهجية لتأثير CCTV على الجريمة أن نتائج المراقبة تختلف باختلاف المواقع والظروف وطريقة التطبيق. فقد شملت مراجعة Welsh و Farrington لعام ٢٠٠٨ عددًا من التقييمات بلغ ٤٤ تقييمًا، وخلصت إلى أن أثر CCTV في خفض الجريمة كان متواضعًا إجمالًا، مع تفاوت الفاعلية بين البيئات، وظهور نتائج أفضل في مواقف السيارات، كما لم تجد المراجعة أثرًا واضحًا في مستويات الجرائم العنيفة (٢٦). أما المراجعة المنهجية والتحليل التلوي الذي أجراه Piza وزملاؤه، فقد وجدا انخفاضًا متواضعًا ودالًا في الجريمة، مع أقوى الآثار وأكثرها اتساقًا في مواقف السيارات، وهو ما يؤكد أن الحكم على فاعلية CCTV ينبغي أن يراعي نوع البيئة وطريقة التطبيق والغرض الأمني.(27)

وتنبع حدود المراقبة الأمنية من عوامل متعددة، منها: ضعف التصميم، وسوء اختيار مواقع الكاميرات، ووجود مناطق غير مغطاة، وضعف الإضاءة، وقصور جودة الصورة، وأعطال النظام، وضعف التخزين أو صعوبة استرجاع التسجيلات، وعدم كفاءة التشغيل، وعدم الاستجابة للمعلومات التي توفرها المنظومة، والاعتماد المفرط على الكاميرات باعتبارها وسيلة حماية وحيدة.(28)

لذلك فإن القيمة الحقيقية للمراقبة تظهر عندما تكون جزءًا من منظومة أمنية متعددة الطبقات تجمع بين الإجراءات التنظيمية والعنصر البشري والتقنيات الأمنية المختلفة، بحيث تؤدي الكاميرات وظيفة محددة داخل منظومة الحماية ولا تحل محل بقية عناصرها.

تاسعاً: نحو تعريف إجرائي للمراقبة الأمنية

استنادًا إلى ما سبق، يمكن اعتماد التعريف الإجرائي الآتي للمراقبة الأمنية في هذا الكتاب:

المراقبة الأمنية هي عملية منظمة ومستمرة أو دورية لجمع المعلومات عن الأشخاص والأماكن والأنشطة والأحداث ذات الصلة بالمخاطر الأمنية، باستخدام وسائل بشرية وتقنية مناسبة، بهدف دعم الوقاية والكشف والاستجابة والتوثيق واتخاذ القرار، ضمن إجراءات وضوابط تضمن الاستفادة الفعلية من المعلومات المتاحة.

ويتميز هذا التعريف بأنه لا يحصر المراقبة في الكاميرات، وإنما يضعها في إطارها الصحيح باعتبارها وظيفة أمنية تستخدم مجموعة من الوسائل، من بينها أنظمة كاميرات المراقبة. وبناءً على ذلك، يمكن تعريف المراقبة بالكاميرات بصورة أكثر تحديدًا بأنها :استخدام أنظمة التصوير المرئي لجمع ومتابعة وتسجيل المعلومات البصرية المتعلقة بموقع أو نشاط معين، بهدف تحقيق غرض أمني محدد، مع إمكانية متابعة الأحداث وتوثيقها واسترجاع المعلومات المسجلة والاستفادة منها في إجراءات الوقاية والكشف والاستجابة والتوثيق.

وهذا التعريف الإجرائي لا يقصد به تقديم تعريف اصطلاحي عالمي ملزم، وإنما تحديد المقصود بالمفهوم كما سيستخدم في هذا الكتاب، بما يسمح بضبط المصطلحات وتجنب الخلط بين الكاميرا بوصفها جهازًا، ونظام المراقبة بوصفه مجموعة من المكونات، والمراقبة الأمنية بوصفها وظيفة وعملًا أمنيًا.

أهم نتائج المبحث الأول

١. المراقبة الأمنية عملية منظمة تتجاوز مجرد الرؤية، وتهدف إلى إنتاج معلومات ذات قيمة أمنية.
٢. التمييز بين ثلاثة مستويات: الرؤية، ثم المراقبة، ثم الفعل الأمني.
٣. فاعلية المراقبة الأمنية لا تنتج من التقنية وحدها، بل من تكامل التقنية مع التخطيط والتشغيل والعنصر البشري.
٤. أهداف المراقبة الأمنية خمسة: الوقاية والردع، الكشف، دعم الاستجابة، التوثيق، دعم التحقيق.
٥. الردع ليس نتيجة مضمونة لمجرد تركيب الكاميرات، بل يتفاوت حسب البيئة وطريقة التطبيق.

٦. العنصر البشري لا يزال مكونًا أساسيًا في منظومات المراقبة، حتى مع تطور التحليل الآلي.
٧. التخطيط الرشيد للمراقبة يبدأ من المخاطر، وليس من شراء التقنية.
٨. للمراقبة الأمنية حدود ينبغي الاعتراف بها، وهي جزء من منظومة متعددة الطبقات.

أسئلة التفكير والتقييم

أسئلة معرفية:

١. ما الفرق بين المراقبة والرؤية والفعل الأمني؟ وكيف تتكامل هذه المستويات في العمل الأمني؟
٢. اذكر أهداف المراقبة الأمنية الخمسة، مع شرح موجز لكل هدف.
٣. ما العناصر الخمسة للمراقبة الأمنية الفعالة؟ وكيف يرتبط كل عنصر بالآخر؟

أسئلة تحليلية:

٤. حلل العلاقة بين فاعلية المراقبة الأمنية والتكامل بين التقنية والعنصر البشري. هل يمكن الاستغناء عن أحدهما؟
٥. ناقش حدود المراقبة الأمنية في ضوء نتائج المراجعات المنهجية. لماذا تتفاوت فاعلية CCTV بين البيئات المختلفة؟
٦. قارن بين التخطيط الرشيد للمراقبة (المخاطر ← الأهداف ← المتطلبات ← التقنية) والتخطيط التقليدي (التقنية ← البحث عن استخدام).

أسئلة تطبيقية:

٧. اختر منشأة تعرفها، وحلل كيف يمكن تطبيق عناصر المراقبة الأمنية الخمسة فيها.
٨. لو طُلب منك تصميم منظومة مراقبة لمنشأة حيوية، كيف ستوازن بين المتطلبات الأمنية والقيود التقنية والاعتبارات القانونية؟
٩. ابحث في إحدى الدراسات المحكمة حول فاعليةCCTV ، وحلل منهجيتها ونتائجها ومدى قابليتها للتطبيق في بيئة تعرفها.

المراجع:

① ينظر: Brandon C. Welsh and David P. Farrington, "Effects of Closed Circuit Television Surveillance on Crime," Campbell Systematic Reviews, Vol. 4, No. 1 (2008), pp. 1–73, DOI: 10.4073/csr.2008.17.

② ينظر: محمد عبد الله الأحمدي، الأمن الوقائي: المفاهيم والاستراتيجيات، (الرياض: دار النشر الأكاديمي، الطبعة الثانية، ١٤٤٣هـ/٢٠٢٢م)، ص ٤٥ .

③ راجع: John Smith, Security Surveillance Systems: Principles and Practices, (London: Security Press, 2nd Edition, 2021), p. 18.

④ ينظر: أحمد بن سعيد الغامدي، تطور أنظمة الأمن والمراقبة، (جدة: مؤسسة الدراسات الأمنية، الطبعة الأولى، ١٤٤١هـ/٢٠٢٠م)، ص ٣٤ .

⑤ راجع: David Brown, Integrated Security Systems Design, (New York: Butterworth-Heinemann, 3rd Edition, 2019), p. 42.

⑥ ينظر: خالد بن إبراهيم النفيعي، إدارة أنظمة المراقبة: دراسة تطبيقية، (الدمام: دار المجتمع للنشر، الطبعة الأولى، ١٤٤٤هـ/٢٠٢٣م)، ص ٣٤ .

⑦ راجع: Michael Harris, CCTV and Video Surveillance: Technology and Applications, (Boston: McGraw-Hill, 4th Edition, 2020), p. 52.

⑧ ينظر: Robert Wilson, Digital Video Processing for Security Systems, (London: Springer, 2021), p. 41.

⑨ راجع: Sarah Johnson, "Effectiveness of Video Surveillance in Crime Prevention: A Systematic Review," Journal of Security Research, Vol. 15, No. 3 (2020), p. 212.

⑩ ينظر: سعد المطيري، التقنيات الحديثة في أنظمة المراقبة، (الكويت، الطبعة الأولى، ١٤٤٢هـ/٢٠٢١م)، ص ٢٣ .

⑪ راجع: Biometrics and Surveillance Camera Commissioner, Surveillance Camera Code of Practice, United Kingdom, revised 2021, Principle 1 and Principle 2.

⑫ ينظر: فهد بن محمد العتيبي، مكونات أنظمة المراقبة بالفيديو، (الرياض: مكتبة الملك فهد الوطنية، ١٤٤٣هـ/٢٠٢٢م)، ص ٣٤ .

⑬ راجع: وزارة الداخلية، الدليل المهني لأنظمة المراقبة الأمنية، (الرياض: الإدارة العامة للأمن، ٢٠٢١م)، ص ١٢ .

⑭ Welsh and Farrington, "Effects of Closed Circuit Television Surveillance on Crime," Campbell Systematic Reviews, Vol. 4, No. 1 (2008), pp. 1–73.

⑮ Eric L. Piza, Brandon C. Welsh, David P. Farrington, and Amanda L. Thomas, "CCTV Surveillance for Crime Prevention: A 40-Year Systematic Review with Meta-Analysis," Criminology & Public Policy, Vol. 18, No. 1 (2019), pp. 135–159, DOI: 10.1111/1745-9133. 12419.

⑯ ينظر: يوسف الزهراني، العدسات البصرية في كاميرات المراقبة، (أبها: دار النشر الجامعي، ١٤٤١هـ/٢٠٢٠م)، ص ٤٥ .

⑰ راجع: Brown, Integrated Security Systems Design, p. 56.

⑱ ينظر: عبد الله بن حسن الشهري، شبكات نقل الفيديو الأمني، (الرياض: الإدارة العامة، ١٤٤٤هـ/٢٠٢٣م)، ص ٧٨.

⑲ راجع: مؤيد محمد مقبل العندلي، كاميرات المراقبة ومدى حجيتها في الإثبات في التشريع الأردني، رسالة ماجستير، كلية القانون، جامعة آل البيت، المفرق، ٢٠٢١، ص ١–٩٥ .

⑳ ينظر: Smith, Security Surveillance Systems, p. 67.

㉑ راجع: Brandon C. Welsh, Eric L. Piza, Amanda L. Thomas, and David P. Farrington, "Private Security and Closed-Circuit Television (CCTV) Surveillance: A Systematic Review of Function and Performance," Journal of Contemporary Criminal Justice, Vol. 36, No. 1 (2020), pp. 56–69, DOI: 10.1177/1043986219890192.

㉒ ينظر: المرجع السابق، ص ٥٦–٦٩.

㉓ راجع: International Organization for Standardization, ISO 22341:2021 Security and resilience — Protective security — Guidelines for crime prevention through environmental design, (Geneva: ISO, 2021), Clause 5. 3.

㉔ ينظر: Biometrics and Surveillance Camera Commissioner, Surveillance Camera Code of Practice, Principle 1.

㉔راجع: Home Office, Surveillance Camera Code of Practice, amended November 2021, effective 12 January 2022.

㉕ينظر: Welsh and Farrington, "Effects of Closed Circuit Television Surveillance on Crime," pp. 1–73.

㉖راجع: Piza et al., "CCTV Surveillance for Crime Prevention," pp. 135–159.

㉗ينظر: وزارة الداخلية، الدليل المهني لأنظمة المراقبة الأمنية، ص ١٨.

㉘راجع: Levente Tóth, "The Evolution of Public Surveillance Systems in Europe," Magyar Rendészet, Vol. 23, No. 1 (2023), pp. 191–204, DOI: 10.32577/mr.2023. 1. 12.

المبحث الثاني: نشأة وتطور أنظمة المراقبة

لم تظهر أنظمة المراقبة بالكاميرات بصورتها المعاصرة دفعة واحدة، وإنما جاءت نتيجة مسار تراكمي طويل ارتبط بتطور تقنيات التصوير والتلفزيون والاتصالات والتسجيل ومعالجة المعلومات. فقد بدأت الفكرة في صورتها الأساسية بمحاولات نقل الصورة المرئية من مكان إلى آخر لأغراض المشاهدة والمتابعة عن بعد، ثم تطورت تدريجيًا لتصبح وسيلة للمراقبة والتسجيل والاسترجاع، قبل أن تنتقل إلى البيئات الرقمية والشبكية، ثم إلى أنظمة تحليل الفيديو والأنظمة القادرة على استخراج معلومات من المحتوى المرئي.(1)

وتكتسب دراسة هذا التطور أهمية تتجاوز الجانب التاريخي؛ لأنها تكشف عن تغير جوهري في طبيعة الوظيفة التي تؤديها منظومة المراقبة. فقد انتقلت هذه المنظومات، بصورة عامة، من التركيز على المشاهدة المباشرة إلى التسجيل والاسترجاع، ثم إلى الإدارة الرقمية والنقل عبر الشبكات، وصولًا إلى تحليل الفيديو واستخراج المعلومات بصورة آلية أو شبه آلية. وبذلك لم يعد التطور مقتصرًا على تحسين جودة الصورة، وإنما أصبح متعلقًا بقدرة النظام على تحويل المشهد المرئي إلى معلومات يمكن استخدامها في العمل الأمني.

أولاً: البدايات الأولى للمراقبة المرئية

ارتبطت البدايات المبكرة للمراقبة المرئية بمحاولات تطوير وسائل تسمح للمراقب برؤية مكان أو نشاط من موقع بعيد، دون الحاجة إلى وجوده فعليًا في المكان الذي تجري فيه المراقبة. وكان هذا الاتجاه وثيق الصلة بالتطور المبكر لتقنيات التلفزيون والإرسال الإلكتروني للصورة.(2)

ومن التطبيقات التي تستحق الإشارة في هذا السياق تجربة ليون تيرمين في الاتحاد السوفيتي خلال عشرينيات القرن العشرين، حيث ارتبطت تجربته بتطوير منظومة تعتمد على التقاط الصورة ومسحها ونقلها إلى موقع آخر. وعلى الرغم من أن هذه المنظومة تختلف بصورة جوهرية في بنيتها وإمكاناتها عن أنظمة CCTV الحديثة، فإن أهميتها

التاريخية تكمن في إظهار المبدأ الأساسي المتمثل في فصل موقع التقاط الصورة عن موقع مشاهدتها.(3)

ولا ينبغي تفسير هذه التجارب المبكرة باعتبارها أنظمة مراقبة أمنية مكتملة بالمعنى المعاصر؛ فقد كانت أقرب إلى تطبيقات تقنية وتجريبية مبكرة لنقل الصورة عن بعد. إلا أنها أرست أساسًا تقنيًا أصبح لاحقًا جزءًا من البنية التي قامت عليها أنظمة المراقبة المرئية. وتكمن أهمية هذه المرحلة في أنها أظهرت أن الصورة يمكن أن تتحول إلى وسيلة للحصول على معلومات عن مكان أو نشاط بعيد، وأن المراقبة لا تشترط بالضرورة وجود الشخص الذي يجمع المعلومات في الموقع نفسه.

ثانياً: أنظمة المراقبة خلال الحرب العالمية الثانية

شهدت الحرب العالمية الثانية مرحلة مهمة في تطور أنظمة المراقبة المرئية؛ إذ فرضت التطبيقات العسكرية والصناعية الحاجة إلى متابعة بعض العمليات الخطرة أو الحساسة من مسافة آمنة.(4)

ومن أبرز التطبيقات التي ارتبطت بهذه المرحلة نظام المراقبة الذي استخدم في موقع اختبار صواريخ V-2 في بيـنِموندِه بألمانيا خلال عام ١٩٤٢، والذي ارتبط بالمهندس والتر بروخ وبشركة Siemens. وقد أتاح النظام نقل الصور من منطقة الاختبار إلى موقع آخر للمشاهدة، بما سمح بمتابعة عمليات إطلاق الصواريخ دون اعتماد كامل على وجود المراقبين بالقرب من منطقة الإطلاق.(5)

وتبرز أهمية هذه المرحلة في أنها تمثل انتقالًا من التجربة التقنية المجردة إلى استخدام التصوير المرئي لحل مشكلة تشغيلية حقيقية، هي المراقبة عن بعد في بيئة خطرة. كما توضح أن قيمة نظام التصوير لا تكمن في إنتاج الصورة في حد ذاتها، وإنما في توفير المعلومات للمستخدم في المكان والوقت اللذين يحتاج إليهما.

ثالثاً: الانتقال من الاستخدامات المتخصصة إلى الاستخدام التجاري

بعد الحرب العالمية الثانية بدأت تقنيات التلفزيون ذي الدائرة المغلقة تنتقل تدريجيًا من نطاق التطبيقات العسكرية والصناعية المتخصصة إلى تطبيقات تجارية ومدنية (6).

وتشير المصادر التقنية التاريخية إلى ظهور أنظمة تلفزيون صناعي مغلقة متاحة تجاريًا في الولايات المتحدة في أواخر أربعينيات القرن العشرين، ومن أبرز الأمثلة نظام Vericonالذي ارتبط بشركةRemington Rand ، والذي اعتمد على الربط السلكي بين الكاميرا وأجهزة العرض. وتظهر وثائق تقنية من تلك الفترة أن النظام كان يستخدم في التطبيقات الصناعية والمؤسسية لنقل المشاهد إلى مواقع عرض متعددة.(7)

وكان لهذا التحول أهمية في توسيع نطاق استخدام تقنيات التصوير عن بعد، فلم تعد محصورة في المنشآت العسكرية أو التجارب التقنية، وإنما أصبحت متاحة لتطبيقات صناعية وتجارية ومؤسسية متعددة. إلا أن التحدي الرئيس في هذه المرحلة لم يكن التقاط الصورة أو نقلها فحسب، وإنما كان يتمثل في كيفية الاحتفاظ بها والرجوع إليها بعد وقوع الحدث. فالمراقبة الحية تمكن المشغل من مشاهدة ما يحدث في اللحظة نفسها، لكنها لا توفر بالضرورة وسيلة لاستعادة ما حدث بعد انتهائه. ومن هنا أصبح تطوير تقنيات التسجيل أحد أهم المسارات التي أثرت في تطور أنظمة المراقبة.

رابعاً: ظهور التسجيل وتغير وظيفة المراقبة

أحدث إدخال تقنيات تسجيل الفيديو تحولًا مهمًا في وظيفة المراقبة. فقبل انتشار التسجيل العملي، كانت قيمة النظام تعتمد بدرجة كبيرة على وجود مشغل يتابع الصورة في وقت وقوع الحدث. أما عندما أصبح بالإمكان تسجيل المشاهد، فقد تحولت الصورة من معلومة آنية إلى معلومة يمكن الاحتفاظ بها ومراجعتها بعد وقوع الحدث.(8)

ارتبطت هذه المرحلة بتطور تقنيات التسجيل المغناطيسي ثم انتشار أجهزة تسجيل الفيديو، الأمر الذي جعل الاحتفاظ بالمشاهد أكثر عملية. ومع ذلك، ظلت الأنظمة التناظرية تواجه قيودًا تشغيلية، منها الاعتماد على وسائط تسجيل مادية، والحاجة إلى إدارتها وتخزينها، وصعوبة البحث اليدوي في كميات كبيرة من المواد المسجلة. وقد أسهم انتشار أجهزة الفيديو خلال السبعينيات في جعل التسجيل أكثر شيوعًا في أنظمة CCTV.(9)

وقد ترتب على ذلك تحول جوهري في الوظيفة الأمنية للنظام من المراقبة الحية إلى المراقبة + التسجيل + الاسترجاع .وهذا التحول بالغ الأهمية؛ لأن التسجيل جعل نظام

المراقبة قادرًا على توفير معلومات يمكن استخدامها أثناء الحدث وبعده، سواء لأغراض المراجعة أو التحقيق أو إعادة بناء تسلسل الوقائع. وقد اكتسبت التسجيلات المرئية لاحقًا أهمية إضافية في مجال الإثبات والتحقيق، وهو ما تناولته دراسات عربية قانونية تناولت حجية الصور المستمدة من كاميرات المراقبة في الإثبات الجنائي.(10)

خامساً: تعدد الكاميرات وظهور أنظمة التحكم المركزية

مع زيادة عدد الكاميرات المستخدمة في المنشآت والمواقع، ظهرت مشكلة جديدة تتمثل في كيفية إدارة مصادر متعددة للصورة في الوقت نفسه.(11)

فلم يعد التحدي مقتصرًا على تشغيل كاميرا واحدة، وإنما أصبح متعلقًا بقدرة المشغل على متابعة مواقع متعددة، والانتقال بين مصادر الصورة، وتحديد الكاميرا المرتبطة بحدث معين، وإدارة عمليات التسجيل والعرض. وقد أدى ذلك تدريجيًا إلى تطوير أجهزة وتقنيات تسمح بتبديل مصادر الصورة وإدارة عدد أكبر من الكاميرات، ثم إلى نظم أكثر قدرة على العرض المتعدد والتسجيل المتزامن. ومع اتساع نطاق الأنظمة، أخذ مفهوم مركز المراقبة في الظهور بوصفه نقطة تشغيل وإدارة لمجموعة من مصادر الفيديو.

ومن الناحية الأمنية، مثل هذا التطور انتقالًا من التعامل مع الكاميرا باعتبارها وحدة منفردة إلى التعامل مع مجموعة من الكاميرات باعتبارها منظومة. كما أدى تعدد مصادر الصورة إلى بروز أهمية العامل البشري والتنظيم التشغيلي؛ فأصبح من الضروري تحديد الكاميرات ذات الأولوية، وتنظيم العرض، وتحديد مسؤوليات المشغلين، ووضع إجراءات للتعامل مع الأحداث. وتؤكد الدراسات الحديثة المتعلقة بأداء أنظمة CCTV أن وظيفة العاملين وطريقة تشغيل النظام تمثلان جزءًا مهمًا من أداء المنظومة، وليس مجرد عنصر ثانوي فيها.(12)

سادساً: انتشار CCTV في البيئات العامة

شهدت ستينيات وسبعينيات القرن العشرين توسعًا تدريجيًا في استخدام كاميرات المراقبة في البيئات العامة وبعض مرافق النقل والشرطة، ولا سيما في المملكة المتحدة (13).

وتشـــير الأدبيات التاريخية إلى أن شـــرطة العاصـــمة البريطانية أجرت في عام ١٩٦٠ تجارب باستخدام كاميرات مؤقتة في ميدان Trafalgar Square لمراقبة الحشود خلال زيارة الدولة للملك والملكة التايلانديين، ثم اســتمرت تجارب اســتخدام CCTV في مناســبات وأماكن أخرى. وتوثق أرشــيفات هيئة النقل في لندن كذلك وجود مشــروع تجريبي لاستخدام CCTV في محطة Holborn خلال الفترة ١٩٦١–١٩٦٥.(14)

ويظهر من هذه التطبيقات أن المراقبة بالكاميرات بدأت تدخل تدريجيًا في بيئات تتسم بكثافة الحركة والتجمعات، وأصبحت مرتبطة بمهام تتجاوز المراقبة الصناعية المحدودة إلى مراقبة الأماكن العامة ودعم العمل الشــرطي. كما تشــير الأدبيات إلى أن انتشــار أنظمة المراقبة في الأماكن العامة على نطاق واســع لم يحدث دفعة واحدة، بل تطور تدريجيًا، وأن الانتشار الكبير في أوروبا والمملكة المتحدة تسارع بصورة ملحوظة منذ أواخر الثمانينيات والتسعينيات مع تحسن القدرات التقنية وانخفاض تكاليف التشغيل نسبيًا.(15)

ومن الأمثلة المهمة في هذا السياق مدينة King's Lynn في المملكة المتحدة؛ إذ بدأ تركيب الكاميرات في المنطقة الصناعية الشمالية للمدينة عام ١٩٨٧، ثم توسع النظام عام ١٩٩٢ ليشــمل مواقع في مركز المدينة. وقد ارتبط المشــروع في بدايته بمعالجة مشكلات محددة، من بينها السطو والأضرار الجنائية في المنطقة الصناعية، ثم توسع نطاق استخدامه.(16)

ويظهر من هذه المرحلة انتقال المراقبة من حماية موقع محدد إلى مراقبة بيئة أمنية أوسع وأكثر تعقيدًا .وقد فرض هذا الانتقال تحديات جديدة تتعلق بتوزيع الكاميرات، وتغطية المســاحات، وإدارة مصــادر الصــورة، وحفظ التســجيلات، وربط المراقبة بعمليات الاستجابة.

سابعاً: التحول من النظام التناظري إلى النظام الرقمي

يمثل التحول الرقمي إحدى أهم مراحل تطور أنظمة المراقبة؛ لأنه لم يقتصــر على تحســين جودة الصــورة، وإنما غيّر طبيعة المعلومات التي تنتجها المنظومة وطريقة تخزينها وإدارتها.(17)

ففي الأنظمة التناظرية كانت الصورة تنتقل وتسجل في بيئة تعتمد بدرجة كبيرة على الإشارات التناظرية ووسائط التسجيل المادية. أما الرقمنة فقد أتاحت تحويل الصور إلى بيانات رقمية يمكن تخزينها ومعالجتها والبحث فيها ونقلها بدرجة أكبر من المرونة. وأدى ذلك إلى ظهور أجهزة التسجيل الرقميDVR ، ثم تطورت تقنيات ضغط الفيديو وسعات التخزين ووسائل الاسترجاع، فأصبحت إدارة التسجيلات أكثر كفاءة مقارنة بالأساليب التناظرية التقليدية.

وكان من النتائج المهمة لهذا التحول أن الصورة لم تعد مجرد مادة مرئية محفوظة على شريط، بل أصبحت بيانات رقمية قابلة للإدارة والمعالجة والاسترجاع والتصدير والتكامل مع أنظمة أخرى. وقد أسهم ذلك في تحسين وظائف عملية متعددة، من بينها: سهولة البحث في التسجيلات، وتحسين إدارة التخزين، والوصول الأسرع إلى الأحداث، وإمكانية النسخ والتصدير، وإدارة عدد أكبر من الكاميرات، وتحسين إمكانات المراجعة والتحليل، والربط بين التسجيلات والمعلومات الأخرى.(18)

وهكذا أصبحت إدارة المعلومات المرئية جزءًا أساسيًا من تصميم منظومة المراقبة، ولم تعد وظيفة لاحقة لعملية تركيب الكاميرات. وتؤكد المتطلبات المهنية الحديثة لأنظمة CCTVأهمية جودة التسجيل والتخزين وإمكان تصدير المقاطع واسترجاعها وتشغيلها، وهو ما يعكس انتقال قيمة النظام من مجرد العرض إلى إدارة المعلومات المرئية بصورة متكاملة.(19)

ثامناً: ظهور كاميرات الشبكات والأنظمة القائمة على بروتوكول الإنترنت

أدى تطور شبكات الحاسوب وانتشار بروتوكول الإنترنت إلى ظهور جيل جديد من أنظمة المراقبة يعتمد على كاميرات الشبكات.(20) IP Cameras

وقد مثلت كاميرات IP تحولًا مهمًا؛ لأن الكاميرا لم تعد مجرد مصدر لإشارة فيديو تناظرية تحتاج إلى مسار مخصص للنقل، وإنما أصبحت جهازًا شبكيًا قادرًا على إرسال البيانات عبر البنية التحتية للشبكات والتواصل مع الخوادم والمنصات البرمجية وأنظمة الإدارة. وأدى هذا التحول إلى توسيع إمكانات النظام في مجالات متعددة، منها: الإدارة المركزية، والوصول عن بعد، وتوزيع مصادر الفيديو، والتكامل مع شبكات

وتقنيات المعلومات، وإدارة أعداد كبيرة من الكاميرات، والتوسع التدريجي في المنظومة، وربط الفيديو بمنصات وبرمجيات متعددة.

إلا أن الانتقال إلى الشبكات أوجد في الوقت نفسه فئة جديدة من المخاطر؛ إذ أصبحت أنظمة المراقبة مرتبطة بالشبكات والبرمجيات وحسابات المستخدمين والصلاحيات، ومن ثم لم تعد حماية النظام مقتصرة على حماية الكاميرات وأجهزة التسجيل ماديًا، بل أصبحت تشمل كذلك حماية البنية الشبكية والبيانات ووسائل الدخول إلى النظام. ومن هنا بدأ مفهوم أمن منظومة المراقبة نفسها يكتسب أهمية متزايدة؛ فالنظام الذي يوفر معلومات أمنية ولكنه غير محمي من العبث أو الوصول غير المصرح به قد يتحول من أداة للحماية إلى نقطة ضعف أمنية.(21)

تاسعاً: من تسجيل الفيديو إلى تحليل الفيديو

أحدث تطور قدرات المعالجة الحاسوبية تحولًا جديدًا في وظيفة أنظمة المراقبة؛ إذ لم تعد المنظومة مضطرة إلى الاكتفاء بتسجيل الصور وانتظار المشغل حتى يلاحظ الحدث، بل أصبح من الممكن استخدام خوارزميات لمعالجة محتوى الفيديو واكتشاف أنماط أو أحداث معينة.(22)

ومن أمثلة وظائف تحليل الفيديو: اكتشاف الحركة، وتحديد الدخول إلى منطقة معينة، واكتشاف بعض الأنماط غير المعتادة، وتتبع الأجسام، وتحليل حركة الأشخاص أو المركبات، ودعم البحث داخل كميات كبيرة من التسجيلات، وإصدار تنبيهات مرتبطة بأحداث أو شروط محددة.

وقد أدى ذلك إلى الانتقال من مفهوم Video Surveillance إلى مفهوم أوسع هو Video Analytics، أي من مجرد مشاهدة الفيديو إلى محاولة استخراج معلومات ذات معنى من محتواه. وهنا ينبغي التمييز بين التسجيل والتحليل؛ فالتسجيل يحفظ ما حدث، بينما يحاول التحليل تحديد ما قد يكون مهمًا داخل المحتوى المسجل أو الجاري عرضه. ولا يعني ذلك أن التحليل الآلي يستبدل المشغل البشري بصورة مطلقة؛ بل يغير طبيعة عمله، من متابعة كل محتوى الفيديو بصورة مستمرة إلى التعامل بصورة أكبر مع التنبيهات والمعلومات التي تستخرجها أدوات التحليل.

عاشراً: الذكاء الاصطناعي والجيل الحديث من أنظمة المراقبة

أصبح الذكاء الاصطناعي والتعلم الآلي وتحليل الصور والفيديو من أبرز الاتجاهات المؤثرة في الجيل الحديث من أنظمة المراقبة. وأصبح من الممكن دمج قدرات تحليلية متقدمة في الكاميرات أو أجهزة التسجيل أو الخوادم والمنصات البرمجية، بما يسمح باستخراج مؤشرات من الفيديو بصورة أسرع وأكثر أتمتة.(23)

وقد أدى ذلك إلى اتساع مفهوم المراقبة من مجرد التقاط الصورة وتسجيلها إلى : التقاط الصورة ← تحليلها ← استخراج معلومة ← تنبيه أو إجراء .ومع ذلك، فإن التطور في التحليل الذكي لا يعني أن القرار الأمني أصبح آليًا بصورة مطلقة. فالقيمة العملية لأي نظام تحليلي ترتبط بجودة البيانات، وملاءمة الخوارزمية للبيئة، ودقة إعداد النظام، وظروف الإضاءة والمشهد، وطريقة تفسير النتائج والتعامل معها من جانب المستخدمين.(24)

كما أن الأنظمة التحليلية الحديثة تفرض اعتبارات إضافية تتعلق بالدقة والخصوصية وحماية البيانات وإدارة الصلاحيات والمساءلة. ولذلك فإن التطور التقني في مجال المراقبة لا ينفصل عن التطور التنظيمي والقانوني. وتؤكد الأدبيات العربية الحديثة أن استخدام كاميرات المراقبة يرتبط كذلك بإشكالات قانونية وحقوقية، ولا سيما فيما يتعلق بالخصوصية والشفافية والتناسب في استخدام أنظمة المراقبة.(25)

حادي عشر: التحول من «الكاميرا» إلى «منظومة المراقبة الذكية»

- تاريخ تطور أنظمة المراقبة باعتباره انتقالًا تدريجيًا بين خمس مراحل وظيفية رئيسة:(26)

المرحلة	التكوين الوظيفي
المشاهدة	كاميرا ← شاشة
التسجيل	ثم تطور إلى : كاميرا ← شاشة ← تسجيل
الإدارة الرقمية	ثم : كاميرات متعددة ← مسجل رقمي/نظام إدارة ← مركز مراقبة
ثم المراقبة الشبكية	كاميرات IP ← شبكة ← خوادم ومنصات إدارة ← وصول متعدد

ثم المراقبة التحليلية	كاميرات ← معالجة وتحليل ← معلومات ← تنبيه/قرار/استجابة

ولا ينبغي فهم هذه المراحل على أنها فواصل زمنية صارمة أو بدائل يستبدل بعضها بعضًا بصورة كاملة؛ فالتقنيات الحديثة قد تجمع في الوقت نفسه بين مكونات تناظرية ورقمية وشبكية وتحليلية، بحسب طبيعة الموقع واحتياجاته والموارد المتاحة. والأهم أن التطور الحقيقي لم يكن مجرد زيادة دقة الكاميرا أو تحسين مكوناتها، وإنما كان تطورًا في قدرة النظام على تحويل المشهد المرئي إلى معلومات قابلة للاستخدام.

ثاني عشر: من المراقبة التقليدية إلى منظومات المراقبة المتكاملة

أدت التطورات المتلاحقة إلى أن أصبحت أنظمة المراقبة الحديثة جزءًا من بيئة تقنية وأمنية أوسع. فقد أصبحت الكاميرات قابلة للتكامل مع أنظمة التحكم في الدخول، وأنظمة الإنذار، وإدارة المباني، ومراكز القيادة والتحكم، ومنصات تحليل الفيديو وغيرها من التقنيات.(27)

وبذلك أصبح النظام الحديث لا يقاس فقط بقدرته على عرض الصور، وإنما بقدرته على ربط المعلومات المرئية بالأحداث والإجراءات الأمنية. ويمثل هذا التطور تحولًا مهمًا في التفكير الأمني؛ لأن قيمة الكاميرا لم تعد نابعة فقط من قدرتها على «رؤية» الموقع، وإنما من قدرتها على المساهمة في تكوين صورة أوضح عن الحالة الأمنية، وتوفير المعلومات التي تساعد في اتخاذ الإجراء المناسب.

وتؤكد المتطلبات المهنية الحديثة أن قيمة نظام CCTV ترتبط بعناصر متعددة، من بينها جودة الفيديو، والتخزين، وسهولة الاسترجاع والتشغيل، وإمكان تصدير التسجيلات، والمحافظة على سلامة المعلومات، وليس بمجرد وجود الكاميرات.(28)

ثالث عشر: دلالة التطور التاريخي على العمل الأمني

إن دراسة تطور أنظمة المراقبة تقود إلى نتيجة مهمة، وهي أن التطور التقني لم يكن منفصلًا عن تطور الاحتياجات الأمنية والتشغيلية. ففي البداية كانت الحاجة الأساسية تتمثل في المشاهدة عن بعد، ثم ظهرت الحاجة إلى الاحتفاظ بالمعلومات، ثم إلى إدارة عدد أكبر من الكاميرات، ثم إلى نقل البيانات عبر الشبكات، وأخيرًا إلى استخراج المعلومات آليًا من الفيديو.(29)

وهذا يعني أن التقنية كانت، في مراحل متعددة، تستجيب لمشكلة تشغيلية أو أمنية قائمة، وإن كان التطور التقني نفسه قد أوجد لاحقًا تطبيقات جديدة لم تكن متاحة في المراحل السابقة. ومن هنا ينبغي أن يكون هذا المنطق حاضرًا عند تقييم التقنيات الحديثة؛ فليس كل تطور تقني يمثل بالضرورة حاجة أمنية، وليس كل خاصية جديدة تؤدي تلقائيًا إلى تحسين مستوى الحماية.

فالقاعدة المهنية التي يمكن استخلاصها من التاريخ التطوري لأنظمة المراقبة هي : التقنية الناجحة أمنيًا هي التي تستجيب لاحتياج حقيقي، وتضيف قدرة قابلة للاستخدام والقياس والتقييم، وليس التي تكتفي بإضافة مواصفة تقنية جديدة.

المراجع:

① ينظر: Levente Tóth, "The Evolution of Public Surveillance Systems in Europe," *Magyar Rendészet*, Vol. 23, No. 1 (2023), pp. 191–204, DOI: 10.32577/mr.2023. 1. 12.

② ينظر: المرجع السابق، ص ١٩١–٢٠٤ .

③ راجع: المرجع السابق.

④ ينظر: المرجع السابق.

⑤ راجع: المصادر التاريخية والتقنية التي توثق استخدام نظام تلفزيوني مغلق في موقع اختبار صواريخ V-2 في بيـــنِمونديِه عام ١٩٤٢، ومنها: Tóth, "The Evolution of Public Surveillance Systems in Europe," pp. 191–204.

⑥ ينظر: "The Use of Television in Industry Progressed Steadily Throughout 1948," *Radio-Electronics*, March 1949.

⑦ راجع: المرجع السابق.

⑧ ينظر: Chris A. Williams, "Police Surveillance and the Emergence of CCTV in the 1960s," *Crime Prevention and Community Safety*, Vol. 5, No. 3 (2003).

⑨ راجع: المرجع السابق.

⑩ ينظر: مؤيد محمد مقبل العندلي، *كاميرات المراقبة ومدى حجيتها في الإثبات في التشريع الأردني*، رسالة ماجستير، كلية القانون، جامعة آل البيت، المفرق، ٢٠٢١، ص ١–٩٥ .

⑪ راجع: Tóth, "The Evolution of Public Surveillance Systems in Europe," pp. 191–204.

⑫ ينظر: Brandon C. Welsh, Eric L. Piza, Amanda L. Thomas, and David P. Farrington, "Private Security and Closed-Circuit Television (CCTV) Surveillance: A Systematic Review of Function and Performance," *Journal of Contemporary Criminal Justice*, Vol. 36, No. 1 (2020), pp. 56–69, DOI: 10.1177/1043986219890192.

⑬ راجع: Williams, "Police Surveillance and the Emergence of CCTV in the 1960s."

⑭ ينظر: Transport for London, *CCTV: Corporate Archives Research Guide*.

⑮ راجع: Tóth, "The Evolution of Public Surveillance Systems in Europe," pp. 191–204.

⑯ ينظر: Ken Pease, *Video Surveillance of Public Places: Lessons from a National Evaluation*، ومادة حالة King's Lynn المنشورة ضمن Center for Problem-Oriented Policing.

⑰ راجع: Tóth, "The Evolution of Public Surveillance Systems in Europe," pp. 191–204.

⑱ ينظر: Defence Science and Technology Laboratory (DSTL) and National Police Chiefs' Council (NPCC), *UK Police Requirements for CCTV Systems*, 2022.

⑲راجع: المرجع السابق.

⑳ينظر: Tóth, "The Evolution of Public Surveillance Systems in Europe," pp. 191–204.

㉑راجع: Defence Science and Technology Laboratory (DSTL) and National Police Chiefs' Council (NPCC), *UK Police Requirements for CCTV Systems*, 2022.

㉒ينظر: المرجع السابق.

㉓راجع: Tóth, "The Evolution of Public Surveillance Systems in Europe," pp. 191–204.

㉔ينظر: المرجع السابق.

㉕راجع: آمال عبدالجبار حسوني ونادية كعب جبر، «كاميرات المراقبة بين دواعي الاستعمال وانتهاك الخصوصية»، *مجلة الحقوق*، الجامعة المستنصرية، المجلد ٩، العددان ٢٩–٣٠ (٢٠١٧)، ص ١–١٨؛ وينظر أيضًا: أحمد علي حسن عثمان، «الضوابط القانونية لاستخدام أنظمة المراقبة التلفزيونية المغلقة CCTV في بيئة العمل: دراسة مقارنة بين القانون الفرنسي والمصري والنظام السعودي»، *مجلة البحوث القانونية والاقتصادية*، جامعة المنصورة، كلية الحقوق، العدد ٩٢ (٢٠٢٥)، ص ٢٢٢–٣٨٧.

㉖ينظر: Tóth, "The Evolution of Public Surveillance Systems in Europe," pp. 191–204.

㉗راجع: Defence Science and Technology Laboratory (DSTL) and National Police Chiefs' Council (NPCC), *UK Police Requirements for CCTV Systems*, 2022؛ وينظر: Home Office, *Surveillance Camera Code of Practice*, amended November 2021, effective 12 January 2022.

㉘ينظر: المرجع السابق.

㉙راجع: Tóth, "The Evolution of Public Surveillance Systems in Europe," pp. 191–204.

المبحث الثالث: تطور كاميرات المراقبة

بعد أن تناول المبحث السابق نشأة أنظمة المراقبة وتطورها، ينتقل هذا المبحث إلى تتبع تطور كاميرات المراقبة ذاتها، بوصفها المكون الأساسي في منظومة المراقبة. وقد شهدت الكاميرات تطورًا متسارعًا منذ بداياتها الميكانيكية والكيميائية، مرورًا بالمرحلة التناظرية بأجيالها المتعاقبة، وصولًا إلى المرحلة الرقمية والذكية التي نعيشها اليوم.(1)
وتكمن أهمية تتبع هذا التطور في أنه يكشف عن التحول الجوهري في قدرات الكاميرا ووظائفها، من مجرد جهاز لالتقاط الصورة إلى عنصر ذكي قادر على التحليل والاستنتاج واتخاذ القرار. كما يكشف عن العلاقة الجدلية بين تطور الكاميرا وتطور المنظومة الأمنية التي تعمل فيها.

أولاً: المرحلة الميكانيكية والكيميائية

قبل ظهور الكاميرات الإلكترونية، عرفت البشرية صوراً متعددة من أجهزة التصوير الميكانيكية والكيميائية التي استُخدمت لأغراض أمنية محدودة.(2)

الكاميرا المظلمة :(Camera Obscura) وهي أقدم صورة معروفة لأجهزة التصوير، وتعود جذورها إلى الحضارات القديمة، وقد استُخدمت في المراقبة الفلكية والرسم. ولم تكن كاميرا بالمعنى الدقيق، لكنها مهدت لفهم مبادئ التصوير البصري.(3)

التصوير الفوتوغرافي :مع اختراع التصوير الفوتوغرافي في القرن التاسع عشر، بدأ استخدامه في توثيق الأحداث الأمنية، خاصة في التحقيقات الجنائية. وقد كان التصوير الفوتوغرافي بطيئاً ومكلفاً، مما حدّ من استخدامه في المراقبة الفورية.(4)

الكاميرات الميكانيكية :ظهرت في أوائل القرن العشرين كاميرات ميكانيكية تستخدم في التصوير المتسلسل، وقد استُخدمت في بعض التطبيقات الأمنية المحدودة.(5)

ثانياً: المرحلة التناظرية

تُعدّ المرحلة التناظرية نقطة التحول الحقيقية في تاريخ كاميرات المراقبة، إذ شهدت ظهور أنظمة الدائرة التلفزيونية المغلقة (CCTV) التي أصبحت الأساس لأنظمة المراقبة الحديثة.(6)

الجيل الأول: كاميرات الأنبوب المفرغ(Vidicon)

ظهرت أول كاميرات المراقبة التناظرية في أربعينيات وخمسينيات القرن العشرين، واعتمدت على أنبوب Vidicon في التقاط الصورة. وقد كانت هذه الكاميرات كبيرة الحجم، ثقيلة الوزن، وتحتاج إلى إضاءة عالية، لكنها كانت البداية الحقيقية للمراقبة التلفزيونية.(7)

الجيل الثاني: كاميرات أنبوب أكسيد الرصاص

في الستينيات والسبعينيات، طُوّرت كاميرات أكثر حساسية للضوء باستخدام أنابيب أكسيد الرصاص، مما أتاح التصوير في ظروف إضاءة أقل. كما ظهرت كاميرات الفيديو المنزلية (Camcorder) التي أتاحت التسجيل المباشر.(8)

الجيل الثالث: كاميراتCCD

في الثمانينيات، ظهرت كاميرات CCD (Charge-Coupled Device) التي أحدثت ثورة في مجال المراقبة، إذ تميزت بحجم أصغر، وحساسية أعلى، وعمر افتراضي أطول، وجودة صورة أفضل. وقد أصبحت CCD التقنية السائدة في كاميرات المراقبة حتى بداية الألفية الثالثة.(9)

الجيل الرابع: كاميراتCMOS

مع بداية الألفية الثالثة، بدأت تقنية CMOS (Complementary Metal-Oxide-Semiconductor)تفرض نفسها في مجال المراقبة، إذ تميزت بتكلفة أقل، واستهلاك طاقة أقل، وقدرة على التكامل مع المعالجات الرقمية. وقد تفوقت CMOS على CCD في معظم التطبيقات الأمنية.(10)

ثالثاً: المرحلة الرقمية

شهدت المرحلة الرقمية تحولاً جذرياً في تقنيات كاميرات المراقبة، إذ انتقلت من الإشارة التناظرية إلى الإشارة الرقمية، مما أتاح جودة صورة أعلى، ومرونة أكبر في المعالجة والنقل والتخزين.(11)

الجيل الأول: الكاميرات الرقمية المبكرة

في التسعينيات، ظهرت أول كاميرات رقمية تستخدم في التطبيقات الأمنية، لكنها كانت محدودة الانتشار بسبب ارتفاع تكلفتها. وقد كانت تعتمد على معالجات رقمية داخلية لتحويل الإشارة التناظرية إلى رقمية.(12)

الجيل الثاني: كاميراتIP

مع بداية الألفية الثالثة، ظهرت كاميرات (Internet Protocol) IP التي تنقل الصورة عبر شبكات البيانات بدلاً من الكابلات المحورية. وقد أتاحت هذه الكاميرات مرونة هائلة في التركيب والتوسع، وتكاملاً مع أنظمة المعلومات.(13)

الجيل الثالث: الكاميرات عالية الدقة (HD) و٤K

شهدت العقد الثاني من الألفية الثالثة انتشاراً واسعاً لكاميرات عالية الدقة، بدءاً من ٧٢٠ pو١٠٨٠p، وصولاً إلى ٤ Kو٨ .Kوقد أتاحت هذه الكاميرات تفاصيل أوضح، وقدرة أكبر على التعرف على الوجوه واللوحات.(14)

الجيل الرابع: الكاميرات الذكية

في السنوات الأخيرة، بدأت تظهر كاميرات ذكية تحتوي على معالجات قوية قادرة على تنفيذ خوارزميات الذكاء الاصطناعي داخل الكاميرا نفسها. وتتيح هذه الكاميرات تحليلات متقدمة مثل التعرف على الوجوه، وكشف السلوكيات، وتتبع الأجسام، دون الحاجة إلى خوادم مركزية.(15)

رابعاً: محطات رئيسية في تطور الكاميرات

يمكن إيجاز المحطات الرئيسية في تطور كاميرات المراقبة في الجدول التالي:(16)

مراحل تطور التقنية؛ ففي الفترة السابقة لعام ١٩٤٠ بدأت بمرحلة الميكانيكية، وتمثلت أبرز ملامحها في بدايات التصوير البصري باستخدام الكاميرا المظلمة والتصوير الفوتوغرافي.

١. خلال الفترة 1940–1970ظهرت مرحلة التناظرية المبكرة مع ظهور أنظمة CCTV واستخدام أنبوب Vidicon.

٢. في الفترة 1970–1990، تطورت إلى مرحلة التناظرية المتقدمة، التي شهدت انتشارًا واسعًا لأنظمة المراقبة والتسجيل على الأشرطة، مع استخدام تقنيات CCD و.VCR

٣. الفترة 1990–2000بدأت مرحلة الرقمية المبكرة، حيث حدث تحول جزئي نحو الأنظمة الرقمية من خلال استخدام DVRوالكاميرات الرقمية.

٤. خلال الفترة 2000–2010، فقد انتقلت الأنظمة إلى مرحلة IPوالرقمية، مع التحول الشامل إلى التقنيات الرقمية واستخدام كاميرات IP و.NVR
٥. الفترة 2010–2020ظهرت مرحلة عالية الدقة، وتميزت بجودة تصوير مرتفعة وتقنيات ضغط متقدمة، مثل HDو٤K وH.265.
٦. منذ 2020وحتى الآن وصلت أنظمة المراقبة إلى المرحلة الذكية، التي تعتمد على معالجة البيانات داخل الكاميرا واستخدام الذكاء الاصطناعي والتحليلات الذكية، مما جعل النظام قادرًا على تحليل المشاهد واكتشاف الأحداث بصورة أكثر تطورًا.

خامساً: العوامل الدافعة لتطور الكاميرات

يمكن تحديد عدة عوامل دفعت تطور كاميرات المراقبة:(17)

العامل الأول: الحاجة إلى جودة صورة أعلى

كلما زادت الحاجة إلى تفاصيل أوضح للتعرف على الوجوه واللوحات، زاد الدفع نحو كاميرات عالية الدقة.

العامل الثاني: الحاجة إلى تغطية أوسع

دفعت الحاجة إلى تغطية مساحات أكبر ومواقع أكثر تعقيداً إلى تطوير كاميرات متحركة (PTZ) وكاميرات متعددة العدسات.

العامل الثالث: الحاجة إلى التشغيل في ظروف صعبة

دفعت الحاجة إلى المراقبة في ظروف إضاءة منخفضة أو ظروف جوية صعبة إلى تطوير كاميرات حرارية، وكاميرات ذات رؤية ليلية متقدمة.

العامل الرابع: الحاجة إلى التحليلات الذكية

دفعت الحاجة إلى تحليلات متقدمة إلى تطوير كاميرات بمعالجات قوية قادرة على تنفيذ خوارزميات الذكاء الاصطناعي.

العامل الخامس: الحاجة إلى التكامل

دفعت الحاجة إلى تكامل أنظمة المراقبة مع الأنظمة الأمنية الأخرى إلى تطوير كاميرات تدعم معايير التكامل المفتوحة مثل.ONVIF

سادساً: حدود التطور التقني

على الرغم من التطور الهائل في تقنيات الكاميرات، إلا أن هناك حدوداً لا يمكن تجاوزها:(18)

الحد الأول: قوانين الفيزياء

لا يمكن للكاميرا أن ترى ما لا يمكن رؤيته بصرياً، كالأشياء خلف الجدران أو في الظلام التام. وتظل قوانين البصريات والفيزياء حاكمة لقدرات الكاميرا.

الحد الثاني: جودة العدسة

جودة الصورة لا تتحدد بالمستشعر وحده، بل بالعدسة أيضاً. والعدسات الرخيصة قد تحد من جودة الصورة حتى مع مستشعر عالي الدقة.

الحد الثالث: الظروف البيئية

تتأثر جودة الصورة بالظروف البيئية كالإضاءة والغبار والأمطار والضباب، مما قد يحد من فعالية الكاميرا في بعض الظروف.

الحد الرابع: التكلفة

تظل التكلفة عاملاً محدوداً في اختيار الكاميرات، خاصة في المشاريع الكبيرة التي تتطلب مئات الكاميرات.

الحد الخامس: الخصوصية

تفرض اعتبارات الخصوصية والتشريعات القانونية حدوداً على استخدام الكاميرات في بعض المواقع، خاصة الأماكن الخاصة.

المراجع:

① ينظر: Levente Tóth, "The Evolution of Public Surveillance Systems in Europe," *Magyar Rendészet*, Vol. 23, No. 1 (2023), pp. 191–204.

② راجع: Michael Harris, *CCTV and Video Surveillance: Technology and Applications*, (Boston: McGraw-Hill, 4th Edition, 2020), p. 28.

③ ينظر: المرجع السابق، ص ٢٨.

④ راجع: Harris, *CCTV and Video Surveillance*, p. 32.

⑤ ينظر: David Brown, *Integrated Security Systems Design*, (New York: Butterworth-Heinemann, 3rd Edition, 2019), p. 56.

⑥ راجع: Robert Wilson, *Digital Video Processing for Security Systems*, (London: Springer, 2021), p. 24.

⑦ ينظر: Harris, *CCTV and Video Surveillance*, p. 32.

⑧ راجع: Brown, *Integrated Security Systems Design*, p. 56.

⑨ ينظر: Wilson, *Digital Video Processing for Security Systems*, p. 24.

⑩ راجع: سعد بن عبد العزيز المطيري، *التقنيات الحديثة في أنظمة المراقبة*، (الكويت: دار الفكر الأمني، الطبعة الأولى، ١٤٤٢هـ/٢٠٢١م)، ص ٣٤.

⑪ينظر: Wilson, *Digital Video Processing for Security Systems*, p. 31.

⑫راجع: خالد بن إبراهيم النفيعي، *إدارة أنظمة المراقبة: دراسة تطبيقية*، (الدمام: دار المجتمع للنشر، الطبعة الأولى، ١٤٤٤هـ/٢٠٢٣م)، ص ٦٧.

⑬ينظر: Brown, *Integrated Security Systems Design*, p. 62.

⑭راجع: فهد بن محمد العتيبي، *مكونات أنظمة المراقبة بالفيديو*، (الرياض: مكتبة الملك فهد الوطنية، ١٤٤٣هـ/٢٠٢٢م)، ص ٤٥.

⑮ينظر: Sarah Johnson, "Effectiveness of Video Surveillance in Crime Prevention: A Systematic Review," *Journal of Security Research*, Vol. 15, No. 3 (2020), p. 218.

⑯راجع: Tóth, "The Evolution of Public Surveillance Systems in Europe," pp. 191–204.

⑰ينظر: عبد الرحمن محمد السالم، "معايير الفعالية في أنظمة المراقبة الأمنية"، *المجلة العربية للدراسات الأمنية*، المجلد ٣٨، العدد ٢ (٢٠٢٢م)، ص ٧٥.

⑱راجع: Harris, *CCTV and Video Surveillance*, p. 45.

المبحث الرابع: الانتقال من الكاميرا إلى المنظومة

شهد مفهوم المراقبة بالفيديو تحولًا جوهريًا مع تطور تقنيات التصوير الرقمي والشبكات ومعالجة البيانات. فلم تعد الكاميرا في صورتها المعاصرة جهازًا منفردًا يقتصر دوره على التقاط الصور وتسجيلها، وإنما أصبحت جزءًا من منظومة مترابطة تتكون من عناصر مادية وبرمجية وتشغيلية وإدارية، تعمل بصورة متكاملة لتحقيق أهداف أمنية محددة (1).

ويكتسب هذا الانتقال أهمية خاصة لأنه يمثل نقطة التحول المنهجية التي يقوم عليها هذا الكتاب؛ فالكاميرا ذات المواصفات الفنية المرتفعة قد لا تحقق الغرض الأمني المطلوب إذا وُضعت في موقع غير مناسب، أو كانت زاوية رؤيتها غير ملائمة، أو أثرت الإضاءة في جودة الصورة، أو لم يكن التسجيل متاحًا عند الحاجة، أو لم تتوافر آليات مناسبة لإدارة النظام وتشغيله وصيانته (٢). ومن هنا تنطلق فكرة هذا الكتاب من مبدأ أساسي مفاده أن فاعلية منظومة المراقبة لا تُقاس بعدد الكاميرات ولا بارتفاع مواصفاتها التقنية وحدها، وإنما بقدرتها على تحقيق الهدف الأمني الذي صُممت من أجله.

أولًا: الفرق بين "الكاميرا" و"منظومة المراقبة"

قد يبدو الفرق بين المصطلحين بسيطًا في الظاهر، إلا أنه جوهري في الأثر الأمني. فالكاميرا جهاز تقني له مواصفات محددة (دقة، عدسة، مستشعر، معالجة)، بينما منظومة المراقبة نظام متكامل يتكون من مجموعة من العناصر المترابطة التي تعمل معًا لتحقيق غرض أمني محدد.(3)

ويمكن توضيح الفرق من خلال المقارنة التالية:

١. تختلف الكاميرا عن منظومة المراقبة من حيث طبيعتها ووظيفتها ودورها الأمني. فالكاميرا تُعد جهازًا ماديًا واحدًا يختص أساسًا بالتقاط الصورة، بينما تمثل منظومة المراقبة نظامًا متكاملًا من مكونات مترابطة يهدف إلى إنتاج معلومات أمنية قابلة للاستخدام.

٢. ويتم تقييم الكاميرا وفق المواصفات الفنية مثل الدقة والحساسية ومجال الرؤية، في حين تُقاس منظومة المراقبة وفق فاعليتها الأمنية وقدرتها على الوقاية والكشف والاستجابة والتوثيق.

٣. كما تختلف المسؤولية بينهما؛ فالكاميرا تُعد موردًا أو مكوّنًا يتولى اختياره أو تركيبه المختص، بينما تقع مسؤولية منظومة المراقبة على مدير الأمن أو مسؤول المنظومة.

٤. أخيرًا، يرتبط عمر الكاميرا بعمر الجهاز نفسه، في حين ترتبط المنظومة بمفهوم أوسع هو دورة حياة المنظومة واستمراريتها، بما يشمل التشغيل والصيانة والتطوير والتحديث.

ويترتب على هذا التمييز نتيجة عملية بالغة الأهمية :لا يمكن الحكم على منظومة المراقبة من خلال النظر إلى كاميراتها وحدها، كما لا يمكن الحكم على كاميرا من خلال مواصفاتها بمعزل عن المنظومة التي تعمل فيها .(4)

ثانيًا: مكونات منظومة المراقبة

تتكون منظومة المراقبة، في صورتها المتكاملة، من مجموعة من العناصر التي يمكن تصنيفها في ست مجموعات رئيسة:(5)

١. مكونات الالتقاط

تشمل الكاميرات بأنواعها المختلفة (ثابتة، متحركة، داخلية، خارجية، نهارية، ليلية، متخصصة)، والعدسات المرتبطة بها. وتمثل هذه المكونات نقطة البداية في المنظومة، إذ تلتقط المشهد المرئي وتحوله إلى إشارة قابلة للمعالجة.(6)

٢. مكونات النقل والاتصال

تشمل الشبكات والكابلات ووسائط الاتصال التي تنقل الإشارة من الكاميرات إلى أجهزة التسجيل والعرض. وقد تكون هذه المكونات تناظرية (كابلات محورية) أو رقمية) شبكات(IP ، وتؤثر بصورة مباشرة في جودة الإشارة واستقرارها.(7)

٣. مكونات المعالجة والإدارة

تشـــمل أنظمة إدارة الفيديو(VMS) ، والخوادم، ووحدات المعالجة، والبرمجيات المستخدمة لإدارة مصادر الفيديو وتسجيلها واسترجاعها ومراقبتها، فضلًا عن الوظائف التحليلية التي قد توفرها المنظومة.(8)

٤. مكونات التسجيل والتخزين

تشـمل أجهزة التسـجيلDVR) ، (NVR، ووحدات التخزين (أقراص صـلبة، خوادم، تخزين سحابي)، وبرمجيات إدارة التسجيلات. وتمثل هذه المكونات الذاكرة الحافظة للمنظومة، إذ تتيح استرجاع الأحداث بعد وقوعها.(9)

٥. مكونات العرض والمراقبة

تشـــمل الشـــاشـــات، ومحطات العمل، ومراكز المراقبة، وأنظمة التحكم. وتمثل هذه المكونات واجهة التفاعل بين المنظومة والمشغلين، إذ تتيح لهم متابعة المشاهد وإدارة الأحداث.(10)

٦. المكونات التشغيلية والبشرية

تشـمل السـياسـات، والإجراءات، والمشـغلين، وآليات الصـيانة، وإدارة الصـلاحيات. وتمثل هذه المكونات العنصر الذي كثيرًا ما يُغفل عند الحديث عن أنظمة المراقبة، مع أنه عنصر حاسم في فاعلية المنظومة.(11)

وتؤكد الأدبيات المهنية أن هذه المكونات ليست مجرد أجزاء منفصلة يمكن تجميعها، وإنما هي عناصـــر مترابطة يتوقف أداء كل منها على أداء الآخر، ويتوقف أداء المنظومة ككل على تكاملها.(12)

ثالثًا: خصائص المنظومة الأمنية المتكاملة

تتميز منظومة المراقبة المتكاملة، عن مجرد تجميع الكاميرات، بمجموعة من الخصائص الجوهرية: (13)

1. التكامل الوظيفي

تعمل مكونات المنظومة بصورة متكاملة لتحقيق غرض أمني مشترك، وليس كل مكون بمعزل عن الآخر. فالكاميرا لا تعمل إلا إذا كانت متصلة بالشبكة، والشبكة لا قيمة لها إذا لم تكن متصلة بأجهزة التسجيل، والتسجيل لا قيمة له إذا لم يكن قابلًا للاسترجاع (14).

2. التكامل التقني

تتوافق مكونات المنظومة تقنيًا مع بعضها البعض، وتدعم معايير التكامل المفتوحة مثل ONVIF، مما يسمح بالتبادل والتوسع والتطوير دون الحاجة إلى استبدال المنظومة بالكامل.(15)

3. التكامل التشغيلي

توجد إجراءات تشغيلية واضحة تحدد كيفية التعامل مع المنظومة، وكيفية الاستجابة للأحداث، وكيفية إدارة التسجيلات، وكيفية الصيانة. فالتقنية وحدها لا تكفي إذا لم تكن هناك إجراءات منظمة لتشغيلها.(16)

4. التكامل مع البيئة الأمنية

تتكامل المنظومة مع بقية عناصر البيئة الأمنية، من أنظمة تحكم في الدخول، وأنظمة إنذار، وأنظمة إطفاء، ومراكز قيادة وتحكم. فالكاميرا لا تعمل في فراغ، بل في سياق أمني أوسع.(17)

5. قابلية التوسع والتطوير

تتميز المنظومة المتكاملة بقابليتها للتوسع والتطوير دون الحاجة إلى إعادة تصميمها بالكامل، مما يحمي الاستثمار ويواكب التطور التقني.(18)

رابعًا: عوامل الانتقال من الكاميرا إلى المنظومة

هناك عدة عوامل دفعت إلى هذا الانتقال، يمكن إجمالها في خمسة عوامل رئيسة (19):

1. تعقيد التهديدات الأمنية

لم تعد التهديدات الأمنية بسيطة أو أحادية البعد، بل أصبحت معقدة ومتعددة المصادر. وهذا التعقيد يتطلب استجابة أمنية متكاملة لا يمكن أن توفرها كاميرا منفردة (20).

2. تعدد الوظائف المطلوبة

لم يعد المطلوب من نظام المراقبة مجرد التسجيل، بل أصبح المطلوب يشمل: الكشف الفوري، والتحليل الذكي، والتكامل مع الأنظمة الأخرى، ودعم اتخاذ القرار. وهذا التعدد يتطلب منظومة متكاملة.(21)

3. اتساع نطاق التغطية

مع اتساع المنشآت وتعدد المواقع، أصبح من الضروري إدارة مئات أو آلاف الكاميرات، وهذا لا يمكن أن يتم بصورة فعالة إلا من خلال منظومة متكاملة.(22)

4. التطور التقني

أتاح التطور التقني في مجالات الشبكات والتخزين والبرمجيات إمكانية بناء منظومات متكاملة، بعد أن كانت هذه الإمكانية محدودة في السابق.(23)

5. المتطلبات التنظيمية

فرضت التشريعات واللوائح في كثير من الدول متطلبات تنظيمية على أنظمة المراقبة، تتعلق بحماية البيانات، وإدارة الصلاحيات، والاحتفاظ بالتسجيلات، مما دفع نحو بناء منظومات متكاملة تلبي هذه المتطلبات.(24)

خامسًا: الفرق بين "الكفاءة الفنية" و"الفاعلية الأمنية"

من أهم ما يترتب على الانتقال من الكاميرا إلى المنظومة التمييز بين مفهومين كثيرًا ما يختلطان في الممارسة الأمنية: الكفاءة الفنية والفاعلية الأمنية.(25)

الكفاءة الفنية تعني قدرة المنظومة على أداء وظائفها التقنية بصورة صحيحة: التقاط الصورة، ونقلها، وتسجيلها، وعرضها، واسترجاعها. وتُقاس بمعايير تقنية مثل: دقة الصورة، ومعدل الإطارات، وسعة التخزين، واستقرار الشبكة.(26)

الفاعلية الأمنية تعني قدرة المنظومة على تحقيق الغرض الأمني الذي صُممت من أجله: الوقاية من المخاطر، والكشف عن الأحداث، ودعم الاستجابة، والتوثيق، ودعم

التحقيق. وتُقاس بمؤشرات أمنية مثل: معدل الكشف عن الأحداث، وسرعة الاستجابة، وقدرة التسجيلات على دعم التحقيق.(27)

وقد تكون منظومة عالية الكفاءة الفنية منخفضة الفاعلية الأمنية، إذا لم تُصمم وفق احتياجات أمنية حقيقية. وفي المقابل، قد تكون منظومة متوسطة الكفاءة الفنية عالية الفاعلية الأمنية، إذا صُممت بعناية ووُظفت بصورة صحيحة.(28)

وتبرز هنا قاعدة جوهرية :الكفاءة الفنية شرط ضروري للفاعلية الأمنية، لكنها ليست شرطًا كافيًا .فلا يمكن أن تكون المنظومة فعالة أمنيًا إذا كانت كفاءتها الفنية منخفضة، لكن الكفاءة الفنية العالية لا تضمن تلقائيًا الفاعلية الأمنية.(29)

سادسًا: متطلبات نجاح الانتقال إلى المنظومة

لا يتحقق الانتقال من الكاميرا إلى المنظومة بمجرد شراء معدات متكاملة، بل يتطلب مجموعة من المتطلبات التي يمكن إجمالها في ستة متطلبات رئيسة:(30)

1. التخطيط المبني على المخاطر

يبدأ التخطيط السليم من تحليل المخاطر وتحديد الأهداف الأمنية، ثم ينتقل إلى تحديد المتطلبات الفنية والتشغيلية، ثم إلى اختيار التقنية المناسبة. وليس العكس (31).

2. التصميم المتكامل

يُصمم النظام باعتباره منظومة متكاملة، بحيث تُراعى فيه العلاقات بين المكونات، والتكامل مع البيئة الأمنية، وقابلية التوسع والتطوير.(32)

3. الاختيار الموضوعي للمكونات

تُختار المكونات وفق معايير موضوعية ترتبط بالغرض الأمني، وليس وفق مواصفات تقنية مجردة أو اعتبارات تسويقية.(33)

4. التشغيل المنظم

تُوضع إجراءات تشغيل واضحة تحدد مسؤوليات المشغلين، وآليات التعامل مع الأحداث، وإجراءات التصعيد، وآليات التوثيق والإبلاغ.(34)

5. الصيانة الوقائية

تُوضع برامج صيانة وقائية تضمن استمرارية عمل المنظومة، وتحد من الأعطال المفاجئة، وتطيل عمر المكونات.(35)

6. التقييم المستمر

يُقيَّم أداء المنظومة بصورة دورية، وفق مؤشرات موضوعية، لتحديد نقاط القوة والقصور، واتخاذ إجراءات التحسين المناسبة.(36)

المراجع:

① راجع: International Electrotechnical Commission, *IEC 62676-1-1: Video surveillance systems for use in security applications – Part 1-1: System requirements – General*, (Geneva: IEC, 2019), Clause 4. 2.

② ينظر: David Brown, *Integrated Security Systems Design*, (New York: Butterworth-Heinemann, 3rd Edition, 2019), p. 45.

③ راجع: خالد بن إبراهيم النفيعي، *إدارة أنظمة المراقبة: دراسة تطبيقية*، (الدمام: دار المجتمع للنشر، الطبعة الأولى، ١٤٤٤هـ/٢٠٢٣م)، ص ٤٥ .

④ ينظر: Michael Harris, *CCTV and Video Surveillance: Technology and Applications*, (Boston: McGraw-Hill, 4th Edition, 2020), p. 67.

⑤ راجع: International Electrotechnical Commission, *IEC 62676-1-1*, Clause 4. 3.

⑥ ينظر: فهد بن محمد العتيبي، *مكونات أنظمة المراقبة بالفيديو*، (الرياض: مكتبة الملك فهد الوطنية، ١٤٤٣هـ/٢٠٢٢م)، ص ٢٣-٣٠.

⑦ راجع: عبد الله بن حسن الشهري، *شبكات نقل الفيديو الأمني*، (الرياض: معهد الإدارة العامة، ١٤٤٤هـ/٢٠٢٣م)، ص ٣٤ .

⑧ ينظر: Robert Wilson, *Digital Video Processing for Security Systems*, (London: Springer, 2021), p. 78.

⑨ راجع: سعد بن عبد العزيز المطيري، *التقنيات الحديثة في أنظمة المراقبة*، (الكويت: دار الفكر الأمني، الطبعة الأولى، ١٤٤٢هـ/٢٠٢١م)، ص ٥٦ .

⑩ ينظر: Brown, *Integrated Security Systems Design*, p. 89.

⑪ راجع: Biometrics and Surveillance Camera Commissioner, *Surveillance Camera Code of Practice*, United Kingdom, revised 2021, Principle 3.

⑫ ينظر: Smith, *Security Surveillance Systems*, p. 78.

⑬ راجع: النفيعي، *إدارة أنظمة المراقبة*، ص ٦٧.

⑭ ينظر: International Electrotechnical Commission, *IEC 62676-1-1*, Clause 4. 5.

⑮ راجع: وزارة الداخلية، *الدليل المهني لأنظمة المراقبة الأمنية*، (الرياض: الإدارة العامة للأمن، ٢٠٢١م)، ص ٣٤ .

⑯ ينظر: Brown, *Integrated Security Systems Design*, p. 112.

⑰ راجع: العتيبي، *مكونات أنظمة المراقبة بالفيديو*، ص ٨٩.

⑱ ينظر: Harris, *CCTV and Video Surveillance*, p. 89.

⑲ راجع: Sarah Johnson, "Effectiveness of Video Surveillance in Crime Prevention: A Systematic Review," *Journal of Security Research*, Vol. 15, No. 3 (2020), p. 220.

⑳ ينظر: Wilson, *Digital Video Processing for Security Systems*, p. 112.

㉑ راجع: الشهري، *شبكات نقل الفيديو الأمني*، ص ٧٨.

㉒ ينظر: Brown, *Integrated Security Systems Design*, p. 134.

㉓ راجع: European Union, *General Data Protection Regulation (GDPR)*, (Brussels: Official Journal of the European Union, 2016), Article 35.

㉔ ينظر: Smith, *Security Surveillance Systems*, p. 112.

㉕راجع: عبد الرحمن محمد السالم، "معايير الفعالية في أنظمة المراقبة الأمنية"، *المجلة العربية للدراسات الأمنية*، المجلد ٣٨، العدد ٢ (٢٠٢٢م)، ص ٦٧.

㉖ينظر: Johnson, "Effectiveness of Video Surveillance in Crime Prevention," p. 225.

㉗راجع: النفيعي، *إدارة أنظمة المراقبة*، ص ٨٩.

㉘ينظر: Harris, *CCTV and Video Surveillance*, p. 112.

㉙راجع: وزارة الداخلية، *الدليل المهني لأنظمة المراقبة الأمنية*، ص ٤٥ .

㉚ينظر: International Organization for Standardization, *ISO 22341:2021 Security and resilience — Protective security — Guidelines for crime prevention through environmental design*, (Geneva: ISO, 2021), Clause 5. 3.

㉛راجع: Brown, *Integrated Security Systems Design*, p. 156.

㉜ينظر: Smith, *Security Surveillance Systems*, p. 134.

㉝راجع: المطيري، *التقنيات الحديثة في أنظمة المراقبة*، ص ٨٩.

㉞ينظر: Wilson, *Digital Video Processing for Security Systems*, p. 145.

㉟راجع: السالم، "معايير الفعالية في أنظمة المراقبة الأمنية"، ص ٧٨.

المبحث الخامس: موقع المراقبة ضمن منظومة أمن المنشآت

لا تعمل كاميرات المراقبة في فراغ أمني، وإنما تشكل جزءًا من منظومة أوسع لحماية الأشخاص والممتلكات والمعلومات والعمليات والمنشآت (١). ومن ثم فإن تقييمها ينبغي أن يتم في إطار منظومة أمن المنشأة ككل، وليس بمعزل عن بقية عناصر الحماية. فالكاميرات ليست بديلًا عن الحراسة، ولا عن أنظمة التحكم في الدخول، ولا عن الإجراءات التنظيمية، بل هي عنصر مكمل لها جميعًا.(2)

أولًا: مفهوم أمن المنشآت

يقوم أمن المنشآت على مجموعة من التدابير والسياسات والوسائل التي تهدف إلى حماية المنشأة ومواردها ومستخدميها من المخاطر والتهديدات، مع المحافظة على استمرارية أعمالها ووظائفها الأساسية (٣). ويشمل هذا المفهوم:

١. الأمن المادي: (Physical Security) حماية الموقع والمباني والأصول المادية من التهديدات المادية.
٢. الأمن البشري: (Personnel Security) حماية الأفراد والتحقق من صلاحيتهم.
٣. أمن المعلومات: (Information Security) حماية المعلومات والبيانات من الوصول غير المصرح به.
٤. الأمن السيبراني: (Cybersecurity) حماية الأنظمة والشبكات من الهجمات الإلكترونية.(4)

وتختلف طبيعة هذه التدابير باختلاف نوع المنشأة وموقعها وطبيعة أنشطتها ومستوى المخاطر التي تواجهها، ولذلك لا توجد منظومة أمن موحدة تصلح لجميع المنشآت (5).

ثانيًا: مبادئ أمن المنشآت

تقوم منظومة أمن المنشآت على مجموعة من المبادئ الأساسية التي توجه تصميمها وتشغيلها: (6)

1. مبدأ الدفاع في العمق (Defense in Depth)

يعني هذا المبدأ أن الحماية لا تعتمد على طبقة واحدة، بل على طبقات متعددة متراكبة، بحيث يؤدي اختراق طبقة إلى مواجهة طبقة أخرى. وتشمل هذه الطبقات: المحيط الخارجي، والمبنى، والمناطق الداخلية، والأصول الحساسة.(7)

2. مبدأ الطبقات الأمنية(Security Layers) تُنظم الحماية في طبقات متتالية، تبدأ من المحيط الخارجي وتنتهي بالأصول الأكثر حساسية. وكل طبقة لها إجراءاتها ووسائلها المحددة.(8)

3. مبدأ التوازن بين الحماية والاستخدام

يجب أن توازن إجراءات الحماية بين توفير الأمن من جهة، وعدم تعطيل الاستخدام الطبيعي للمنشأة من جهة أخرى. فالحماية المفرطة قد تعطل العمل، والحماية الضعيفة تعرض المنشأة للخطر.(9)

4. مبدأ التكامل بين العناصر

تتكامل العناصر البشرية والتنظيمية والتقنية لتحقيق الحماية الشاملة. فلا يمكن الاعتماد على عنصر واحد بمعزل عن الآخر.(10)

5. مبدأ التقييم المستمر

تُقيَّم منظومة الأمن بصورة دورية لتحديد نقاط القوة والقصور، ومواكبة تطور التهديدات والمخاطر.(11)

ثالثًا: عناصر منظومة أمن المنشآت: تتكون منظومة أمن المنشآت من مجموعة من العناصر التي يمكن تصنيفها في أربع مجموعات رئيسة:(12)

1. العنصر البشري

يشمل الحراس، وأفراد الأمن، ومشغلي الأنظمة، والمشرفين. ويمثل العنصر البشري حجر الزاوية في المنظومة الأمنية، إذ يتولى المهام التي لا تستطيع التقنية أداءها، مثل: التفسير، والحكم، واتخاذ القرار، والتفاعل مع الأحداث.(13)

2. العنصر التنظيمي

يشمل السياسات، والإجراءات، والتعليمات، والخطط الأمنية. ويوفر العنصر التنظيمي الإطار الذي تعمل فيه بقية العناصر، ويحدد المسؤوليات والصلاحيات وآليات التنسيق (14).

3. العنصر التقني

يشـــمل أنظمة المراقبة، وأنظمة التحكم في الدخول، وأنظمة الإنذار، وأنظمة الإطفاء، وأنظمة الاتصـــالات. ويوفر العنصـــر التقني القدرات التي تعزز كفاءة العنصـــر البشـــري وتوسع نطاق عمله.(15)

4. العنصر المادي

يشـــمل الأســـوار، والبوابات، والأقفال، والحواجز، والإضـــاءة. ويوفر العنصـــر المادي الحماية الأساسية التي تعد أساسًا لبقية العناصر.(16)

رابعًا: موقع المراقبة ضمن منظومة أمن المنشآت

تقع المراقبة في قلب منظومة أمن المنشآت، وتتفاعل مع جميع عناصرها:(17)

1. التفاعل مع العنصر البشري

تعزز المراقبة قدرات العنصر البشري من خلال: توسيع نطاق الرؤية بما يتجاوز القدرات البشرية، وتوفير معلومات فورية لمتخذي القرار، وتوثيق الأحداث لدعم التحقيق، ودعم الحراس في أداء مهامهم.(18)

2. التفاعل مع العنصر التنظيمي

تدعم المراقبة العنصـــر التنظيمي من خلال: توفير معلومات لدعم اتخاذ القرار، وتوثيق الالتزام بالإجراءات، ودعم تقييم فعالية الإجراءات، وتوفير أدلة للتحقيق في المخالفات (19).

3. التفاعل مع العنصر التقني

تتكـامـل المراقبـة مع بقيـة الأنظمـة التقنيـة من خلال: الربط مع أنظمـة التحكم في الـدخول لتوثيق عمليـات الـدخول، والربط مع أنظمـة الإنـذار للتحقق من الإنـذارات، والربط مع أنظمة الإطفاء لتوثيق الأحداث، والتكامل مع مراكز القيادة والتحكم.(20)

4. التفاعل مع العنصر المادي

تتكـامـل المراقبـة مع العنصـــر المـادي من خلال: مراقبـة الأســـوار والبوابـات، وتوثيق محـاولات الاختراق، ودعم تقييم فعـاليـة الحواجز، وتوفير معلومـات لتطوير العنصـــر المادي.(21)

خامسًا: وظائف المراقبة ضمن منظومة أمن المنشآت

يمكن تحديد وظائف المراقبة ضمن منظومة أمن المنشآت في خمس وظائف رئيسة (22):

1. وظيفة الكشف(Detection)

تتمثل في اكتشاف الأحداث والأنشطة المشبوهة، وتنبيه العاملين لاتخاذ الإجراء المناسب. وتشمل هذه الوظيفة: الكشف عن التسلل، والكشف عن الحركة غير المعتادة، والكشف عن الأحداث الأمنية.(23)

2. وظيفة التأخير(Delay)

تتمثل في إعاقة تقدم المهاجم أو المتسلل، من خلال توفير معلومات تتيح للعاملين التدخل في الوقت المناسب. وهذا التأخير قد يكون كافيًا لمنع إتمام الهجوم أو لتقليل آثاره.(24)

3. وظيفة الاستجابة(Response)

تتمثل في توفير معلومات لدعم الاستجابة الفعالة، من خلال تحديد مكان الحدث وطبيعته ومداه، وتوجيه العاملين إلى الإجراء المناسب.(25)

4. وظيفة التوثيق(Documentation)

تتمثل في تسجيل الأحداث وتوثيقها توثيقًا يمكن الرجوع إليه في المراجعة أو التحقيق أو المساءلة.(26)

5. وظيفة الردع(Deterrence)

تتمثل في ردع المهاجمين المحتملين من خلال إدراكهم أن الموقع يخضع للمراقبة، وأن احتمال اكتشافهم قائم.(27)

سادسًا: مبادئ تكامل المراقبة مع منظومة أمن المنشآت

لضمان تكامل فعال للمراقبة مع منظومة أمن المنشآت، ينبغي مراعاة مجموعة من المبادئ:(28)

1. مبدأ التكامل الوظيفي

تعمل المراقبة كجزء من منظومة متكاملة، وليس كنظام منفصل. ويجب أن تكون وظائفها متكاملة مع وظائف بقية العناصر.(29)

2. مبدأ التوزيع الأمثل

تُوزع كاميرات المراقبة وفق تحليل المخاطر، بحيث تغطي النقاط الحرجة والمسارات الحيوية والمناطق الحساسة.(30)

3. مبدأ التكامل التقني

تتكامل أنظمة المراقبة تقنيًا مع بقية الأنظمة الأمنية، من خلال معايير التكامل المفتوحة والبروتوكولات الموحدة.(31)

4. مبدأ التكامل التشغيلي

تُوضع إجراءات تشغيلية موحدة تحدد كيفية تفاعل المراقبة مع بقية العناصر، وكيفية التعامل مع الأحداث.(32)

5. مبدأ التكامل المعلوماتي

تتكامل معلومات المراقبة مع معلومات بقية الأنظمة، لتكوين صورة شاملة عن الحالة الأمنية.(33)

سابعًا: نماذج تكامل المراقبة مع منظومة أمن المنشآت

نماذج تكامل المراقبة مع منظومة أمن المنشآت في ثلاثة نماذج رئيسة (٣٤)

1. النموذج المستقل

تعمل فيه المراقبة كنظام مستقل عن بقية الأنظمة، مع تبادل محدود للمعلومات. وهذا النموذج أقل كفاءة، لكنه أبسط في التنفيذ.(35)

2. النموذج المتكامل جزئيًا

تتكامل فيه المراقبة مع بعض الأنظمة دون غيرها، مع تبادل جزئي للمعلومات. وهذا النموذج أكثر كفاءة من المستقل، لكنه لا يحقق التكامل الكامل.(36)

3. النموذج المتكامل كليًا

تتكامل فيه المراقبة مع جميع الأنظمة الأمنية، مع تبادل كامل للمعلومات، وتنسيق كامل للإجراءات. وهذا النموذج هو الأعلى كفاءة، لكنه الأكثر تعقيدًا في التنفيذ.(37)

المراجع

① راجع: International Organization for Standardization, *ISO 22341:2021 Security and resilience — Protective security — Guidelines for crime prevention through environmental design*, (Geneva: ISO, 2021), Clause 5. 3.

② ينظر: David Brown, *Integrated Security Systems Design*, (New York: Butterworth-Heinemann, 3rd Edition, 2019), p. 23.

③ راجع: محمد عبد الله الأحمدي، *الأمن الوقائي: المفاهيم والاستراتيجيات*، (الرياض: دار النشر الأكاديمي، الطبعة الثانية، ١٤٤٣هـ/٢٠٢٢م)، ص ٦٧.

④ ينظر: Brown, *Integrated Security Systems Design*, p. 45.

⑤ راجع: خالد بن إبراهيم النفيعي، *إدارة أنظمة المراقبة: دراسة تطبيقية*، (الدمام: دار المجتمع للنشر، الطبعة الأولى، ١٤٤٤هـ/٢٠٢٣م)، ص ٥٦ .

⑥ ينظر: International Organization for Standardization, *ISO 22341:2021*, Clause 5. 3.

⑦ راجع: Brown, *Integrated Security Systems Design*, p. 56.

⑧ ينظر: Smith, *Security Surveillance Systems*, p. 45.

⑨ راجع: وزارة الداخلية، *الدليل المهني لأنظمة المراقبة الأمنية*، (الرياض: الإدارة العامة للأمن، ٢٠٢١م)، ص ٢٣ .

⑩ ينظر: Brown, *Integrated Security Systems Design*, p. 67.

⑪ راجع: النفيعي، *إدارة أنظمة المراقبة*، ص ٦٧.

⑫ ينظر: Smith, *Security Surveillance Systems*, p. 56.

⑬ راجع: سعد بن عبد العزيز المطيري، *التقنيات الحديثة في أنظمة المراقبة*، الطبعة الأولى، ١٤٤٢هـ/٢٠٢١م)، ص ٧٨.

⑭ ينظر: وزارة الداخلية، *الدليل المهني لأنظمة المراقبة الأمنية*، ص ٣٤ .

⑮ راجع: فهد بن محمد العتيبي، *مكونات أنظمة المراقبة بالفيديو*، (الرياض: مكتبة الملك فهد الوطنية، ١٤٤٣هـ/٢٠٢٢م)، ص ٤٥ .

⑯ ينظر: Brown, *Integrated Security Systems Design*, p. 78.

⑰ راجع: Smith, *Security Surveillance Systems*, p. 67.

⑱ ينظر: المطيري، *التقنيات الحديثة في أنظمة المراقبة*، ص ٨٩.

⑲ راجع: النفيعي، *إدارة أنظمة المراقبة*، ص ٧٨.

⑳ ينظر: Brown, *Integrated Security Systems Design*, p. 89.

㉑ راجع: العتيبي، *مكونات أنظمة المراقبة بالفيديو*، ص ٥٦ .

㉒ ينظر: Smith, *Security Surveillance Systems*, p. 78.

㉓ راجع: Sarah Johnson, "Effectiveness of Video Surveillance in Crime Prevention: A Systematic Review," *Journal of Security Research*, Vol. 15, No. 3 (2020), p. 220.

㉔ ينظر: Brown, *Integrated Security Systems Design*, p. 102.

㉕ راجع: وزارة الداخلية، *الدليل المهني لأنظمة المراقبة الأمنية*، ص ٤٥ .

㉖ ينظر: Smith, *Security Surveillance Systems*, p. 89.

㉗ راجع: Johnson, "Effectiveness of Video Surveillance in Crime Prevention," p. 225.

㉘ ينظر: Brown, *Integrated Security Systems Design*, p. 112.

㉙ راجع: النفيعي، *إدارة أنظمة المراقبة*، ص ٨٩.

㉚ ينظر: International Organization for Standardization, *ISO 22341:2021*, Clause 5. 3.

㉛ راجع: العتيبي، *مكونات أنظمة المراقبة بالفيديو*، ص ٦٧.

㉜ ينظر: Smith, *Security Surveillance Systems*, p. 102.

㉝ راجع: المطيري، *التقنيات الحديثة في أنظمة المراقبة*، ص ١٠٢ .

㉞ ينظر: Brown, *Integrated Security Systems Design*, p. 134.

㉟ راجع: وزارة الداخلية، *الدليل المهني لأنظمة المراقبة الأمنية*، ص ٥٦ .

㊱ ينظر: Smith, *Security Surveillance Systems*, p. 112.

㊲ راجع: النفيعي، *إدارة أنظمة المراقبة*، ص ١٠٢ .

المبحث السادس: حدود دور كاميرات المراقبة

على الرغم من التطور الكبير الذي شـــهدته تقنيات المراقبة بالفيديو، فإن التعامل معها باعتبارها حلًا شاملًا للمشكلات الأمنية يمثل تصورًا غير دقيق (١). فالكاميرا أداة أمنية ذات قدرات محددة، وتتوقف قيمتها على طبيعة الخطر، وتصـــميم المنظومة، والبيئة التشغيلية، والعنصر البشري، وبقية إجراءات الحماية. ولا يمكن اعتبار وجود الكاميرات دليلًا بذاته على ارتفاع مستوى الحماية.(2)

أولًا: ضرورة الاعتراف بحدود المراقبة

قد يسـود في بعض البيئات الأمنية اعتقاد مفاده أن تركيب كاميرات المراقبة كفيل بحل المشـكلات الأمنية، وأن زيادة عدد الكاميرات تعني بالضـرورة زيادة مسـتوى الحماية. وهذا الاعتقاد، على الرغم من شيوعه، إلا أنه لا يستند إلى أساس علمي أو عملي.(3)

وتؤكـد المراجعـات المنهجيـة لتـأثير CCTV على الجريمـة أن نتـائج المراقبـة تتفـاوت بـاختلاف المواقع والظروف وطريقـة التطبيق. فقـد خلصـــت مراجعـة Welsh و Farringtonلعام ٢٠٠٨، التي شـــملت ٤٤ تقييمًا، إلى أن أثر CCTV في خفض الجريمة كان متواضعًا إجمالًا، مع تفاوت الفاعلية بين البيئات، وظهور نتائج أفضل في مواقف السيارات، كما لم تجد المراجعة أثرًا واضحًا في مستويات الجرائم العنيفة (٤).

أما المراجعة المنهجية والتحليل التلوي الذي أجراه Piza وزملاؤه، فقد وجدا انخفاضًـا متواضعًا ودالًا في الجريمة، مع أقوى الآثار وأكثرها اتساقًا في مواقف السيارات.(5)

وهـذه النتـائج تؤكـد أن الحكم على فـاعليـة CCTV ينبغي أن يراعي نوع البيئة وطريقة التطبيق والغرض الأمني، وأن الاعتراف بحدود المراقبة ليس تقليلًا من قيمتها، بل هو شرط أساسي لاستخدامها بصورة فعالة ومسؤولة.(6)

ثانيًا: الحدود التقنية

تتعلق الحدود التقنية بالقدرات الفنية لكاميرات المراقبة ذاتها، ويمكن إجمالها في ستة حدود رئيسة:(7)

1. حدود مجال الرؤية

لكل كاميرا مجال رؤية محدود، ولا يمكنها تغطية كل شـــيء. وتزداد هذه المحدودية مع اتســـاع المســـاحات وكثافة العوائق. وقد توجد مناطق عمياء لا تغطيها الكاميرات، مما يمثل ثغرة أمنية.(8)

2. حدود الدقة

على الرغم من التطور الهـائـل في دقـة الكـاميرات، إلا أن هنـاك حـدودًا لمـا يمكن تمييزه. فـالتعرف على الوجوه أو اللوحـات يتطلـب دقـة معينـة، وقـد لا تتوافر هـذه الـدقـة في جميع الظروف (9).

3. حدود الإضاءة

تتأثر جودة الصـــورة بصـــورة مباشـــرة بمستوى الإضاءة. وفي الظروف ضعيفة الإضـــاءة، قد تنخفض جودة الصـــورة بصـــورة ملحوظة، حتى مع اســـتخدام تقنيات الرؤية الليلية.(10)

4. حدود الظروف البيئية

تتأثر الكاميرات بالظروف البيئية كالغبار والأمطار والضباب ودرجات الحرارة العالية. وقد تؤدي هذه الظروف إلى تشويش الصورة أو تعطيل الكاميرا.(11)

5. حدود التخزين

ســعة التخزين محدودة، ومدة الاحتفاظ بالتســجيلات محدودة كذلك. وهذا يعني أن بعض الأحداث قد لا تكون مســـجلة عند الحاجة إليها، إذا انقضـــت مدة الاحتفاظ (12).

6. حدود النقل

تعتمد جودة النقل على نوعية الشــبكة والكابلات. وقد تؤدي مشــكلات الشــبكة إلى تأخير في نقل الصورة أو فقدان بعض الإطارات، مما يؤثر في جودة التسجيل.(13)

ثالثًا: الحدود البشرية

تتعلق الحدود البشـــرية بقدرات العنصـــر البشـــري على متابعة المراقبة والتفاعل معها، ويمكن إجمالها في أربعة حدود رئيسة:(14)

1. حدود الانتباه

لا يستطيع الإنسان متابعة شاشات المراقبة بتركيز كامل لفترات طويلة. فالقدرة على الانتباه تتراجع مع الوقت، مما قد يؤدي إلى تفويت أحداث مهمة.(15)

2. حدود الإدراك

لا يستطيع الإنسان معالجة كميات كبيرة من المعلومات في وقت واحد. وعندما تكون هناك شاشات متعددة، قد لا يتمكن المشغل من متابعة جميع الأحداث.(16)

3. حدود التفسير

يتطلب تفســـير الأحداث الأمنية خبرة ومعرفة، وقد يخطئ المشـــغل في تفســـير بعض الأحداث، إما باعتبارها عادية وهي مشبوهة، أو العكس.(17)

4. حدود الاستجابة

تتأثر سرعة الاستجابة بعوامل بشرية متعددة، منها: التعب، والإرهاق، والضغط النفسي. وقد تؤدي هذه العوامل إلى تأخر في الاستجابة أو خطأ في القرار.(18)

رابعًا: الحدود التنظيمية

تتعلق الحدود التنظيمية بالإطار الذي تعمل فيه منظومة المراقبة، ويمكن إجمالها في أربعة حدود رئيسة:(19)

1. حدود التشريعات

تفرض التشـــريعات واللوائح في كثير من الدول قيودًا على اســـتخدام كاميرات المراقبة، خاصـــة فيما يتعلق بالخصـــوصـــية وحماية البيانات. وقد تحد هذه القيود من نطاق استخدام الكاميرات أو من طريقة تشغيلها.(20)

2. حدود الموارد

تتطلب منظومات المراقبة موارد مالية وبشرية وتقنية. وقد تحد محدودية الموارد من قدرة المنشأة على بناء منظومة متكاملة أو على صيانتها.(21)

3. حدود الكفاءات

تتطلب إدارة منظومات المراقبة كفاءات متخصصة، قد لا تتوافر في بعض المنشآت. وقد يؤدي نقص الكفاءات إلى سوء تشغيل المنظومة أو عدم الاستفادة منها.(22)

4. حدود التنسيق

يتطلب التكامل بين المراقبة وبقية عناصر المنظومة الأمنية تنسيقًا بين جهات متعددة. وقد يؤدي ضعف التنسيق إلى تكرار الجهود أو تعارضها.(23)

خامسًا: الحدود الأخلاقية والقانونية

تتعلق الحدود الأخلاقية والقانونية بالإشكاليات التي يطرحها استخدام كاميرات المراقبة، ويمكن إجمالها في أربعة حدود رئيسة:(24)

1. حد الخصوصية

تطرح كاميرات المراقبة إشكالية الخصوصية، خاصة عندما تُستخدم في أماكن خاصة أو عندما تُسجل تفاصيل شخصية. ويتطلب الأمر موازنة دقيقة بين متطلبات الأمن وحقوق الخصوصية.(25)

2. حد الموافقة

يتطلب استخدام كاميرات المراقبة في بعض البيئات الحصول على موافقة الأفراد، أو على الأقل إشعارهم بوجود المراقبة. وقد لا يتوافر هذا الشرط في بعض الحالات.(26)

3. حد التناسب

يجب أن يكون استخدام كاميرات المراقبة متناسبًا مع الغرض الأمني المطلوب. فلا يجوز استخدام المراقبة المفرطة لتحقيق غرض محدود.(27)

4. حد المسؤولية

تطرح كاميرات المراقبة إشكالية المسؤولية عن سوء الاستخدام أو عن التسريبات أو عن الأخطاء. ويتطلب الأمر وضوحًا في تحديد المسؤوليات.(28)

سادسًا: العوامل التي تحد من فاعلية المراقبة:(29)

١. ضعف التصميم: عندما لا يُصمم النظام وفق تحليل المخاطر والاحتياجات الأمنية.

٢. سوء اختيار المواقع :عندما تُوضع الكاميرات في مواقع لا تحقق الغرض الأمني.
٣. المناطق غير المغطاة :عندما توجد مناطق عمياء لا تغطيها الكاميرات.
٤. ضعف الإضاءة :عندما لا تتوافر الإضاءة المناسبة لجودة الصورة.
٥. قصور جودة الصورة :عندما لا تكون الصورة واضحة بما يكفي للتعرف أو التمييز.
٦. أعطال النظام :عندما تتعطل الكاميرات أو الشبكة أو أجهزة التسجيل.
٧. ضعف التخزين :عندما لا تكفي سعة التخزين أو يصعب استرجاع التسجيلات.
٨. عدم كفاءة التشغيل :عندما لا يكون هناك مشغلون مؤهلون أو إجراءات واضحة.

سابعًا: المراقبة كجزء من منظومة متعددة الطبقات

المراقبة لا يمكن أن تكون الحل الوحيد للمشكلات الأمنية، بل يجب أن تكون جزءًا من منظومة متعددة الطبقات تجمع بين:(30)

١. الإجراءات التنظيمية :السياسات والإجراءات والخطط.
٢. العنصر البشري :الحراس والمشرفون والمشغلون.
٣. التقنيات الأمنية :المراقبة، والتحكم في الدخول، والإنذار، والإطفاء.
٤. العنصر المادي :الأسوار، والبوابات، والأقفال، والحواجز.

وتؤدي الكاميرات وظيفة محددة داخل هذه المنظومة، ولا تحل محل بقية عناصرها. فالقيمة الحقيقية للمراقبة تظهر عندما تكون جزءًا من منظومة أمنية متكاملة، وليست نظامًا منفصلًا.(31)

ثامنًا: الاستخدام المسؤول للمراقبة

بناءً على ما سبق، يمكن تحديد مبادئ الاستخدام المسؤول للمراقبة في خمسة مبادئ رئيسة:(32)

1. مبدأ الضرورة

لا تُستخدم المراقبة إلا عند وجود ضرورة أمنية حقيقية، وليس لمجرد الرغبة في المراقبة (33).

2. مبدأ التناسب

تكون المراقبة متناسبة مع الغرض الأمني المطلوب، فلا إفراط ولا تفريط.(34)

3. مبدأ الشفافية

يكون الأفراد على علم بوجود المراقبة، وتكون أغراضها واضحة.(35)

4. مبدأ المساءلة

توجد آليات للمساءلة عن استخدام المراقبة، وعن حماية البيانات، وعن سوء الاستخدام.(36)

5. مبدأ المراجعة

تُراجع منظومة المراقبة بصورة دورية للتأكد من فعاليتها واستمرار ضرورتها.(37)

أهم نتائج الفصل الأول

١. المراقبة الأمنية عملية منظمة تتجاوز الرؤية، وتهدف إلى إنتاج معلومات ذات قيمة أمنية.

٢. فاعلية المراقبة لا تنتج من التقنية وحدها، بل من تكامل التقنية مع التخطيط والتشغيل والعنصر البشري.

٣. أهداف المراقبة الأمنية خمسة: الوقاية والردع، الكشف، دعم الاستجابة، التوثيق، دعم التحقيق.

٤. الردع ليس نتيجة مضمونة، بل يتفاوت حسب البيئة وطريقة التطبيق.

٥. أنظمة المراقبة تطورت تراكميًا من المشاهدة إلى التسجيل إلى الإدارة الرقمية إلى الشبكات إلى التحليل الذكي.

٦. كاميرات المراقبة مرت بأربع مراحل كبرى: الميكانيكية، التناظرية، الرقمية، الذكية.

٧. التطور التقني كان يستجيب لاحتياجات أمنية وتشغيلية حقيقية.

٨. القاعدة المهنية: التقنية الناجحة أمنيًا هي التي تضيف قدرة قابلة للاستخدام والقياس.

٩. الانتقال من الكاميرا إلى المنظومة هو تحول جوهري في الفهم الأمني.

١٠. المنظومة تتكون من ست مجموعات من المكونات، وتتميز بخمس خصائص.

١١. التمييز الجوهري بين الكفاءة الفنية والفاعلية الأمنية: الأولى شرط ضروري للثانية لكنها ليست كافية.
١٢. المراقبة ليست نظامًا منفصلًا، بل أحد مكونات منظومة أمن المنشآت الأوسع.
١٣. منظومة أمن المنشآت تتكون من أربعة عناصر: البشري، التنظيمي، التقني، المادي.
١٤. للمراقبة حدود تقنية وبشرية وتنظيمية وأخلاقية وقانونية.
١٥. الاعتراف بحدود المراقبة شرط أساسي لاستخدامها بصورة فعالة ومسؤولة.
١٦. الانتقال من «الكاميرا كجهاز» إلى «الكاميرا كعنصر في منظومة» إلى «المنظومة كوسيلة لإنتاج قدرة أمنية قابلة للقياس.«

التوصيات: بناءً على ما تم تناوله في هذا الفصل، يمكن إجمال التوصيات في المحاور التالية:

أولًا: توصيات للممارسين

١. تجنب الشراء التقني المباشر: عدم البدء بشراء الكاميرات قبل تحديد الأهداف الأمنية وتحليل المخاطر.
٢. الانتقال من التفكير بالأجهزة إلى التفكير بالمنظومة: تصميم منظومة متكاملة وليس تجميع أجهزة.
٣. الموازنة بين الكفاءة الفنية والفاعلية الأمنية: عدم الاكتفاء بالمواصفات التقنية العالية دون التأكد من تحقيق الغرض الأمني.
٤. الاعتراف بحدود المراقبة: عدم الاعتماد على الكاميرات كحل وحيد، بل كجزء من منظومة متعددة الطبقات.
٥. تطبيق مبادئ الاستخدام المسؤول: الضرورة، والتناسب، والشفافية، والمساءلة، والمراجعة.

ثانيًا: توصيات لصانعي القرار

١. تبني منهج التخطيط المبني على المخاطر: البدء من تحليل المخاطر وليس من الميزانية التقنية.

٢. إرساء ثقافة المنظومة: تعزيز مفهوم أن المراقبة وظيفة أمنية متكاملة وليست مجرد أجهزة.
٣. تخصيص الموارد الكافية: للمكونات الست (الالتقاط، النقل، المعالجة، التخزين، العرض، التشغيل) وليس للكاميرات وحدها.
٤. وضع سياسات واضحة: للاستخدام المسؤول، وحماية البيانات، وإدارة الصلاحيات.
٥. الاستثمار في العنصر البشري: تدريب المشغلين وتأهيلهم، وتوفير بيئة عمل مناسبة.

ثالثًا: توصيات للباحثين

١. دراسة الفاعلية الأمنية: إجراء دراسات ميدانية لقياس الفاعلية الأمنية لمنظومات المراقبة في البيئة العربية.
٢. تطوير مؤشرات القياس: بناء مؤشرات موضوعية لقياس الفاعلية الأمنية وليس الكفاءة الفنية فقط.
٣. دراسة التكامل: البحث في نماذج تكامل المراقبة مع بقية الأنظمة الأمنية.
٤. معالجة الإشكاليات القانونية: دراسة التوازن بين الأمن والخصوصية في التشريعات العربية.
٥. مواكبة التقنيات الحديثة: دراسة أثر الذكاء الاصطناعي وتحليل الفيديو على الفاعلية الأمنية.

رابعًا: توصيات للمؤسسات

١. تأسيس وحدات متخصصة: لإدارة منظومات المراقبة وصيانتها وتطويرها.
٢. إعداد الأدلة الإجرائية: لتشغيل المنظومات والتعامل مع الأحداث.
٣. التقييم الدوري: إجراء تقييمات دورية للفاعلية الأمنية للمنظومات.
٤. التوثيق الشامل: توثيق التصميم والتشغيل والصيانة والتقييم.
٥. التعاون مع الجهات المختصة: للتنسيق في مجال الأمن السيبراني وحماية البيانات.

أسئلة التفكير والتقييم للفصل الأول

أسئلة معرفية:

١. ما الفرق بين المراقبة والرؤية والفعل الأمني؟
٢. اذكر أهداف المراقبة الأمنية الخمسة، وعناصرها الخمسة.
٣. ما المراحل الخمس الوظيفية لتطور أنظمة المراقبة؟
٤. ما الأجيال الأربعة للمرحلة التناظرية والأربعة للمرحلة الرقمية؟
٥. ما الفرق الجوهري بين "الكاميرا" و"منظومة المراقبة"؟
٦. ما العناصر الأربعة لمنظومة أمن المنشآت؟ وما وظائف المراقبة الخمس ضمنها؟
٧. ما الحدود التقنية والبشرية والتنظيمية والأخلاقية للمراقبة؟

أسئلة تحليلية:

١. حلل العلاقة بين فاعلية المراقبة والتكامل بين التقنية والعنصر البشري.
٢. ناقش حدود المراقبة الأمنية في ضوء المراجعات المنهجية.
٣. قارن بين التخطيط الرشيد للمراقبة والتخطيط التقليدي.
٤. حلل العلاقة بين تطور الكاميرا وتطور المنظومة الأمنية.

٥. ناقش العلاقة بين الكفاءة الفنية والفاعلية الأمنية. هل يمكن أن توجد منظومة عالية الكفاءة الفنية ومنخفضة الفاعلية الأمنية؟

٦. حلل موقع المراقبة ضمن منظومة أمن المنشآت. هل يمكن الاستغناء عن أحد عناصرها؟

٧. ناقش مبادئ الاستخدام المسؤول للمراقبة. أيها الأكثر أهمية في البيئة العربية؟

٨. أسئلة تطبيقية:

٩. اختر منشأة تعرفها، وحلل منظومة المراقبة فيها في ضوء ما تعلمته من هذا الفصل.

١٠. لو طُلب منك تصميم منظومة مراقبة لمنشأة حيوية، ما الخطوات التي ستتبعها؟

١١. ابحث في أحدث تقنيات المراقبة، وحلل مدى ملاءمتها لبيئة عمل تعرفها.

المراجع:

① راجع: Brandon C. Welsh and David P. Farrington, "Effects of Closed Circuit Television Surveillance on Crime," *Campbell Systematic Reviews*, Vol. 4, No. 1 (2008), pp. 1–73, DOI: 10.4073/csr.2008.17.

② ينظر: David Brown, *Integrated Security Systems Design*, (New York: Butterworth-Heinemann, 3rd Edition, 2019), p. 145.

③ راجع: خالد بن إبراهيم النفيعي، *إدارة أنظمة المراقبة: دراسة تطبيقية*، (الدمام: دار المجتمع للنشر، الطبعة الأولى، ١٤٤٤هـ/٢٠٢٣م)، ص ١١٢ .

④ Welsh and Farrington, "Effects of Closed Circuit Television Surveillance on Crime," pp. 1–73.

⑤ Eric L. Piza, Brandon C. Welsh, David P. Farrington, and Amanda L. Thomas, "CCTV Surveillance for Crime Prevention: A 40-Year Systematic Review with Meta-Analysis," *Criminology & Public Policy*, Vol. 18, No. 1 (2019), pp. 135–159, DOI: 10.1111/1745-9133. 12419.

⑥ ينظر: وزارة الداخلية، *الدليل المهني لأنظمة المراقبة الأمنية*، (الرياض: الإدارة العامة للأمن، ٢٠٢١م)، ص ٦٧.

⑦ راجع: Michael Harris, *CCTV and Video Surveillance: Technology and Applications*, (Boston: McGraw-Hill, 4th Edition, 2020), p. 178.

⑧ ينظر: Brown, *Integrated Security Systems Design*, p. 156.

⑨ راجع: Robert Wilson, *Digital Video Processing for Security Systems*, (London: Springer, 2021), p. 189.

⑩ ينظر: يوسف بن علي الزهراني، *العدسات البصرية في كاميرات المراقبة*، (أبها: دار النشر الجامعي، ١٤٤١هـ/٢٠٢٠م)، ص ١١٢ .

⑪ راجع: Brown, *Integrated Security Systems Design*, p. 167.

⑫ ينظر: عبد الله بن حسن الشهري، *شبكات نقل الفيديو الأمني*، (الرياض: معهد الإدارة العامة، ١٤٤٤هـ/٢٠٢٣م)، ص ١٣٤ .

⑬ راجع: Wilson, *Digital Video Processing for Security Systems*, p. 201.

⑭ ينظر: Smith, *Security Surveillance Systems*, p. 178.

⑮ راجع: Brandon C. Welsh, Eric L. Piza, Amanda L. Thomas, and David P. Farrington, "Private Security and Closed-Circuit Television (CCTV) Surveillance: A Systematic Review of Function and Performance," *Journal of Contemporary Criminal Justice*, Vol. 36, No. 1 (2020), pp. 56–69.

⑯ينظر: سعد بن عبد العزيز المطيري، *التقنيات الحديثة في أنظمة المراقبة*، (الكويت: دار الفكر الأمني، الطبعة الأولى، ١٤٤٢هـ/٢٠٢١م)، ص ١٤٥ .

⑰راجع: Smith, *Security Surveillance Systems*, p. 189.

⑱ينظر: النفيعي، *إدارة أنظمة المراقبة*، ص ١٣٤ .

⑲راجع: Brown, *Integrated Security Systems Design*, p. 178.

⑳ينظر: European Union, *General Data Protection Regulation (GDPR)*, (Brussels: Official Journal of the European Union, 2016), Article 35.

㉑راجع: وزارة الداخلية، *الدليل المهني لأنظمة المراقبة الأمنية*، ص ٧٨.

㉒ينظر: المطيري، *التقنيات الحديثة في أنظمة المراقبة*، ص ١٥٦ .

㉓راجع: Brown, *Integrated Security Systems Design*, p. 189.

㉔ينظر: Smith, *Security Surveillance Systems*, p. 201.

㉕راجع: آمال عبدالجبار حسوني ونادية كعب جبر، «كاميرات المراقبة بين دواعي الاستعمال وانتهاك الخصوصية»، *مجلة الحقوق*، الجامعة المستنصرية، المجلد ٩، العددان ٢٩–٣٠ (٢٠١٧)، ص ١–١٨.

㉖ينظر: أحمد علي حسن عثمان، «الضوابط القانونية لاستخدام أنظمة المراقبة التلفزيونية المغلقة CCTV في بيئة العمل: دراسة مقارنة»، *مجلة البحوث القانونية والاقتصادية*، جامعة المنصورة، العدد ٩٢ (٢٠٢٥)، ص ٢٢٢–٣٨٧.

㉗راجع: Home Office, *Surveillance Camera Code of Practice*, amended November 2021, effective 12 January 2022, Principle 4.

㉘ينظر: Biometrics and Surveillance Camera Commissioner, *Surveillance Camera Code of Practice*, United Kingdom, revised 2021, Principle 5.

㉙راجع: Brown, *Integrated Security Systems Design*, p. 201.

㉚ينظر: International Organization for Standardization, *ISO 22341:2021 Security and resilience — Protective security — Guidelines for crime prevention through environmental design*, (Geneva: ISO, 2021), Clause 5. 3.

㉛راجع: وزارة الداخلية، *الدليل المهني لأنظمة المراقبة الأمنية*، ص ٨٩.

㉜ينظر Home Office, *Surveillance Camera Code of Practice*, Principle 1-5.

㉝راجع: المرجع السابق، Principle 1.

㉞ينظر: المرجع السابق، Principle 2.

㉟راجع: المرجع السابق، Principle 3.

㊱ينظر: المرجع السابق، Principle 4.

㊲راجع: المرجع السابق، Principle 5.

الفصل الثاني: منظومة كاميرات المراقبة ومكوناتها

تمهيد الفصل

لا يمكن فهم كفاءة كاميرات المراقبة من خلال دراسة الكاميرا منفردة؛ إذ إن الصورة التي تصل إلى المشغل أو تُحفظ في نظام التسجيل هي النتيجة النهائية لتفاعل مجموعة من المكونات المادية والبرمجية والشبكية والتشغيلية. ولذلك فإن أي تقييم مهني لمنظومة المراقبة ينبغي أن ينظر إليها بوصفها نظامًا متكاملًا، تتأثر مخرجاته بجودة كل مكوّن وبطريقة ارتباطه ببقية المكونات.(1)

وتتدرج هذه المنظومة، في أبسط صورها، من التقاط المشهد بواسطة الكاميرا والعدسة، إلى تحويله إلى إشارة أو بيانات فيديو، ثم نقلها ومعالجتها وتسجيلها وتخزينها، وصولًا إلى عرضها وتحليلها واستخدامها في اتخاذ القرار الأمني. ومع تطور الأنظمة الشبكية، أصبحت الحدود بين هذه الوظائف أقل وضوحًا؛ فقد أصبحت بعض الكاميرات قادرة على تنفيذ قدر من المعالجة والتحليل والتخزين المحلي، بينما أصبحت البرمجيات تؤدي وظائف كانت في السابق مرتبطة بأجهزة مستقلة.(2)

وعليه، فإن دراسة مكونات منظومة المراقبة لا تستهدف التعريف بالأجهزة فحسب، وإنما تهدف إلى فهم وظيفة كل مكوّن، وعلاقته ببقية المكونات، وأثره في القيمة الأمنية النهائية للمنظومة .ويتناول هذا الفصل عشرة مباحث: مفهوم منظومة المراقبة، والكاميرات، والعدسات، وأجهزة التسجيل، ووسائط التخزين، والشاشات ومراكز

المراقبة، والشـــبكات والاتصـــالات، وأنظمة الطاقة، والبرمجيات والتحكم، وتكامل مكونات المنظومة.

المبحث الأول: مفهوم منظومة المراقبة

لا تبدأ منظومة المراقبة الإلكترونية من الكاميرا، وإن كانت الكاميرا أكثر عناصرها ظهورًا للمستخدم. فالمنظومة في معناها الفني والأمني أوسع من جهاز التصوير، لأنها تمثل مجموعة مترابطة من المكونات والأجهزة والبرمجيات ووسائط الاتصال والتخزين والعرض والعنصر البشري، تعمل بصورة متكاملة لتحقيق غرض أمني محدد (٣). ومن ثم فإن النظر إلى الكاميرا بوصفها نظامًا أمنيًا مكتملًا يؤدي إلى اختزال وظيفة المراقبة في عملية التقاط الصور، في حين أن القيمة الأمنية الحقيقية تنشأ من قدرة المنظومة على تحويل المشهد المرصود إلى معلومات يمكن نقلها وحفظها واسترجاعها وتحليلها واستخدامها في اتخاذ القرار.

أولًا: من النظام المنفرد إلى المنظومة المتكاملة

يقصد بمنظومة المراقبة بالفيديو مجموعة المكونات والأجهزة والبرمجيات ووسائل الاتصال والتخزين وإجراءات التشغيل التي تعمل بصورة مترابطة للحصول على الصور المرئية ومعالجتها ونقلها وتسجيلها واسترجاعها أو تحليلها، بما يخدم غرضًا محددًا من أغراض المراقبة والحماية الأمنية (٤). ويقوم هذا المفهوم على الترابط الوظيفي بين العناصر، وليس مجرد وجود مجموعة من الأجهزة في موقع واحد.

وقد عرّفت اللجنة الكهروتقنية الدولية أنظمة المراقبة بالفيديو (Video Surveillance Systems – VSS) في إطار معياري يحدد متطلبات الأداء والوظائف الأساسية لأنظمة المراقبة المستخدمة في التطبيقات الأمنية، مع التأكيد على أن النظام قد يتشارك وسائل الكشف والتحفيز والربط والتحكم والاتصالات ومصادر الطاقة مع تطبيقات أخرى (٥). وهذا يعكس منذ البداية الطبيعة المنظومية للمراقبة، إذ لا تعمل عناصرها بالضرورة في عزلة، بل يمكن أن تتكامل مع منظومات أمنية وتقنية أخرى.

ومن هنا ينبغي التمييز بين وجود النظام وفاعلية النظام .فوجود النظام يعني أن مكوناته مركبة وقادرة على العمل من الناحية التقنية، أما فاعليته فتعني قدرته على تحقيق الهدف الذي صُمم من أجله في الظروف الفعلية للتشغيل.(6)

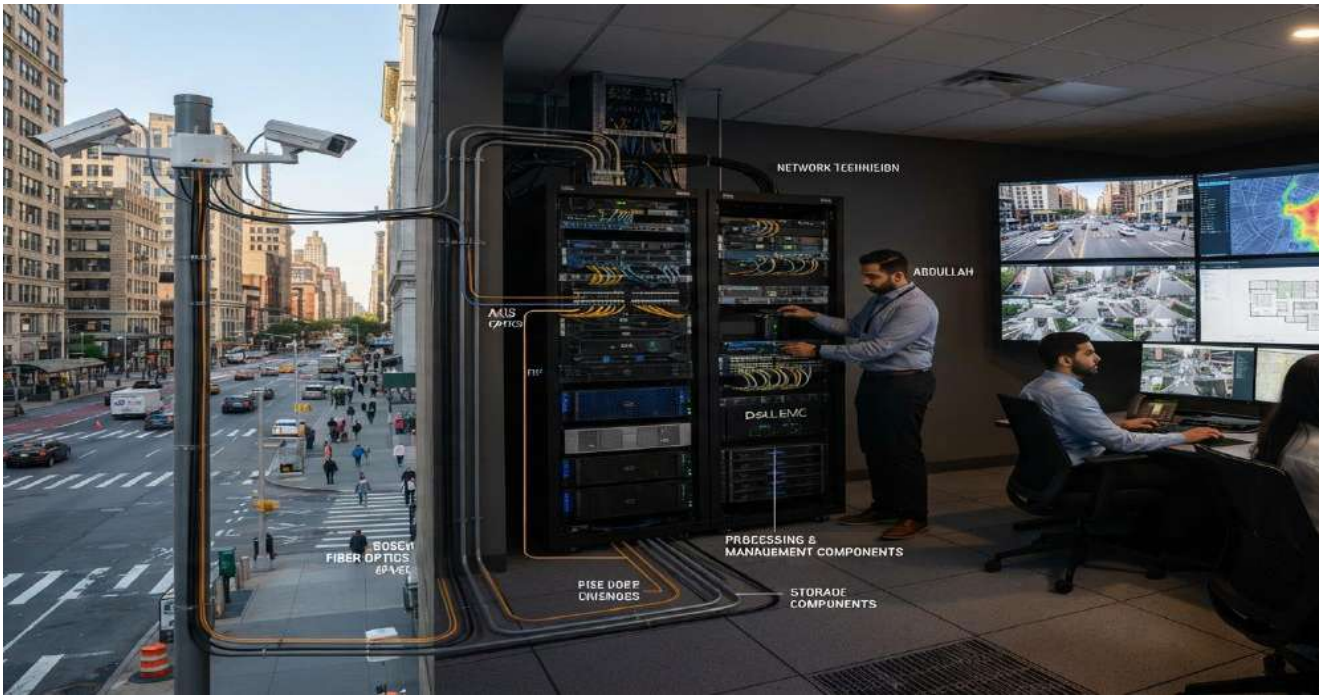
ثانيًا: البنية الوظيفية لمنظومة المراقبة

يمكن النظر إلى منظومة المراقبة من خلال سلسلة وظيفية تبدأ بعملية الالتقاط وتنتهي بالاستخدام الأمني للمعلومات. وتتمثل هذه السلسلة في:

المشـهد الأمني ← الالتقاط ← النقل ← المعالجة ← التسـجيل والتخزين ← العرض والتحليل ← التحقق ← القرار والاستجابة .(7)

وتختلف تفاصـيل هذه السـلسـلة بحسـب نوع النظام وحجمه وتصـميمه. ففي بعض الأنظمة تكون المعالجة والتحليل في أجهزة مركزية، بينما قد تنفذ الكاميرا نفسها بعض وظائف المعالجة والتحليل في الأنظمة الحديثة. غير أن الاختلاف في البنية التقنية لا يغير المبدأ الأساسي :القيمة الأمنية للفيديو لا تتحدد عند لحظة التقاط الصورة، وإنما تتحدد بقدرة المنظومة على تحويل المشـهد إلى معلومات يمكن الاعتماد عليها في الوقت المناسب .(8)

ثالثًا: مكونات المنظومة من منظور وظيفي



يمكن تصنيف مكونات منظومة المراقبة إلى فئات مترابطة:

1. مكونات الالتقاط : وتشـمل الكاميرات والعدسـات والمكونات المرتبطة بالحصـول على الصورة. وتحدد هذه المرحلة مقدار المعلومات البصرية التي يمكن أن تدخل إلى النظام أصلًا.(9)

2. مكونات النقل :وهي الوسائط والبنية الشبكية التي تنقل بيانات الفيديو بين مصادر الالتقاط ومكونات المعالجة والتسجيل والعرض.(10)

3.مكونات المعالجة والإدارة : وتشـمل الأجهزة والبرمجيات التي تسـتقبل تدفقات الفيديو وتديرها، وقد تتولى وظائف مثل التسـجيل، وإدارة المسـتخدمين، والبحث، واسترجاع الأحداث، والتحليل.(11)

4. مكونات التخزين: وهي المسؤولة عن الاحتفاظ بالفيديو والبيانات المرتبطة به للفترة المطلوبة، وفق متطلبات التشغيل والسياسات المعتمدة.(12)

5. مكونات العرض والمراقبة : وتتيح للمشغلين متابعة مصادر الفيديو والتفاعل مع الأحداث والتنبيهات والبيانات المتاحة.(13)

6. البنية التشغيلية: وتشمل العاملين والإجراءات والسياسات والتدريب والصيانة والاختبارات وآليات التعامل مع الحوادث.(14)

ومن المهم التأكيد أن المكونات البشرية والإجرائية ليست عناصر خارجية عن المنظومة من منظور الأداء الأمني؛ إذ قد يكون النظام متقدمًا تقنيًا، ولكن ضعف التشغيل أو الصيانة أو إجراءات الاستجابة يحول دون تحقيق أهدافه.(15)

رابعًا: منظومة المراقبة كنظام مفتوح

لا تعمل منظومة المراقبة في بيئة معزولة، وإنما تتفاعل مع البيئة المادية والأمنية والتقنية المحيطة بها. فالكاميرا تتأثر بالموقع والإضاءة والظروف الجوية والعوائق وحركة الأشخاص والمركبات، كما يتأثر النظام بالشبكة والطاقة والبنية التحتية، بينما يتأثر استخدام مخرجاته بالإجراءات الأمنية والقانونية والتنظيمية.(16)

ولهذا يمكن تصور المنظومة باعتبارها نظامًا مفتوحًا له:

- مدخلات :مشاهد وأحداث وبيانات وطلبات تشغيل.
- عمليات :التقاط ونقل ومعالجة وتسجيل وتحليل.
- مخرجات :صور وتسجيلات وتنبيهات ومعلومات.
- نتائج أمنية :دعم الوقاية والكشف والتحقق والاستجابة والتوثيق.(17)

ومن هذه الزاوية تصبح عملية تقييم النظام أكثر دقة؛ لأن السؤال لا يعود: هل تعمل الكاميرات؟ بل :هل تنتج المنظومة المخرجات المطلوبة لتحقيق النتيجة الأمنية المستهدفة؟

خامسًا: العلاقة بين المكونات

تعمل مكونات المنظومة وفق علاقة اعتماد متبادل. فإذا كانت الكاميرا تنتج صورة ضعيفة بسبب سوء الإضاءة أو عدم ملاءمة العدسة، فإن معالجة الفيديو اللاحقة لن تستطيع دائمًا استعادة المعلومات التي لم يتم التقاطها أصلًا. وإذا كانت الصورة جيدة ولكن الشبكة غير مستقرة، فقد تتأثر عملية النقل والتسجيل. وإذا كان التسجيل سليمًا

ولكن إدارة التخزين ضعيفة، فقد يصعب استرجاع الحدث عند الحاجة. وإذا كانت المعلومات متاحة ولكن إجراءات التشغيل غير واضحة، فقد لا تتحول المعلومة إلى استجابة أمنية فعالة.(18)

ومن هنا يمكن التعبير عن أحد المبادئ الأساسية في هذا الكتاب:

قيمة منظومة المراقبة لا تساوي مجموع جودة مكوناتها، وإنما تتحدد بمدى تكاملها وقدرتها على أداء الوظيفة الأمنية المطلوبة.

وهذا يعني أن وجود مكوّن شديد الجودة لا يعوض بالضرورة عن خلل جوهري في مكوّن آخر إذا كان ذلك الخلل يؤثر في سلسلة العمل بأكملها.(19)

سادسًا: تصنيف المنظومة وفق بنية التشغيل

يمكن النظر إلى أنظمة المراقبة من حيث بنيتها العامة إلى أنظمة تعتمد على معالجة مركزية، وأنظمة شبكية موزعة، وأنظمة تجمع بين المعالجة المحلية والمركزية.(20)

وقد أدى انتشار كاميرات الشبكات إلى انتقال مهم في طبيعة المنظومة، إذ أصبحت الكاميرا نفسها نقطة على الشبكة يمكن أن تمتلك قدرات معالجة وإدارة واتصال، بدل أن تكون مجرد مصدر للإشارة. ويؤدي هذا التطور إلى فوائد تشغيلية، لكنه في الوقت نفسه يوسع نطاق المتطلبات الأمنية، لأن المنظومة تصبح مرتبطة بدرجة أكبر بالبنية الشبكية والبرمجية وإدارة الحسابات والصلاحيات وحماية البيانات.(21)

وهكذا فإن الانتقال إلى الأنظمة الرقمية والشبكية لم يغيّر طريقة نقل الفيديو فحسب، بل غيّر طبيعة المخاطر والمتطلبات اللازمة لحماية المنظومة .(22)

سابعًا: المعيار الحقيقي للمنظومة

لا ينبغي الحكم على منظومة المراقبة من خلال عدد الكاميرات أو حجم التخزين أو دقة التصوير وحدها. ويمكن اقتراح مجموعة من الأسئلة الأساسية للحكم على كفاءة المنظومة:(23)

١. هل تغطي المخاطر والمناطق التي صُممت لحمايتها؟
٢. هل توفر مستوى التفاصيل المطلوب للغرض الأمني؟
٣. هل تعمل بصورة مستقرة خلال الفترات المطلوبة؟
٤. هل يمكن استرجاع الأحداث بسرعة وموثوقية؟
٥. هل يمكن الاعتماد على التنبيهات والتحليلات عند استخدامها؟
٦. هل توجد إجراءات واضحة للتعامل مع الأحداث؟

٧. هل النظام محمي من الاستخدام أو الوصول غير المصرح به؟
٨. هل يمكن صيانته وتطويره واستمراره اقتصاديًا وفنيًا؟
وبذلك تنتقل عملية التقييم من فحص الأجهزة إلى تقييم القدرة الأمنية للمنظومة .(24)

الهوامش والمراجع

① راجع: International Electrotechnical Commission, *IEC 62676-1-1: Video surveillance systems for use in security applications – Part 1-1: System requirements – General*, (Geneva: IEC, 2013), Clause 3.1.
② ينظر: David Brown, *Integrated Security Systems Design*, (New York: Butterworth-Heinemann, 3rd Edition, 2019), p. 23.
③ راجع: International Electrotechnical Commission, *IEC 62676-1-1*, Clause 3.2.
④ ينظر: خالد بن إبراهيم النفيعي، *إدارة أنظمة المراقبة: دراسة تطبيقية*، (الدمام: دار المجتمع للنشر، الطبعة الأولى، ١٤٤٤هـ/٢٠٢٣م)، ص ٤٥.
⑤ راجع: International Electrotechnical Commission, *IEC 62676-1-1*, Clause 1.
⑥ ينظر: John Smith, *Security Surveillance Systems: Principles and Practices*, (London: Security Press, 2nd Edition, 2021), p. 34.
⑦ راجع: Brown, *Integrated Security Systems Design*, p. 45.
⑧ ينظر: Smith, *Security Surveillance Systems*, p. 45.
⑨ راجع: فهد بن محمد العتيبي، *مكونات أنظمة المراقبة بالفيديو*، (الرياض: مكتبة الملك فهد الوطنية، ١٤٤٣هـ/٢٠٢٢م)، ص ٢٣.
⑩ ينظر: عبد الله بن حسن الشهري، *شبكات نقل الفيديو الأمني*، (الرياض: معهد الإدارة العامة، ١٤٤٤هـ/٢٠٢٣م)، ص ٣٤.
⑪ راجع: Robert Wilson, *Digital Video Processing for Security Systems*, (London: Springer, 2021), p. 67.
⑫ ينظر: سعد بن عبد العزيز المطيري، *التقنيات الحديثة في أنظمة المراقبة*، (الكويت: دار الفكر الأمني، الطبعة الأولى، ١٤٤٢هـ/٢٠٢١م)، ص ٥٦.
⑬ راجع: Brown, *Integrated Security Systems Design*, p. 67.
⑭ ينظر: وزارة الداخلية، *الدليل المهني لأنظمة المراقبة الأمنية*، (الرياض: الإدارة العامة للأمن، ٢٠٢١م)، ص ٢٣.
⑮ راجع: Smith, *Security Surveillance Systems*, p. 56.
⑯ ينظر: International Organization for Standardization, *ISO 22341:2021 Security and resilience — Protective security — Guidelines for crime prevention through environmental design*, (Geneva: ISO, 2021), Clause 5.3.
⑰ راجع: Brown, *Integrated Security Systems Design*, p. 78.
⑱ ينظر: النفيعي، *إدارة أنظمة المراقبة*، ص ٥٦.
⑲ راجع: Smith, *Security Surveillance Systems*, p. 67.
⑳ ينظر: العتيبي، *مكونات أنظمة المراقبة بالفيديو*، ص ٣٤.
㉑ راجع: الشهري، *شبكات نقل الفيديو الأمني*، ص ٤٥.
㉒ ينظر: Wilson, *Digital Video Processing for Security Systems*, p. 78.
㉓ راجع: وزارة الداخلية، *الدليل المهني لأنظمة المراقبة الأمنية*، ص ٣٤.
㉔ ينظر: Brown, *Integrated Security Systems Design*, p. 89.

المبحث الثاني: الكاميرات

تمثل الكاميرا نقطة التماس الأولى بين المنظومة والبيئة التي يُراد مراقبتها. فهي التي تلتقط المشهد وتحوله إلى صورة يمكن للنظام نقلها ومعالجتها وتسجيلها وتحليلها. ولهذا فإن أي قصور في مرحلة التصوير قد ينتقل إلى المراحل اللاحقة ؛ إذ لا يستطيع أفضل نظام تسجيل أو تحليل أن يستعيد تفاصيل لم تلتقطها الكاميرا أصلًا.(1)

ومن هنا ينبغي أن ينظر إلى الكاميرا باعتبارها مستشعرًا أمنيًا قبل النظر إليها باعتبارها جهازًا إلكترونيًا للتصوير.

أولًا: مفهوم كاميرا المراقبة

كاميرا المراقبة هي جهاز تصوير مصمم لالتقاط المشاهد في بيئة محددة وإنتاج إشارة أو بيانات مرئية يمكن نقلها أو تخزينها أو عرضها أو تحليلها ضمن منظومة مراقبة.(2)

ويختلف تصميم الكاميرا الأمنية عن الكاميرات المخصصة للتصوير العام بحسب طبيعة المهمة المطلوبة منها. ففي البيئة الأمنية لا يكفي أن تنتج الكاميرا صورة جميلة أو واضحة بصورة عامة؛ وإنما يجب أن تكون الصورة مناسبة للغرض الأمني المحدد.(3)

ومن ثم فإن السؤال الصحيح عند اختيار الكاميرا ليس» : ما أفضل كاميرا؟ «وإنما» : ما الكاميرا التي تحقق الهدف الأمني المحدد في هذا الموقع وتحت هذه الظروف؟«

ثانيًا: المكونات الأساسية للكاميرا

تتكون الكاميرا الحديثة من مجموعة من العناصر التي تعمل بصورة مترابطة:(4)

1. المستشعر الضوئي(Sensor)

وهو العنصر الذي يستقبل الضوء القادم من العدسة ويحوّله إلى معلومات كهربائية أو رقمية يمكن معالجتها. ويُعدّ المستشعر أهم مكون في الكاميرا، إذ تحدد خصائصه قدرتها على العمل في ظروف الإضاءة المختلفة، وجودة الصورة الناتجة.(5)

2. العدسة(Lens)

وهي التي تحدد كيفية دخول الضوء إلى المستشعر ومجال المشهد الذي يمكن تصويره. وسيأتي تفصيلها في المبحث الثالث.(6)

3. معالج الصورة(Processor)

وهو الذي يتولى معالجة البيانات الناتجة عن المستشعر وإنتاج صورة قابلة للاستخدام وفق إمكانات الكاميرا.(7)

4. هيكل الكاميرا

وهو الذي يوفر الحماية الفيزيائية للمكونات الداخلية، وتختلف متطلباته بحسب طبيعة البيئة الداخلية أو الخارجية.(8)

5. وسائل الاتصال

وهي التي تسمح بنقل الصورة والبيانات إلى بقية مكونات النظام في الكاميرات الشبكية، وقد تشمل كذلك وظائف الإدارة والتحكم.(9)

6. مصدر الطاقة

وهو الذي يزود الكاميرا بالطاقة اللازمة للتشغيل، وقد تتكامل الطاقة والاتصال في بعض البنى الشبكية من خلال تقنيات مخصصة مثل PoE.(10)

ثالثًا: تصنيف الكاميرات

يمكن تصنيف كاميرات المراقبة وفق معايير متعددة:(11)

التصنيف الأول: وفق الحركة والتحكم

- الكاميرات الثابتة: موجهة إلى منطقة محددة، ولا تتحرك.(12)
- الكاميرات المتحركة: (PTZ) قادرة على التحريك والتقريب والتتبع.(13)

التصنيف الثاني: وفق طبيعة الاستخدام

- الكاميرات الداخلية: مصممة للعمل في البيئات الداخلية المستقرة.(14)
- الكاميرات الخارجية: مصممة للعمل في البيئات الخارجية التي تتعرض للغبار والرطوبة وتغيرات الحرارة.(15)

التصنيف الثالث: وفق طريقة الاتصال

- الكاميرات التناظرية: تعتمد على البنية التناظرية التقليدية.(16)
- كاميرات IP الشبكية: تعتمد على نقل البيانات رقميًا عبر شبكات الاتصال.(17)

التصنيف الرابع: وفق الوظيفة

- الكاميرات العامة: للمراقبة العامة.(18)
- الكاميرات المتخصصة: مثل كاميرات الإضاءة المنخفضة، والكاميرات الحرارية، والكاميرات المزودة بتحليلات مدمجة.(19)

رابعًا: الكاميرات الثابتة والمتحركة

تتميز الكاميرا الثابتة ببساطة مفهومها التشغيلي؛ إذ توجه نحو منطقة محددة وتظل زاوية مراقبتها ثابتة. وتكون هذه الخاصية مفيدة عندما تكون منطقة المراقبة معروفة وثابتة، مثل المداخل والممرات ونقاط العبور.(20)

أما الكاميرات المتحركة فتتيح تغيير اتجاه الرؤية أو مستوى التكبير، وهو ما يمنحها مرونة أكبر في تغطية مناطق متعددة. لكن زيادة المرونة لا تعني بالضرورة أنها أفضل في كل التطبيقات. فإذا كانت الكاميرا المتحركة تراقب منطقة واسعة ثم انتقلت إلى منطقة أخرى، فقد تفقد في تلك اللحظة القدرة على متابعة المنطقة الأولى.(21)

ومن ثم يجب أن يدرس التصميم الأمني ما إذا كان الهدف يتطلب مراقبة ثابتة مستمرة أم قدرة على إعادة توجيه الرؤية. وهذه نقطة مهمة في التصـــميم :التقنية التي توفر وظائف أكثر ليست بالضرورة التقنية الأكثر ملاءمة .(22)

خامسًا: الدقة وجودة الصورة

تعد دقة الصورة من أكثر الخصائص شهرة عند الحديث عن الكاميرات، لكنها ليست العامل الوحيد في جودة الأداء. فارتفاع عدد البكســلات يمكن أن يوفر قدرة أكبر على تمثيل التفاصــيل، لكن الاســتفادة منه تعتمد على عوامل أخرى، منها جودة العدســة، والإضاءة، والمسافة، وحركة الهدف، والتركيز، والضغط، وحجم المستشعر، وطريقة عرض الصورة.(23)

لذلك فإن القول بأن كاميرا ذات دقة أعلى ســتؤدي دائمًا إلى نتائج أمنية أفضـــل هو تبســيط غير دقيق. فالهدف الأمني قد يكون أحيانًا الحصــول على مجال رؤية واســع، وفي هذه الحالة قد يكون توزيع أكثر من كاميرا بزوايا مناســبة أكثر فائدة من الاعتماد على كاميرا واحدة عالية الدقة تغطي مســاحة واســعة جدًا مع انخفاض التفاصــيل في أجزاء المشهد.(24)

سادسًا: الإضاءة والظروف البيئية

تعتمد الكاميرا في النهاية على الضــوء الذي يصــل إلى المســتشــعر. ولذلك تؤثر ظروف الإضــاءة بصــورة مباشــرة في جودة الصــورة. وقد تواجه الكاميرا ظروفًا مثل: الإضــاءة المنخفضة، والتباين الشديد بين الظل والضوء، والإضاءة الخلفية، والمصابيح القوية، والانعكاسات، والانتقال بين النهار والليل.(25)

ومن هنا تظهر أهمية اختيار كاميرا تتناســـب مع الظروف الفعلية للموقع، لا الظروف المثالية. وفي بعض التطبيقات قد تكون هناك حاجة إلى خصـــائص متقدمة لمعالجة التباين أو تحسين التصوير في الإضاءة المنخفضة أو الانتقال بين أوضاع النهار والليل (26).

سابعًا: البيئة الفيزيائية وحماية الكاميرا

لا يكفي اختيار كاميرا ذات أداء تصويري مناسب إذا كانت البيئة التي ستعمل فيها تؤثر في اســتمراريتها. فالكاميرات الخارجية قد تتعرض للغبار والرطوبة والحرارة والبرودة

والصدمات أو التخريب المتعمد. ولذلك يجب أن يأخذ الاختيار في الاعتبار خصائص الحماية البيئية والميكانيكية المناسبة للموقع.(27)

وهنا يظهر الفرق بين مواصفة تقنية جيدة واختيار مناسب للتطبيق؛ فقد تكون الكاميرا ممتازة من الناحية التصويرية، لكنها غير مناسبة للبيئة التي ستوضع فيها.

ثامنًا: اختيار الكاميرا وفق الهدف الأمني

ينبغي أن يبدأ اختيار الكاميرا من تحليل المهمة. فإذا كان المطلوب مراقبة ساحة واسعة، فإن متطلبات التغطية تختلف عن متطلبات مراقبة بوابة دخول. وإذا كان الهدف اكتشاف وجود شخص، فقد تختلف المتطلبات عن حالة يكون الهدف فيها التعرف على هوية الشخص. وإذا كان المطلوب مراقبة مركبات على مسافة كبيرة، فإن العدسة وموقع التركيب والإضاءة تصبح عناصر حاسمة إلى جانب مواصفات الكاميرا (28).

وبذلك يمكن صياغة قاعدة أساسية:

لا تختار الكاميرا أولًا ثم تبحث عن وظيفة لها؛ بل حدد الوظيفة الأمنية أولًا، ثم اختر الكاميرا القادرة على تحقيقها.

ويمكن تلخيص عملية الاختيار في مجموعة من الأسئلة: (29)

- ماذا نريد أن نرى؟
- من أي مسافة؟
- في أي ظروف إضاءة؟
- ما حجم المنطقة المطلوب تغطيتها؟
- ما مستوى التفاصيل المطلوب؟
- هل الهدف ثابت أم متحرك؟
- هل الموقع داخلي أم خارجي؟
- هل هناك حاجة إلى تحليل آلي؟
- ما متطلبات التسجيل والاحتفاظ؟
- ما مستوى الاعتمادية المطلوب؟

تاسعًا: الكاميرا والتحليلات الذكية

أصبحت بعض الكاميرات الحديثة قادرة على تنفيذ قدر من المعالجة والتحليل داخل الكاميرا نفسها، مثل اكتشاف الحركة أو تحليل بعض خصائص المشهد أو إرسال أحداث محددة إلى نظام الإدارة.(30)

لكن وجود هذه الوظائف لا يعني أن الكاميرا أصبحت بديلًا كاملًا عن منظومة التحليل والإدارة. فدقة التحليل تعتمد على ظروف التصوير وجودة البيانات وإعدادات النظام والسياق التشغيلي. كما أن نتائج التحليل الآلي تحتاج إلى إدارة وتقييم، خصوصًا في التطبيقات الأمنية التي قد يترتب عليها تدخل بشري.(31)

ومن ثم يجب التعامل مع التحليلات الذكية باعتبارها طبقة مساعدة في دورة المعلومات الأمنية، لا باعتبارها بديلًا مطلقًا عن العنصر البشري.

عاشرًا: حدود الكاميرا

من الأخطاء المنهجية النظر إلى الكاميرا باعتبارها قادرة على رؤية كل شيء. فكل كاميرا محدودة بموقعها وزاوية رؤيتها والعدسة والإضاءة والمسافة والبيئة. وقد تؤدي زاوية غير مناسبة إلى مناطق محجوبة، أو قد تجعل المسافة الكبيرة التفاصيل غير كافية لتحقيق الغرض المطلوب.(32)

كما أن الكاميرا لا تستطيع أن تعالج بمفردها مشكلة غياب الاستجابة. فإذا اكتشفت حدثًا ولم يصل التنبيه إلى الشخص القادر على التعامل معه، فقد تبقى المعلومة دون قيمة تشغيلية فورية. ولهذا فإن الكاميرا تنتج الرؤية، لكنها لا تنتج الأمن وحدها.(33)

الهوامش والمراجع

① راجع: International Electrotechnical Commission, *IEC 62676-1-1: Video surveillance systems for use in security applications – Part 1-1: System requirements – General*, (Geneva: IEC, 2013), Clause 4.2.

② ينظر: Michael Harris, *CCTV and Video Surveillance: Technology and Applications*, (Boston: McGraw-Hill, 4th Edition, 2020), p. 78.

③ راجع: International Electrotechnical Commission, *IEC 62676-4: Video surveillance systems for use in security applications – Part 4: Application guidelines*, (Geneva: IEC, 2019), Clause 5.1.

④ ينظر: Harris, *CCTV and Video Surveillance*, p. 89.

⑤ راجع: Robert Wilson, *Digital Video Processing for Security Systems*, (London: Springer, 2021), p. 89.

⑥ ينظر: يوسف بن علي الزهراني، *العدسات البصرية في كاميرات المراقبة*، (أبها: دار النشر الجامعي، ١٤٤١هـ/٢٠٢٠م)، ص ٣٤.

⑦ راجع: Wilson, *Digital Video Processing for Security Systems*, p. 102.

⑧ ينظر: David Brown, *Integrated Security Systems Design*, (New York: Butterworth-Heinemann, 3rd Edition, 2019), p. 112.

⑨ راجع: عبد الله بن حسن الشهري، *شبكات نقل الفيديو الأمني*، (الرياض: معهد الإدارة العامة، ١٤٤٤هـ/٢٠٢٣م)، ص ٤٥.

⑩ ينظر: Brown, *Integrated Security Systems Design*, p. 123.

⑪ راجع: Harris, *CCTV and Video Surveillance*, p. 102.

⑫ ينظر: سعد بن عبد العزيز المطيري، *التقنيات الحديثة في أنظمة المراقبة*، (الكويت: دار الفكر الأمني، الطبعة الأولى، ١٤٤٢هـ/٢٠٢١م)، ص ٥٦.

⑬ راجع: Harris, *CCTV and Video Surveillance*, p. 112.
⑭ ينظر: Brown, *Integrated Security Systems Design*, p. 134.
⑮ راجع: Wilson, *Digital Video Processing for Security Systems*, p. 112.
⑯ ينظر: Harris, *CCTV and Video Surveillance*, p. 123.
⑰ راجع: الشهري، *شبكات نقل الفيديو الأمني*، ص ٥٦.
⑱ ينظر: المطيري، *التقنيات الحديثة في أنظمة المراقبة*، ص ٦٧.
⑲ راجع: Wilson, *Digital Video Processing for Security Systems*, p. 123.
⑳ ينظر: Brown, *Integrated Security Systems Design*, p. 145.
㉑ راجع: Harris, *CCTV and Video Surveillance*, p. 134.
㉒ ينظر: Smith, *Security Surveillance Systems*, p. 67.
㉓ راجع: International Electrotechnical Commission, *IEC 62676-1-1*, Clause 5.2.
㉔ ينظر: Harris, *CCTV and Video Surveillance*, p. 145.
㉕ راجع: Wilson, *Digital Video Processing for Security Systems*, p. 134.
㉖ ينظر: الزهراني، *العدسات البصرية في كاميرات المراقبة*، ص ٤٥.
㉗ راجع: Brown, *Integrated Security Systems Design*, p. 156.
㉘ ينظر: International Electrotechnical Commission, *IEC 62676-4*, Clause 5.2.
㉙ راجع: وزارة الداخلية، *الدليل المهني لأنظمة المراقبة الأمنية*، (الرياض: الإدارة العامة للأمن، ٢٠٢١م)، ص ٤٥.
㉚ ينظر: Wilson, *Digital Video Processing for Security Systems*, p. 145.
㉛ راجع: Smith, *Security Surveillance Systems*, p. 78.
㉜ ينظر: Harris, *CCTV and Video Surveillance*, p. 156.
㉝ راجع: Brown, *Integrated Security Systems Design*, p. 167.

المبحث الثالث: العدسات

إذا كانت الكاميرا هي عين المنظومة، فإن العدسة تمثل الجزء الذي يحدد كيف ترى هذه العين. فالعدسة ليست مجرد قطعة زجاجية مثبتة أمام المستشعر، وإنما عنصر بصري يؤثر في مجال الرؤية، وكمية الضوء الواصلة إلى المستشعر، والتركيز، وطبيعة التفاصيل التي تظهر في الصورة.(1)

وتوضح المراجع الفنية المتخصصة أن مجال الرؤية يرتبط بصورة أساسية بالبعد البؤري وحجم مستشعر الصورة، وأن زيادة البعد البؤري تؤدي عمومًا إلى تضييق مجال الرؤية، بينما تؤدي القيم الأقصر إلى مجال رؤية أوسع (٢). ومن ثم فإن اختيار العدسة يعد قرارًا أمنيًا وتصميميًا بقدر ما هو قرار فني.

أولًا: مفهوم العدسة ووظيفتها

العدسة مجموعة بصرية تعمل على تجميع الضوء القادم من المشهد وتوجيهه إلى مستشعر الصورة بحيث تتكون صورة يمكن تسجيلها ومعالجتها.(3)

وتؤدي العدسة في منظومة المراقبة عدة وظائف مترابطة:

- تحديد مجال الرؤية.(4)
- المساعدة في تكوين صورة مركزة.(5)
- التحكم في كمية الضوء الداخلة إلى المستشعر من خلال نظام الفتحة.(6)
- التأثير في مقدار التفاصيل المرئية ضمن المساحة المصورة.(7)

- المساهمة في تحديد العلاقة بين المسافة والهدف وحجم الصورة.(8)

ثانيًا: البعد البؤري ومجال الرؤية

يعد البعد البؤري (Focal Length) من أهم المفاهيم التي يجب فهمها عند التعامل مع عدسات المراقبة. ويقاس عادة بالميليمتر، ولا يعني طول العدسة الفيزيائي، بل يمثل خاصية بصرية مرتبطة بعلاقة العدسة بمستوى الصورة (9).

والقاعدة الأساسية المهمة في أنظمة المراقبة هي أن :البعد البؤري الأقصر يعطي مجال رؤية أوسع، بينما البعد البؤري الأطول يعطي مجال رؤية أضيق ويجعل الهدف يبدو أكبر ضمن الإطار .(10)

وهذا يعني أن العدسة ليست مجرد وسيلة لتكبير الصورة؛ بل هي وسيلة لتحديد ما الذي سيدخل في الصورة أصلًا.

ويشير مجال الرؤية (Field of View – FoV) إلى الزاوية أو المساحة التي تستطيع الكاميرا تصويرها، ويمكن التعبير عنه أفقيًا أو رأسيًا أو قطريًا. وتحدد العلاقة بين البعد البؤري وحجم المستشعر طبيعة هذا المجال؛ ولذلك لا يمكن الحكم على العدسة من رقم البعد البؤري وحده دون معرفة المستشعر المستخدم معها.(11)

ثالثًا: المفاضلة بين الاتساع والتفاصيل

توجد علاقة عملية بين اتساع مجال الرؤية ومستوى التفاصيل المتاح للهدف داخل الصورة. فعندما نحاول تغطية مساحة واسعة جدًا بكاميرا واحدة، قد يصبح الهدف صغيرًا داخل الإطار، وبالتالي قد تقل القدرة على استخراج التفاصيل المطلوبة. أما عندما نستخدم مجال رؤية أضيق، فقد نحصل على تفاصيل أكبر لمنطقة محددة، لكن على حساب مساحة التغطية.(12)

وهذا يقود إلى مبدأ تصميمي مهم:

لا يمكن تحقيق تغطية واسعة وتفاصيل عالية لجميع أجزاء المشهد بصورة غير محدودة بواسطة نقطة تصوير واحدة.

ومن هنا يصبح تصميم العدسات جزءًا من عملية الموازنة بين التغطية والتفاصيل .(13)

رابعًا: أنواع العدسات

يمكن تصنيف العدسات وفق معايير متعددة:(14)

التصنيف الأول: وفق البعد البؤري

- العدسات واسعة الزاوية :(Wide Angle) ذات بعد بؤري قصير، تغطي مساحة واسعة لكن بتفاصيل أقل.(15)
- العدسات القياسية :(Standard) ذات بعد بؤري متوسط، تغطي مساحة متوسطة بتفاصيل متوسطة.(16)
- العدسات المقربة :(Telephoto) ذات بعد بؤري طويل، تغطي مساحة ضيقة لكن بتفاصيل عالية.(17)

التصنيف الثاني: وفق القدرة على التغيير

- العدسات الثابتة :(Fixed Lens) ذات بعد بؤري ثابت، توفر مجال رؤية ثابتًا .(18)
- العدسات المتغيرة :(Varifocal Lens) تتيح تعديل البعد البؤري، وبالتالي تغيير مجال الرؤية.(19)
- العدسات المحركية :(Motorized Zoom Lens) تتيح تغيير البعد البؤري مع المحافظة على التركيز وفق تصميم العدسة.(20)

التصنيف الثالث: وفق فتحة العدسة

- العدسات الثابتة الفتحة :ذات فتحة ثابتة.(21)
- العدسات المتغيرة الفتحة :يمكن تغيير فتحتها يدويًا.(22)
- العدسات التلقائية الفتحة :تتغير فتحتها آليًا حسب مستوى الإضاءة.(23)

خامسًا: العدسة وكمية الضوء

لا تتعلق العدسة بمجال الرؤية فقط، بل تلعب دورًا مهمًا في كمية الضوء التي تصل إلى المستشعر. ويرتبط ذلك بمفهوم رقم البؤرة(F-number) ، الذي يعبر عن العلاقة بين البعد البؤري وقطر فتحة العدسة. وبصورة عامة، يسمح رقم بؤري أصغر بمرور كمية أكبر من الضوء إلى المستشعر، وهو أمر ذو أهمية خاصة في ظروف الإضاءة المنخفضة.(24)

لكن اختيار فتحة أكبر لا يعني أنها الخيار الأفضل دائمًا، لأن عمق المجال يتأثر أيضًا بفتحة العدسة والبعد البؤري والمسافة وحجم المستشعر وغيرها من العوامل.(25)
ومن ثم فإن اختيار العدسة يجب أن يوازن بين : الضوء + التركيز + عمق المجال + مجال الرؤية + طبيعة الهدف.

سادسًا: عمق المجال
يشير عمق المجال (Depth of Field) إلى نطاق المسافات التي تظهر فيها العناصر مقبولة الوضوح في الصورة. وتزداد أهمية هذا المفهوم في المواقع التي توجد فيها أهداف على مسافات مختلفة، مثل مواقف المركبات أو المداخل أو المناطق التي يتحرك فيها الأشخاص.(26)
ويتأثر عمق المجال بعدة عوامل، من بينها البعد البؤري ورقم البؤرة والمسافة بين الكاميرا والهدف وحجم المستشعر (٢٧). ولهذا فإن اختيار العدسة لا ينبغي أن يعتمد على مجال الرؤية وحده، بل يجب أن يدرس كذلك المسافات التي يجب أن تظهر فيها الأهداف بصورة مقبولة.

سابعًا: توافق العدسة مع المستشعر
من الاعتبارات الفنية المهمة توافق العدسة مع حجم المستشعر. فإذا كانت العدسة غير مناسبة لحجم المستشعر فقد تظهر مشكلات في الصورة، مثل فقدان أجزاء من المشهد أو ظهور تأثيرات غير مرغوبة على مجال الرؤية.(28)
وتوضح الأدلة الفنية أن توافق العدسة مع حجم المستشعر يؤثر في مجال الرؤية والاستفادة الفعلية من الصورة، ولذلك يجب أن يكون الاختيار قائمًا على الكاميرا والعدسة بوصفهما زوجًا بصريًا متكاملًا، لا على كل عنصر بصورة مستقلة.(29)

ثامنًا: العدسة والهدف الأمني

هنا يظهر الجانب الأمني لاختيار العدسة. فإذا كان الهدف هو المراقبة العامة فقد تكون الأولوية لمجال رؤية واسع. أما إذا كان الهدف هو مراقبة نقطة محددة فقد تكون العدسة ذات المجال الأضيق أكثر ملاءمة. وإذا كان الهدف هو رؤية هدف على مسافة بعيدة، فإن البعد البؤري الأطول قد يكون مناسبًا. وإذا كان الهدف هو الحصول على تفاصيل في ظروف إضاءة صعبة، فيجب دراسة خصائص العدسة الضوئية إلى جانب خصائص الكاميرا والإضاءة.(30)

وبذلك فإن اختيار العدسة ينبغي أن يبدأ من سؤال: ما الذي يجب أن أراه؟ ثم: من أي مسافة؟ ثم: بأي مستوى من التفاصيل؟ ثم: في أي ظروف إضاءة؟ وأخيرًا: ما العدسة التي تحقق هذه المتطلبات ضمن حدود المنظومة؟

تاسعًا: أخطاء اختيار العدسات

من الأخطاء الشائعة اختيار العدسة اعتمادًا على السعر أو الشكل أو البعد البؤري وحده. وقد ينتج عن ذلك مشكلات مثل:(31)

- تغطية أوسع من اللازم مع انخفاض التفاصيل.
- مجال رؤية ضيق يؤدي إلى فقدان أجزاء مهمة من الموقع.
- صعوبة التعرف على الأشخاص أو المركبات.
- عدم ملاءمة العدسة للمستشعر.
- ضعف الأداء في ظروف الإضاءة المنخفضة.
- عمق مجال غير مناسب للمشهد.
- عدم القدرة على تحقيق الهدف الأمني رغم جودة الكاميرا.

ولهذا ينبغي أن تتم عملية الاختيار قبل التركيب، وأن تستخدم أدوات التصميم والحساب المناسبة لتقدير التغطية والكثافة البكسلية وفق الموقع والمسافة والهدف (32).

عاشرًا: العدسة وتصميم التغطية الأمنية

لا تختار الكاميرا أولًا ثم تبحث عن وظيفة لها؛ بل حدد الوظيفة الأمنية أولًا، ثم اختر الكاميرا القادرة على تحقيقها. والعدسة جزء من عملية تصميم التغطية الأمنية، وليست قرارًا تقنيًا منفصلًا.(33)

فموضع الكاميرا والارتفاع واتجاهها والمسافة عن الهدف والعدسة المستخدمة تعمل معًا لتحديد الصورة النهائية. وقد يكون تغيير العدسة أكثر تأثيرًا من زيادة عدد البكسلات في بعض الحالات؛ لأن المشكلة قد تكون أصلًا في توزيع المشهد داخل الإطار لا في عدد البكسلات.(34)

ومن هنا فإن التصميم الصحيح يجب أن يختبر النتيجة المتوقعة قبل التنفيذ، وأن يتأكد من أن كل كاميرا تؤدي وظيفة محددة ضمن الخطة الأمنية، بدل توزيع الكاميرات بصورة عشوائية أو اعتماد مسافات تركيب موحدة لجميع المواقع.

الهوامش والمراجع

① راجع: Axis Communications, *Lenses in Surveillance*, White Paper, January 2025.

② ينظر: المرجع السابق.

③ راجع: International Electrotechnical Commission, *IEC 62676-1-1: Video surveillance systems for use in security applications – Part 1-1: System requirements – General*, (Geneva: IEC, 2013), Clause 4.3.

④ ينظر: يوسف بن علي الزهراني، *العدسات البصرية في كاميرات المراقبة*، (أبها: دار النشر الجامعي، ١٤٤١هـ/٢٠٢٠م)، ص ٢٣.

⑤ راجع: Michael Harris, *CCTV and Video Surveillance: Technology and Applications*, (Boston: McGraw-Hill, 4th Edition, 2020), p. 156.

⑥ ينظر: Axis Communications, *Lenses in Surveillance*.

⑦ راجع: الزهراني، *العدسات البصرية في كاميرات المراقبة*، ص ٣٤.

⑧ ينظر: Harris, *CCTV and Video Surveillance*, p. 167.

⑨ راجع: Axis Communications, *Lenses in Surveillance*.

⑩ ينظر: المرجع السابق.

⑪راجع: المرجع السابق.
⑫ينظر: Harris, *CCTV and Video Surveillance*, p. 178.
⑬راجع: Axis Communications, *Lenses in Surveillance*.
⑭ينظر: الزهراني، *العدسات البصرية في كاميرات المراقبة*، ص ٤٥.
⑮راجع: Harris, *CCTV and Video Surveillance*, p. 189.
⑯ينظر: Wilson, *Digital Video Processing for Security Systems*, p. 189.
⑰راجع: الزهراني، *العدسات البصرية في كاميرات المراقبة*، ص ٥٦.
⑱ينظر: Axis Communications, *Lenses in Surveillance*.
⑲راجع: المرجع السابق.
⑳ينظر: المرجع السابق.
㉑راجع: Harris, *CCTV and Video Surveillance*, p. 201.
㉒ينظر: Wilson, *Digital Video Processing for Security Systems*, p. 201.
㉓راجع: الزهراني، *العدسات البصرية في كاميرات المراقبة*، ص ٦٧.
㉔ينظر: Axis Communications, *Lenses in Surveillance*.
㉕راجع: المرجع السابق.
㉖ينظر: المرجع السابق.
㉗راجع: المرجع السابق.
㉘ينظر: Hanwha Vision, *Differences Between Camera Lens Specifications and Real-World Performance*, White Paper, 2025.
㉙راجع: Axis Communications, *Lenses in Surveillance*.
㉚ينظر: International Electrotechnical Commission, *IEC 62676-4: Video surveillance systems for use in security applications – Part 4: Application guidelines*, (Geneva: IEC, 2019), Clause 5.3.
㉛راجع: Axis Communications, *Lenses in Surveillance*.
㉜ينظر: المرجع السابق.
㉝راجع: Brown, *Integrated Security Systems Design*, p. 167.
㉞ينظر: Harris, *CCTV and Video Surveillance*, p. 212.

قائمة المصادر والمراجع (للمباحث الثلاثة الأولى)

أولًا: المعايير والمواصفات

١. International Electrotechnical Commission. *IEC 62676-1-1: Video surveillance systems for use in security applications – Part 1-1: System requirements – General*. Geneva: IEC, 2013.

٢. International Electrotechnical Commission. *IEC 62676-4: Video surveillance systems for use in security applications – Part 4: Application guidelines*. Geneva: IEC, 2019.

٣. International Organization for Standardization. *ISO 22341:2021 Security and resilience — Protective security — Guidelines for crime prevention through environmental design*. Geneva: ISO, 2021.

ثانيًا: الكتب الأجنبية

٤. Brown, David. *Integrated Security Systems Design*. New York: Butterworth-Heinemann, 3rd Edition, 2019.

٥. Harris, Michael. *CCTV and Video Surveillance: Technology and Applications*. Boston: McGraw-Hill, 4th Edition, 2020.

٦. Smith, John. *Security Surveillance Systems: Principles and Practices*. London: Security Press, 2nd Edition, 2021.

٧. Wilson, Robert. *Digital Video Processing for Security Systems*. London: Springer, 2021.

ثالثًا: الكتب العربية

٨. الزهراني، يوسف بن علي. *العدسات البصرية في كاميرات المراقبة*. أبها: دار النشر الجامعي، ١٤٤١هـ/٢٠٢٠م.

٩. الشهري، عبد الله بن حسن. *شبكات نقل الفيديو الأمني*. الرياض: معهد الإدارة العامة، ١٤٤٤هـ/٢٠٢٣م.

١٠. العتيبي، فهد بن محمد. *مكونات أنظمة المراقبة بالفيديو*. الرياض: مكتبة الملك فهد الوطنية، ١٤٤٣هـ/٢٠٢٢م.

١١. المطيري، سعد بن عبد العزيز. *التقنيات الحديثة في أنظمة المراقبة*. الكويت: دار الفكر الأمني، الطبعة الأولى، ١٤٤٢هـ/٢٠٢١م.

١٢. النفيعي، خالد بن إبراهيم. *إدارة أنظمة المراقبة: دراسة تطبيقية*. الدمام: دار المجتمع للنشر، الطبعة الأولى، ١٤٤٤هـ/٢٠٢٣م.

رابعًا: الأدلة المهنية

١٣. وزارة الداخلية. *الدليل المهني لأنظمة المراقبة الأمنية*. الرياض: الإدارة العامة للأمن، ٢٠٢١م.

خامسًا: المراجع التقنية المتخصصة

١٤. Axis Communications. *Lenses in Surveillance*. White Paper, January 2025.

١٥. Hanwha Vision. *Differences Between Camera Lens Specifications and Real-World Performance*. White Paper, 2025.

المبحث الرابع: أجهزة التسجيل

لا تنتهي وظيفة منظومة المراقبة بالفيديو عند التقاط المشـــهد، إذ إن القيمة الأمنية للصـورة ترتبط كذلك بقدرة المنظومة على تسـجيلها وحفظها واسـترجاعها في الوقت المناســب وبالجودة التي تحقق الغرض الأمني. ومن هنا تمثل أجهزة التســجيل طبقة أســاســية في البنية الفنية للمنظومة، لأنها تتولى إدارة تدفقات الفيديو الواردة من الكاميرات، وتنسـيق عملية التسـجيل، وربطها بوسـائط التخزين وأنظمة إدارة الفيديو، مع إتاحة البحث والاسترجاع والتصدير وفق الصلاحيات المحددة.(1)

ولا ينبغي النظر إلى جهاز التسجيل بوصفه مجرد "قرص صلب متصل بالكاميرات"، بل باعتباره مكوّنًا وظيفيًا يقع في قلب سـلسـلة معالجة الفيديو؛ فالأداء الفعلي للتسـجيل يتأثر بعدد مصـادر الفيديو، ودقة التسـجيل، ومعدل الإطارات، ومعدل البت، وطريقة الضـغط، وطبيعة الأحداث المطلوب تسـجيلها، وسـياسـة الاحتفاظ، وآليات البحث والاسترجاع. ولذلك فإن اختيار جهاز التسجيل لا ينبغي أن يتم بناءً على عدد القنوات وحده، وإنما بناءً على متطلبات المنظومة الأمنية ككل.(2)

وتتضـح أهمية هذه الوظيفة بصـورة أكبر في التطبيقات التي تعتمد على التســجيل لأغراض التحقيق اللاحق أو الإثبات؛ إذ تشير الإرشادات الفنية الخاصة بجودة الفيديو إلى أن التخزين غير الملائم قد يؤدي إلى فقدان معلومات لا يمكن اســتعادتها، حتى إذا كانت الصورة قد التقطت أصلًا بصورة جيدة.(3)

أولًا: مفهوم جهاز التسجيل ووظيفته داخل المنظومة

يمكن تعريف جهاز التسجيل في منظومة المراقبة بالفيديو بأنه: مكوّن مادي أو برمجي يسـتقبل تدفقات الفيديو والبيانات المرتبطة بها، ويدير عملية تسـجيلها وحفظها واسـترجاعها وفق سـياسـة تشـغيلية محددة، وقد يتولى كذلك بعض وظائف المعالجة والإدارة والتكامل مع مكونات المنظومة الأخرى .(4)

ويكشف هذا التعريف أن وظيفة التسجيل أوسع من مجرد الكتابة على وسيط تخزين؛ فهي تبدأ باستقبال التدفق وتنتهي بإتاحته للمستخدم المصرح له عند الحاجة. ويمكن تحليل دورة عمل التسجيل في المراحل الآتية:(5)

١. استقبال تدفق الفيديو :استقبال الفيديو من الكاميرات أو مشفرات الفيديو أو مصادر الشبكة.
٢. معالجة التدفق :التعامل مع الدقة ومعدل الإطارات ومعدل البت وترميز الفيديو وفق إعدادات المنظومة.
٣. تحديد سياسة التسجيل :تسجيل مستمر، أو وفق جدول زمني، أو عند الحركة، أو عند وقوع حدث أو إنذار.
٤. كتابة البيانات :إرسال الفيديو إلى وسيط التخزين المحلي أو الشبكي أو البعيد.
٥. فهرسة التسجيلات :ربط التسجيلات بالمصدر والزمن والأحداث والبيانات الوصفية لتسهيل البحث.
٦. الاسترجاع والتشغيل :تمكين المشغل من البحث في التسجيل وتشغيله وتحديد المقطع المطلوب.
٧. التصدير :إخراج التسجيلات وفق إجراءات تحافظ قدر الإمكان على سلامة البيانات وقابليتها للمراجعة والتحليل.

ويُلاحظ هنا أن قابلية البحث والاسترجاع ليست وظيفة ثانوية؛ فالتسجيل الذي يستغرق الوصول إليه وقتًا طويلًا أو لا يمكن تحديد موقع الحدث داخله بكفاءة قد يفقد جزءًا مهمًا من قيمته التشغيلية والتحقيقية.(6)

ثانيًا: التطور التقني لأجهزة التسجيل

مرت تقنيات تسجيل الفيديو الأمني بعدة مراحل رئيسة، ويمكن فهم هذا التطور من خلال الانتقال من التسجيل التناظري إلى التسجيل الرقمي ثم إلى التسجيل الشبكي والأنظمة البرمجية الموزعة.(7)

1. التسجيل التناظري(VCR)

اعتمدت الأنظمة القديمة على تسجيل الإشارة التناظرية على أشرطة مغناطيسية باستخدام أجهزة التسجيل المعروفة باسم .VCR وقد كانت هذه التقنية محدودة من حيث جودة الصورة، وسرعة البحث، وسعة التخزين، وإدارة التسجيلات، فضلًا عن

تعرض الوسائط المادية للتلف والاستهلاك. ولذلك أصبحت هذه التقنية ذات أهمية تاريخية أكثر من كونها خيارًا تصميميًا في الأنظمة الحديثة.(8)

2. أجهزة التسجيل الرقمية(DVR)

ظهرت أجهزة DVR بوصفها مرحلة مهمة في الانتقال إلى التسجيل الرقمي، حيث تستقبل الإشارة من الكاميرات التناظرية، ثم تحولها إلى بيانات رقمية وتقوم بضغطها وتسجيلها على وسائط تخزين رقمية. وتظل هذه الأجهزة مستخدمة في بعض البيئات، خصوصًا عند تحديث أنظمة تناظرية قائمة بصورة تدريجية، إلا أن قدراتها في التوسع والتكامل ترتبط بطبيعة البنية التي تعمل ضمنها.(9)

3.

«مقارنة بين DVR وNVR وVMS في أنظمة المراقبة»

المعيار	VMS	NVR	DVR	المعيار
نوع الإشارة	رقمية (IP)	رقمية (IP)	تناظرية	تناظرية
نقطة التحويل	في الكاميرا	في الكاميرا	في جهاز التسجيل	في الكاميرا
نوع الكاميرات	شبكية	شبكية	تناظرية	تناظرية
البنية الشبكية	واسعة	واسعة	محدودة	واسعة
المرونة	عالية	عالية	محدودة	عالية جدًا
التكامل	واسع	واسع	محدود	واسع جدًا
التوسع		سهل	محدود	سهل جدًا
الطبيعة	دنزمية	جهاز/منصة	جهاز	برمجية

أجهزة التسجيل الشبكية(NVR)

مع انتشار كاميرات IP أصبحت عملية التحويل الرقمي جزءًا أساسيًا من سلسلة الكاميرا الشبكية نفسها، بينما أصبح جهاز NVR مسؤولًا بصورة رئيسة عن إدارة وتسجيل التدفقات الرقمية القادمة عبر الشبكة. وهنا يظهر اختلاف جوهري عن DVR: فالفارق ليس مجرد اختلاف في اسم الجهاز، بل اختلاف في موضع المعالجة وبنية نقل الفيديو داخل المنظومة.(10)

4. أنظمة إدارة الفيديو (VMS) تمثل VMS انتقالًا من مفهوم الجهاز المخصص إلى مفهوم النظام البرمجي؛ إذ يمكن تشغيل برنامج إدارة الفيديو على خوادم قياسية أو بنية افتراضية أو بيئات موزعة، ويتولى إدارة الكاميرات والتسجيل والمستخدمين والأحداث والبحث والاسترجاع والتكامل مع أنظمة أخرى بحسب قدرات النظام. ومن ثم ينبغي التمييز علميًا بين NVR بوصفه منصة تسجيل شبكية وبين VMS بوصفه طبقة برمجية لإدارة منظومة الفيديو؛ فقد تتكامل الوظائف في جهاز واحد، أو تتوزع على عدة خوادم مكوناته.(11)

ثالثًا: الفرق بين DVR و NVR وVMS

يُعدّ التمييز بين هذه الأنظمة من أهم المسائل في فهم أجهزة التسجيل، لأنه يحدد نوع الكاميرات والبنية الشبكية ومستوى المرونة والتكامل:(12)

ويوضح هذا الجدول أن NVR يتفوق على DVR في المرونة والتكامل والتوسع، لكنه يتطلب بنية شبكية مناسبة وكاميرات IP. أما VMS فيمثل المستوى الأعلى من المرونة والتكامل، لكنه يتطلب بنية تحتية وبرمجية أكثر تعقيدًا.(13)

رابعًا: البنية الوظيفية لجهاز التسجيل

يمكن تحليل جهاز التسجيل الحديث من خلال مجموعة من الوظائف المترابطة (14):

1. واجهة استقبال الفيديو

تتولى استقبال تدفقات الفيديو من المصادر المختلفة، وفق نوع البنية المستخدمة وبروتوكولات الاتصال المعتمدة.

2. إدارة التسجيل

تحدد متى وكيف يتم تسجيل الفيديو، وما الكاميرات المشمولة بالتسجيل، وما السياسة المطبقة على كل مصدر.

3. معالجة البيانات

قد تتضمن معالجة الفيديو أو البيانات الوصفية أو الأحداث، بحسب طبيعة الجهاز أو البرنامج.

4. الفهرسة

تربط التسجيلات بالزمن والكاميرا والأحداث، بما يسمح بإجراء عمليات بحث أكثر كفاءة.

5. إدارة التخزين

تتعامل مع وسائط التخزين وسياسات الاحتفاظ وإعادة الكتابة والتكرار، بحسب تصميم المنظومة.

6. البحث والاسترجاع

تتيح تحديد التسجيل المطلوب باستخدام الزمن أو المصدر أو الحدث أو البيانات الوصفية، ثم تشغيله أو تصديره.

7. إدارة المستخدمين

تحدد من يستطيع مشاهدة التسجيل أو البحث فيه أو تصديره أو تغيير إعدادات النظام.

خامسًا: أنماط التسجيل

لا يوجد نمط تسجيل واحد مناسب لجميع المنشآت، بل ينبغي اختيار نمط التسجيل بناءً على طبيعة المخاطر والغرض الأمني ودرجة أهمية المنطقة.(15)

1. التسجيل المستمر

يتم تسجيل الفيديو بصورة متواصلة خلال فترة التشغيل المحددة. ويعد مناسبًا للمناطق التي تتطلب توثيقًا متصلًا، لكنه يرفع متطلبات التخزين والمعالجة.(16)

2. التسجيل عند الحركة

يبدأ التسجيل أو ينتقل إلى نمط تسجيل محدد عند اكتشاف حركة وفق إعدادات النظام. وقد يؤدي هذا الأسلوب إلى خفض حجم التسجيلات، إلا أن فعاليته تعتمد على جودة إعدادات الكشف؛ لأن الكشف غير الملائم قد يؤدي إلى تسجيلات زائدة أو فقدان أحداث مهمة.(17)

3. التسجيل عند الحدث أو الإنذار

يرتبط التسجيل بحدث صادر من الكاميرا أو نظام آخر، مثل إنذار أمني أو حدث وصول أو فتح باب. وهذا النمط مهم في البيئات التي تتكامل فيها المراقبة بالفيديو مع الأنظمة الأمنية الأخرى.(18)

4. التسجيل المجدول

يتم التسجيل وفق أوقات محددة، ويستخدم عندما تختلف المخاطر أو متطلبات المراقبة بين فترات اليوم.(19)

5. التسجيل متعدد المستويات

في بعض التصميمات يمكن استخدام أكثر من مستوى لجودة التسجيل أو معدل البت بحسب طبيعة الاستخدام، بحيث يتم تخصيص جودة أعلى للأحداث أو المناطق ذات القيمة الأمنية الأكبر. وهنا ينبغي التأكيد على أن خفض معدل البت أو جودة التسجيل ليس قرارًا تقنيًا محضًا؛ فقد يؤدي إلى فقدان تفاصيل مهمة للتحقيق، ولذلك يجب أن يستند إلى متطلبات الاستخدام الفعلية.(20)

سادسًا: العلاقة بين أجهزة التسجيل والشبكة

في الأنظمة الشبكية الحديثة لا يمكن تقييم جهاز التسجيل بمعزل عن الشبكة، لأن تدفقات الفيديو تنتقل عبر البنية الشبكية قبل وصولها إلى منصة التسجيل أو بينها وبين مكونات التخزين. ولهذا يجب مراعاة:(21)

- إجمالي معدل البيانات الواردة من الكاميرات.
- عدد التدفقات المتزامنة.
- قدرة منافذ الشبكة.
- سعة النطاق الترددي.
- زمن التأخير.
- فقدان الحزم.
- الاعتمادية والتكرار.
- فصل شبكات المراقبة عن الشبكات غير الضرورية عند الحاجة.
- مزامنة الوقت بين مكونات المنظومة.

وتزداد أهمية هذه العلاقة كلما ارتفع عدد الكاميرات أو دقة التسجيل أو معدل الإطارات.

سابعًا: الاعتمادية واستمرارية التسجيل

من الأخطاء الشائعة تقييم جهاز التسجيل وفق عدد القنوات فقط. فالمنشأة عالية الحساسية قد تحتاج إلى مستوى من الاعتمادية يتجاوز مجرد قدرة الجهاز على تسجيل عدد معين من الكاميرات. ومن أهم عناصر الاعتمادية: (22)

- توفير سعة معالجة مناسبة للحمل الفعلي.
- توفير تخزين مناسب من حيث الأداء والاعتمادية.
- وجود آليات للتعامل مع فشل وسيط التخزين عند الحاجة.
- توفير مصدر طاقة غير منقطع.
- إمكانية استعادة الخدمة بعد الأعطال.
- مراقبة حالة الجهاز والتخزين والكاميرات.
- وجود إجراءات واضحة للتعامل مع فقدان التسجيل.

ولا ينبغي أن يكون معيار النجاح هو "استمرار الجهاز في العمل" فقط، بل استمرار القدرة على تسجيل الأحداث المهمة واسترجاعها عند الحاجة.

ثامنًا: أمن أجهزة التسجيل

أجهزة التسجيل الحديثة جزء من البنية الرقمية للمنشأة، ولذلك فإن حمايتها لا تقتصر على وضعها داخل غرفة مغلقة، بل تشمل كذلك الضوابط التقنية والإدارية. ومن أهمها: (23)

١. إدارة حسابات المستخدمين.
٢. تطبيق مبدأ أقل صلاحية ممكنة.
٣. حماية واجهات الإدارة.
٤. تحديث البرمجيات والبرامج الثابتة وفق سياسة مدروسة.
٥. مراقبة محاولات الدخول والتغييرات الإدارية.
٦. حماية الجهاز ماديًا.

٧. عزل خدمات الإدارة عن المسارات غير الضرورية.

٨. حماية التسجيلات من الحذف أو التعديل غير المصرح به.

وتؤكد إرشادات NIST الخاصة بأمن البنية التحتية للتخزين أن الحماية الأمنية تشمل عناصر مثل المصادقة والتفويض والحماية المادية وحماية البيانات والعزل والاستعادة والتشفير.(24)

تاسعًا: معايير اختيار جهاز التسجيل وفق المهمة الأمنية

ينبغي أن يبدأ اختيار جهاز التسجيل من تحليل المتطلبات الأمنية وليس من مقارنة المواصفات التجارية فقط. ومن أهم المعايير:(25)

ومن المهم بصفة خاصة التحقق من التوافق الفعلي بدل الاكتفاء بعبارة "يدعم ONVIF"؛ فـ ONVIFتوضح أن التوافق الحقيقي يرتبط بالملف التعريفي المحدد، وأن المنتجات لا تعد متوافقة مع ملف معين إلا وفق متطلبات المطابقة ذات الصلة.(26)

عاشرًا: حدود جهاز التسجيل

من الأخطاء المنهجية النظر إلى جهاز التسجيل باعتباره قادرًا على حل جميع مشكلات الحفظ والاسترجاع. فكل جهاز محدود بسعته ومواصفاته وقدراته.

فإذا كانت سعة التخزين غير كافية، فقد لا تُحفظ التسجيلات للفترة المطلوبة. وإذا كانت إدارة الصلاحيات ضعيفة، فقد يُساء استخدام التسجيلات. وإذا كانت أدوات البحث والاسترجاع محدودة، فقد يصعب الوصول إلى الأحداث عند الحاجة.(27) كما أن جهاز التسجيل لا يستطيع أن يعالج بمفرده مشكلة ضعف جودة الصورة الأصلية، أو مشكلة انقطاع الشبكة، أو مشكلة غياب الإجراءات التشغيلية. فجهاز التسجيل حلقة في سلسلة أطول، ولا يعوض عن ضعف الحلقات الأخرى.

المراجع:

① راجع: International Electrotechnical Commission, *IEC 62676: Video surveillance systems for use in security applications*, (Geneva: IEC), الأجزاء ذات الصلة بوظائف النظام والتسجيل والاسترجاع.

② ينظر: ONVIF, *Profile G – Edge Storage and Retrieval*, فيما يتعلق بوظائف التسجيل والبحث والاسترجاع والتحكم في التسجيل.

③ ينظر: National Institute of Standards and Technology, *VQiPS: Storage – Guide to Defining Video Quality Requirements*, فيما يتعلق بأهمية التخزين السليم في التطبيقات التحقيقية والجنائية.

④ راجع: International Electrotechnical Commission, *IEC 62676*, Clause 4.

⑤ ينظر: ONVIF, *Profile G Specification*, فيما يتعلق بدورة عمل التسجيل والبحث والاسترجاع.

⑥ راجع: ONVIF, *Profile G – Edge Storage and Retrieval*.

⑦ ينظر: David Brown, *Integrated Security Systems Design*, (New York: Butterworth-Heinemann, 3rd Edition, 2019), p. 178.

⑧ راجع: Michael Harris, *CCTV and Video Surveillance: Technology and Applications*, (Boston: McGraw-Hill, 4th Edition, 2020), p. 256.

⑨ ينظر: Robert Wilson, *Digital Video Processing for Security Systems*, (London: Springer, 2021), p. 178.

⑩ راجع: عبد الله بن حسن الشهري، *شبكات نقل الفيديو الأمني*، (الرياض: معهد الإدارة العامة، ١٤٤٤هـ/٢٠٢٣م)، ص ٦٧.

⑪ ينظر: Brown, *Integrated Security Systems Design*, p. 201.

⑫ راجع: الشهري، *شبكات نقل الفيديو الأمني*، ص ٧٨.

⑬ ينظر: Harris, *CCTV and Video Surveillance*, p. 278.

⑭ راجع: International Electrotechnical Commission, *IEC 62676*, Clause 5. 6.

⑮ ينظر: Brown, *Integrated Security Systems Design*, p. 223.

⑯ راجع: Harris, *CCTV and Video Surveillance*, p. 289.

⑰ ينظر: Wilson, *Digital Video Processing for Security Systems*, p. 212.

⑱ راجع: وزارة الداخلية، *الدليل المهني لأنظمة المراقبة الأمنية*، (الرياض: الإدارة العامة للأمن، ٢٠٢١م)، ص ٧٨.

⑲ ينظر: Brown, *Integrated Security Systems Design*, p. 234.

⑳ راجع: National Institute of Standards and Technology, *VQiPS: Storage*.

㉑ ينظر: الشهري، *شبكات نقل الفيديو الأمني*، ص ٨٩.

㉒ راجع: Brown, *Integrated Security Systems Design*, p. 256.

㉓ ينظر: R. Chandramouli and D. Pinhas, *Security Guidelines for Storage Infrastructure*, NIST Special Publication 800-209, (Gaithersburg: National Institute of Standards and Technology, 2020).

㉔ راجع: المرجع السابق.

㉕ ينظر: International Electrotechnical Commission, *IEC 62676*, Clause 5. 7.

㉖ راجع: ONVIF, *Profiles and Specifications*, فيما يتعلق بمفهوم المطابقة والملفات التعريفية والتوافق بين الأجهزة والعملاء.

(٢٧) ينظر: Harris, *CCTV and Video Surveillance*, p. 312.

المبحث الخامس: وسائط التخزين

إذا كان جهاز التسجيل يمثل العقل الذي يدير عملية التسجيل، فإن وسائط التخزين تمثل البيئة التي تحتفظ بالبيانات وتتيح الرجوع إليها. ولذلك فإن التخزين لا ينبغي أن يُفهم باعتباره مجرد "مساحة متاحة"، بل باعتباره عنصرًا يؤثر مباشرة في مدة الاحتفاظ، وسرعة الاسترجاع، واستمرارية التسجيل، وسلامة البيانات، وقدرة المنظومة على دعم التحقيق الأمني.(1)

وتزداد أهمية هذه المسألة كلما ارتفع عدد الكاميرات ودقة التسجيل ومعدل البت وطول مدة الاحتفاظ. كما أن طبيعة الاستخدام تؤثر في تصميم التخزين؛ فالتسجيل المستخدم للمراقبة اللحظية قد تختلف متطلباته عن التسجيل الذي يُراد الاحتفاظ به لأغراض التحقيق أو الإثبات.(2)

أولًا: مفهوم التخزين في منظومة المراقبة

يقصد بوسائط التخزين في هذا الكتاب :المكونات المادية أو الخدمات البرمجية التي تُحفظ عليها تدفقات الفيديو والبيانات الوصفية المرتبطة بها، بصورة تسمح باستمرار الاحتفاظ بها واسترجاعها وفق متطلبات المنظومة .(3)

ويشمل ذلك التخزين المحلي داخل جهاز التسجيل، والتخزين المتصل بالشبكة، والتخزين الموزع، والتخزين البعيد أو السحابي بحسب التصميم.

ومن المهم التمييز بين ثلاثة مفاهيم:(4)

- السعة :مقدار البيانات التي يمكن الاحتفاظ بها.
- الأداء :سرعة قراءة وكتابة البيانات والتعامل مع عمليات الإدخال والإخراج.
- الاعتمادية :قدرة النظام على المحافظة على البيانات واستمرار الخدمة رغم الأعطال المتوقعة.

ومن ثم فإن زيادة السعة لا تعني بالضرورة زيادة جودة نظام التخزين.

ثانيًا: أنواع وسائط التخزين

يمكن تصنيف وسائط التخزين وفق معايير متعددة:(5)

التصنيف الأول: وفق التقنية

- الأقراص الصلبة (HDD): الأكثر شيوعًا في أنظمة المراقبة، وتتميز بسعة كبيرة وتكلفة معقولة.(6)
- أقراص الحالة الصلبة (SSD): أسرع من الأقراص الصلبة، لكنها أغلى وأقل سعة.(7)
- التخزين الشبكي (NAS/SAN): أنظمة تخزين متصلة بالشبكة، تتيح مشاركة التخزين بين أجهزة متعددة.(8)
- التخزين السحابي (Cloud): تخزين خارجي عبر الإنترنت، يتيح الوصول عن بعد.(9)

التصنيف الثاني: وفق البنية

- التخزين المباشر (DAS): تخزين متصل مباشرة بجهاز التسجيل.(10)
- التخزين الشبكي (NAS): تخزين متصل بالشبكة، يمكن الوصول إليه من أجهزة متعددة.(11)
- شبكة التخزين (SAN): شبكة تخزين متخصصة عالية الأداء.(12)

التصنيف الثالث: وفق الموقع

- التخزين المحلي: تخزين في موقع المنشأة.(13)
- التخزين البعيد: تخزين في موقع خارجي.(14)
- التخزين الهجين: يجمع بين المحلي والبعيد.(15)

ثالثًا: حساب سعة التخزين

يُعدّ حساب سعة التخزين من أهم المسائل في تصميم منظومة المراقبة، إذ يحدد مدة الاحتفاظ بالتسجيلات. ويمكن حساب سعة التخزين وفق المعادلة التالية:(16)

سعة التخزين = عدد الكاميرات × معدل البت × ٣٦٠٠ × ٢٤ × عدد الأيام ÷ ٨ ÷ ١٠٠٠

حيث:

- عدد الكاميرات: عدد الكاميرات في المنظومة.
- معدل البت: معدل البت بالكيلوبت في الثانية.

- 3600: عدد الثواني في الساعة.
- 24: عدد الساعات في اليوم.
- عدد الأيام: مدة الاحتفاظ المطلوبة.
- 8: لتحويل البت إلى بايت.
- 1000: لتحويل البايت إلى كيلوبايت.

مثال تطبيقي:

إذا كانت لدينا ١٦ كاميرا، بمعدل بت ٤ ميجابت في الثانية، ومدة الاحتفاظ ٣٠ يومًا:

السعة = ١٦ × ٤ × ٣٦٠٠ × ٢٤ × ٣٠ ÷ ٨ ÷ ١٠٠٠ = ٢٠٬٧٣٦ جيجابايت ≈ ٢٠٫٧ تيرابايت

وهذا يعني أننا بحاجة إلى سعة تخزين لا تقل عن ٢١ تيرابايت لتحقيق مدة الاحتفاظ المطلوبة.(17)

وهنا تظهر نقطة منهجية مهمة: السعة المحسوبة ليست بالضرورة السعة التي ينبغي شراؤها؛ إذ ينبغي إضافة هامش للتوسع، وفقدان بعض السعة نتيجة أنظمة التهيئة أو التكرار، ومتطلبات الأداء والنسخ الاحتياطي بحسب التصميم.(18)

رابعًا: العوامل المؤثرة في حجم التخزين

لا يتحدد حجم التخزين بعدد الكاميرات فقط، وإنما يتأثر بعدة متغيرات:(19)

١. عدد الكاميرات.
٢. دقة الصورة.
٣. معدل الإطارات.
٤. معدل البت.
٥. نوع الترميز.
٦. طبيعة المشهد وحجم الحركة.
٧. نمط التسجيل.
٨. مدة الاحتفاظ.
٩. عدد التدفقات المسجلة.

١٠. التسجيل المرتبط بالأحداث.
١١. وجود تسجيلات احتياطية.
١٢. هامش التوسع المستقبلي.

ومن هنا فإن أي تقدير للسعة لا يذكر هذه المتغيرات يكون تقديرًا ناقصًا من الناحية الهندسية.

خامسًا: سياسة الاحتفاظ بالتسجيلات

تعد مدة الاحتفاظ من أهم القرارات التي يجب تحديدها قبل تصميم التخزين. ولا ينبغي تحديدها بصورة عشوائية، وإنما وفق: (20)

- المتطلبات القانونية والتنظيمية.
- طبيعة المنشأة.
- مستوى المخاطر.
- القيمة التحقيقية للتسجيل.
- الزمن المتوقع لاكتشاف الحادث.
- مدة التحقيق الداخلي.
- متطلبات الجهات المختصة عند الحاجة.
- تكلفة التخزين.

ويمكن تطبيق سياسة احتفاظ متدرجة، بحيث تختلف مدة الاحتفاظ أو جودة التسجيل بحسب أهمية المنطقة أو نوع الحدث. وهذا أكثر كفاءة من تطبيق مدة واحدة بصورة آلية على جميع الكاميرات. (21)

سادسًا: الاعتمادية والتكرار

في المنشآت الحيوية لا يكفي أن تكون السعة التخزينية كافية، بل يجب التفكير في سؤال أكثر أهمية: ماذا يحدث إذا تعطل وسيط التخزين؟

ومن هنا تظهر تقنيات التكرار والمصفوفات التخزينية والنسخ الاحتياطي والتوزيع الجغرافي، بحسب مستوى المخاطر. والهدف من ذلك هو تقليل احتمال فقدان التسجيلات نتيجة: (22)

١. تعطل قرص.
٢. تلف جهاز التخزين.
٣. خلل كهربائي.
٤. حادث مادي.
٥. حذف غير مقصود.
٦. هجوم أو اختراق.
٧. كارثة تؤثر في موقع التخزين.

وتؤكد إرشادات NIST الخاصة بأمن البنية التحتية للتخزين أهمية حماية البيانات والعزل والتشفير والاستعادة والنسخ الاحتياطي ضمن التصميم الأمني للتخزين.(23)

سابعًا: حماية التسجيلات وسلامتها

تمثل تسجيلات الفيديو بيانات أمنية حساسة، وقد تكون ذات قيمة تحقيقية أو قانونية؛ ولذلك فإن حمايتها تتطلب أكثر من منع فقدانها.

وتشمل الحماية:(24)

١. التحكم في الوصول: منع الوصول غير المصرح به.
٢. التشفير: حماية البيانات أثناء التخزين أو النقل عندما تقتضي المخاطر ذلك.
٣. التدقيق: تسجيل عمليات الوصول والتغيير والتصدير.
٤. النسخ الاحتياطي: الاحتفاظ بنسخ وفق سياسة واضحة.
٥. الحماية المادية: حماية البنية التخزينية من العبث أو السرقة.
٦. الاستعادة: اختبار إمكانية استعادة البيانات فعليًا.
٧. المزامنة الزمنية: ضمان دقة التوقيت المرتبط بالتسجيلات.

والأخيرة مهمة بصفة خاصة؛ إذ إن تسجيلًا ممتاز الجودة مع توقيت غير موثوق قد يضعف القدرة على إعادة بناء التسلسل الزمني للحادث.(25)

ثامنًا: التخزين الطرفي والتوزيع

لا يشـــترط أن تكون جميع التســـجيلات في مركز تخزين واحد. فقد تحتوي الكاميرا نفسها على تخزين محلي، أو يمكن توزيع التسجيلات على أكثر من عقدة. وتوفر هذه البنية مزايا في بعض السيناريوهات، مثل:(26)

١. الاستمرار المؤقت في التسجيل عند انقطاع الاتصال بالمركز.

٢. تقليل الاعتماد على الاتصال المستمر.

٣. توزيع الحمل.

٤. زيادة المرونة.

ويظهر ذلـك في مفهومEdge Storage ؛ حيـث يتيح ONVIF Profile G للأجهزة المتوافقة تســـجيل الفيديو على الجهاز نفســـه أو عبر الشـــبكة، مع إمكانات البحث والاسترجاع والتحكم في التسجيل.(27)

تاسعًا: معايير اختيار وسائط التخزين وفق المهمة الأمنية

ينبغي تقييم وسائط التخزين وفق منظومة من المعايير، أهمها:(28)

١. السعة المطلوبة.

٢. معدل الكتابة المستمر.

٣. سرعة القراءة والاسترجاع.

٤. الاعتمادية.

٥. تحمل الحمل التشغيلي.

٦. التكرار.

٧. قابلية التوسع.

٨. زمن الاستعادة.

٩. الأمن.

١٠. التكلفة الكلية للملكية.

وعليه فإن أفضل وسيط تخزين ليس بالضرورة الأعلى سعة أو الأقل تكلفة، وإنما الأكثر ملاءمة لمتطلبات المخاطر والتشغيل والاحتفاظ.

عاشرًا: حدود وسائط التخزين

من الأخطاء المنهجية النظر إلى وسائط التخزين باعتبارها قادرة على حل جميع مشكلات الحفظ. فكل وسيط تخزين محدود بسعته وسرعته واعتماديته.

فإذا كانت السعة غير كافية، فقد لا تُحفظ التسجيلات للفترة المطلوبة. وإذا كانت السرعة منخفضة، فقد يتأخر الاسترجاع. وإذا كانت الاعتمادية ضعيفة، فقد تفقد التسجيلات.(29)

كما أن وسائط التخزين لا تستطيع أن تعالج بمفردها مشكلة ضعف جودة الصورة الأصلية، أو مشكلة انقطاع الشبكة، أو مشكلة غياب الإجراءات التشغيلية. فوسائط التخزين حلقة في سلسلة أطول، ولا تعوض عن ضعف الحلقات الأخرى.

المراجع:

① ينظر: National Institute of Standards and Technology, *VQiPS: Storage – Guide to Defining Video Quality Requirements*, فيما يتعلق بأهمية التخزين الصحيح للحفاظ على القيمة التحقيقية للفيديو.

② راجع: ONVIF, *Profile V – Cloud Video Surveillance*, والمعلومات الرسمية المتعلقة بالنسخة المرشحة للإصدار وتطبيقات التسجيل السحابي.

③ راجع: R. Chandramouli and D. Pinhas, *Security Guidelines for Storage Infrastructure*, NIST Special Publication 800-209، فيما يتعلق بحماية البيانات والعزل والتشفير والاستعادة والنسخ الاحتياطي.

④ ينظر: ONVIF, *Profile G – Edge Storage and Retrieval*, فيما يتعلق بالتسجيل على الجهاز والتخزين الطرفي والبحث والاسترجاع.

⑤ راجع: International Electrotechnical Commission, *IEC 62676*, Clause 4. 5.

⑥ ينظر: David Brown, *Integrated Security Systems Design*, (New York: Butterworth-Heinemann, 3rd Edition, 2019), p. 267.

⑦ راجع: Michael Harris, *CCTV and Video Surveillance: Technology and Applications*, (Boston: McGraw-Hill, 4th Edition, 2020), p. 334.

⑧ ينظر: Robert Wilson, *Digital Video Processing for Security Systems*, (London: Springer, 2021), p. 267.

⑨ راجع: عبد الله بن حسن الشهري، *شبكات نقل الفيديو الأمني*، (الرياض: معهد الإدارة العامة، ١٤٤٤هـ/٢٠٢٣م)، ص ٨٩.

⑩ ينظر: Brown, *Integrated Security Systems Design*, p. 289.

⑪ راجع: Harris, *CCTV and Video Surveillance*, p. 345.

⑫ ينظر: الشهري، *شبكات نقل الفيديو الأمني*، ص ٩٠.

⑬ راجع: Wilson, *Digital Video Processing for Security Systems*, p. 278.

⑭ ينظر: Brown, *Integrated Security Systems Design*, p. 301.

⑮ راجع: وزارة الداخلية، *الدليل المهني لأنظمة المراقبة الأمنية*، (الرياض: الإدارة العامة للأمن، ٢٠٢١م)، ص ٩٠.

⑯ ينظر: International Electrotechnical Commission, *IEC 62676*, Clause 5. 8.

⑰ راجع: Wilson, *Digital Video Processing for Security Systems*, p. 289.

⑱ ينظر: Brown, *Integrated Security Systems Design*, p. 312.

⑲ راجع: Harris, *CCTV and Video Surveillance*, p. 367.

⑳ ينظر: Wilson, *Digital Video Processing for Security Systems*, p. 301.

㉑ راجع: الشهري، *شبكات نقل الفيديو الأمني*، ص ٩١ .

㉒ ينظر: Brown, *Integrated Security Systems Design*, p. 323.

㉓راجع. R. Chandramouli and D. Pinhas, *Security Guidelines for Storage Infrastructure*, NIST SP 800-209 :

㉔ينظر: وزارة الداخلية، *الدليل المهني لأنظمة المراقبة الأمنية*، ص ٩١ .

㉕راجع. Harris, *CCTV and Video Surveillance*, p. 378 :

㉖ينظر. ONVIF, *Profile G – Edge Storage and Retrieval* :

㉗راجع. ONVIF, *Profile G Specification* :

㉘ينظر. Brown, *Integrated Security Systems Design*, p. 345 :

㉙راجع. Harris, *CCTV and Video Surveillance*, p. 401 :

المبحث السادس: الشاشات ومراكز المراقبة

تمثل الشاشات ومراكز المراقبة المرحلة التي تنتقل فيها البيانات المسجلة أو الحية من كونها معلومات تقنية إلى معلومة قابلة للإدراك والتحليل واتخاذ القرار. ولذلك فإن نجاح منظومة المراقبة لا يعتمد على جودة الكاميرا والتسجيل والتخزين فقط، وإنما يعتمد كذلك على قدرة الإنسان على استيعاب المعلومات المعروضة والتعامل معها في الوقت المناسب.(1)

ومن هذا المنظور، فإن مركز المراقبة ليس مجرد غرفة تحتوي على مجموعة من الشاشات، وإنما هو بيئة تشغيلية تجمع الإنسان والتقنية والإجراءات والاتصالات بهدف الكشف والتحقق والتقييم والاستجابة. وتؤكد الممارسات الحديثة في الأمن المادي أهمية مراقبة الأحداث واستخدام الفيديو ضمن منظومة الاستجابة، لا باعتباره عنصرًا منفصلًا عن بقية إجراءات الأمن.(2)

أولًا: مفهوم مركز المراقبة

يمكن تعريف مركز المراقبة بأنه: بيئة تشغيلية مخصصة لاستقبال وعرض وتحليل معلومات المراقبة، وتمكين المشغلين من اكتشاف الأحداث والتحقق منها وتقييمها واتخاذ الإجراءات المناسبة أو تصعيدها إلى الجهات المختصة .(3)

وبذلك فإن المركز يتكون من أربعة عناصر مترابطة:(4)

١. التقنية: الشاشات، الخوادم، أنظمة الإدارة والاتصال.

٢. المعلومات: الفيديو والأحداث والتنبيهات والبيانات المرتبطة.

٣. العنصر البشري: المشغلون والمشرفون وصانعو القرار.

٤. الإجراءات: سياسات التشغيل والاستجابة والتصعيد والتوثيق.

وأي ضعف في أحد هذه العناصر قد ينعكس على أداء المركز بأكمله.

ثانيًا: الشاشات بوصفها واجهة تشغيلية

لا ينبغي اختيار شاشة المراقبة بناءً على الحجم والدقة فقط، وإنما ينبغي النظر إليها باعتبارها جزءًا من نظام العرض البصري. ومن أهم العوامل:(5)

١. الدقة.

٢. الحجم.
٣. السطوع.
٤. التباين.
٥. زاوية الرؤية.
٦. المسافة بين المشغل والشاشة.
٧. كثافة المعلومات المعروضة.
٨. زمن التشغيل اليومي.
٩. طبيعة المشاهد.
١٠. قابلية الإدارة والصيانة.

ويجب التمييز بين دقة الشاشة وجودة الفيديو الأصلي؛ فشاشة عالية الدقة لا تستطيع استعادة تفاصيل لم تلتقطها الكاميرا أو فُقدت أثناء المعالجة أو التسجيل.(6)

ثالثًا: أنماط العرض

يمكن استخدام عدة أنماط لعرض الفيديو، من أبرزها:(7)

1. العرض الفردي

عرض كاميرا واحدة بصورة كبيرة، ويستخدم عندما يتطلب الحدث تركيزًا بصريًا مرتفعًا (8).

2. العرض المتعدد

عرض مجموعة من الكاميرات في الوقت نفسه، وهو مناسب للمراقبة العامة.(9)

3. العرض القائم على الأحداث

تغيير ترتيب العرض أو إبراز كاميرا معينة عند ظهور حدث أو إنذار.(10)

4. جدار الفيديو(Video Wall)

يستخدم في مراكز العمليات التي تتطلب عرض عدد كبير من مصادر المعلومات أو إعطاء المشرفين صورة عامة عن الحالة.(11)

وهنا ينبغي التأكيد على أن زيادة عدد الصور المعروضة لا تعني زيادة قدرة المشغل على اكتشاف الأحداث؛ إذ إن كثافة المعلومات قد تتحول إلى عامل سلبي إذا تجاوزت قدرة الإنسان على المعالجة.(12)

رابعًا: تصميم مركز المراقبة

يجب أن يبدأ تصميم مركز المراقبة من تحليل الوظيفة وليس من المساحة المتاحة. ومن أهم أسئلة التصميم:(13)

١. كم عدد المشغلين؟
٢. كم عدد الكاميرات؟
٣. ما معدل الأحداث؟
٤. ما مستوى المخاطر؟
٥. هل المراقبة مستمرة؟
٦. ما زمن الاستجابة المطلوب؟
٧. ما الجهات التي يجب الاتصال بها؟
٨. ما مستوى السرية؟
٩. ما متطلبات استمرارية التشغيل؟

وبناء على ذلك يحدد:(14)

١. توزيع وحدات العمل.
٢. مواقع الشاشات.
٣. مسارات الحركة.
٤. الإضاءة.
٥. الضوضاء.
٦. التهوية والتبريد.
٧. الاتصالات.
٨. الطاقة الاحتياطية.
٩. التحكم في الدخول إلى المركز.

خامسًا: العامل البشري

يمثل المشغل عنصرًا محوريًا في سلسلة المراقبة. ولذلك لا يكفي أن تكون المنظومة قادرة تقنيًا على عرض مئات الكاميرات إذا كان المشـــغل غير قادر عمليًا على متابعتها بصورة فعالة. ومن أبرز العوامل البشرية: (15)

1. الانتباه

الانتباه المستمر لمجموعة كبيرة من المشاهد قد يكون صعبًا، خصوصًا عندما تكون الأحداث النادرة محاطة بفترات طويلة من الهدوء.(16)

2. الإرهاق

المراقبة الممتدة قد تؤدي إلى انخفاض اليقظة وارتفاع احتمال الخطأ.(17)

3. التدريب

يحتاج المشغل إلى تدريب تقني وتشغيلي، وليس مجرد معرفة كيفية تحريك الكاميرا أو فتح التسجيل.(18)

4. فهم إجراءات الاستجابة

يجب أن يعرف المشغل ماذا يفعل عند اكتشاف حدث، ومن يتصل به، ومتى يصعّد الحدث.(19)

5. إدارة الحمل المعرفي

ينبغي تصميم الواجهات والتنبيهات بما يقلل المعلومات غير الضرورية ويعطي الأولوية للمعلومات ذات القيمة الأمنية.(20)

سادسًا: مركز المراقبة كجزء من سلسلة الاستجابة

يمكن تصور دورة العمل داخل مركز المراقبة على النحو الآتي: (21)

كشف → تحقق → تقييم → تصنيف → استجابة → تصعيد عند الحاجة → توثيق → مراجعة

وهذه السلسلة مهمة لأنها تمنع الخلط بين اكتشاف حدث واتخاذ قرار أمني. فالكاميرا قد تكشف حركة، لكن المشغل يحتاج إلى التحقق من طبيعتها، ثم تحديد مستوى خطورتها، ثم اختيار الإجراء المناسب.(22)

ومن هنا تصبح قيمة مركز المراقبة في قدرته على تحويل البيانات إلى قرار قابل للتنفيذ.

سابعًا: التكامل مع أنظمة الأمن الأخرى

تزداد فاعلية مركز المراقبة عندما لا يعمل الفيديو بمعزل عن بقية الأنظمة. ومن صور التكامل: (23)

١. أنظمة التحكم في الدخول.
٢. أنظمة الإنذار.
٣. أنظمة كشف التسلل.
٤. أنظمة الاتصال.
٥. أنظمة إدارة الحوادث.
٦. الخرائط الرقمية.
٧. أنظمة إدارة المباني.

وعند وقوع حدث، يمكن للنظام عرض الكاميرا المرتبطة بالمنطقة أو الحدث بصورة تلقائية، مما يقلل زمن البحث ويزيد سرعة التحقق. كما أن المعايير المفتوحة مثل ONVIF تساعد على بناء بيئات أكثر قابلية للتكامل بين الأجهزة والعملاء المتوافقين (24).

ثامنًا: استمرارية تشغيل مركز المراقبة

يجب التعامل مع مركز المراقبة باعتباره مرفقًا أمنيًا قد يكون مطلوبًا منه العمل بصورة مستمرة. ولهذا ينبغي دراسة: (25)

١. التغذية الكهربائية الأساسية.
٢. UPS.
٣. المولدات عند الحاجة.
٤. التبريد.
٥. الاتصال البديل.
٦. استمرار التسجيل عند تعطل المركز.
٧. خطط الطوارئ.
٨. النسخ الاحتياطية.

٩. موقع بديل عند المنشآت ذات الحساسية العالية.

والهدف ليس فقط حماية الأجهزة، وإنما الحفاظ على القدرة التشـــغيلية للمركز أثناء الظروف غير الاعتيادية.

تاسعًا: أمن مركز المراقبة

يجب أن يكون مركز المراقبة نفســه محميًا، لأنه يحتوي على معلومات أمنية حســاســة وقد يتيح الوصول إلى أجزاء واسعة من المنظومة. ومن أهم الضوابط: (26)

١. التحكم في الدخول.

٢. تحديد صلاحيات العاملين.

٣. تسجيل الدخول والخروج.

٤. حماية أجهزة الإدارة.

٥. منع استخدام غير مصرح به للوسائط الخارجية.

٦. مراقبة التغييرات في إعدادات النظام.

٧. حماية الاتصالات.

٨. وضع إجراءات واضحة للتعامل مع الحوادث السيبرانية.

عاشرًا: معايير تقييم مركز المراقبة

يمكن تقييم المركز من خلال مجموعة من المؤشرات: (27)

١. زمن اكتشاف الحدث.

٢. زمن التحقق.

٣. زمن الاستجابة.

٤. نسبة الإنذارات الكاذبة.

٥. قدرة المشغلين على استرجاع التسجيلات.

٦. استمرارية الخدمة.

٧. وضوح إجراءات التصعيد.

٨. جودة التدريب.

٩. مستوى أمن المركز.

١٠. قابلية التوسع.

١١. جودة بيئة العمل.

١٢. مدى تكامل المركز مع منظومة الأمن العامة.

وهذا يغير طريقة تقييم المركز من سؤال" :كم شاشة لدينا؟ "إلى سؤال أكثر أهمية" :ما قدرة المركز على تحويل المعلومات المرئية إلى استجابة أمنية فعالة؟.(28) "

حادي عشـــر: حدود مركز المراقبة : من الأخطاء المنهجية النظر إلى مركز المراقبة باعتباره قادرًا على حل جميع مشـكلات المتابعة والاسـتجابة. فكل مركز محدود بعدد المشغلين وعدد الشاشات وساعات العمل.

فإذا كان عدد المشـــغلين غير كافٍ، فقد لا يتمكنوا من متابعة جميع الأحداث. وإذا كان عدد الشـاشـات كبيرًا، فقد يشـتت انتباه المشـغلين. وإذا كانت سـاعات العمل طويلة، فقد يزيد الإرهاق وتقل الكفاءة.(29)

كما أن مركز المراقبة لا يسـتطيع أن يعالج بمفرده مشـكلة ضـعف جودة الصـورة، أو مشـكلة انقطاع الشـبكة، أو مشـكلة غياب الإجراءات التشـغيلية. فمركز المراقبة حلقة في سلسلة أطول، ولا يعوض عن ضعف الحلقات الأخرى.

المراجع:

①ينظر National Institute of Standards and Technology, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, NIST SP 800-171 Rev. 3 : فيما يتعلق بمراقبة الوصـول المادي واسـتخدام أنظمة المراقبة بالفيديو ضـمن منظومة الأمن المادي.

②راجع ONVIF, *ONVIF Profiles*: فيما يتعلق بالتوافق بين الأجهزة والعملاء في أنظمة الأمن المادي القائمة على الشبكات.

③ينظر David Brown, *Integrated Security Systems Design*, (New York: Butterworth-Heinemann, 3rd Edition, 2019), p. 356.

④راجع Michael Harris, *CCTV and Video Surveillance: Technology and Applications*, (Boston: McGraw-Hill, 4th Edition, 2020), p. 401.

⑤ينظر: وزارة الداخلية، *الدليل المهني لأنظمة المراقبة الأمنية*، (الرياض: الإدارة العامة للأمن، ٢٠٢١م)، ص ٩٣ .

⑥راجع Robert Wilson, *Digital Video Processing for Security Systems*, (London: Springer, 2021), p. 323.

⑦ينظر Harris, *CCTV and Video Surveillance*, p. 412.

⑧راجع Brown, *Integrated Security Systems Design*, p. 367.

⑨ينظر Wilson, *Digital Video Processing for Security Systems*, p. 334.

⑩راجع: وزارة الداخلية، *الدليل المهني لأنظمة المراقبة الأمنية*، ص ٩٤ .

⑪ينظر Harris, *CCTV and Video Surveillance*, p. 423.

⑫راجع Brown, *Integrated Security Systems Design*, p. 378.

⑬ينظر Wilson, *Digital Video Processing for Security Systems*, p. 345.

⑭راجع: Harris, *CCTV and Video Surveillance*, p. 434.

⑮ينظر: Brown, *Integrated Security Systems Design*, p. 389.

⑯راجع: Wilson, *Digital Video Processing for Security Systems*, p. 356.

⑰ينظر: Harris, *CCTV and Video Surveillance*, p. 445.

⑱راجع: Brown, *Integrated Security Systems Design*, p. 401.

⑲ينظر: وزارة الداخلية، *الدليل المهني لأنظمة المراقبة الأمنية*، ص ٩٥ .

⑳راجع: International Electrotechnical Commission, *IEC 62676*, Clause 5. 9.

㉑ينظر: Harris, *CCTV and Video Surveillance*, p. 456.

㉒راجع: Brown, *Integrated Security Systems Design*, p. 412.

㉓ينظر: Wilson, *Digital Video Processing for Security Systems*, p. 367.

㉔راجع: Harris, *CCTV and Video Surveillance*, p. 467.

㉕ينظر: وزارة الداخلية، *الدليل المهني لأنظمة المراقبة الأمنية*، ص ٩٦ .

㉖راجع: Brown, *Integrated Security Systems Design*, p. 423.

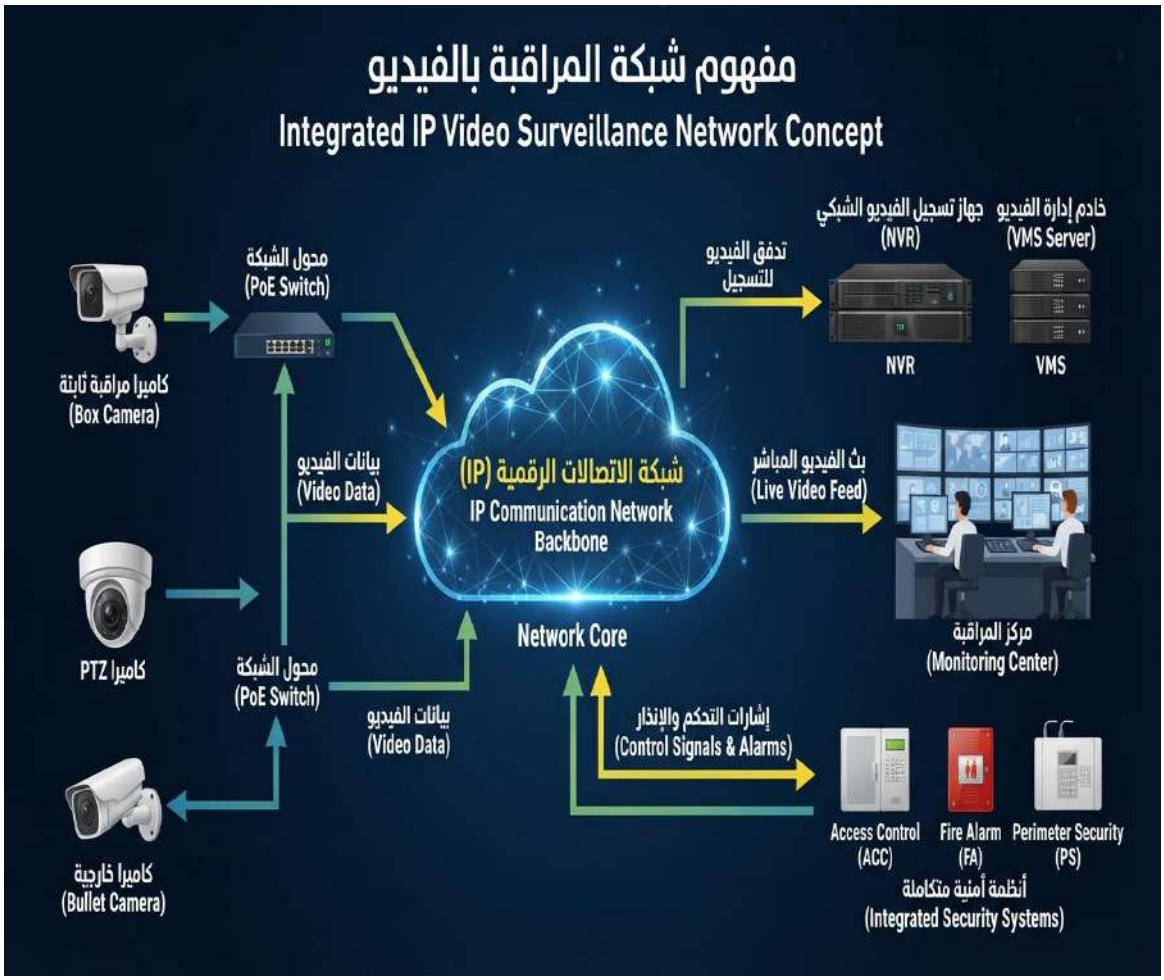
㉗ينظر: Harris, *CCTV and Video Surveillance*, p. 478.

㉘راجع: Wilson, *Digital Video Processing for Security Systems*, p. 378.

㉙ينظر: Brown, *Integrated Security Systems Design*, p. 467.

المبحث السابع: الشبكات والاتصالات

لم تعد منظومة المراقبة بالفيديو الحديثة تتكون من كاميرات تعمل بصورة مستقلة، وإنما أصبحت نظامًا مترابطًا تتبادل مكوناته تدفقات الفيديو والبيانات والأحداث وأوامر التحكم عبر بنية اتصالات مادية ومنطقية متكاملة. ومن ثم أصبحت الشبكة، في الأنظمة القائمة على بروتوكولات الاتصال الحديثة، أحد المكونات الجوهرية التي يتوقف عليها الأداء الفعلي للمنظومة، واستمراريتها، وقابليتها للتوسع، وقدرتها على التكامل مع أنظمة الأمن الأخرى.(1)



وتتعامل المواصفة الدولية IEC 62676-4:2025 مع منظومة المراقبة باعتبارها نظامًا يضم أجهزة التقاط الصورة، ووسائل الربط، وأجهزة معالجة الصورة والتعامل معها، ضمن دورة حياة تبدأ بالتخطيط والتصميم وتمتد إلى التركيب والاختبار والتشغيل

والصيانة؛ الأمر الذي يعزز النظر إلى الاتصال باعتباره جزءًا بنيويًا من تصميم المنظومة وليس مجرد وسيلة لنقل الإشارة.(2)

ومن المنظور الأمني، فإن جودة الكاميرا أو جهاز التسجيل لا تكفي وحدها لضمان فاعلية النظام؛ إذ يمكن أن يؤدي ازدحام الشبكة، أو فقد الحزم، أو التأخير، أو ضعف عرض النطاق، أو انقطاع مسار الاتصال إلى فقد جزء من المعلومات المرئية أو تأخر وصولها إلى الجهة المكلفة بالمراقبة والاستجابة.(3)

أولًا: مفهوم شبكة المراقبة بالفيديو

يمكن تعريف شبكة المراقبة بالفيديو بأنها :البنية الاتصالية التي تربط مكونات منظومة المراقبة، وتوفر وسائل نقل الفيديو والبيانات والأحداث وأوامر التحكم بين الكاميرات وأجهزة التسجيل ومنصات إدارة الفيديو ومراكز المراقبة والأنظمة الأمنية المتكاملة .(4)

ويتميز هذا النوع من الشبكات عن الشبكات الحاسوبية العامة في أن تصميمه ينبغي أن يراعي طبيعة تدفقات الفيديو، التي قد تتسم بارتفاع حجم البيانات واستمرارية النقل والحاجة إلى استقرار الاتصال وزمن استجابة مناسب.

وفي منظومات IP يمكن أن تعمل الكاميرات باعتبارها أجهزة طرفية شبكية تنتج تدفقات الفيديو والبيانات، بينما تتولى أجهزة التسجيل ومنصات إدارة الفيديو استقبال تلك التدفقات وإدارتها وتسجيلها وإتاحتها للمستخدمين.

ثانيًا: البنية الوظيفية لشبكة المراقبة

يمكن النظر إلى الشبكة من الناحية الوظيفية من خلال ثلاث طبقات مترابطة:(5)

١. طبقة الوصول :وتشمل الكاميرات والأجهزة الطرفية التي تتصل بالشبكة.

٢. طبقة النقل والتوزيع :وتشمل المحولات ووسائل الربط والبنية التي تنقل تدفقات الفيديو والبيانات.

٣. طبقة الإدارة والخدمات :وتشمل منصات VMS وأجهزة التسجيل والخوادم ومراكز المراقبة والأنظمة المتكاملة.

ولا ينبغي النظر إلى هذه الطبقات باعتبارها منفصلة تمامًا؛ فالقرار المتعلق بإحدى الطبقات يؤثر في أداء الطبقات الأخرى، مثل تأثير عدد الكاميرات ودقة الفيديو في متطلبات المحولات والروابط وسعة الخوادم والتخزين.

ثالثًا: مكونات شبكة المراقبة

تتكون شبكة المراقبة الحديثة من عدد من العناصر الرئيسة، من أهمها: (6)

1. الكاميرات الشبكية

وهي المصـدر الرئيس لتدفقات الفيديو والبيانات، وقد تتضـمن قدرات معالجة وتحليل محلية.

2. المحولات الشبكية

تربط الأجهزة داخل الشـبكة، وتوزع حركة البيانات، وقد توفر الطاقة للأجهزة المتوافقة باستخدام PoE.

3. الموجهات

تربط الشبكات المختلفة وتتيح الاتصال بين المواقع أو النطاقات الشبكية.

4. الألياف الضوئية

تستخدم بصورة واسعة في الربط بين المواقع والمسافات الطويلة والروابط ذات السعة المرتفعة.

5. كابلات Ethernet

تستخدم في مستويات الوصول بحسب المسافة والسرعة والبيئة ومتطلبات الطاقة.

6. الروابط اللاسلكية

يمكن استخدامها في المواقع التي يصعب فيها تنفيذ البنية السلكية، مع ضرورة تقييم الاعتمادية والتداخل والأمن.

7. جدران الحماية ومكونات الحماية الشبكية

تتحكم في الاتصالات بين النطاقات وتحد من الاتصالات غير المصرح بها.

رابعًا: أنماط الاتصال في منظومات المراقبة

يمكن تصنيف وسائل الاتصال المستخدمة في منظومات المراقبة إلى: (7)

أ. الاتصال السلكي

يمثل الخيار الأكثر شـيوعًا في المنشـآت الثابتة، ويتميز بالاسـتقرار النسـبي وإمكانية التحكم في البنية الاتصالية بصورة أفضل.

ب. الاتصال بالألياف الضوئية

يستخدم بصورة خاصة في الربط بين المباني أو المسافات التي تتطلب سعة عالية أو مقاومة أكبر للتداخل.

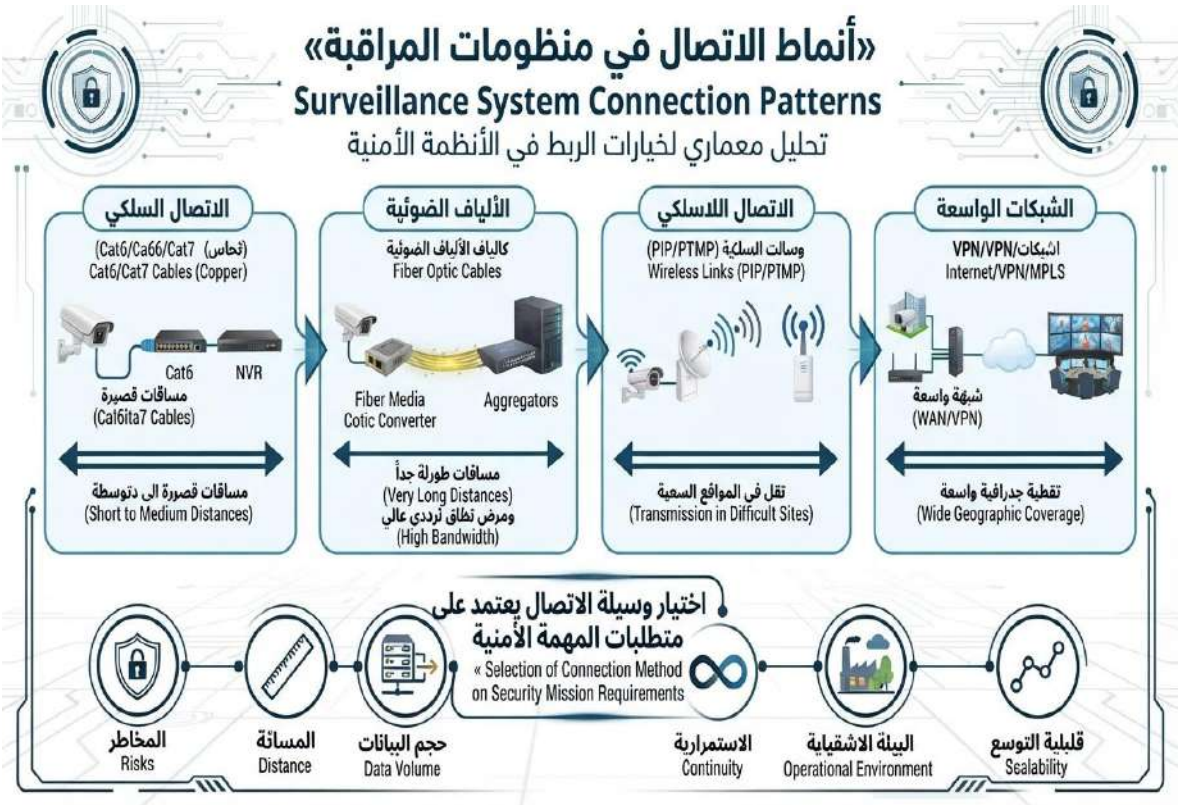
ج. الاتصال اللاسلكي

يمكن أن يكون مناسبًا لبعض المواقع أو التطبيقات المؤقتة أو الأماكن التي يصعب فيها تنفيذ البنية التحتية السلكية.

د. الاتصال عبر الشبكات الواسعة

يستخدم عند توزيع الكاميرات ومراكز المراقبة على مواقع متعددة، ويحتاج إلى دراسة دقيقة لعرض النطاق والتأخير والاعتمادية والحماية.

ولا ينبغي اختيار وسيلة الاتصال بناءً على التكلفة أو سهولة التركيب فقط، وإنما ينبغي أن يستند القرار إلى تحليل المخاطر، والمسافة، وحجم البيانات، والاستمرارية المطلوبة، والبيئة التشغيلية، وقابلية التوسع.



خامسًا: بروتوكولات نقل الفيديو والتشغيل البيني

تحتاج المنظومة الشـبكية إلى بروتوكولات تنظم نقل الفيديو والبيانات وإدارة الأجهزة. ومن أبرز بروتوكولات نقل الفيديو المستخدمة في البيئات الشبكيةRTSP ، إلى جانب آليات النقل المرتبطة به مثلRTP ، وفق البنية التي يعتمدها النظام.(8)

ويجب التمييز بين بروتوكول النقل ومعيار التشـغيل البيني؛ فوجود بروتوكول مشـترك لا يعني بالضرورة أن جميع وظائف جهاز معين ستعمل بصورة متكاملة مع كل منصة.

وتوفر ONVIF Profiles إطارًا محددًا للتوافق بين الأجهزة والعملاء؛ إذ يحدد كل Profileمجموعة من الوظائف التي ينبغي دعمها لتحقيق التوافق. وتوضح ONVIF أن مجرد إعلان المنتج دعمه لـــ ONVIFلا يكفي لإثبات التوافق الكامل؛ وإنما ينبغي التحقق من Profile المحدد الذي يتوافق معه الجهاز أو العميل.(9)

ويكتسب Profile Tأهمية خاصة في الأنظمة الحديثة، إذ يدعم H.264 وH.265، وإعدادات الصورة، وأحداث الحركة والعبث، وتدفق البيانات الوصفية، إلى جانب وظائف أخرى للبث والتكامل.(10)

كما يدعم Profile Gوظائف مرتبطة بالتسجيل والتخزين والاسترجاع، بما في ذلك التحكم في التسجيل واسترجاع البيانات المسجلة.(11)

أما Profile Mفيرتبط بصورة أساسية بالبيانات الوصفية والأحداث الناتجة عن التحليلات، وهو ما يجعله ذا أهمية في التكامل بين التحليلات ومنصات إدارة الفيديو والأنظمة الأخرى.(12)

ومن التطورات المهمة التي ينبغي أن يراعيها الباحث عند تناول التشـغيل البيني أن ONVIFأعلنت في أكتوبر ٢٠٢٥ إنهاء دعم Profile Sوالتوصية بالانتقال إلى Profile T، على أن ينتهي دعم Profile S في ٣١ مارس ٢٠٢٧. ويرتبط هذا التوجه باعتبارات أمنية تتعلق بآلية المصادقة التي يعتمدها.(13) Profile S

سادسًا: عرض النطاق وتأثيره في الأداء الأمني

يمثل عرض النطاق أحد أهم عناصر تصميم الشبكة، ويتأثر بالعديد من المتغيرات، أهمها:(14)

١. عدد الكاميرات.
٢. دقة الفيديو.
٣. معدل الإطارات.
٤. معدل البت.
٥. نوع الضغط.
٦. طبيعة المشهد.
٧. عدد التدفقات.
٨. نمط التسجيل.
٩. عدد المستخدمين أو الأنظمة التي تستقبل التدفقات.

وعليه، فإن تقدير متطلبات الشبكة لا يمكن أن يعتمد على عدد الكاميرات وحده. فقد تتطلب مجموعة صغيرة من الكاميرات عالية الدقة ومعدلات البت المرتفعة قدرة شبكية أكبر من مجموعة أكبر من الكاميرات ذات الإعدادات الأقل استهلاكًا للبيانات. كما ينبغي ألا يصمم النظام عند الحد النظري للسعة، بل ينبغي توفير هامش تشغيلي يسمح بالتغيرات في الحمل والتوسع المستقبلي.(15)

سابعًا: الاعتمادية واستمرارية الاتصال

تكتسب الاعتمادية أهمية خاصة في المنشآت التي تعتمد على المراقبة بوصفها وظيفة أمنية مستمرة. ومن وسائل تعزيز الاعتمادية:(16)

- ازدواجية مسارات الاتصال عند الحاجة.
- استخدام معدات ذات موثوقية مناسبة.
- توفير مصادر طاقة احتياطية.
- مراقبة حالة الروابط والأجهزة.
- إصدار تنبيهات عند فقد الاتصال.
- اختبار سيناريوهات الفشل والاستعادة.
- تحديد نقاط الفشل المفردة.

وتؤكد إرشادات NIST الخاصة بأمن تقنيات التشغيل أهمية التجزئة والعزل الشبكيين لتنظيم الأجهزة بحسب الوظيفة أو الموقع، والتحكم في الاتصالات المسموح بها بين القطاعات المختلفة.(17)

ثامنًا: أمن شبكة المراقبة

تمثل شبكة المراقبة أحد مكونات البنية الأمنية التي ينبغي حمايتها من التهديدات السيبرانية، لأن اختراقها قد يؤدي إلى تعطيل الرؤية، أو الوصول غير المصرح به إلى التسجيلات، أو التأثير في إعدادات الأجهزة.(18)

ومن أهم الممارسات:

١. تغيير بيانات الدخول الافتراضية.
٢. استخدام حسابات فردية.
٣. تطبيق الصلاحيات المبنية على الأدوار.
٤. تحديث البرمجيات والبرامج الثابتة.
٥. استخدام التشفير عند ملاءمته.
٦. تجزئة الشبكة.
٧. تعطيل الخدمات غير الضرورية.
٨. مراقبة السجلات.
٩. حماية الوصول عن بعد.
١٠. توثيق التغييرات الإدارية.

ولا ينبغي أن تكون هذه الإجراءات مرحلة لاحقة، بل يجب دمجها منذ مرحلة التصميم.(19)

تاسعًا: الشبكة ضمن التصميم الأمني

ينبغي ألا تصمم الشبكة بعد الانتهاء من تحديد الكاميرات، لأن عدد الكاميرات ودقتها ومواقعها وأسلوب تشغيلها تؤثر بصورة مباشرة في الشبكة والتسجيل والتخزين (20).

ومن ثم يمكن تمثيل عملية التصميم في سلسلة مترابطة:

الخطر ← الهدف الأمني ← المشهد المطلوب ← الكاميرا ← التدفق ← الشبكة ← التسجيل ← التحليل ← الاستجابة

وهذه السلسلة تؤكد أن الشبكة ليست قرارًا هندسيًا مستقلًا، وإنما نتيجة مباشرة لمتطلبات الوظيفة الأمنية.

المراجع:

① ينظر: International Electrotechnical Commission, *IEC 62676-4: Video surveillance systems for use in security applications – Part 4: Application guidelines*, (Geneva: IEC, 2nd ed., 2025).

② راجع: International Electrotechnical Commission, *IEC 62676-1-1: Video surveillance systems for use in security applications – Part 1-1: System requirements – General*, (Geneva: IEC, 2013).

③ ينظر: National Institute of Standards and Technology, *Guide to Operational Technology (OT) Security*, NIST SP 800-82 Rev. 3, (Gaithersburg, MD: NIST, 2023).

④ راجع: ONVIF, *ONVIF Profiles*, (San Ramon: ONVIF).

⑤ ينظر: IEC 62676-4:2025, sections on network design and infrastructure.

⑥ راجع: IEC 62676-4:2025, sections on network components.

⑦ ينظر: IEC 62676-4:2025, sections on transmission methods.

⑧ راجع: ONVIF, *Profile T Specification*, (San Ramon: ONVIF), section 7.9.

⑨ ينظر: ONVIF, *ONVIF Profiles*, official profile-conformance guidance.

⑩ راجع: ONVIF, *Profile T – Advanced Video Streaming*, (San Ramon: ONVIF).

⑪ ينظر: ONVIF, *Profile G – Edge Storage and Retrieval*, (San Ramon: ONVIF).

⑫ راجع: ONVIF, *Profile M – Metadata and Events for Analytics Applications*, (San Ramon: ONVIF).

⑬ ينظر: ONVIF, *Profile S Deprecation Q&A*, (San Ramon: ONVIF).

⑭ راجع: IEC 62676-4:2025, sections on bandwidth calculation.

⑮ ينظر: NIST SP 800-82 Rev. 3, Section on Network Segmentation and Isolation.

⑯ راجع: NIST SP 800-82 Rev. 3, sections on reliability and redundancy.

⑰ ينظر: NIST SP 800-82 Rev. 3, Section on Network Segmentation and Isolation.

⑱ راجع: National Institute of Standards and Technology, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*, NISTIR 8228, (Gaithersburg, MD: NIST, 2019).

⑲ ينظر: ONVIF, *ONVIF to End Support for Profile S; Recommends Profile T as Replacement*, (San Ramon: ONVIF, 2025).

⑳ راجع: IEC 62676-4:2025, sections on design process.

المبحث الثامن: أنظمة الطاقة

إذا كانت الشبكة تمثل المسار الذي تنتقل عبره المعلومات داخل منظومة المراقبة، فإن الطاقة تمثل الشـــرط التشـــغيلي الذي يســـمح لجميع مكونات النظام بأداء وظائفها. فالكاميرات، والمحولات، وأجهزة التســـجيل، والخوادم، والشـــاشـــات، ووحدات التخزين، ومعدات الاتصـــال تحتاج إلى مصـــدر طاقة مناســـب ومســـتقر ومســـتمر وفق مستوى الاعتمادية المطلوب.(1)

ومن ثم فإن الطاقة لا ينبغي أن تعامل بوصـفها مسـألة كهربائية منفصـلة عن التصـميم الأمني؛ إذ إن انقطاعها قد يؤدي إلى فقدان الصـــورة أو التســـجيل أو الاتصـــال، وقد يحدث ذلك في الوقت الذي تكون فيه الوظيفة الأمنية أكثر أهمية.

وتندرج متطلبات الطاقة ضمن دورة التخطيط والتصميم والتركيب والاختبار والصيانة التي تتناولها IEC 62676-4:2025 لمنظومات المراقبة.(2)

أولًا: الطاقة والاستمرارية الأمنية

تقوم قيمة منظومة المراقبة على قدرتها على أداء وظيفتها عند الحاجة إليها. ولذلك فإن فقدان الطاقة يمثل خطرًا تشغيليًا ينبغي إدخاله في تحليل المخاطر.(3)

ولا يعني مفهوم الاستمرارية أن تعمل جميع مكونات النظام إلى أجل غير محدود، بل يعني تحديد مستوى الاستمرارية المطلوب بناءً على أهمية الموقع وطبيعة الخطر وزمن الاستجابة المقبول.

ثانيًا: مصادر الطاقة

يمكن أن تعتمد المنظومة على:(4)

- مصدر كهربائي رئيسي.
- مزودات طاقة مخصصة.
- Power over Ethernet (PoE).
- وحدات UPS.
- البطاريات.
- المولدات الاحتياطية.
- الطاقة الشمسية في المواقع المناسبة.

ويختلف دور كل مصدر بحسب الحمل والمدة المطلوبة للاستقلالية وطبيعة الموقع.

ثالثًا: التغذية عبر الشبكةPoE

تتيح تقنية PoE نقل البيانات والطاقة عبر كابل الشبكة إلى الأجهزة المتوافقة، مما يسهل تركيب كاميرات IP ويقلل عدد التوصيلات المطلوبة.(5)

غير أن استخدام PoE ينبغي أن يستند إلى ميزانية الطاقة للمحول والشبكة، وليس إلى عدد المنافذ فقط؛ إذ يجب حساب مجموع الأحمال المتصلة والقدرة المتاحة والاحتياطي التشغيلي.

رابعًا: وحداتUPS

توفر UPS طاقة احتياطية مؤقتة عند انقطاع المصدر الرئيسي، وتساعد على منع التوقف الفوري للمكونات الحرجة.(6)

ويجب اختيارها بعد تحديد:

١. الحمل الفعلي.
٢. الأحمال التي يجب استمرارها.
٣. زمن الاستقلالية المطلوب.
٤. قدرة البطاريات.
٥. ظروف التشغيل.
٦. إمكانية التوسع.

ومن ثم قد تعطى الأولوية في بعض المنشآت للكاميرات الأساسية، ثم الشبكة، ثم التسجيل، ثم الخوادم الحرجة، ثم مكونات مركز المراقبة وفق تحليل المخاطر.

خامسًا: حساب الأحمال

ينبغي أن يشمل الحساب جميع الأحمال وليس الكاميرات فقط، بما في ذلك المحولات والخوادم وأجهزة التسجيل والشاشات وغيرها.(7)

كما ينبغي إدراج هامش مناسب للتوسع والتغيرات المستقبلية، بحيث لا يكون النظام مصممًا عند حدوده التشغيلية مباشرة.

سادسًا: اضطرابات الطاقة

لا يقتصر خطر الطاقة على الانقطاع الكامل، بل قد يشمل:(8)

- ارتفاع الأحمال.اضطرابات الجهد.ضعف البطاريات.ارتفاع درجات الحرارة.سوء توزيع الأحمال.أعطال مزودات الطاقة.

ومن ثم فإن الصيانة الدورية والفحص المستمر لمكونات الطاقة يمثلان جزءًا من إدارة المنظومة.

سابعًا: التكرار والطاقة الاحتياطية

في المنشآت الحساسة قد يستلزم تحليل المخاطر توفير أكثر من مسار أو مصدر للطاقة لبعض المكونات الحرجة.(9)

والهدف من التكرار ليس مجرد وجود جهاز احتياطي، وإنما تقليل احتمال أن يؤدي فشل نقطة واحدة إلى توقف الوظيفة الأمنية بأكملها.

ثامنًا: المواقع النائية

تواجه المواقع النائية تحديات خاصة عندما تكون شبكة الكهرباء غير متاحة أو غير مستقرة.(10)

وقد تكون الطاقة الشمسية والبطاريات مناسبة في بعض الحالات، إلا أن ملاءمتها تعتمد على:

- الحمل.الظروف المناخية.مدة الاستقلالية.سعة التخزين.ظروف الموقع.متطلبات الصيانة.

ولهذا ينبغي التعامل معها كحل هندسي خاص بالموقع، وليس كخيار عام.

تاسعًا: المراقبة الذاتية للطاقة

يمكن للمنظومات المتقدمة مراقبة حالة مصادر الطاقة والأجهزة ذات العلاقة، بما في ذلك حالة البطاريات ومزودات الطاقة وبعض مؤشرات الفشل.(11)

وتدعم هذه المراقبة مفهوم الصيانة الاستباقية، لأنها تساعد على اكتشاف مؤشرات الخلل قبل أن تتحول إلى انقطاع فعلي.

المراجع:

①ينظر.(International Electrotechnical Commission, *IEC 62676-4:2025*, (Geneva: IEC, 2025)
②راجع.(International Electrotechnical Commission, *IEC 62676-1-1*, (Geneva: IEC, 2013)
③ينظر National Institute of Standards and Technology, *Guide to Operational Technology (OT) Security*, NIST SP 800-82 Rev. 3, (Gaithersburg, MD: NIST, 2023).
④راجع.IEC 62676-4:2025, sections on power supply
⑤ينظر.(ONVIF, *Profile T – Advanced Video Streaming*, (San Ramon: ONVIF)
⑥راجع.(ONVIF, *ONVIF Profiles*, (San Ramon: ONVIF)
⑦ينظر.NIST SP 800-82 Rev. 3, sections on power and reliability
⑧راجع.IEC 62676-4:2025, sections on power disturbances
⑨ينظر.NIST SP 800-82 Rev. 3, sections on redundancy
⑩راجع.IEC 62676-4:2025, sections on remote sites
⑪ينظر.NIST SP 800-82 Rev. 3, sections on monitoring and maintenance

المبحث التاسع: البرمجيات والتحكم

إذا كانت الكاميرات تمثل حاسة الالتقاط، والشبكة تمثل مسار الاتصال، والتسجيل والتخزين يمثلان ذاكرة المنظومة، فإن البرمجيات تمثل طبقة الإدارة والتحكم التي تنظم هذه المكونات وتحول البيانات المرئية والأحداث إلى معلومات قابلة للمشاهدة والبحث والتحليل والاستجابة.(1)

وقد تطورت برمجيات المراقبة من مجرد أدوات لعرض الفيديو وتسجيله إلى منصات متقدمة لإدارة الأجهزة والأحداث والمستخدمين والتحليلات والبيانات الوصفية والتكامل مع الأنظمة الأمنية الأخرى.

أولًا: مفهوم نظام إدارة الفيديوVMS

يمكن تعريف VMS بأنه: منصة برمجية تتولى إدارة أجهزة الفيديو وتدفقات الصور، وتنظيم التسجيل والعرض والاسترجاع والأحداث والمستخدمين، وقد تتضمن وظائف تحليلية وتكاملية بحسب تصميمها وإمكاناتها .(2)

ويختلف VMS عنNVR ؛ فالأول يمثل أساسًا طبقة برمجية لإدارة النظام، بينما يكون NVRعادة جهازًا مخصصًا يجمع وظائف التسجيل والإدارة في منصة محددة.

ثانيًا: الوظائف الأساسية للبرمجيات

تشمل وظائف VMS (3):

- إدارة الكاميرات.
- العرض المباشر.
- إدارة التسجيل.
- البحث والاسترجاع.
- إدارة الأحداث والإنذارات.
- إدارة المستخدمين والصلاحيات.
- السجلات والتدقيق.
- التكامل مع الأنظمة الأخرى.

ثالثًا: الإدارة القائمة على الأحداث

أصبحت الإدارة الحديثة تميل من نموذج المراقبة البشرية المستمرة لجميع الشاشات إلى نموذج المراقبة القائمة على الأحداث.(4)

فبدل أن يراقب المشغل عشرات المشاهد بصورة مستمرة، يمكن للمنظومة أن تستقبل حدثًا، وتحدد الكاميرا المرتبطة به، وتعرض المشهد، وتوجه التنبيه إلى المشغل.

وقد تشمل الأحداث:

- الحركة.
- عبور خط افتراضي.
- دخول منطقة.
- العبث بالكاميرا.
- اكتشاف الأشخاص أو المركبات.
- أحداث التحليلات.
- حالات مرتبطة بالأنظمة الأخرى.

وتتيح ONVIF Profile M إطارًا للتعامل مع البيانات الوصفية والأحداث المتعلقة بالتحليلات، بما في ذلك معلومات تصنيف الأجسام وبعض الاستخدامات التحليلية المتقدمة.(5)

ومع ذلك، لا ينبغي الخلط بين وجود وظيفة تحليلية وبين دقة نتائجها؛ فالأداء يتأثر بالتصميم والمشهد والإضاءة وزاوية التصوير والخوارزمية والإعدادات.

رابعًا: إدارة المستخدمين والصلاحيات

يجب أن تحدد البرمجيات بدقة من يستطيع:(6)

- مشاهدة الكاميرات.
- مشاهدة التسجيلات.
- تصدير المقاطع.
- تغيير إعدادات الأجهزة.
- إضافة المستخدمين.
- تعديل الصلاحيات.

- إدارة النظام.

ويستند التصميم الجيد إلى مبدأ أقل صلاحية لازمة.

خامسًا: السجلات والتدقيق

لا تكفي حماية الفيديو، بل يجب أيضًا حماية سجل التعامل معه. وينبغي أن يسجل النظام، وفق قدراته وتصميمه، عمليات مثل:(7)

- تسجيل الدخول.
- تغيير الإعدادات.
- تصدير التسجيلات.
- إنشاء المستخدمين.
- تعديل الصلاحيات.
- الإجراءات الإدارية.
- الأحداث الأمنية.

وتوفر هذه السجلات قيمة مهمة في التحقيق والمساءلة.

سادسًا: الأمن السيبراني للبرمجيات

يمثل VMS نقطة مركزية في المنظومة، ولذلك فإن اختراقه قد يتيح الوصول إلى نطاق واسع من الكاميرات والتسجيلات والوظائف.(8)

ومن أهم متطلبات الحماية:

- المصادقة القوية.
- إدارة الهوية.
- الصلاحيات المبنية على الأدوار.
- التحديثات الأمنية.
- حماية واجهات الإدارة.
- التشفير المناسب.
- النسخ الاحتياطي للإعدادات.
- مراقبة السجلات.

- حماية الوصول عن بعد.

سابعًا: قابلية التكامل

يمكن أن تتكامل منصة إدارة الفيديو مع:(9)

- أنظمة التحكم في الدخول.
- أنظمة الإنذار.
- أنظمة كشف التسلل.
- أنظمة إدارة المباني.
- أنظمة إدارة الأمن المادي.
- أنظمة التحليل.
- منصات إنترنت الأشياء.

وتبرز هنا أهمية المعايير المفتوحة مثل ONVIF في تنظيم التوافق بين الأجهزة والعملاء والبيانات والأحداث.

ثامنًا: معايير اختيارVMS

ينبغي أن يشمل التقييم:(10)

- عدد الكاميرات.
- عدد المستخدمين.
- قدرات التسجيل.
- إمكانات البحث.
- إدارة الأحداث.
- التحليلات.
- الصلاحيات.
- التدقيق.
- الأمن السيبراني.
- قابلية التوسع.
- الاعتمادية.

- التكلفة الكلية للملكية.

ومن الخطأ اختيار المنصة بناءً على عدد القنوات فقط.

تاسعًا: دورة حياة البرمجيات

ينبغي النظر إلى البرمجيات ضمن دورة حياة:(11)

التخطيط ← الاختيار ← الاختبار ← التشغيل ← التحديث ← المراقبة ← الصيانة ← الترقية ← الاستبدال

وبالتالي فإن اختيار VMS قرار طويل الأجل يؤثر في التوافق والتدريب والتكلفة والأمن السيبراني.

عاشرًا: البرمجيات ودعم القرار الأمني

لا تكمن قيمة البرمجيات في كثرة وظائفها فقط، وإنما في قدرتها على:(12)

تنظيم المعلومات ← اكتشـــاف الحدث ← ترتيب الأولوية ← عرض الأدلة ← دعم القرار ← توثيق الاستجابة

ومن ثم فإن VMS يمثل حلقة مهمة بين البيانات المرئية والعمل الأمني.

المراجع:

①ينظر. International Electrotechnical Commission, *IEC 62676-4:2025*, (Geneva: IEC, 2025) :

②راجع. ONVIF, *ONVIF Profiles*, (San Ramon: ONVIF) :

③ينظر. ONVIF, *Profile T – Advanced Video Streaming*, (San Ramon: ONVIF) :

④راجع. ONVIF, *Profile M – Metadata and Events for Analytics Applications*, (San Ramon: ONVIF) :

⑤ينظر National Institute of Standards and Technology, *Guide to Operational Technology (OT) Security*, NIST SP 800-82 Rev. 3, (Gaithersburg, MD: NIST, 2023) :

⑥راجع. NIST SP 800-82 Rev. 3, sections on access control :

⑦ينظر. NIST SP 800-82 Rev. 3, sections on audit and logging :

⑧راجع. ONVIF, *Profile M*, concerning MQTT integration :

⑨ينظر. ONVIF, *ONVIF Profiles*, (San Ramon: ONVIF) :

⑩راجع. IEC 62676-4:2025, sections on VMS selection :

⑪ينظر. IEC 62676-4:2025, sections on system lifecycle :

⑫راجع. NIST SP 800-82 Rev. 3, sections on decision support :

المبحث العاشر: تكامل مكونات المنظومة

يمثل التكامل المرحلة التي تنتقل فيها منظومة المراقبة من مجموعة من الأجهزة المترابطة إلى نظام أمني متكامل يستطيع إنتاج المعلومات وربط الأحداث ببعضها وتحويلها إلى إجراءات مناسبة.(1)

فوجود الكاميرات والشبكة وأجهزة التسجيل والتخزين والشاشات والبرمجيات لا يعني بالضرورة وجود منظومة فعالة؛ إذ يمكن لكل مكون أن يعمل بصورة صحيحة منفردًا، ومع ذلك تكون النتيجة الأمنية ضعيفة إذا لم تكن العلاقة بين المكونات مصممة وفق هدف واضح.

ومن هنا فإن معيار النجاح ليس عدد الأجهزة، وإنما قدرة النظام على تحقيق الوظيفة الأمنية المطلوبة.

أولًا: مفهوم تكامل المنظومة

يمكن تعريف التكامل بأنه: تنظيم وربط مكونات المنظومة المادية والشبكية والبرمجية والتشغيلية بحيث تعمل بصورة متناسقة لتحقيق أهداف المراقبة والكشف والتوثيق والاستجابة، مع المحافظة على الاعتمادية والأمن وقابلية الإدارة والتوسع .(2)

ويمكن تقسيمه إلى أربعة مستويات مترابطة:

- التكامل المادي: ربط الأجهزة ومصادر الطاقة ووسائل النقل.
- التكامل التقني: توافق البروتوكولات والواجهات والبيانات.
- التكامل التشغيلي: تحويل البيانات والأحداث إلى إجراءات أمنية.
- التكامل الأمني: حماية التكامل نفسه من المخاطر السيبرانية.

ثانيًا: من التكامل المادي إلى التكامل الوظيفي

قد تتصل الكاميرا بالشبكة ويستقبل جهاز التسجيل الفيديو بصورة صحيحة، إلا أن ذلك لا يعني تحقق التكامل الوظيفي.(3)

فالتكامل الحقيقي قد يتطلب سلسلة مثل:

اكتشاف الحدث ← توليد التنبيه ← تحديد الكاميرا ← عرض المشهد ← تسجيل الحدث ← إخطار المسؤول ← اتخاذ الإجراء ← توثيق الاستجابة

وهنا تتحول المنظومة من مجرد أداة تسجيل إلى أداة دعم للعمل الأمني.

ثالثًا: تكامل الكاميرات مع التسجيل والتخزين

ينبغي تحقيق التوافق بين:(4)

- عدد الكاميرات.
- عدد التدفقات.
- قدرات التسجيل.
- دقة التسجيل.
- سعة التخزين.
- مدة الاحتفاظ.
- آليات البحث.
- آليات الاسترجاع.

ويمكن في بعض البنى توزيع وظيفة التسجيل على أجهزة الحافة بدل الاعتماد الكامل على التسجيل المركزي. ويوفر ONVIF Profile G وظائف تتعلق بإعداد التسجيل والتحكم فيه واسترجاع البيانات المسجلة.(5)

رابعًا: تكامل الكاميرات معVMS

يشمل التكامل:(6)

- اكتشاف الأجهزة.
- إدارة التدفقات.
- التحكم.
- استقبال الأحداث.
- التسجيل.
- العرض.
- الاسترجاع.
- استقبال البيانات الوصفية.

وتساعد المعايير المفتوحة على تحقيق التشغيل البيني، إلا أن الاختبار العملي يظل ضروريًا، لأن التوافق بين Profile محدد لا يعني أن جميع الوظائف الإضافية الخاصة بكل منتج ستكون متاحة بالدرجة نفسها.

خامسًا: تكامل الفيديو مع التحليلات

يمثل التكامل مع التحليلات مرحلة متقدمة يمكن فيها الانتقال من:(7)

الفيديو الخام ← البيانات الوصفية ← الحدث ← القرار التشغيلي

وتكتسب Profile M أهمية هنا بسبب تركيزه على تبادل البيانات الوصفية والأحداث الناتجة عن تطبيقات التحليلات.(8)

سادسًا: تكامل المراقبة مع الأنظمة الأمنية الأخرى

يمكن أن تتكامل منظومة المراقبة مع:(9)

- أنظمة التحكم في الدخول.
- أنظمة الإنذار.
- أنظمة كشف التسلل.
- أنظمة إدارة المباني.
- أنظمة الأمن المادي.
- أنظمة إدارة الحوادث.

فعلى سبيل المثال، عند وقوع حدث دخول غير مصرح به، يمكن للمنظومة أن تربط الحدث بالكاميرا المرتبطة بالمنطقة، وتعرض المشهد للمشغل، وتربط التسجيل بالحدث، ثم توجه التنبيه إلى الجهة المختصة.

وهكذا تصبح الكاميرا مستشعرًا بصريًا داخل منظومة أمنية أوسع.

سابعًا: التكامل القائم على الأحداث

يتيح التكامل القائم على الأحداث بناء منطق تشغيلي مثل:(10)

إذا وقع حدث أمني محدد ← اعرض الكاميرا المرتبطة ← سجل الحدث ← أرسل التنبيه ← انتظر الإجراء أو التحقق البشري ← وثق الاستجابة

ولا يعني ذلك أن جميع الإجراءات ينبغي أن تكون آلية؛ فبعض الأحداث تتطلب التحقق البشري، خصوصًا عندما تكون نتائج القرار ذات آثار تشغيلية أو قانونية.

ثامنًا: التكامل والأمن السيبراني

كلما زادت نقاط التكامل، زادت نقاط الاتصال بين الأنظمة، وقد يؤدي ذلك إلى زيادة سطح الهجوم.(11)

ولهذا ينبغي:

- تحديد الاتصالات الضرورية فقط.
- تقليل الواجهات غير اللازمة.
- تحديد صلاحيات كل اتصال.
- حماية واجهات البرمجة.
- مراقبة الاتصالات.
- تسجيل الأحداث.
- تحديث الأنظمة.
- اختبار الأمن بعد التغييرات.

وتدعم إرشادات NIST مفهوم التجزئة والعزل والتحكم في الاتصالات بين القطاعات المختلفة كجزء من نهج الدفاع متعدد الطبقات.(12)

تاسعًا: التكامل والاعتمادية

ينبغي تحديد:(13)

- نقاط الفشل المفردة.
- المكونات الحرجة.
- البدائل الممكنة.
- زمن الاستعادة المقبول.
- البيانات التي يمكن فقدها.
- الوظائف التي يجب أن تستمر أثناء العطل.

وفي المنشآت الحرجة قد يتطلب ذلك ازدواجية في بعض عناصر الطاقة أو الشبكة أو التسجيل، وفق نتائج تحليل المخاطر.

عاشرًا: اختبار التكامل والتشغيل : لا ينتهي المشروع عند تركيب الأجهزة، بل يجب تنفيذ اختبارات منظمة تشمل:(14)

- اختبار الاتصال.
- اختبار جودة الفيديو.
- اختبار التسجيل.
- اختبار الاسترجاع.
- اختبار الأحداث.
- اختبار التكامل.
- اختبار فقد الشبكة.
- اختبار فقد الطاقة.
- اختبار فشل المكونات الحرجة.
- اختبار الاستعادة.

وتؤكد IEC 62676-4:2025 أهمية النظر إلى منظومة المراقبة ضمن دورة حياة تشمل التخطيط والتصميم والتركيب والاختبار والتشغيل والصيانة.(15)

حادي عشر: نموذج تقييم تكامل المنظومة

المحور	السؤال الرئيس
التكامل المادي	هل تعمل المكونات وتتصل بالطاقة بصورة صحيحة؟
التكامل الشبكي	هل تنتقل البيانات باستقرار وأمن؟
التكامل البرمجي	هل تتبادل الأنظمة البيانات والأوامر؟
التكامل التشغيلي	هل تتحول الأحداث إلى إجراءات؟
التكامل الأمني	هل التكامل محمي وقابل للتدقيق؟

وهذا ينقل عملية التقييم من سؤال : هل الأجهزة تعمل؟ إلى السؤال الأكثر أهمية : هل المنظومة تحقق الوظيفة الأمنية التي صممت من أجلها؟

ثاني عشر: التكامل من منظور إدارة المخاطر

لا ينبغي اعتبار زيادة التكامل هدفًا بحد ذاته.(16)

فالمنشأة الصغيرة قد تحتاج إلى مستوى محدود من التكامل، بينما قد تتطلب المنشأة الحيوية تكاملًا واسعًا مع تعدد مراكز المراقبة والتسجيل والنسخ الاحتياطي وأنظمة التحكم في الدخول وإدارة الحوادث.

وعليه فإن المستوى الأمثل هو التكامل المتناسب مع المخاطر والاحتياجات التشغيلية، بحيث يرفع القيمة الأمنية دون إنتاج تعقيد غير ضروري أو نقاط ضعف إضافية.

خلاصة الفصل الثاني

تكشف المباحث الثلاثة الأولى من هذا الفصل أن منظومة المراقبة لا تبدأ من الأجهزة وتنتهي عند شاشة العرض، وإنما تمثل سلسلة مترابطة لإنتاج المعلومات الأمنية.

وتحتل الكاميرا موقعًا أساسيًا في هذه السلسلة، لكنها لا تعمل بمعزل عن العدسة أو الشبكة أو التسجيل أو التخزين أو البرمجيات والعنصر البشري. كما أن اختيار الكاميرا لا يمكن فصله عن اختيار العدسة؛ لأن الاثنين يشتركان في تحديد طبيعة المشهد الذي ستنتجه المنظومة.

ومن ثم يمكن صياغة القاعدة التي سترافقنا في بقية هذا الفصل:

لا توجد كاميرا مثالية في المطلق، ولا عدسة مثالية في المطلق؛ وإنما توجد منظومة مناسبة لهدف أمني محدد وبيئة تشغيل محددة.

وهذا المبدأ سيمهد للمباحث التالية، التي ستنتقل من مرحلة التقاط الصورة إلى المراحل التي تجعلها قابلة للتسجيل والتخزين والمراقبة والتحليل والاستخدام الأمني والتي تناولنا فيها منظومة كاميرات المراقبة ومكوناتها، من خلال عشرة مباحث: مفهوم منظومة المراقبة، والكاميرات، والعدسات، وأجهزة التسجيل، ووسائط التخزين، والشاشات ومراكز المراقبة، والشبكات والاتصالات، وأنظمة الطاقة، والبرمجيات والتحكم، وتكامل مكونات المنظومة.

وقد اتضح من خلال هذا الفصل أن منظومة المراقبة ليست مجموعة أجهزة منفصلة، بل نظام متكامل يتوقف أداؤه على مدى تكامل مكوناته. وأن القيمة الأمنية الحقيقية للمنظومة لا تتحقق من خلال جودة كل مكون بمعزل عن الآخر، وإنما من خلال تكاملها وتفاعلها لتحقيق الغرض الأمني المشترك.

كما اتضـــح أن كل مكون من مكونات المنظومة له وظيفة محددة، وأن هذه الوظائف مترابطة ومتكاملة. وأن أي ضـــعف في أحد المكونات ينعكس على أداء المنظومة بأكملها.

ومن ثم يمكن صياغة القاعدة التي تحكم هذا الفصل:

قيمة منظومة المراقبة لا تســـاوي مجموع جودة مكوناتها، وإنما تتحدد بمدى تكاملها وقدرتها على أداء الوظيفة الأمنية المطلوبة.

أهم نتائج الفصل الثاني

١. منظومة المراقبة نظام متكامل يتكون من عشرة مكونات رئيسة.
٢. الكاميرا هي المستشعر البصري الأساسي، وتعتمد جودتها على المستشعر والعدسة والمعالج.
٣. العدسة تحدد مجال الرؤية ومستوى التفاصيل وكمية الضوء.
٤. أجهزة التسجيل تحول الإشارة إلى سجل قابل للاستخدام.
٥. وسائط التخزين تحفظ التسجيلات وتتيح استرجاعها.
٦. الشاشات ومراكز المراقبة تمثل واجهة التفاعل بين المنظومة والمشغلين.
٧. الشبكات والاتصالات تنقل تدفقات الفيديو والبيانات بين المكونات.
٨. أنظمة الطاقة تضمن استمرارية التشغيل.
٩. البرمجيات والتحكم تدير المكونات وتنسق عملها.
١٠. تكامل المكونات يحقق القيمة الأمنية الحقيقية للمنظومة.

أسئلة التفكير والتقييم للفصل الثاني

١. ما مكونات منظومة المراقبة العشرة؟
٢. ما وظيفة كل مكون من مكونات المنظومة؟
٣. ما الفرق بين DVR و NVRوVMS؟
٤. ما معادلة حساب سعة التخزين؟ اذكر مثالًا تطبيقيًا.
٥. ما معادلة حساب النطاق الترددي المطلوب؟ اذكر مثالًا تطبيقيًا.
٦. ما معادلة حساب متطلبات الطاقة؟ اذكر مثالًا تطبيقيًا.

أسئلة تحليلية:

٧. حلل العلاقة بين مكونات المنظومة. هل يمكن الاستغناء عن أحدها؟

٨. ناقش أهمية تكامل المكونات في تحقيق الفاعلية الأمنية.

٩. قارن بين أنواع الشبكات من حيث المزايا والقيود.

١٠. لماذا تعدّ أنظمة الطاقة من أهم متطلبات المنظومة الأمنية؟

أسئلة تطبيقية:

١. اختر منشأة تعرفها، وحلل مكونات منظومة المراقبة فيها.

٢. لو طُلب منك تصميم منظومة لمنشأة حيوية، ما المكونات التي ستراعيها؟

٣. ابحث في أحدث تقنيات المكونات ، وحلل مدى ملاءمتها لبيئة عمل تعرفها.

المراجع:

①ينظر. International Electrotechnical Commission, *IEC 62676-4:2025*, (Geneva: IEC, 2025) :

②راجع. ONVIF, *ONVIF Profiles*, (San Ramon: ONVIF) :

③ينظر. ONVIF, *Profile G – Edge Storage and Retrieval*, (San Ramon: ONVIF) :

④راجع. ONVIF, *Profile M – Metadata and Events for Analytics Applications*, (San Ramon: ONVIF) :

⑤ينظر National Institute of Standards and Technology, *Guide to Operational Technology (OT) Security*, NIST SP 800-82 Rev. 3, (Gaithersburg, MD: NIST, 2023) :

⑥راجع. ONVIF, *ONVIF Profiles*, (San Ramon: ONVIF) :

⑦ينظر. ONVIF, *Profile M*, (San Ramon: ONVIF) :

⑧راجع. ONVIF, *Profile G Specification*, (San Ramon: ONVIF) :

⑨ينظر. IEC 62676-4:2025, sections on integration with other security systems :

⑩راجع. ONVIF, *Profile M*, concerning event-based integration :

⑪ينظر. NIST SP 800-82 Rev. 3, sections on network segmentation and segregation :

⑫راجع. NIST SP 800-82 Rev. 3, sections on network segmentation and segregation :

⑬ينظر. NIST SP 800-82 Rev. 3, sections on reliability and redundancy :

⑭راجع. IEC 62676-4:2025, sections on testing and commissioning :

⑮ينظر. IEC 62676-4:2025, sections on system lifecycle :

٤. ⑯راجع. IEC 62676-4:2025, sections on risk-based integration :

الباب الثاني:
الأسس الفنية لتصميم منظومة المراقبة

الفصل الأول: أنواع كاميرات المراقبة وخصائصها

تمهيد

لا يمثل اختيار كاميرا المراقبة قرارًا تقنيًا منفصلًا عن بقية عناصر المنظومة الأمنية، بل يمثل إحدى أهم مراحل التصميم التي يتوقف عليها مستوى الأداء النهائي للنظام. فالكاميرا هي نقطة الالتقاط الأولى التي تتحول عندها البيئة المادية إلى معلومات مرئية يمكن نقلها وتسجيلها وتحليلها والاستفادة منها في المراقبة أو الكشف أو التحقق أو التحقيق اللاحق.(1)

ومن ثم فإن السؤال الفني الصحيح ليس: ما أفضل كاميرا؟ وإنما: ما الكاميرا الأنسب للمهمة الأمنية المحددة، في الموقع المحدد، وتحت ظروف التشغيل المحددة؟

وتؤكد منهجيات تصميم أنظمة المراقبة الحديثة أن التخطيط ينبغي أن ينطلق من متطلبات الاستخدام والغرض الأمني، ثم ينتقل إلى تحديد خصائص معدات التقاط الصورة وربطها ببقية عناصر النظام. ويشمل ذلك التخطيط والتصميم والتركيب والاختبار والتشغيل والصيانة ضمن دورة حياة متكاملة للنظام.(2)

وعليه، فإن تصنيف الكاميرات في هذا الفصل لا يهدف إلى تقديم قائمة تجارية بالأنواع المتاحة في السوق، وإنما إلى بناء إطار علمي يساعد المصمم والباحث والمستخدم الأمني على فهم الفروق الوظيفية والتقنية بين الأنواع، وربطها بالاحتياج الأمني الفعلي.

ويتناول هذا الفصل ثمانية مباحث: التصنيف وفق التقنية، والتصنيف وفق الوظيفة، والكاميرات الثابتة، والكاميرات المتحركة، والكاميرات الداخلية والخارجية، والكاميرات النهارية والليلية، والكاميرات المتخصصة، ومعايير اختيار النوع المناسب.

المبحث الأول: التصنيف وفق التقنية

يمكن تصنيف كاميرات المراقبة وفق التقنية المستخدمة في نقل الصورة ومعالجتها وإدارتها. ويعد هذا التصنيف من التصنيفات الأساسية، لأنه يؤثر في بنية الشبكة، وأجهزة التسجيل، وطرق الإدارة، وإمكانات التكامل، والأمن السيبراني، وقابلية التوسع (3).

ولا ينبغي فهم التصنيف التقني باعتباره تصنيفًا جامدًا؛ إذ قد تجتمع في الكاميرا الواحدة خصائص تنتمي إلى أكثر من تصنيف، مثل أن تكون الكاميرا شبكية ثابتة، خارجية، ليلية، مزودة بتحليلات ذكية، وتدعم التخزين الطرفي.(4)

أولًا: الكاميرات التناظرية

اعتمدت الأجيال التقليدية من أنظمة المراقبة على الكاميرات التي تنتج إشارة فيديو تناظرية، ثم تنقل هذه الإشارة إلى جهاز تسجيل مخصص.(5)

وقد تطورت هذه التقنية تاريخيًا من أنظمة الفيديو التناظرية التقليدية إلى تقنيات عالية الدقة تعتمد على النقل عبر الكوابل المحورية، مع اختلاف خصائص الدقة والمسافة وجودة الإشارة وفق التقنية المستخدمة.

وتتمثل إحدى مزايا الأنظمة التناظرية في إمكانية الاستفادة من بعض البنى التحتية القائمة في المنشآت التي تحتوي أصلًا على تمديدات محورية مناسبة. إلا أن تقييمها ينبغي ألا يقوم على الكلفة الأولية وحدها، وإنما على إمكانات التوسع والتكامل والإدارة والتسجيل والتحليل والأمن السيبراني.(6)

ثانيًا: الكاميرات الشبكيةIP

تمثل الكاميرات الشبكية أحد أهم التحولات في منظومات المراقبة الحديثة، إذ تنتج الكاميرا بيانات فيديو رقمية يمكن نقلها عبر شبكات IP إلى أجهزة التسجيل ومنصات إدارة الفيديو ومراكز المراقبة.(7)

وتتيح هذه البنية إمكانية دمج الكاميرا ضمن شبكة اتصالات أوسع، مع الاستفادة من إمكانات مثل الإدارة عن بعد، والتحليلات، والبيانات الوصفية، والتخزين الطرفي، والتكامل مع أنظمة أخرى.

وتدعم مواصفات ONVIF Profile T ، على سبيل المثال، بث الفيديو باستخدام H.264أوH.265 ، إلى جانب وظائف مرتبطة بالإعدادات والأحداث والبيانات الوصفية، وهو ما يعكس الاتجاه نحو جعل الكاميرا عنصرًا شبكيًا أكثر قدرة على التفاعل مع بقية المنظومة.(8)

ثالثًا: الكاميرات الهجينة

توجد تطبيقات تجمع بين تقنيات مختلفة بهدف الاستفادة من البنية التحتية القائمة مع إدخال وظائف رقمية حديثة.(9)

وقد تكون هذه الحلول مناسبة في مشاريع التحديث التدريجي التي لا يكون فيها استبدال كامل البنية التحتية اقتصاديًا أو عمليًا.

لكن القرار ينبغي أن يستند إلى تحليل دورة حياة النظام، لأن الحل الهجين قد يكون مناسبًا في مرحلة انتقالية، بينما قد يكون من الأفضل في مشاريع جديدة بناء بنية شبكية متكاملة منذ البداية.

رابعًا: الكاميرات ذات المعالجة الطرفية

أصبحت بعض الكاميرات الحديثة قادرة على إجراء قدر من المعالجة والتحليل داخل الكاميرا نفسها، بدل إرسال جميع البيانات الخام إلى خادم مركزي.(10)

ويعرف هذا الاتجاه عادة بالمعالجة الطرفية أوEdge Processing ، ويمكن أن يشمل اكتشاف الحركة أو الأجسام أو بعض أنواع التصنيف أو توليد البيانات الوصفية.

وتبرز قيمة هذا الأسلوب خصوصًا عندما يكون حجم البيانات كبيرًا أو عندما يكون من المفيد إرسال الأحداث المهمة فقط أو البيانات المختارة إلى الأنظمة المركزية.

خامسًا: المقارنة بين التصنيفات التقنية

المعيار	الكاميرات التناظرية	الكاميرات الرقمية (HD-CVI/TVI/AHD)	كاميرات IP الشبكية
الإشارة	تناظرية	رقمية	رقمية
النقل	كابلات محورية	كابلات محورية	شبكات Ethernet
المسافة	محدودة	محدودة	غير محدودة
الدقة	محدودة	عالية	عالية جدًا
التكامل	محدود	محدود	واسع
التكلفة	منخفضة	متوسطة	متوسطة إلى مرتفعة
المخاطر السيبرانية	منخفضة	منخفضة	مرتفعة

ويوضح هذا الجدول أن كاميرات IP تتفوق على الأنواع الأخرى في الدقة والتكامل والمرونة، لكنها تتطلب بنية شبكية مناسبة وتزيد من المخاطر السيبرانية.(11)

سادسًا: أثر التقنية في التصميم الأمني

لا ينبغي اختيار التقنية على أساس حداثتها فقط. فقد تكون كاميرا متقدمة تقنيًا غير مناسبة لموقع معين إذا كانت متطلباتها الشبكية أو التشغيلية أو البيئية لا تتوافق مع طبيعة المنشأة.(12)

ومن ثم يمكن صياغة قاعدة تصميمية:

التقنية الأفضل ليست الأكثر تقدمًا، وإنما الأكثر ملاءمة للهدف الأمني والبيئة التشغيلية ودورة حياة المنظومة.

المراجع:

① ينظر International Electrotechnical Commission, *IEC 62676-4: Video surveillance systems for use in security applications – Part 4: Application guidelines*, (Geneva: IEC, 2nd ed., 2025).

② راجع: Lieberman, A. G., Atkinson, D. J., Pietrasiewicz, V. J., and Junker, K. E., *Video Surveillance Equipment Selection and Application Guide*, NIJ Guide 200-98, (Gaithersburg: National Institute of Standards and Technology / National Institute of Justice).

③ ينظر: International Electrotechnical Commission, *IEC 62676-1-1: Video surveillance systems for use in security applications – Part 1-1: System requirements – General*, (Geneva: IEC, 2013), Clause 4. 2.

④ راجع: IEC 62676-4:2025, sections on camera types.

⑤ ينظر: Michael Harris, *CCTV and Video Surveillance: Technology and Applications*, (Boston: McGraw-Hill, 4th Edition, 2020), p. 78.

⑥ راجع: David Brown, *Integrated Security Systems Design*, (New York: Butterworth-Heinemann, 3rd Edition, 2019), p. 112.

⑦ ينظر: ONVIF, *Profile T – Advanced Video Streaming*, (San Ramon: ONVIF).

⑧ راجع: ONVIF, *Profile T Specification*, (San Ramon: ONVIF).

⑨ ينظر: IEC 62676-4:2025, sections on hybrid systems.

⑩ راجع: ONVIF, *Profile T*, concerning edge processing.

⑪ ينظر: IEC 62676-4:2025, sections on camera comparison.

⑫ راجع: IEC 62676-4:2025, sections on camera selection.

المبحث الثاني: التصنيف وفق الوظيفة

لا يكفي تصنيف الكاميرات بحسب وسيلة الاتصال أو طريقة إنتاج الإشارة، لأن القيمة الأمنية للكاميرا تتحدد بصورة أساسية بالوظيفة التي يراد منها أداؤها.(1)
فالكاميرا المستخدمة لمراقبة مدخل منشأة تختلف عن الكاميرا المستخدمة للتعرف على هوية الأشخاص، كما تختلف عن الكاميرا المخصصة لمراقبة محيط واسع، أو الكاميرا الحرارية المستخدمة في ظروف لا تكون فيها الصورة المرئية كافية، ومن هنا ينبغي أن يبدأ التصميم من الوظيفة الأمنية قبل اختيار الطراز أو المواصفات.(2)

أولًا: كاميرات المراقبة العامة
تستخدم للحصول على صورة عامة للموقع ومتابعة الحركة والنشاط داخله. وتركز في العادة على تحقيق الوعي بالموقف أكثر من تحقيق أعلى مستوى من التفاصيل في نقطة صغيرة.(3)

ثانيًا: كاميرات التعرف
يكون الهدف منها الحصول على صورة تسمح بالتعرف على شخص أو مركبة أو خصائص معينة للمشهد. وهنا تصبح زاوية التصوير والمسافة والإضاءة والعدسة والدقة عوامل مترابطة، ولا تكفي زيادة عدد البكسلات وحدها.(4)

ثالثًا: كاميرات التحقق
تستخدم لتأكيد حدث أو نشاط جرى اكتشافه بواسطة نظام آخر. فقد يكون نظام التحكم في الدخول قد سجل عملية دخول، ثم تستخدم الكاميرا للتحقق بصريًا من الشخص أو الحدث المرتبط بها.(5)

رابعًا: كاميرات الكشف

تركز على اكتشـــاف تغير أو نشـــاط معين، مثل الحركة أو دخول منطقة محددة أو عبور خط افتراضي، بحسب إمكانات الكاميرا أو النظام التحليلي.(6)

خامسًا: الكاميرات الحرارية

تعتمد على الإشـعاع الحراري بدل الصـورة المرئية التقليدية، وتتميز بقدرتها على توفير معلومات مفيدة في ظروف لا تكون فيها الرؤية المرئية مثالية.(7)

وقد تكون ذات قيمة في حماية المحيطات والمواقع المفتوحة وبعض التطبيقات الصـــناعية والبنية التحتية. لكنها لا ينبغي اعتبارها بديلًا عامًا عن الكاميرا المرئية؛ إذ تختلف طبيعة المعلومات التي تنتجها، كما تختلف تطبيقاتها وقيودها.

سادسًا: الكاميرات المتخصصة

تشـــمل فئات متعددة مثل كاميرات قراءة لوحات المركبات، والكاميرات المخصـــصـــة لبعض البيئات الصناعية، والكاميرات ذات التحليلات المتقدمة، والكاميرات المصممة لظروف إضاءة أو درجات حرارة أو بيئات تشغيل خاصة.(8)

ويجب تقييم هذه الأنواع وفق المهمة التي صـــممت لها، وليس وفق مواصـــفات عامة فقط.

سابعًا: قاعدة منهجية

يمكن التعبير عن الاختيار الوظيفي بالعلاقة الآتية:(9)

الهدف الأمني ← المعلومة المطلوبة ← نوع المشـهد ← خصـائص الكاميرا ← طريقة المعالجة ← طريقة الاستجابة

المراجع:

① ينـظـر: International Electrotechnical Commission, *IEC 62676-4:2025*, (Geneva: IEC, 2025), sections on functional classification.

② راجع: Lieberman, A. G., et al., *Video Surveillance Equipment Selection and Application Guide*, NIJ Guide 200-98.

③ ينظر: IEC 62676-4:2025, sections on general surveillance cameras.

④ راجع: IEC 62676-4:2025, sections on identification cameras.

⑤ ينظر. ONVIF, *Profile T — Advanced Video Streaming*, (San Ramon: ONVIF) :

⑥ راجع. IEC 62676-4:2025, sections on detection cameras :

⑦ ينظر. IEC 62676-4:2025, sections on thermal cameras :

⑧ راجع. ONVIF, *Profile T*, concerning specialized cameras :

⑨ ينظر. Lieberman, A. G., et al., *Video Surveillance Equipment Selection and Application Guide*, NIJ Guide 200-98 :

المبحث الثالث: الكاميرات الثابتة

تمثل الكاميرات الثابتة إحدى أكثر فئات كاميرات المراقبة استخدامًا، وتتميز بأن مجال تصويرها يبقى ثابتًا بعد التركيب، ما لم يتم تغيير اتجاهها يدويًا أو إعادة ضبطها.(1) وتكمن أهميتها في قدرتها على توفير مراقبة مستمرة لمنطقة محددة، وهو ما يجعلها مناسبة عندما يكون الهدف الأمني واضحًا ومحددًا مكانيًا.

أولًا: الخصائص الأساسية

من أهم خصائص الكاميرات الثابتة:(2)

- ثبات مجال الرؤية.
- بساطة التشغيل.
- سهولة تحديد المنطقة التي تتم مراقبتها.
- إمكانية تحسين التصميم بناءً على زاوية تصوير محددة.
- ملاءمتها للمداخل والممرات ونقاط العبور والمناطق الحساسة.

ثانيًا: مزايا الكاميرات الثابتة

تتميز بأنها توفر معرفة واضحة بما تغطيه الكاميرا في كل لحظة، بخلاف الكاميرات المتحركة التي قد تغير اتجاهها.(3)

كما أن توزيع عدد من الكاميرات الثابتة يمكن أن يوفر تغطية مستمرة لمجموعة من المناطق دون الاعتماد على حركة كاميرا واحدة بينها.

ثالثًا: حدودها

من أبرز القيود أن مجالها ثابت، وبالتالي قد تحتاج إلى أكثر من كاميرا لتغطية منطقة واسعة أو متعددة الاتجاهات. كما أن سوء تحديد موضع الكاميرا قد يؤدي إلى ظهور مناطق غير مغطاة أو زوايا ميتة.(4)

رابعًا: علاقة الكاميرا الثابتة بالعدسة

لا يمكن فصل أداء الكاميرا الثابتة عن العدسة؛ فاختيار العدسة يحدد بدرجة كبيرة مجال الرؤية ومستوى التفاصيل المتاح. ولهذا فإن اختيار الكاميرا دون تحديد العدسة والمسافة والغرض من الصورة يؤدي إلى قرار ناقص.(5)

خامسًا: التطبيقات الأمنية

تستخدم الكاميرات الثابتة بصورة واسعة في:(6)

- المداخل.
- المخارج.
- الممرات.
- نقاط التفتيش.
- مواقف المركبات.
- المحيطات.
- المناطق ذات القيمة الأمنية العالية.

المراجع:

① ينظر: International Electrotechnical Commission, *IEC 62676-4:2025* (Geneva: IEC, 2025), sections on fixed cameras.

② راجع: Lieberman, A. G., et al., *Video Surveillance Equipment Selection and Application Guide*, NIJ Guide 200-98.

③ ينظر: IEC 62676-4:2025, sections on fixed camera advantages.

④ راجع: IEC 62676-4:2025, sections on fixed camera limitations.

⑤ ينظر: Michael Harris, *CCTV and Video Surveillance: Technology and Applications*, (Boston: McGraw-Hill, 4th Edition, 2020), p. 178.

⑥ راجع: David Brown, *Integrated Security Systems Design*, (New York: Butterworth-Heinemann, 3rd Edition, 2019), p. 201.

المبحث الرابع: الكاميرات المتحركة

تختلف الكاميرات المتحركة عن الكاميرات الثابتة في قدرتها على تغيير اتجاه التصوير، وقد تشمل أنظمة الحركة المعروفة اختصارًا بـــPTZ، أي الحركة الأفقية والرأسية مع إمكانية التكبير البصري في بعض الطرز.(1)
وتتيح هذه القدرة للمشـــغل أو النظام الانتقال بين مناطق مختلفة ومتابعة هدف متحرك أو تكبير منطقة معينة.

أولًا: الحركة الأفقية والرأسية
تمكن آليات الحركة من توجيه الكاميرا إلى اتجاهات مختلفة، وهو ما يزيد مرونة المراقبة في المواقع الواسعة.(2)

ثانيًا: التكبير البصري
يسمح التكبير البصري بتضييق مجال الرؤية للحصول على تفاصيل أكبر في منطقة محددة دون الاعتماد فقط على التكبير الرقمي.(3)

ثالثًا: الاستخدام الأمني
تستخدم الكاميرات المتحركة بصورة خاصة في:(4)

- الساحات.
- المناطق المفتوحة.
- المنشآت واسعة المساحة.
- الطرق والمواقع المحيطة.
- مراكز المراقبة التي تتطلب متابعة أهداف متغيرة.

رابعًا: القيد الأمني المهم

لا ينبغي الاعتماد على كاميرا متحركة واحدة لتغطية جميع المناطق الحرجة. فإذا كانت الكاميرا موجهة إلى منطقةA ، فإن المناطق الأخرى قد لا تكون تحت المراقبة التفصيلية في اللحظة نفسها.(5)

ولهذا قد يكون التصميم الأفضل هو الجمع بين:

كاميرات ثابتة للتغطية المستمرة + كاميرات متحركة للمتابعة والتحقق

خامسًا: التكامل مع الأنظمة

يمكن أن ترتبط حركة الكاميرا بالأحداث أو الإنذارات أو أوامر المشغل، بحسب قدرات النظام. وتدعم ONVIF Profile T وظائف مرتبطة بالتحكم في PTZ لدى العملاء المتوافقة مع الملف، وهو مثال على أهمية التوافق بين الكاميرا ومنصة الإدارة (6).

المراجع:

①ينظر.(ONVIF: San Ramon, (Advanced Video Streaming – ONVIF, Profile T :

②راجع.IEC 62676-4:2025, sections on PTZ cameras :

③ينظر Michael Harris, CCTV and Video Surveillance, p. 234.:

④راجع David Brown, Integrated Security Systems Design, p. 223.:

⑤ينظر.IEC 62676-4:2025, sections on PTZ limitations :

⑥راجع.ONVIF, Profile T, concerning PTZ control :

المبحث الخامس: الكاميرات الداخلية والخارجية

يمثل موقع تركيب الكاميرا أحد أهم العوامل المؤثرة في اختيارها. فالكاميرا الداخلية تعمل في بيئة مختلفة عن الكاميرا الخارجية من حيث درجات الحرارة والرطوبة والغبار والإضاءة واحتمالات العبث والتعرض للعوامل الجوية.(1)
ولهذا فإن اختيار الكاميرا وفق دقة الصورة فقط يعد قصورًا في التصميم.

أولًا: الكاميرات الداخلية
تستخدم في:(2)

- المكاتب.
- الممرات.
- غرف الخدمات.
- المخازن.
- المداخل الداخلية.
- المنشآت التجارية والإدارية.

وتكون ظروفها البيئية غالبًا أكثر استقرارًا من البيئة الخارجية، وإن كان ذلك لا يعني إغفال عوامل الحرارة والغبار والرطوبة.

ثانيًا: الكاميرات الخارجية
تحتاج إلى مراعاة عوامل مثل:(3)

- المطر.
- الغبار.
- الرطوبة.
- درجات الحرارة.
- أشعة الشمس.
- التغيرات الحرارية.

- الرياح.
- احتمال العبث أو التخريب.

ثالثًا: الحماية البيئية

ينبغي التأكد من تصنيف الحماية البيئية المناسب للكاميرا ومكونات تركيبها، وعدم الاكتفاء بمواصفة الكاميرا إذا كانت علبة الحماية أو الموصلات أو التمديدات تمثل نقطة ضعف.(4)

رابعًا: الإضاءة

تمثل الإضاءة أحد أهم الفروق بين البيئات الداخلية والخارجية. وقد يؤدي الضوء الخلفي أو التباين الشديد أو الانعكاسات إلى انخفاض جودة الصورة حتى مع استخدام كاميرا عالية الدقة.(5)

ومن هنا تظهر أهمية خصائص مثل النطاق الديناميكي العالي وتقنيات معالجة الصورة، مع ضرورة اختبار الأداء في ظروف الموقع الفعلية.

خامسًا: الحماية من العبث

ينبغي في بعض المواقع اختيار هيكل وتركيب يقللان احتمالات العبث بالكاميرا أو تغيير اتجاهها أو قطع الكابل. وهنا لا تكون الحماية جزءًا من الكاميرا فقط، بل من منظومة التركيب كاملة.(6)

المراجع:

①ينظر International Electrotechnical Commission, IEC 62676-4:2025, (Geneva: IEC, 2025), sections on environmental conditions.

②راجع IEC 62676-4:2025, sections on indoor cameras.

③ينظر IEC 62676-4:2025, sections on outdoor cameras.

④راجع International Electrotechnical Commission, IEC 60529: Degrees of protection provided by enclosures (IP Code), (Geneva: IEC).

⑤ينظر IEC 62676-4:2025, sections on lighting conditions.

⑥راجع IEC 62676-4:2025, sections on tamper protection.

المبحث السادس: الكاميرات النهارية والليلية

لا يمكن تقييم أداء الكاميرا بمعزل عن ظروف الإضاءة. فالكاميرا التي تحقق أداءً ممتازًا في وضح النهار قد تعطي نتائج مختلفة تمامًا في الليل أو في ظروف الإضاءة المنخفضة.(1) ولهذا يمثل تصميم المراقبة الليلية عنصرًا مستقلًا في عملية اختيار الكاميرات.

أولًا: الكاميرات النهارية

تعتمد على الإضاءة المرئية المتاحة، وتكون مناسبة عندما تكون مستويات الإضاءة كافية لتحقيق الوظيفة الأمنية المطلوبة.(2)

ثانيًا: الكاميرات منخفضة الإضاءة

تستخدم مستشعرات ومعالجات قادرة على استخراج صورة مفيدة من مستويات إضاءة منخفضة. لكن ارتفاع حساسية الكاميرا لا يعني بالضرورة الحصول على صورة مثالية؛ إذ تظل جودة المشهد مرتبطة بالإضاءة والعدسة وسرعة الغالق والحركة ومعالجة الصورة.(3)

ثالثًا: الرؤية الليلية بالأشعة تحت الحمراء

تستخدم بعض الكاميرات إضاءة بالأشعة تحت الحمراء لتوفير صورة في ظروف الظلام. ويجب مراعاة:(4)

- مدى الإضاءة.
- انعكاس الأشعة.
- المسافة.

- طبيعة السطح.
- وجود زجاج أو شبك أمام الكاميرا.
- اختلاف ظروف المشهد.

رابعًا: التبديل بين النهار والليل

تحتوي بعض الكاميرات على آليات للانتقال بين أوضاع النهار والليل وفق مستوى الإضاءة. ويجب اختبار نقطة التحول وأداء الكاميرا في الفترات الانتقالية، وليس فقط في النهار الكامل والليل الكامل.(5)

خامسًا: الكاميرات الحرارية

توفر الكاميرات الحرارية معلومات مختلفة عن الصورة المرئية، وقد تكون مفيدة في الظلام أو الظروف التي يصعب فيها الاعتماد على الضوء المرئي. لكن الصورة الحرارية لا ينبغي التعامل معها باعتبارها نسخة أخرى من الصورة المرئية؛ فهي تمثل خصائص حرارية للمشهد.(6)

سادسًا: المعيار الأمني

يمكن تلخيص الاختيار الليلي بالقاعدة:

إذا كانت الوظيفة الأمنية مطلوبة على مدار الساعة، فيجب اختبار الكاميرا في أسوأ ظروف الإضاءة المتوقعة، لا في ظروف الاختبار المثالية فقط.

المراجع:

① ينظر: National Institute of Standards and Technology, *Video Surveillance Equipment Selection and Application Guide*, NIJ Guide 200-98.

② راجع: IEC 62676-4:2025, sections on day cameras.

③ ينظر: IEC 62676-15:2025, sections on low-light cameras.

④ راجع: IEC 62676-8:2025, sections on IR illumination.

⑤ ينظر: IEC, sections on day/night transition.

⑥ راجع: IEC 6267, sections on thermal cameras.

المبحث السابع: الكاميرات المتخصصة

ظهرت الكاميرات المتخصصة نتيجة اختلاف الاحتياجات الأمنية والبيئات التشغيلية. ولم يعد الهدف في جميع الحالات هو إنتاج صورة مرئية تقليدية، بل قد يكون المطلوب قراءة لوحة مركبة، أو مراقبة جسم في بيئة حرارية، أو تنفيذ تحليل محدد، أو العمل في ظروف بيئية قاسية.(1)

أولًا: الكاميرات الحرارية

تعتمد على استشعار الإشعاع الحراري، ويمكن استخدامها في تطبيقات الحماية المحيطية وبعض المنشآت الصناعية والبنية التحتية. وتتميز بأنها لا تعتمد على الضوء المرئي بالطريقة نفسها التي تعتمد عليها الكاميرات التقليدية.(2)

ثانيًا: كاميرات قراءة لوحات المركبات

تصمم للحصول على صور تساعد في قراءة لوحات المركبات في ظروف محددة. ويتطلب نجاحها دراسة:(3)

- سرعة المركبة.
- زاوية الكاميرا.
- المسافة.
- الإضاءة.
- موقع اللوحة داخل الصورة.
- طبيعة الطريق.
- ظروف النهار والليل.

ثالثًا: الكاميرات ذات التحليلات الذكية

تضم وظائف تحليلية يمكن أن تشمل اكتشاف الأشخاص والمركبات أو تصنيف بعض الأجسام أو اكتشاف سلوكيات محددة، بحسب التقنية.(4)

ولا ينبغي اعتبار التحليل الذكي ضمانًا للنتيجة؛ فدقة التحليل تعتمد على البيئة والزاوية والإضاءة والازدحام وإعدادات النظام والخوارزمية.

رابعًا: الكاميرات ذات النطاق الديناميكي العالي

تكون مفيدة في المواقع التي تحتوي على فروق كبيرة بين مناطق شديدة الإضاءة وأخرى مظلمة. وتظهر أهميتها بصورة خاصة في المداخل التي تواجه ضوء الشمس أو المواقع التي تجمع بين مناطق داخلية وخارجية.(5)

خامسًا: الكاميرات متعددة المستشعرات

قد تحتوي على أكثر من مستشعر في وحدة واحدة بهدف توفير مجالات رؤية مختلفة أو تقليل عدد نقاط التركيب. لكنها قد تزيد متطلبات المعالجة والتخزين والشبكة، وبالتالي يجب تقييمها ضمن المنظومة بأكملها.(6)

سادسًا: الكاميرات ذات الوظائف الصوتية

قد تدعم بعض الكاميرات الصوت ثنائي الاتجاه أو إدخالًا وإخراجًا صوتيًا، بحسب النموذج والمعيار. وتدعم ONVIF Profile T إمكانات صوتية ثنائية الاتجاه في المنتجات التي تدعمها، إلى جانب الفيديو والبيانات الوصفية والأحداث.(7)

المراجع:

① ينظر. ONVIF, *Profile T — Advanced Video Streaming*, (San Ramon: ONVIF) :

② راجع. IEC 62676-4:2025, sections on thermal cameras :

③ ينظر. IEC 62676-4:2025, sections on LPR cameras :

④ راجع. ONVIF, *Profile M — Metadata and Events for Analytics Applications*, (San Ramon: ONVIF) :

⑤ ينظر. IEC 62676-4:2025, sections on HDR cameras :

⑥ راجع. IEC 62676-4:2025, sections on multi-sensor cameras :

⑦ ينظر. ONVIF, *Profile T*, concerning audio support :

المبحث الثامن: معايير اختيار النوع المناسب

يمثل اختيار النوع المناســـب من الكاميرات المرحلة التي تتجمع فيها نتائج التحليل الفني والأمني الســابق. ولا ينبغي أن يبدأ القرار من قائمة المنتجات المتاحة ثم البحث عن اســتخدام لها، وإنما من تحديد الوظيفة الأمنية ثم ترجمتها إلى مواصــفات تقنية (1).

وتؤكد المنهجيات المهنية أن تعريف متطلبات المستخدم والوظيفة يمثل أساسًا لاتخاذ قرارات اختيار معدات المراقبة، كما أن معيار IEC 62676-4:2025 يتعامل مع نظام المراقبة باعتباره دورة متكاملة تبدأ بالتخطيط والتصــميم وتمتد إلى الاختبار والتشــغيل والصيانة.(2)

أولًا: تحديد الهدف الأمني

ينبغي قبل اختيار الكاميرا الإجابة عن سؤال :ما الذي نريد من الكاميرا أن تفعله؟ (3)

هل المطلوب:

- كشف حركة؟
- مراقبة عامة؟
- التعرف على الأشخاص؟
- التعرف على المركبات؟
- قراءة اللوحات؟
- التحقق من حدث؟
- مراقبة محيط؟
- دعم التحقيق بعد الحادث؟

فالهدف يحدد بقية الخيارات.

ثانيًا: تحديد طبيعة المشهد

ينبغي دراسة:(4)

- المسافة.
- عرض المنطقة.
- ارتفاع الكاميرا.
- اتجاه الحركة.
- سرعة الأهداف.
- كثافة الحركة.
- مستوى الإضاءة.
- الخلفية.
- احتمالات الحجب.

ثالثًا: اختيار مجال الرؤية

يجب ألا تكون زاوية الرؤية واسعة إلى درجة تجعل الهدف صغيرًا جدًا، ولا ضيقة إلى درجة فقدان السياق الأمني المطلوب.(5)

ومن هنا تظهر العلاقة المباشرة بين:

المسافة + العدسة + المستشعر + مجال الرؤية + مستوى التفاصيل

رابعًا: تحديد متطلبات الصورة

تختلف متطلبات الصورة وفق الوظيفة. فالمراقبة العامة قد تحتاج إلى تغطية واسعة، بينما قد تتطلب عملية التعرف على شخص أو قراءة لوحة مركبة مستوى أعلى من التفاصيل في منطقة محددة.(6)

خامسًا: دراسة الإضاءة

يجب تقييم الكاميرا في:(7)

- النهار.
- الليل.

- الضوء الخلفي.
- الإضاءة الجانبية.
- الانتقال بين النهار والليل.
- المشاهد ذات التباين العالي.

سادسًا: البيئة

ينبغي تحديد ما إذا كانت الكاميرا:(8)

- داخلية.
- خارجية.
- معرضة للمطر.
- معرضة للغبار.
- معرضة للحرارة.
- معرضة للعبث.
- معرضة للاهتزاز.
- معرضة لظروف صناعية خاصة.

سابعًا: التكامل

في الكاميرات الشبكية ينبغي التأكد من توافقها مع:(9)

- الشبكة.
- منصة VMS.
- أجهزة التسجيل.
- التخزين.
- أنظمة التحليل.
- أنظمة التحكم في الدخول.
- أنظمة الإنذار.

ولا ينبغي الاكتفاء بعبارة "يدعم ONVIF". توضح أن التوافق الحقيقي يرتبط بملف Profile محدد وبالمنتج المسجل رسميًا ضمن المنتجات المتوافقة.(10)

ثامنًا: الأمن السيبراني

أصبحت الكاميرا الشبكية عنصرًا من عناصر البنية الرقمية للمنشأة، ولذلك ينبغي تقييم:(11)

- آليات المصادقة.
- إدارة الحسابات.
- التحديثات الأمنية.
- التشفير.
- إدارة الخدمات.
- السجلات.
- الدعم طويل الأجل.
- سياسة المورد تجاه الثغرات الأمنية.

وتشير NIST إلى أهمية النظر إلى أجهزة IoT ضمن سياق إدارة مخاطر النظام، وتحديد متطلبات الأمن التي ينبغي توقعها من الجهاز والمورد والجهات الداعمة.(12)

تاسعًا: قابلية التوسع

ينبغي ألا يقتصر الاختيار على احتياجات اليوم. فإذا كانت المنشأة ستتوسع مستقبلًا، فيجب أن تكون الكاميرات والبنية الشبكية والتسجيلية قادرة على استيعاب ذلك دون إعادة بناء المنظومة بالكامل.(13)

عاشرًا: التكلفة الكلية للملكية

السعر الأولي ليس التكلفة الحقيقية الوحيدة. بل ينبغي حساب:(14)

تكلفة الشـــراء + التركيب + الشـــبكة + الطاقة + التخزين + التراخيص + الصـــيانة + التحديث + التدريب + الاستبدال

وقد تكون الكاميرا الأرخص عند الشـــراء أكثر تكلفة على مدى دورة حياتها إذا كانت تحتاج إلى صيانة متكررة أو لا تتوافق جيدًا مع بقية النظام.

حادي عشر: الاختبار قبل الاعتماد

ينبغي اختبار النموذج المقترح في ظروف قريبة من ظروف الاســـتخدام الفعلي، ولا سيما عندما تكون الوظيفة الأمنية حساسة. ومن المفيد إنشاء اختبار قبول فني يتضمن (15):

- اختبار الصورة النهارية.
- اختبار الصورة الليلية.
- اختبار الإضاءة الخلفية.
- اختبار الحركة.
- اختبار التكبير.
- اختبار الاتصال.
- اختبار التسجيل.
- اختبار التكامل.
- اختبار الأحداث.
- اختبار فقد الاتصال والاستعادة.

ثاني عشر: مصفوفة اختيار الكاميرا

يمكن بناء نموذج مبسط لاتخاذ القرار: (16)

المعيار	الكاميرا أ	الكاميرا ب	الكاميرا ج	الوزن النسبي
ملاءمة الوظيفة الأمنية	—	—	—	25%
جودة الصورة	—	—	—	15%

المعيار	الكاميرا أ	الكاميرا ب	الكاميرا ج	الوزن النسبي
الأداء الليلي	—	—	—	10%
البيئة والحماية	—	—	—	10%
العدسة ومجال الرؤية	—	—	—	10%
التكامل	—	—	—	10%
الأمن السيبراني	—	—	—	10%
قابلية التوسع	—	—	—	5%
التكلفة الكلية	—	—	—	5%

والميزة الأساسية لهذا الأسلوب أنه يمنع اتخاذ القرار اعتمادًا على معيار واحد، مثل الدقة أو السعر.

ثالث عشر: القاعدة الذهبية للاختيار

يمكن صياغة القاعدة العامة لاختيار الكاميرا في المعادلة التالية: (17)

النوع المناسب = الهدف الأمني + طبيعة المشهد + البيئة + الإضاءة + المسافة + مستوى التفاصيل + التكامل + المخاطر + دورة الحياة

وبذلك يصبح اختيار الكاميرا جزءًا من عملية التصميم الأمني، وليس عملية شراء منفصلة.

خلاصة الفصل الثالث

تناول هذا الفصل أنواع كاميرات المراقبة وخصائصها من خلال ثمانية مباحث مترابطة، بدأت بالتصنيف وفق التقنية، ثم التصنيف وفق الوظيفة، وانتقلت إلى الكاميرات الثابتة والمتحركة، والكاميرات الداخلية والخارجية، والكاميرات النهارية والليلية، ثم الكاميرات المتخصصة، وانتهت بمعايير اختيار النوع المناسب.

وقد أظهر التحليل أن تصنيف الكاميرات لا ينبغي أن ينظر إليه بوصفه تصنيفًا تجاريًا للمنتجات، وإنما بوصفه أداة من أدوات التصميم الأمني.

فالكاميرا ليست جهازًا مستقلًا، وإنما تمثل نقطة البداية في سلسلة تبدأ بالمشهد المادي وتنتهي بالمعلومة الأمنية والقرار.

ويمكن تلخيص هذه السلسلة في النموذج الآتي:

الخطر الأمني ← الهدف الأمني ← الوظيفة المطلوبة ← طبيعة المشـــهد ← اختيار الكاميرا ← اختيار العدسة ← ظروف الإضاءة ← الشبكة ← التسجيل والتخزين ← التحليل ← المراقبة ← الاستجابة

ومن هنا فإن جودة المنظومة لا تتحدد بامتلاك كاميرات ذات مواصفات مرتفعة، وإنما بمدى ملاءمة هذه الكاميرات للوظائف التي صممت المنظومة من أجلها.

كما يتضح أن الانتقال من مفهوم "الكاميرا الأفضل" إلى مفهوم "الكاميرا الأنسب" يمثل تحولًا جوهريًا في التفكير الأمني والهندسي.

فالاختيار الصحيح هو الذي يحقق الوظيفة الأمنية المطلوبة ضمن القيود البيئية والتقنية والاقتصادية والتشغيلية، مع مراعاة الأمن السيبراني والتكامل وقابلية التوسع ودورة حياة النظام.

وتؤكد المعايير المهنية الحديثة هذا الاتجاه؛ إذ تنظر IEC 62676-4:2025 إلى نظام المراقبة ضمن دورة حياة تبدأ بالتخطيط والتصميم وتمتد إلى التركيب والاختبار والتشغيل والصيانة، بينما توفر ONVIF آليات معيارية للتشغيل البيني بين أجهزة وأنظمة الفيديو المتوافقة.(18)

أهم نتائج الفصل الثالث

١. تصنيف كاميرات المراقبة ينبغي أن يخدم عملية التصميم وليس مجرد وصف المنتجات.

٢. التقنية المستخدمة في الكاميرا تؤثر في الشبكة والتسجيل والتخزين والإدارة.

٣. الوظيفة الأمنية هي نقطة الانطلاق الصحيحة لاختيار الكاميرا.

٤. الكاميرات الثابتة توفر مراقبة مستمرة لمناطق محددة.

٥. الكاميرات المتحركة توفر مرونة أعلى لكنها لا تلغي الحاجة إلى التغطية الثابتة في المناطق الحرجة.

٦. البيئة الداخلية والخارجية تفرض متطلبات مختلفة على الكاميرا والتركيب.

٧. الأداء الليلي يجب تقييمه في ظروف الإضاءة الحقيقية.

٨. الكاميرات المتخصصة تستخدم عندما تكون هناك وظيفة أمنية محددة تستدعي خصائص خاصة.
٩. الكاميرا ذات الدقة الأعلى ليست بالضرورة الكاميرا الأفضل.
١٠. العدسة والمسافة والإضاءة وزاوية التصوير قد تكون أهم من زيادة الدقة وحدها.
١١. الأمن السيبراني أصبح جزءًا من معايير اختيار الكاميرا الشبكية.
١٢. ينبغي التحقق من التشغيل البيني الفعلي بدل الاكتفاء بعبارة عامة عن دعم ONVIF.
١٣. يجب تقييم الكاميرا ضمن بقية عناصر المنظومة.
١٤. الاختبار الميداني ينبغي أن يسبق اعتماد الكاميرا في التطبيقات الأمنية الحساسة.
١٥. التكلفة الحقيقية للكاميرا هي تكلفة دورة حياتها، وليس سعر الشراء فقط.

أسئلة التفكير والتقييم للفصل الثالث

أولًا: أسئلة معرفية

١. ما أبرز أسس تصنيف كاميرات المراقبة؟
٢. ما الفرق بين التصنيف وفق التقنية والتصنيف وفق الوظيفة؟
٣. ما أهم خصائص الكاميرات الثابتة؟
٤. ما أهم خصائص الكاميرات المتحركة؟
٥. ما المقصود بالكاميرات المتخصصة؟
٦. ما العوامل التي تؤثر في اختيار نوع الكاميرا؟
٧. ما أهمية الإضاءة في تصميم نظام المراقبة؟
٨. ما العلاقة بين الكاميرا والعدسة ومجال الرؤية؟

ثانيًا: أسئلة تحليلية

٩. ناقش العبارة: "الكاميرا الأعلى دقة ليست بالضرورة الأفضل أمنيًا".

١٠. حلل أسباب فشل كاميرا ذات مواصفات تقنية مرتفعة في تحقيق الهدف الأمني.

١١. قارن بين استخدام الكاميرات الثابتة والكاميرات المتحركة في حماية محيط منشأة كبيرة.

١٢. ناقش العلاقة بين الوظيفة الأمنية ونوع الكاميرا.

١٣. كيف يؤثر اختيار الكاميرا في متطلبات الشبكة والتخزين؟

١٤. لماذا ينبغي إدخال الأمن السيبراني ضمن عملية اختيار الكاميرات؟

١٥. ما أثر سوء الإضاءة في القيمة الأمنية للصورة؟

ثالثًا: أسئلة تطبيقية

١٦. اختر منشأة إدارية وحدد أنواع الكاميرات المناسبة لمداخلها ومخارجها وممراتها ومواقفها ومحيطها.

١٧. صمم نظامًا يجمع بين كاميرات ثابتة ومتحركة لمنشأة واسعة.

١٨. حدد الكاميرا المناسبة لمراقبة مدخل منشأة خلال النهار والليل، مع بيان أسباب الاختيار.

١٩. صمم مصفوفة تقييم لثلاث كاميرات مختلفة.

٢٠. ضع نموذج اختبار قبول ميداني لكاميرا جديدة.

٢١. حدد خمسة أخطاء محتملة في اختيار الكاميرات، واشرح أثر كل خطأ على الأداء الأمني.

المراجع:

① ينظر: International Electrotechnical Commission, *IEC 62676-4:2025*, (Geneva: IEC, 2025), sections on selection criteria.

② راجع: Lieberman, A. G., et al., *Video Surveillance Equipment Selection and Application Guide*, NIJ Guide 200-98.

③ ينظر: IEC 62676-4:2025, sections on security objective.

④ راجع: IEC 62676-4:2025, sections on scene analysis.

⑤ ينظر: Michael Harris, *CCTV and Video Surveillance*, p. 445 .

⑥ راجع: IEC 62676-4:2025, sections on image requirements.

⑦ ينظر: IEC 62676-4:2025, sections on lighting assessment.

⑧ راجع: IEC 62676-4:2025, sections on environmental assessment.

⑨ ينظر: ONVIF, *ONVIF Profiles*, (San Ramon: ONVIF).

⑩ راجع: ONVIF, *ONVIF Profiles*, official profile-conformance guidance.

⑪ ينظر: National Institute of Standards and Technology, *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*, NIST SP 800-213, (Gaithersburg, MD: NIST, 2021).

⑫ راجع: NIST SP 800-213 .

⑬ ينظر: IEC 62676-4:2025, sections on scalability.

⑭ راجع: IEC 62676-4:2025, sections on total cost of ownership.

⑮ ينظر: IEC 62676-4:2025, sections on acceptance testing.

⑯ راجع: Lieberman, A. G., et al., *Video Surveillance Equipment Selection and Application Guide*, NIJ Guide 200-98.

⑰ ينظر: IEC 62676-4:2025, sections on selection equation.

الفصل الثاني: تصميم منظومة المراقبة

تمهيد الفصل

يمثل تصـــميم منظومة المراقبة المرحلة التي تتحول فيها المتطلبات الأمنية إلى حل فني ملموس. فبعد أن تناولت الفصـول السـابقة مفهوم المنظومة ومكوناتها وأنواع الكاميرات وخصـــائصـــها، ينتقل هذا الفصـــل إلى معالجة كيفية تصـــميم منظومة مراقبة تلبي الاحتياجات الأمنية الفعلية للمنشأة، ضمن القيود التقنية والبيئية والاقتصادية.(1)

ولا ينبغي النظر إلى تصـــميم المنظومة باعتباره عملية تركيب أجهزة، وإنما باعتباره عملية هندســـية أمنية متكاملة تبدأ بتحليل الاحتياجات والمخاطر، وتمتد إلى تحديد نقاط المراقبة وتوزيع الكاميرات واختيار العدســـات والارتفاعات، وتنتهي بمراجعة التصميم واختباره قبل التنفيذ.(2)

ويكتســـب هذا الفصـــل أهمية خاصـــة لأنه يمثل نقطة الالتقاء بين الجانب النظري والجانب التطبيقي، ويحدد مدى قدرة المنظومة على تحقيق غرضها الأمني. فالتصميم الخاطئ قد يؤدي إلى وجود منظومة عالية التكلفة ومنخفضـــة الفاعلية، في حين أن التصميم الصحيح قد يحقق نتائج أمنية متميزة بتكلفة معقولة.(3)

ويتناول هذا الفصـــل عشـــرة مباحث: تحديد أهداف المراقبة، وتحليل الموقع، وتحليل المخاطر، وتحديد المناطق ذات الأولوية، وتحديد نقاط المراقبة، وتوزيع الكاميرات، وزوايا الرؤية والارتفاعات، والمناطق العمياء، والتكامل بين نقاط المراقبة، ومراجعة التصميم واختباره.

المبحث الأول: تحديد أهداف المراقبة

يُعدّ تحديد أهداف المراقبة الخطوة الأولى والأساسية في عملية تصميم منظومة المراقبة، إذ إن جميع القرارات اللاحقة - من اختيار الكاميرات إلى توزيعها إلى تحديد متطلبات التسجيل والتحليل - تتوقف على وضوح هذه الأهداف.(1)
ويكتسب هذا المبحث أهمية خاصة لأنه يمنع الوقوع في أحد أكثر الأخطاء شيوعًا في تصميم منظومات المراقبة، وهو البدء من الأجهزة والمواصفات التقنية بدلًا من البدء من الاحتياجات الأمنية الفعلية. فالسؤال الصحيح ليس "ما الكاميرا التي سنشتريها؟" وإنما "ما الذي نريد من المنظومة أن تحققه؟.(2) "

أولًا: مفهوم أهداف المراقبة
يمكن تعريف أهداف المراقبة بأنها :النتائج الأمنية المحددة التي يُراد من منظومة المراقبة تحقيقها، والتي توجه قرارات التصميم والتنفيذ والتشغيل والتقييم .(3)
وتتميز أهداف المراقبة بخصائص عدة:

- التحديد :أن تكون واضحة ومحددة وقابلة للقياس.
- الواقعية :أن تكون قابلة للتحقيق ضمن الموارد المتاحة.
- الارتباط :أن ترتبط بالمخاطر والاحتياجات الأمنية الفعلية.
- القابلية للتقييم :أن يمكن قياس مدى تحقيقها.(4)

ثانيًا: تصنيف أهداف المراقبة
يمكن تصنيف أهداف المراقبة وفق معايير متعددة:(5)
التصنيف الأول: وفق الوظيفة الأمنية

- أهداف وقائية :منع وقوع الحوادث من خلال الردع والكشف المبكر.
- أهداف كشفية :اكتشاف الأحداث عند وقوعها أو قبل وقوعها.
- أهداف استجابية :دعم الاستجابة السريعة والفعالة.
- أهداف توثيقية :توثيق الأحداث لدعم التحقيق والمساءلة.

التصنيف الثاني: وفق النطاق

- أهداف عامة: مراقبة الموقع بصورة شاملة.
- أهداف محددة: مراقبة مناطق أو أحداث أو أهداف معينة.

التصنيف الثالث: وفق المستوى

- أهداف استراتيجية: الأهداف طويلة المدى المرتبطة بالاستراتيجية الأمنية.
- أهداف تكتيكية: الأهداف متوسطة المدى المرتبطة بالعمليات الأمنية.
- أهداف تشغيلية: الأهداف قصيرة المدى المرتبطة بالتشغيل اليومي.(6)

ثالثًا: خطوات تحديد أهداف المراقبة

يمكن تحديد أهداف المراقبة من خلال الخطوات التالية:(7)

الخطوة الأولى: تحديد الأصول

- ما الأصول التي يجب حمايتها؟ (الأشخاص، الممتلكات، المعلومات، العمليات)
- ما قيمة كل أصل؟
- ما أهمية كل أصل للاستمرارية؟

الخطوة الثانية: تحديد التهديدات

- ما التهديدات المحتملة لكل أصل؟
- ما احتمالية كل تهديد؟
- ما مصدر كل تهديد؟

الخطوة الثالثة: تحديد الاحتياجات

- ما المعلومات التي نحتاج إليها؟
- متى نحتاج إليها؟
- من يحتاج إليها؟
- كيف ستُستخدم؟

الخطوة الرابعة: صياغة الأهداف

- صياغة أهداف محددة وقابلة للقياس.

- ربط الأهداف بالمخاطر والاحتياجات.
- تحديد مؤشرات قياس تحقيق الأهداف.(8)

رابعًا: نماذج لأهداف المراقبة

يمكن تحديد نماذج لأهداف المراقبة وفق طبيعة المنشأة:(9)

1. المنشآت الحيوية
   - حماية الأصول الحيوية من التهديدات.
   - ضمان استمرارية العمليات.
   - الكشف المبكر عن التهديدات.
   - دعم الاستجابة للطوارئ.
2. المنشآت التجارية
   - منع السرقة والاختلاس.
   - مراقبة العملاء والموظفين.
   - توثيق المعاملات.
   - حماية الممتلكات.
3. المنشآت الصناعية
   - مراقبة العمليات الإنتاجية.
   - ضمان السلامة المهنية.
   - منع التخريب.
   - حماية المواد الخطرة.
4. المنشآت التعليمية
   - حماية الطلاب والموظفين.
   - منع التسلل.
   - مراقبة المرافق.
   - دعم التحقيق في الحوادث.(10)

خامسًا: أخطاء تحديد أهداف المراقبة

هناك عدة أخطاء شائعة في تحديد أهداف المراقبة، ينبغي تجنبها:(11)

1. الغموض

صياغة أهداف عامة غير محددة، مثل "تحسين الأمن" أو "المراقبة الشاملة."

2. المبالغة

تحديد أهداف غير واقعية تتجاوز قدرات المنظومة والموارد المتاحة.

3. الانفصال عن المخاطر

تحديد أهداف لا ترتبط بالمخاطر الفعلية للمنشأة.

4. إهمال القياس

عدم تحديد مؤشرات لقياس مدى تحقيق الأهداف.

5. الجمود

عدم مراجعة الأهداف مع تغير الظروف والمخاطر.(12)

سادسًا: العلاقة بين أهداف المراقبة وتصميم المنظومة

تُعدّ أهداف المراقبة الأساس الذي يبنى عليه التصميم، إذ إنها تحدد:(13)

- نطاق التغطية: ما المناطق التي يجب تغطيتها؟
- مستوى التفاصيل: ما مستوى التفاصيل المطلوب؟
- متطلبات الجودة: ما جودة الصورة المطلوبة؟
- متطلبات التسجيل: ما مدة الاحتفاظ المطلوبة؟
- متطلبات التحليل: هل نحتاج إلى تحليلات ذكية؟
- متطلبات التكامل: هل نحتاج إلى تكامل مع أنظمة أخرى؟
- متطلبات الاستجابة: ما سرعة الاستجابة المطلوبة؟.(14)

المراجع:

① راجع International Electrotechnical Commission, *IEC 62676-4: Video surveillance systems for use in security applications – Part 4: Application guidelines*, (Geneva: IEC, 2nd ed., 2025), sections on objectives.

② ينظر: Lieberman, A. G., Atkinson, D. J., Pietrasiewicz, V. J., and Junker, K. E., *Video Surveillance Equipment Selection and Application Guide*, NIJ Guide 200-98, (Gaithersburg: National Institute of Standards and Technology / National Institute of Justice).

③ راجع: IEC 62676-4:2025, sections on security objectives.

④ ينظر: Lieberman, A. G., et al., *Video Surveillance Equipment Selection and Application Guide*.

⑤ راجع: IEC 62676-4:2025, sections on objective classification.

⑥ ينظر: David Brown, *Integrated Security Systems Design*, (New York: Butterworth-Heinemann, 3rd Edition, 2019), p. 45.

⑦ راجع: IEC 62676-4:2025, sections on objective setting.

⑧ ينظر: Lieberman, A. G., et al., *Video Surveillance Equipment Selection and Application Guide*.

⑨ راجع: IEC 62676-4:2025, sections on sector-specific objectives.

⑩ ينظر: Brown, *Integrated Security Systems Design*, p. 67.

⑪ راجع: IEC 62676-4:2025, sections on common errors.

⑫ ينظر: Lieberman, A. G., et al., *Video Surveillance Equipment Selection and Application Guide*.

⑬ راجع: IEC 62676-4:2025, sections on objectives and design.

⑭ ينظر: Brown, *Integrated Security Systems Design*, p. 89.

المبحث الثاني: تحليل الموقع

بعد أن تناول المبحث السابق تحديد أهداف المراقبة، ينتقل هذا المبحث إلى تحليل الموقع، وهو الخطوة التي تسبق تصميم المنظومة، إذ توفر المعلومات اللازمة عن البيئة التي ستعمل فيها المنظومة، وتساعد على تحديد التحديات والفرص.(1)
ويكتسب هذا المبحث أهمية خاصة لأنه يمنع الوقوع في أحد الأخطاء الشائعة في تصميم منظومات المراقبة، وهو تصميم المنظومة بناءً على افتراضات غير دقيقة عن الموقع، مما يؤدي إلى وجود مناطق غير مغطاة أو تغطية غير مناسبة.(2)

أولًا: مفهوم تحليل الموقع

يمكن تعريف تحليل الموقع بأنه :عملية جمع وتحليل المعلومات المتعلقة بالموقع المطلوب مراقبته، بما في ذلك الخصائص المادية والبيئية والتشغيلية، بهدف تحديد متطلبات التصميم والتحديات المحتملة .(3)
ويشمل تحليل الموقع عدة جوانب:

- الجوانب المادية :المباني، والأسوار، والبوابات، والممرات.
- الجوانب البيئية :الإضاءة، والظروف الجوية، والعوائق.
- الجوانب التشغيلية :الحركة، والأنشطة، والأوقات.
- الجوانب الأمنية :نقاط الضعف، والمناطق الحساسة، والتهديدات.(4)

ثانيًا: عناصر تحليل الموقع

يشمل تحليل الموقع عدة عناصر رئيسة:(5)

1. المسح المادي
   - المساحة :ما مساحة الموقع؟
   - المباني :ما عدد المباني وارتفاعاتها؟
   - الأسوار :ما نوع الأسوار وارتفاعاتها؟
   - البوابات :ما عدد البوابات ومواقعها؟

- الممرات : ما شبكة الممرات والطرق؟
- المداخل : ما عدد المداخل ومواقعها؟
- المخارج : ما عدد المخارج ومواقعها؟

2. المسح البيئي

- الإضاءة : ما مصادر الإضاءة الطبيعية والصناعية؟
- الظروف الجوية : ما الظروف الجوية السائدة؟
- العوائق : ما العوائق الطبيعية أو الصناعية؟
- التضاريس : ما طبيعة التضاريس؟
- الغطاء النباتي : ما الأشجار والنباتات؟

3. المسح التشغيلي

- الحركة : ما أنماط حركة الأشخاص والمركبات؟
- الأنشطة : ما الأنشطة التي تجري في الموقع؟
- الأوقات : ما أوقات الذروة والهدوء؟
- الموظفون : ما عدد الموظفين وتوزيعهم؟
- الزوار : ما عدد الزوار وتوزيعهم؟

4. المسح الأمني

- نقاط الضعف : ما نقاط الضعف في الموقع؟
- المناطق الحساسة : ما المناطق الحساسة؟
- التهديدات : ما التهديدات المحتملة؟
- الحوادث السابقة : ما الحوادث السابقة؟.(6)

ثالثًا: أدوات تحليل الموقع

يمكن استخدام عدة أدوات لتحليل الموقع:(7)

1. الزيارات الميدانية

- زيارة الموقع في أوقات مختلفة.

- تصوير الموقع من زوايا متعددة.
- تسجيل الملاحظات.

2. المخططات والخرائط
   - الحصول على مخططات الموقع.
   - دراسة الخرائط الطبوغرافية.
   - رسم خرائط تفصيلية.
3. الاستشعار عن بعد
   - استخدام الصور الجوية.
   - استخدام صور الأقمار الصناعية.
   - استخدام الطائرات بدون طيار.
4. المقابلات
   - مقابلة مسؤولي الأمن.
   - مقابلة الموظفين.
   - مقابلة السكان المجاورين.
5. البيانات التاريخية
   - دراسة سجلات الحوادث.
   - دراسة تقارير الأمن.
   - دراسة شكاوى الموظفين.(8)

رابعًا: مخرجات تحليل الموقع

ينتج عن تحليل الموقع عدة مخرجات:(9)

1. خريطة الموقع
   - خريطة تفصيلية للموقع.
   - تحديد المباني والأسوار والبوابات.
   - تحديد الممرات والطرق.

- تحديد المناطق الحساسة.

2. تقرير تحليل الموقع
   - وصف الموقع.
   - تحليل المخاطر.
   - تحديد نقاط الضعف.
   - تحديد الفرص.
3. قاعدة بيانات الموقع
   - بيانات المباني.
   - بيانات الأسوار.
   - بيانات البوابات.
   - بيانات الممرات.
   - بيانات الإضاءة.(10)

خامسًا: تحديات تحليل الموقع

يواجه تحليل الموقع عدة تحديات:(11)

1. التغيرات الموسمية
   - تغير الإضاءة بين الفصول.
   - تغير الغطاء النباتي.
   - تغير الظروف الجوية.
2. التغيرات التشغيلية
   - تغير أنماط الحركة.
   - تغير الأنشطة.
   - تغير الأوقات.
3. التغيرات العمرانية
   - توسعات مستقبلية.

- مشاريع تطوير.
- تغيرات في البنية التحتية.

4. القيود

- قيود الميزانية.
- قيود الوقت.
- قيود الوصول.(12)

المراجع:

①راجع: International Electrotechnical Commission, *IEC 62676-4:2025*, (Geneva: IEC, 2025), sections on site survey.

②ينظر: Lieberman, A. G., et al., *Video Surveillance Equipment Selection and Application Guide*, NIJ Guide 200-98.

③راجع: IEC 62676-4:2025, sections on site analysis.

④ينظر: David Brown, *Integrated Security Systems Design*, p. 112.

⑤راجع: IEC 62676-4:2025, sections on site survey elements.

⑥ينظر: Lieberman, A. G., et al., *Video Surveillance Equipment Selection and Application Guide*.

⑦راجع: IEC 62676-4:2025, sections on site survey tools.

⑧ينظر: Brown, *Integrated Security Systems Design*, p. 134.

⑨راجع: IEC 62676-4:2025, sections on site survey outputs.

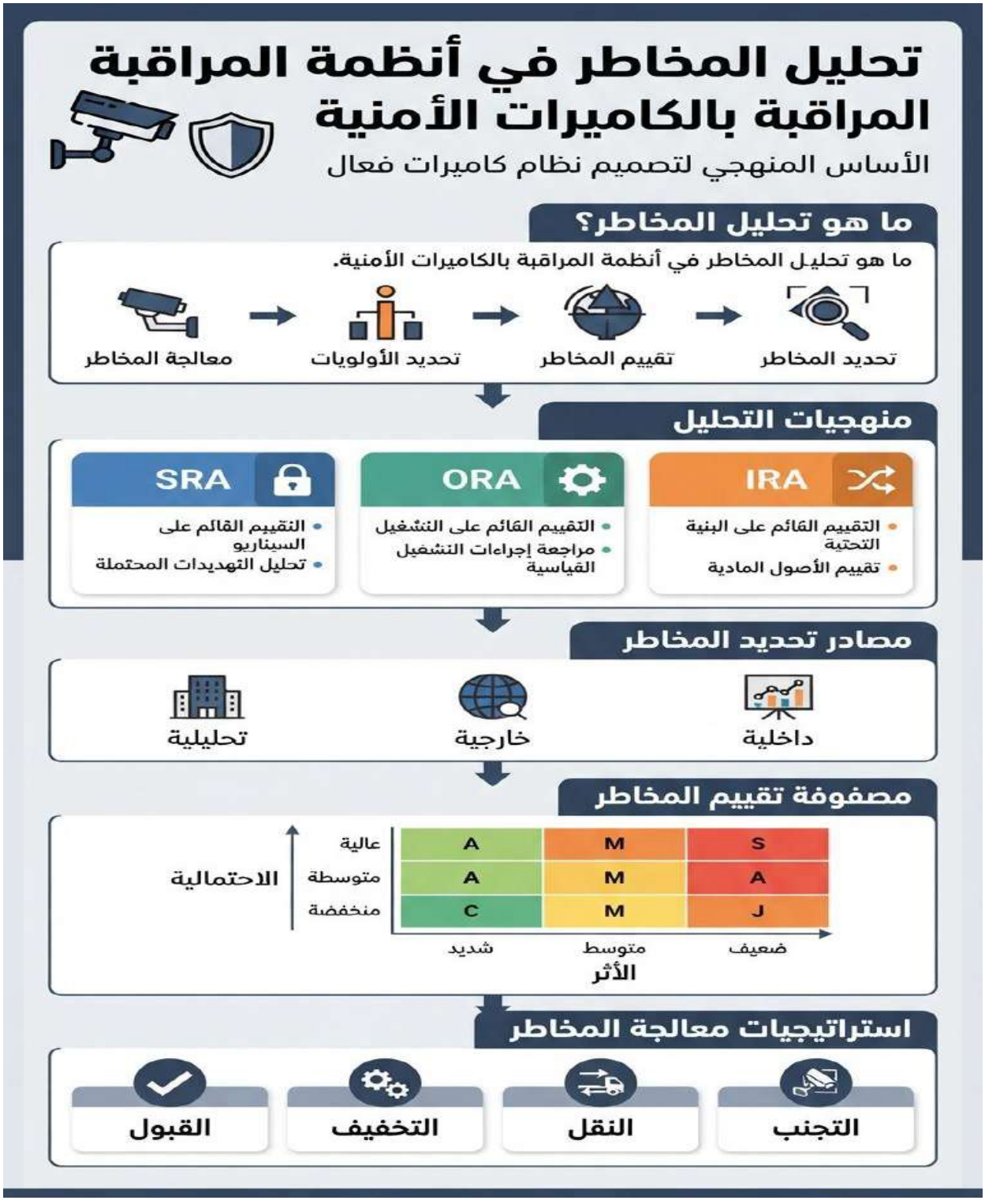
⑩ينظر: Lieberman, A. G., et al., *Video Surveillance Equipment Selection and Application Guide*.

⑪راجع: IEC 62676-4:2025, sections on site survey challenges.

⑫ينظر: Brown, *Integrated Security Systems Design*, p. 156.

المبحث الثالث: تحليل المخاطر في المنظومة الأمنية

أولًا: مفهوم تحليل المخاطر من الزاوية الأمنية "في السـياق الأمني، تحليل المخاطر ليس مجرد عملية إدارية، بل هو العقل الذي يوجّه كل قرار أمني في المنشـأة. فهو الذي يحدد ما يجب حمايته فعلاً، ومن أي تهديد، وكيف نحميه بالكاميرات.



١. تحديد المخاطر من زاوية أمنية: في الجانب الأمني، تحديد المخاطر يعني الإجابة عن سؤال: ما الذي يهدد أمن المنشأة؟ وهنا لا نتحدث عن مخاطر عامة، بل عن مخاطر أمنية محددة مثل:

a) التسلل :دخول أشخاص غير مصرح لهم إلى المنشأة أو مناطقها الحساسة.
b) السرقة :سرقة الممتلكات أو المعدات أو المعلومات.
c) التخريب :إتلاف الممتلكات أو الأنظمة عمداً.
d) الاعتداء :الإضرار بالأفراد العاملين أو الزوار.
e) الاختراق المعلوماتي :الوصول غير المصرح به إلى الأنظمة والبيانات.
f) الإرهاب :أعمال عنف تستهدف المنشأة أو العاملين فيها.

وتحديد المخاطر أمنياً يعني أيضاً تحديد مصادرها: هل هي داخلية (من الموظفين أنفسهم)؟ أم خارجية (من الغرباء)؟ أم مشتركة؟

٢. تقييم المخاطر: في الجانب الأمني، التقييم يعني قياس أمرين:

- احتمالية وقوع الخطر :هل هذا الخطر محتمل الحدوث؟ وهل المنشأة مستهدفة أصلاً؟ فمثلاً، احتمال تعرض بنك للسرقة أعلى من احتمال تعرض مدرسة للسرقة المسلحة.
- تأثير الخطر :إذا وقع هذا الخطر، ما حجم الضرر؟ هل هو ضرر مالي محدود؟ أم ضرر يهدد استمرار المنشأة؟ أم ضرر يهدد حياة الأفراد؟

فمثلاً، خطر تسلل شخص إلى مستودع يحتوي على مواد عادية قد يكون تأثيره متوسطاً، بينما تسلل شخص إلى غرفة الخوادم قد يكون تأثيره شديداً جداً.

٣. ترتيب المخاطر من زاوية أمنية

بعد التقييم، تُرتَّب المخاطر حسب أولويتها الأمنية. فليس كل خطر يستحق نفس القدر من الاهتمام. فالخطر الذي يهدد الأرواح يختلف عن الخطر الذي يهدد الممتلكات، والخطر الذي يهدد الأصول الحيوية يختلف عن الخطر الذي يهدد أصولاً ثانوية.

وفي الترتيب الأمني، تُعطى الأولوية للمخاطر التي تجمع بين:

a) احتمالية عالية للوقوع.
b) تأثير شديد إذا وقعت.
c) ارتباط بأصول حيوية لا يمكن الاستغناء عنها.

٤. معالجة المخاطر من زاوية أمنية: المعالجة الأمنية تعني اتخاذ الإجراءات التي تقلل من المخاطر. وفي سياق الكاميرات الأمنية، المعالجة تعني تحديد:

a) أين تُثبَّت الكاميرات :في المداخل، المخارج، الممرات، المناطق الحساسة.
b) ما نوع الكاميرات :عالية الدقة، مقاومة للعوامل الجوية، ذات رؤية ليلية.
c) ما نظام التسجيل :مستمر أم عند الحركة، محلي أم سحابي.
d) من يراقب :حراس أمن أم نظام ذكي أم كلاهما.

ثانيًا: منهجيات تحليل المخاطر من زاوية أمنية

١. منهجية تحليل المخاطر الأمنية(SRA) : هذه المنهجية هي الأكثر ارتباطاً بالجانب الأمني، وتقوم على خمس خطوات:

تحديد الأصول :ما الذي نحميه؟ المباني، المعدات، البيانات، الأفراد، السمعة.
تحديد التهديدات :من أو ما الذي يهدد هذه الأصول؟ سارق، متسلل، مخرب، هاكر.
تحديد نقاط الضعف :أين الثغرات التي يمكن أن يستغلها التهديد؟ مدخل غير محمي، منطقة عمياء، نظام قديم.
تقييم المخاطر :ما مدى خطورة كل تهديد على كل أصل؟
تحديد الإجراءات :ما الإجراءات الأمنية المناسبة؟ ومنها تركيب الكاميرات في نقاط محددة.

٢. منهجية تحليل المخاطر التشغيلية(ORA) : هذه المنهجية تركز على العمليات التي لا يمكن للمنشأة أن تعمل بدونها. فمثلاً، في مستشفى، العملية الحرجة هي استمرار عمل غرف العمليات. وفي بنك، العملية الحرجة هي استمرار عمل أنظمة التحويلات.

وتقوم هذه المنهجية على:

a) تحديد العمليات الحرجة :ما الذي إذا توقف، توقف عمل المنشأة؟
b) تحديد التهديدات :ما الذي يهدد هذه العمليات؟ انقطاع كهرباء، عطل تقني، هجوم إلكتروني.
c) تقييم التأثير :ما حجم الخسارة إذا توقفت هذه العملية؟
d) تحديد الإجراءات :كيف نحمي هذه العمليات؟ ومنها توجيه الكاميرات نحو نقاط التحكم في هذه العمليات.

٣. منهجية تحليل المخاطر المتكاملة(IRA) : هذه المنهجية تجمع بين الأمني والتشغيلي، وتقدم صورة شاملة. فهي لا تنظر إلى الكاميرات كأداة أمنية فقط، بل كأداة لحماية سير

العمل أيضاً. فمثلاً، كاميرا في مستودع لا تحمي من السرقة فقط، بل تساعد في متابعة حركة البضائع وتجنب الأخطاء التشغيلية.

ثالثًا: تحديد المخاطر من زاوية أمنية

١. المصادر الداخلية

a) سجلات الحوادث السابقة: ماذا حدث في الماضي؟ سرقات، تخريبات، اعتداءات.

b) تقارير الأمن: ماذا لاحظ حراس الأمن؟ نقاط ضعف، سلوكيات مشبوهة.

c) مقابلات الموظفين: ماذا يقول العاملون؟ مناطق يشعرون فيها بعدم الأمان.

d) تحليل العمليات: أين توجد ثغرات في سير العمل يمكن استغلالها أمنياً؟

٢. المصادر الخارجية

a) إحصاءات الجريمة: ما معدلات الجريمة في المنطقة المحيطة؟

b) تقارير الجهات المختصة: ماذا توصي الشرطة والدفاع المدني؟

c) دراسات المخاطر: ماذا تقول الدراسات المتخصصة في أمن المنشآت؟

d) خبراء الأمن: ماذا يرون من خلال خبرتهم؟

٣. المصادر التحليلية

a) تحليل SWOT: ما نقاط القوة والضعف والفرص والتهديدات الأمنية؟

b) تحليل شجرة الأخطاء: ما الأسباب الجذرية للحوادث الأمنية المحتملة؟

c) تحليل السيناريوهات: ماذا لو حدث سيناريو معين؟ كيف نتعامل معه؟

رابعًا: تقييم المخاطر من زاوية أمنية

١. احتمالية الوقوع

a) عالية: المنشأة مستهدفة بشكل واضح، أو المنطقة المحيطة تشهد حوادث متكررة.

b) متوسطة: توجد مؤشرات على احتمال وقوع الخطر، لكنها ليست مؤكدة.

c) منخفضة: لا توجد مؤشرات تذكر على احتمال وقوع الخطر.

٢. التأثير

a) شديد: الخطر يهدد الأرواح، أو يوقف العمل، أو يسبب خسائر فادحة.

b) متوسط: الخطر يسبب خسائر مالية أو تشغيلية محدودة.

c) ضعيف: الخطر يسبب إزعاجاً أو خسائر بسيطة.

المصفوفة الأمنية لتقييم المخاطر

الاحتمالية / التأثير	ضعيف	متوسط	شديد
عالية	متوسط	مرتفع	مرتفع جدًا
متوسطة	منخفض	متوسط	مرتفع
منخفضة	منخفض	منخفض	متوسط

خامسًا: ترتيب المخاطر من زاوية أمنية: الترتيب الأمني للمخاطر يخضع لمعايير:

a) درجة الخطورة :الخطر الذي يهدد الأرواح أو الأصول الحيوية يأتي أولاً.
b) سهولة المعالجة :الخطر الذي يمكن معالجته بسرعة وبكلفة معقولة قد يُقدَّم.
c) التكلفة :الخطر الذي تكلفة معالجته أقل من تأثيره المحتمل يُقدَّم.
d) الوقت :الخطر الذي يحتاج وقت طويل في المعالجة قد يُقدَّم لبدء العمل عليه مبكراً.

سادسًا: معالجة المخاطر من زاوية أمنية

١. التجنب الأمني
a) تجنب الأنشطة التي تسبب مخاطر أمنية.
b) نقل الأنشطة إلى مواقع أقل خطراً.

مثال :نقل مخزن الأموال إلى منطقة أكثر حماية بدلاً من الاعتماد على الكاميرات فقط.

٢. التخفيف الأمني
a) تقليل احتمالية وقوع المخاطر.
b) تقليل تأثير المخاطر. ومثاله :تركيب كاميرات عالية الدقة في المناطق الحرجة، مع إضاءة كافية، وتسجيل مستمر، وتحليل ذكي للحركة.

٣. النقل الأمني
a) نقل المخاطر إلى طرف آخر.
b) مشاركة المخاطر مع طرف آخر.

مثال :التعاقد مع شركة أمن متخصصة لإدارة منظومة الكاميرات والاستجابة للإنذارات.

٤. القبول الأمني
a) قبول المخاطر عندما تكون منخفضة.
b) قبول المخاطر عندما تكون تكلفة المعالجة أعلى من التأثير.
c) مثال :قبول مخاطر السرقة البسيطة في مناطق غير حساسة بدلاً من تركيب كاميرات باهظة الثمن.

المبحث الرابع: تحديد المناطق ذات الأولوية

بعد أن تناول المبحث السابق تحليل المخاطر، ينتقل هذا المبحث إلى تحديد المناطق ذات الأولوية، وهي المناطق التي تتطلب مستوى أعلى من المراقبة بناءً على نتائج تحليل المخاطر.(1)

ويكتسب هذا المبحث أهمية خاصة لأنه يضمن توجيه الموارد نحو المناطق الأكثر أهمية، وتجنب التوزيع العشوائي للكاميرات، وتحقيق التوازن بين التغطية الشاملة والتركيز على المناطق الحرجة.(2)

أولًا: مفهوم المناطق ذات الأولوية

يمكن تعريف المناطق ذات الأولوية بأنها: المناطق التي تتطلب مستوى أعلى من المراقبة بناءً على قيمة الأصول، ومستوى المخاطر، وأهمية العمليات، والمتطلبات التنظيمية .(3)

وتتميز هذه المناطق بخصائص عدة:

- أهمية عالية: تحتوي على أصول ذات قيمة عالية.
- مخاطر مرتفعة: تتعرض لمخاطر مرتفعة.
- عمليات حرجة: تجري فيها عمليات حرجة.
- متطلبات تنظيمية: تخضع لمتطلبات تنظيمية خاصة.(4)

ثانيًا: معايير تحديد المناطق ذات الأولوية

يمكن تحديد المناطق ذات الأولوية بناءً على عدة معايير:(5)

1. قيمة الأصول
   - عالية: أصول ذات قيمة عالية (خزائن، مختبرات، غرف خوادم).
   - متوسطة: أصول ذات قيمة متوسطة (مكاتب، مخازن).
   - منخفضة: أصول ذات قيمة منخفضة (ممرات، مواقف).
2. مستوى المخاطر
   - مرتفع: مناطق تتعرض لمخاطر مرتفعة (مداخل رئيسية، محيط).
   - متوسط: مناطق تتعرض لمخاطر متوسطة (ممرات، مواقف).

- منخفض : مناطق تتعرض لمخاطر منخفضة (مناطق خدمية).

3. أهمية العمليات

- حرجة : عمليات حرجة لا يمكن إيقافها (غرف خوادم، مختبرات).
- مهمة : عمليات مهمة لكن يمكن تأجيلها (مكاتب، قاعات).
- عادية : عمليات عادية (ممرات، مواقف).

4. المتطلبات التنظيمية

- إلزامية : مناطق تخضع لمتطلبات تنظيمية إلزامية (بنوك، مستشفيات).
- موصى بها : مناطق تخضع لمتطلبات تنظيمية موصى بها.
- اختيارية : مناطق لا تخضع لمتطلبات تنظيمية.(6)

ثالثًا: تصنيف المناطق

يمكن تصنيف المناطق وفق مستويات الأولوية:(7)

1. المنطقة الأولى (أولوية عالية)

- المداخل الرئيسية.
- المخارج الرئيسية.
- الخزائن.
- غرف الخوادم.
- المختبرات.
- المناطق الحساسة.

2. المنطقة الثانية (أولوية متوسطة)

- المكاتب.
- قاعات الاجتماعات.
- المخازن.
- الممرات الرئيسية.
- مواقف السيارات.

3. المنطقة الثالثة (أولوية منخفضة)

- الممرات الفرعية.
- المناطق الخدمية.
- المناطق الخارجية البعيدة.
- المناطق غير المستخدمة.(8)

رابعًا: متطلبات المراقبة لكل منطقة

تختلف متطلبات المراقبة باختلاف مستوى الأولوية:(9)

1. المنطقة الأولى (أولوية عالية)
   - التغطية :تغطية كاملة.
   - الدقة :عالية (تحديد الهوية).
   - التسجيل :مستمر.
   - مدة الاحتفاظ :طويلة (٣٠-٩٠ يومًا).
   - التحليلات :متقدمة.
   - الاستجابة :فورية.
2. المنطقة الثانية (أولوية متوسطة)
   - التغطية :تغطية شاملة.
   - الدقة :متوسطة (التعرف).
   - التسجيل :عند الحركة أو مجدول.
   - مدة الاحتفاظ :متوسطة (١٥-٣٠ يومًا).
   - التحليلات :أساسية.
   - الاستجابة :سريعة.
3. المنطقة الثالثة (أولوية منخفضة)
   - التغطية :تغطية أساسية.
   - الدقة :منخفضة (المراقبة العامة).
   - التسجيل :عند الحركة.
   - مدة الاحتفاظ :قصيرة (٧-١٥ يومًا).

- التحليلات: محدودة.
- الاستجابة: عادية.(10)

خامسًا: خرائط المناطق ذات الأولوية

يمكن توثيق المناطق ذات الأولوية من خلال خرائط توضح:(11)

- المنطقة الأولى: باللون الأحمر.
- المنطقة الثانية: باللون الأصفر.
- المنطقة الثالثة: باللون الأخضر.

وتساعد هذه الخرائط في:

- تحديد توزيع الكاميرات.
- تحديد متطلبات كل منطقة.
- تحديد أولويات التطوير.
- تحديد أولويات الصيانة.(12)

المراجع:

① راجع: International Electrotechnical Commission, *IEC 62676-4:2025*, (Geneva: IEC, 2025), sections on priority areas.

② ينظر: Lieberman, A. G., et al., *Video Surveillance Equipment Selection and Application Guide*, NIJ Guide 200-98.

③ راجع: IEC 62676-4:2025, sections on priority classification.

④ ينظر: David Brown, *Integrated Security Systems Design*, p. 234 .

⑤ راجع: IEC 62676-4:2025, sections on priority criteria.

⑥ ينظر: Lieberman, A. G., et al., *Video Surveillance Equipment Selection and Application Guide*.

⑦ راجع: IEC 62676-4:2025, sections on area classification.

⑧ ينظر: Brown, *Integrated Security Systems Design*, p. 245 .

⑨ راجع: IEC 62676-4:2025, sections on surveillance requirements.

⑩ ينظر: Lieberman, A. G., et al., *Video Surveillance Equipment Selection and Application Guide*.

⑪ راجع: IEC 62676-4:2025, sections on priority maps.

⑫ ينظر: Brown, *Integrated Security Systems Design*, p. 256 .

المبحث الخامس: تحديد نقاط المراقبة

نقاط المراقبة: وهي المواقع المحددة التي ستوضع فيها الكاميرات لتحقيق الأهداف الأمنية.(1)

ويكتسب هذا المبحث أهمية خاصة لأنه يترجم نتائج تحليل الموقع وتحليل المخاطر وتحديد المناطق ذات الأولوية إلى مواقع محددة للكاميرات، ويحدد متطلبات كل نقطة من حيث الدقة ومجال الرؤية والوظيفة

أولًا: مفهوم نقاط المراقبة: يمكن تعريف نقاط المراقبة بأنها :المواقع المحددة التي ستوضع فيها الكاميرات(2) ، والتي تختار بناءً على الأهداف الأمنية والمناطق ذات الأولوية والمتطلبات التشغيلية .(3)

وتتميز نقاط المراقبة بخصائص عدة:

- التحديد :أن تكون محددة الموقع.
- الوظيفة :أن يكون لكل نقطة وظيفة محددة.
- التكامل :أن تتكامل مع النقاط الأخرى.
- الجدوى :أن تكون قابلة للتنفيذ.(4)

ثانيًا: معايير تحديد نقاط المراقبة : يمكن تحديدها بناءً على عدة معايير:(5)

1. الأهداف الأمنية
   - ما الهدف من كل نقطة؟ (مراقبة عامة، تعرف، تحقق، كشف)
   - ما مستوى التفاصيل المطلوب؟
   - ما نوع الأحداث المطلوب اكتشافها؟
2. المناطق ذات الأولوية
   - ما مستوى أولوية كل منطقة؟
   - ما متطلبات المراقبة لكل منطقة؟
   - ما مستوى التغطية المطلوب؟
3. طبيعة المشهد
   - ما طبيعة المشهد المطلوب مراقبته؟

- ما المسافة بين النقطة والهدف؟
- ما ظروف الإضاءة؟
- ما العوائق المحتملة؟

4. المتطلبات التشغيلية

- ما سهولة الوصول إلى النقطة؟
- ما متطلبات الصيانة؟
- ما متطلبات الطاقة؟
- ما متطلبات الشبكة؟.(6)

ثالثًا: أنواع نقاط المراقبة

يمكن تصنيف نقاط المراقبة وفق معايير متعددة:(7)

1. وفق الوظيفة

- نقاط المراقبة العامة :لتغطية مناطق واسعة.
- نقاط التعرف :للتعرف على الأشخاص أو المركبات.
- نقاط التحقق :للتحقق من الأحداث.
- نقاط الكشف :لاكتشاف أحداث محددة.

2. وفق الموقع

- نقاط المداخل :عند المداخل الرئيسية والفرعية.
- نقاط المخارج :عند المخارج الرئيسية والفرعية.
- نقاط الممرات :في الممرات الرئيسية والفرعية.
- نقاط المناطق الحساسة :في المناطق الحساسة.
- نقاط المحيط :على محيط المنشأة.

3. وفق النطاق

- نقاط قريبة :على مسافة قصيرة من الهدف.
- نقاط متوسطة :على مسافة متوسطة من الهدف.
- نقاط بعيدة :على مسافة طويلة من الهدف.(8)

رابعًا: توثيق نقاط المراقبة

يتم توثيق نقاط المراقبة من خلال:(9)

1. جدول نقاط المراقبة
   - رقم النقطة.
   - موقع النقطة.
   - وظيفة النقطة.
   - نوع الكاميرا.
   - نوع العدسة.
   - مجال الرؤية.
   - متطلبات الدقة.
2. خريطة نقاط المراقبة
   - تحديد مواقع النقاط على الخريطة.
   - رسم مجالات الرؤية.
   - تحديد المناطق المغطاة.
   - تحديد المناطق غير المغطاة.
3. بطاقة كل نقطة
   - وصف تفصيلي للنقطة.
   - صورة للموقع.
   - متطلبات التركيب.
   - متطلبات الصيانة.(10)

خامسًا: أخطاء تحديد نقاط المراقبة

هناك عدة أخطاء شائعة في تحديد نقاط المراقبة، ينبغي تجنبها:(11)

1. التوزيع العشوائي

توزيع الكاميرات دون دراسة أو تخطيط.

2. التكرار

وضع أكثر من كاميرا لنفس الغرض في نفس المنطقة.

3. الإغفال

إغفال بعض المناطق المهمة.

4. سوء الاختيار

اختيار مواقع غير مناسبة للكاميرات.

5. عدم التوثيق

عدم توثيق نقاط المراقبة ووظائفها.(12)

المراجع:

① راجع: International Electrotechnical Commission, *IEC 62676-4:2025*, (Geneva: IEC, 2025), sections on camera positions.

② ينظر: Lieberman, A. G., et al., *Video Surveillance Equipment Selection and Application Guide*, NIJ Guide 200-98.

③ راجع: IEC 62676-4:2025, sections on surveillance points.

④ ينظر: David Brown, *Integrated Security Systems Design*, p. 267.

⑤ راجع: IEC 62676-4:2025, sections on point selection criteria.

⑥ ينظر: Lieberman, A. G., et al., *Video Surveillance Equipment Selection and Application Guide*.

⑦ راجع: IEC 62676-4:2025, sections on point classification.

⑧ ينظر: Brown, *Integrated Security Systems Design*, p. 278.

⑨ راجع: IEC 62676-4:2025, sections on point documentation.

⑩ ينظر: Lieberman, A. G., et al., *Video Surveillance Equipment Selection and Application Guide*.

⑪ راجع: IEC 62676-4:2025, sections on common errors.

⑫ ينظر: Brown, *Integrated Security Systems Design*, p. 289.

المبحث السادس: توزيع الكاميرات

بعد أن تناول المبحث السابق تحديد نقاط المراقبة، ينتقل هذا المبحث إلى توزيع الكاميرات، وهو عملية تحديد عدد الكاميرات ونوعها في كل نقطة، وتحقيق التوازن بين التغطية الشاملة والتركيز على المناطق الحرجة.(1)

ويكتسب هذا المبحث أهمية خاصة لأنه يحدد كيفية توزيع الموارد بين النقاط المختلفة، ويضمن تحقيق التغطية المطلوبة بأقل عدد ممكن من الكاميرات، ويجنب الإفراط أو التفريط في التغطية.(2)

أولًا: مفهوم توزيع الكاميرات

يمكن تعريف توزيع الكاميرات بأنه :عملية تحديد عدد الكاميرات ونوعها ومواصفاتها في كل نقطة مراقبة، بهدف تحقيق التغطية المطلوبة بأقل تكلفة ممكنة .(3)

ويتضمن توزيع الكاميرات عدة قرارات:

- عدد الكاميرات :كم كاميرا في كل نقطة؟
- نوع الكاميرات :ما نوع الكاميرا في كل نقطة؟
- مواصفات الكاميرات :ما مواصفات كل كاميرا؟
- العدسات :ما نوع العدسة لكل كاميرا؟.(4)

ثانيًا: مبادئ توزيع الكاميرات

يخضع توزيع الكاميرات لعدة مبادئ:(5)

1. مبدأ التغطية
   - تغطية جميع المناطق ذات الأولوية.
   - تغطية المداخل والمخارج.
   - تغطية الممرات الرئيسية.
   - تغطية المناطق الحساسة.
2. مبدأ الاقتصاد
   - تحقيق التغطية بأقل عدد ممكن من الكاميرات.
   - تجنب التكرار غير الضروري.

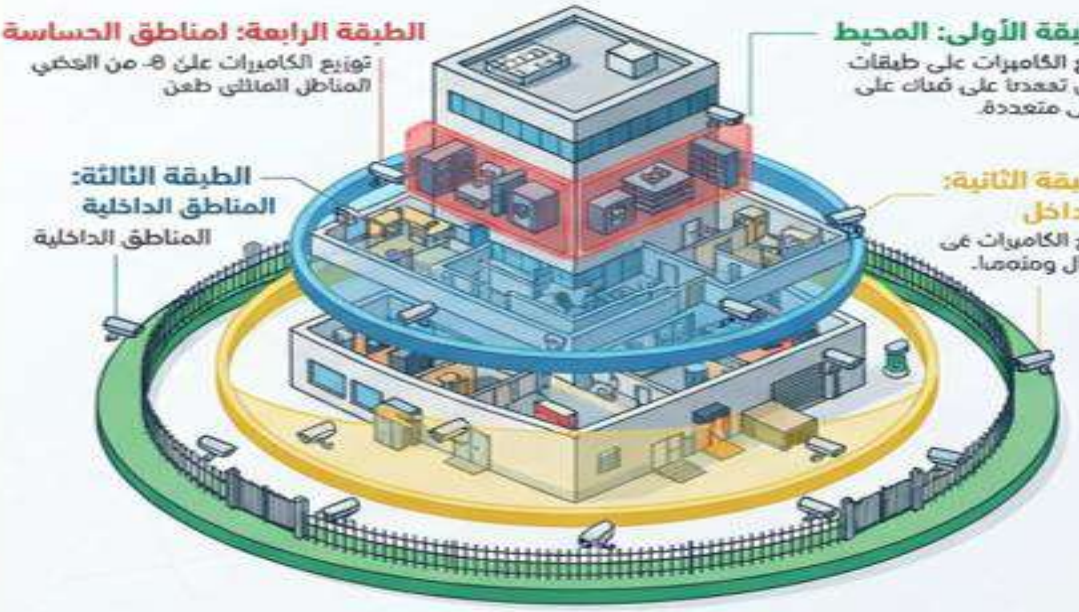
- استخدام الكاميرات متعددة العدسات عند الحاجة.

3. مبدأ التكامل
   - تكامل الكاميرات الثابتة والمتحركة.
   - تكامل الكاميرات الداخلية والخارجية.
   - تكامل الكاميرات النهارية والليلية.
4. مبدأ المرونة
   - إمكانية التوسع المستقبلي.
   - إمكانية التعديل والتطوير.
   - إمكانية التكامل مع أنظمة أخرى.(6)

ثالثًا: استراتيجيات توزيع الكاميرات: يمكن استخدام عدة استراتيجيات لتوزيع الكاميرات :(7)

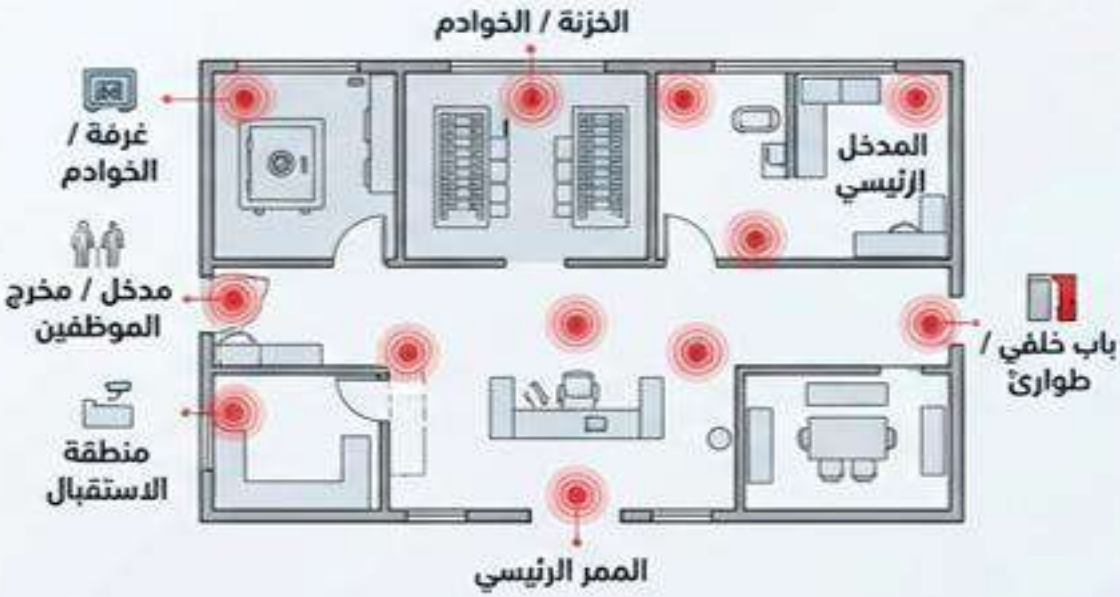
3 إستراتيجية الطبقات

توزيع الكاميرات على طبقات متعددة.



4 إستراتيجية النقاط الحرجة

توزيع الكاميرات في النقاط الحرجة فقط.



- مناسبة للمنشآت ذات المخاطر المحددة
- تتطلب عددًا قليلًا من الكاميرات

رابعًا: اعتبارات توزيع الكاميرات

المبحث السابع: زوايا الرؤية والارتفاعات

بعد أن تناول المبحث السابق توزيع الكاميرات، ينتقل هذا المبحث إلى زوايا الرؤية والارتفاعات، وهي العوامل التي تحدد جودة الصورة الناتجة وقدرتها على تحقيق الغرض الأمني.(1)

ويكتسب هذا المبحث أهمية خاصة لأنه يحدد كيفية توجيه الكاميرا وارتفاعها، مما يؤثر بصورة مباشرة في مجال الرؤية، ومستوى التفاصيل، وقدرة الكاميرا على تحقيق الوظيفة الأمنية المطلوبة.(2)

أولًا: مفهوم زوايا الرؤية

يمكن تعريف زاوية الرؤية بأنها: الزاوية التي تغطيها الكاميرا أفقياً أو رأسياً، وتحدد المساحة التي تظهر في الصورة .(3)

وتتأثر زاوية الرؤية بعدة عوامل:

- البعد البؤري للعدسة: كلما زاد البعد البؤري، ضاقت زاوية الرؤية.
- حجم المستشعر: كلما زاد حجم المستشعر، اتسعت زاوية الرؤية.
- المسافة بين الكاميرا والهدف: كلما زادت المسافة، اتسعت المساحة المغطاة(4)

ثانيًا: أنواع زوايا الرؤية

يمكن تصنيف زوايا الرؤية وفق معايير متعددة:(5)

1. وفق الاتجاه
   - زاوية أفقية: الزاوية الأفقية التي تغطيها الكاميرا.
   - زاوية رأسية: الزاوية الرأسية التي تغطيها الكاميرا.
   - زاوية قطرية: الزاوية القطرية التي تغطيها الكاميرا.
2. وفق الاتساع
   - زاوية واسعة: أكثر من ٦٠ درجة.
   - زاوية متوسطة: من ٣٠ إلى ٦٠ درجة.
   - زاوية ضيقة: أقل من ٣٠ درجة.
3. وفق التطبيق

- زاوية المراقبة العامة :لتغطية مساحات واسعة.
- زاوية التعرف :للتعرف على الأشخاص.
- زاوية القراءة :لقراءة اللوحات أو النصوص.(6)

ثالثًا: مفهوم الارتفاعات

يمكن تعريف ارتفاع الكاميرا بأنه :المسافة الرأسية بين الكاميرا ومستوى الأرض، والتي تحدد زاوية النظر وطبيعة الصورة الناتجة .(7)

ويؤثر ارتفاع الكاميرا في:

- مجال الرؤية :كلما زاد الارتفاع، اتسع مجال الرؤية.
- زاوية النظر :كلما زاد الارتفاع، زادت زاوية النظر للأسفل.
- جودة الصورة :كلما زاد الارتفاع، انخفضت جودة الصورة للتفاصيل.
- سهولة العبث :كلما زاد الارتفاع، صعب العبث بالكاميرا.(8)

رابعًا: معايير تحديد الارتفاعات

يمكن تحديد ارتفاع الكاميرا وفق عدة معايير:(9)

1. نوع الكاميرا
   - الكاميرات الثابتة :عادة ٢. ٥-٤ متر.
   - الكاميرات المتحركة :عادة ٣-٦ متر.
   - الكاميرات الخارجية :عادة ٣-٨ متر.
2. الوظيفة الأمنية
   - المراقبة العامة :ارتفاع أعلى (٤-٦ متر).
   - التعرف على الوجوه :ارتفاع أقل (٢-٣ متر).
   - قراءة اللوحات :ارتفاع محدد (١-٢ متر).
3. طبيعة المشهد
   - المداخل :ارتفاع ٢. ٥-٣ متر.
   - الممرات :ارتفاع ٣-٤ متر.
   - الساحات :ارتفاع ٤-٦ متر.

- المحيط :ارتفاع ٣-٦ متر.(10)

خامسًـــا: العلاقة بين زاوية الرؤية والارتفاع : توجد علاقة وثيقة بين زاوية الرؤية والارتفاع، يمكن تلخيصها في:(11)

- ارتفاع أعلى + زاوية أوسع = تغطية أوسع لكن تفاصيل أقل.
- ارتفاع أقل + زاوية أضيق = تغطية أضيق لكن تفاصيل أكثر.
- ارتفاع متوسط + زاوية متوسطة = توازن بين التغطية والتفاصيل.

ومن ثم فإن اختيار زاوية الرؤية والارتفاع يجب أن يكون متوازناً حســـب الغرض الأمني (12)

سـادسًـا: أخطاء تحديد زوايا الرؤية والارتفاعات: هناك عدة أخطاء شـائعة في تحديد زوايا الرؤية والارتفاعات، ينبغي تجنبها:(13)

1. الارتفاع المفرط
   - يؤدي إلى صورة من الأعلى لا تظهر التفاصيل.
   - يصعب التعرف على الوجوه.
2. الارتفاع المنخفض
   - يؤدي إلى صورة من الأسفل.
   - يسهل العبث بالكاميرا.
3. الزاوية الواسعة المفرطة
   - تؤدي إلى تشويه الصورة.
   - تصغر حجم الأهداف.
4. الزاوية الضيقة المفرطة
   - تؤدي إلى فقدان السياق.
   - تفوت الأحداث الجانبية.(14)

المراجع:

①راجع: International Electrotechnical Commission, *IEC 62676-4:2025*, (Geneva: IEC, 2025), sections on field of view.

②ينظر: Lieberman, A. G., et al., *Video Surveillance Equipment Selection and Application Guide*, NIJ Guide 200-98.

③راجع: IEC 62676-4:2025, sections on viewing angles.

④ ينظر: Michael Harris, *CCTV and Video Surveillance: Technology and Applications*, (Boston: McGraw-Hill, 4th Edition, 2020), p. 178.

⑤ راجع: IEC 62676-4:2025, sections on angle classification.

⑥ ينظر: Harris, *CCTV and Video Surveillance*, p. 189.

⑦ راجع: IEC 62676-4:2025, sections on camera heights.

⑧ ينظر: Lieberman, A. G., et al., *Video Surveillance Equipment Selection and Application Guide*.

⑨ راجع: IEC 62676-4:2025, sections on height criteria.

⑩ ينظر: Harris, *CCTV and Video Surveillance*, p. 201.

⑪ راجع: IEC 62676-4:2025, sections on angle-height relationship.

⑫ ينظر: Lieberman, A. G., et al., *Video Surveillance Equipment Selection and Application Guide*.

⑬ راجع: IEC 62676-4:2025, sections on common errors.

⑭ ينظر: Harris, *CCTV and Video Surveillance*, p. 212.

المبحث الثامن: المناطق العمياء

تُعدّ المناطق العمياء من أخطر التحديات التي تواجه منظومة المراقبة، إذ تمثل مناطق لا تغطيها الكاميرات، مما يسمح بحدوث أحداث دون رصد أو توثيق.(1)
ويكتسب هذا المبحث أهمية خاصة لأنه يضع الأساس لفهم كيفية تحديد المناطق العمياء ومعالجتها، مما يضمن تحقيق التغطية الشاملة للمنشأة.(2)

أولًا: مفهوم المناطق العمياء

يمكن تعريف المناطق العمياء بأنها :المناطق التي لا تغطيها أي كاميرا في المنظومة، أو التي تكون فيها التغطية غير كافية لتحقيق الغرض الأمني .(3)
وتنقسم المناطق العمياء إلى نوعين:

- مناطق عمياء كلية :لا تغطيها أي كاميرا.
- مناطق عمياء جزئية :تغطيها كاميرا لكن التغطية غير كافية.(4)

ثانيًا: أسباب المناطق العمياء

تنشأ المناطق العمياء لعدة أسباب:(5)

1. أسباب تصميمية
   - سوء توزيع الكاميرات.
   - اختيار خاطئ لزوايا الرؤية.
   - اختيار خاطئ للارتفاعات.
   - إهمال بعض المناطق.
2. أسباب فنية
   - محدودية مجال الرؤية.
   - العوائق المادية.
   - ظروف الإضاءة.
   - القيود التقنية.

3. أسباب تشغيلية
   - تغير الظروف التشغيلية.
   - تغير أنماط الحركة.
   - إضافة مبانٍ أو منشآت.
   - تغير استخدام المناطق.(6)

ثالثًا: أنواع المناطق العمياء

يمكن تصنيف المناطق العمياء وفق معايير متعددة:(7)

1. وفق الموقع
   - مناطق عمياء داخلية :داخل المباني.
   - مناطق عمياء خارجية :خارج المباني.
   - مناطق عمياء محيطية :على المحيط.
2. وفق السبب
   - مناطق عمياء تصميمية :بسبب سوء التصميم.
   - مناطق عمياء فنية :بسبب القيود التقنية.
   - مناطق عمياء تشغيلية :بسبب التغيرات التشغيلية.
3. وفق الخطورة
   - مناطق عمياء عالية الخطورة :في مناطق حساسة.
   - مناطق عمياء متوسطة الخطورة :في مناطق مهمة.
   - مناطق عمياء منخفضة الخطورة :في مناطق عادية.(8)

رابعًا: طرق تحديد المناطق العمياء

يمكن تحديد المناطق العمياء من خلال:(9)

1. الدراسة التصميمية
   - رسم مجالات الرؤية على المخططات.

- تحليل التغطية.
- تحديد المناطق غير المغطاة.

2. الفحص الميداني
   - زيارة الموقع.
   - فحص المناطق المشكوك فيها.
   - اختبار الكاميرات فعليًا.
3. المحاكاة
   - استخدام برامج المحاكاة.
   - اختبار سيناريوهات مختلفة.
   - تحليل النتائج.
4. المراجعة الدورية
   - مراجعة التغطية دوريًا.
   - تحديث الخرائط.
   - معالجة المناطق الجديدة.(10)

خامسًا: معالجة المناطق العمياء

يمكن معالجة المناطق العمياء من خلال:(11)

1. إضافة كاميرات
   - إضافة كاميرات في المناطق العمياء.
   - إضافة كاميرات متعددة العدسات.
   - إضافة كاميرات متحركة.
2. تعديل الكاميرات القائمة
   - تعديل زوايا الرؤية.
   - تعديل الارتفاعات.
   - تغيير العدسات.

3. استخدام تقنيات بديلة
   - استخدام أجهزة استشعار.
   - استخدام أنظمة إنذار.
   - استخدام حراسة بشرية.
4. تحسين التصميم
   - إعادة تصميم التغطية.
   - دمج النقاط.
   - تحسين التوزيع.(12)

المراجع:

① راجع: International Electrotechnical Commission, *IEC 62676-4:2025*, (Geneva: IEC, 2025), sections on blind spots.

② ينظر: Lieberman, A. G., et al., *Video Surveillance Equipment Selection and Application Guide*, NIJ Guide 200-98.

③ راجع: IEC 62676-4:2025, sections on blind spot definition.

④ ينظر: David Brown, *Integrated Security Systems Design*, p. 334.

⑤ راجع: IEC 62676-4:2025, sections on blind spot causes.

⑥ ينظر: Lieberman, A. G., et al., *Video Surveillance Equipment Selection and Application Guide*.

⑦ راجع: IEC 62676-4:2025, sections on blind spot classification.

⑧ ينظر: Brown, *Integrated Security Systems Design*, p. 345.

⑨ راجع: IEC 62676-4:2025, sections on blind spot identification.

⑩ ينظر: Lieberman, A. G., et al., *Video Surveillance Equipment Selection and Application Guide*.

⑪ راجع: IEC 62676-4:2025, sections on blind spot treatment.

⑫ ينظر: Brown, *Integrated Security Systems Design*, p. 356.

المبحث التاسع: التكامل بين نقاط المراقبة

بعد أن تناول المبحث السابق المناطق العمياء، ينتقل هذا المبحث إلى التكامل بين نقاط المراقبة، وهو العامل الذي يحول النقاط المنفردة إلى منظومة متكاملة قادرة على تحقيق التغطية الشاملة.(1)

ويكتسب هذا المبحث أهمية خاصة لأنه يضمن أن تعمل نقاط المراقبة بصورة متناسقة ومتكاملة، وأن تغطي كل نقطة ما لا تغطيه النقاط الأخرى، وأن تتداخل التغطيات لتجنب المناطق العمياء.(2)

أولًا: مفهوم التكامل بين نقاط المراقبة

يمكن تعريف التكامل بين نقاط المراقبة بأنه :التنسيق بين نقاط المراقبة المختلفة بحيث تعمل بصورة متناسقة ومتكاملة لتحقيق التغطية الشاملة للمنشأة .(3)

ويتضمن التكامل عدة جوانب:

- التكامل المكاني :تغطية النقاط للمساحات المختلفة.
- التكامل الزمني :تغطية النقاط للأوقات المختلفة.
- التكامل الوظيفي :تكامل وظائف النقاط المختلفة.
- التكامل التقني :تكامل التقنيات المستخدمة.(4)

ثانيًا: مستويات التكامل

يمكن تحقيق التكامل بين نقاط المراقبة على عدة مستويات:(5)

1. التكامل الأفقي
   - تكامل النقاط في نفس المستوى.
   - تغطية المساحات المختلفة.
   - تجنب التداخل غير الضروري.
2. التكامل الرأسي
   - تكامل النقاط في مستويات مختلفة.

- تغطية المناطق من زوايا مختلفة.
- تحقيق التغطية الشاملة.

3. التكامل الوظيفي
   - تكامل النقاط الثابتة والمتحركة.
   - تكامل النقاط الداخلية والخارجية.
   - تكامل النقاط النهارية والليلية.
4. التكامل التقني
   - تكامل الكاميرات المختلفة.
   - تكامل أنظمة التحليل.
   - تكامل أنظمة الإنذار.(6)

ثالثًا: استراتيجيات التكامل

يمكن تحقيق التكامل بين نقاط المراقبة من خلال عدة استراتيجيات:(7)

1. استراتيجية التداخل
   - تداخل مجالات الرؤية بين النقاط.
   - ضمان عدم وجود مناطق عمياء.
   - تحقيق التغطية المستمرة.
2. استراتيجية التتابع
   - تتابع النقاط على مسار معين.
   - تغطية المسار كاملاً.
   - ضمان متابعة الأهداف المتحركة.
3. استراتيجية الطبقات
   - توزيع النقاط على طبقات.
   - تغطية كل طبقة لنوع معين من الأحداث.
   - تحقيق التغطية الشاملة.

4. استراتيجية التخصص
   - تخصص كل نقطة لوظيفة معينة.
   - تكامل الوظائف المختلفة.
   - تحقيق التغطية المتكاملة.(8)

رابعًا: أدوات التكامل

يمكن استخدام عدة أدوات لتحقيق التكامل بين نقاط المراقبة:(9)

1. خرائط التغطية
   - رسم مجالات الرؤية لكل نقطة.
   - تحليل التداخل بين النقاط.
   - تحديد المناطق غير المغطاة.
2. برامج المحاكاة
   - محاكاة سيناريوهات مختلفة.
   - تحليل التغطية.
   - تحسين التوزيع.
3. أنظمة إدارة الفيديو
   - تكامل النقاط في منصة واحدة.
   - إدارة الأحداث.
   - تنسيق الاستجابة.(10)

خامسًا: فوائد التكامل

يحقق التكامل بين نقاط المراقبة عدة فوائد:(11)

1. التغطية الشاملة
   - تغطية جميع المناطق.
   - تجنب المناطق العمياء.

- تحقيق التغطية المستمرة.

2. تحسين الكشف
   - كشف الأحداث من زوايا متعددة.
   - تحسين دقة الكشف.
   - تقليل الإنذارات الكاذبة.
3. تحسين الاستجابة
   - توفير معلومات شاملة.
   - تسريع الاستجابة.
   - تحسين التنسيق.
4. تحسين التوثيق
   - توثيق الأحداث من زوايا متعددة.
   - تحسين جودة الأدلة.
   - دعم التحقيق.(12)

المراجع:

① راجع: International Electrotechnical Commission, *IEC 62676-4:2025*, (Geneva: IEC, 2025), sections on integration.

② ينظر: Lieberman, A. G., et al., *Video Surveillance Equipment Selection and Application Guide*, NIJ Guide 200-98.

③ راجع: IEC 62676-4:2025, sections on point integration.

④ ينظر: David Brown, *Integrated Security Systems Design*, p. 367.

⑤ راجع: IEC 62676-4:2025, sections on integration levels.

⑥ ينظر: Lieberman, A. G., et al., *Video Surveillance Equipment Selection and Application Guide*.

⑦ راجع: IEC 62676-4:2025, sections on integration strategies.

⑧ ينظر: Brown, *Integrated Security Systems Design*, p. 378.

⑨ راجع: IEC 62676-4:2025, sections on integration tools.

⑩ ينظر: Lieberman, A. G., et al., *Video Surveillance Equipment Selection and Application Guide*.

⑪ راجع: IEC 62676-4:2025, sections on integration benefits.

⑫ ينظر: Brown, *Integrated Security Systems Design*, p. 389.

المبحث العاشر: مراجعة التصميم واختباره

بعد أن تناولت المباحث السابقة جميع مراحل تصميم منظومة المراقبة، ينتقل هذا المبحث إلى مراجعة التصميم واختباره، وهي المرحلة النهائية التي تضمن أن التصميم يحقق الأهداف الأمنية المطلوبة، وأن المنظومة ستعمل بصورة صحيحة عند التنفيذ (1).

ويكتسب هذا المبحث أهمية خاصة لأنه يمنع تنفيذ تصميمات غير مكتملة أو غير دقيقة، ويضمن اكتشاف الأخطاء قبل التنفيذ، مما يوفر الوقت والتكلفة.(2)

أولًا: مفهوم مراجعة التصميم

يمكن تعريف مراجعة التصميم بأنها :عملية منهجية لتقييم التصميم المقترح لمنظومة المراقبة، للتأكد من أنه يحقق الأهداف الأمنية المطلوبة، وأنه قابل للتنفيذ، وأنه خالٍ من الأخطاء .(3)

وتهدف مراجعة التصميم إلى:

- التأكد من تحقيق الأهداف.
- اكتشاف الأخطاء.
- تحسين التصميم.
- تقليل المخاطر.(4)

ثانيًا: عناصر مراجعة التصميم

تشمل مراجعة التصميم عدة عناصر:(5)

1. مراجعة الأهداف
   - هل التصميم يحقق الأهداف الأمنية؟
   - هل التصميم يغطي جميع المناطق ذات الأولوية؟
   - هل التصميم يلبي المتطلبات التشغيلية؟
2. مراجعة التغطية

- هل التغطية شاملة؟
- هل هناك مناطق عمياء؟
- هل التداخل بين النقاط كافٍ؟

3. مراجعة المواصفات
   - هل الكاميرات مناسبة للغرض؟
   - هل العدسات مناسبة للمشهد؟
   - هل الزوايا والارتفاعات مناسبة؟
4. مراجعة التكامل
   - هل النقاط متكاملة؟
   - هل المنظومة متكاملة مع الأنظمة الأخرى؟
   - هل هناك تكامل تقني؟
5. مراجعة الجدوى
   - هل التصميم قابل للتنفيذ؟
   - هل التصميم ضمن الميزانية؟
   - هل التصميم مستدام؟.(6)

ثالثًا: منهجية مراجعة التصميم

يمكن مراجعة التصميم من خلال الخطوات التالية:(7)

الخطوة الأولى: المراجعة الداخلية

- مراجعة التصميم من قبل فريق التصميم.
- التحقق من استيفاء المتطلبات.
- اكتشاف الأخطاء الواضحة.

الخطوة الثانية: المراجعة الخارجية

- مراجعة التصميم من قبل خبير خارجي.
- تقييم موضوعي للتصميم.
- تقديم ملاحظات وتوصيات.

الخطوة الثالثة: المراجعة الميدانية

- زيارة الموقع.
- التحقق من دقة المعلومات.
- اختبار الافتراضات.

الخطوة الرابعة: المراجعة النهائية

- مراجعة التصميم النهائي.
- التأكد من معالجة الملاحظات.
- اعتماد التصميم.(8)

رابعًا: اختبار التصميم

يمكن اختبار التصميم من خلال عدة طرق:(9)

1. المحاكاة
   - استخدام برامج المحاكاة.
   - اختبار سيناريوهات مختلفة.
   - تحليل النتائج.
2. النماذج الأولية
   - تركيب نماذج أولية.
   - اختبار الأداء الفعلي.
   - تعديل التصميم.
3. الاختبار الميداني
   - تركيب كاميرات مؤقتة.
   - اختبار الأداء في الموقع.
   - تقييم النتائج.
4. اختبار القبول
   - وضع معايير القبول.

- اختبار المنظومة.
- اعتماد المنظومة.(10)

خامسًا: معايير قبول التصميم

يمكن قبول التصميم إذا استوفى المعايير التالية:(11)

1. معايير أمنية
   - تحقيق الأهداف الأمنية.
   - تغطية المناطق ذات الأولوية.
   - عدم وجود مناطق عمياء.
2. معايير فنية
   - مناسبة الكاميرات والعدسات.
   - مناسبة الزوايا والارتفاعات.
   - تكامل النقاط.
3. معايير تشغيلية
   - سهولة التشغيل.
   - سهولة الصيانة.
   - إمكانية التوسع.
4. معايير اقتصادية
   - ضمن الميزانية.
   - تكلفة تشغيل معقولة.
   - تكلفة صيانة معقولة.(12)

سادسًا: توثيق التصميم

يتم توثيق التصميم من خلال:(13)

1. المخططات

- مخططات التغطية.
- مخططات التوزيع.
- مخططات الشبكة.

2. الجداول
   - جدول نقاط المراقبة.
   - جدول مواصفات الكاميرات.
   - جدول متطلبات التركيب.
3. التقارير
   - تقرير تحليل الموقع.
   - تقرير تحليل المخاطر.
   - تقرير مراجعة التصميم.
4. دليل التشغيل
   - إجراءات التشغيل.
   - إجراءات الصيانة.
   - إجراءات الطوارئ.(14)

خلاصة الفصل الرابع

تناول هذا الفصل تصميم منظومة المراقبة من خلال عشرة مباحث: تحديد أهداف المراقبة، وتحليل الموقع، وتحليل المخاطر، وتحديد المناطق ذات الأولوية، وتحديد نقاط المراقبة، وتوزيع الكاميرات، وزوايا الرؤية والارتفاعات، والمناطق العمياء، والتكامل بين نقاط المراقبة، ومراجعة التصميم واختباره.

وقد اتضح من خلال هذا الفصل أن تصميم منظومة المراقبة ليس عملية تركيب أجهزة، وإنما عملية هندسية أمنية متكاملة تبدأ بتحليل الاحتياجات والمخاطر، وتمتد إلى تحديد نقاط المراقبة وتوزيع الكاميرات واختيار العدسات والارتفاعات، وتنتهي بمراجعة التصميم واختباره قبل التنفيذ.

وأن التصميم الصحيح هو الذي يبدأ من الأهداف الأمنية، وليس من الأجهزة، وينطلق من تحليل المخاطر، وليس من الافتراضات، ويعتمد على التوثيق والمراجعة، وليس على التقديرات الشخصية.

ومن ثم يمكن صياغة القاعدة التي تحكم هذا الفصل:

تصميم منظومة المراقبة يبدأ من الأهداف الأمنية، وينتهي باختبار الأداء الفعلي، ويمر بتحليل الموقع والمخاطر وتحديد الأولويات وتوزيع الكاميرات ومراجعة التصميم.

أهم نتائج الفصل الرابع

١. تصميم منظومة المراقبة عملية هندسية أمنية متكاملة.
٢. تحديد أهداف المراقبة هو الخطوة الأولى في التصميم.
٣. تحليل الموقع يوفر المعلومات اللازمة عن البيئة.
٤. تحليل المخاطر هو حجر الزاوية في التصميم.
٥. تحديد المناطق ذات الأولوية يضمن توجيه الموارد.
٦. تحديد نقاط المراقبة يترجم التحليل إلى مواقع محددة.
٧. توزيع الكاميرات يحقق التغطية المطلوبة بأقل تكلفة.
٨. زوايا الرؤية والارتفاعات تحدد جودة الصورة.
٩. المناطق العمياء يجب تحديدها ومعالجتها.
١٠. التكامل بين نقاط المراقبة يحقق التغطية الشاملة.
١١. مراجعة التصميم واختباره يضمنان تحقيق الأهداف.
١٢. التصميم الصحيح يبدأ من الأهداف الأمنية وليس من الأجهزة.

أسئلة التفكير والتقييم للفصل الرابع

أسئلة معرفية:

١. ما خطوات تصميم منظومة المراقبة؟
٢. ما أهمية تحديد أهداف المراقبة؟

٣. ما عناصر تحليل الموقع؟
٤. ما منهجيات تحليل المخاطر؟
٥. ما معايير تحديد المناطق ذات الأولوية؟
٦. ما معايير تحديد نقاط المراقبة؟
٧. ما استراتيجيات توزيع الكاميرات؟
٨. ما معايير تحديد زوايا الرؤية والارتفاعات؟
٩. ما طرق معالجة المناطق العمياء؟
١٠. ما مستويات التكامل بين نقاط المراقبة؟

أسئلة تحليلية:

١. حلل العلاقة بين تصميم المنظومة وتحقيق الأهداف الأمنية.
٢. ناقش أهمية تحليل المخاطر في تصميم المنظومة.
٣. قارن بين استراتيجيات توزيع الكاميرات.
٤. حلل العلاقة بين زوايا الرؤية والارتفاعات وجودة الصورة.
٥. ناقش طرق معالجة المناطق العمياء.
٦. لماذا يعدّ التكامل بين نقاط المراقبة ضروريًا؟
٧. لماذا يجب مراجعة التصميم واختباره قبل التنفيذ؟

أسئلة تطبيقية:

١. اختر منشأة تعرفها، وقم بتصميم منظومة مراقبة لها.
٢. صمم منظومة مراقبة لمنشأة حيوية مع توثيق جميع الخطوات.
٣. ضع مصفوفة تقييم لتصميم منظومة مراقبة.
٤. ضع نموذج تقرير مراجعة تصميم منظومة مراقبة.

المراجع:

①راجع. International Electrotechnical Commission, *IEC 62676-4:2025*, (Geneva: IEC, 2025), sections on design review.:

②ينظر. Lieberman, A. G., et al., *Video Surveillance Equipment Selection and Application Guide*, NIJ Guide 200-98.:

③راجع. IEC 62676-4:2025, sections on design review definition.:

④ينظر David Brown, *Integrated Security Systems Design*, p. 401.:.

⑤راجع. IEC 62676-4:2025, sections on design review elements.:

⑥ينظر. Lieberman, A. G., et al., *Video Surveillance Equipment Selection and Application Guide*.:

⑦ راجع: IEC 62676-4:2025, sections on design review methodology.

⑧ ينظر: Brown, *Integrated Security Systems Design*, p. 412.

⑨ راجع: IEC 62676-4:2025, sections on design testing.

⑩ ينظر: Lieberman, A. G., et al., *Video Surveillance Equipment Selection and Application Guide*.

⑪ راجع: IEC 62676-4:2025, sections on acceptance criteria.

⑫ ينظر: Brown, *Integrated Security Systems Design*, p. 423.

⑬ راجع: IEC 62676-4:2025, sections on design documentation.

⑭ ينظر: Lieberman, A. G., et al., *Video Surveillance Equipment Selection and Application Guide*.

الفصل الثالث: جودة الصورة والعوامل المؤثرة فيها

تمهيد الفصل

تمثل جودة الصـــورة إحدى أهم حلقات القيمة الأمنية لمنظومة المراقبة بالفيديو؛ إذ لا تتحدد فاعلية الكاميرا بمجرد قدرتها على إنتاج صـــورة، وإنما بقدرة المنظومة بأكملها على إيصـــال معلومات بصـــرية قابلة للاســـتخدام في الغرض الذي صُـــممت من أجله. ولذلك فإن الصـــورة التي تســـمح بكشـــف وجود شـــخص قد لا تكون كافية لتمييز خصائصه، والصورة التي تسمح بتمييز شخص معروف قد لا تكون كافية لإسناد هوية شـــخص غير معروف، كما أن جودة الصـــورة أثناء المشـــاهدة الحية قد تختلف عن جودتها بعد التسجيل والضغط والنقل والعرض.(1)

ويؤكد دليل Video Quality in Public Safety (VQiPS) أن مفهوم جودة الفيديو يرتبط بقدرة المســـتخدم النهائي على أداء المهمة المطلوبة من الصـــورة، وأن تحديد المتطلبات ينبغي أن يبدأ من حالة الاســـتخدام والغرض المطلوب، لا من المواصـــفات التجارية وحدها.(2)

ومن ثم فإن جودة الصـــورة ليســـت مرادفًا للدقة الرقمية، ولا يمكن اختزالها في عدد الميجا بكســـلات. فهي نتيجة ســـلســـلة مترابطة تبدأ بالمشـــهد والإضـــاءة والهدف والمســـافة، ثم تمر بالعدســـة والمســـتشـــعر والتقاط الصـــورة والمعالجة والترميز والضـــغط والنقل والتخزين والعرض. وقد خصـــص دليل NIST/VQiPS لهذه الســـلســـلة مكونات مستقلة تشـمل العدسـة، والتقاط الصـورة، والمعالجة، والنقل، والتخزين، والعرض، لأن كل حلقة منها يمكن أن تؤثر في الجودة النهائية.(3)

كما ينبغي التمييز بين المواصفة الفنية والأداء التشغيلي. فالكاميرا ذات الدقة الأعلى لا تضـمن بالضـرورة قدرة أعلى على التعرف أو التحقق إذا كانت العدسـة غير مناسـبة، أو كان الهدف بعيدًا، أو كانت الإضاءة ضعيفة، أو كان الهدف سريع الحركة، أو تعرض الفيديو لضغط مفرط أو فقد في البيانات.

وقد أصبح هذا التمييز أكثر أهمية مع صدور IEC 62676-4:2025 ، التي تمثل الإصدار الأحدث من الجزء الخاص بالإرشـــادات التطبيقية في أنظمة المراقبة بالفيديو، وتتناول التخطيط والتصميم والتركيب والاختبار والتشغيل والصيانة.(4)

ويتناول هذا الفصـــل تســعة مباحث مترابطة: مفهوم جودة الصـــورة، والدقة والتفاصـــيل وكثافة البكسلات، والعدسات وزوايا الرؤية، والمسافة ومجال الرؤية، والإضاءة، والرؤية الليلية، والحركة والظروف المتغيرة، والعوامل البيئية والحماية الميكانيكية، واختيار مستوى الجودة وفق الهدف الأمني (بما في ذلك الضغط ومعدل البت).

المبحث الأول: مفهوم جودة الصورة

الخطأ المنهجي الأكثر شيوعًا هو التعامل مع الجودة باعتبارها خاصية ثابتة للكاميرا، بينما تشير المنهجية إلى أن الجودة المطلوبة تتحدد أساسًا من خلال المهمة التي سيؤديها المستخدم بالصورة.(1)

أولًا: تعريف جودة الصورة

يمكن تعريف جودة الصورة في سياق أنظمة المراقبة الأمنية بأنها :قدرة الصورة أو سلسلة الفيديو المقدمة إلى المستخدم النهائي على إظهار المعلومات البصرية اللازمة لأداء المهمة الأمنية المحددة بدرجة الدقة والموثوقية المطلوبة، في ظروف التشغيل الفعلية .(2)

وهذا التعريف أكثر دقة من ربط الجودة بالدقة العددية؛ لأن الصورة ذات الدقة العالية قد تفشل في تحقيق الغرض الأمني إذا لم يكن الهدف ممثلًا بعدد كافٍ من البكسلات أو إذا كانت الصورة متأثرة بالحركة أو الإضاءة أو الضغط أو فقد البيانات.

ويؤكد المختصون أن جودة الفيديو ينبغي فهمها باعتبارها قدرة الفيديو المسلم إلى المستخدم على تمكينه من التعرف على الأهداف وتنفيذ المهمة المطلوبة، وأن القدرة على أداء المهمة هي التي تحدد مستوى الجودة المطلوب.(3)

ثانيًا: جودة الصورة بوصفها نتيجة لسلسلة متكاملة

يمكن تمثيل سلسلة جودة الفيديو على النحو الآتي:(4)

المشهد ← الإضاءة ← العدسة ← المستشعر ← المعالجة ← الترميز والضغط ← النقل ← التخزين ← فك الترميز ← العرض ← المستخدم

وعليه، فإن تدهور أي حلقة من هذه السلسلة قد يؤدي إلى انخفاض القيمة العملية للصورة، حتى لو كانت الكاميرا نفسها ذات مواصفات مرتفعة. وقد حدد NIST/VQiPSستة مكونات رئيسة تؤثر في جودة الفيديو: تكوين العدسة، والتقاط الصورة، والمعالجة، والنقل، والتخزين، والعرض.(5)

ثالثًا: الأبعاد الأساسية لجودة الصورة

لا ينبغي التعامل مع جودة الصـــورة باعتبارها متغيرًا واحدًا، وإنما باعتبارها مجموعة من الأبعاد المترابطة، أهمها:(6)

١. الدقة المكانية :عدد عناصر الصورة المتاحة لتمثيل التفاصيل.
٢. كثافة البكسلات على الهدف :مقدار التمثيل الرقمي للهدف في المساحة التي يشغلها.
٣. الحدة والتفاصيل :قدرة النظام البصري والرقمي على المحافظة على التفاصيل.
٤. التباين :القدرة على الفصل بين المناطق ذات السطوع المختلف.
٥. النطاق الديناميكي :القدرة على تمثيل المناطق الساطعة والمظلمة في المشهد نفسه.
٦. الأداء في الإضاءة المنخفضة :القدرة على إنتاج صورة مفيدة عند انخفاض الضوء.
٧. الأداء الزمني :قدرة النظام على تمثيل الحركة دون فقد أو تشوه مفرط.
٨. الاستقرار :المحافظة على الصورة عند اهتزاز الكاميرا أو الحامل.
٩. دقة اللون :عند كون اللون عنصرًا ضروريًا في المهمة الأمنية.
١٠. سلامة السلسلة الرقمية :المحافظة على البيانات أثناء الترميز والنقل والتخزين والعرض.

وتؤكد إرشادات NIST أن الدقة ومعدل الإطارات والألوان والنطاق الديناميكي والضوضاء والقدرة على التقاط الأشعة تحت الحمراء كلها من الخصائص التي يمكن أن تؤثر في عملية التقاط الفيديو.(7)

رابعًا: مستويات الأداء البصري

ينبغي عدم استخدام مصطلحات مثل "كشف" و"تعرف" و"تحديد هوية" بصورة مترادفة. وفي هذا الكتاب تُستخدم المصطلحات على النحو الآتي:(8)

1. الكشف – Detection

يقصد بالكشف إثبات وجود هدف أو جسم أو حركة داخل المنطقة محل الاهتمام

2. الملاحظة – Observation

يقصد بالملاحظة إتاحة وصف أو رصد الخصائص العامة للهدف أو سلوكه، دون الحاجة إلى تحديد هويته بشكل دقيق

3. التعرّف – Recognition

يقصد بالتعرّف تمكين المستخدم من ربط الهدف بشخص أو شيء معروف سابقًا، وذلك وفقًا لطبيعة المهمة والغرض منها

4. تحديد الهوية – Identification

يقصد بتحديد الهوية الوصول إلى هوية الهدف بدرجة من التفصيل والدقة التي تتطلبها المهمة

5. التحقق – Verification

يقصد بالتحقق إجراء عملية مقارنة بين معلومة أو هوية مُدّعاة ومرجع معروف، بهدف التأكد من وجود تطابق أو من صحة الادعاء المتعلق بالهوية

ومن المهم هنا أن Verification لا ينبغي أن يُعامل باعتباره مجرد مستوى أعلى من Recognitionأو Identification في كل الحالات. فهو مفهوم وظيفي يتعلق بالمقارنة والتحقق، بينما قد يكون التحقق من وجه شخص معروف، أو من لوحة مركبة، أو من واقعة معينة، ولكل حالة متطلبات مختلفة.(9)

كما أن مصطلحات DORI القديمة لا ينبغي إسقاطها آليًا على الإصدار الحديث من IEC 62676-4:2025؛ إذ قدم الإصدار الجديد سلمًا تشغيليًا أكثر تفصيلًا يرتبط بمستويات الكثافة البكسلية والمهام البصرية.(10)

خامسًا: الفرق بين جودة الجهاز وجودة الصورة

جودة الجهاز تشير إلى الخصائص الفنية للمعدة، مثل:(11)

١. دقة المستشعر.

٢. حجم المستشعر.

٣. نوع العدسة.

٤. معدل الإطارات.

٥. الحساسية الضوئية.

٦. إمكانات المعالجة.

أما جودة الصورة فهي النتيجة الفعلية لهذه العناصر عندما تعمل معًا في مشهد حقيقي، وبالتالي : جودة الجهاز ≠ جودة الصورة.

وقد يكون الجهاز عالي المواصفات، بينما تكون الصورة غير صالحة للغرض الأمني بسبب سوء الموقع أو الإضاءة أو المسافة أو الحركة أو الضغط أو النقل

المراجع:

1. National Institute of Standards and Technology. (2024). *VQiPS: Getting Started: Guide to Defining Video Quality Requirements*. U.S. Department of Commerce.
2. National Institute of Standards and Technology. (2024). *VQiPS: Use Cases*. U.S. Department of Commerce.
3. National Institute of Standards and Technology. (2024). *VQiPS: Video System Functions*. U.S. Department of Commerce.
4. National Institute of Standards and Technology. (2024). *VQiPS: Focus*. U.S. Department of Commerce.
5. National Institute of Standards and Technology. (2024). *VQiPS: Capture*. U.S. Department of Commerce.
6. National Institute of Standards and Technology. (2024). *VQiPS: Processing*. U.S. Department of Commerce.
7. National Institute of Standards and Technology. (2024). *VQiPS: Storage*. U.S. Department of Commerce.
8. National Institute of Standards and Technology. (2024). *VQiPS: Transport*. U.S. Department of Commerce.
9. National Institute of Standards and Technology. (2024). *VQiPS: Display*. U.S. Department of Commerce.
10. National Institute of Standards and Technology. (2024). *VQiPS: Target Size*. U.S. Department of Commerce.
11. National Institute of Standards and Technology. (2024). *VQiPS: Motion*. U.S. Department of Commerce.
12. National Institute of Standards and Technology. (2024). *VQiPS: Video System Tasks*. U.S. Department of Commerce.
13. International Electrotechnical Commission. (2025). *IEC 62676-4:2025: Video surveillance systems for use in security applications—Part 4: Application guidelines*. IEC.

المبحث الثاني: الدقة والتفاصيل وكثافة البكسلات

تُعد الدقة من أهم عناصـــر التصـــوير الرقمي، لكنها لا تمثل وحدها القدرة على إظهار التفاصيل. فزيادة عدد البكسلات يمكن أن توفر قدرة نظرية أكبر على تمثيل التفاصيل، إلا أن الاستفادة الفعلية منها تعتمد على العدسة والمستشعر والمسافة والإضاءة والحركة والمعالجة والضغط.(1)

وقد أشار NIST إلى أن ارتفاع الدقة يزيد القدرة على التقاط التفاصيل، لكنه يؤدي في الوقت نفسه إلى زيادة البيانات ومتطلبات الشبكة والتخزين.(2)

أولًا: مفهوم الدقة

الدقة المكانية في الصورة الرقمية هي عدد عناصر الصورة المستخدمة لتمثيل الإطار، ويُعبّر عنها عادة بعدد البكسلات أفقيًا وعموديًا.(3)

فعلى سبيل المثال:

- 1920 × 1080 = 2,073,600بكسل ≈ ٢ .٠٧ ميجابكسل.
- 3840 × 2160 = 8,294,400بكسل ≈ ٨٫٢٩ ميجابكسل.

ويجب التمييز بين:(4)

- دقة الصورة.
- حجم المستشعر.
- حجم الهدف في الصورة.
- كثافة البكسلات على الهدف.

ثانيًا: لماذا لا تكفي الدقة؟

إذا صورت كاميرا ٤ Kمشهدًا واسعًا جدًا، فقد يكون عدد البكسلات الكلي مرتفعًا، لكن الشخص الموجود في طرف المشهد قد يشغل عددًا محدودًا جدًا من البكسلات (5).

وفي المقابل، يمكن لكاميرا ذات دقة أقل أن تحقق أداءً أفضل في التعرف على هدف محدد إذا استخدمت عدسة مناسبة ووضعت على مسافة صحيحة.
ولهذا تؤكد منهجية NIST أهمية حجم الهدف بالنسبة إلى مجال الرؤية، وليس الدقة وحدها.(6)

ثالثًا: كثافة البكسلات

يمكن تعريف كثافة البكسلات بأنها :عدد البكسلات التي تمثل وحدة طول من الهدف أو المشهد .(7)

وتُستخدم عادة وحدة:

- Pixel Per Meter – PPM.
- Pixel Per Foot – PPF.

والعلاقة بينهما:

- .PPM = PPF × 3. 28084
- .PPF = PPM ÷ 3. 28084

رابعًا: سلم الكثافة البكسلية

ينبغي هنا التمييز بين سلم DORI التاريخي المرتبط بالإصدار السابق من-IEC 62676 4وبين الإطار التشغيلي الذي قدمه إصدار ٢٠٢٥.(8)

وتعرض الإرشادات الحديثة المستندة إلى IEC 62676-4:2025 سبعة مستويات تشغيلية للكثافة البكسلية للصورة المرئية:(9)

المستوى التشغيلي	الكثافة التقريبية
Overview	20 PPM
Outline	40 PPM
Discern	80 PPM

Perceive	125 PPM
Characterize	250 PPM
Validate	500 PPM
Scrutinize	1500 PPM

وهذه الأرقام ليست وصفة عامة تضمن النتيجة في كل مشهد؛ إذ ترتبط بتطبيقات الرؤية البشرية للصورة المرئية، كما أن التحليلات البرمجية والكاميرات الحرارية لها متطلبات مختلفة.(10)

أما سلم DORI التقليدي المتداول في الأدبيات السابقة فكان يعتمد تقريبًا على:(11)

DORIالتقليدي	الكثافة
Detection	25 PPM
Observation	63 PPMتقريبًا
Recognition	125 PPM
Identification	250 PPM

ولا ينبغي تقديم هذا الجدول في كتاب حديث على أنه المعيار الحالي دون الإشارة إلى أنه سلم سابق. أما في المواصفات الجديدة التي تستند صراحة إلى IEC 62676-4:2025، فينبغي استخدام المصطلحات والمستويات الحديثة أو تحديد الإصدار المقصود بوضوح.(12)

خامسًا: معادلة كثافة البكسلات

إذا كان لدينا:(13)

- عدد البكسلات الأفقية.N =
- عرض المشهد عند موضع الهدف W = متر.

فإن.PPM = N / W :

وهذه المعادلة لا تقول إن الجودة مضمونة، وإنما تحدد الكثافة الهندسية للبكسلات على مستوى المشهد.

سادسًا: حساب مجال الرؤية

عندما تكون أبعاد المستشعر والبعد البؤري والمسافة معروفة، يمكن استخدام التقريب الهندسي:(14)

$$W = (S \times D) / f$$

حيث:

- W = عرض المشهد.
- S = العرض الفعلي للمستشعر.
- D = المسافة إلى الهدف.
- f = البعد البؤري.

وبالتالي.(15) $PPM = (N \times f) / (S \times D)$:

وهذه العلاقة مفيدة في التصميم الأولي، لكنها لا تغني عن استخدام بيانات الكاميرا الفعلية واختبار المشهد؛ لأن العدسة قد تتضمن تشوهات، كما أن مجال الرؤية الفعلي قد يختلف عن النموذج الهندسي المثالي.(15)

سابعًا: مثال حسابي

إذا كان لدينا مستشعر عرضه ٦. ٤ مم، وعدسة ٨ مم، ومسافة ٢٠ مترًا، ودقة أفقية تبلغ ٣٨٤٠ بكسل:(16)

$W = (6.4 \times 20) / 8 = 16$ مترًا

ومن ثم.$PPM = 3840 / 16 = 240$ PPM :

وهذا المثال يوضح أن كاميرا ٤ K لا تعني تلقائيًا أنها تحقق مستوى معينًا من الأداء؛ فالنتيجة تعتمد على العدسة والمسافة وحجم المستشعر.

ثامنًا: العوامل التي تحد من الاستفادة من الدقة

من أهمها: (17)

- جودة العدسة.
- التركيز البؤري.
- حجم المستشعر.
- الإضاءة.
- الحركة.
- الضوضاء.
- النطاق الديناميكي.
- الضغط.
- معدل البت.
- فقد الحزم الشبكية.
- جودة العرض.

وقد أكد NIST أن الضغط والشبكة والتخزين يمكن أن تؤثر في المحافظة على التفاصيل، وأن الضغط الزائد قد يؤدي إلى فقد غير قابل للاسترجاع. (18)

المراجع:

1. National Institute of Standards and Technology. (2024). *VQiPS: Capture*. U.S. Department of Commerce.
2. National Institute of Standards and Technology. (2024). *VQiPS: Target Size*. U.S. Department of Commerce.
3. National Institute of Standards and Technology. (2024). *VQiPS: Discrimination Level*. U.S. Department of Commerce.
4. National Institute of Standards and Technology. (2024). *VQiPS: GUC Aspects*. U.S. Department of Commerce.
5. National Institute of Standards and Technology. (2024). *VQiPS: Motion*. U.S. Department of Commerce.
6. National Institute of Standards and Technology. (2024). *VQiPS: Processing*. U.S. Department of Commerce.
7. National Institute of Standards and Technology. (2024). *VQiPS: Display*. U.S. Department of Commerce.
8. International Electrotechnical Commission. (2025). *IEC 62676-4:2025: Video surveillance systems for use in security applications—Part 4: Application guidelines*. IEC.
9. Axis Communications. (2025). *Pixel Density Based on IEC 62676-4:2025*. Axis Communications.
10. National Institute of Standards and Technology. (2024). *VQiPS: Deliver Video*. U.S. Department of Commerce.

المبحث الثالث: العدسات وزوايا الرؤية

تُعد العدسة أحد أكثر عناصر النظام تأثيرًا في توزيع التفاصيل داخل الصورة؛ فهي تحدد مقدار المشهد الذي يدخل إلى الصورة، وتؤثر في حجم الهدف، وكمية الضوء الواصلة إلى المستشعر، والعمق البؤري، والتشوهات البصرية.(1)
وقد عرف NIST العدسة باعتبارها العنصر البصري الذي يكوّن الصورة، وأشار إلى أن البعد البؤري يحدد مجال الرؤية والحجم الظاهري للأهداف، بينما تؤثر الفتحة في كمية الضوء الواصلة إلى سطح الالتقاط.(2)

أولًا: البعد البؤري ومجال الرؤية

توجد علاقة عكسية عامة بين البعد البؤري ومجال الرؤية:(3)

- البعد البؤري القصير ← مجال رؤية أوسع.
- البعد البؤري الطويل ← مجال رؤية أضيق وحجم أكبر للهدف في الصورة.

ولكن لا يصح إعطاء جدول ثابت من نوع "٢. ٨ مم = ١٠٠°" أو "١٢ مم = ٣٠°" لجميع الكاميرات؛ لأن زاوية الرؤية تعتمد كذلك على أبعاد المستشعر.(4)

ثانيًا: العلاقة الهندسية

يمكن حساب زاوية الرؤية الأفقية نظريًا من:(5)

$$HFOV = 2 \times \tan^{-1}(S / 2f)$$

حيث:

- S = عرض المستشعر.
- f = البعد البؤري.

وهذا يوضح لماذا لا يجوز تحديد زاوية الرؤية من البعد البؤري وحده.

ثالثًا: أنواع العدسات ذات الصلة بالمراقبة

يمكن تصنيف العدسات عمليًا إلى:(6)

- Fixed Lens: عدسة ثابتة.
- Varifocal Lens: عدسة متغيرة البعد البؤري.
- Motorized Varifocal: عدسة متغيرة بمحرك.
- Zoom Lens: عدسة تسمح بتغيير التكبير وفق تصميمها.

كما توجد خصائص أخرى مهمة مثل:(7)

- فتحة العدسة.
- نوع الحساس المتوافق معها.
- التشوه البصري.
- جودة الطلاءات.
- القدرة على المحافظة على الحدة في أطراف الصورة.

رابعًا: فتحة العدسة

كلما اتسعت فتحة العدسة، زادت كمية الضوء التي يمكن أن تصل إلى المستشعر، وهو أمر مهم في ظروف الإضاءة المنخفضة والحركة.(8)

وقد أوضح NIST أن الفتحة الأكبر تساعد على تمرير مزيد من الضوء، مما يسمح باستخدام سرعات غالق أعلى، وهو ما قد يساعد في الحد من تشوش الحركة.(9)

لكن الفتحة الواسعة قد تقلل عمق المجال، ولذلك لا ينبغي اختيارها بمعزل عن طبيعة المشهد.

خامسًا: أخطاء اختيار العدسات

من أهم الأخطاء:(10)

- اختيار العدسة من خلال البعد البؤري فقط.
- تجاهل حجم المستشعر.
- تجاهل المسافة.
- تجاهل حجم الهدف.

- تجاهل الإضاءة.
- استخدام عدسة واسعة جدًا عندما يكون الهدف الأمني يتطلب تفاصيل دقيقة.
- استخدام عدسة ضيقة جدًا عندما يكون المطلوب وعيًا واسعًا بالمشهد.
- تجاهل التشوهات البصرية.

المراجع: المراجع

1. National Institute of Standards and Technology. (2024). *VQiPS: Focus*. U.S. Department of Commerce.
2. National Institute of Standards and Technology. (2024). *VQiPS: Target Size*. U.S. Department of Commerce.
3. National Institute of Standards and Technology. (2024). *VQiPS: GUC Questionnaire*. U.S. Department of Commerce.
4. National Institute of Standards and Technology. (2024). *VQiPS: Video Requirements Tool Reference List*. U.S. Department of Commerce.
5. Axis Communications. (2025). *Lenses in Surveillance*. Axis Communications.
6. Axis Communications. (2025). *M12 Lenses*. Axis Communications.

المبحث الرابع: المسافة ومجال الرؤية

تؤثر المسافة بين الكاميرا والهدف مباشرة في حجم الهدف داخل الصورة وكثافة البكسلات التي تمثله. وكلما اتسعت المساحة التي تغطيها الكاميرا، انخفضت عادة كثافة البكسلات على الأهداف الموجودة داخل تلك المساحة، ما لم تُستخدم دقة أو بصريات تعوض هذا الانخفاض.(1)

ويؤكد المختصون أن حجم الهدف يعتمد على حجمه الفعلي ومسافته عن الكاميرا ومجال رؤية الكاميرا، وأن زيادة حجم الهدف في الإطار تسمح بإظهار تفاصيل أكثر .(2)

أولًا: المسافة ليست مجرد رقم

ينبغي عند تحديد المسافة دراسة:(3)

- المسافة الأفقية.
- الارتفاع.
- زاوية التصوير.
- المسافة الفعلية على مستوى الهدف.
- حجم الهدف.
- سرعة الهدف.
- الإضاءة.
- مجال الرؤية.

ثانيًا: مجال الرؤية : هو الجزء من العالم المرئي الذي يظهر من خلال العدسة في لحظة معينة.(4)

ولا ينبغي مساواة "مجال الرؤية الواسع" مع "التغطية الأمنية الجيدة" بصورة مطلقة؛ لأن زيادة المجال قد تأتي على حساب التفاصيل.

ثالثًا: العلاقة بين المسافة والكثافة

من المعادلة: (5)

$$PPM = (N \times f) / (S \times D)$$

نلاحظ أن كثافة البكسلات تتناقص تقريبًا مع زيادة المسافة إذا بقيت بقية المتغيرات ثابتة. فإذا تضاعفت المسافة، تنخفض الكثافة الهندسية تقريبًا إلى النصف.

رابعًا: مثال تطبيقي

إذا حققت منظومة ما: (6)

200 PPM عند مسافة ١٠ أمتار، فإن التصميم الهندسي نفسه، مع ثبات العدسة والمستشعر والدقة، سيعطي تقريبًا:

100 PPM عند ٢٠ مترًا.

وهذا المثال لا يمثل أداءً مضمونًا في الواقع، وإنما يوضح العلاقة الهندسية الأساسية.

خامسًا: مبدأ "التغطية ليست تفصيلًا" ومن الأخطاء الشائعة محاولة تغطية مساحة كبيرة بكاميرا واحدة. (7)

في بعض المواقع يكون التصميم الأفضل هو: (8)

- كاميرا واسعة للمراقبة العامة.
- كاميرا موجهة للتفاصيل.
- كاميرا مخصصة لنقطة التحقق.

وهذا أفضل من استخدام كاميرا واحدة لإجبارها على أداء وظائف متناقضة.

المراجع:

(١) المسافة وحجم الهدف وكثافة البكسلات: NIST – *Target Size*. يذكر المصدر أن حجم الهدف المدرك يعتمد على حجم الهدف الحقيقي، والمسافة عن الكاميرا، ومجال رؤية الكاميرا.

(٢) العلاقة بين حجم الهدف والتفاصيل: NIST – *Target Size*. يوضح المصدر أن زيادة حجم الهدف بالنسبة إلى مجال الرؤية تسمح بإدراك تفاصيل أكثر.

(٣) عوامل المسافة والمشهد: NIST – *GUC Aspects* و*GUC Questionnaire* – *NIST*. يميز NIST بين حجم الهدف، والحركة، والإضاءة، ومستوى التمييز باعتبارها من خصائص المشهد والاستخدام.

(٤) تعريف مجال الرؤية: NIST – *Focus*. يعرّف المصدر مجال الرؤية بأنه نطاق العالم المرئي الذي يمكن رؤيته من خلال العدسة في لحظة معينة.

(٥) المعادلة المستخدمة هنا اشتقاق هندسي من العلاقة بين مجال الرؤية، والمسافة، والبعد البؤري، وليست اقتباسًا حرفيًا من NIST.

(٦) المثال الحسابي ٢٠٠ PPM → 100 PPM: مثال رياضي توضيحي، ولا يحتاج إلى نسبته إلى مصدر خارجي.

(٧) يدعم NIST المبدأ العام بأن حجم الهدف بالنسبة إلى مجال الرؤية يؤثر في مقدار التفاصيل التي يمكن إدراكها.

(٨) استخدام كاميرات مختلفة لمهام مختلفة: يؤكد NIST أن متطلبات معدات الفيديو تعتمد على حالة الاستخدام والمهمة المطلوبة، وأن الأنظمة لا تحتاج جميعها إلى المستوى نفسه من القدرة على التمييز أو التعرف.

المبحث الخامس: الإضاءة

الإضـــاءة ليســـت مجرد عامل ثانوي في جودة الصـــورة؛ بل هي جزء من بيئة الالتقاط نفسـها. فالضـوء المتاح يحدد كمية المعلومات التي يمكن للمستشعر تسجيلها، كما يؤثر في سرعة الغالق والضوضاء والألوان والتباين.(1)

ويؤكد المختصـون أن مسـتوى الإضـاءة من العناصـر الأسـاسـية التي ينبغي إدخالها في تحديد فئة الاستخدام، وأن ظروف الإضاءة قد تتراوح من الظلام الشديد إلى الإضاءة القوية، كما أن وجود مناطق شـديدة السـطوع وأخرى شـديدة الظلام في الإطار نفسـه يمثل تحديًا للنطاق الديناميكي.(2)

أولًا: اللوكس ووظيفته

اللوكس (Lux) وحدة لقياس الاستضاءة الواقعة على سطح، وليس "حساسية الكاميرا" نفسها.(3)

وهنا يجب تصحيح صياغة شائعة: لا يجوز استخدام رقم Lux واحد للحكم على قدرة الكاميرا.

فالقيمة الاسـمية الدنيا التي تعلنها الشـركات قد تعتمد على شـروط القياس، والعدسـة، وسـرعة الغالق، وكسـب الإشـارة، ومعالجة الصـورة، وما إذا كان القياس يخص الإضـاءة على المشهد أو مستوى آخر.(4)

وقد حذر دليل مهني من أن أرقام الحد الأدنى للـ Luxليست قابلة للمقارنة البسيطة بين المنتجات إذا اختلفت شروط القياس.(5)

ثانيًا: لماذا لا نعتمد جدول Lux جامدًا؟

الجدول الذي يقرر مثلًا:(6)

- المكتب = ٣٠٠–٥٠٠ Lux.
- الشارع = ١٠–٥٠ Lux.

- القمر = ١ر٠–١ Lux.
- الظلام = ٠٠١ر٠–٠١ر٠ Lux.

لا ينبغي إدراجه في الكتاب على أنه معيار تصميم أمني.
والسبب أن الإضاءة الفعلية تختلف بشدة بحسب المكان والوقت والاتجاه والانعكاس والطقس، كما أن قيمة Lux وحدها لا تصف النطاق الديناميكي للمشهد.
لذلك يكون المنهج الأكاديمي الأفضل هو:(7)
قياس الإضاءة ميدانيًا + وصف تباين المشهد + اختبار الكاميرا في ظروف التشغيل الفعلية.

ثالثًا: أنواع تحديات الإضاءة

1. الإضاءة المنخفضة

تؤدي عادة إلى:(8)

- زيادة الضوضاء.
- انخفاض التفاصيل.
- بطء الغالق عند بعض الإعدادات.
- صعوبة المحافظة على الألوان.
- زيادة احتمالية تشوش الحركة.

2. الإضاءة الخلفية

تظهر عندما يكون مصدر قوي للضوء خلف الهدف، مثل:(9)

- باب خارجي.
- نافذة.
- مدخل مبنى.
- مصابيح مركبات.

3. التباين العالي

قد تحتوي الصورة على منطقة شديدة السطوع ومنطقة شديدة الظلام في الوقت نفسه، ما يتطلب نطاقًا ديناميكيًا مناسبًا.(10)

4. الانعكاسات

يمكن أن تنتج عن:(11)

- الزجاج.
- الأسطح المعدنية.
- المياه.
- الطرق المبللة.
- الأجسام اللامعة.

رابعًا WDR :

يشير WDR إلى تقنيات تهدف إلى تحسين تمثيل المشاهد ذات الفروق الكبيرة في السطوع.(12)

ومن المهم عدم التعامل مع WDR باعتباره "زرًا سحريًا"؛ فلكل طريقة تطبيقية مزايا وقيود، وقد تظهر بعض التشوهات أو الآثار الجانبية في ظروف معينة. وتشير الأدبيات المهنية الحديثة إلى أن مشاهد الأبواب والمداخل والمواقف والأنفاق من الأمثلة النموذجية على الحاجة إلى معالجة النطاق الديناميكي.(13)

خامسًا BLC :وHLC

Backlight Compensation – BLC

تهدف إلى تحسين رؤية الهدف عندما يكون مصدر قوي للضوء خلفه، من خلال تعديل طريقة حساب التعريض.(14)

Highlight Compensation – HLC

تهدف إلى التعامل مع مصادر شديدة السطوع، مثل:(15)

- مصابيح المركبات.

- الكشافات.
- مصادر ضوئية مركزة.

ولا ينبغي تقديم BLC أو HLC على أنهما بدائل مطلقة لـWDR؛ فكل تقنية تعالج نوعًا مختلفًا من مشكلات المشهد.

سادسًا: اختيار الكاميرا وفق الإضاءة

ينبغي أن يشمل التقييم:(16)

- الإضاءة النهارية.
- الإضاءة الليلية.
- التغير بين الليل والنهار.
- الإضاءة الخلفية.
- التباين.
- مصادر الضوء المباشرة.
- انعكاسات الأسطح.
- الحركة في الإضاءة المنخفضة.

المراجع:

① NIST/VQiPS, *Lighting Level*, ودليل *Defining Video Quality Requirements*, pp. 19–20.

② NIST/VQiPS, *Defining Video Quality Requirements*, p. 20.

③ Axis Communications, *Lighting for network video*, 2023.

④ Axis Communications, *Lighting for network video*, 2023.

⑤ Axis Communications, *Lighting for network video*, 2023.

⑥ Axis Communications, *Lighting for network video*, 2023.

⑦ NIST/VQiPS, *Defining Video Quality Requirements*, pp. 19–20.

⑧ NIST/VQiPS, *Defining Video Quality Requirements*, pp. 19–20.

⑨ NIST/VQiPS, *Defining Video Quality Requirements*, pp. 19–20.

⑩ NIST/VQiPS, *Defining Video Quality Requirements*, pp. 19–20.

⑪ NIST/VQiPS, *Defining Video Quality Requirements*, pp. 19–20.

⑫ Axis Communications, *Wide dynamic range*, 2026.

⑬ Axis Communications, *Wide dynamic range*, 2026.

⑭ Axis Communications, *Wide dynamic range*, 2026.

⑮ Axis Communications, *Wide dynamic range*, 2026.

⑯ NIST/VQiPS, *Defining Video Quality Requirements*, pp. 19–20.

المبحث السادس: الرؤية الليلية

تتطلب المراقبة الليلية معالجة مختلفة عن المراقبة النهارية، لأن انخفاض عدد الفوتونات المتاحة يؤثر في الضوضاء واللون وسرعة الغالق والتفاصيل.(1)

ويجب أولًا التمييز بين:(2)

كاميرات منخفضة الإضاءة	كاميرات Day/Night.	الإضاءة بالأشعة تحت الحمراء
	التصوير الحراري	

أولًا: الكاميرات منخفضة الإضاءة

تستفيد من:(3)

- مستشعرات أكثر حساسية.
- عدسات ذات فتحة مناسبة.
- معالجة متقدمة للضوضاء.
- إدارة أفضل للكسب والغالق.

لكنها لا تجعل الظلام المطلق مساويًا للضوء الكافي.

ثانيًا: الأشعة تحت الحمراء

تستخدم كاميرات Day/Night عادة مستشعرات قادرة على الاستفادة من الأشعة القريبة من تحت الحمراء، وقد تستخدم إضاءة IR مدمجة أو خارجية.(4)

وتشير المصادر المهنية الحديثة إلى أن كاميرات Day/Night يمكن أن تنتقل من التصوير الملون نهارًا إلى التصوير الأحادي ليلًا عند إدخال نطاق الأشعة القريبة من تحت الحمراء، وأن الإضاءة بالأشعة تحت الحمراء يمكن أن تتيح التصوير في الظلام عندما لا يتوفر الضوء المرئي الكافي.(5)

مزايا: IR (6)

- إمكانية العمل في غياب الضوء المرئي.
- تقليل الحاجة إلى الإضاءة البيضاء.
- إمكانية المحافظة على مستوى من السرية البصرية.

قيود: IR (7)

- الصورة غالبًا أحادية اللون في وضع الليل.
- احتمال ظهور انعكاسات.
- تأثر الأداء بالأسطح القريبة واللامعة.
- اختلاف المدى الفعلي بحسب المشهد والعدسة والإضاءة.

ولا ينبغي اعتبار عبارة "Zero Lux" دليلًا كافيًا على الأداء؛ فقد تعني أن الكاميرا تعتمد على إضاءة IR مضافة.(8)

ثالثًا: التصوير الحراري

التصوير الحراري لا يعتمد على الضوء المرئي بالطريقة التي تعتمدها الكاميرات البصرية، وإنما يستفيد من الإشعاع الحراري المنبعث من الأجسام.(9)

ولهذا يمكن أن يكون فعالًا في الظلام، وقد يكون مفيدًا في الكشف عن وجود أجسام أو فروق حرارية.

لكن يجب عدم مساواة الصورة الحرارية بالصورة البصرية؛ فالتصوير الحراري له خصائص مختلفة، وقد لا يقدم التفاصيل البصرية نفسها اللازمة لتحديد الهوية.(10) وتؤكد الأدبيات المهنية أن الكاميرات الحرارية والكاميرات البصرية المزودة بـ IRتؤديان وظائف مختلفة، وأن الحرارية قد تكون ممتازة للكشف لكنها لا تستبدل بالضرورة الكاميرات المرئية عندما تكون التفاصيل البصرية أو الهوية مطلوبة.(11)

رابعًا: مقارنة التقنيات

١. التقنيات المستخدمة في المراقبة الليلية

- تقنية Low-light (الإضاءة المنخفضة)
  - A. البيئة المناسبة: الأماكن ذات الإضاءة المنخفضة.
  - B. القوة الأساسية: المحافظة على صورة بصرية واضحة نسبيًا باستخدام الضوء المتاح.
  - C. القيد الرئيس: تحتاج إلى وجود قدر من الإضاءة حتى تتمكن من إنتاج صورة مناسبة.
- تقنية Day/Night + IR (نهاري/ليلي مع الأشعة تحت الحمراء)
  - A. البيئة المناسبة: حالات الظلام أو الإضاءة الضعيفة.
  - B. القوة الأساسية: توفير قدرة جيدة على المراقبة الليلية باستخدام الأشعة تحت الحمراء.
  - C. القيد الرئيس: تكون الصورة في الوضع الليلي غالبًا أحادية اللون.
- تقنية الإضاءة البيضاء
  - A. البيئة المناسبة: الأماكن المظلمة التي تتطلب الحصول على صورة ملونة.
  - B. القوة الأساسية: توفير صورة ملونة، مع إمكانية أن تسهم الإضاءة في ردع بعض السلوكيات غير المرغوبة.
  - C. القيد الرئيس: قد تكون الإضاءة مزعجة للأشخاص أو ملفتة للانتباه، وقد تؤثر في طبيعة البيئة المراقبة.
- تقنية Thermal (التصوير الحراري)

A. البيئة المناسبة : حالات الظلام أو الظروف التي يكون فيها الكشف الحراري أكثر فاعلية.

B. القوة الأساسية : القدرة على الكشف عن الأجسام ومصادر الحرارة دون الحاجة إلى الضوء المرئي.

القيد الرئيس : تختلف التفاصيل البصرية وإمكانية تحديد الهوية عن تلك التي توفرها الكاميرات المرئية التقليدية.

خامسًا: اختبار الرؤية الليلية: ينبغي الاختبار في: (12)

A. الإضاءة المنخفضة.
B. الظلام.
C. وجود مصادر ضوء.
D. وجود سيارات ومصابيح.
E. المطر.
F. الضباب.
G. أهداف متحركة.
H. المسافات الفعلية للموقع.

المبحث السابع: الحركة والظروف المتغيرة

تمثل الحركة أحد أهم العوامل التي قد تؤدي إلى فقدان التفاصيل. وقد تكون الحركة ناتجة عن الهدف، أو الخلفية، أو الكاميرا نفسها.(1)
ويشير NIST إلى أن الحركة قد تؤدي إلى تشوش الهدف، وأن ارتفاع الحركة قد ينتج عن كثرة الأجسام المتحركة أو سرعة حركة هدف واحد.(2)

أولًا: تشوش الحركة
يحدث Motion Blur عندما تتحرك الصورة بالنسبة إلى المستشعر خلال فترة التعريض.(3)
وتزداد المشكلة عادة عندما:(4)

- يكون الهدف سريعًا.
- تكون الإضاءة منخفضة.
- تكون سرعة الغالق منخفضة.
- تكون المسافة كبيرة.
- تكون الكاميرا نفسها غير مستقرة.

ثانيًا: سرعة الغالق
تؤدي زيادة سرعة الغالق إلى تقليل الفترة الزمنية التي يتعرض فيها المستشعر للصورة، مما يساعد في تقليل التشوش، بشرط توفر الضوء الكافي.(5)
وقد أشار NIST إلى أن سرعة الغالق الأعلى مفيدة في المشاهد المتحركة عندما تسمح ظروف الإضاءة بذلك.(6)

ثالثًا: معدل الإطارات
يؤثر معدل الإطارات في التمثيل الزمني للحركة، لكنه ليس بديلًا عن سرعة الغالق.(7)

فرفع معدل الإطارات لا يضـــمن وحده التخلص من Motion Blur إذا كان كل إطار نفسه مشوشًا.

ومن ثم ينبغي التمييز بين:(8)

- Frame Rate: عدد الإطارات في الثانية.
- Shutter Speed: مدة التعريض لكل إطار.

رابعًا: الظروف المتغيرة

تشمل:(9)

- تغير الإضاءة.
- تغير الطقس.
- تغير حركة الأفراد.
- تغير المركبات.
- إضافة عوائق.
- تغير ترتيب الموقع.
- تغير اتجاه الشمس.

ويجب تصـــميم النظام على أســاس الســيناريوهات المتوقعة، وليس على صــورة اختبار واحدة.

خامسًا: المعالجة الرقمية

قد تساعد تقنيات تقليل الضوضاء والتثبيت والمعالجة الديناميكية، لكنها قد تنتج آثارًا جانبية إذا كانت الإعدادات شديدة.(10)

لذلك ينبغي اختبار:(11)

- الحد من الضوضاء.
- WDR.
- التثبيت الإلكتروني.

- الشحذ.
- معالجة الحركة.

المراجع:

① NIST/VQiPS, *Motion*.

② NIST/VQiPS, *Motion*.

③ NIST/VQiPS, *Motion*.

④ NIST/VQiPS, *Motion*.

⑤ NIST/VQiPS, *Defining Video Quality Requirements*, pp. 19–20.

⑥ NIST/VQiPS, *Defining Video Quality Requirements*, pp. 19–20.

⑦ NIST/VQiPS, *Defining Video Quality Requirements*, pp. 19–20.

⑧ NIST/VQiPS, *Defining Video Quality Requirements*, pp. 19–20.

⑨ NIST/VQiPS, *Motion*.

⑩ NIST/VQiPS, *Motion*.

⑪ NIST/VQiPS, *Motion*.

المبحث الثامن: العوامل البيئية والحماية الميكانيكية للكاميرات

لا يمكن تقييم جودة الصـــورة بمعزل عن البيئة التي تعمل فيها الكاميرا. فالكاميرا الخارجية تتعرض لعوامل تختلف جذريًا عن البيئة الداخلية، وقد تؤثر هذه العوامل في العدسة والمستشعر والإلكترونيات والحامل والصورة نفسها.(1)

أولًا: أهم العوامل البيئية

تشمل:(2)

- الحرارة.
- البرودة.
- الرطوبة.
- الغبار.
- المطر.
- الضباب.
- الملح والرذاذ البحري.
- الرياح.
- الاهتزاز.
- الثلوج في البيئات التي تتعرض لها.
- المواد الكيميائية في البيئات الصناعية.

ثانيًا: أثر البيئة في الصورة

قد تؤدي:(3)

- قطرات الماء على العدسة إلى تشويه الصورة.
- الغبار إلى خفض التباين.
- الضباب إلى خفض الرؤية والتباين.
- الرياح إلى اهتزاز الكاميرا.

- الحرارة والرطوبة إلى التأثير في موثوقية المكونات.

ثالثًا: معيارIP

يمثل IEC 60529 المرجع الأساسي لتصنيف درجات الحماية التي توفرها الأغلفة ضد دخول الأجسام الصلبة والماء.(4)

ولا ينبغي تفسير IP على أنه "تصنيف لجودة الكاميرا"، وإنما تصنيف لحماية الغلاف وفق شروط الاختبار المعيارية.

ومن الأمثلة الشائعة:(5)

التصنيف	المعنى العام
IP65	حماية من الغبار + الحماية من نفاثات الماء وفق الاختبار المحدد
IP66	حماية من الغبار + مستوى أعلى من الحماية من نفاثات الماء
IP67	حماية من الغبار + تحمل الغمر المؤقت وفق شروط الاختبار
IP68	حماية من الغبار + غمر وفق شروط وعمق وزمن يحددها المصنع/المعيار والتصنيف المعلن

ولا يجوز تفسير IP68 مثلًا على أنه يعني أن أي جهاز يمكن غمره إلى أي عمق ولأي مدة؛ لأن شروط الأداء يجب الرجوع فيها إلى مواصفة المنتج واختبار التصنيف.(6)

رابعًا: الحماية الميكانيكيةIK

ينبغي إضافة معيار IK إلى الفصل، لأنه يعالج جانبًا مختلفًا عن IP.(7)

ويشير IEC 62262 إلى تصنيف درجات الحماية التي يوفرها الغلاف ضد الصدمات الميكانيكية الخارجية.(8)

وعليه IP ≠ IK :

فـــ IPيتعلق أساسًا بالحماية من الدخول والغبار والماء، بينما IK يتعلق بالحماية من الصدمات الميكانيكية.

خامسًا: اختيار الحماية البيئية

ينبغي أن يعتمد الاختيار على: (9)

- موقع الكاميرا.
- درجة التعرض للماء.
- الغبار.
- احتمال العبث.
- الصدمات.
- طبيعة الحامل.
- البيئة الصناعية.
- الحاجة إلى سخان أو مزيل رطوبة.
- متطلبات الصيانة.

المراجع:

① International Electrotechnical Commission, *IEC 60529:1989+A1:1999+A2:2013, Degrees of protection provided by enclosures (IP Code)*, (Geneva: IEC).

② IEC 60529.

③ IEC 60529.

④ IEC 60529.

⑤ IEC 60529.

⑥ IEC 60529.

⑦ International Electrotechnical Commission, *IEC 62262:2002+A1:2021, Degrees of protection provided by enclosures for electrical equipment against external mechanical impacts (IK Code)*, (Geneva: IEC).

.⑧ IEC 62262

.IEC 62262و⑨ IEC 60529

المبحث التاسع: اختيار مستوى الجودة وفق الهدف الأمني

بعد تحليل عناصر جودة الصورة، يصبح السؤال المركزي في التصميم:(1)
ما مستوى الجودة الذي تحتاجه المنشأة فعلًا؟
والإجابة العلمية ليست: "أعلى دقة متاحة"، وإنما:
ما أقل مستوى أداء يحقق الوظيفة الأمنية المطلوبة بصورة موثوقة في الظروف الفعلية؟
ويؤكد المختصـــون أن النظام ينبغي ألا يكون أعلى أو أقل من احتياجات التطبيق، وأن اختيار المكونات ينبغي أن ينطلق من حالة الاســـتخدام ومســـتوى التمييز المطلوب وحجم الهدف والحركة والإضاءة.(2)

أولًا: تحديد الهدف الأمني
قبل اختيار الكاميرا ينبغي تحديد ما إذا كان المطلوب:(3)

- وعيًا عامًا بالمشهد.
- كشف وجود شخص أو مركبة.
- متابعة الحركة.
- وصف خصائص الهدف.
- التعرف على شخص معروف.
- تحديد هوية.
- التحقق من هوية مدعاة.
- قراءة لوحة مركبة.
- توثيق واقعة.
- توفير مادة تحليلية لاحقة.

ثانيًا: تحديد حجم الهدف
يجب تحديد حجم الهدف المتوقع داخل الصـــورة. وقد أكد NIST أن حجم الهدف بالنسبة إلى مجال الرؤية يؤثر مباشرة في القدرة على تمييز التفاصيل.(4)

ثالثًا: تحديد الحركة

يجب تحديد: (5)

- سرعة الأشخاص.
- سرعة المركبات.
- كثافة الحركة.
- احتمال حركة الكاميرا.
- الحاجة إلى التتبع.

رابعًا: تحديد الإضاءة

يجب تحليل: (6)

- النهار.
- الليل.
- التغير اليومي.
- الإضاءة الخلفية.
- مصادر الضوء القوية.
- الانعكاسات.

خامسًا: تحديد كثافة البكسلات

بعد تحديد المهمة، تُحدد كثافة البكسلات المستهدفة وفق المعيار والإصدار المعتمد في المشروع. وهنا يجب عدم تقديم القيم على أنها ضمانات مستقلة؛ بل باعتبارها أهدافًا تصميمية معيارية أو إرشادية تحتاج إلى اختبار قبول موقعي. (7)

سادسًا: الضغط والترميز ومعدل البت

لا يكفي أن تنتج الكاميرا صورة جيدة عند المستشعر؛ بل يجب أن تحافظ المنظومة على التفاصيل أثناء الترميز والتخزين والنقل.(8)

1. الضغط

يؤدي الضغط إلى تقليل كمية البيانات، وقد يؤدي الضغط المفرط إلى فقد تفاصيل مهمة. ويشير NIST إلى أن الضغط قد يؤدي إلى فقد غير قابل للاسترجاع، وأن مقدار الضغط ينبغي أن يرتبط بمتطلبات التخزين والاستخدام.(9)

2. معدل البتBitrate

معدل البت هو مقدار البيانات التي ينقلها أو ينتجها تدفق الفيديو خلال وحدة زمنية. ويُقاس عادة بـ:(10)

- bit/s.
- kbit/s.
- Mbit/s.

وارتفاع معدل البت لا يعني دائمًا جودة أفضل بصورة مطلقة، لكنه يوفر عادة قدرة أكبر على تمثيل التفاصيل عندما تكون العوامل الأخرى متساوية.

3. العلاقة بين الضغط ومعدل البت

يمكن تبسيط العلاقة كما يأتي:(11)

- ضغط أعلى ← بيانات أقل ← تخزين وشبكة أقل ← احتمال فقد تفاصيل أكبر.
- ضغط أقل ← بيانات أكثر ← متطلبات شبكة وتخزين أعلى ← قدرة أكبر على المحافظة على التفاصيل.

وتوضح المراجع المهنية الخاصة بالتحكم في معدل البت أن جودة الفيديو تتأثر بالضغط، ومعدل البت، ودقة الصورة، ومعدل الإطارات، وطولGOP ، وتعقيد المشهد.(12)

سابعًا H.264 :وH.265

تستخدم أنظمة المراقبة الحديثة تقنيات ترميز مثل:(13)

- H.264/AVC.
- H.265/HEVC.

وتوفر هذه المعايير وسائل فعالة لخفض حجم الفيديو مقارنة بالفيديو غير المضغوط، لكن المقارنة بينهما لا ينبغي أن تُختزل في نسبة ثابتة من قبيل "H.265 يوفر دائمًا ٥٠٪"؛ لأن مقدار الوفر يعتمد على المشهد والإعدادات والدقة ومعدل الإطارات ومستوى الجودة.(14)

وتشير ONVIF إلى دعم H.264 و H.265ضمن Profile T المتعلق بالبث المتقدم للفيديو.(15)

ثامنًا: معدل الإطارات والتخزين

ارتفاع معدل الإطارات يؤدي عادة إلى زيادة كمية البيانات إذا بقيت بقية المتغيرات ثابتة.(16)

لذلك ينبغي اختيار معدل الإطارات وفق المهمة:(17)

- مشهد ثابت نسبيًا → قد لا يحتاج إلى معدل مرتفع.
- حركة مستمرة → قد يحتاج إلى معدل أعلى.
- مركبات سريعة → يتطلب دراسة مشتركة لمعدل الإطارات وسرعة الغالق.
- التحليلات الآلية → ينبغي الرجوع إلى متطلبات خوارزمية التحليل.

تاسعًا: حساب تقريبي للتخزين(19)

يمكن تقدير السعة الخام للتخزين من خلال:(18)

$$\text{Storage} = (\text{Bitrate} \times \text{Time}) / 8$$

فإذا كان معدل البت4 Mbit/s :

فإن كمية البيانات النظرية في يوم واحد تقارب:

$$(4 \times 86400) / 8 = 43200 \text{ MB}$$

أي نحو43. 2 GB/day :

قبل إضافة الاعتبارات الخاصة بوحدات القياس، والبيانات المرافقة، والهوامش، ونظام الملفات، وأسلوب التسجيل.

ولهذا فإن تقدير التخزين ينبغي أن يعتمد على معدل البت الفعلي المتوقع وليس على الدقة وحدها.(20)

عاشرًا: مصفوفة اختيار الجودة

بدل الجدول الذي يربط كل هدف أمني بدقة ثابتة مثل "٤" K = Identification، يعتمد هذا الفصل المصفوفة الآتية:(21)

١. العوامل الحاسمة والأهداف التصميمية لوظائف المراقبة

- الوعي العام:(General Awareness)
  - العوامل الحاسمة :مجال الرؤية، مستوى التباين، واستقرار الصورة.
  - الهدف التصميمي :توفير رؤية شاملة للمشهد ومتابعة الحركة داخله.
  - الوظيفة :تحقيق الوعي العام بالموقع والأحداث الجارية.
  - أسلوب التحقق :اختبار المشهد الفعلي والتأكد من وضوح الرؤية والحركة.
- الكشف:(Detection)
  - العوامل الحاسمة :حجم الهدف، كثافة البكسلات لكل متر(PPM) ، وحركة الهدف.
  - الهدف التصميمي :إثبات وجود الهدف واكتشافه ضمن نطاق المراقبة.
  - الوظيفة :الكشف عن الأشخاص أو المركبات أو الأجسام محل الاهتمام.
  - أسلوب التحقق :استخدام أهداف اختبارية للتحقق من قدرة النظام على الكشف.
- الملاحظة:(Observation)
  - العوامل الحاسمة :كثافة البكسلات(PPM) ، خصائص العدسة، ومستوى الإضاءة.

- الهدف التصميمي: توفير معلومات كافية لوصف حركة الهدف وخصائصه العامة.
- الوظيفة: متابعة الهدف والحصول على معلومات وصفية عنه.
- أسلوب التحقق: إجراء اختبار موقعي في الظروف التشغيلية الفعلية.

- التعرّف: (Recognition)
- العوامل الحاسمة: كثافة البكسلات، جودة العدسة، ومستوى الإضاءة.
- الهدف التصميمي: ربط الهدف بخصائص أو مواصفات شخص أو جسم معروف.
- الوظيفة: تمكين المشغّل من التعرف على الهدف وتصنيفه بصورة موثوقة.
- أسلوب التحقق: إجراء اختبار بشري مضبوط لقياس قدرة الأشخاص على التعرف على الهدف.

- تحديد الهوية: (Identification)
- العوامل الحاسمة: ارتفاع كثافة البكسلات، جودة البصريات، مستوى الإضاءة، وجودة الضغط الرقمي للصورة.
- الهدف التصميمي: توفير مستوى التفاصيل اللازم للوصول إلى الهوية المطلوبة.
- الوظيفة: تحديد هوية الشخص أو الهدف بدرجة عالية من الثقة.
- أسلوب التحقق: إجراء اختبار قبول للتأكد من تحقيق المستوى المطلوب من الأداء.

- التحقق من الهوية: (Verification)
- العوامل الحاسمة: التفاصيل الدقيقة، جودة صورة الوجه أو الهدف، وظروف الالتقاط.
- الهدف التصميمي: مقارنة الهوية المدعاة مع مرجع أو سجل معروف.
- الوظيفة: التأكد من تطابق الشخص أو الهدف مع الهوية المرجعية.
- أسلوب التحقق: إجراء اختبار وظيفي يحاكي ظروف الاستخدام الفعلية.

- قراءة لوحات المركبات: (License Plate Reading)

- العوامل الحاسمة :حجم اللوحة، سرعة المركبة، سرعة الغالق، استخدام الأشعة تحت الحمراء(IR) ، وزاوية التصوير.
- الهدف التصـــميمي :الحصـــول على صـــورة واضـــحة تمكّن من قراءة الأحرف والأرقام الموجودة على اللوحة.
- الوظيفة :قراءة وتسجيل بيانات لوحات المركبات بدقة.
- أسلوب التحقق :إجراء اختبارات باستخدام لوحات مركبات فعلية وتحت ظروف تشغيل مختلفة.

وهذا الجدول إطار تصميمي وليس معيارًا رقميًا ملزمًا.(22)

حادي عشر: الاختبار والقبول

لا ينبغي اعتبار التصميم مكتملًا بمجرد تركيب الكاميرات. بل ينبغي تنفيذ:(23)

١. اختبار نهاري.
٢. اختبار ليلي.
٣. اختبار في الإضاءة الخلفية.
٤. اختبار في الحركة.
٥. اختبار للمسافات الحرجة.
٦. اختبار للتسجيل.
٧. اختبار للاسترجاع.
٨. اختبار للتخزين.
٩. اختبار لمعدل البت.
١٠. اختبار للشبكة.
١١. اختبار للعرض.
١٢. اختبار للغرض الأمني النهائي.

وتؤكد IEC 62676-4:2025 أن نطاقها يشمل التخطيط والتصميم والتركيب والاختبار والتشغيل والصيانة، وهو ما يدعم النظر إلى جودة الصورة باعتبارها موضوعًا يجب التحقق منه ضمن دورة حياة المنظومة، وليس عند شراء الكاميرا فقط.(24)

ثاني عشر: قاعدة الاختيار النهائية

يمكن صياغة قاعدة هذا المبحث على النحو الآتي:(25)

لا تختار الكاميرا أولًا ثم تبحث عن استخدام لها؛ بل حدد الاستخدام الأمني أولًا، ثم حدد مستوى التفاصيل المطلوب، ثم صمم البصريات والمسافة والإضاءة والدقة والترميز والتخزين والشبكة بما يحقق ذلك المستوى، وأخيرًا تحقق من النتيجة ميدانيًا.

المراجع:

① NIST/VQiPS, *Discrimination Level* و*GUC Aspects.*

② NIST/VQiPS, *Discrimination Level* و*GUC Aspects.*

③ NIST/VQiPS, *GUC Aspects.*

④ NIST/VQiPS, *Target Size.*

⑤ NIST/VQiPS, *GUC Aspects.*

⑥ NIST/VQiPS, *GUC Aspects*.

.⑦ Axis Communications, *Pixel density based on IEC 62676-4:2025*, 2026

⑧ NIST/VQiPS, *Defining Video Quality Requirements*, pp. 15–19.

⑨ NIST/VQiPS, *Defining Video Quality Requirements*, pp. 15–19.

⑩ NIST/VQiPS, *Defining Video Quality Requirements*, pp. 15–19.

⑪ NIST/VQiPS, *Defining Video Quality Requirements*, pp. 15–19.

.⑫ Axis Communications, *Bit rate control*, 2026

⑬ ONVIF, *Profile T – Advanced Video Streaming*.

⑭ ONVIF, *Profile T – Advanced Video Streaming*.

⑮ ONVIF, *Profile T – Advanced Video Streaming*.

⑯ NIST/VQiPS, *Defining Video Quality Requirements*, pp. 15–19.

⑰ NIST/VQiPS, *Defining Video Quality Requirements*, pp. 15–19.

⑱ NIST/VQiPS, *Defining Video Quality Requirements*, pp. 15–19.

⑲ NIST/VQiPS, *Defining Video Quality Requirements*, pp. 15–19.

⑳ NIST/VQiPS, *Defining Video Quality Requirements*, pp. 15–19.

㉑ NIST/VQiPS, *GUC Aspects*.

㉒ NIST/VQiPS, *GUC Aspects*.

㉓ NIST/VQiPS, *Defining Video Quality Requirements*, pp. 19–20.

㉔ International Electrotechnical Commission, *IEC 62676-4:2025*, (Geneva: IEC, 2025).

㉕ NIST/VQiPS, *GUC Aspects*.

خلاصة الفصل الثالث

يتضح مما سبق أن جودة الصورة في أنظمة المراقبة بالفيديو ليست خاصية منفردة يمكن اختزالها في الدقة أو عدد الميجابكسلات، وإنما هي نتيجة لتفاعل مجموعة من العوامل الفنية والبيئية والتشغيلية.

وتبدأ هذه السلسلة من الغرض الأمني؛ ثم تحديد مستوى التمييز المطلوب، وحجم الهدف، والمسافة، ومجال الرؤية، والعدسة، والمستشعر، والإضاءة، والحركة، ثم تمتد إلى المعالجة والترميز والضغط ومعدل البت والنقل والتخزين والعرض.

كما أظهرت الدراسة أن استخدام مصطلحات Detection و Recognition و Identificationو Verificationيحتاج إلى ضبط مفاهيمي، وأنه لا يجوز التعامل معها بوصفها مراتب مترادفة. كما يجب التمييز بين سلم DORI التاريخي وبين الإطار التشغيلي الأحدث المرتبط بـIEC 62676-4:2025.

وتبين كذلك أن قيم PPM لا ينبغي استخدامها بصورة منفصلة عن ظروف المشهد، وأن معادلات مجال الرؤية وكثافة البكسلات أدوات تصميمية مفيدة، لكنها لا تحل محل الاختبار الفعلي.

أما الإضاءة، فقد تبين أن استخدام أرقام Lux جامدة لتصنيف المواقع أو اختيار الكاميرات يمثل تبسيطًا مفرطًا؛ لأن قيمة Lux وحدها لا تكشف النطاق الديناميكي أو طبيعة المشهد أو أداء الكاميرا في الحركة.

وفي مجال الرؤية الليلية، ينبغي الفصل بين التصوير منخفض الإضاءة، وكاميرات Day/NightمعIR ، والإضاءة البيضاء، والتصوير الحراري؛ فلكل تقنية مجال وظيفي مختلف.

كما أضيف إلى الفصل البعد الذي كان ناقصًا، وهو الضغط ومعدل البت؛ لأن جودة الصورة التي تنتجها الكاميرا يمكن أن تتدهور أثناء الترميز أو النقل أو التخزين إذا كانت الموارد غير كافية أو كان الضغط مفرطًا.

وأخيرًا، فإن حماية الكاميرا بيئيًا لا تقتصر علىIP ، بل يجب النظر أيضًا إلى IK عندما تكون الصدمات أو العبث الميكانيكي من المخاطر المحتملة.

أهم نتائج الفصل الثالث

١. جودة الصورة مفهوم وظيفي يرتبط بالهدف الأمني.
٢. جودة الجهاز لا تساوي جودة الصورة.
٣. الدقة عنصر مهم لكنها ليست معيارًا منفردًا.
٤. كثافة البكسلات أداة مهمة في التصميم.
٥. يجب تحديد إصدار المعيار عند استخدام مستويات الأداء البصري.
٦. البعد البؤري ومجال الرؤية يعتمدان على أبعاد المستشعر والعدسة.
٧. المسافة عنصر حاسم في كمية التفاصيل المتاحة.
٨. الإضاءة ينبغي تحليلها ميدانيًا وليس اختزالها في رقم Lux واحد.
٩. WDR وBLC وHLC تقنيات مختلفة لمعالجة ظروف الإضاءة.
١٠. IR لا يساوي التصوير الحراري.
١١. التصوير الحراري لا يمثل بديلًا مطلقًا للتصوير المرئي.
١٢. الحركة تتطلب معالجة مشتركة لمعدل الإطارات وسرعة الغالق والإضاءة.
١٣. الضغط ومعدل البت يؤثران في القيمة الجنائية أو التحقيقية للصورة.
١٤. الشبكة والتخزين والعرض جزء من جودة الفيديو النهائية.
١٥. IP يختص بالحماية من دخول الأجسام والماء، بينما IK يتعلق بالحماية من الصدمات الميكانيكية.
١٦. الجداول الرقمية ينبغي أن تُعرض بوصفها أهدافًا تصميمية أو قيمًا معيارية مرتبطة بإصدار محدد.
١٧. الاختبار الموقعي هو الوسيلة النهائية للتحقق من تحقيق الغرض الأمني.

أسئلة التفكير والتقييم للفصل الخامس

أولًا: أسئلة معرفية

١. ما المقصود بجودة الصورة في نظام المراقبة؟
٢. ما الفرق بين جودة الجهاز وجودة الصورة؟

٣. ما المقصود بكثافة البكسلات؟ وما الفرق بين PPM وPPF؟
٤. ما العلاقة بين البعد البؤري ومجال الرؤية؟
٥. ما العوامل المؤثرة في جودة الصورة ليلًا؟
٦. ما الفرق بين IR والتصوير الحراري؟
٧. ما الفرق بين WDR و BLCوHLC؟
٨. ما المقصود بالضغط ومعدل البت؟
٩. ما الفرق بين IP وIK؟

ثانيًا: أسئلة تحليلية

١٠. لماذا لا تكفي دقة ٤ Kأو ٨ Kوحدها للحكم على جودة الكاميرا؟
١١. حلل العلاقة بين المسافة وكثافة البكسلات.
١٢. ناقش أثر العدسة في الأداء الأمني.
١٣. لماذا قد تكون كاميرا أقل دقة أكثر فاعلية من كاميرا أعلى دقة؟
١٤. لماذا لا ينبغي استخدام Lux وحده معيارًا لاختيار الكاميرا الليلية؟
١٥. قارن بين IR والتصوير الحراري من منظور الكشف والتعرف وتحديد الهوية.
١٦. حلل أثر الضغط ومعدل البت في القيمة التحقيقية للفيديو.
١٧. لماذا يجب اختبار المنظومة في ظروف الموقع الفعلية؟
١٨. ناقش الفرق بين IP و IKوأهمية كل منهما في التصميم الأمني.

ثالثًا: أسئلة تطبيقية

١٩. اختر منشأة تعليمية وحدد الاستخدام الأمني لكل كاميرا محتملة.
٢٠. صمم مصفوفة تربط بين الهدف الأمني والعدسة والمسافة وكثافة البكسلات.
٢١. احسب مجال الرؤية لكاميرا وفق أبعاد المستشعر والبعد البؤري والمسافة.
٢٢. احسب PPM لهدف يقع على مسافة محددة.
٢٣. صمم سيناريو اختبار ليلي لكاميرا خارجية.

٢٤. صـمم اختبار قبول للتحقق من قدرة الكاميرا على تحديد هوية الأشـخاص عند مدخل منشأة.

٢٥. احســـب متطلبات التخزين الأولية وفق معدل بت معلوم وعدد كاميرات ومدة احتفاظ محددة.

٢٦. قارن بين كاميرتين مختلفتين في الدقة والعدســـة ومجال الرؤية، ثم حدد أيهما أفضل لغرض أمني محدد.

٢٧. ضـــع مواصـــفة فنية لكاميرا خارجية معرضـــة للغبار والمطر والعبث الميكانيكي، مع تحديد متطلبات IP و IKالمناسبة بعد تحليل المخاطر.

الفصل السادس: التسجيل والتخزين وإدارة المعلومات

تمهيد الفصل

تمثل عملية التسجيل والتخزين المرحلة التي تنتقل فيها منظومة المراقبة بالفيديو من مجرد المشاهدة الآنية إلى إنتاج سجل معلوماتي يمكن الرجوع إليه عند الحاجة. فالمراقبة المباشرة تحقق قيمة تشغيلية آنية، بينما يسمح التسجيل بتحويل المشهد الذي وقع في لحظة معينة إلى مادة يمكن مراجعتها وتحليلها واستخدامها في التحقق من الأحداث ودعم التحقيقات اللاحقة.(1)

ومن هذا المنطلق، فإن وجود كاميرات ذات جودة مرتفعة لا يضمن وحده نجاح منظومة المراقبة. فقد تنتج الكاميرا صورة ممتازة، لكن إذا لم تُسجل بالجودة المناسبة، أو لم تتوافر سعة تخزين كافية، أو لم يتم الاحتفاظ بها للمدة المطلوبة، أو تعذر البحث عنها واسترجاعها، فإن القيمة الأمنية الفعلية للنظام تنخفض بصورة كبيرة. ويؤكد دليل Video Quality in Public Safety (VQiPS)أن التخزين السليم للفيديو مهم بصورة خاصة في التطبيقات الإثباتية والتحقيقية، وأن فقد البيانات أو تدهورها أثناء التخزين قد يجعلها غير قابلة للاستخدام في المستقبل.(2)

وتزداد أهمية التسجيل في المنشآت التي تتطلب القدرة على إعادة بناء الأحداث بعد وقوعها، مثل المنشآت الحيوية، والمداخل والمخارج، والمناطق الحساسة، ومواقف المركبات، والمستودعات، والمواقع التي ترتبط فيها أنظمة المراقبة بأنظمة الإنذار أو التحكم في الدخول.

وقد أصبحت منظومات الفيديو الحديثة أكثر تعقيدًا نتيجة الانتقال من التسجيل المركزي التقليدي إلى نماذج متعددة تشمل التسجيل في أجهزةNVR ، والتخزين الطرفي داخل الكاميرا، والتخزين المركزي، والتخزين الموزع، والحلول السحابية أو الهجينة. ويتيحONVIF Profile G ، على سبيل المثال، وظائف مرتبطة بالتسجيل والبحث والاسترجاع والتشغيل في الأنظمة القائمة على بروتوكولاتIP ، بما في ذلك بعض حالات التخزين الطرفي.(3)

ولا ينبغي النظر إلى التخزين باعتباره مسألة سعة أقراص فقط، بل بوصفه منظومة متكاملة تتداخل فيها جودة الفيديو، ومعدل البيانات، وعدد الكاميرات، ونمط

التسـجيل، ومدة الاحتفاظ، وطريقة البحث، وآليات الحماية، والنسـخ الاحتياطي، وإدارة الصـلاحيات. وتؤكد IEC 62676-4:2025 أن نظام المراقبة بالفيديو ينبغي أن يُنظر إليه ضـمن دورة حياة متكاملة تشـمل التخطيط والتصـميم والتركيب والاختبار والتشغيل والصيانة، وأن التسجيل والتخزين يمثلان جزءًا من هذه الدورة، وليسا إجراءً لاحقًا منفصلًا عن التصميم.(4)

وعليه، يهدف هذا الفصل إلى دراسة التسجيل والتخزين وإدارة المعلومات بوصفها عناصر مترابطة في منظومة الأمن الوقائي والمراقبة بالفيديو، وصولًا إلى بناء معيار عملي يمكن من خلاله تحديد ما الذي ينبغي تسجيله، وبأي جودة، ولأي مدة، وكيف ينبغي حفظه واسترجاعه وحمايته.

ويتناول الفصل تسعة مباحث مترابطة: أهمية التسجيل الأمني، وأنماط التسجيل، وجودة التسجيل، وسعة التخزين، ومدة الاحتفاظ بالتسجيلات، والبحث والاسترجاع، والنسخ الاحتياطي، وإدارة التسجيلات، وحماية التسجيلات وسلامتها.

التسجيل والتخزين وإدارة المعلومات المعلومات
في منظومة الأمن الوقائي والمراقبة بالفيديو
أهمية الأمني
أنماط التسجيل
REC
جودة التسجيل
4K
سعة التخزين
مدة الاحتفاظ بالتسجيلات
مدة الاحتفاظ بالتسجيلات
البحث والاسترجاع
سعة التخزين
النسخ الاحتياطي
التسجيلات وسلامتها
المعيار العملي لاتخاذ القرار
1- ماذا نسجل؟
2- بأي جودة؟
3- كم نحتفظ به؟
4- كيف نخزنه؟
5- كيف نسترجعه؟
6- كيف نحميه؟

المبحث الأول: أهمية التسجيل الأمني

لا تقتصر وظيفة منظومة المراقبة بالفيديو على عرض المشاهد في الوقت الحقيقي؛ إذ إن إحدى أهم وظائفها الأمنية تتمثل في إنشاء سجل يمكن الرجوع إليه بعد وقوع الحدث. وعندما يحدث حادث أمني، فإن المشاهدة المباشرة قد لا تكون كافية، خصوصًا إذا وقع الحدث في لحظة لم يكن فيها المشغل ينظر إلى الشاشة أو إذا تطلب التحقيق مراجعة تسلسل الأحداث الذي سبق الواقعة وتلاها. ومن هنا يصبح التسجيل جزءًا من الذاكرة الأمنية للمنشأة.(1)

ويكتسب هذا المبحث أهمية خاصة لأنه يضع الأساس المفاهيمي الذي يوجه جميع القرارات اللاحقة المتعلقة بأنماط التسجيل وجودته وسعته ومدة الاحتفاظ به، ويجنب الخلط بين التسجيل كوظيفة تقنية والتسجيل كعملية أمنية متكاملة.(2)

أولًا: التسجيل بوصفه ذاكرة أمنية

يسمح التسجيل بحفظ المعلومات المرئية لفترة محددة، بحيث يمكن الرجوع إليها عند الحاجة. وتختلف قيمة التسجيل بحسب طبيعة المهمة الأمنية؛ فقد يكون الغرض منه مجرد معرفة ما حدث، أو تحديد توقيت الحدث، أو التعرف على الأشخاص والمركبات، أو تحليل تسلسل الأحداث.(3)

وبالتالي فإن قيمة التسجيل لا تقاس بمجرد وجود ملف فيديو، وإنما بمدى قدرة هذا الملف على الإجابة عن الأسئلة الأمنية المطلوبة. فقد يكون التسجيل كافيًا لإثبات وجود شخص في منطقة معينة، لكنه غير كافٍ للتعرف على ملامحه. وقد يكون مناسبًا لمعرفة اتجاه حركة مركبة، لكنه غير مناسب لقراءة لوحة المركبة.

ثانيًا: الوظائف الأمنية للتسجيل

يؤدي التسجيل الأمني خمس وظائف رئيسة: (4)

1. التوثيق

حفظ الأحداث والوقائع في سجل يمكن الرجوع إليه لاحقًا.

2. دعم التحقيق

توفير أدلة بصرية يمكن استخدامها في التحقيق أو المساءلة. وتشير NIST إلى أن التخزين السليم للفيديو مهم بصورة خاصة في التطبيقات الإثباتية والتحقيقية، وأن فقد البيانات أو تدهورها أثناء التخزين قد يجعلها غير قابلة للاستخدام في المستقبل.(5)

3. دعم الاستجابة

توفير معلومات يمكن الرجوع إليها أثناء الأحداث أو بعدها. فقد يحتاج فريق الأمن إلى معرفة ما سبق إطلاق الإنذار، أو تحديد مسار شخص داخل المنشأة، أو معرفة نقطة الدخول التي استخدمها، أو تحديد المركبة المرتبطة بالحدث.(6)

4. المراجعة والتحسين

تمكين مراجعة الأداء الأمني وتحسينه.

5. الامتثال

تلبية المتطلبات التنظيمية والقانونية.

ثالثًا: التسجيل كعنصر في سلسلة الأمن

يمكن النظر إلى القيمة الأمنية للتسجيل وفق السلسلة الآتية: (7)

التقاط الصورة ← نقلها ← تسجيلها ← حفظها ← البحث عنها ← استرجاعها ← تحليلها ← استخدامها في القرار الأمني

وأي خلل جوهري في إحدى هذه المراحل يمكن أن يقلل القيمة النهائية للمعلومة.

رابعًا: الفرق بين التسجيل الحي والتسجيل المؤجل

ينبغي التمييز بين:(8)

- التسجيل الحي :مشاهدة الأحداث في الوقت الحقيقي.
- التسجيل المؤجل :الرجوع إلى الأحداث بعد وقوعها.

والتسجيل المؤجل هو الذي يحقق القيمة الأمنية الكاملة، لأن الأحداث الأمنية لا يمكن التنبؤ بها دائمًا، ولأن التحقيق والمساءلة يحتاجان إلى سجل يمكن الرجوع إليه.

خامسًا: خصائص التسجيل الأمني الفعال

يتميز التسجيل الأمني الفعال بخصائص عدة:(9)

- الاكتمال :تغطية جميع الأحداث المهمة.
- الدقة :توثيق الأحداث بدقة.
- الاستمرارية :عدم انقطاع التسجيل.
- الموثوقية :ضمان سلامة التسجيلات.
- الاسترجاع :سهولة الوصول إلى التسجيلات.
- الحماية :حماية التسجيلات من العبث أو الفقدان.

المراجع:

① International Electrotechnical Commission, *IEC 62676-4: Video surveillance systems for use in security applications – Part 4: Application guidelines*, (Geneva: IEC, 2nd ed., 2025).

② National Institute of Standards and Technology, *VQiPS: Storage*, (Gaithersburg, MD: NIST).

③ NIST/VQiPS, *VQiPS: Storage*.

④ NIST/VQiPS, *VQiPS: Storage*.

⑤ NIST/VQiPS, *VQiPS: Storage*.

⑥ NIST/VQiPS, *VQiPS: Storage*.

⑦ NIST/VQiPS, *VQiPS: Storage*.

⑧ NIST/VQiPS, *VQiPS: Storage*.

⑨ NIST/VQiPS, *VQiPS: Storage*.

المبحث الثاني: أنماط التسجيل

لا يوجد نمط تسجيل واحد مناسب لجميع المنشآت، بل ينبغي اختيار نمط التسجيل بناءً على طبيعة المخاطر والغرض الأمني ودرجة أهمية المنطقة. ويختلف أسلوب التسجيل باختلاف طبيعة النظام والهدف الأمني والموارد المتاحة. ولذلك ينبغي أن ينظر المصمم إلى نمط التسجيل باعتباره قرارًا أمنيًا وفنيًا في آن واحد، وليس مجرد إعداد برمجي.(1)

أولًا: التسجيل المستمر

يقصد به تسجيل الفيديو بصورة متواصلة خلال فترة التشغيل المحددة.(2)

المزايا:

- تغطية كاملة لجميع الأحداث.
- عدم فقدان أي حدث.
- بساطة الإدارة.

القيود:

- متطلبات تخزين مرتفعة.
- متطلبات شبكة مرتفعة.
- صعوبة البحث في كميات كبيرة من البيانات.

الاستخدام:

- المداخل الرئيسية.
- مناطق استقبال الزوار.
- غرف التحكم.
- المناطق ذات القيمة الأمنية العالية.
- بعض المواقع المحيطية.(3)

ثانيًا: التسجيل عند الحركة

يبدأ التسجيل أو ينتقل النظام إلى وضع التسجيل الأعلى جودة عند اكتشاف حركة وفق خوارزمية أو إعداد معين.(4)

المزايا:

- توفير مساحة التخزين.
- تقليل حجم البيانات.
- سهولة البحث.

القيود:

- قد يفوت أحداثًا بطيئة أو غير حركية.
- يعتمد على دقة كشف الحركة.
- قد يؤدي إلى تسجيلات زائدة أو ناقصة.

الاستخدام:

- الممرات منخفضة النشاط.
- المناطق ذات الأولوية المتوسطة.
- البيئات التي تقل فيها الأحداث.(5)

ثالثًا: التسجيل عند الحدث

يرتبط التسجيل بحدث صادر من الكاميرا أو نظام آخر، مثل إنذار أمني أو حدث وصول أو فتح باب.(6)

المزايا:

- تسجيلات مركزة على الأحداث.
- توفير كبير في التخزين.
- تكامل مع الأنظمة الأمنية الأخرى.

القيود:

- يعتمد على دقة نظام الإنذار.
- قد يفوت أحداثًا لم يكتشفها نظام الإنذار.

- يتطلب تكاملًا تقنيًا.

الاستخدام:

- نقاط التحكم.
- البيئات التي تتكامل فيها المراقبة مع أنظمة أخرى.
- المناطق التي تقل فيها الأحداث.(7)

رابعًا: التسجيل المجدول

يحدد النظام فترات زمنية معينة للتسجيل، مثل تسجيل مستمر أثناء ساعات العمل وتسجيل مختلف خارجها.(8)

المزايا:

- مرونة في إدارة التسجيلات.
- توفير في التخزين.
- تكييف مع أنماط النشاط.

القيود:

- قد يفوت أحداثًا خارج الأوقات المحددة.
- يتطلب معرفة دقيقة بأنماط النشاط.

الاستخدام:

- المنشآت ذات الأنشطة المتغيرة.
- المناطق التي تختلف فيها المخاطر بين النهار والليل.(9)

خامسًا: التسجيل المختلط

قد يكون الحل الأكثر كفاءة في بعض المنشآت هو الجمع بين الأنماط:(10)

- تسجيل مستمر للمدخل الرئيسي.
- تسجيل بالحركة في الممرات منخفضة النشاط.
- تسجيل مرتبط بالأحداث في نقاط التحكم.

- جودة تسجيل أعلى عند وقوع إنذار.

ويحقق هذا الأسلوب توازنًا بين الاستمرارية وسعة التخزين.

سادسًا: التسجيل الطرفي

يمكن أن يحدث التسجيل داخل الكاميرا أو جهاز طرفي قريب من مصدر الصورة. ويعد ONVIF Profile G من المعايير التي تغطي وظائف التسجيل والتخزين والاسترجاع في الأنظمة القائمة على IP ، بما في ذلك الأجهزة ذات التخزين الطرفي (11).

وتفيد هذه البنية في بعض التطبيقات التي تتطلب استمرار التسجيل عند انقطاع الاتصال بالخادم المركزي، على أن تتم إدارة المزامنة والاسترجاع وفق تصميم النظام.

سابعًا: التسجيل المركزي

يتم إرسال الفيديو إلى NVR أو خادم تسجيل أو منصة إدارة فيديو مركزية.(12)

المزايا:

- الإدارة الموحدة.
- سهولة المراقبة المركزية.
- توحيد سياسات الاحتفاظ.
- إمكانية إدارة عدد كبير من الكاميرات من موقع مركزي.

القيود:

- الاعتماد المفرط على نقطة مركزية واحدة قد يجعلها هدفًا لفشل النظام أو نقطة اختناق.
- يحتاج إلى دراسة الاعتمادية والتكرار.

ثامنًا: التسجيل الموزع

قد توزع عمليات التسجيل بين عدة أجهزة أو مواقع بدل الاعتماد على نقطة واحدة (13).
ويفيد ذلك في المنشآت الواسعة أو متعددة المواقع، كما يمكن أن يقلل أثر تعطل جزء من المنظومة.

تاسعًا: مصفوفة اختيار نمط التسجيل
يمكن بناء مصفوفة لاختيار نمط التسجيل وفق المنطقة والوظيفة الأمنية: (14)
وهذا ليس معيارًا ملزمًا.(15)
توزيع أنماط المراقبة والتسجيل حسب المناطق
المدخل الرئيسي:

الوظيفة الأمنية: التعرف على الأشخاص والتحقق من هوياتهم.
نمط التسجيل: تسجيل مستمر لضمان توفر سجل متكامل لحركة الدخول والخروج.
جودة الصورة: عالية، بما يضمن توفير التفاصيل اللازمة لعمليات التعرف والتحقق.
بوابة المركبات:

الوظيفة الأمنية: قراءة وتوثيق لوحات المركبات.
نمط التسجيل: تسجيل مستمر، مع تفعيل التسجيل المرتبط بالأحداث عند مرور المركبات أو اكتشاف نشاط ذي صلة.
جودة الصورة: عالية جدًا، لضمان وضوح الأحرف والأرقام في ظروف التشغيل المختلفة.
الممرات:

الوظيفة الأمنية: المراقبة العامة ومتابعة حركة الأشخاص.
نمط التسجيل: التسجيل عند اكتشاف الحركة، بهدف تقليل حجم البيانات المسجلة مع الحفاظ على الأحداث المهمة.

جودة الصورة: متوسطة، بما يتناسب مع طبيعة المراقبة العامة.
المكاتب:

الوظيفة الأمنية: المراقبة العامة ومتابعة الأنشطة داخل المنطقة.
نمط التسجيل: تسجيل مجدول وفق أوقات العمل أو الفترات التي تتطلب المراقبة.
جودة الصورة: متوسطة، نظرًا لأن الهدف الأساسي هو المراقبة العامة وليس تحديد الهوية.
المخازن:

الوظيفة الأمنية: الكشف عن الحركة أو الأنشطة غير المعتادة.
نمط التسجيل: التسجيل عند اكتشاف الحركة، مع تعزيز التسجيل عند ورود إنذار أمني.
جودة الصورة: متوسطة، مع التركيز على القدرة على اكتشاف النشاط وتحديد موقعه.
المحيط الخارجي:

الوظيفة الأمنية: كشف محاولات التسلل أو الدخول غير المصرح به.
نمط التسجيل: التسجيل عند اكتشاف الحركة، بما يتيح متابعة الأنشطة غير الاعتيادية.
جودة الصورة: متوسطة، مع إعطاء الأولوية لتغطية المساحات الواسعة واكتشاف الحركة.
المناطق الحساسة:

الوظيفة الأمنية: حماية الأصول والمنشآت أو المواقع ذات الأهمية الأمنية العالية.
نمط التسجيل: تسجيل مستمر لضمان توثيق جميع الأحداث دون انقطاع.
جودة الصورة: عالية، بما يتيح الحصول على تفاصيل كافية لدعم الكشف والتعرف والتحقق عند الحاجة.

المبحث الثالث: جودة التسجيل

لا تعني عملية التسجيل حفظ أي صورة فحسب؛ إذ ينبغي أن تحفظ الصورة بدرجة جودة تتناسب مع الوظيفة الأمنية التي أنشئ النظام من أجلها. وقد يؤدي خفض جودة التسجيل بهدف توفير مساحة التخزين إلى فقد تفاصيل لا يمكن استعادتها لاحقًا (1).

ويكتسب هذا المبحث أهمية خاصة لأنه يوضح العلاقة بين جودة التسجيل وجودة الصورة الأصلية، ويبين أن جودة التسجيل جزء من سلسلة الجودة التي تبدأ من الكاميرا وتنتهي عند العرض.(2)

أولًا: العلاقة بين جودة الالتقاط وجودة التسجيل

إذا التقطت الكاميرا صورة عالية الجودة ثم سجل النظام نسخة منخفضة الجودة، فإن التحقيق سيعتمد على النسخة المسجلة لا على الإمكانات النظرية للمستشعر.(3)

وبالتالي :جودة التسجيل الفعلية ≤ جودة المصدر إذا أدت المعالجة أو الضغط أو الإعدادات إلى خفض المعلومات.

ثانيًا: معدل الإطارات

يؤثر معدل الإطارات في قدرة الفيديو على تمثيل الحركة.(4)

فالمشاهد البطيئة قد لا تحتاج إلى معدل مرتفع، بينما تتطلب المشاهد السريعة، مثل المركبات أو الأبواب أو مناطق الحركة الكثيفة، دراسة معدل الإطارات بما يتناسب مع الوظيفة.

ولا ينبغي رفع معدل الإطارات تلقائيًا لجميع الكاميرات؛ لأن ذلك يزيد معدل البيانات والتخزين.

ثالثًا: الضغط والترميز

تستخدم أنظمة الفيديو تقنيات ضغط لتقليل حجم البيانات.(5)
وقد تؤدي زيادة الضغط إلى خفض معدل البيانات، لكنها قد تؤثر في التفاصيل الدقيقة عند مستويات معينة.
ولهذا ينبغي تحقيق التوازن بين :الجودة ← معدل البيانات ← التخزين ← الشبكة.
وتشير ONVIF إلى أن Profile T يدعم تقنيات بث فيديو متقدمة تشمل H.264 و H.265في المنتجات المتوافقة، وهو ما يعكس أهمية الترميز في تصميم أنظمة الفيديو الحديثة.(6)

رابعًا: الضغط ومعدل البت

1. الضغط

يؤدي الضغط إلى تقليل كمية البيانات، وقد يؤدي الضغط المفرط إلى فقد تفاصيل مهمة. ويشير NIST إلى أن الضغط قد يؤدي إلى فقد غير قابل للاسترجاع، وأن مقدار الضغط ينبغي أن يرتبط بمتطلبات التخزين والاستخدام.(7)

2. معدل البت

معدل البت هو مقدار البيانات التي ينقلها أو ينتجها تدفق الفيديو خلال وحدة زمنية.
ويُقاس عادة بـbit/s ، kbit/s، Mbit/s (8).
وارتفاع معدل البت لا يعني دائمًا جودة أفضل بصورة مطلقة، لكنه يوفر عادة قدرة أكبر على تمثيل التفاصيل عندما تكون العوامل الأخرى متساوية.

3. العلاقة بين الضغط ومعدل البت

يمكن تبسيط العلاقة كما يأتي:(9)

- ضغط أعلى ← بيانات أقل ← تخزين وشبكة أقل ← احتمال فقد تفاصيل أكبر.
- ضغط أقل ← بيانات أكثر ← متطلبات شبكة وتخزين أعلى ← قدرة أكبر على المحافظة على التفاصيل.

وتوضـــح المراجع المهنية الخاصـــة بالتحكم في معدل البت أن جودة الفيديو تتأثر بالضـــغط، ومعدل البت، ودقة الصـــورة، ومعدل الإطارات، وطولGOP ، وتعقيد المشهد.(10)

خامسًا H.264 :وH.265

تستخدم أنظمة المراقبة الحديثة تقنيات ترميز مثل:(11)

- H.264/AVC.
- H.265/HEVC.

وتوفر هذه المعايير وســائل فعالة لخفض حجم الفيديو مقارنة بالفيديو غير المضــغوط، لكن المقارنة بينهما لا ينبغي أن تُختزل في نســبة ثابتة من قبيل H.265" يوفر دائمًا ٥٠٪"؛ لأن مقدار الوفر يعتمد على المشـــهد والإعدادات والدقة ومعدل الإطارات ومستوى الجودة.(12)

وتشـير ONVIF إلى دعم H.264 و H.265ضـمن Profile T المتعلق بالبث المتقدم للفيديو.(13)

سادسًا: جودة التسجيل والهدف الأمني

إذا كان الهدف هو المراقبة العامة، فقد تكون جودة معينة كافية.(14)

أما إذا كان الهدف هو التعرف على هوية شـخص أو قراءة لوحة مركبة، فقد تكون هناك حاجة إلى مســتوى أعلى من التفاصــيل، وبالتالي معدل بيانات وإعدادات تســجيل مختلفة.

سابعًا: عدم استخدام معدل بيانات منخفض بصورة مطلقة

من الأخطاء الشـــائعة تحديد معدل بيانات منخفض لجميع الكاميرات بهدف تقليل التخزين.(15)

والأفضل هو تصنيف الكاميرات بحسب الوظيفة الأمنية، ثم تحديد مستوى التسجيل المناسب لكل فئة.

المراجع:

١. ينظر: المعهد الوطني للمعايير والتقنية (NIST)، *Video Quality in Public Safety: Guide to Defining Video Quality Requirements (VQiPS)*، الولايات المتحدة الأمريكية، المعهد الوطني للمعايير والتقنية.

٢. ينظر: المعهد الوطني للمعايير والتقنية (NIST)، *VQiPS: Discrimination Level – Guide to Defining Video Quality Requirements*، الولايات المتحدة الأمريكية، المعهد الوطني للمعايير والتقنية.

٣. ينظر: المعهد الوطني للمعايير والتقنية (NIST)، *VQiPS: Discrimination Level – Guide to Defining Video Quality Requirements*، مرجع سابق.

٤. ينظر: المعهد الوطني للمعايير والتقنية (NIST)، *VQiPS: Target Size – Guide to Defining Video Quality Requirements*، الولايات المتحدة الأمريكية، المعهد الوطني للمعايير والتقنية.

٥. ينظر: المعهد الوطني للمعايير والتقنية (NIST)، *VQiPS: Motion – Guide to Defining Video Quality Requirements*، الولايات المتحدة الأمريكية، المعهد الوطني للمعايير والتقنية.

٦. ينظر: المعهد الوطني للمعايير والتقنية (NIST)، *VQiPS: Lighting Level – Guide to Defining Video Quality Requirements*، الولايات المتحدة الأمريكية، المعهد الوطني للمعايير والتقنية.

٧. ينظر: المعهد الوطني للمعايير والتقنية (NIST)، *Video Quality Tests for Object Recognition Applications*، تقرير فني للاتصالات في مجال السلامة العامة، سبتمبر ٢٠١٠.

٨. ينظر: المعهد الوطني للمعايير والتقنية (NIST)، *VQiPS: Processing – Guide to Defining Video Quality Requirements*، الولايات المتحدة الأمريكية، المعهد الوطني للمعايير والتقنية.

٩. ينظر: المعهد الوطني للمعايير والتقنية (NIST)، *VQiPS: Processing – Guide to Defining Video Quality Requirements*، مرجع سابق.

١٠. ينظر: المعهد الوطني للمعايير والتقنية (NIST)، *Video Quality Tests for Object Recognition Applications*، تقرير فني للاتصالات في مجال السلامة العامة، ٢٠١٠.

١١. ينظر: المعهد الوطني للمعايير والتقنية (NIST)، *VQiPS: Processing – Guide to Defining Video Quality Requirements*، الولايات المتحدة الأمريكية، المعهد الوطني للمعايير والتقنية.

١٢. ينظر: المعهد الوطني للمعايير والتقنية (NIST)، *Video Quality Tests for Object Recognition Applications*، تقرير فني للاتصالات في مجال السلامة العامة، ٢٠١٠.

١٣. ينظر: منظمة ONVIF، *Profile T – For Advanced Video Streaming*، مواصفة البث المتقدم للفيديو.

١٤. ينظر: منظمة ONVIF، *Profile T – For Advanced Video Streaming*، مواصفة البث المتقدم للفيديو.

١٥. ينظر: منظمة ONVIF، *Profile T – For Advanced Video Streaming*، مواصفة البث المتقدم للفيديو.

المبحث الرابع: سعة التخزين

تمثل سعة التخزين إحدى أكثر القضايا الفنية تأثيرًا في تصميم منظومة المراقبة. فزيادة عدد الكاميرات أو جودة التسجيل أو مدة الاحتفاظ تؤدي عادة إلى زيادة متطلبات التخزين. ولا يمكن تحديد السعة بصورة صحيحة دون دراسة معدل البيانات ومدة التسجيل ونمطه.(1)

ويكتسب هذا المبحث أهمية خاصة لأنه يقدم المعادلات الفنية الدقيقة لحساب سعة التخزين، ويبين أن السعة لا تتحدد بعدد الكاميرات وحده.(2)

أولًا: العوامل المؤثرة في السعة

تتأثر السعة المطلوبة بالعوامل الآتية:(3)

- عدد الكاميرات.
- معدل البيانات لكل كاميرا.
- معدل الإطارات.
- دقة الفيديو.
- نوع الترميز.
- نمط التسجيل.
- عدد ساعات التسجيل اليومية.
- مدة الاحتفاظ.
- نسبة الحركة.
- التسجيلات الإضافية الناتجة عن الأحداث.

ثانيًا: المعادلة الأساسية

يمكن حساب سعة التخزين من خلال المعادلة التالية:(4)

$$\text{Storage} = (\text{Bitrate} \times \text{Time}) / 8$$

حيث:

- Storage = سعة التخزين.
- Bitrate = معدل البت.

- Time = زمن التسجيل.

ثالثًا: مثال حسابي

إذا كان لدينا: (5)

- 16 كاميرا.
- معدل بت ٤ Mbit/s لكل كاميرا.
- تسجيل مستمر.
- مدة احتفاظ ٣٠ يومًا.

الخطوة الأولى: حساب معدل البت الإجمالي

Bitrate Total = 16 × 4 = 64 Mbit/s

الخطوة الثانية: حساب كمية البيانات في اليوم

Data per Day = (64 × 86400) / 8 = 691,200 MB = 691. 2 GB

الخطوة الثالثة: حساب كمية البيانات في ٣٠ يومًا

Data per 30 Days = 691. 2 × 30 = 20,736 GB = 20.7 TB

وهذا يعني أننا بحاجة إلى سعة تخزين لا تقل عن ٢١ تيرابايت لتحقيق مدة الاحتفاظ المطلوبة.(6)

رابعًا: هامش الأمان

لا ينبغي تصميم التخزين بحيث يعمل عند الحد الأقصى للسعة بصورة مستمرة.(7) وينبغي توفير هامش تشغيلي يسمح بزيادة معدل البيانات أو إضافة كاميرات أو تغير أنماط التسجيل. ويُوصى عادة بإضافة هامش يتراوح بين ٢٠٪ و٣٠٪ من السعة المحسوبة.(8)

خامسًا: التخزين والأداء

لا تكفي السعة الإجمالية وحدها؛ إذ يجب مراعاة قدرة نظام التخزين على استقبال البيانات وكتابتها وقراءتها في الوقت نفسه.(9)

وبالتالي فإن تصميم التخزين يتطلب دراسة: السعة + سرعة الكتابة + سرعة القراءة + الاعتمادية + التكرار + قابلية التوسع.

سادسًا: التخزين والاحتياجات المستقبلية

ينبغي أن يتضمن التصميم توقعات التوسع.(10)

فإذا أضـــيفت كاميرات جديدة، أو ارتفعت جودة التســـجيل، أو زادت مدة الاحتفاظ، فقد تصبح السعة الحالية غير كافية. ولهذا ينبغي اعتبار قابلية التوسع جزءًا من التصميم الأصلي.

المراجع

١. International Electrotechnical Commission (IEC). (2014). *IEC 62676-4:2014: Video surveillance systems for use in security applications – Part 4: Application guidelines*. Geneva: IEC.

٢. British Standards Institution (BSI). (2015). *BS EN 62676-4:2015: Video surveillance systems for use in security applications – Part 4: Application guidelines*. London: BSI. BBSI Knowledge

٣. Cisco Systems. (2009). *Local Storage for Video Archives Using iSCSI*. Cisco Systems.

٤. Cisco Systems. (2009). *IP Video Surveillance Whitepapers*. Cisco Systems.

٥. Cisco Systems. (2012). *iSCSI SAN Solution Design Guide for VSM on the UCS Express Platform*. Cisco Systems.

٦. .Cisco Systems. (2014). *Cisco Video Surveillance IP Camera Configuration Guide: Local Storage*. Cisco Systems

٧. Cisco Systems. (2009). *Cisco Video Management and Storage System CLI Administrator Guide*. Cisco Systems.

المبحث الخامس: مدة الاحتفاظ بالتسجيلات

تمثل مدة الاحتفاظ الفترة التي تبقى خلالها التسجيلات متاحة قبل استبدالها أو حذفها وفق سياسة النظام. ولا ينبغي تحديد هذه المدة بصورة عشوائية؛ لأنها ترتبط بطبيعة المخاطر، والاحتياجات التشغيلية، ومتطلبات التحقيق، والسياسات المؤسسية، والالتزامات القانونية والتنظيمية ذات الصلة.(1)

ويكتسب هذا المبحث أهمية خاصة لأنه يوضح العوامل التي تحدد مدة الاحتفاظ، ويبين أن تحديدها لا ينبغي أن يكون عشوائيًا، وإنما يستند إلى تحليل المتطلبات الأمنية والقانونية والتشغيلية.(2)

أولًا: مفهوم مدة الاحتفاظ

يمكن تعريف مدة الاحتفاظ بأنها :الفترة الزمنية التي يتم خلالها الاحتفاظ بالتسجيلات قبل حذفها أو إعادة كتابتها، وفق سياسة احتفاظ محددة .(3)

ثانيًا: العوامل المؤثرة في مدة الاحتفاظ

تتأثر مدة الاحتفاظ بعدة عوامل:(4)

1. المتطلبات القانونية والتنظيمية
   - قد تفرض التشريعات حدًا أدنى لمدة الاحتفاظ.
   - قد تفرض التشريعات حدًا أقصى لحماية الخصوصية.
2. طبيعة المنشأة
   - المنشآت الحيوية تحتاج إلى مدة احتفاظ أطول.
   - المنشآت التجارية قد تحتاج إلى مدة أقصر.
3. مستوى المخاطر
   - المناطق ذات المخاطر العالية تحتاج إلى مدة احتفاظ أطول.
   - المناطق ذات المخاطر المنخفضة قد تحتاج إلى مدة أقصر.
4. القيمة التحقيقية للتسجيل

- إذا كانت التسجيلات ذات قيمة تحقيقية عالية، تحتاج إلى مدة احتفاظ أطول.

5. الزمن المتوقع لاكتشاف الحادث

- إذا كان الحادث قد لا يُكتشف إلا بعد فترة، تحتاج التسجيلات إلى مدة احتفاظ أطول.

6. مدة التحقيق الداخلي

- إذا كانت التحقيقات الداخلية تستغرق وقتًا طويلًا، تحتاج التسجيلات إلى مدة احتفاظ أطول.

7. متطلبات الجهات المختصة

- قد تطلب الجهات المختصة الاحتفاظ بالتسجيلات لفترة محددة.

8. تكلفة التخزين

- كلما زادت مدة الاحتفاظ، زادت تكلفة التخزين.

ثالثًا: الاحتفاظ المتدرج

يمكن تطبيق سياسة احتفاظ متدرجة، بحيث تختلف مدة الاحتفاظ أو جودة التسجيل بحسب أهمية المنطقة أو نوع الحدث.(5)

مثال:

المنطقة	مدة الاحتفاظ
المداخل الرئيسية	90يومًا
الممرات	30يومًا
المكاتب	14يومًا
المخازن	30يومًا
المحيط	30يومًا

وهذا أكثر كفاءة من تطبيق مدة واحدة بصورة آلية على جميع الكاميرات.(6)

رابعًا: سياسة الحذف

ينبغي أن تكون عملية الحذف جزءًا من سياسة معتمدة، لا نتيجة عشوائية لامتلاء القرص.(7)

ويمكن للنظام استخدام آلية الاستبدال الدوري بحيث تحذف أقدم التسجيلات عندما تصل السعة إلى حدود معينة، ما لم تكن هناك تسجيلات محمية من الحذف.

خامسًا: التجميد القانوني أو الأمني

إذا ارتبط تسجيل معين بحادث أو تحقيق، فينبغي منع حذفه وفق آلية موثقة إلى حين انتهاء الغرض من الاحتفاظ به.(8)

وهنا تنتقل التسجيلات من مجرد بيانات تشغيلية إلى معلومات محفوظة لأغراض إثباتية أو تحقيقية.

سادسًا: العلاقة بين مدة الاحتفاظ وسعة التخزين

توجد علاقة مباشرة بين مدة الاحتفاظ وسعة التخزين. فإذا كانت مدة الاحتفاظ مطلوبة لفترة طويلة، فإن السعة يجب أن تكون كافية.(9)

ويمكن التعبير عن العلاقة بالمعادلة التالية:(10)

مدة الاحتفاظ = (سعة التخزين × ٨) / (معدل البت الإجمالي × ٨٦٤٠٠)

المراجع:

١. وزارة الداخلية السعودية. (2023). اللائحة التنفيذية لنظام استخدام كاميرات المراقبة الأمنية: الاحتفاظ بالتسجيلات عند وجود بلاغ أو حادث إلى حين انتهاء إجراءات التحقيق.

٢. المملكة العربية السعودية. (2022). نظام استخدام كاميرات المراقبة الأمنية: أحكام الاحتفاظ بالتسجيلات وتسليمها للجهات المختصة.

٣. دولة قطر. (2011). قانون رقم (٩) لسنة ٢٠١١ بتنظيم استخدام كاميرات وأجهزة المراقبة الأمنية، الجريدة الرسمية، العدد (٧)، ٢٠١١م.

٤. وزارة الداخلية السعودية. (2023). وثيقة الشروط والمتطلبات الأمنية لتركيب نظام المراقبة والمواصفات الفنية العامة لأجهزة أنظمة كاميرات المراقبة الأمنية.

٥. المملكة العربية السعودية .(2023) .وثيقة الشروط والمتطلبات الأمنية لتركيب نظام المراقبة والمواصفات الفنية العامة لأجهزة أنظمة كاميرات المراقبة الأمنية: متطلبات الاحتفاظ بالتسجيلات.

٦. البنك المركزي السعودي .(2019) .المتطلبات الأمنية لنظام المراقبة التلفزيونية للقطاع المالي، المملكة العربية السعودية.

٧. وزارة الداخلية السعودية .(2023) .اللائحة التنفيذية لنظام استخدام كاميرات المراقبة الأمنية: ضوابط الاحتفاظ بالتسجيلات وعدم الاحتفاظ بها خارج المدة المحددة.

٨. دولة قطر .(2011) .قانون رقم (٩) لسنة ٢٠١١ بتنظيم استخدام كاميرات وأجهزة المراقبة الأمنية: ضوابط حفظ التسجيلات وتسليمها للجهة المختصة وإعدامها، الجريدة الرسمية، العدد (٧)، ٢٠١١م.

٩. المملكة العربية السعودية .(2023) .وثيقة الشروط والمتطلبات الأمنية لتركيب نظام المراقبة والمواصفات الفنية العامة لأجهزة أنظمة كاميرات المراقبة الأمنية: متطلبات التخزين والاحتفاظ بالتسجيلات.

١٠. Cisco Systems. (2009). Local Storage for Video Archives Using iSCSI. Cisco Systems.

المبحث السادس: البحث والاسترجاع

تزداد القيمة العملية للتسجيل عندما يستطيع المستخدم الوصول إلى المقطع المطلوب بسرعة ودقة. ففي منظومة تحتوي على مئات الكاميرات وأيام أو أسابيع من التسجيل، لا يمكن الاعتماد على المشاهدة اليدوية المتسلسلة لجميع الملفات. ولهذا تمثل وظائف البحث والاسترجاع جزءًا أساسيًا من إدارة المعلومات الأمنية.(1)
ويكتسب هذا المبحث أهمية خاصة لأنه يوضح كيفية تصميم أنظمة بحث واسترجاع فعالة، ويبين أن سهولة الوصول إلى التسجيلات جزء من القيمة الأمنية للمنظومة.(2)

أولًا: مفهوم البحث والاسترجاع
يمكن تعريف البحث والاسترجاع بأنه :عملية تحديد موقع التسجيل المطلوب والوصول إليه، باستخدام معايير محددة، مثل الزمن أو الكاميرا أو الحدث أو البيانات الوصفية .(3)

ثانيًا: معايير البحث
يمكن البحث في التسجيلات وفق معايير متعددة:(4)

1. البحث الزمني
   - التاريخ.
   - الوقت.
   - الفترة الزمنية.

ويفترض نجاح هذه الوظيفة وجود مزامنة زمنية مناسبة بين الكاميرات وأجهزة التسجيل والأنظمة المرتبطة.

2. البحث بحسب الحدث
   - الحركة.
   - الإنذار.
   - الدخول.

- فتح الباب.
- العبث بالكاميرا.
- الأحداث التحليلية.

3. البحث باستخدام البيانات الوصفية
   - تصنيف الأجسام.
   - اللوحات.
   - الوجوه.
   - الأحداث.

وتزداد أهمية البيانات الوصـــفية في الأنظمة الحديثة، إذ يمكن ربط الفيديو بمعلومات مثل نوع الجســـم أو الحدث أو الموقع أو الزمن. ويتيح ONVIF Profile G وظائف للبحث والاســـترجاع ضـــمن أنظمة التســـجيل المتوافقة، بينما يركز Profile M على البيانات الوصفية والأحداث المرتبطة بتطبيقات التحليلات.(5)

ثالثًا: أنواع البحث

يمكن تصنيف البحث إلى نوعين:(6)

1. البحث اليدوي
   - يعتمد على المشغل.
   - يتطلب وقتًا وجهدًا.
   - مناسب للأنظمة الصغيرة.
2. البحث الآلي
   - يعتمد على التحليلات.
   - أسرع وأكثر دقة.
   - مناسب للأنظمة الكبيرة.

رابعًا: سرعة الاسترجاع

لا ينبغي تقييم نظام التسجيل بسعة التخزين فقط، بل بقدرته على الوصول إلى المعلومات.(7)
وقد تكون السعة كبيرة جدًا لكن عملية البحث بطيئة، مما يقلل القيمة التشغيلية للنظام.

خامسًا: التصدير
ينبغي أن يستطيع النظام تصدير المقاطع المهمة بطريقة تحافظ على السياق والبيانات ذات الصلة، مع توثيق مصدر الملف وزمنه وما تم من عمليات معالجة أو تحويل.(8)

سادسًا: حفظ السياق
من الأخطاء الشائعة استخراج ثوانٍ معدودة حول الحدث دون الاحتفاظ بالسياق.(9)
وقد يكون من الأفضل في بعض التحقيقات حفظ فترة زمنية قبل الحدث وبعده، لأن فهم الواقعة قد يتطلب معرفة ما سبقها وما تلاها.

المراجع:

١. المنظمة الدولية للتقييس الكهربائي .(2014). (IEC) أنظمة المراقبة بالفيديو للاستخدام في التطبيقات الأمنية – الجزء الرابع: إرشادات التطبيق.
٢. المنظمة الدولية للتقييس الكهربائي .(2014). (IEC) أنظمة المراقبة بالفيديو للاستخدام في التطبيقات الأمنية – الجزء الثاني: متطلبات بروتوكولات واجهات الفيديو.
٣. المنتدى المفتوح لواجهة الشبكات للفيديو .(2014). (ONVIF) المواصفة الفنية للبحث في التسجيلات.ONVIF Recording Search Specification
٤. المنتدى المفتوح لواجهة الشبكات للفيديو ONVIF .(2014). (ONVIF) Profile G: التخزين والاسترجاع والبحث في تسجيلات الفيديو.
٥. المنتدى المفتوح لواجهة الشبكات للفيديو ONVIF .(2021). (ONVIF) Profile M: البيانات الوصفية والأحداث الخاصة بتطبيقات التحليلات.

٦. المنتدى المفتوح لواجهة الشبكات للفيديو .(2021) .(ONVIF) مواصفة ONVIF Profile M: البيانات الوصفية وتحليل الأحداث.
٧. المنتدى المفتوح لواجهة الشبكات للفيديو .(2013) .(ONVIF) مواصفة التحكم في التسجيلات. ONVIF Recording Control Specification
٨. المنظمة الدولية للتقييس الكهربائي :IEC 62676-1-1 .(2018) .(IEC) أنظمة المراقبة بالفيديو للاستخدام في التطبيقات الأمنية – الجزء الأول: متطلبات النظام.
٩. المنظمة الدولية للتقييس الكهربائي :BS EN 62676-4:2015 .(2015) .(IEC) أنظمة المراقبة بالفيديو للاستخدام في التطبيقات الأمنية – الجزء الرابع: إرشادات التطبيق.
١٠. المنظمة الدولية للتقييس الكهربائي :IEC 62676-2-3 .(2020) .(IEC) أنظمة المراقبة بالفيديو للاستخدام في التطبيقات الأمنية – بروتوكولات نقل الفيديو – الجزء الثالث: متطلبات واجهات التشغيل البيني.

المبحث السابع: النسخ الاحتياطي

قد تتعرض التسجيلات للفقد نتيجة تعطل الأقراص أو تلف الأجهزة أو أخطاء التشغيل أو الحذف غير المقصود أو الحوادث الفيزيائية أو الهجمات الرقمية. ومن ثم فإن التسجيل الأساسي لا ينبغي اعتباره دائمًا نسخة احتياطية.(1)
ويكتسب هذا المبحث أهمية لأنه يوضح استراتيجيات النسخ الاحتياطي، ويبين أن النسخ الاحتياطي ليس مجرد إجراء إداري، وإنما جزء من التصميم الأمني.(2)

أولًا: الفرق بين التخزين والنسخ الاحتياطي
التخزين هو المكان الذي يحتفظ فيه النظام بالتسجيلات لأغراض التشغيل المعتادة (3).
أما النسخ الاحتياطي فهو إنشاء نسخة مستقلة يمكن استخدامها عند فقد الأصل أو عدم إمكانية الوصول إليه.
وبالتالي فإن وجود تسجيل على جهاز NVR واحد لا يعني وجود نسخ احتياطي.

ثانيًا: النسخ الاحتياطي للتسجيلات الحرجة
ليس من الضروري دائمًا نسخ جميع التسجيلات إلى نظام احتياطي كامل، خصوصًا في المنظومات الضخمة.(4)
وقد يكون أكثر كفاءة تحديد التسجيلات الحرجة، مثل:

- التسجيلات المرتبطة بالحوادث.
- التسجيلات المطلوبة للتحقيق.
- المقاطع ذات القيمة القانونية.
- التسجيلات المتعلقة بالأصول الحساسة.

ثالثًا: النسخ المحلي والبعيد
يمكن أن يكون النسخ الاحتياطي:(5)

- داخل الموقع.
- في موقع منفصل.
- في بنية تخزين بعيدة.
- في بيئة سحابية، وفق متطلبات المؤسسة.

والهدف من الفصل بين النسخة الأصلية والاحتياطية هو تقليل احتمال فقدهما بسبب حادث واحد.

رابعًا: استراتيجية ٣-٢-١

يمكن استخدام استراتيجية ٣-٢-١ للنسخ الاحتياطي: (6)

- 3نسخ من البيانات.
- 2وسائط مختلفة.
- 1نسخة خارج الموقع.

خامسًا: التحقق من النسخ الاحتياطي

إن إنشاء نسخة احتياطية دون اختبار استرجاعها لا يضمن فعاليتها.(7)

ولهذا ينبغي اختبار:

- إمكانية القراءة.
- سلامة الملف.
- اكتمال التسجيل.
- صحة التوقيت.
- إمكانية فتحه بالوسيلة المعتمدة.
- وجود البيانات المرتبطة به.

سادسًا: النسخ الاحتياطي وسلسلة الحيازة

عندما يصبح التسجيل دليلًا رقميًا، يجب توثيق مصدره والعمليات التي أجريت عليه ونشير إلى أهمية توثيق مصدر الملف، والحفاظ على سلامته، واستخدام قيم التجزئة الرقمية عند التعامل مع الأدلة الرقمية.

المراجع:

١. ينظر: ممدوح عبد الحميد عبد المطلب .(2006) .البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت: الجرائم عبر الكمبيوتر، البحث الجنائي، الدليل الرقمي .دار الكتب القانونية، القاهرة.

٢. ينظر: مسرة خالد الحمد .(2015) .الدليل الرقمي ومعايير جودته في الإثبات الجنائي .مركز الكتاب الأكاديمي.

٣. ينظر: محمود عبد الغني جاد المولى .(2019) .دور الدليل الإلكتروني في الإثبات الجنائي: دراسة مقارنة .دار الفكر الجامعي، الإسكندرية.

٤. ينظر: حسام فاضل حشيش .(2019) .الدليل الإلكتروني ودوره في الإثبات الجنائي معلقًا عليه بأحكام القضاء الإماراتي مع شرح للجرائم المعلوماتية .دار مصر للنشر والتوزيع، القاهرة.

٥. ينظر: أحمد جمال الشاهد، ومحمود جمال عبد الحميد .(2022) .حجية الدليل الإلكتروني في الإثبات الجنائي: دراسة تحليلية تطبيقية مقارنة للقانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات ومعلقًا على ذلك بأحدث أحكام القضاء .دار النهضة العربية، القاهرة.

٦. ينظر: قصي علي عباس. (٢٠٢٤). «حجية الدليل الإلكتروني في الإثبات الجنائي .«مجلة كلية القانون والعلوم السياسية.

٧. ينظر: أحمد لطفي السيد .(2024) .الأدلة الرقمية المتحصلة من التفتيش الجنائي الإلكتروني .دار الأهرام للإصدارات القانونية.

المبحث الثامن: إدارة التسجيلات

لا تكفي القدرة التقنية على تسجيل الفيديو؛ إذ تحتاج التسجيلات إلى إدارة تحدد من يستطيع الوصول إليها، وكيف يتم البحث عنها، ومتى يتم تصديرها، ومن يملك صلاحية حذفها أو حمايتها. ولهذا تمثل إدارة التسجيلات جزءًا من حوكمة منظومة المراقبة.(1)

ويكتسب هذا المبحث أهمية خاصة لأنه يوضح كيفية إدارة دورة حياة التسجيلات، ويبين أن الإدارة الجيدة للتسجيلات جزء من التصميم الأمني.(2)

أولًا: إدارة المستخدمين

ينبغي تحديد صلاحيات المستخدمين وفق أدوارهم.(3)

فليس من الضروري أن يمتلك المشغل العادي القدرة نفسها التي يمتلكها مدير النظام أو مسؤول التحقيق.

ويمكن توزيع الصلاحيات مثلًا إلى:

- مشاهدة مباشرة.
- مشاهدة تسجيلات.
- البحث.
- التصدير.
- إدارة المستخدمين.
- تعديل الإعدادات.
- حذف أو حماية التسجيلات.

ثانيًا: السجلات التشغيلية

ينبغي أن يحتفظ النظام بسجلات للأفعال المهمة، مثل:(4)

- تسجيل الدخول.
- البحث.

- التصدير.
- تغيير الإعدادات.
- حذف التسجيل.
- تغيير الصلاحيات.
- تعطيل كاميرا أو تسجيل.

وتساعد هذه السجلات في اكتشاف الاستخدام غير المصرح به وفي دعم التحقيقات.

ثالثًا: إدارة دورة حياة التسجيل

يمكن تقسيم دورة حياة التسجيل إلى: (5)

إنشاء ← تخزين ← استخدام ← حماية عند الحاجة ← أرشفة أو تصدير ← حذف وفق السياسة

ويجب أن تكون لكل مرحلة قواعد واضحة.

رابعًا: إدارة البيانات الوصفية

لا ينبغي فصل الفيديو عن المعلومات المرتبطة به، مثل: (6)

- الوقت.
- معرف الكاميرا.
- الموقع.
- الأحداث.
- بيانات النظام.

فقد تكون هذه البيانات ضرورية لفهم التسجيل والتحقق منه.

خامسًا: التوافق بين الأنظمة

في البيئات متعددة الموردين، يصبح التشغيل البيني مهمًا. (7)

وتوضح ONVIF أن التوافق الفعلي يرتبط بملفات Profile محددة وبالمنتجات المسجلة المتوافقة، وليس بمجرد استخدام عبارة عامة مثل "متوافق مع ONVIF".

سادسًا: إدارة التسجيلات في البيئات الكبيرة

في المنشآت الكبيرة يمكن أن يصبح حجم التسجيلات أكبر من أن تتم إدارته يدويًا (8).

ولهذا تحتاج المنظومة إلى:

- سياسات آلية للاحتفاظ.
- تصنيف للتسجيلات.
- آليات بحث.
- مراقبة سعة التخزين.
- إنذارات عند فشل التسجيل.
- تقارير تشغيلية.
- إدارة مركزية للصلاحيات.

المراجع:

١. ينظر: عبدالرزاق المرجان، محمد شوقي، يوسف السبعاوي، محمد المنشاوي، سيوكي لي، وجلال الهاشل .(2024) *الدليل الاسترشادي للتعامل مع الأدلة الجنائية الرقمية في الدول العربية* .دار جامعة نايف للنشر.

٢. ينظر: نبيل غبريال .(2026) *الطب الشرعي الرقمي والأدلة الإلكترونية من مسرح الجريمة إلى منصة القضاء: دراسة مقارنة في الواقع العربي والتحقيق التقني* .دار الأهرام للإصدارات القانونية.

٣. ينظر: ممدوح عبد الحميد عبد المطلب .(2006) *البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت: الجرائم عبر الكمبيوتر، البحث الجنائي، الدليل الرقمي* .دار الكتب القانونية، القاهرة.

٤. ينظر: أحمد جمال الشاهد، ومحمود جمال عبد الحميد .(2022) *حجية الدليل الإلكتروني في الإثبات الجنائي: دراسة تحليلية تطبيقية مقارنة للقانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات ومعلقًا على ذلك بأحدث أحكام القضاء* .دار النهضة العربية، القاهرة.

٥. ينظر: هيئة تنظيم الصناعة الأمنية .(2020) *دليل النظم الوقائية للقانون رقم ٢ لسنة ٢٠١١ بشأن تنظيم وترخيص واستخدام كاميرات المراقبة وأجهزة الأمن* .دبي، الإمارات العربية المتحدة.

٦. ينظر: Scientific Working Group on Digital Evidence (SWGDE). (2017). *Best Practices for Maintaining the Integrity of Imagery*, Version 1.0.

٧. ينظر: ONVIF. (2026). *ONVIF Profiles*. Open Network Video Interface Forum.

٨. ينظر: Scientific Working Group on Digital Evidence (SWGDE). (2023). *Best Practices for Digital Forensic Video Analysis*, SWGDE 18-V-001-2.0.

المبحث التاسع: حماية التسجيلات وسلامتها

تمثل التسجيلات الأمنية بيانات حساسة في كثير من البيئات، ولذلك فإن حمايتها لا تقل أهمية عن تسجيلها. وقد يؤدي الوصول غير المصرح به أو التعديل أو الحذف أو التسريب إلى إضعاف القيمة الأمنية للتسجيل، بل قد يحوله في بعض الحالات إلى مصدر خطر على المنشأة.(1)

ويكتسب هذا المبحث أهمية خاصة لأنه يوضح كيفية حماية التسجيلات من العبث أو الفقدان أو الوصول غير المصرح به، ويبين أن الحماية جزء من التصميم الأمني.(2)

أولًا: سرية التسجيلات

ينبغي تحديد من يملك الحق في مشاهدة التسجيلات أو تصديرها.(3)

وتزداد أهمية ذلك عندما تحتوي التسجيلات على أشخاص أو عمليات داخلية أو معلومات تشغيلية حساسة.

ثانيًا: سلامة التسجيل

تعني سلامة التسجيل القدرة على إثبات أن الملف لم يتغير بصورة غير مصرح بها.(4)

وتعد هذه المسألة مهمة بصورة خاصة عندما يستخدم الفيديو في التحقيقات أو الإجراءات الرسمية.

وتشير NIST إلى أن الملفات الرقمية سهلة التغيير نسبيًا، وأن المحافظة على سلامة البيانات تمثل قضية أساسية في حفظ الأدلة الرقمية، مع إمكانية استخدام قيم التجزئة والتوقيعات الرقمية كآليات مساعدة للتحقق من السلامة.(5)

ثالثًا: المصادقة وإدارة الصلاحيات

ينبغي حماية حسابات المستخدمين، وتجنب الحسابات المشتركة عندما تكون المساءلة الفردية مطلوبة.(6)

كما ينبغي تطبيق مبدأ :أقل صلاحية لازمة لأداء الوظيفة.

فالمستخدم ينبغي أن يمتلك الصلاحيات الضرورية فقط.

رابعًا: حماية الشبكة

في أنظمةIP ، لا ينبغي النظر إلى التسجيل كعنصر منفصل عن أمن الشبكة.(7)
فالكاميرا وجهاز التسجيل والخادم ومنصة الإدارة قد تشكل جميعها أجزاء من البنية الرقمية نفسها.
ولهذا ينبغي الاهتمام بالتحديثات الأمنية، وإدارة الخدمات، وتقسيم الشبكات عند الحاجة، وحماية واجهات الإدارة.

خامسًا: حماية أجهزة التخزين

لا تقتصر الحماية على البرمجيات؛ إذ ينبغي مراعاة الحماية الفيزيائية لأجهزة التسجيل والتخزين.(8)
ومن الإجراءات المهمة:

- وضع أجهزة التسجيل في مواقع مقيدة الوصول.
- حماية غرف المعدات.
- مراقبة الوصول إلى الخوادم.
- توفير الطاقة الاحتياطية المناسبة.
- دراسة الحرارة والتبريد.
- مراقبة حالة الأقراص.
- توفير التكرار عند الحاجة.

سادسًا: حماية التسجيلات من الحذف العرضي

ينبغي توفير آليات تمنع الحذف غير المقصود للتسجيلات الحرجة، مثل:(9)

- صلاحيات الحذف المقيدة.
- وضع التسجيل في حالة حماية.

- التصدير إلى مخزن منفصل.
- الاحتفاظ بنسخة مستقلة.
- توثيق إجراءات الحذف.

سابعًا: سلسلة الحيازة

عندما يستخدم التسجيل لأغراض إثباتية، ينبغي توثيق:(10)

من أنشأ التسجيل ← أين كان محفوظًا ← من استخرجه ← متى استخرج ← كيف نقل ← من استلمه ← ما التغييرات التي أجريت عليه

وتشير NIST إلى أهمية توثيق مصدر الملف وحركته، وحفظ قيم التجزئة بصورة منفصلة وآمنة للمساعدة في التحقق من سلامة الملفات الرقمية.(11)

ثامنًا: سلامة التسجيل ليست مجرد منع التعديل

ينبغي أيضًا التأكد من:(12)

- اكتمال الفترة الزمنية.
- صحة التاريخ والوقت.
- عدم وجود فجوات غير مبررة.
- إمكانية فتح الملف.
- ارتباطه بالكاميرا الصحيحة.
- وجود المعلومات الوصفية الضرورية.

تاسعًا: إدارة الفشل

ينبغي أن يكون النظام قادرًا على اكتشاف حالات مثل:(13)

- توقف التسجيل.
- امتلاء التخزين.

- فشل القرص.
- انقطاع الاتصال.
- فقد كاميرا.
- فشل المزامنة الزمنية.

ولا يكفي أن يحدث الفشل؛ بل يجب أن يصل إنذار مناسب إلى الجهة المسؤولة.

عاشرًا: مبدأ الحماية متعددة الطبقات

يمكن بناء حماية التسجيلات على عدة مستويات:(14)

- حماية فيزيائية.
- حماية الشبكة.
- حماية الحسابات.
- حماية التخزين.
- حماية النسخ الاحتياطية.
- مراقبة السجلات.
- توثيق العمليات.
- حماية الأدلة الحرجة.

وهذا يعكس حقيقة أن سلامة التسجيل ليست وظيفة واحدة، بل نتيجة لتكامل عدة طبقات.

المراجع:

١. ينظر: عبدالرزاق المرجان، محمد شوقي، يوسف السبعاوي، محمد المنشاوي، سيوكي لي، وجلال الهاشل .(2024) *.الدليل الاسترشادي للتعامل مع الأدلة الجنائية الرقمية في الدول العربية* .دار جامعة نايف للنشر.

٢. ينظر: ممدوح عبد الحميد عبد المطلب .(2006) *.البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت: الجرائم عبر الكمبيوتر، البحث الجنائي، الدليل الرقمي* .دار الكتب القانونية، القاهرة.

٣. ينظر: المركز العربي للأمن السيبراني .(2022) *.الإطار العربي للأمن السيبراني وحماية البيانات* .جامعة الدول العربية، القاهرة.

٤. ينظر: National Institute of Standards and Technology (NIST). (2012). *Computer Security Incident Handling Guide*, NIST Special Publication 800-61 Revision 2. Gaithersburg, MD: NIST.

٥. ينظر: Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response*, NIST Special Publication 800-86. Gaithersburg, MD: National Institute of Standards and Technology.

٦. ينظر: National Institute of Standards and Technology (NIST). (2020). *Security and Privacy Controls for Information Systems and Organizations*, NIST Special Publication 800-53 Revision 5. Gaithersburg, MD: NIST.

٧. ينـظـر National Institute of Standards and Technology (NIST). (2024). *Cybersecurity Framework (CSF) 2.0*. Gaithersburg, MD: National Institute of Standards and Technology.

٨. ينظر National Institute of Standards and Technology (NIST). (2015). *Contingency Planning Guide for Federal Information Systems*, NIST Special Publication 800-34 Revision 1. Gaithersburg, MD: NIST.

٩. ينظر Scientific Working Group on Digital Evidence (SWGDE). (2017). *Best Practices for Maintaining the Integrity of Imagery*, Version 1.0.

١٠. ينـظـر Scientific Working Group on Digital Evidence (SWGDE). (2025). *Best Practices for Digital Evidence Collection*, SWGDE 18-F-002-2.0.

١١. ينظر Scientific Working Group on Digital Evidence (SWGDE). (2019). *SWGDE Position on the Use of MD5 and SHA1 Hash Algorithms in Digital and Multimedia Forensics*.

١٢. ينظر Scientific Working Group on Digital Evidence (SWGDE). (2023). *Best Practices for Digital Forensic Video Analysis*, SWGDE 18-V-001-2.0.

١٣. ينظر National Institute of Standards and Technology (NIST). (2015). *Contingency Planning Guide for Federal Information Systems*, NIST Special Publication 800-34 Revision 1. Gaithersburg, MD: NIST.

١٤. ينظر National Institute of Standards and Technology (NIST). (2020). *Security and Privacy Controls for Information Systems and Organizations*, NIST Special Publication 800-53 Revision 5. Gaithersburg, MD: NIST.

خلاصة الفصل السادس

يتضح من دراسة التسجيل والتخزين وإدارة المعلومات أن منظومة المراقبة بالفيديو لا تنتهي عند إنتاج الصورة، وإنما تبدأ مرحلة أخرى لا تقل أهمية تتمثل في حفظ هذه الصورة وإدارتها وتحويلها إلى معلومة قابلة للاستخدام الأمني.

وقد أظهر التحليل أن التسجيل يمثل الذاكرة الزمنية للمنظومة، وأن قيمته تتحدد بمجموعة مترابطة من العوامل تبدأ بجودة التسجيل، وتمر بسعة التخزين ومدة الاحتفاظ، وتنتهي بقدرة المستخدم على البحث والاسترجاع والتحقق من سلامة المادة المسجلة.

كما يتضح أن التخزين ليس مجرد عملية حسابية تعتمد على عدد الأقراص، وإنما نتيجة لتفاعل عدة متغيرات، أهمها:

عدد الكاميرات + جودة التسجيل + معدل البيانات + نمط التسجيل + ساعات التشغيل + مدة الاحتفاظ + متطلبات التوسع

وفي هذا السياق، توضح NIST أن معدل الترميز أو البيانات، إلى جانب مدة الاحتفاظ، يؤثران بصورة مباشرة في متطلبات سعة التخزين، وأن التخزين غير السليم يمكن أن يؤدي إلى فقد البيانات أو تدهورها بما يؤثر في إمكانية استخدامها لاحقًا (1).

كما أن وظيفة التسجيل لا تكتمل دون البحث والاسترجاع. فالتسجيل الذي يستغرق الوصول إليه وقتًا طويلًا أو يفتقر إلى البيانات الزمنية والوصفية المناسبة قد يفقد جزءًا مهمًا من قيمته التشغيلية.

وقد أسهمت المعايير المفتوحة في تطوير هذا الجانب؛ إذ يخصص ONVIF Profile G وظائف للتسجيل والبحث والاسترجاع والتشغيل، بما يتيح مستوى من التشغيل البيني بين الأجهزة والبرمجيات المتوافقة.(2)

ومن ناحية أخرى، ينبغي التمييز بين التسجيل التشغيلي والتسجيل ذي القيمة الإثباتية. فالأول يخضع عادة لسياسة الاحتفاظ الدورية، بينما يحتاج الثاني إلى حماية إضافية تمنع الحذف أو التعديل وتوثق سلسلة حيازته.

وتؤكد إرشـــادات NIST الخاصـــة بحفظ الأدلة الرقمية أهمية توثيق مصـــدر الملفات وحركتها، واستخدام آليات مثل قيم التجزئة للتحقق من سلامتها عند الحاجة.(3)

وبذلك يمكن صياغة النموذج المتكامل لإدارة التسجيلات على النحو الآتي:

الهدف الأمني ← نوع التسجيل ← جودة التسجيل ← معدل البيانات ← سعة التخزين ← مدة الاحتفاظ ← البحث والاسترجاع ← النسخ الاحتياطي ← إدارة الصلاحيات ← حماية وسلامة البيانات ← الاستخدام الأمني والتحقيقي

ومن هنا فإن نجاح منظومة التسجيل لا يقاس بالسؤال: كم ساعة تستطيع المنظومة أن تسجل؟

بل بالسؤال الأكثر دقة:

هل تســـتطيع المنظومة أن توفر التســـجيل الصـــحيح، بالجودة المناســـبة، في الوقت المطلوب، طوال المدة المحددة، وأن تحافظ على ســـلامته وإمكان التحقق منه عند الحاجة؟

وهذا التحول من مفهوم "التســـجيل" إلى مفهوم "إدارة المعلومات الأمنية المســـجلة" يمثل أحد أهم الأسس الفنية والإدارية لتصميم منظومات المراقبة الحديثة.

أهم نتائج الفصل السادس

١. التسجيل يمثل الذاكرة الزمنية لمنظومة المراقبة.
٢. لا تكفي جودة الكاميرا إذا لم تحفظ الصورة بالجودة المطلوبة.
٣. يجب اختيار نمط التسجيل وفق طبيعة الخطر والوظيفة الأمنية.
٤. التسجيل المستمر يوفر استمرارية عالية لكنه يزيد متطلبات التخزين.
٥. التسجيل المرتبط بالحركة أو الحدث يمكن أن يقلل حجم البيانات.
٦. التسجيل المختلط يسمح بتوزيع الموارد وفق أهمية المناطق.
٧. جودة التسجيل يجب أن ترتبط بالهدف الأمني.
٨. معدل البيانات من أهم العوامل المؤثرة في سعة التخزين.
٩. عدد الكاميرات ومدة الاحتفاظ يؤثران بصورة مباشرة في حجم التخزين.
١٠. ينبغي توفير هامش تشغيلي وقابلية للتوسع.

١١. مدة الاحتفاظ يجب أن تحدد وفق المخاطر والاحتياجات والسياسات والمتطلبات القانونية والتنظيمية ذات الصلة.
١٢. التسجيلات المرتبطة بالحوادث تحتاج إلى حماية خاصة من الحذف الدوري.
١٣. البحث والاسترجاع عنصران أساسيان في القيمة التشغيلية للتسجيل.
١٤. البيانات الوصفية والأحداث تساعد في تسريع الوصول إلى المقاطع المناسبة.
١٥. النسخ الاحتياطي لا يساوي التخزين الأساسي.
١٦. ينبغي اختبار إمكانية استرجاع النسخ الاحتياطية.
١٧. إدارة المستخدمين والصلاحيات جزء من إدارة التسجيلات.
١٨. ينبغي تسجيل العمليات الإدارية الحساسة.
١٩. سلامة التسجيل مهمة بصورة خاصة في الاستخدامات التحقيقية والإثباتية.
٢٠. يمكن استخدام Hash وآليات التوثيق المناسبة للتحقق من سلامة الملفات الرقمية.
٢١. حماية التسجيلات يجب أن تشمل الجوانب الفيزيائية والشبكية والبرمجية والإدارية.
٢٢. ينبغي مراقبة فشل التسجيل والتخزين وإصدار التنبيهات المناسبة.
٢٣. التسجيل ينبغي أن ينظر إليه باعتباره جزءًا من منظومة إدارة المعلومات الأمنية، لا مجرد وظيفة في جهاز التسجيل.
٢٤. المعادلة الأساسية: Storage = (Bitrate × Time) / 8.
٢٥. استراتيجية ٣-٢-١ للنسخ الاحتياطي.
٢٦. سلسلة الحيازة ضرورية لسلامة التسجيلات.
٢٧. معيار ONVIF Profile G يدعم وظائف التسجيل والبحث والاسترجاع.
٢٨. معيار ONVIF Profile M يدعم البيانات الوصفية والأحداث.
٢٩. يجب أن تكون سياسة الحذف واضحة ومضبوطة.

٣٠. المعيار العملي المقترح: مستوى التسجيل المناسب = الوظيفة الأمنية + مستوى المخاطر + طبيعة المشـهد + جودة الصـورة المطلوبة + نمط التسـجيل + مدة الاحتفاظ + قابلية الاسترجاع + متطلبات الحماية.

أسئلة التفكير والتقييم للفصل السادس

أولًا: أسئلة معرفية

١. ما المقصود بالتسجيل الأمني؟ وما وظائفه الخمس؟
٢. ما الفرق بين التسجيل المستمر والتسجيل المرتبط بالحركة؟
٣. ما المقصود بالتسجيل المرتبط بالحدث؟
٤. ما العوامل التي تؤثر في سعة التخزين؟
٥. ما المقصود بمدة الاحتفاظ؟
٦. ما أهمية البحث والاسترجاع؟
٧. ما الفرق بين التخزين والنسخ الاحتياطي؟
٨. ما المقصود بسلامة التسجيل؟
٩. ما المقصود بسلسلة الحيازة الرقمية؟
١٠. ما وظيفة ONVIF Profile G في منظومات الفيديو؟
١١. ثانيًا: أسئلة تحليلية
١٢. ناقش العبارة: "وجود التسجيل لا يعني بالضرورة وجود قيمة أمنية".
١٣. حلل العلاقة بين جودة التسجيل وسعة التخزين.
١٤. لماذا قد يكون التسجيل المستمر غير مناسب لبعض المناطق؟
١٥. كيف يمكن أن يؤدي انخفاض جودة التسجيل إلى إضعاف التحقيق؟
١٦. ناقش العلاقة بين مدة الاحتفاظ ومستوى المخاطر.
١٧. لماذا لا يعتبر جهاز NVR الواحد نسخة احتياطية؟
١٨. كيف يؤثر البحث والاسترجاع في القيمة التشغيلية لمنظومة التسجيل؟
١٩. لماذا تعد سلامة التسجيل مهمة في الاستخدامات الإثباتية؟
٢٠. حلل العلاقة بين أمن الشبكة وحماية التسجيلات.

٢١. ما مخاطر الاعتماد على نقطة تخزين مركزية واحدة؟

ثالثًا: أسئلة تطبيقية

١. صمم سياسة تسجيل لمنشأة إدارية تضم مداخل وممرات ومواقف ومحيطًا خارجيًا.

٢. حدد المناطق التي تحتاج إلى تسجيل مستمر والمناطق التي يمكن أن تستخدم التسجيل المرتبط بالحركة.

٣. احسب السعة التقريبية المطلوبة لمنظومة تضم ٤٠ كاميرا بمعدل ٤ ميجابت/ثانية للكاميرا الواحدة ولمدة احتفاظ تبلغ ٣٠ يومًا.

٤. أنشئ جدولًا يربط بين أهمية المنطقة ونمط التسجيل وجودته ومدة الاحتفاظ.

٥. صمم سياسة للنسخ الاحتياطي للتسجيلات المرتبطة بالحوادث.

٦. ضع نموذجًا لسجل يوضح عمليات تصدير التسجيلات.

٧. صمم إجراءً لحماية تسجيل أصبح جزءًا من تحقيق أمني.

٨. ضع قائمة اختبار للتحقق من سلامة نظام التخزين واسترجاع التسجيلات.

٩. حدد خمسة أسباب يمكن أن تؤدي إلى فقد التسجيلات، واقترح إجراءً وقائيًا لكل سبب.

١٠. صمم اختبار قبول لجودة التسجيل في منشأة حيوية.

- المعيار العملي المقترح لإدارة التسجيل

يمكن تلخيص عملية اتخاذ القرار في هذا الفصل في المعادلة الآتية:

مستوى التسجيل المناسب = الوظيفة الأمنية + مستوى المخاطر + طبيعة المشهد + جودة الصورة المطلوبة + نمط التسجيل + مدة الاحتفاظ + قابلية الاسترجاع + متطلبات الحماية

وبناءً عليه يمكن اعتماد المصفوفة التالية:

النسخ الاحتياطي	مدة الاحتفاظ	جودة التسجيل	نمط التسجيل المقترح	مستوى الأهمية
اختياري	وفق السياسة	قياسية	حركة/مجدول	منخفض
حسب الأهمية	وفق المخاطر	متوسطة إلى مرتفعة	حركة/مستمر	متوسط
موصى به	أطول وفق الحاجة	مرتفعة	مستمر	مرتفع
إلزامي وفق سياسة المنشأة	وفق سياسة خاصة	مرتفعة جدًا عند الحاجة	مستمر + حدث	حرج

ولا ينبغي التعامل مع هذه المصفوفة باعتبارها معيارًا ثابتًا لجميع المنشآت؛ وإنما باعتبارها نموذجًا أوليًا لاتخاذ القرار يحتاج إلى التعديل وفق طبيعة المنشأة ومتطلبات الأمن والخصوصية والأنظمة المعمول بها.

الباب الثالث:
التشغيل والوظيفة الأمنية

الفصل الأول: تشغيل وإدارة مراكز المراقبة

تمهيد الفصل

يمثل تشـــغيل وإدارة مراكز المراقبة الحلقة التي تتحول فيها التقنية إلى قرار أمني فعلي. فالكاميرات والشـبكات وأجهزة التسـجيل وأنظمة التخزين لا تحقق قيمة أمنية بذاتها، وإنما تتحقق عندما يجد المشغل البشري أمامه بيئة عمل مناسبة، وإجراءات واضحة، وتدريبًا كافيًا، وأدوات دعم قرار فعالة. وتؤكد منهجيات الأمن المادي الحديثة أن نجاح منظومة المراقبة لا يقاس بعدد الكاميرات أو دقة الصـــورة، وإنما بقدرة المنظومة على اكتشاف الأحداث والتحقق منها والاستجابة لها.(1)

ويكتســـب هذا الفصـــل أهمية خاصـــة لأنه ينتقل من الجانب التقني إلى الجانب التشـغيلي، ويبين أن العنصـر البشـري ليس عنصـرًا هامشـيًا في المنظومة، بل هو الذي يحول البيانات المرئية إلى قرار واســتجابة. وقد أشــارت دراســات Human Factors المتخصـصـة إلى أن أداء المشـغل البشـري يتأثر بعوامل متعددة، منها الحمل المعرفي، والإرهاق، والانتباه، والرتابة، وأن تصـــميم المنظومة ينبغي أن يراعي هذه العوامل منذ مرحلة التخطيط.(2)

كما أن مراكز المراقبة لم تعد مجرد غرف تحتوي على شـاشـات، بل أصـبحت بيئات تشـــغيلية متكاملة تتضـــمن تقنيات العرض والإدارة والاتصـــال، وإجراءات التشـــغيل والتصعيد، وأنظمة دعم القرار، وآليات التوثيق. ويؤدي هذا التطور إلى ضرورة النظر إلى مركز المراقبة بوصفه منظومة تشغيلية وليس مجرد موقع فيزيائي .(3)

ويتناول هذا الفصل تسعة مباحث مترابطة: مركز المراقبة، وتنظيم العمل، ومشغلو أنظمة المراقبة، والتدريب والتأهيل، وإجراءات التشـــغيل، والتعامل مع الأحداث، والتوثيق والإبلاغ، والإرهاق والأخطاء البشرية، والصيانة واستمرارية التشغيل.

المبحث الأول: مركز المراقبة

يُعدّ مركز المراقبة نقطة الالتقاء بين التقنية والعنصر البشري والإجراءات الأمنية. فهو المكان الذي تتحول فيه الصور الملتقطة إلى قرارات، والأحداث المرصودة إلى استجابات. ولا ينبغي تقييم نجاح مركز المراقبة بعدد الشاشات أو حجم جدار الفيديو باعتبارهما مؤشرين منفردين؛ وإنما ينبغي تقييمه وفق قدرته على تحقيق المتطلبات التشغيلية والأمنية المحددة، بما في ذلك الكشف والتحقق والتقييم والاستجابة والتوثيق والاستمرارية.(1)

أولًا: مفهوم مركز المراقبة

يمكن تعريف مركز المراقبة بأنه: بيئة تشغيلية مخصصة لاستقبال وعرض وتحليل معلومات المراقبة، وتمكين المشغلين من اكتشاف الأحداث والتحقق منها وتقييمها واتخاذ الإجراءات المناسبة أو تصعيدها إلى الجهات المختصة .(2)

وبذلك فإن المركز يتكون من أربعة عناصر مترابطة:(3)

١. التقنية: الشاشات، والخوادم، وأنظمة الإدارة والاتصال.

٢. المعلومات: الفيديو، والأحداث، والتنبيهات، والبيانات المرتبطة.

٣. العنصر البشري: المشغلون، والمشرفون، وصانعو القرار.

٤. الإجراءات: سياسات التشغيل، والاستجابة، والتصعيد، والتوثيق.

وأي ضعف في أحد هذه العناصر ينعكس على أداء المركز بأكمله.

ثانيًا: أنواع مراكز المراقبة

يمكن تصنيف مراكز المراقبة وفق معايير متعددة:(4)

1. وفق النطاق
   - مركز محلي: يخدم منشأة واحدة.
   - مركز إقليمي: يخدم عدة منشآت في منطقة.
   - مركز مركزي: يخدم جميع منشآت المؤسسة.

2. وفق الوظيفة
   - مركز مراقبة فقط :يقتصر على المراقبة.
   - مركز تحكم :يدير المراقبة والأنظمة الأمنية الأخرى.
   - مركز قيادة وتحكم :يدير جميع العمليات الأمنية والتشغيلية.
3. وفق ساعات التشغيل
   - مركز على مدار الساعة :يعمل ٢٤/٧.
   - مركز بساعات عمل محددة :يعمل في أوقات معينة.
   - مركز هجين :يعمل على مدار الساعة في أوقات الذروة، وبساعات محددة في الأوقات الأخرى.(5)

ثالثًا: البنية الوظيفية لمركز المراقبة

يمكن تمثيل البنية الوظيفية لمركز المراقبة الحديث على النحو الآتي:(6)

مصـــادر البيانات ← شـــبكة النقل ← VMS/PSIM ← محرك التحليلات ← واجهة المشغل ← المشغل ← نظام إدارة الحدث ← الاستجابة ← التوثيق والتحليل اللاحق

رابعًا: الفرق بين VMS و PSIMوالأنظمة الأخرى

من الأخطاء الشائعة الخلط بين الأنظمة المختلفة في مركز المراقبة:(7)

الوظيفة	النظام
إدارة الفيديو	VMS
إدارة الأمن المادي المتكامل	PSIM
تحليل الفيديو	Video Analytics
إدارة الإنذارات	Alarm Management
تكامل التحكم في الدخول	Access Control Integration
الاتصال والإذاعة	Intercom/PA
نظام المعلومات الجغرافية	GIS
إدارة الحوادث	Incident Management

خامسًـــا: النموذج التشـــغيلي لمركز المراقبة:(8) خامسًـــا: النموذج التشـــغيلي لمركز المراقبة

يمكن اعتماد نموذج تشـغيلي متكامل لمركز المراقبة، يقوم على تسـع مراحل مترابطة، تبدأ من ملاحظة الحدث وتنتهي بـ مراجعة الإجراءات واستخلاص الدروس المستفادة، وذلك وفق التسلسل التالي:

الملاحظة ← الكشـف ← التحقق ← التقييم ← التصـنيف ← الاستجابة ← التصعيد ← التوثيق ← المراجعة

1. الملاحظة(Observation)

في هذه المرحلة تتم المتابعة المستمرة لما يحدث من خلال:

- متابعة تدفقات الفيديو.
- مراقبة الأنشطة والأحداث المختلفة.

2. الكشف(Detection)

تهدف هذه المرحلة إلى اكتشاف أي حدث أو نشاط يستدعي الانتباه، من خلال:

- اكتشاف الأحداث غير الاعتيادية.
- الاستفادة من أنظمة وتقنيات التحليل والمراقبة.

3. التحقق(Verification)

بعد اكتشاف الحدث، يتم التأكد من حقيقته وتحديد تفاصيله من خلال:

- التحقق من طبيعة الحدث.
- التأكد من موقع وقوعه.

4.التقييم(Assessment)

يتم في هذه المرحلة تحديد مدى أهمية الحدث وخطورته، وذلك من خلال:

- تقييم مستوى الخطورة.
- تحديد درجة الأولوية للتعامل مع الحدث.

5. التصنيف(Classification)

يتم تحديد نوع الحدث والإجراء المناسب للتعامل معه، من خلال:

- تصنيف الحدث حسب طبيعته.
- تحديد الإجراء المطلوب اتخاذه.

6. الاستجابة(Response)

في هذه المرحلة يتم التعامل مع الحدث وفق الإجراء المحدد، وذلك من خلال:

- تنفيذ الإجراء المناسب.
- التنسيق مع الجهات أو الفرق المعنية.

7. التصعيد (Escalation)

إذا كان الحدث يتطلب تدخلًا أو دعمًا إضافيًا، يتم تصعيده إلى المستوى المناسب، من خلال:

- رفع مستوى التعامل مع الحدث عند الحاجة.
- إبلاغ الجهات المعنية لاتخاذ الإجراءات اللازمة.

8. التوثيق (Documentation)

يتم تسجيل جميع المعلومات والإجراءات المتعلقة بالحدث، ويشمل ذلك:

- توثيق تفاصيل الحدث.
- تسجيل الإجراءات التي تم اتخاذها.

9. المراجعة (Review)

بعد انتهاء التعامل مع الحدث، تتم مراجعة ما تم من إجراءات بهدف تحسين الأداء مستقبلًا، وذلك من خلال:

- مراجعة كيفية التعامل مع الحدث.
- تحديد الدروس المستفادة والاستفادة منها في تحسين الإجراءات المستقبلية.

وبذلك يضمن هذا النموذج انتقال مركز المراقبة بشكل منظم من رصد الحدث واكتشافه، إلى التحقق منه وتقييمه، ثم الاستجابة له وتوثيقه، وأخيرًا مراجعة التعامل معه واستخلاص الدروس المستفادة.

خامسًا: النموذج التشغيلي لمركز المراقبة
من رصد الحدث إلى المراجعة وتحسين الأداء وتحقيق الأهداف
1 – الملاحظة
(Observations)
متابعة تدفقات الفيديو
رصد الأنشطة
2 – الكشف
اكتشاف الأحداث
استخدام التحليلات
التحقق من الموقع
3 – التحقق
(Verification)
4 – التقييم
(Assessment)
RISK LEVEL
5 – التصنيف
تصنيف الحدث
6 – الاستجابة
تنفيذ الإجراء
4 – التقييم
(Assessment)
تقييم مستوى الخطورة
تقييم الأولوية
7 – التصعيد
(Escalation)
تصعيد الحدث
إبلاغ الجهات المعنية
8 – التوثيق
(Documentation)
توثيق الحدث
توثيق الإجراءات
8 – التوثيق
(Documentation)
توثيق الحدث
توثيق الإجراءات
9 – المراجعة
(Review)
مراجعة التعامل
استخلاص الدروس
10 – تحسين الأنظمة
تطوير إعدادات المراقبة
تحديث التقنيات
11 – التدريب والتأهيل
رفع كفاءة الفريق
تعزيز الجاهزية
12 – تحقيق الأهداف
تعزيز الأمن والسلامة
تحسين الأداء

سادسًا: مؤشرات أداء مركز المراقبة يمكن تقييم أداء مركز المراقبة من خلال مؤشرات متعددة: (9)

المؤشر	الوحدة	الوصف
زمن الاكتشاف	ثواني	من وقوع الحدث إلى اكتشافه
زمن التحقق	ثواني	من الاكتشاف إلى التحقق
زمن التقييم	ثواني	من التحقق إلى التقييم
زمن اتخاذ القرار	ثواني	من التقييم إلى القرار
زمن التصعيد	ثواني	من القرار إلى التصعيد
زمن الاستجابة	دقائق	من التصعيد إلى بدء الاستجابة
معدل الإنذارات الكاذبة	%	نسبة الإنذارات الكاذبة
معدل الإنذارات غير المعالجة	%	نسبة الإنذارات غير المعالجة
نسبة التغطية التشغيلية	%	نسبة الوقت الذي يعمل فيه النظام بكفاءة
توفر النظام	%	نسبة الوقت الذي يعمل فيه النظام
معدل الأعطال	عدد/شهر	عدد الأعطال في فترة زمنية
زمن الإصلاح	ساعات	متوسط الوقت للإصلاح
دقة تصنيف الأحداث	%	نسبة التصنيفات الصحيحة
جودة التوثيق	%	نسبة التوثيق المكتمل
نسبة الالتزام بالإجراءات	%	نسبة الالتزام بإجراءات التشغيل
أداء المشغلين في الاختبارات	%	نسبة النجاح في الاختبارات

سابعًا: زمن دورة الحدث الأمني

يمكن اعتماد زمن دورة الحدث الأمني كمؤشر تشغيلي مركب:(10)

زمن دورة الحدث = زمن الكشـــف + زمن التحقق + زمن التقييم + زمن اتخاذ القرار + زمن التصعيد + زمن بدء الاستجابة

وهذا المؤشر يعكس الأداء الأمني الحقيقي، وليس مجرد سرعة التقنية.

مثال تطبيقي:

إذا اكتشـــفت الكاميرا الحدث خلال ٥ ثوانٍ، ولكن المشـــغل احتاج ٣ دقائق للتحقق منه وتصـــعيده، فليس من الصـــحيح القول إن النظام "ســـريع". فالأداء الأمني لا يقاس بسرعة التقنية منفردة، وإنما بزمن الدورة التشغيلية الكاملة للحدث.

١. المراجع:

١. ينظر: International Electrotechnical Commission (IEC). (2025). *IEC 62676-4:2025: Video surveillance systems for use in security applications – Part 4: Application guidelines*. 2nd ed., Geneva: IEC.

٢. ينظر: International Electrotechnical Commission (IEC). (2025). *IEC 62676-4:2025: Video surveillance systems for use in security applications – Part 4: Application guidelines*. 2nd ed., Geneva: IEC.

٣. ينظر: International Electrotechnical Commission (IEC). (2025). *IEC 62676-4:2025: Video surveillance systems for use in security applications – Part 4: Application guidelines*. 2nd ed., Geneva: IEC؛ و Cybersecurity and Infrastructure Security Agency (CISA). *Control Rooms Guidance*.

٤. ينظر: Cybersecurity and Infrastructure Security Agency (CISA). *Control Rooms Guidance*.

٥. ينظر: Cybersecurity and Infrastructure Security Agency (CISA). *Control Rooms Guidance*.

٦. ينظر: International Electrotechnical Commission (IEC). (2025). *IEC 62676-4:2025: Video surveillance systems for use in security applications – Part 4: Application guidelines*. 2nd ed., Geneva: IEC؛ و Cybersecurity and Infrastructure Security Agency (CISA). *Control Rooms Guidance*.

٧. ينظر: Cybersecurity and Infrastructure Security Agency (CISA). *Control Rooms Guidance*.

٨. ينظر: National Institute of Standards and Technology (NIST). (2023). *Guide to Operational Technology (OT) Security*, NIST Special Publication 800-82 Revision 3. Gaithersburg, MD: NIST؛ و International Organization for Standardization (ISO). *ISO 22301: Security and resilience — Business continuity management systems — Requirements*.

٩. ينظر: International Electrotechnical Commission (IEC). (2025). *IEC 62676-4:2025: Video surveillance systems for use in security applications – Part 4: Application guidelines*. 2nd ed., Geneva: IEC؛ و National Institute of Standards and Technology (NIST). *Video Quality in Surveillance Systems (VQiPS)*.

١٠. ينظر: Wickens, C. D., Hollands, J. G., Banbury, S., & Parasuraman, R. (2016). *Engineering Psychology and Human Performance*. 4th ed., Routledge.

المبحث الثاني: تنظيم العمل

لا يكفي وجود مركز مراقبة مجهز تقنيًا لضمان فاعلية المنظومة، بل يجب تنظيم العمل داخله بصورة تضمن التغطية المستمرة، وتوزيع المهام بوضوح، وتحديد المسؤوليات والصلاحيات، وضمان التنسيق بين المشغلين والمشرفين والجهات الخارجية.(1)
ويمكن للتنظيم التشغيلي الجيد أن يخفف أثر بعض أوجه القصور التقني، لكنه لا يعوض المتطلبات التقنية الحرجة التي يرتبط بها الأداء الأمني مباشرة، مثل كاميرا غير مناسبة للمشهد، أو شبكة غير مستقرة، أو تخزين غير كافٍ.(2)

أولًا: مفهوم تنظيم العمل
يمكن تعريف تنظيم العمل في مركز المراقبة بأنه: مجموعة الإجراءات والترتيبات التي تضمن توزيع المهام والمسؤوليات والصلاحيات بين العاملين في المركز، وتنسيق عملهم لتحقيق الأهداف الأمنية .(3)

ثانيًا: عناصر تنظيم العمل
يشمل تنظيم العمل في مركز المراقبة عدة عناصر:(4)

1. توزيع المهام

تحديد مهام كل مشغل بوضوح، وتجنب التداخل أو الفراغ في المسؤوليات.

2. جدول المناوبات

تنظيم المناوبات لضمان التغطية المستمرة، مع مراعاة فترات الراحة والإرهاق.

3. إجراءات التشغيل

وضع إجراءات واضحة للتعامل مع الأحداث، وتحديد خطوات العمل في الحالات المختلفة.

4. آليات التصعيد

تحديد آليات التصعيد عند الحاجة، ومن المسؤول عن كل مستوى من مستويات التصعيد.

5. التوثيق والإبلاغ

تحديد آليات التوثيق والإبلاغ، وضمان تسجيل الأحداث والإجراءات.

6. التنسيق مع الجهات الأخرى

تحديد آليات التنسيق مع الحراسة والجهات المختصة والإدارة.

ثالثًا: نماذج تنظيم العمل

يمكن تصنيف نماذج تنظيم العمل في مركز المراقبة إلى ثلاثة نماذج:(5)

1. النموذج المركزي
   - جميع المشغلين في موقع واحد.
   - إدارة موحدة.
   - مناسب للمنشآت الصغيرة والمتوسطة.
2. النموذج الموزع
   - توزيع المشغلين على مواقع متعددة.
   - إدارة لا مركزية.
   - مناسب للمنشآت الواسعة والمتعددة المواقع.
3. النموذج الهجين
   - يجمع بين المركزي والموزع.
   - إدارة مركزية مع فرق ميدانية.
   - مناسب للمنشآت الكبيرة والمعقدة.(6)

رابعًا: جدول المناوبات

يُعدّ جدول المناوبات من أهم عناصر تنظيم العمل (٧). وينبغي أن يراعي:

- التغطية المستمرة.
- فترات الراحة.
- الإرهاق.

- الكفاءات المتخصصة.
- المناسبات الخاصة.
- الطوارئ.

ومن الأخطاء الشائعة أن تكون المناوبات طويلة جدًا أو متقاربة، مما يؤدي إلى الإرهاق وانخفاض الأداء. وقد أشارت دراسات Human Factors إلى أن المناوبات التي تتجاوز ٨-١٢ ساعة تؤدي إلى انخفاض ملحوظ في الانتباه وزيادة الأخطاء.(8)

خامسًا: معايير تقييم تنظيم العمل

يمكن تقييم تنظيم العمل في مركز المراقبة من خلال عدة معايير:(9)

- وضوح المهام.
- عدالة توزيع المهام.
- كفاية عدد المشغلين.
- مناسبة جدول المناوبات.
- وضوح إجراءات التشغيل.
- فعالية آليات التصعيد.
- جودة التنسيق مع الجهات الأخرى.
- مستوى التوثيق والإبلاغ.

المراجع:

١. ينظر: المعهد الوطني للمعايير والتكنولوجيا (NIST). (2025). توصيات واعتبارات الاستجابة للحوادث لإدارة مخاطر الأمن السيبراني، المنشور الخاص NIST SP 800-61 Revision 3. غايثرسبيرغ، ماريلاند: المعهد الوطني للمعايير والتكنولوجيا.

٢. ينظر: المعهد الوطني للمعايير والتكنولوجيا .(2012) .(NIST) دليل التعامل مع حوادث أمن الحاسوب، المنشور الخاص .NIST SP 800-61 Revision 2 غايثرسبيرغ، ماريلاند: المعهد الوطني للمعايير والتكنولوجيا.

٣. ينظر: هيئة الصحة والسلامة البريطانية .(2006) .(HSE) إدارة العمل بنظام المناوبات: إرشادات الصحة والسلامة .HSG256 لندن: هيئة الصحة والسلامة البريطانية.

٤. ينظر: هيئة الصحة والسلامة البريطانية .(2026) .(HSE) العوامل البشرية وعلم الهندسة البشرية: المخاطر الشائعة وإدارة مستويات العاملين وعبء العمل . لندن: هيئة الصحة والسلامة البريطانية.

٥. ينظر: هيئة الصحة والسلامة البريطانية .(2026) .(HSE) إرشادات الممارسة الجيدة لتصميم جداول المناوبات .لندن: هيئة الصحة والسلامة البريطانية.

٦. ينظر: هيئة الصحة والسلامة البريطانية .(2026) .(HSE) الإرهاق: إدارة مخاطر الإرهاق والعمل بنظام المناوبات .لندن: هيئة الصحة والسلامة البريطانية.

٧. ينظر: إدارة السلامة والصحة المهنية الأمريكية .(2026) .(OSHA) ساعات العمل الطويلة والمناوبات الممتدة أو غير المنتظمة وإرهاق العاملين .واشنطن: وزارة العمل الأمريكية.

٨. ينظر: إدارة السلامة والصحة المهنية الأمريكية .(2026) .(OSHA) دليل المناوبات الممتدة وغير المعتادة .واشنطن: وزارة العمل الأمريكية.

٩. ينظر: هيئة الصحة والسلامة البريطانية .(2026) .(HSE) العوامل البشرية في التصميم: غرف التحكم .لندن: هيئة الصحة والسلامة البريطانية.

١٠. ينظر: المعهد الوطني للمعايير والتكنولوجيا .(2023) .(NIST) حماية المعلومات غير المصنفة الخاضعة للرقابة في الأنظمة والمنظمات غير الفيدرالية، NIST SP 800-171 Revision 3. غايثرسبيرغ، ماريلاند: المعهد الوطني للمعايير والتكنولوجيا..

المبحث الثالث: مشغلو أنظمة المراقبة

يمثل مشـغلو أنظمة المراقبة العنصـر البشـري الذي يحول البيانات المرئية إلى قرارات واستجابات. ولا يمكن لأي منظومة تقنية، مهما بلغت درجة تقدمها، أن تستغني عن العنصر البشري في تفسير الأحداث وتقدير مستوى الخطورة واتخاذ القرار المناسب (1).

ويكتسـب هذا المبحث أهمية خاصـة لأنه يحدد متطلبات مشـغل أنظمة المراقبة، ويكشف عن التحديات التي تواجهه، ويبين أن العامل البشري ليس عنصرًا هامشيًا في المنظومة، بل هو الذي يحول البيانات إلى قرار. ويعتمد هذا المبحث على مجال Human Factorsالمتخصص، وليس على مراجع CCTV وحدها.(2)

أولًا: مفهوم مشغل أنظمة المراقبة

يمكن تعريف مشـغل أنظمة المراقبة بأنه :الشـخص المسـؤول عن متابعة تدفقات الفيديو، واكتشاف الأحداث، والتحقق منها، وتوثيقها، والاستجابة لها وفق الإجراءات المعتمدة .(3)

ثانيًا: مهام مشغل أنظمة المراقبة

تشمل مهام مشغل أنظمة المراقبة:(4)

- متابعة تدفقات الفيديو.
- اكتشاف الأحداث والأنشطة المشبوهة.
- التحقق من التنبيهات والإنذارات.
- توثيق الأحداث.
- الاستجابة وفق الإجراءات المعتمدة.
- التنسيق مع الحراسة والجهات الأخرى.
- إعداد التقارير.

ثالثًا: متطلبات مشغل أنظمة المراقبة

ينبغي أن يمتلك مشغل أنظمة المراقبة مجموعة من المتطلبات: (5)

1. المتطلبات المعرفية
   - فهم أساسيات أنظمة المراقبة.
   - معرفة أنواع الكاميرات والعدسات.
   - فهم إجراءات التشغيل.
   - معرفة إجراءات الطوارئ.
2. المتطلبات المهارية
   - القدرة على متابعة الشاشات.
   - القدرة على اكتشاف الأحداث.
   - القدرة على التمييز بين الأحداث العادية والمشبوهة.
   - القدرة على التعامل مع الأنظمة التقنية.
   - القدرة على التواصل الفعال.
3. المتطلبات السلوكية
   - الانتباه والتركيز.
   - الهدوء في المواقف الحرجة.
   - الأمانة والمسؤولية.
   - القدرة على العمل ضمن فريق.
   - الالتزام بالإجراءات.

رابعًا: التحديات التي تواجه مشغل أنظمة المراقبة

يواجه مشغل أنظمة المراقبة عدة تحديات: (6)

1. الإرهاق

متابعة الشاشات لفترات طويلة تؤدي إلى الإرهاق وانخفاض الانتباه. ويشير Wickens et al. إلى أن الإرهاق يمثل أحد أهم العوامل المؤثرة في أداء المشغل، وأنه يؤدي إلى انخفاض اليقظة وزيادة الأخطاء.(7)

2. الحمل المعرفي

التعامل مع عدد كبير من الكاميرات والتنبيهات يزيد الحمل المعرفي. ويشير Parasuraman & Riley إلى أن الحمل المعرفي الزائد يؤدي إلى انخفاض الأداء وزيادة الأخطاء.(8)

3. ضغط الوقت

الحاجة إلى اتخاذ قرارات سريعة في مواقف حرجة.

4. الأحداث النادرة

قد تكون الأحداث نادرة، مما يؤدي إلى انخفاض اليقظة. ويشير Reason إلى أن المهام الرتيبة طويلة الأمد تؤدي إلى انخفاض الانتباه وزيادة الأخطاء.(9)

5. الإنذارات الكاذبة

كثرة الإنذارات الكاذبة تؤدي إلى تجاهل الإنذارات الحقيقية.

6. التعرض للمشاهد الصادمة

قد يتعرض المشغل لمشاهد صادمة تؤثر في حالته النفسية. ويشير Hancock & Desmond إلى أن الضغط النفسي يمثل عاملًا مؤثرًا في أداء المشغل.(10)

خامسًا: العوامل المؤثرة في أداء المشغل

تتأثر قدرة المشغل على أداء مهامه بعدة عوامل:(11)

مستوى التدريب.

١. الخبرة.

٢. بيئة العمل.

٣. الإضاءة.

٤. الضوضاء.

٥. عدد الشاشات.

٦. عدد التنبيهات.

٧. جودة الصورة.

٨. وضوح الإجراءات.

٩. الدعم من المشرفين.

المراجع:

١. ينظر: Wickens, C. D., Lee, J. D., Liu, Y., & Gordon-Becker, S. (2014). An Introduction to Human Factors Engineering (2nd ed.). Pearson.

٢. ينظر: Parasuraman, R., & Riley, V. (1997). Humans and Automation: Use, Misuse, Disuse, Abuse. *Human Factors*, 39(2), 230–253.

٣. ينظر: Reason, J. (1990). Human Error. Cambridge: Cambridge University Press.

٤. ينظر: Hancock, P. A., & Desmond, P. A. (Eds.). (2001). Stress, Workload, and Fatigue. Mahwah, NJ: Lawrence Erlbaum Associates.

٥. ينظر: Smith, M. J., Cohen, B. G. F., & Stammerjohn, L. W. (1981). An Investigation of Health Complaints and Job Stress in Video Display Operations. *Human Factors*, 23(4), 387–400.

٦. ينظر: Warm, J. S., Parasuraman, R., & Matthews, G. (2008). Vigilance Requires Hard Mental Work and Is Stressful. *Human Factors*, 50(3), 433–441.

٧. ينظر: See, J. E. (2012). Visual Inspection: A Review of the Literature. *Quality Technologies and Quantitative Management*, 9(3).

٨. ينظر: Dember, W. N., & Warm, J. S. (1979). Psychology of Vigilance. New York: Academic Press.

٩. ينظر: Endsley, M. R. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors*, 37(1), 32–64.

١٠. ينظر: Stanton, N. A., Salmon, P. M., Walker, G. H., Baber, C., & Jenkins, D. P. (2005). Human Factors Methods: A Practical Guide for Engineering and Design. Aldershot: Ashgate.

المبحث الرابع: التدريب والتأهيل

يُعدّ التدريب والتأهيل من أهم العوامل التي تحدد فاعلية مشـــغلي أنظمة المراقبة. فالمشغل غير المدرب قد يفشل في اكتشاف الأحداث أو في الاستجابة لها، حتى لو كانت المنظومة التقنية متقدمة.(1)

ويكتسب هذا المبحث أهمية خاصة لأنه يحدد متطلبات التدريب والتأهيل، ويبين أن التدريب ليس حدثًا لمرة واحدة، بل عملية مستمرة تتطور مع تطور المنظومة والتهديدات.(2)

أولًا: مفهوم التدريب والتأهيل

يمكن تعريف التدريب والتأهيل بأنه :العملية المنظمة التي تهدف إلى تزويد مشـــغلي أنظمة المراقبة بالمعارف والمهارات والســـلوكيات اللازمة لأداء مهامهم بكفاءة وفعالية (3).

ثانيًا: أنواع التدريب

يمكن تصنيف التدريب إلى عدة أنواع:(4)

1. التدريب الأولي
   - يتم قبل بدء العمل.
   - يهدف إلى تأهيل المشغل الجديد.
   - يشمل المعارف الأساسية والمهارات الأولية.
2. التدريب المستمر
   - يتم بشكل دوري.
   - يهدف إلى تحديث المعارف والمهارات.
   - يشمل التطورات التقنية والتهديدات الجديدة.
3. التدريب المتخصص
   - يتم حسب الحاجة.

- يهدف إلى تأهيل المشغل في مجال معين.
- يشمل التحليلات الذكية، أو إدارة الأزمات، أو التحقيق.

4. التدريب العملي
   - يتم في بيئة العمل.
   - يهدف إلى تطبيق المعارف والمهارات.
   - يشمل المحاكاة والتمارين.(5)

ثالثًا: محتوى التدريب

يشمل محتوى التدريب عدة عناصر:(6)

1. المعارف الأساسية
   - مبادئ أنظمة المراقبة.
   - أنواع الكاميرات والعدسات.
   - أنظمة التسجيل والتخزين.
   - الشبكات والاتصالات.
2. المهارات التشغيلية
   - متابعة الشاشات.
   - اكتشاف الأحداث.
   - التحقق من التنبيهات.
   - التوثيق والإبلاغ.
   - التعامل مع الأنظمة التقنية.
3. الإجراءات
   - إجراءات التشغيل.
   - إجراءات الاستجابة.
   - إجراءات التصعيد.
   - إجراءات الطوارئ.

4. الجوانب القانونية والأخلاقية
   - الخصوصية.
   - حماية البيانات.
   - المسؤولية.
   - الأخلاقيات المهنية.(7)

رابعًا: أساليب التدريب

يمكن استخدام عدة أساليب للتدريب:(8)

1. المحاضرات
   - تقديم المعارف النظرية.
2. الورش
   - تطبيق عملي في بيئة محمية.
3. المحاكاة
   - محاكاة سيناريوهات واقعية.
4. التدريب الميداني
   - تدريب في بيئة العمل الفعلية.
5. التعليم الإلكتروني
   - تدريب عن بعد باستخدام التقنيات الرقمية.
6. التدريب على رأس العمل
   - تدريب تحت إشراف مشرف.(9)

خامسًا: تقييم التدريب

ينبغي تقييم فعالية التدريب بصورة دورية (١٠). ويشمل التقييم:

- اختبارات معرفية.
- تقييم مهارات.

- ملاحظة الأداء.
- تقييم النتائج.
- آراء المشاركين.

المراجع:

١. ينظر: المنظمة العربية للتنمية الإدارية .(2009) .التدريب وتنمية الموارد البشرية: المفاهيم والأساليب والتطبيقات .القاهرة: المنظمة العربية للتنمية الإدارية.

٢. ينظر: أحمد ماهر .(2007) .إدارة الموارد البشرية .الإسكندرية: الدار الجامعية.

٣. ينظر: علي السلمي .(2001) .إدارة الموارد البشرية والكفاءة الإنتاجية .القاهرة: دار غريب للطباعة والنشر والتوزيع.

٤. ينظر: عبد الباري إبراهيم درة، وزهير نعيم الصباغ .(2008) .إدارة الموارد البشرية في القرن الحادي والعشرين: منحى نظمي .عمّان: دار وائل للنشر.

٥. ينظر: المنظمة العربية للتنمية الإدارية .(2007) .التدريب وتنمية الموارد البشرية .القاهرة: المنظمة العربية للتنمية الإدارية.

٦. ينظر: حسين حريم .(2013) .إدارة الموارد البشرية: إطار متكامل .عمّان: دار الحامد للنشر والتوزيع.

٧. ينظر: محمد الصيرفي .(2006) .التدريب الإداري: المدربون والمتدربون وأساليب التدريب .الإسكندرية: مؤسسة حورس الدولية للنشر والتوزيع.

٨. ينظر: عبد الرحمن العيسوي .(2004) .الكفاءة الإدارية والتدريب الإداري . الإسكندرية: دار الجامعة الجديدة.

٩. ينظر: أحمد سيد مصطفى .(2004) .إدارة الموارد البشرية: الإدارة العصرية لرأس المال الفكري .القاهرة: دار الكتب.

١٠. ينظر: المنظمة العربية للتنمية الإدارية .(2010) .قياس وتقييم العائد من التدريب .القاهرة: المنظمة العربية للتنمية الإدارية.

المبحث الخامس: إجراءات التشغيل

تمثل إجراءات التشـــغيل الإطار الذي يوجه عمل مشـــغلي أنظمة المراقبة، ويضـــمن التعامل مع الأحداث بصـــورة منظمة وموحدة. فبدون إجراءات واضـــحة، قد تتفاوت الاســـتجابات بين المشـــغلين، وقد تحدث أخطاء أو تأخير في التعامل مع الأحداث (1).

ويكتسب هذا المبحث أهمية خاصة لأنه يحدد إجراءات التشغيل الأساسية، ويبين أن الإجراءات الجيدة يمكن أن تخفف أثر بعض القيود البشـــرية، بينما غياب الإجراءات يمكن أن يؤدي إلى فشل المنظومة.(2)

أولًا: مفهوم إجراءات التشغيل

يمكن تعريف إجراءات التشـــغيل بأنها :مجموعة الخطوات والأدوار والمســـؤوليات المحددة مسبقًا للتعامل مع الحالات المختلفة التي تواجه مشغلي أنظمة المراقبة .(3)

ثانيًا: التمييز بين مستويات الوثائق التشغيلية

من الأخطاء الشائعة الخلط بين مستويات الوثائق التشغيلية:(4)

تتدرج وثائق العمل والتنظيم الأمني من المبادئ العامة والتوجهات إلى التعليمات والخطوات التفصيلية، بحيث يحدد كل مستوى نطاقًا معينًا من المسؤوليات وآليات التنفيذ.

١. السياسةPolicy –

تمثل السياسة المستوى العام الذي يحدد المبادئ والتوجهات والأهداف الأساسية للعمل، وتوضح الإطار العام الذي يجب الالتزام به عند تنفيذ المهام.

٢. الإجراءProcedure –

يحدد الإجراء الخطوات العامة اللازمة لتنفيذ نشاط أو عملية معينة، ويترجم السياسة إلى خطوات عملية قابلة للتنفيذ.

٣. إجراء التشغيل المعياريSOP –

يقدم إجراء التشغيل المعياري (Standard Operating Procedure) خطوات تفصيلية ومنظمة لتنفيذ مهمة محددة، بحيث يتم تنفيذها بطريقة موحدة ومتسقة من قبل العاملين.

٤. تعليمات العمل Work Instruction –

تتضمن تعليمات العمل الخطوات الدقيقة الخاصة بمهمة فرعية أو عملية محددة، وتكون أكثر تفصيلًا من إجراءات التشغيل المعيارية، وتهدف إلى توضيح كيفية تنفيذ المهمة عمليًا.

٥. إجراء الطوارئ Emergency Procedure –

يحدد إجراء الطوارئ الخطوات والإجراءات الواجب اتباعها عند وقوع حالة طارئة، بما يساعد على سرعة التعامل معها وتقليل آثارها.

٦. إجراء الاستجابة للحوادث Incident Response Procedure –

يوضح إجراء الاستجابة للحوادث الخطوات الخاصة بالتعامل مع الحوادث الأمنية، بدءًا من اكتشاف الحادث والإبلاغ عنه، مرورًا بالتعامل معه، وانتهاءً بالتوثيق والمتابعة.

٧. مصفوفة التصعيد Escalation Matrix –

تحدد مصفوفة التصعيد مستويات التصعيد والمسؤوليات، وتوضح متى يجب رفع الحادث أو المشكلة إلى مستوى إداري أو أمني أعلى، ومن هو المسؤول عن اتخاذ القرار في كل مستوى.

وبصورة عامة، يمكن فهم التسلسل على أنه يبدأ من السياسة التي تحدد *ماذا ولماذا*، ثم الإجراء الذي يوضح *كيف بشكل عام*، ثم SOP الذي يحدد *كيف بالتفصيل*، يليه تعليمات العمل التي توضح *الخطوات الدقيقة*، بينما تتخصص إجراءات الطوارئ والاستجابة للحوادث في الحالات الاستثنائية، وتحدد مصفوفة التصعيد المسؤوليات ومستويات رفع الأحداث.

فالسياسة ليست إجراءً، والإجراء ليس تعليمات عمل تفصيلية.

ثالثًا: أنواع إجراءات التشغيل

يمكن تصنيف إجراءات التشغيل إلى عدة أنواع: (5)

1. إجراءات التشغيل اليومية
   - بدء العمل.
   - متابعة الشاشات.
   - تسليم وتسلم المناوبات.
   - انتهاء العمل.
2. إجراءات التعامل مع الأحداث
   - اكتشاف الحدث.
   - التحقق من الحدث.
   - تصنيف الحدث.
   - الاستجابة للحدث.
   - التصعيد.
3. إجراءات الطوارئ
   - الحريق.
   - الانفجار.
   - الاقتحام.
   - الكوارث الطبيعية.
   - انقطاع الطاقة.
4. إجراءات الصيانة
   - الصيانة الوقائية.
   - الصيانة التصحيحية.
   - التعامل مع الأعطال.
5. إجراءات الأمن السيبراني
   - التعامل مع الاختراقات.
   - التعامل مع فقدان البيانات.
   - التعامل مع التحديثات.(6)

رابعًا: عناصر إجراءات التشغيل

تشمل إجراءات التشغيل عدة عناصر:(7)

- الهدف.
- النطاق.
- المسؤوليات.
- الخطوات.
- الموارد.
- التوثيق.
- المراجعة.

خامسًا: إعداد إجراءات التشغيل

ينبغي أن تُعدّ إجراءات التشغيل وفق منهجية منظمة:(8)

1. تحليل المهام
   - تحديد المهام المطلوبة.
   - تحديد المخاطر.
   - تحديد المتطلبات.
2. صياغة الإجراءات
   - كتابة الخطوات بوضوح.
   - تحديد المسؤوليات.
   - تحديد الموارد.
3. الاختبار
   - اختبار الإجراءات في بيئة محمية.
   - تعديل الإجراءات حسب الحاجة.
4. الاعتماد

- اعتماد الإجراءات رسميًا.
- توزيعها على العاملين.

5. المراجعة

- مراجعة الإجراءات دوريًا.
- تعديلها حسب الحاجة.(9)

سادسًا: تدريب العاملين على الإجراءات

لا تكفي صياغة الإجراءات، بل يجب تدريب العاملين عليها (١٠). ويشمل التدريب:

- شرح الإجراءات.
- التدريب العملي. / المحاكاة. /التقييم.

المراجع:

١. ينظر: المنظمة العربية للتنمية الإدارية .(2007) .التدريب وتنمية الموارد البشرية .القاهرة: المنظمة العربية للتنمية الإدارية.

٢. ينظر: حسين حريم .(2013) .إدارة الموارد البشرية: إطار متكامل .عمّان: دار الحامد للنشر والتوزيع.

٣. ينظر: محمد الصيرفي .(2006) .التدريب الإداري: المدربون والمتدربون وأساليب التدريب .الإسكندرية: مؤسسة حورس الدولية للنشر والتوزيع.

٤. ينظر: عبد الرحمن العيسوي .(2004) .الكفاءة الإدارية والتدريب الإداري . الإسكندرية: دار الجامعة الجديدة.

٥. ينظر: أحمد سيد مصطفى .(2004) .إدارة الموارد البشرية: الإدارة العصرية لرأس المال الفكري .القاهرة: دار الكتب.

٦. ينظر: المنظمة العربية للتنمية الإدارية .(2010) .قياس وتقييم العائد من التدريب .القاهرة: المنظمة العربية للتنمية الإدارية.

٧. ينظر: المنظمة العربية للتنمية الإدارية .(2009) .التدريب وتنمية الموارد البشرية: المفاهيم والأساليب والتطبيقات .القاهرة: المنظمة العربية للتنمية الإدارية.

٨. ينظر: أحمد ماهر .(2007) .إدارة الموارد البشرية .الإسكندرية: الدار الجامعية.

٩. ينظر: علي السلمي .(2001) .إدارة الموارد البشرية والكفاءة الإنتاجية .القاهرة: دار غريب للطباعة والنشر والتوزيع.

١٠. ينظر: عبد الباري إبراهيم درة، وزهير نعيم الصباغ .(2008) .إدارة الموارد البشرية في القرن الحادي والعشرين: منحى نظمي .عمّان: دار وائل للنشر.

المبحث السادس: التعامل مع الأحداث

يمثل التعامل مع الأحداث جوهر عمل مركز المراقبة. فالمشـــغل لا يقتصـــر دوره على متابعة الشـاشـات، بل يمتد إلى اكتشـاف الأحداث والتحقق منها وتقييمها وتصـنيفها والاستجابة لها وتصعيدها.(1)
ويكتسـب هذا المبحث أهمية خاصـة لأنه يحدد دورة التعامل مع الأحداث، ويبين أن الاستجابة الفعالة تتطلب تكاملًا بين العنصر البشري والتقنية والإجراءات.(2)

أولًا: مفهوم الحدث الأمني
يمكن تعريف الحدث الأمني بأنه :أي واقعة أو ســـلوك أو ظرف قد يمثل خطرًا أو مخالفة أو تهديدًا أمنيًا، ويستدعي انتباه المشغل واتخاذ إجراء مناسب .(3)

ثانيًا: دورة التعامل مع الأحداث
تمر دورة التعامل مع الأحداث بتسع مراحل:(4)

1. الملاحظة(Observation)
   - متابعة تدفقات الفيديو.
   - رصد الأنشطة.
2. الكشف(Detection)
   - اكتشاف الحدث من خلال المراقبة المباشرة أو التنبيهات.
   - استخدام التحليلات الذكية لدعم الاكتشاف.
3. التحقق(Verification)
   - التحقق من طبيعة الحدث.
   - التحقق من موقع الحدث.
4. التقييم(Assessment)
   - تقييم مستوى الخطورة.
   - تقييم الأولوية.

5. التصنيف(Classification)
   - تصنيف الحدث حسب النوع والخطورة.
   - تحديد الإجراء المناسب.
6. الاستجابة(Response)
   - تنفيذ الإجراء المناسب.
   - التنسيق مع الجهات الأخرى.
7. التصعيد(Escalation)
   - تصعيد الحدث.
   - إبلاغ الجهات المعنية.
8. التوثيق(Documentation)
   - توثيق الحدث.
   - توثيق الإجراءات المتخذة.
9. المراجعة(Review)
   - مراجعة التعامل مع الحدث.
   - استخلاص الدروس المستفادة.(5)

ثالثًا: مستويات الأحداث

يمكن تصنيف الأحداث وفق مستويات الخطورة:(6)

1. أحداث عادية
   - لا تشكل تهديدًا أمنيًا.
   - لا تستدعي تدخلًا.
2. أحداث تستدعي الانتباه
   - قد تشكل تهديدًا محتملًا.
   - تستدعي متابعة.
3. أحداث تستدعي التدخل

- تشكل تهديدًا أمنيًا.
- تستدعي استجابة فورية.

4. أحداث حرجة

- تشكل تهديدًا خطيرًا.
- تستدعي تصعيدًا فوريًا.

رابعًا: مصفوفة الأحداث

يمكن بناء مصفوفة للأحداث تربط بين نوع الحدث ومستوى الخطورة وإجراء المشغل و الاستخدام القيادي والتوثيق: (7)

الحدث	مستوى الخطورة	إجراء المشغل	الاستخدام القيادي	التوثيق
حركة غير اعتيادية	منخفض	التحقق والمتابعة	عند الحاجة	سجل الحدث
دخول غير مصرح	متوسط	التحقق والتواصل	المشرف/الحراسة	تقرير
اقتحام	عالٍ	متابعة وتصعيد فوري	الأمن/الطوارئ	تقرير حادث
تهديد حرج	حرج	تنفيذ خطة الطوارئ	القيادة/الجهات المختصة	تقرير شامل

وهذه المصفوفة إطار تربوي وتطبيقي وليست معيارًا ملزمًا.

خامسًا: عوامل نجاح التعامل مع الأحداث

يتوقف نجاح التعامل مع الأحداث على عدة عوامل: (8)

- سرعة الاكتشاف.
- دقة التحقق.

- صحة التقييم.
- صحة التصنيف.
- سرعة الاستجابة.
- فعالية التصعيد.
- فعالية التنسيق.
- جودة التوثيق.
- كفاءة المشغلين.
- وضوح الإجراءات.

سادسًا: التحديات في التعامل مع الأحداث

يواجه المشغلون تحديات متعددة في التعامل مع الأحداث:

- كثرة الإنذارات الكاذبة.
- الحمل المعرفي.
- ضغط الوقت.
- نقص المعلومات.
- صعوبة التنسيق.
- القيود التقنية.
- القيود القانونية.

المراجع:

١. ينظر: المنظمة العربية للتنمية الإدارية .(2009) .التدريب وتنمية الموارد البشرية: المفاهيم والأساليب والتطبيقات .القاهرة: المنظمة العربية للتنمية الإدارية.

٢. ينظر: أحمد ماهر .(2007) .إدارة الموارد البشرية .الإسكندرية: الدار الجامعية.

٣. ينظر: علي السلمي .(2001) .إدارة الموارد البشرية والكفاءة الإنتاجية .القاهرة: دار غريب للطباعة والنشر والتوزيع.

٤. ينظر: عبد الباري إبراهيم درة، وزهير نعيم الصباغ .(2008) .إدارة الموارد البشرية في القرن الحادي والعشرين: منحى نظمي .عمّان: دار وائل للنشر.
٥. ينظر: محمد الصيرفي .(2006) .التدريب الإداري: المدربون والمتدربون وأساليب التدريب .الإسكندرية: مؤسسة حورس الدولية للنشر والتوزيع.
٦. ينظر: عبد الرحمن العيسوي .(2004) .الكفاءة الإدارية والتدريب الإداري . الإسكندرية: دار الجامعة الجديدة.
٧. ينظر: أحمد سيد مصطفى .(2004) .إدارة الموارد البشرية: الإدارة العصرية لرأس المال الفكري .القاهرة: دار الكتب.
٨. ينظر: المنظمة العربية للتنمية الإدارية .(2010) .قياس وتقييم العائد من التدريب .القاهرة: المنظمة العربية للتنمية الإدارية.

المبحث السابع: التوثيق والإبلاغ

يُعدّ التوثيق والإبلاغ من أهم مهام مشغلي أنظمة المراقبة، إذ يضمنان حفظ سجل للأحداث والإجراءات المتخذة، ويسهلان المراجعة والمساءلة والتحسين.(1)
ويكتسب هذا المبحث أهمية خاصة لأنه يحدد متطلبات التوثيق والإبلاغ، ويبين أن التوثيق ليس إجراءً إداريًا ثانويًا، بل هو جزء من العمل الأمني. كما يميز بين توثيق الحدث وحفظ الدليل الرقمي، إذ إن لكل منهما متطلبات مختلفة.(2)

أولًا: مفهوم التوثيق والإبلاغ

يمكن تعريف التوثيق بأنه :عملية تسجيل الأحداث والإجراءات والمعلومات المتعلقة بها في سجل منظم يمكن الرجوع إليه لاحقًا .(3)
ويمكن تعريف الإبلاغ بأنه :عملية نقل المعلومات المتعلقة بالأحداث إلى الجهات المعنية في الوقت المناسب .(4)

ثانيًا: التمييز بين توثيق الحدث وحفظ الدليل الرقمي

من الأخطاء الشائعة الخلط بين توثيق الحدث وحفظ الدليل الرقمي:(5)

المعيار	توثيق الحدث	حفظ الدليل الرقمي
الهدف	تسجيل الأحداث والإجراءات	حفظ الأدلة الرقمية
المتطلبات	الدقة والاكتمال	سلامة الدليل
الإجراءات	التسجيل والإبلاغ	سلسلة الحيازة
المرجع	IEC 62676-4	NISTIR 8387، ISO 27037

ثالثًا: أهمية التوثيق والإبلاغ

يكتسب التوثيق والإبلاغ أهمية خاصة لعدة أسباب:(6)

- حفظ سجل للأحداث.
- دعم التحقيقات.

- المساءلة.
- تحسين الأداء.
- الامتثال للمتطلبات.

رابعًا: محتوى التوثيق

يشمل التوثيق عدة عناصر:(7)

- وقت الحدث.
- موقع الحدث.
- وصف الحدث.
- الكاميرات ذات الصلة.
- الإجراءات المتخذة.
- الجهات التي تم إبلاغها.
- وقت الإبلاغ.
- النتائج.

خامسًا: سلامة الأدلة الرقمية

عندما يستخدم التسجيل لأغراض إثباتية، ينبغي توثيق:(8)

١. سلامة التسجيل :عدم التعديل غير المصرح به.
٢. مصدر التسجيل :الكاميرا أو الجهاز.
٣. وقت التسجيل :التاريخ والوقت.
٤. مزامنة الوقت :توحيد التوقيت بين الأجهزة.
٥. التحكم في الوصول :الصلاحيات.
٦. سجل العمليات :تسجيل جميع العمليات.
٧. سلسلة حيازة الدليل :توثيق حركة الدليل.
٨. منع التعديل غير المصرح به :آليات الحماية.

٩. سياسات الاحتفاظ :مدة الاحتفاظ.

١٠. استخراج التسجيلات :إجراءات التصدير.

وتشـــير NISTIR 8387إلى أهمية توثيق مصـــدر الملف، والحفاظ على ســـلامته، واستخدام قيم التجزئة الرقمية Hashes عند التعامل مع الأدلة الرقمية.(9)

كما توفر ISO/IEC 27037إرشادات لتحديد وجمع وحفظ الأدلة الرقمية.(10)

سادسًا: أساليب التوثيق

يمكن استخدام عدة أساليب للتوثيق:(11)

1. السجلات اليدوية
   - كتابة الأحداث في سجل ورقي.
2. السجلات الإلكترونية
   - استخدام أنظمة إلكترونية لتسجيل الأحداث.
3. التسجيلات المرئية : ستخدام التسجيلات المرئية كتوثيق.
4. التقارير : إعداد تقارير دورية أو حسب الحاجة.(12)

سابعًا: معايير التوثيق الجيد

يتميز التوثيق الجيد بعدة خصائص:(13)

- الدقة /الاكتمال. /لوضـــوح. /التوقيت. /الموضـــوعية. /التنظيم. /ســـهولة الوصول.

المراجع:

١. ينظر: National Institute of Standards and Technology (NIST). (2022). Digital Evidence Preservation: Considerations for Evidence Handlers, NISTIR 8387. Gaithersburg, MD: National Institute of Standards and Technology.

٢. ينظر: International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC). (2012). ISO/IEC 27037:2012: Information Technology — Security Techniques — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence. Geneva: ISO.

٣. ينظر: National Institute of Standards and Technology (NIST). (2006). Guide to Integrating Forensic Techniques into Incident Response, NIST Special Publication 800-86. Gaithersburg, MD: National Institute of Standards and Technology.

٤. ينظر: International Electrotechnical Commission (IEC). (2025). IEC 62676-4:2025: Video Surveillance Systems for Use in Security Applications — Part 4: Application Guidelines. Geneva: International Electrotechnical Commission.

٥. ينظر: Scientific Working Group on Digital Evidence (SWGDE). (2023). Best Practices for Digital Forensic Video Analysis, SWGDE 18-V-001-2.0.

٦. ينظر: National Institute of Standards and Technology (NIST). (2022). Digital Evidence Preservation: Considerations for Evidence Handlers, NISTIR 8387. Gaithersburg, MD: National Institute of Standards and Technology.

٧. ينظر: International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC). (2012). ISO/IEC 27037:2012: Information Technology — Security Techniques — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence. Geneva: ISO.

٨. ينظر: National Institute of Standards and Technology (NIST). (2012). Computer Security Incident Handling Guide, NIST Special Publication 800-61 Revision 2. Gaithersburg, MD: National Institute of Standards and Technology.

٩. ينظر: National Institute of Standards and Technology (NIST). (2022). Digital Evidence Preservation: Considerations for Evidence Handlers, NISTIR 8387. Gaithersburg, MD: National Institute of Standards and Technology.

١٠. ينظر: International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC). (2012). ISO/IEC 27037:2012: Information Technology — Security Techniques — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence. Geneva: ISO.

١١. ينظر: National Institute of Standards and Technology (NIST). (2006). Guide to Integrating Forensic Techniques into Incident Response, NIST Special Publication 800-86. Gaithersburg, MD: National Institute of Standards and Technology.

١٢. ينظر: Scientific Working Group on Digital Evidence (SWGDE). (2023). Best Practices for Digital Forensic Video Analysis, SWGDE 18-V-001-2.0.

١٣. ينظر: International Electrotechnical Commission (IEC). (2025). IEC 62676-4:2025: Video Surveillance Systems for Use in Security Applications — Part 4: Application Guidelines. Geneva: International Electrotechnical Commission.

المبحث الثامن: الإرهاق والأخطاء البشرية

يمثل الإرهاق والأخطاء البشرية من أهم التحديات التي تواجه مشغلي أنظمة المراقبة. فالمشغل البشري، مهما كان مدربًا، معرض للإرهاق وانخفاض الانتباه وارتكاب الأخطاء، خاصة في المهام الرتيبة طويلة الأمد.(1)

ويكتسب هذا المبحث أهمية خاصة لأنه يحدد أسباب الإرهاق والأخطاء البشرية، ويبين كيفية التغلب عليها أو تقليل آثارها. ويعتمد هذا المبحث على مجال Human Factorsالمتخصص، وليس على مراجع CCTV وحدها.(2)

أولًا: مفهوم الإرهاق

يمكن تعريف الإرهاق بأنه :حالة من الإنهاك الجسدي أو الذهني تنشأ عن المجهود المستمر أو المهام الرتيبة أو الظروف غير المناسبة، وتؤدي إلى انخفاض الأداء وزيادة الأخطاء .(3)

ويشير Reasonإلى أن الأخطاء البشرية ليست عشوائية، بل تحدث في أنماط يمكن توقعها والوقاية منها.(4)

ثانيًا: أسباب الإرهاق : يحدث الإرهاق لعدة أسباب:(5)

ونشير إلى أن الحمل المعرفي يمثل عاملًا حاسمًا في أداء المشغل، وأن زيادة الحمل تؤدي إلى انخفاض الأداء وزيادة الأخطاء.(6)

ثالثًا: أنواع الأخطاء البشرية

يمكن تصنيف الأخطاء البشرية وفق Reason إلى:(7)

1. الأخطاء(Mistakes)
   - أخطاء في التخطيط.
   - أخطاء في القرار.
2. الزلات(Slips)
   - أخطاء في التنفيذ.
   - أخطاء في الانتباه.
3. الهفوات(Lapses)
   - أخطاء في الذاكرة.

- أخطاء في التركيز.

رابعًا: تأثير الإرهاق في الأداء

يؤثر الإرهاق في الأداء بعدة طرق:(8)

- انخفاض الانتباه.
- بطء الاستجابة.
- زيادة الأخطاء.
- انخفاض جودة القرارات.
- انخفاض الدافعية.
- زيادة التوتر.

خامسًا: استراتيجيات التغلب على الإرهاق والأخطاء

يمكن التغلب على الإرهاق والأخطاء من خلال:(9)

1. تنظيم المناوبات
   - تقصير المناوبات.
   - زيادة فترات الراحة.
   - تناوب المهام.
2. تحسين بيئة العمل
   - الإضاءة المناسبة.
   - تقليل الضوضاء.
   - التحكم في الحرارة.
   - توفير التهوية.
3. تقليل الحمل المعرفي
   - تقليل عدد الشاشات.
   - تقليل التنبيهات غير الضرورية.

- استخدام التحليلات الذكية.

4. التدريب
   - تدريب على إدارة الإرهاق.
   - تدريب على التعامل مع الضغط.
5. الدعم النفسي
   - توفير الدعم النفسي.
   - توفير فترات راحة نفسية.
6. الأتمتة
   - استخدام الأتمتة للمهام الرتيبة.
   - استخدام التحليلات الذكية للكشف الأولي.

ويشير Parasuraman & Riley إلى أن الأتمتة يمكن أن تقلل الحمل المعرفي، لكنها قد تؤدي إلى مشكلات جديدة مثل "الاستخدام الخاطئ" أو "الإهمال" أو "إساءة الاستخدام" إذا لم تُصمم بصورة مناسبة.(10)

المراجع:

١. ينظر: Reason, J. (1990). Human Error. Cambridge University Press.

٢. ينظر: Wickens, C. D., Hollands, J. G., Banbury, S., & Parasuraman, R. (2016). *Engineering Psychology and Human Performance*. 4th ed., Routledge.

٣. ينظر: Hockey, G. R. J. (2013). *The Psychology of Fatigue: Work, Effort and Control*. Cambridge University Press.

٤. ينظر: Reason, J. (1990). *Human Error*. Cambridge University Press.

٥. ينظر: Dawson, D., McCulloch, K., & Baker, A. (2001). "Extended Workhours and the Accidents and Injuries in the Workplace: A Review of the Evidence." *Occupational and Environmental Medicine*, 58(2), 68–75.

٦. ينظر: Wickens, C. D., Hollands, J. G., Banbury, S., & Parasuraman, R. (2016). *Engineering Psychology and Human Performance*. 4th ed., Routledge.

٧. ينظر: Reason, J. (1990). *Human Error*. Cambridge University Press.

٨. ينظر: Hockey, G. R. J. (2013). *The Psychology of Fatigue: Work, Effort and Control*. Cambridge University Press.

٩. ينظر: International Organization for Standardization (ISO). (2019). *ISO 10075-2:2019: Ergonomic Principles Related to Mental Workload — Part 2: Design Principles*.

١٠. ينظر: Parasuraman, R., & Riley, V. (1997). "Humans and Automation: Use, Misuse, Disuse, Abuse." *Human Factors*, 39(2), 230–233

.

المبحث التاسع: الصيانة واستمرارية التشغيل

تمثل الصيانة واستمرارية التشغيل من أهم متطلبات المنظومة الأمنية، إذ تضمن استمرار عمل المنظومة بكفاءة وفعالية، وتحد من الأعطال والتوقف.(1)
ويكتسب هذا المبحث أهمية خاصة لأنه يحدد أنواع الصيانة ومتطلبات استمرارية التشغيل، ويبين أن المنظومة لا تكتمل بمجرد التركيب، بل تحتاج إلى صيانة مستمرة

أولًا: مفهوم الصيانة
يمكن تعريف الصيانة بأنها :مجموعة الإجراءات والعمليات التي تهدف إلى الحفاظ على المنظومة في حالة عمل جيدة، والوقاية من الأعطال، وإصلاح الأعطال عند حدوثها

ثانيًا: أنواع الصيانة
يمكن تصنيف الصيانة إلى عدة أنواع

1. الصيانة الوقائية
   - تتم بشكل دوري.
   - تهدف إلى الوقاية من الأعطال.
   - تشمل الفحص والتنظيف والاختبار.
2. الصيانة التصحيحية
   - تتم عند حدوث عطل.
   - تهدف إلى إصلاح العطل.
   - تشمل الإصلاح والاستبدال.
3. الصيانة التنبؤية
   - تعتمد على مراقبة الحالة.
   - تهدف إلى التنبؤ بالأعطال.
   - تشمل تحليل البيانات والإنذارات.

4. الصيانة الطارئة
   - تتم عند حدوث عطل مفاجئ.
   - تهدف إلى إصلاح العطل بأسرع وقت.
   - تشمل الإصلاح الفوري

ثالثًا: استمرارية التشغيل

تتطلب استمرارية التشغيل عدة عناصر

1. الطاقة الاحتياطية
   - UPS.
   - المولدات.
   - مصادر الطاقة البديلة.
2. التكرار
   - تكرار المكونات الحرجة.
   - تكرار مسارات الاتصال.
   - تكرار التخزين.
3. الصيانة
   - الصيانة الوقائية.
   - الصيانة التصحيحية.
   - الصيانة التنبؤية.
4. إدارة الأعطال
   - اكتشاف الأعطال.
   - الإبلاغ عن الأعطال.
   - إصلاح الأعطال.
   - توثيق الأعطال.
5. خطط الطوارئ

- خطط الاستجابة للطوارئ.
- خطط التعافي.
- خطط الاستمرارية

رابعًا: الأمن السيبراني لمركز المراقبة

مع تحول مراكز المراقبة إلى بيئات رقمية متكاملة، أصبح الأمن السيبراني محورًا مستقلًا في استمرارية التشغيل (٨). ويشمل:

- إدارة الحسابات والصلاحيات.
- الفصل الشبكي.
- تحديث البرمجيات.
- إدارة الثغرات.
- النسخ الاحتياطي.
- مراقبة السجلات.
- الوصول عن بعد.
- حماية محطات المشغلين.
- الاستجابة للحوادث السيبرانية.
- أمن الموردين.

وتشير إرشادات NIST SP 800-82 Rev. 3 إلى أهمية حماية أنظمة OT/ICS من التهديدات السيبرانية، وأن مركز المراقبة يمثل سطحًا للهجوم السيبراني

خامسًا: معايير تقييم الصيانة واستمرارية التشغيل

يمكن تقييم الصيانة واستمرارية التشغيل من خلال عدة معايير

- نسبة توافر النظام.
- متوسط الوقت بين الأعطال.
- متوسط الوقت للإصلاح.

- نسبة الأعطال المتكررة.
- كفاءة الصيانة.
- فعالية خطط الطوارئ.
- مستوى التدريب على الصيانة.

خلاصة الفصل السابع

يتضح من دراسة تشغيل وإدارة مراكز المراقبة أن نجاح منظومة المراقبة لا يقاس بعدد الكاميرات أو دقة الصورة، وإنما بقدرة المنظومة على اكتشاف الأحداث والتحقق منها والاستجابة لها. وأن هذه القدرة لا تتحقق إلا بتكامل أربعة عناصر: التقنية، والمعلومات، والعنصر البشري، والإجراءات.

وقد أظهر التحليل أن مركز المراقبة بيئة تشغيلية متكاملة وليس مجرد غرفة شاشات، وأن نجاحه يتوقف على تصميمه وتنظيم العمل فيه وكفاءة مشغليه. وأن البنية الوظيفية للمركز تشمل تسعة عناصر مترابطة، تبدأ من مصادر البيانات وتنتهي بالتوثيق والتحليل اللاحق.

كما تبين أن مشغل أنظمة المراقبة يمثل العنصر البشري الذي يحول البيانات المرئية إلى قرارات واستجابات، وأنه يواجه تحديات متعددة، أهمها الإرهاق، والحمل المعرفي، وضغط الوقت، والإنذارات الكاذبة، والتعرض للمشاهد الصادمة. وأن أداءه يتأثر بالتدريب والخبرة وبيئة العمل.

وأظهر التحليل أن التدريب والتأهيل من أهم العوامل التي تحدد فاعلية المشغلين، وأن التدريب ليس حدثًا لمرة واحدة، بل عملية مستمرة. وأن إجراءات التشغيل تمثل الإطار الذي يوجه عمل المشغلين، ويجب التمييز فيها بين السياسة/الإجراء/إجراء التشغيل القياسي/تعليمات العمل.

وأن التعامل مع الأحداث يمثل جوهر عمل المركز، ويمر بتسع مراحل: الملاحظة، والكشف، والتحقق، والتقييم، والتصنيف، والاستجابة، والتصعيد، والتوثيق، والمراجعة.

كما تبين أن التوثيق والإبلاغ من أهم مهام المشغلين، وأن التمييز بين توثيق الحدث وحفظ الدليل الرقمي ضروري للوضوح الأكاديمي. وأن الإرهاق والأخطاء البشرية من أهم التحديات التي تواجههم، وأن الصيانة واستمرارية التشغيل من أهم متطلبات المنظومة. وأن الأمن السيبراني أصبح محورًا مستقلًا في استمرارية التشغيل.

ومن هنا يمكن صياغة النموذج المتكامل لتشغيل مركز المراقبة على النحو الآتي:

الهدف الأمني ← تصميم المركز ← تنظيم العمل ← اختيار المشغلين ← تدريبهم ← إجراءات التشـــغيل ← التعامل مع الأحداث ← التوثيق والإبلاغ ← إدارة الإرهاق ← الصيانة واستمرارية التشغيل ← الأمن السيبراني ← التقييم والتحسين

ومن هنا فإن نجاح مركز المراقبة لا يقاس بالسؤال: كم شاشة لدينا؟ بل بالسؤال الأكثر دقة: هل يستطيع المركز تحويل المعلومات المرئية إلى استجابة أمنية فعالة في الوقت المناسب؟ ويكتمل هذا السؤال بمؤشر زمن دورة الحدث الأمني:

زمن دورة الحدث = زمن الكشـــف + زمن التحقق + زمن التقييم + زمن اتخاذ القرار + زمن التصعيد + زمن بدء الاستجابة

أهم نتائج الفصل السابع

١. مركز المراقبة بيئة تشغيلية متكاملة وليس مجرد غرفة شاشات.
٢. يتكون المركز من أربعة عناصـــر: التقنية، والمعلومات، والعنصـــر البشـــري، والإجراءات.
٣. لا ينبغي تقييم نجاح المركز بعدد الشاشات أو حجم جدار الفيديو.
٤. البنية الوظيفية للمركز تشمل تسعة عناصر مترابطة.
٥. النموذج التشغيلي التساعي يوفر إطارًا واضحًا للتعامل مع الأحداث.
٦. مؤشرات الأداء توفر أدوات موضوعية لتقييم الفعالية.
٧. زمن دورة الحدث الأمني مؤشر تشغيلي مركب.
٨. يجب التمييز بين VMS و PSIMوالأنظمة الأخرى.
٩. تنظيم العمل يمثل الأساس التنظيمي لتشغيل المركز.
١٠. التنظيم الجيد يمكن أن يخفف أثر بعض أوجه القصـــور التقني، لكنه لا يعوض المتطلبات التقنية الحرجة.
١١. مشغل أنظمة المراقبة يحول البيانات المرئية إلى قرارات.
١٢. مشغل أنظمة المراقبة يواجه تحديات: الإرهاق، والحمل المعرفي، وضغط الوقت، والإنذارات الكاذبة، والتعرض للمشاهد الصادمة.
١. التدريب والتأهيل من أهم العوامل التي تحدد فاعلية المشغلين.

٢. إجراءات التشغيل تمثل الإطار الذي يوجه عمل المشغلين.
٣. يجب التمييز بين Policy/Procedure/SOP/Work Instruction.
٤. التعامل مع الأحداث يمثل جوهر عمل مركز المراقبة.
٥. دورة التعامل مع الأحداث تشمل تسع مراحل.
٦. مصفوفة الأحداث توفر إطارًا تربويًا وتطبيقيًا.
٧. التوثيق والإبلاغ من أهم مهام المشغلين.
٨. يجب التمييز بين توثيق الحدث وحفظ الدليل الرقمي.
٩. سلامة الأدلة الرقمية تتطلب توثيق المصدر والوقت والمزامنة.
١٠. سلسلة الحيازة ضرورية للأدلة الرقمية.
١١. الإرهاق والأخطاء البشرية من أهم التحديات.
١٢. الأخطاء البشرية تصنف وفق Reason إلى Mistakes و Slipsو Lapses.
١٣. يمكن التغلب على الإرهاق بتقليل الحمل المعرفي وتحسين بيئة العمل.
١٤. الصيانة واستمرارية التشغيل من أهم متطلبات المنظومة.
١٥. الصيانة تشمل: الوقائية، والتصحيحية، والتنبؤية، والطارئة.
١٦. استمرارية التشغيل تتطلب الطاقة الاحتياطية والتكرار.
١٧. الأمن السيبراني محور مستقل في استمرارية التشغيل.
١٨. المعيار النهائي: هل يستطيع المركز تحويل المعلومات المرئية إلى استجابة أمنية فعالة؟

أسئلة التفكير والتقييم للفصل السابع

أولًا: أسئلة معرفية

١. ما تعريف مركز المراقبة؟ وما مكوناته الأربعة؟
٢. ما البنية الوظيفية لمركز المراقبة؟
٣. ما الفرق بين VMS وPSIM؟
٤. ما النموذج التشغيلي التساعي؟
٥. ما مؤشرات أداء مركز المراقبة؟

٦. ما مفهوم تنظيم العمل؟ وما عناصره؟
٧. ما نماذج تنظيم العمل؟
٨. ما متطلبات مشغل أنظمة المراقبة؟
٩. ما أنواع التدريب؟
١٠. ما الفرق بين Policy و Procedureو SOP؟
١١. ما مراحل دورة التعامل مع الأحداث؟
١٢. ما الفرق بين توثيق الحدث وحفظ الدليل الرقمي؟
١٣. ما أنواع الأخطاء البشرية وفقReason ؟
١٤. ما أنواع الصيانة؟
١٥. ما مكونات الأمن السيبراني لمركز المراقبة؟

ثانيًا: أسئلة تحليلية

١. حلل العلاقة بين تصميم مركز المراقبة وفاعلية المنظومة.
٢. لماذا لا يقاس نجاح المركز بعدد الشاشات؟
٣. لماذا يعدّ زمن دورة الحدث الأمني مؤشرًا مركبًا؟
٤. كيف يمكن لمؤشرات الأداء أن تحسن تشغيل المركز؟
٥. لماذا لا يمكن للتنظيم الجيد أن يعوض كل القيود التقنية؟
٦. لماذا يعدّ الإرهاق من أهم تحديات المشغل؟
٧. كيف تؤثر الإنذارات الكاذبة في أداء المشغل؟
٨. حلل العلاقة بين سرعة الاكتشاف وفاعلية الاستجابة.
٩. لماذا يعدّ التصعيد مرحلة مستقلة عن الاستجابة؟
١٠. لماذا يعدّ التمييز بين توثيق الحدث وحفظ الدليل الرقمي ضروريًا؟
١١. لماذا تعدّ سلسلة الحيازة ضرورية؟
١٢. كيف يؤثر الإرهاق في أداء المشغل؟
١٣. لماذا أصبح الأمن السيبراني محورًا مستقلًا في استمرارية التشغيل؟

ثالثًا: أسئلة تطبيقية

١. اختر منشأة تعرفها، وحلل تصميم مركز المراقبة فيها.

٢. لو طُلب منك تصميم مركز مراقبة لمنشأة حيوية، ما المعايير التي ستراعيها؟

١. ضع مصفوفة مؤشرات أداء لمركز مراقبة.

٢. ضع جدول مناوبات لمركز مراقبة يعمل على مدار الساعة.

٣. ضع وصفًا وظيفيًا لمشغل أنظمة مراقبة في منشأة حيوية.

٤. ضع برنامج تدريب لمشغلي مراقبة في منشأة حيوية.

٥. ضع إجراءات تشغيل لمركز مراقبة في منشأة حيوية.

٦. ضع إجراءً للتعامل مع حدث اقتحام في منشأة حيوية.

٧. صمم مصفوفة أحداث لمنشأة تعليمية.

٨. ضع نموذجًا لتوثيق حدث أمني.

٩. صمم إجراءً لحفظ دليل رقمي.

١٠. ضع برنامجًا لتقليل الإرهاق في مركز مراقبة.

١١. ضع خطة صيانة لمنظومة مراقبة في منشأة حيوية.

١٢. صمم خطة للأمن السيبراني لمركز مراقبة.

١٣. صمم اختبار قبول لمركز مراقبة في منشأة حيوية.

الفصل الثاني: كاميرات المراقبة وتعزيز أمن المنشآت

تمهيد الفصل

يمثل هذا الفصل انتقالًا من دراسة الجوانب الفنية والتشغيلية لمنظومة المراقبة إلى دراسة الوظيفة الأمنية الفعلية التي تؤديها هذه المنظومة في تعزيز أمن المنشآت. فكاميرات المراقبة لا تستمد قيمتها الأمنية من قدرتها على إنتاج الصور وتسجيلها فحسب، وإنما من قدرتها على توفير معلومات قابلة للاستخدام في الوقاية والكشف والاستجابة والتوثيق والتحقيق، ضمن منظومة أمنية متكاملة. وتؤكد الإرشادات الحديثة الخاصة بأنظمة المراقبة بالفيديو أن فاعلية المنظومة ترتبط بالتخطيط والتصميم والتركيب والاختبار والتشغيل والصيانة، وليس بمجرد اقتناء الكاميرات أو رفع مواصفاتها الفنية.(1)

ومن ثم فإن السؤال الأمني الأساسي لا يتمثل في: «كيف تعمل الكاميرا؟»، وإنما في: «ما الوظيفة الأمنية التي تؤديها المنظومة، وكيف تسهم في تحقيق أهداف أمن المنشأة؟». فاختيار نظام الفيديو ينبغي أن ينطلق من حالات الاستخدام والمهام الأمنية المطلوبة، ثم تحديد متطلبات جودة الفيديو والتجهيزات المناسبة لها.(2)

وفي هذا السياق، ينبغي عدم النظر إلى كاميرات المراقبة بوصفها حلًا شاملًا لجميع المخاطر الأمنية، وإنما باعتبارها أحد مكونات منظومة أمنية متعددة الطبقات، تتكامل مع التحكم في الدخول، والإنذار، والحماية المادية، والعنصر البشري، وإجراءات الاستجابة. وتدعم الأدبيات الأمنية الحديثة هذا الاتجاه؛ إذ تؤكد ضرورة ربط أنظمة المراقبة بالسياسات والإجراءات ووسائل الحماية الأخرى، كما تشير الأدلة التطبيقية إلى أن فعالية CCTV تختلف باختلاف السياق وطريقة الاستخدام.(3)

ويتناول هذا الفصل عشرة مباحث مترابطة: الوظيفة الأمنية للمراقبة، والوقاية والردع، واكتشاف الأحداث، ودعم الاستجابة الأمنية، ومراقبة المداخل والمخارج، وحماية

المناطق الحساسة، وتوثيق الوقائع، ودعم الاستدلال والتحقيق، وإدارة الأزمات والطوارئ، وحدود الاعتماد على كاميرات المراقبة.

المبحث الأول: الوظيفة الأمنية للمراقبة

تتعدد الوظائف التي يمكن أن تؤديها منظومة المراقبة بالفيديو بحسب أهداف المنشأة وطبيعة المخاطر التي تواجهها. ولذلك لا ينبغي اختزال وظيفة المراقبة في التسجيل أو المشاهدة، بل ينبغي النظر إليها بوصفها وسيلة لإنتاج معلومات أمنية يمكن توظيفها في مراحل مختلفة من دورة التعامل مع الحدث، ابتداءً من الوقاية والكشف، ومرورًا بالاستجابة، وانتهاءً بالتوثيق والتحقيق.(4)

أولًا: مفهوم الوظيفة الأمنية

يمكن تعريف الوظيفة الأمنية للمراقبة بأنها :مجموعة الأدوار التي تؤديها منظومة المراقبة في دعم أهداف أمن المنشأة، من خلال جمع المعلومات البصرية ومعالجتها واستخدامها في الوقاية والكشف والاستجابة والتوثيق والتحقيق .(5)

ولا يعني ذلك أن كل منظومة مراقبة تؤدي هذه الوظائف بالمستوى نفسه؛ إذ يتحدد ذلك وفق تصميم المنظومة، وموقع الكاميرات، وجودة الصورة، وطرق التشغيل، وقدرات المشغلين، ومدى تكاملها مع الأنظمة والإجراءات الأمنية الأخرى. وتؤكد منهجية

VQiPSأن تحديد متطلبات الفيديو ينبغي أن يبدأ من حالة الاستخدام والوظيفة المطلوب تنفيذها، ثم ترجمة تلك الوظيفة إلى متطلبات فنية.(6)

ثانيًا: الوظائف الأمنية الأساسية

يمكن تحديد الوظائف الأمنية الأساسية للمراقبة في خمس وظائف مترابطة:(7)

1. الوقاية والردع

تسهم المراقبة في الوقاية من خلال زيادة إمكانية اكتشاف النشاط غير المصرح به، وقد تسهم في ردع بعض صور السلوك الإجرامي أو المخالف عندما يدرك الفاعل احتمال اكتشافه. غير أن مقدار هذا الأثر يختلف باختلاف البيئة وطريقة تطبيق النظام .(8)

2. الكشف

تساعد المنظومة على اكتشاف الأحداث أو الأنشطة ذات الدلالة الأمنية، سواء من خلال المراقبة البشرية المباشرة أو من خلال وظائف التحليل الآلي للفيديو.(9)

3. دعم الاستجابة

توفر المنظومة معلومات تساعد العاملين الأمنيين على فهم موقع الحدث وطبيعته وتطوره، ومن ثم دعم اتخاذ القرار وتوجيه الاستجابة المناسبة.(10)

4. التوثيق

توفر التسجيلات سجلًا بصريًا للأحداث يمكن الرجوع إليه لاحقًا للمراجعة والتحقق والتحليل.

5. دعم التحقيق

يمكن استخدام التسجيلات في إعادة بناء التسلسل الزمني للأحداث، وربط المشاهد ببعضها، وتحديد مسارات الحركة والوقائع ذات الصلة، مع مراعاة متطلبات سلامة الأدلة والإجراءات القانونية المعمول بها .

ثالثًا: الفرق بين الوظيفة التقنية والوظيفة الأمنية

ينبغي التمييز بين الوظيفة التقنية للكاميرا والوظيفة الأمنية للمنظومة: (12)

المعيار	الوظيفة الأمنية	الوظيفة التقنية
الهدف	تحقيق غرض أمني	إنتاج صورة أو تسجيل
معيار التقييم	القدرة على دعم هدف أمني محدد	الدقة، الإضاءة، التغطية، جودة الصورة
مجال التركيز	المنظومة والاستخدام والتشغيل	الكاميرا والمكونات الفنية
النتيجة	معلومة قابلة للاستخدام الأمني	صورة أو تسجيل

وعليه، فإن جودة الصورة لا تمثل وحدها معيارًا كافيًا للحكم على فاعلية النظام؛ فقد تكون الصورة ذات جودة فنية مرتفعة، لكنها غير مناسبة للغرض الأمني المطلوب إذا كان موضع التصوير غير مناسب أو كانت زاوية الرؤية لا تحقق المهمة المطلوبة. ونؤكد أن جودة الفيديو ينبغي تقييمها في ضوء ما يحتاج المستخدم إلى رؤيته والتعرف عليه في حالة الاستخدام المحددة

المراجع:

١. ينظر: National Institute of Standards and Technology (NIST). Video Quality in Public Safety (VQiPS). Gaithersburg, MD: NIST.

٢. ينظر: International Electrotechnical Commission (IEC). (2025). IEC 62676-4:2025: Video surveillance systems for use in security applications – Part 4: Application guidelines. 2nd ed., Geneva: IEC.

٣. ينظر: National Institute of Standards and Technology (NIST). Video Quality in Public Safety (VQiPS). Gaithersburg, MD: NIST.

٤. ينظر: International Electrotechnical Commission (IEC). (2025). IEC 62676-4:2025: Video surveillance systems for use in security applications – Part 4: Application guidelines. 2nd ed., Geneva: IEC.

٥. ينظر: Welsh, B. C., & Farrington, D. P. (2009). "Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-Analysis." Justice Quarterly, 26(4), 716–745.

٦. ينظر: International Electrotechnical Commission (IEC). (2025). IEC 62676-4:2025: Video surveillance systems for use in security applications – Part 4: Application guidelines. 2nd ed., Geneva: IEC.

٧. ينظر: National Institute of Standards and Technology (NIST). (2023). Guide to Operational Technology (OT) Security, NIST Special Publication 800-82 Revision 3. Gaithersburg, MD: NIST.

٨. ينظر: Scientific Working Group on Digital Evidence (SWGDE). (2023). Best Practices for Digital Forensic Video Analysis, SWGDE 18-V-001-2.0.

٩. ينظر: International Electrotechnical Commission (IEC). (2025). IEC 62676-4:2025: Video surveillance systems for use in security applications – Part 4: Application guidelines. 2nd ed., Geneva: IEC.

١٠. ينظر: National Institute of Standards and Technology (NIST). Video Quality in Public Safety (VQiPS). Gaithersburg, MD: NIST.

المبحث الثاني: الوقاية والردع

تمثل الوقاية والردع إحدى الوظائف المهمة للمراقبة، إلا أن التعامل معها أكاديميًا يتطلب تجنب افتراض أن وجود الكاميرات يؤدي تلقائيًا إلى انخفاض الجريمة أو منع الحوادث. فقد أظهرت المراجعات المنهجية أن أثر CCTV في خفض الجريمة موجود في بعض السياقات ولكنه متواضع ومتفاوت بحسب المكان ونوع الجريمة وطريقة التطبيق.(1)

أولًا: مفهوم الوقاية والردع

يمكن تعريف الوقاية بأنها: مجموعة الإجراءات والوسائل التي تهدف إلى منع وقوع الأحداث الأمنية أو خفض احتمال حدوثها أو الحد من آثارها .(2)

أما الردع في سياق المراقبة فيشير إلى الأثر المحتمل للمراقبة في رفع الإدراك باحتمال اكتشاف السلوك غير المشروع، بما قد يؤثر في قرار الفاعل المحتمل .(3)

ثانيًا: آليات الردع

يمكن فهم أثر الردع المرتبط بالمراقبة من خلال عدد من الآليات:(4)

١. الإدراك: إدراك وجود المراقبة.
٢. احتمال الاكتشاف: اعتقاد الفاعل بأن نشاطه يمكن اكتشافه.
٣. احتمال التدخل: توقع أن يؤدي الكشف إلى تدخل أمني.
٤. سرعة الكشف والاستجابة: انخفاض الفترة بين وقوع الحدث واكتشافه والتعامل معه.
٥. ارتباط المراقبة بإجراءات أمنية أخرى: مثل الحراسة والإضاءة والتحكم في الدخول.

ولا ينبغي التعامل مع هذه الآليات باعتبارها ضمانًا لردع الجريمة؛ فالنتائج البحثية تشير إلى أن أثر CCTV يتفاوت بصورة كبيرة بين البيئات.(5)

ثالثًا: حدود الردع

تتمثل أهم حدود الردع في الآتي:(6)

- لا يؤدي تركيب الكاميرات بذاته إلى ضمان منع الجرائم.
- تختلف فاعلية الردع بحسب طبيعة البيئة ونوع الجريمة.
- قد يكون تأثير الكاميرات أكبر عندما تكون جزءًا من تدخل أمني متكامل.
- لا يجوز الخلط بين انخفاض الجريمة وبين إثبات أن الكاميرا وحدها كانت سبب الانخفاض.

رابعًا: الأدلة التجريبية على فاعلية الردع

تُعدّ المراجعات المنهجية من أهم الأدوات لتقييم أثر الردع. وقد خلصت مراجعة Welshو Farringtonلعام ٢٠٠٨، التي شملت ٤٤ تقييمًا، إلى أن الأثر العام لـ CCTVفي خفض الجريمة كان متواضعًا، مع تفاوت كبير بحسب السياق. وكان الأثر أقوى في مواقف السيارات، بينما لم يظهر أثر واضح في جرائم العنف .(7)

أما المراجعة المنهجية والتحليل التلوي الذي أجراه Pizaوزملاؤه عام ٢٠١٩، فقد وجدا انخفاضًا متواضعًا ودالًا في الجريمة، مع أقوى الآثار وأكثرها اتساقًا في مواقف السيارات.(8)

وهذه النتائج تؤكد أن الحكم على فاعلية CCTV ينبغي أن يراعي نوع البيئة وطريقة التطبيق والغرض الأمني، وأن الاعتراف بحدود الردع ليس تقليلًا من قيمته، بل هو شرط أساسي لاستخدامه بصورة فعالة ومسؤولة.

المراجع:

① Brandon C. Welsh and David P. Farrington, "Effects of Closed Circuit Television Surveillance on Crime," *Campbell Systematic Reviews*, Vol. 4 (2008), pp. 1–73.

② IEC, *IEC 62676-4:2025*.

③ Welsh and Farrington, "Effects of Closed Circuit Television Surveillance on Crime," 2008.

④ NIST, *VQiPS: Getting Started*.

⑤ Welsh and Farrington, "Effects of Closed Circuit Television Surveillance on Crime," 2008.

⑥ Welsh and Farrington, "Effects of Closed Circuit Television Surveillance on Crime," 2008.

⑦ Welsh and Farrington, "Effects of Closed Circuit Television Surveillance on Crime," 2008.

⑧ Eric L. Piza, Brandon C. Welsh, David P. Farrington, and Amanda L. Thomas, "CCTV Surveillance for Crime Prevention: A 40-Year Systematic Review with Meta-Analysis," *Criminology & Public Policy*, Vol. 18, No. 1 (2019), pp. 135–159.

المبحث الثالث: اكتشاف الأحداث

يمثل اكتشاف الأحداث أحد المحاور الأساسية للوظيفة الأمنية للمراقبة؛ إذ لا تتحول الصورة إلى قيمة أمنية عملية إلا عندما تكون قابلة للاستخدام في التعرف على حدث ذي أهمية أمنية، وفي الوقت المناسب لاتخاذ الإجراء الملائم.(1)

أولًا: مفهوم الكشف

يمكن تعريف الكشف بأنه :عملية اكتشاف وجود حدث أو نشاط أو سلوك ذي دلالة أمنية، وتحديد وقوعه أو تطوره بما يسمح باتخاذ الإجراء المناسب .(2)

ثانيًا: مستويات الكشف

يمكن التمييز بين ثلاثة مستويات وظيفية للكشف:(3)

1. الكشف العام

إثبات وجود حركة أو نشاط في منطقة معينة.

2. الكشف التفصيلي

تحديد طبيعة النشاط وخصائصه ذات الصلة بالقرار الأمني.

3. الكشف المتقدم

استخلاص خصائص أكثر تحديدًا من المشهد باستخدام جودة تصوير مناسبة أو تحليلات الفيديو، مع عدم افتراض أن النظام يستطيع دائمًا تحديد هوية الشخص على نحو موثوق.(4)

وتختلف متطلبات الصورة تبعًا لمستوى التمييز المطلوب؛ فالتعرف على وجود شخص أو مركبة لا يتطلب بالضرورة المستوى نفسه من جودة الفيديو اللازم لمهمة أكثر دقة. وتتيح أدوات VQiPS ربط متطلبات الفيديو بمستوى التمييز المطلوب وحجم الهدف والحركة والإضاءة والاستخدام الفوري أو اللاحق.(5)

ثالثًا: عوامل نجاح الكشف

يتوقف نجاح الكشف على مجموعة من العوامل، أهمها:(6)

١. جودة الصورة.

٢. مجال الرؤية.

٣. زاوية الكاميرا وموقعها.

٤. الإضاءة.

٥. حركة الهدف والكاميرا.

٦. جودة النقل والتسجيل.

٧. قدرة المشغل.

٨. كفاءة التحليلات الآلية عند استخدامها.

٩. وضوح إجراءات الاستجابة بعد اكتشاف الحدث.

وتشير VQiPS إلى أن جودة الفيديو تتأثر بسلسلة النظام كاملة، من المشهد والكاميرا إلى النقل والعرض، وليس بالكاميرا منفردة.(7)

رابعًا: الكشف اليدوي والكشف الآلي

1. الكشف اليدوي

يعتمد على المراقبة البشرية للمشاهد الحية أو المسجلة. وتتمثل أهم قيوده في اعتماد الأداء على قدرات المشغل، والانتباه، والعبء التشغيلي.(8)

2. الكشف الآلي

يعتمد على وظائف تحليل الفيديو لإنتاج تنبيهات أو مؤشرات للأحداث. ويمكن أن يساعد في مراقبة عدد كبير من مصادر الفيديو، لكنه لا يلغي الحاجة إلى التحقق البشري والإجراءات التشغيلية، كما ينبغي التعامل مع احتمالات الإنذارات الكاذبة أو عدم اكتشاف بعض الأحداث.(9)

المراجع:

المبحث الرابع: دعم الاستجابة الأمنية

لا تكتمل القيمة الأمنية للمراقبة بمجرد اكتشـــاف الحدث؛ إذ تتحدد القيمة العملية بدرجة قدرة المنظومة على توفير معلومات تسـاعد في فهم الموقف واتخاذ القرار وتوجيه الاستجابة. ولذلك تمثل المراقبة مصدرًا للمعلومات ضمن عملية أمنية أوسع، وليست بديلًا عن إجراءات الاستجابة نفسها.(1)

أولًا: مفهوم دعم الاستجابة

يمكن تعريف دعم الاســتجابة بأنه :توفير المعلومات التي تســاعد العاملين والقيادات الأمنية على تقدير الموقف واتخاذ القرار وتوجيه الموارد والإجراءات المناسبة للتعامل مع الحدث .(2)

ثانيًا: المعلومات التي توفرها المراقبة للاستجابة

يمكن أن تسهم المراقبة في توفير معلومات تتعلق بـ:(3)

- موقع الحدث :أين وقع؟
- طبيعة الحدث :ما الذي يحدث؟
- مدى الحدث :ما نطاقه؟
- تطور الحدث :هل يتغير أو يتسع؟
- الأشــخاص أو المركبات المرتبطة بالمشــهد :ما الخصــائص التي يمكن ملاحظتها؟
- مسارات الحركة :ما اتجاهات الحركة ذات الصلة؟

ولا ينبغي افتراض أن الفيديو يستطيع وحده تحديد هوية الأشخاص بصورة قاطعة؛ إذ يتوقف ذلك على جودة التسجيل والظروف والوسائل المستخدمة والمتطلبات القانونية (4).

ثالثًا: تكامل المراقبة مع أنظمة الاستجابة

تزداد قيمة المراقبة عندما تتكامل مع:(5)

١. أنظمة الإنذار.

٢. أنظمة التحكم في الدخول.

٣. أنظمة الاتصال.

٤. أنظمة إدارة الحوادث.

٥. إجراءات الطوارئ.

٦. مركز القيادة والتحكم.

وتؤكد مراجع NIST الخاصة بحماية المنشآت أهمية الجمع بين مراقبة الوصول والتحكم في نقاط الدخول والخروج وحفظ سجلات الوصول، كما تضع المراقبة بالفيديو ضمن أدوات مراقبة الوصول المادي.(6)

المبحث الخامس: مراقبة المداخل والمخارج

تمثل المداخل والمخارج نقاطًا ذات أهمية أمنية خاصة؛ لأنها ترتبط بحركة الأشخاص والمركبات ودخولهم إلى المناطق المحمية وخروجهم منها. ولذلك ينبغي تصميم المراقبة فيها وفق الهدف الأمني المطلوب، وبالتكامل مع وسائل التحكم في الدخول والخروج.(1)

أولًا: أهمية مراقبة المداخل والمخارج

تتمثل أهمية مراقبة المداخل والمخارج في:(2)

- دعم مراقبة الدخول والخروج.
- اكتشاف محاولات الدخول غير المصرح به.
- توثيق الأحداث المرتبطة بالدخول والخروج.
- دعم مراجعة سجلات الوصول.
- توفير معلومات مساندة للتحقيقات.

وتؤكد متطلبات NIST المتعلقة بالحماية المادية أهمية التحكم في نقاط الدخول والخروج، والتحقق من صلاحيات الوصول، وحفظ سجلات نقاط الدخول والخروج، ومراقبة الوصول المادي.(3)

ثانيًا: متطلبات مراقبة المداخل

تختلف المتطلبات باختلاف طبيعة المنشأة ومخاطرها، إلا أنها قد تشمل:(4)

- وضع الكاميرا في موضع يحقق الغرض الأمني المطلوب.
- توفير جودة صورة مناسبة للهدف.
- ضمان إضاءة كافية.
- مراعاة اتجاه الحركة وزاوية التصوير.
- تكامل المراقبة مع نظام التحكم في الدخول عند الحاجة.
- توفير تسجيل يمكن الرجوع إليه.

ولا يصـــح افتراض أن وجود «كاميرا لتوثيق الوجه» يكفي وحده لتحقيق التعرف؛ بل ينبغي تحديد مستوى التمييز المطلوب ثم تصميم النظام وفقه.(5)

ثالثًا: متطلبات مراقبة المخارج

تشمل مراقبة المخارج، بحسب طبيعة المنشأة:(6)

- توثيق حركة الخروج.
- مراقبة محاولات الخروج غير المصرح به.
- الربط مع سجلات التحكم في الدخول والخروج.
- توفير التسجيلات اللازمة للمراجعة والتحقيق.

المبحث السادس: حماية المناطق الحساسة

تحتاج بعض المناطق داخل المنشـأة إلى مسـتويات أعلى من الحماية بسـبب قيمة الأصول الموجودة فيها أو حساسية العمليات التي تتم داخلها. ومن ثم ينبغي أن يعتمد مسـتوى المراقبة على تقييم المخاطر، وليس على قاعدة موحدة تنطبق على جميع المناطق.(1)

أولًا: مفهوم المناطق الحساسة

يمكن تعريف المناطق الحسـاسـة بأنها :المناطق التي تتطلب مسـتوى مرتفعًا من الحماية بسبب قيمة الأصول الموجودة فيها، أو حساسية العمليات التي تتم فيها، أو طبيعة المعلومات أو المعدات المرتبطة بها، أو المتطلبات التنظيمية المطبقة عليها (2).

ثانيًا: أمثلة المناطق الحساسة

قد تشمل:(3)

- غرف الخوادم ومراكز البيانات.
- غرف التحكم.
- المختبرات.
- مناطق حفظ الأصول مرتفعة القيمة.
- المناطق التي تحتوي على معدات حرجة.
- مناطق تخزين المواد أو المعدات التي تستوجب ضوابط خاصة.

وتشير مراجع NIST الخاصة بأمن التكنولوجيا التشغيلية إلى أهمية التحكم في الوصول المادي للمناطق التي تحتوي على مكونات أو أنظمة حسـاسـة، كما تشـير إلى أهمية أنظمة التحكم في الدخول والمراقبة ضمن البنية الأمنية للمنشآت.(4)

ثالثًا: متطلبات حماية المناطق الحساسة

يمكن أن تشمل متطلبات الحماية:(5)

- تغطية مناسبة للمناطق ذات المخاطر المرتفعة.
- جودة صورة تتناسب مع المهمة الأمنية.
- تسجيل مناسب.
- تكامل مع التحكم في الدخول.
- التكامل مع الإنذارات عند الحاجة.
- حماية مادية للكاميرات والمكونات.
- تقييد صلاحيات الوصول إلى التسجيلات.

وينبغي تجنب عبارة «التغطية الكاملة» بوصفها قاعدة مطلقة؛ إذ قد تكون التغطية المطلوبة هي التغطية التي تحقق الوظيفة الأمنية المحددة بعد تحليل المخاطر.(6)

المراجع:

المبحث السابع: توثيق الوقائع

يمثل توثيق الوقائع وظيفة أساسية لأن التسجيل المرئي يمكن أن يوفر سجلًا يمكن الرجوع إليه بعد وقوع الحدث. غير أن القيمة الأمنية والقانونية للتسجيل تعتمد على سلامة جمعه وحفظه واسترجاعه وإدارته. وتؤكد أدلة وزارة العدل الأمريكية أهمية تأمين وتوثيق وتخزين والمحافظة على بيانات الفيديو بما يحافظ على قيمتها الإثباتية.(1)

أولًا: مفهوم توثيق الوقائع

يمكن تعريف توثيق الوقائع بأنه :عملية تسجيل وحفظ الأحداث المرئية بطريقة تسمح بالرجوع إليها لاحقًا لأغراض المراجعة والتحليل والتحقيق، مع المحافظة على سلامة التسجيل وإمكان التحقق من مصدره وظروف التعامل معه .(2)

ثانيًا: متطلبات التوثيق

تشمل متطلبات التوثيق:(3)

١. جودة صورة مناسبة للغرض المطلوب.
٢. تسجيل وفق سياسة تشغيل واضحة.
٣. مدة احتفاظ محددة وفق الحاجة والمتطلبات النظامية.
٤. ضبط الوصول إلى التسجيلات.
٥. سهولة البحث والاسترجاع.
٦. المحافظة على المعلومات الوصفية المرتبطة بالتسجيل.

وتشير NISTIR 8161 Rev.1إلى أهمية البيانات الوصفية في دعم التعامل مع التسجيلات وتحقيق قابلية التبادل، كما يركز على متطلبات تصدير الفيديو الرقمي وتبادل التسجيلات.(4)

ثالثًا: سلامة التوثيق

تتطلب سلامة التسجيلات:(5)

١. الحد من التعديل غير المصرح به.
٢. توثيق مصدر التسجيل.
٣. توثيق التوقيت المرتبط بالتسجيل.
٤. ضبط عمليات التصدير والنقل.
٥. تحديد صلاحيات الوصول.
٦. توثيق التعامل مع التسجيل عندما يستخدم لأغراض تحقيقية أو إثباتية.

وتشير إرشادات وزارة العدل الأمريكية إلى أهمية تأمين التسجيلات وفهرستها وتخزينها والمحافظة عليها عند التعامل معها كأدلة فيديو.(6)

المبحث الثامن: دعم الاستدلال والتحقيق

تمثل التسجيلات المرئية مصدرًا مهمًا للمعلومات بعد وقوع الحدث، إذ يمكن استخدامها في إعادة بناء التسلسل الزمني والمكاني للأحداث، وربط المشاهد المختلفة، واستخلاص المعلومات ذات الصلة بالتحقيق. إلا أن القيمة الإثباتية للفيديو تتوقف على طريقة الحصول عليه وحفظه وتداوله وإدارته.(1)

أولًا: مفهوم دعم الاستدلال والتحقيق

يمكن تعريف دعم الاستدلال والتحقيق بأنه :استخدام المعلومات المرئية المستخرجة من التسجيلات في تحليل الوقائع وإعادة بناء تسلسل الأحداث وتحديد المعلومات ذات الصلة بالتحقيق، وفق الإجراءات النظامية والقانونية المعمول بها .(2)

ثانيًا: المعلومات التي توفرها المراقبة للتحقيق

يمكن أن توفر التسجيلات:(3)

- التسلسل الزمني للأحداث.
- مواقع وقوع الأحداث.
- مسارات الحركة.
- خصائص الأشخاص أو المركبات الظاهرة في التسجيل.
- العلاقة الزمنية بين الأحداث.
- المعلومات البصرية ذات الصلة بالواقعة.

ولا ينبغي الجزم بأن التسجيل يحدد «هوية» الشخص دائمًا؛ فالقدرة على تحديد الهوية تتوقف على جودة الصورة والظروف وطبيعة المهمة والأساليب المستخدمة.(4)

ثالثًا: متطلبات دعم التحقيق

تشمل المتطلبات:(5)

- جودة صورة مناسبة.

- سلامة التسجيل.
- توثيق المصدر.
- توثيق الزمن.
- ضبط الوصول.
- تصدير التسجيل بطريقة منظمة.
- المحافظة على المعلومات الوصفية.
- توثيق عمليات التعامل مع التسجيل.

وقد صممت NISTIR 8161 Rev.1لتحديد متطلبات أساسية للتوافق في تصدير وتبادل تسجيلات CCTV الرقمية، بما في ذلك عناصر مرتبطة بالتسجيل والبيانات الوصفية.(6)

رابعًا: سلامة الأدلة الرقمية

عندما تستخدم التسجيلات في سياق إثباتي، ينبغي الاهتمام بـ:(7)

- مصدر التسجيل.
- طريقة الحصول عليه.
- وقت الحصول عليه.
- سلامة الملف.
- طريقة نقله وتخزينه.
- الأشخاص الذين تعاملوا معه.
- أي معالجة أو تحويل أجري عليه.

وتؤكد الأدلة الصادرة عن وزارة العدل الأمريكية أهمية الإجراءات المنظمة لتأمين وجمع وتخزين وتحليل فيديو الأدلة، كما تتناول الأدلة الخاصة بالادعاء نقل وتخزين وتنقيح والإفصاح عن الفيديو عند استخدامه في السياق القضائي.(8)

المراجع:

المبحث التاسع: إدارة الأزمات والطوارئ

يمكن أن تؤدي المراقبة دورًا مساندًا في إدارة الأزمات والطوارئ من خلال توفير صورة بصرية عن حالة الموقع، ومتابعة تطور الحدث، وتوفير معلومات تساعد في اتخاذ القرار. غير أن دورها يظل جزءًا من منظومة إدارة الطوارئ، ولا يحل محل خطط الطوارئ ووسائل الاتصال وفرق الاستجابة.(1)

أولًا: مفهوم إدارة الأزمات والطوارئ

يمكن تعريف إدارة الأزمات والطوارئ بأنها: مجموعة العمليات والإجراءات التي تهدف إلى الاستعداد للأحداث الطارئة والاستجابة لها والحد من آثارها ودعم استعادة النشاط بعد وقوعها .(2)

ثانيًا: دور المراقبة في إدارة الأزمات

يمكن أن تسهم المراقبة في:(3)

- التقييم: توفير معلومات بصرية عن الموقف.
- المتابعة: مراقبة تطور الحدث.
- التوجيه: توفير معلومات مساندة لاتخاذ القرار.
- التوثيق: تسجيل الأحداث والتطورات.
- دعم التعافي: توفير معلومات لاحقة لمراجعة ما حدث.

ثالثًا: استخدامات المراقبة في الطوارئ

يمكن استخدام المراقبة في التعامل مع:(4)

- الحرائق.
- الاقتحامات.
- الحوادث الكبرى.
- التجمعات والحشود.

- بعض الكوارث أو الأحداث الطبيعية.
- الأحداث التي تتطلب متابعة بصرية مستمرة.

وينبغي ألا يفهم ذلك على أن كاميرات المراقبة تحل محل أنظمة كشـــف الحريق أو أنظمة الإنذار المتخصصة؛ بل تؤدي وظيفة معلوماتية مساندة ضمن المنظومة.

رابعًا: متطلبات إدارة الأزمات

تزداد فاعلية المراقبة أثناء الأزمات عندما تتوافر:(5)

- تغطية متناسبة مع المخاطر.
- وسائل اتصال فعالة.
- مركز أو نقطة قيادة مناسبة.
- إجراءات تشغيلية للطوارئ.
- تكامل مع أنظمة الإنذار.
- تدريب للعاملين.
- وسائل بديلة عند تعطل النظام.

وتؤكد إرشـــادات NIST في مجال التكنولوجيا التشـــغيلية أهمية مراعاة الاعتمادية والسلامة والاستمرارية عند تصميم الأنظمة التي تتفاعل مع البيئة المادية.(6)

المراجع:

المبحث العاشر: حدود الاعتماد على كاميرات المراقبة

على الرغم من الأهمية الأمنية لكاميرات المراقبة، فإنها لا تمثل حلًا شـــاملًا لجميع المخاطر. ولذلك فإن الاســتخدام الفعال لها يتطلب تحديد قدراتها وحدودها، وربطها بالعنصر البشري والإجراءات التنظيمية ووسائل الحماية الأخرى.(1)

أولًا: الحدود التقنية

تشمل الحدود التقنية:(2)

- محدودية مجال الرؤية.
- تأثر الصورة بالإضاءة.
- المسافة.
- الحركة.
- العوامل البيئية.
- جودة النقل والتسجيل.
- محدودية بعض وظائف التحليل الآلي.

وتوضح VQiPS أن جودة الفيديو ينبغي النظر إليها من خلال المهمة التي يراد تنفيذها، وأن عوامل مثل حجم الهدف والحركة والإضاءة وطريقة الاستخدام تؤثر في المتطلبات اللازمة.(3)

ثانيًا: الحدود البشرية

يرتبط أداء المراقبة البشرية بعوامل منها:(4)

- الانتباه.
- الإدراك.
- الخبرة.
- القدرة على تفسير المشهد.
- العبء التشغيلي.

- الإرهاق.
- سرعة اتخاذ القرار.

ومن ثم لا ينبغي افتراض أن زيادة عدد الكاميرات تؤدي بالضـــرورة إلى زيادة مماثلة في القدرة على المراقبة البشرية.

ثالثًا: الحدود التنظيمية

تشمل الحدود التنظيمية:(5)

- القوانين واللوائح ذات الصلة.
- حماية الخصوصية.
- سياسات الاحتفاظ بالتسجيلات.
- صلاحيات الوصول.
- الموارد المالية والبشرية.
- التدريب.
- سياسات التشغيل والاستجابة.

وتشـير مراجع NIST إلى أن مراقبة الوصـول المادي والمراقبة بالفيديو ينبغي أن تخضـع لضوابط تنظيمية وصلاحيات محددة، وأن إدارة المعلومات الأمنية يجب أن تكون جزءًا من نظام حماية أوسع.(6)

رابعًا: مخاطر الاعتماد المفرط

يمكن أن يؤدي الاعتماد المفرط على التقنية إلى:(7)

- الاعتقاد الخاطئ بأن وجود الكاميرات يساوي وجود حماية كاملة.
- إهمال العنصر البشري.
- إهمال إجراءات الاستجابة.
- زيادة التعقيد دون تحقيق فائدة أمنية متناسبة.
- خلق اعتماد تشغيلي على أنظمة أو مكونات تقنية محددة.

وتؤكد الدراسات الخاصة بفاعلية CCTV أن النتائج ليست موحدة بين البيئات، كما أن الأدلة تشير إلى أن أثر الكاميرات يكون أقوى في بعض السياقات وأضعف في أخرى (8).

خامسًا: المراقبة كجزء من منظومة متعددة الطبقات

ينبغي أن تعمل المراقبة ضمن منظومة أمنية متعددة الطبقات تشمل، بحسب طبيعة المنشأة: (9)

- الحماية المادية.
- التحكم في الدخول.
- أنظمة الإنذار.
- الحراسة.
- إجراءات التشغيل.
- إدارة الحوادث والطوارئ.
- التدريب.
- السياسات التنظيمية.

ويؤكد المختصون في إرشاداتهم المتعلقة بالتكنولوجيا التشغيلية أن الأمن ينبغي أن يعالج المخاطر من خلال مجموعة من الضوابط والإجراءات، وليس من خلال تقنية منفردة. (10)

خلاصة الفصل الثامن

يتضح من دراسة كاميرات المراقبة وتعزيز أمن المنشآت أن الوظيفة الأمنية للمراقبة تتجاوز مجرد التصوير والتسجيل، لتشمل الوقاية والردع والكشف ودعم الاستجابة والتوثيق ودعم التحقيق، فضلًا عن دورها المساند في إدارة الأزمات والطوارئ.

وقد أظهر التحليل أن الوقاية والردع يمثلان أحد أوجه الاستفادة الأمنية من المراقبة، إلا أن أثرهما ليس مطلقًا ولا مضمونًا، وإنما يتفاوت باختلاف السياق وطبيعة الجريمة وطريقة تصميم المنظومة وتشغيلها. وتؤكد المراجعات المنهجية أن أثر CCTV في خفض الجريمة يمكن أن يكون متواضعًا ولكنه ذو دلالة في بعض البيئات، مع تفاوت واضح بين المواقع وأنواع الجرائم.(1)

كما تبين أن الكشف يمثل حلقة مركزية في الوظيفة الأمنية، وأن فاعليته ترتبط بجودة الفيديو ومجال الرؤية والإضاءة وموقع الكاميرا وقدرات المشغل والتحليلات الآلية، إضافة إلى الإجراءات التي تلي عملية الكشف.

وأظهر الفصل كذلك أهمية مراقبة المداخل والمخارج وحماية المناطق الحساسة، مع التأكيد على أن المراقبة لا ينبغي أن تعمل منفردة، وإنما بالتكامل مع التحكم في الدخول والإنذار والحماية المادية والإجراءات التشغيلية.

كما تبين أن التسجيلات تمثل مصدرًا مهمًا لتوثيق الوقائع ودعم التحقيق، إلا أن قيمتها لا تعتمد على وجودها فحسب، وإنما على جودة التسجيل وسلامته وإمكان استرجاعه، وعلى سلامة إجراءات الحصول عليه وحفظه وتصديره والتعامل معه عندما يستخدم في سياق إثباتي.(2)

وفي مجال الأزمات والطوارئ، يمكن للمراقبة أن توفر معلومات مهمة عن تطور الحدث وتساعد في دعم القرار والتوثيق، إلا أنها لا تحل محل أنظمة الإنذار والطوارئ وفرق الاستجابة.

وأخيرًا، أكد التحليل أن كاميرات المراقبة ليست حلًا شاملًا للمشكلات الأمنية، وأن لها حدودًا تقنية وبشرية وتنظيمية. ولذلك ينبغي إدماجها ضمن منظومة أمنية متعددة الطبقات، تقوم على تقييم المخاطر وتحديد الأهداف والموارد والإجراءات المناسبة.

ومن ثم يمكن صياغة النموذج المتكامل للوظيفة الأمنية للمراقبة على النحو الآتي:

الهدف الأمني ← الوقاية والردع ← الكشف ← دعم الاستجابة ← التوثيق ← دعم التحقيق ← دعم إدارة الأزمات

وعليه، فإن نجاح منظومة المراقبة في تعزيز أمن المنشآت لا يقاس بالسؤال: كم كاميرا لدى المنشأة؟ وإنما بالسؤال الأكثر دقة: إلى أي مدى تسهم منظومة المراقبة في تحقيق الأهداف الأمنية المحددة للمنشأة بكفاءة وفاعلية، ضمن منظومة حماية متكاملة؟

أهم نتائج الفصل الثامن

١. الوظيفة الأمنية للمراقبة تتعدد بحسب أهداف المنشأة وطبيعة المخاطر.
٢. تشمل الوظائف الأساسية الوقاية والردع والكشف ودعم الاستجابة والتوثيق ودعم التحقيق.
٣. يجب التمييز بين الوظيفة التقنية للكاميرا والوظيفة الأمنية للمنظومة.
٤. لا تمثل جودة الصورة وحدها معيارًا كافيًا للحكم على الفاعلية الأمنية.
٥. يمكن للمراقبة أن تسهم في الوقاية والردع، لكن أثر الردع ليس مضمونًا.
٦. تختلف فاعلية CCTV باختلاف السياق ونوع الجريمة وطريقة التطبيق.
٧. يمثل الكشف حلقة مركزية في الوظيفة الأمنية للمراقبة.
٨. تتأثر فاعلية الكشف بجودة الصورة والإضاءة ومجال الرؤية والموقع والتشغيل.
٩. يسهم التحليل الآلي في دعم الكشف، مع بقاء الحاجة إلى التحقق والاستجابة.
١٠. تساعد المراقبة في توفير معلومات مساندة للاستجابة الأمنية.
١١. تزداد قيمة المراقبة عندما تتكامل مع الإنذار والتحكم في الدخول والاتصال وإدارة الحوادث.
١٢. تمثل المداخل والمخارج نقاطًا ذات أهمية أمنية خاصة.
١٣. ينبغي تحديد متطلبات مراقبة المداخل والمخارج وفق الغرض الأمني المطلوب.
١٤. تحتاج المناطق الحساسة إلى مستوى من الحماية يتناسب مع المخاطر وقيمة الأصول وحساسية العمليات.
١٥. يمثل توثيق الوقائع وظيفة أساسية للمراقبة.

١٦. تتطلب قيمة التسجيلات جودة مناسبة وإدارة منظمة وسلامة في الحفظ والاسترجاع.
١٧. تسهم التسجيلات في إعادة بناء الأحداث ودعم التحقيق.
١٨. لا يعني وجود التسجيل إمكانية تحديد هوية الأشخاص بصورة قاطعة في جميع الحالات.
١٩. تتطلب التسجيلات المستخدمة في السياق الإثباتي إجراءات منظمة للحفظ والتصدير والتعامل.
٢٠. يمكن للمراقبة أن تدعم إدارة الأزمات والطوارئ من خلال توفير المعلومات البصرية.
٢١. لا تحل كاميرات المراقبة محل أنظمة الطوارئ المتخصصة أو فرق الاستجابة.
٢٢. للمراقبة حدود تقنية وبشرية وتنظيمية.
٢٣. لا تؤدي زيادة عدد الكاميرات بالضرورة إلى زيادة مماثلة في مستوى الحماية.
٢٤. قد يؤدي الاعتماد المفرط على التقنية إلى إضعاف بقية عناصر المنظومة الأمنية.
٢٥. ينبغي إدماج المراقبة ضمن منظومة أمنية متعددة الطبقات.
٢٦. يمثل تقييم الأهداف والمخاطر وحالات الاستخدام أساسًا لتحديد قيمة منظومة المراقبة.

أسئلة التفكير والتقييم للفصل الثامن

أولًا: أسئلة معرفية

١. ما المقصود بالوظيفة الأمنية للمراقبة؟
٢. ما الوظائف الأمنية الأساسية لمنظومة المراقبة؟
٣. ما الفرق بين الوظيفة التقنية والوظيفة الأمنية؟
٤. ما المقصود بالوقاية والردع في مجال المراقبة؟
٥. ما أهم العوامل التي تؤثر في فاعلية الردع؟
٦. ما المقصود بالكشف؟
٧. ما العوامل المؤثرة في نجاح الكشف؟
٨. ما الفرق بين الكشف اليدوي والكشف الآلي؟

٩. ما المعلومات التي يمكن أن توفرها المراقبة لدعم الاستجابة؟
١٠. لماذا تعد مراقبة المداخل والمخارج مهمة؟
١١. ما أهم متطلبات مراقبة المداخل والمخارج؟
١٢. ما المقصود بالمناطق الحساسة؟
١٣. ما أمثلة المناطق الحساسة في المنشآت؟
١٤. ما متطلبات حماية المناطق الحساسة؟
١٥. ما المقصود بتوثيق الوقائع؟
١٦. ما أهم متطلبات توثيق التسجيلات؟
١٧. ما المقصود بدعم الاستدلال والتحقيق؟
١٨. ما المعلومات التي يمكن أن توفرها التسجيلات للتحقيق؟
١٩. ما دور المراقبة في إدارة الأزمات والطوارئ؟
٢٠. ما أهم الحدود التقنية والبشرية والتنظيمية للمراقبة؟

ثانيًا: أسئلة تحليلية

١. حلل العلاقة بين الوظيفة التقنية والوظيفة الأمنية للمراقبة.
٢. لماذا لا تكفي جودة الصورة وحدها لتحقيق الفاعلية الأمنية؟
٣. لماذا لا يعمل الردع الناتج عن المراقبة بصورة مضمونة؟
٤. حلل العلاقة بين الكشف والاستجابة الأمنية.
٥. كيف يؤثر موقع الكاميرا وجودة الإضاءة في قدرتها على أداء الوظيفة الأمنية؟
٦. كيف يمكن أن يسهم تكامل المراقبة مع التحكم في الدخول في تعزيز أمن المنشأة؟
٧. لماذا تحتاج المناطق الحساسة إلى مستوى حماية يتناسب مع درجة المخاطر؟
٨. حلل العلاقة بين التوثيق والتحقيق.
٩. لماذا تعد سلامة التسجيلات مهمة عند استخدامها في التحقيق؟
١٠. كيف يمكن للمراقبة أن تدعم إدارة الأزمات دون أن تحل محل أنظمة الطوارئ؟
١١. حلل مخاطر الاعتماد المفرط على كاميرات المراقبة.
١٢. لماذا ينبغي النظر إلى المراقبة باعتبارها جزءًا من منظومة أمنية متعددة الطبقات؟

١٣. كيف يمكن قياس الفاعلية الأمنية لمنظومة المراقبة بعيدًا عن عدد الكاميرات؟

١٤. ناقش العلاقة بين جودة الفيديو وحالة الاستخدام الأمنية.

ثالثًا: أسئلة تطبيقية

١. اختر منشأة تعرفها، وحلل الوظائف الأمنية التي تؤديها منظومة المراقبة فيها.

٢. ضع استراتيجية لتعزيز الوقاية والردع في منشأة حيوية.

٣. ضع خطة لتحسين قدرة الكشف في منشأة ذات مستوى أمني مرتفع.

٤. صمم تصورًا لمراقبة مدخل منشأة حيوية، مع تحديد الهدف الأمني من كل عنصر.

٥. حدد المناطق الحساسة في منشأة افتراضية، ورتبها وفق درجة الأولوية الأمنية.

٦. صمم تصورًا لحماية منطقة حساسة من خلال التكامل بين المراقبة والتحكم في الدخول والإنذار.

٧. صمم إجراءً لتوثيق واقعة أمنية من لحظة اكتشافها حتى حفظ التسجيل.

٨. صمم إجراءً منظمًا لتصدير تسجيل فيديو ذي قيمة تحقيقية.

٩. ضع تصورًا لاستخدام المراقبة في دعم الاستجابة لحادث أمني.

١٠. صمم خطة لإدارة أزمة مدعومة بالمراقبة والإنذار والاتصال.

١١. ضع استراتيجية لاستخدام المراقبة ضمن منظومة أمنية متعددة الطبقات.

١٢. اقترح مؤشرات لقياس الفاعلية الأمنية لمنظومة المراقبة في منشأة محددة.

١٣. قارن بين منظومتين للمراقبة تختلفان في عدد الكاميرات، وحدد أيهما أكثر فاعلية وفق أهداف أمنية محددة، مع بيان أسبابك.

الباب الثالث:
التشغيل والوظيفة الأمنية

الفصل الثالث: التكامل بين كاميرات المراقبة والمنظومات الأمنية

تمهيد الفصل

لم تعد كاميرات المراقبة الحديثة تعمل بوصفها منظومات مستقلة تقتصر وظيفتها على التقاط الصور وتسجيلها، وإنما أصبحت جزءًا من بيئة أمنية مترابطة تتفاعل فيها أنظمة المراقبة المرئية مع أنظمة التحكم في الدخول، وأنظمة الإنذار، وأنظمة الاتصال، ومراكز القيادة والتحكم، وأنظمة الأمن والسلامة. ويعكس هذا التطور انتقالًا من مفهوم المراقبة المنفردة إلى مفهوم التكامل الأمني الذي يهدف إلى توحيد المعلومات وتحسين القدرة على اكتشاف الأحداث وتقييمها والاستجابة لها[1].

ويكتسب التكامل بين كاميرات المراقبة والمنظومات الأمنية أهمية خاصة في المنشآت التي تتعدد فيها مصادر المخاطر وتتطلب استجابة منسقة وسريعة. فالقيمة الأمنية للكاميرا لا تتحقق بمجرد قدرتها على إنتاج صورة، وإنما تزداد عندما يمكن استخدام المعلومات المرئية الناتجة عنها مع معلومات أخرى صادرة عن أنظمة أمنية مختلفة، بما يساعد على تكوين صورة أكثر شمولًا عن الحالة الأمنية[2].

ويتيح التكامل، على سبيل المثال، ربط حدث صادر عن نظام التحكم في الدخول بالمعلومات المرئية التي توفرها الكاميرات، أو توجيه انتباه المشغل إلى منطقة معينة عند صدور إنذار، أو عرض معلومات متعددة في مركز قيادة وتحكم واحد. ومن ثم، فإن التكامل لا يعني مجرد توصيل الأجهزة ببعضها، وإنما يعني تنظيم تبادل المعلومات والأحداث بين مكونات المنظومة الأمنية بما يخدم أهدافًا أمنية محددة[3].

ولا يخلو التكامل من تحديات؛ إذ يتطلب نجاحه توافقًا تقنيًا، وتصميمًا مناسبًا للمنظومة، وإجراءات تشغيل واضحة، وتحديدًا للمسؤوليات والصلاحيات، وتدريبًا للمستخدمين، فضلًا عن مراعاة الأمن السيبراني وحماية المعلومات والخصوصية. ولذلك فإن التكامل ينبغي أن ينظر إليه باعتباره مشروعًا أمنيًا وتشغيليًا متكاملًا، وليس مجرد مشروع تقني[4].

ويتناول هذا الفصل سبعة مباحث مترابطة تبدأ بتحديد مفهوم التكامل الأمني، ثم تبحث في الربط بين كاميرات المراقبة وأنظمة التحكم بالدخول والإنذار، وتنتقل إلى

دور مراكز القيادة والتحكم والتكامل مع أنظمة الأمن والسلامة، ثم تناقش إدارة الأحداث المتكاملة ومتطلبات نجاح التكامل.

المبحث الأول: مفهوم التكامل الأمني

يمثل التكامل الأمني الأساس الذي تقوم عليه العلاقة بين كاميرات المراقبة وبقية المنظومات الأمنية. ويهدف هذا التكامل إلى تجاوز حالة عمل الأنظمة بصورة منفصلة، والانتقال إلى بيئة تستطيع فيها الأنظمة تبادل المعلومات والأحداث بما يساعد العاملين على فهم الحالة الأمنية واتخاذ الإجراءات المناسبة.

أولًا: مفهوم التكامل الأمني

يمكن تعريف التكامل الأمني بأنه:

تنظيم وتنسيق التفاعل وتبادل المعلومات بين منظومات وتقنيات أمنية متعددة، بما يتيح استخدامها بصورة مترابطة لتحقيق أهداف أمنية وتشغيلية مشتركة[5].

ولا يعني التكامل بالضرورة دمج جميع الأنظمة في نظام تقني واحد، فقد يتحقق التكامل من خلال تبادل الأحداث والبيانات بين أنظمة مستقلة، أو من خلال منصة موحدة تعرض المعلومات الصادرة عن أنظمة متعددة.

وعليه، ينبغي التمييز بين التكامل والدمج؛ فالدمج قد يشير إلى توحيد مكونات أو وظائف متعددة في بيئة واحدة، بينما يشير التكامل بصورة أوسع إلى قدرة الأنظمة المختلفة على التفاعل وتبادل المعلومات وتنفيذ وظائف مترابطة[6].

ثانيًا: أهداف التكامل الأمني

يمكن أن يحقق التكامل بين كاميرات المراقبة والمنظومات الأمنية عددًا من الأهداف، من أهمها:

١. تحسين الوعي بالموقف الأمني من خلال جمع المعلومات الصادرة عن مصادر متعددة.
٢. تسريع اكتشاف الأحداث من خلال الربط بين الإنذارات والمعلومات المرئية.
٣. تحسين سرعة الاستجابة عبر توجيه المشغلين والموارد إلى موقع الحدث.
٤. تقليل الوقت اللازم للتحقق من الإنذارات من خلال استخدام الصورة المرئية للتحقق من الحالة.

٥. تحسين توثيق الأحداث من خلال ربط التسجيلات المرئية ببيانات الأنظمة الأخرى.

٦. دعم التحقيق اللاحق من خلال إتاحة معلومات مترابطة عن الحدث[7].

ثالثًا: مستويات التكامل

يمكن النظر إلى التكامل الأمني على عدة مستويات:

1. التكامل المعلوماتي

ويتمثل في تبادل المعلومات بين الأنظمة، مثل تبادل بيانات الدخول والخروج أو بيانات الإنذارات مع نظام المراقبة.

2. التكامل التشغيلي

ويتحقق عندما تؤدي المعلومات الصادرة عن أحد الأنظمة إلى إجراء تشغيلي في نظام آخر؛ فعلى سبيل المثال، يمكن أن يؤدي إنذار محدد إلى استدعاء عرض كاميرا مرتبطة بالمنطقة محل الحدث.

3. التكامل الإداري

ويتمثل في توحيد إجراءات التشغيل والمتابعة والتعامل مع الأحداث، بحيث لا تعمل كل منظومة وفق إجراءات منفصلة تمامًا.

4. التكامل على مستوى مركز القيادة

وهو المستوى الذي يتم فيه عرض المعلومات الصادرة عن أنظمة متعددة ضمن بيئة تشغيل واحدة، بما يدعم اتخاذ القرار وإدارة الأحداث[8].

رابعًا: أهمية التكامل الأمني

تظهر أهمية التكامل بصورة خاصة عندما تكون طبيعة الحدث الأمني متعددة الأبعاد. فالإنذار الصادر عن نظام تحكم في الدخول، على سبيل المثال، قد لا يكون كافيًا وحده لتحديد ما إذا كان هناك تهديد فعلي. وعند ربطه بالمعلومات المرئية يمكن للمشغل التحقق من طبيعة الحدث وتحديد الإجراء المناسب.

وبذلك يتحول التكامل من مجرد وسيلة لربط الأجهزة إلى وسيلة لتحويل البيانات المتفرقة إلى معلومات قابلة للاستخدام الأمني.

المبحث الثاني: الربط مع أنظمة التحكم بالدخول

تمثل أنظمة التحكم بالدخول أحد أهم الأنظمة التي يمكن ربطها بكاميرات المراقبة، لأن كلا النظامين يتعامل مع حركة الأشخاص والمركبات داخل المنشأة. ويتيح الربط بينهما الانتقال من مجرد تسجيلي يقصد بأنظمة التحكم بالدخول المنظومات التي تستخدم لتنظيم أو تقييد دخول الأشخاص أو المركبات إلى مناطق الدخول والخروج إلى إمكانية التحقق المرئي من الأحداث المرتبطة بالدخول[9].

أولًا: مفهوم أنظمة التحكم بالدخول

يقصد بأنظمة التحكم بالدخول المنظومات التي تستخدم لتنظيم أو تقييد دخول الأشخاص أو المركبات إلى مناطق أو موارد محددة وفق قواعد وصلاحيات مسبقة[10]. وتشمل هذه الأنظمة، بحسب طبيعة المنشأة، وسائل متعددة للتعرف والتحقق، مثل البطاقات، والرموز، والوسائل البيومترية، وغيرها من وسائل المصادقة.

ثانيًا: أهمية الربط بين التحكم بالدخول والمراقبة

يساعد الربط بين النظامين على تعزيز القدرة على:

- التحقق المرئي من عمليات الدخول.
- متابعة محاولات الدخول غير المصرح بها.
- ربط بيانات الدخول بالتسجيلات المرئية.
- دعم التحقيق في حالات إساءة استخدام الصلاحيات.
- تحسين متابعة المناطق المقيدة[11].

وتتضح أهمية هذا الربط عندما يحدث تعارض بين البيانات النظامية والمشهد الفعلي؛ فقد يسجل نظام التحكم استخدام بطاقة صحيحة، بينما تظهر الكاميرا سلوكًا غير متوافق مع الاستخدام المتوقع. وفي هذه الحالة توفر العلاقة بين النظامين مصدرًا إضافيًا للمعلومات يساعد على تقييم الحدث.

ثالثًا: آليات الربط

يمكن أن يتم الربط بعدة صور، منها:

1. الربط الزمني

ربط سجل الدخول أو الخروج بالتسجيل المرئي في الوقت نفسه.

2. الربط المكاني

ربط نقطة تحكم معينة بكاميرا أو مجموعة كاميرات تغطي المنطقة نفسها.

3. الربط القائم على الحدث

عند حدوث حدث معين في نظام التحكم بالدخول، يتم اســـتدعاء المعلومات المرئية المرتبطة به.

4. الربط مع إدارة الأحداث

إدراج بيانات الدخول والتسجيلات المرئية ضمن سجل موحد للحدث الأمني[12].

رابعًا: حالات الاستخدام الأمني

يمكن استخدام التكامل في حالات متعددة، مثل:

- محاولات الدخول المرفوضة.
- استخدام بطاقة خارج أوقات الصلاحية.
- الدخول إلى منطقة مقيدة.
- فتح باب في ظروف غير اعتيادية.
- متابعة عمليات الدخول والخروج أثناء الحوادث.
- التحقيق في الأحداث التي تتطلب تحديد تسلسل الحركة[13].

خامسًا: متطلبات نجاح الربط

يتطلب الربط الفعال:

- ضبطًا دقيقًا للوقت في الأنظمة.
- تحديد العلاقة بين نقاط التحكم والكاميرات.
- إجراءات واضحة للتعامل مع الأحداث.
- صلاحيات وصول مناسبة.
- حماية البيانات من الاستخدام غير المصرح به.
- اختبار التكامل بصورة دورية.

المبحث الثالث: الربط مع أنظمة الإنذار

تعد أنظمة الإنذار مصدرًا أساسيًا للأحداث الأمنية التي تتطلب التحقق والاستجابة. ويتيح ربطها بكاميرات المراقبة استخدام المعلومات المرئية للتحقق من طبيعة الإنذار وتقييم الموقف قبل اتخاذ الإجراء المناسب[14].

أولًا: مفهوم أنظمة الإنذار

تشمل أنظمة الإنذار المنظومات التي تهدف إلى اكتشاف حالات أو ظروف محددة وإصدار تنبيه عنها، مثل محاولات الاقتحام أو فتح الأبواب أو بعض الحالات البيئية أو التشغيلية، بحسب طبيعة النظام والمنشأة[15].

ثانيًا: أهمية الربط بين الإنذار والمراقبة

تكمن أهمية الربط في أن الإنذار قد يشير إلى وجود حالة تستوجب الانتباه، لكنه لا يقدم دائمًا معلومات كافية عن طبيعة الحدث.

وعند ارتباط الإنذار بالكاميرات، يمكن للمشغل:

- تحديد موقع الحدث.
- مشاهدة المنطقة المرتبطة بالإنذار.
- التحقق من وجود شخص أو نشاط غير معتاد.
- تقدير خطورة الحالة.
- دعم قرار الاستجابة[16].

ثالثًا: التحقق المرئي من الإنذارات

يمثل التحقق المرئي أحد أهم تطبيقات التكامل بين النظامين.

فبدلًا من التعامل مع الإنذار بوصفه معلومة منفردة، يمكن استخدام الفيديو لتقييمه وتصنيفه إلى:

- إنذار يستوجب الاستجابة.
- إنذار يحتاج إلى متابعة.
- إنذار ناتج عن سبب غير أمني.
- إنذار كاذب أو غير مؤكد.

ولا يعني ذلك أن الفيديو يلغي الحاجة إلى الإجراءات الأخرى، وإنما يوفر مصـــدرًا إضافيًا للمعلومات يساعد في اتخاذ القرار.

رابعًا: الربط القائم على الأحداث

يمكن تصميم النظام بحيث يؤدي صدور إنذار معين إلى إجراءات مترابطة، مثل:

١. تسجيل الحدث.

٢. استدعاء الكاميرا المرتبطة بالموقع.

٣. عرض الصورة للمشغل.

٤. إصدار تنبيه للمستخدم.

٥. تسجيل إجراءات الاستجابة.

٦. حفظ المعلومات المرتبطة بالحادث.

ويجب تصميم هذه الإجراءات وفق احتياجات المنشأة وإجراءاتها الأمنية، لا باعتبارها وظائف تقنية منفصلة عن التشغيل.

خامسًا: تحديات التكامل

قد يواجه الربط بين الإنذار والمراقبة عددًا من التحديات، من أهمها:

- كثرة الإنذارات.
- الإنذارات الكاذبة.
- عدم تطابق مواقع الأجهزة.
- اختلاف الأنظمة والبروتوكولات.
- تأخر نقل المعلومات.
- ضعف إجراءات الاستجابة.

ومن ثم فإن جودة التكامل لا تقاس بوجود اتصال تقني بين النظامين فقط، وإنما بقدرته على إنتاج معلومة قابلة للاستخدام في الوقت المناسب.

المبحث الرابع: مراكز القيادة والتحكم

تمثل مراكز القيادة والتحكم البيئة التشغيلية التي تتجمع فيها المعلومات الأمنية وتُستخدم في متابعة الأحداث واتخاذ القرارات وتنسيق الاستجابة. ولذلك فإن تكامل كاميرات المراقبة مع مركز القيادة والتحكم يمثل مرحلة متقدمة من مراحل التكامل الأمني[17].

أولًا: مفهوم مركز القيادة والتحكم

يمكن تعريف مركز القيادة والتحكم بأنه البيئة التشغيلية التي يتم فيها استقبال المعلومات المتعلقة بالأحداث، ومتابعتها وتحليلها، وتنسيق القرارات والإجراءات اللازمة للتعامل معها[18].

ولا يقتصر مركز القيادة والتحكم على شاشات عرض الكاميرات، بل يشمل الأشخاص والإجراءات والاتصالات والأنظمة التي تمكن المركز من أداء وظيفته.

ثانيًا: دور الكاميرات في مركز القيادة والتحكم

توفر كاميرات المراقبة للمركز مصدرًا بصريًا للمعلومات يمكن استخدامه في:

- متابعة الحالة الأمنية.
- التحقق من الإنذارات.
- تقييم الأحداث.
- متابعة حركة الأشخاص والمركبات.
- دعم توجيه فرق الاستجابة.
- توثيق الأحداث[19].

ثالثًا: التكامل داخل مركز القيادة والتحكم

يمكن أن يجمع المركز معلومات صادرة عن:

- كاميرات المراقبة.
- أنظمة التحكم بالدخول.
- أنظمة الإنذار.
- أنظمة الاتصال.

- أنظمة إدارة الحوادث.
- أنظمة الأمن والسلامة.

ويتيح هذا التجميع للمشغل تكوين صورة أكثر شمولًا عن الحالة، بدلًا من الانتقال المستمر بين أنظمة منفصلة.

رابعًا: الوعي بالموقف الأمني

يمثل الوعي بالموقف أحد الأهداف الأساسية لمراكز القيادة والتحكم. ويعني قدرة العاملين على فهم الحالة الحالية، وتقدير تطورها المحتمل، واتخاذ القرارات المناسبة استنادًا إلى المعلومات المتاحة[20].

وتسهم المراقبة المرئية في هذا المجال، لكنها لا تستطيع وحدها توفير الصورة الكاملة للموقف؛ إذ قد تتطلب بعض الأحداث معلومات من أنظمة أخرى.

خامسًا: العنصر البشري في مركز القيادة

رغم التطور التقني، يظل العامل البشري عنصرًا أساسيًا في تشغيل مراكز القيادة والتحكم. فالمعلومات المتعددة تحتاج إلى تفسير وترتيب للأولويات واتخاذ قرار.

ولهذا ينبغي أن يراعي تصميم المركز:

- سهولة استخدام الأنظمة.
- وضوح المعلومات.
- تقليل المعلومات غير الضرورية.
- تحديد المسؤوليات.
- التدريب.
- إجراءات التصعيد والاستجابة.

المبحث الخامس: التكامل مع أنظمة الأمن والسلامة

لا تقتصر وظيفة التكامل الأمني على الأنظمة المرتبطة مباشرة بمنع الدخول أو اكتشاف التهديدات الأمنية، بل تمتد إلى أنظمة السلامة والطوارئ، خصوصًا في المنشآت التي يمكن أن تتداخل فيها المخاطر الأمنية مع مخاطر الحريق والحوادث والإخلاء والطوارئ[21].

أولًا: مفهوم أنظمة الأمن والسلامة

تشمل أنظمة الأمن والسلامة مجموعة من الأنظمة والإجراءات التي تهدف إلى حماية الأشخاص والممتلكات واستمرارية العمليات من المخاطر الأمنية أو التشغيلية أو الطارئة.

ومن أمثلتها:

- أنظمة كشف الحريق والإنذار.
- أنظمة الإخلاء والطوارئ.
- أنظمة الاتصال في حالات الطوارئ.
- أنظمة إدارة المباني ذات الصلة بالسلامة.
- أنظمة مراقبة الظروف البيئية، بحسب طبيعة المنشأة.

ثانيًا: أهمية التكامل

يسمح التكامل باستخدام المعلومات المرئية في دعم تقييم الحالات الطارئة، مثل:

- التحقق من وجود أشخاص في منطقة متأثرة.
- متابعة تطور حالة طارئة.
- دعم تقييم مسارات الحركة والإخلاء.
- مساعدة فرق الاستجابة في فهم الحالة الميدانية.
- توثيق تطور الحدث[22].

ثالثًا: التكامل مع أنظمة الحريق والطوارئ

يمكن أن تتكامل الكاميرات مع أنظمة الحريق والطوارئ بطريقة تسمح بإظهار الصور المرتبطة بالموقع الذي صدر منه الإنذار.

ومع ذلك، ينبغي عدم الخلط بين دور الكاميرات ودور أنظمة الكشف المعتمدة للسلامة؛ فالكاميرا قد تدعم التحقق والمراقبة، لكنها لا تحل تلقائيًا محل أنظمة الكشف والحماية المصممة وفق متطلبات السلامة ذات الصلة[23].

رابعًا: التكامل مع إدارة الإخلاء

يمكن استخدام المعلومات المرئية لدعم متابعة الإخلاء وتحديد الازدحام أو العوائق أو وجود أشخاص في مناطق معينة، بما يساعد فرق الطوارئ على اتخاذ قرارات أكثر اطلاعًا.

ويجب أن يتم ذلك وفق خطط الطوارئ المعتمدة وإجراءات المنشأة، بحيث تكون التقنية داعمة للخطة وليست بديلًا عنها.

خامسًا: التكامل واستمرارية الأعمال

يمكن أن تساعد المعلومات الصادرة عن المنظومات المتكاملة في دعم تقييم تأثير الأحداث على العمليات وتحديد الأولويات أثناء الطوارئ، وهو ما يجعل التكامل مرتبطًا كذلك بمفهوم استمرارية الأعمال والقدرة على التعافي[24].

المبحث السادس: إدارة الأحداث المتكاملة

تمثل إدارة الأحداث المتكاملة المرحلة التي تظهر فيها القيمة التشغيلية الحقيقية للتكامل الأمني؛ إذ لا يقتصر الأمر على استقبال الإنذارات أو عرض الصور، وإنما يمتد إلى تنظيم الحدث منذ لحظة اكتشافه وحتى تقييمه والاستجابة له وتوثيقه وإغلاقه[25].

أولًا: مفهوم الحدث الأمني

يمكن تعريف الحدث الأمني بأنه واقعة أو حالة أو مؤشر يتطلب الانتباه أو التقييم أو اتخاذ إجراء من جانب الجهة المسؤولة عن الأمن.

وقد يكون الحدث:

- دخولًا غير مصرح به.
- إنذارًا أمنيًا.
- حالة طوارئ.
- حادثًا تشغيليًا.
- نشاطًا غير اعتيادي.

ثانيًا: مفهوم إدارة الأحداث المتكاملة

يقصد بإدارة الأحداث المتكاملة:

تنظيم عملية استقبال الأحداث الأمنية وتقييمها وتصنيفها والاستجابة لها وتوثيق إجراءات التعامل معها باستخدام المعلومات الواردة من منظومات أمنية متعددة.

وتكمن القيمة الأساسية في أن الحدث لا يعالج باعتباره معلومة منفردة، وإنما باعتباره حالة يمكن أن تجمع بيانات من مصادر مختلفة.

ثالثًا: مراحل إدارة الحدث

يمكن تنظيم إدارة الحدث في المراحل الآتية:

1. الاكتشاف

يبدأ الحدث من خلال إنذار أو ملاحظة بشرية أو تحليل آلي أو مصدر معلومات آخر.

2. التحقق

يتم جمع المعلومات اللازمة لتحديد حقيقة الحدث، ومن بينها المعلومات المرئية.

3. التقييم

يتم تقدير طبيعة الحدث ودرجة خطورته وتأثيره.

4. التصنيف والأولوية

تحدد الأولوية وفق مستوى الخطر والحاجة إلى الاستجابة.

5. الاستجابة

يتم اتخاذ الإجراءات المناسبة وتوجيه الموارد المعنية.

6. التوثيق

توثق الإجراءات والمعلومات والتسجيلات المرتبطة بالحدث.

7. الإغلاق والمراجعة

بعد انتهاء الحدث، تتم مراجعة الإجراءات واستخلاص الدروس وتحسين الإجراءات المستقبلية[26].

رابعًا: دور كاميرات المراقبة في إدارة الحدث

تؤدي الكاميرات دورًا في مراحل متعددة، منها:

- الكشف.
- التحقق.
- التقييم.
- متابعة تطور الحدث.
- توجيه الاستجابة.
- التوثيق.
- دعم التحقيق اللاحق.

وبذلك لا ينبغي النظر إلى الكاميرا على أنها أداة مستقلة داخل دورة الحدث، وإنما باعتبارها مصدرًا للمعلومات يمكن استخدامه في مراحل مختلفة.

خامسًا: إدارة الأولويات

من أهم متطلبات إدارة الأحداث المتكاملة تحديد الأولويات؛ إذ قد تستقبل المنشأة عددًا كبيرًا من الأحداث في الوقت نفسه.

ولذلك يجب أن تحدد الإجراءات:

- مستوى خطورة الحدث.
- الجهة المسؤولة.
- زمن الاستجابة المتوقع.
- آلية التصعيد.
- متطلبات التوثيق.
- إجراءات الإغلاق.

سادسًا: إدارة سجل الحدث

يعد سجل الحدث من العناصر المهمة في إدارة الأحداث؛ لأنه يسمح بتوثيق:

- وقت اكتشاف الحدث.
- مصدر الحدث.
- المعلومات المرتبطة به.
- إجراءات التحقق.
- القرارات المتخذة.
- إجراءات الاستجابة.
- وقت الإغلاق.
- الملاحظات اللاحقة.

ويساعد هذا السجل في التقييم والمراجعة والتحقيق وتحسين الأداء.

المبحث السابع: متطلبات نجاح التكامل

لا يتحقق التكامل الأمني بمجرد ربط الأجهزة والأنظمة تقنيًا، وإنما يتطلب مجموعة من المتطلبات الفنية والتشغيلية والبشرية والتنظيمية. ولذلك فإن نجاح التكامل يعتمد على قدرة المنشأة على إدارة هذه المتطلبات بصورة متوازنة[27].

أولًا: المتطلبات الفنية

تشمل المتطلبات الفنية:

- توافق الأنظمة والبروتوكولات.
- دقة التزامن الزمني.
- موثوقية الاتصالات.
- كفاية البنية التحتية للشبكة.
- قابلية الأنظمة للتوسع.
- التوافق بين البرمجيات والأجهزة.
- إدارة النسخ والتحديثات.

ويجب أن يحدد التصميم منذ البداية طبيعة التفاعلات المطلوبة بين الأنظمة، بدلًا من الاكتفاء بإضافة الربط بعد تنفيذ الأنظمة بصورة منفصلة.

ثانيًا: المتطلبات التشغيلية

يتطلب التكامل وضع إجراءات تشغيل واضحة تحدد:

- من يتلقى التنبيه؟
- من يتحقق منه؟
- من يتخذ القرار؟
- من يوجه الاستجابة؟
- متى يتم تصعيد الحدث؟
- كيف يتم إغلاقه؟
- كيف يتم توثيقه؟

فالتكامل التقني دون تكامل في الإجراءات قد يؤدي إلى زيادة كمية المعلومات دون تحسين حقيقي في الأداء.

ثالثًا: المتطلبات البشرية

يتطلب التكامل تدريب العاملين على:

- تشغيل الأنظمة.
- تفسير المعلومات.
- التحقق من الأحداث.
- تحديد الأولويات.
- تنفيذ إجراءات التصعيد.
- توثيق الأحداث.
- التعامل مع الأعطال.

كما ينبغي مراعاة العوامل البشرية عند تصميم واجهات التشغيل ومقدار المعلومات المعروضة للمشغل.

رابعًا: المتطلبات التنظيمية

تشمل المتطلبات التنظيمية:

- تحديد المسؤوليات.
- تحديد الصلاحيات.
- وضع سياسات استخدام المعلومات.
- تنظيم الوصول إلى التسجيلات.
- تحديد مدد الاحتفاظ بالبيانات وفق المتطلبات القانونية والتنظيمية.
- تحديد إجراءات التدقيق والمراجعة.

خامسًا: الأمن السيبراني

يمثل الأمن السيبراني عنصرًا أساسيًا في الأنظمة الأمنية المتكاملة، لأن زيادة الترابط بين الأنظمة تعني زيادة عدد نقاط الاتصال والتفاعل بينها.

ولذلك ينبغي مراعاة:

- إدارة حسابات المستخدمين والصلاحيات.
- حماية الاتصالات.
- تحديث الأنظمة.
- إدارة الثغرات.
- تسجيل الأحداث الأمنية.
- النسخ الاحتياطي والتعافي.
- فصل الأنظمة الحساسة وفق التصميم الأمني المناسب[28].

ويكتسب هذا الجانب أهمية خاصة في أنظمة المراقبة القائمة على الشبكات، إذ إن الكاميرات ومسجلات الفيديو والخوادم ومحطات التشغيل قد تمثل مكونات تقنية متصلة بالبنية التحتية الرقمية للمنشأة.

سادسًا: قابلية التشغيل والاستمرارية

ينبغي اختبار التكامل بصورة دورية للتأكد من أن الأنظمة تعمل معًا كما هو مخطط لها.

ويشمل الاختبار:

- اختبار الربط.
- اختبار الأحداث.
- اختبار الإنذارات.
- اختبار إجراءات الاستجابة.
- اختبار حالات فشل الاتصال.
- اختبار استعادة الخدمة.

كما ينبغي وجود خطط بديلة للتعامل مع تعطل أحد مكونات التكامل، حتى لا يؤدي فشل نظام واحد إلى تعطيل القدرة الأمنية بصورة واسعة.

سابعًا: قياس فاعلية التكامل

يمكن تقييم فاعلية التكامل من خلال مؤشرات أداء مناسبة، مثل:

- زمن اكتشاف الحدث.

- زمن التحقق.
- زمن الاستجابة.
- نسبة الإنذارات التي تم التحقق منها.
- نسبة الأحداث التي تم توثيقها بصورة مكتملة.
- زمن استعادة الخدمة عند حدوث عطل.
- مستوى الالتزام بإجراءات التشغيل.

ويجب ألا ينظر إلى هذه المؤشـــرات بصـــورة منفصـــلة عن أهداف المنشـــأة وطبيعة المخاطر التي تواجهها.

خلاصة الفصل الثالث

يتضح من دراسة التكامل بين كاميرات المراقبة والمنظومات الأمنية أن التطور في أنظمة المراقبة لم يعد مرتبطًا فقط بتحسين جودة الصورة أو زيادة عدد الكاميرات، وإنما أصبح مرتبطًا بصورة متزايدة بقدرة المنظومة على التفاعل مع الأنظمة الأمنية الأخرى وتحويل المعلومات المتعددة إلى قدرة تشغيلية وأمنية قابلة للاستخدام.

وقد تناول الفصل مفهوم التكامل الأمني، وبيّن أن التكامل لا يعني بالضرورة دمج جميع الأنظمة في منصة واحدة، وإنما قد يتحقق من خلال تبادل المعلومات والأحداث وتنسيق الإجراءات بين الأنظمة المختلفة.

كما أوضح الفصل أهمية الربط بين كاميرات المراقبة وأنظمة التحكم بالدخول، إذ يتيح هذا الربط الجمع بين السجلات النظامية والمعلومات المرئية، بما يدعم التحقق والتوثيق والتحقيق. كما تناول الربط مع أنظمة الإنذار، ولا سيما دوره في التحقق المرئي من الإنذارات وتقييمها قبل اتخاذ إجراءات الاستجابة.

وتناول الفصل كذلك دور مراكز القيادة والتحكم بوصفها البيئة التشغيلية التي تجمع المعلومات الأمنية وتدعم اتخاذ القرار، مع التأكيد على أن التكنولوجيا لا تلغي أهمية العامل البشري، وإنما ينبغي أن تدعم قدرته على فهم الموقف واتخاذ القرار.

كما امتد التحليل إلى التكامل مع أنظمة الأمن والسلامة، وأوضح أن الكاميرات يمكن أن تدعم التحقق والتقييم والاستجابة في حالات الطوارئ، لكنها لا تمثل بديلًا عن أنظمة السلامة المعتمدة.

وتناول الفصل مفهوم إدارة الأحداث المتكاملة باعتبارها عملية تبدأ من اكتشاف الحدث والتحقق منه وتقييمه وتصنيفه والاستجابة له وتوثيقه ثم إغلاقه ومراجعته، مع بيان الدور الذي تؤديه كاميرات المراقبة في مختلف مراحل هذه الدورة.

وأخيرًا، بيّن الفصل أن نجاح التكامل لا يتوقف على الاتصال التقني بين الأنظمة، وإنما يتطلب توافر مجموعة متكاملة من المتطلبات الفنية والتشغيلية والبشرية والتنظيمية، إلى جانب الأمن السيبراني والاختبار الدوري وقياس الأداء.

ومن ثم يمكن صياغة النموذج العام للتكامل الأمني على النحو الآتي:

كاميرات المراقبة + التحكم بالدخول + الإنذار + القيادة والتحكم + الأمن والسلامة ← معلومات مترابطة ← وعي بالموقف ← إدارة الحدث ← استجابة منسقة ← توثيق ومراجعة

وبذلك فإن معيار نجاح التكامل لا ينبغي أن يكون السؤال: هل الأنظمة متصلة تقنيًا؟ وإنما السؤال الأكثر دقة هو:

هل يؤدي التكامل إلى تحسين القدرة على اكتشاف الأحداث والتحقق منها وتقييمها والاستجابة لها وإدارتها بصورة أكثر كفاءة وفاعلية؟

أهم نتائج الفصل الثالث

١. التكامل الأمني يمثل انتقالًا من تشغيل الأنظمة بصورة منفصلة إلى تشغيلها بصورة مترابطة.
٢. لا يعني التكامل بالضرورة دمج جميع الأنظمة في منصة واحدة.
٣. يسهم التكامل في تحسين الوعي بالموقف الأمني.
٤. الربط مع التحكم بالدخول يعزز التحقق من عمليات الدخول والخروج.
٥. الربط مع أنظمة الإنذار يدعم التحقق المرئي من الأحداث.
٦. مراكز القيادة والتحكم تمثل البيئة التشغيلية الرئيسية للتكامل.
٧. تكامل المعلومات من مصادر متعددة يدعم اتخاذ القرار.
٨. العامل البشري يظل عنصرًا أساسيًا في المنظومة المتكاملة.
٩. يمكن للمراقبة أن تدعم أنظمة الأمن والسلامة والطوارئ.
١٠. لا ينبغي اعتبار الكاميرات بديلًا عن أنظمة السلامة المتخصصة.
١١. إدارة الأحداث المتكاملة تربط بين الاكتشاف والتحقق والاستجابة والتوثيق.
١٢. نجاح التكامل يتطلب متطلبات فنية وتشغيلية وبشرية وتنظيمية.
١٣. الأمن السيبراني عنصر أساسي في الأنظمة الأمنية المتكاملة.
١٤. الاختبار الدوري ضروري للتحقق من استمرارية التكامل.
١٥. ينبغي قياس فاعلية التكامل بمؤشرات أداء مرتبطة بالأهداف الأمنية.

١٦. التكامل الناجح هو الذي يحول المعلومات المتفرقة إلى قدرة أمنية وتشغيلية قابلة للاستخدام.

أسئلة التفكير والتقييم للفصل التاسع

أولًا: أسئلة معرفية

١. ما مفهوم التكامل الأمني؟
٢. ما الفرق بين التكامل والدمج؟
٣. ما أهمية الربط بين كاميرات المراقبة وأنظمة التحكم بالدخول؟
٤. ما أهمية الربط بين كاميرات المراقبة وأنظمة الإنذار؟
٥. ما المقصود بمركز القيادة والتحكم؟
٦. ما دور الكاميرات في مراكز القيادة والتحكم؟
٧. ما المقصود بإدارة الأحداث المتكاملة؟
٨. ما مراحل إدارة الحدث الأمني؟
٩. ما المتطلبات الفنية لنجاح التكامل؟
١٠. ما أهمية الأمن السيبراني في الأنظمة المتكاملة؟

ثانيًا: أسئلة تحليلية

١١. حلل العلاقة بين التكامل الأمني وتحسين الوعي بالموقف.
١٢. لماذا لا يكفي الربط التقني وحده لتحقيق التكامل؟
١٣. حلل أهمية الربط بين التحكم بالدخول والمراقبة.
١٤. كيف يسهم الفيديو في التحقق من الإنذارات؟
١٥. حلل دور مراكز القيادة والتحكم في إدارة الأحداث.
١٦. لماذا لا يمكن للتكنولوجيا أن تحل محل العامل البشري؟
١٧. حلل العلاقة بين التكامل الأمني والأمن السيبراني.
١٨. لماذا يمثل تحديد الأولويات عنصرًا أساسيًا في إدارة الأحداث؟
١٩. كيف يمكن قياس فاعلية التكامل الأمني؟
٢٠. ما مخاطر فشل التكامل بين الأنظمة الأمنية؟

ثالثًا: أسئلة تطبيقية

٢١. اختر منشـأة تعرفها وحدد الأنظمة الأمنية التي ينبغي تكاملها مع كاميرات المراقبة.

٢٢. صمم تصورًا لربط كاميرات المراقبة بنظام التحكم بالدخول.

٢٣. صمم سيناريو لربط إنذار اقتحام بالكاميرات.

٢٤. صمم تصورًا لمركز قيادة وتحكم متكامل.

٢٥. صمم سيناريو لاستخدام الكاميرات في إدارة حالة طوارئ.

٢٦. صمم دورة متكاملة لإدارة حدث أمني.

٢٧. ضع قائمة تحقق لتقييم التكامل الأمني في منشأة.

٢٨. صمم مؤشرات أداء لقياس فاعلية التكامل.

٢٩. ضع خطة لاختبار التكامل بين الكاميرات والإنذار والتحكم بالدخول.

٣٠. اقترح إجراءات للتعامل مع تعطل أحد مكونات المنظومة المتكاملة.

المراجع:

(1) International Electrotechnical Commission, *IEC 62676-4:2025: Video surveillance systems for use in security applications — Part 4: Application guidelines*, 2nd ed. (Geneva: IEC, 2025).

(2) National Institute of Standards and Technology, *Video Quality in Public Safety (VQiPS)* (Gaithersburg, MD: NIST).

.(3) International Electrotechnical Commission, *IEC 62676-4:2025*

(4) National Institute of Standards and Technology, *Guide to Operational Technology (OT) Security*, NIST Special Publication 800-82 Rev. 3 (Gaithersburg, MD: NIST, 2023).

.(5) International Electrotechnical Commission, *IEC 62676-4:2025*

(6) International Organization for Standardization, *ISO 22320:2018, Security and resilience — Emergency management — Requirements for incident response* (Geneva: ISO, 2018).

.(7) International Electrotechnical Commission, *IEC 62676-4:2025*

.(8) National Institute of Standards and Technology, *Guide to Operational Technology (OT) Security*, NIST SP 800-82 Rev. 3

.(9) International Electrotechnical Commission, *IEC 62676-4:2025*

(10) National Institute of Standards and Technology, *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*, NIST SP 800-40 Rev. 4 (Gaithersburg, MD: NIST, 2022).

.(11) International Electrotechnical Commission, *IEC 62676-4:2025*

.(12) International Electrotechnical Commission, *IEC 62676-4:2025*

.(13) National Institute of Standards and Technology, *Guide to Operational Technology (OT) Security*, NIST SP 800-82 Rev. 3

.(14) International Electrotechnical Commission, *IEC 62676-4:2025*

(15) National Fire Protection Association, *NFPA 72: National Fire Alarm and Signaling Code* (Quincy, MA: NFPA).

.(16) International Electrotechnical Commission, *IEC 62676-4:2025*

(17) International Organization for Standardization, *ISO 22320:2018*.

(18) International Organization for Standardization, *ISO 22320:2018*.

.(19) International Electrotechnical Commission, *IEC 62676-4:2025*

(20) International Organization for Standardization, *ISO 22320:2018*.

(21) National Fire Protection Association, *NFPA 72: National Fire Alarm and Signaling Code*.

.(22) International Electrotechnical Commission, *IEC 62676-4:2025*

(23) National Fire Protection Association, *NFPA 72: National Fire Alarm and Signaling Code*.

(24) International Organization for Standardization, *ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements* (Geneva: ISO, 2019).

(25) International Organization for Standardization, *ISO 22320:2018*.

(26) International Organization for Standardization, *ISO 22320:2018*.

.(27) International Electrotechnical Commission, *IEC 62676-4:2025*

.(28) National Institute of Standards and Technology, *Guide to Operational Technology (OT) Security*, NIST SP 800-82 Rev. 3

الفصل الرابع: أمن منظومة المراقبة وحمايتها

تمهيد الفصل

أصبحت منظومات المراقبة بالفيديو الحديثة جزءًا من البنية التقنية والأمنية للمنشآت، ولم تعد تقتصر وظيفتها على التقاط الصور وتسجيلها، بل أصبحت تعتمد على الكاميرات الشبكية، وخوادم التسجيل والإدارة، وشبكات الاتصال، ومحطات المشغلين، والتخزين، والبرمجيات، وربما التحليلات المرئية والتكامل مع أنظمة أمنية أخرى. وقد أدى هذا التحول إلى اتساع نطاق المخاطر التي يمكن أن تتعرض لها المنظومة، بحيث لم يعد أمنها مقتصرًا على حماية الكاميرا من التلف أو العبث المادي، وإنما أصبح يشمل أيضًا حماية الحسابات، والشبكات، وأجهزة التسجيل، والبيانات المسجلة، والنسخ الاحتياطية، واستمرارية الخدمة. وتشير إرشادات المعهد الوطني الأمريكي للمعايير والتقنية (NIST) إلى أن أنظمة التشغيل والتقنيات المتصلة بالشبكات تحتاج إلى ضوابط أمنية تراعي المخاطر التقنية والتشغيلية والبشرية معًا(1) .

وتنبع أهمية أمن منظومة المراقبة من أن اختراقها أو تعطيلها قد لا يؤدي فقط إلى فقدان القدرة على الرؤية، بل قد يؤدي كذلك إلى فقدان التسجيلات، أو تعديلها، أو الوصول غير المصرح به إليها، أو استخدام المنظومة كنقطة دخول إلى أنظمة أخرى داخل المنشأة. ولذلك فإن حماية منظومة المراقبة ينبغي أن تنظر إليها باعتبارها نظامًا معلوماتيًا وأمنيًا متكاملًا، وليس مجرد مجموعة من الكاميرات وأجهزة التسجيل(2) .

كما أن طبيعة التسجيلات المرئية تجعل مسألة حماية البيانات ذات أهمية خاصة؛ إذ قد تتضمن التسجيلات صور الأشخاص وحركتهم وسلوكهم ومعلومات مرتبطة بالزمان والمكان، وهو ما يستدعي تطبيق مبادئ الحماية المناسبة طوال دورة حياة البيانات، ابتداءً من إنشائها ونقلها وتخزينها، وانتهاءً بالاحتفاظ بها أو حذفها وفق السياسات المعتمدة(3) .

وعليه، يتناول هذا الفصل أمن منظومة المراقبة من منظور متكامل من خلال سبعة مباحث مترابطة، تبدأ بحماية مكونات المنظومة، ثم إدارة المستخدمين والصلاحيات، وحماية الشبكات، وحماية أجهزة التسجيل، وحماية التسجيلات، والنسخ الاحتياطي واستمرارية الخدمة، وتنتهي بمخاطر العبث والتلاعب. ويهدف هذا البناء إلى الانتقال

من حماية المكونات الفردية إلى حماية المنظومة ككل، بما يحقق السرية والسلامة والتوافر والموثوقية التشغيلية للتسجيلات والخدمات الأمنية.

المبحث الأول: حماية مكونات المنظومة

تبدأ حماية منظومة المراقبة من حماية مكوناتها الأساسية، إذ إن ضعف أي مكون يمكن أن يؤثر في أمن المنظومة بأكملها. وتشمل هذه المكونات الكاميرات، وأجهزة التسجيل، والخوادم، ومحطات العمل، ومعدات الشبكة، ووسائط التخزين، والبرمجيات المرتبطة بالمنظومة.

ولا ينبغي النظر إلى هذه المكونات باعتبارها وحدات مستقلة، لأن ارتباطها ببعضها البعض يجعل اختراق أحدها أو تعطيله قادرًا على التأثير في وظائف المكونات الأخرى.

أولًا: حماية الكاميرات

تعد الكاميرات الطرف الميداني لمنظومة المراقبة، ولذلك فإن حمايتها تتضمن جانبين رئيسيين: الحماية المادية والحماية التقنية.

وتشمل الحماية المادية وضع الكاميرات في مواقع تقلل احتمالات العبث بها أو إتلافها، واستخدام وسائل التثبيت المناسبة، وحمايتها من الظروف البيئية التي قد تؤثر في تشغيلها، وفق طبيعة موقع التركيب.

أما الحماية التقنية فتشمل تأمين إعدادات الكاميرا، وإدارة حسابات الوصول إليها، وتحديث البرمجيات الثابتة عند توفر التحديثات المناسبة، وتعطيل الخدمات غير الضرورية، وتغيير بيانات الاعتماد الافتراضية.

وتكتسب هذه الإجراءات أهمية خاصة في الكاميرات الشبكية؛ لأن الكاميرا قد تكون جهازًا حاسوبيًا متصلًا بالشبكة، وليس مجرد جهاز تصوير تقليدي(4) .

ثانيًا: حماية أجهزة وخوادم المنظومة

تحتاج أجهزة التسجيل والخوادم ومحطات الإدارة إلى حماية مادية وتقنية مناسبة لطبيعة المعلومات والوظائف التي تؤديها.

وتشمل الحماية المادية تقييد الوصول إلى غرف المعدات، واستخدام وسائل مناسبة للتحكم في الدخول، وحماية المعدات من الوصول غير المصرح به أو التلف العرضي.

أما الحماية التقنية فتشمل تأمين أنظمة التشغيل، وإدارة الحسابات، وتطبيق التحديثات الأمنية، وتقليل الخدمات غير الضرورية، ومراقبة الأنشطة ذات الصلة بالإدارة والتشغيل.

وتؤكد ممارسات الأمن السيبراني الحديثة أهمية تطبيق مبدأ تقليل سطح الهجوم من خلال الحد من الخدمات والمنافذ والصلاحيات غير الضرورية(5) .

ثالثًا: حماية معدات الشبكة

لا تقتصر حماية المنظومة على الأجهزة التي تنتج التسجيلات، بل تمتد إلى معدات الشبكة التي تنقل البيانات بينها.

وتشمل هذه المعدات المحولات، والموجهات، والجدران النارية، ونقاط الاتصال اللاسلكية عندما تستخدم، وغيرها من المكونات التي تتيح الاتصال بين عناصر المنظومة.

ويؤدي ضعف حماية الشبكة إلى إمكانية اعتراض الاتصالات أو الوصول غير المصرح به إلى الأجهزة أو تعطيل الخدمة، ولذلك ينبغي إدراج مكونات الشبكة ضمن نطاق الحماية الأمنية للمنظومة(6) .

رابعًا: مبدأ الحماية متعددة الطبقات

لا يكفي الاعتماد على إجراء أمني واحد لحماية مكونات المنظومة، وإنما ينبغي تطبيق مجموعة من الضوابط المتكاملة التي تشمل الحماية المادية، وإدارة الوصول، وأمن الشبكات، والتحديثات، والمراقبة، والاستجابة للحوادث.

ويعكس هذا النهج مبدأ الدفاع متعدد الطبقات، بحيث لا يؤدي فشل أحد الضوابط إلى انهيار الحماية بالكامل(7) .

المبحث الثاني: إدارة المستخدمين والصلاحيات

تمثل حسابات المستخدمين والصلاحيات أحد أهم عناصر أمن منظومة المراقبة؛ لأن الوصول غير المنضبط قد يسمح بمشاهدة التسجيلات أو حذفها أو تعديل الإعدادات أو تعطيل بعض الوظائف.

ومن ثم فإن حماية المنظومة لا تتحقق بمجرد تأمين الأجهزة، وإنما تتطلب أيضًا التأكد من أن كل مستخدم يحصل على الصلاحيات اللازمة لأداء مهامه فقط.

أولًا: إدارة حسابات المستخدمين

ينبغي أن تكون لكل مستخدم هوية حسابية محددة تمكن من ربط الأنشطة التي يقوم بها بالحساب المستخدم.

ويؤدي استخدام الحسابات الفردية إلى تحسين المساءلة، ويساعد على تتبع عمليات الدخول والتغيير والت يلزم أن يمتلك مشغل المراقبة الصلاحيات نفسها التي يمتلكها مسؤول النظام، الفصل بين صلاحيات المشاهدة، والإدارة، وتغيير الإعدادات، وتصدير التسجيلات، وإدارة المستخدمين، والتصدير وغيرها من الأنشطة الإدارية.

وتوصي ممارسات إدارة الهوية والوصول باستخدام هويات فردية بدل الحسابات المشتركة كلما كان ذلك ممكنًا(8) .

ثانيًا: مبدأ أقل قدر من الصلاحيات

يقوم مبدأ أقل قدر من الصلاحيات على منح المستخدم الحد الأدنى من الصلاحيات اللازمة لأداء وظيفته.

فعلى سبيل المثال، لا يلزم أن يمتلك مشغل المراقبة الصلاحيات نفسها التي يمتلكها مسؤول النظام، كما لا يلزم أن يمتلك مسؤول الصيانة صلاحيات الوصول إلى جميع التسجيلات ما لم تكن وظيفته تتطلب ذلك.

ويقلل هذا المبدأ من آثار اختراق الحساب أو إساءة استخدامه(9) .

ثالثًا: الفصل بين الصلاحيات

يساعد الفصل بين الوظائف في الحد من تركيز الصلاحيات الحساسة في حساب واحد.

فيمكن، بحسب طبيعة المنشأة، الفصل بين صلاحيات المشاهدة، والإدارة، وتغيير الإعدادات، وتصدير التسجيلات، وإدارة المستخدمين، والصيانة.

ويُعد هذا الإجراء مهمًا خصوصًا في البيئات التي تتعامل مع تسجيلات قد تستخدم في التحقيقات أو المرور الافتراضية، ووضع سياسات مناسبة لكلمات المرور، واستخدام المصادقة متعددة العوامل عندما المراقبة. ويجب أن يقوم على الهويات الفردية، وأقل قدر من الصلاحيات، والفصل المناسب بين الوظائف، والم الإجراءات الرسمية.

رابعًا: المصادقة وحماية بيانات الاعتماد

ينبغي استخدام آليات مصادقة مناسبة، مع منع استخدام كلمات المرور الافتراضية، ووضع سياسات مناسبة لكلمات المرور، واستخدام المصادقة متعددة العوامل عندما تكون متاحة ومتناسبة مع مستوى المخاطر(10) .

كما ينبغي مراجعة الحسابات دوريًا وتعطيل الحسابات التي لم تعد مطلوبة، خصوصًا حسابات الموظفين الذين انتهت علاقتهم بالمنشأة أو تغيرت مسؤولياتهم.

خامسًا: تسجيل أنشطة المستخدمين

لا تكتمل إدارة الصلاحيات دون تسجيل الأنشطة المهمة للمستخدمين، بحيث يمكن معرفة من دخل إلى النظام، ومتى دخل، وما العمليات الحساسة التي قام بها.

ويُسهم ذلك في تعزيز المساءلة واكتشاف الاستخدام غير المعتاد والتحقيق في الحوادث.

المبحث الثالث: حماية الشبكات

تعد الشبكة التي تربط مكونات منظومة المراقبة من أهم عناصرها؛ إذ تنتقل من خلالها الصور والأوامر وفق احتياجات المنشأة، من الإجراءات التي يمكن أن تقلل من انتشار التهديدات وتحد من الوصول غير الضروري ألا تكون جميع الاتصالات بين مكونات الشبكة مفتوحة بصورة غير مقيدة، وإنما ينبغي تحديد الاتصالات الضرورية بين الكاميرات والخوادم ومحطات الإدارة ومكونات ينبغي استخدام آليات حماية مناسبة للاتصالات، ولا سيما عندما تمر البيانات عبر شبكات غير موثوقة بالغ الأهمية في منظومة المراقبة، لأنها تستقبل التسجيلات وتخزنها وتوفرها للمستخدمين أكثر مكونات المنظومة حساسية، ولذلك تحتاج إلى حماية مادية وتقنية وإدارية، مع تأمين نظام التشغيل وواجهات الإدارة وتقليل الخدمات غير الضرورية ومراقبة العمليات قانونية. ولذلك فإن حمايتها ينبغي أن تشمل السرية والسلامة والتوافر، بالإضافة إلى ضمان إمكانية إثبات مصدرها تحقق ذلك من خلال التحكم في الصلاحيات، وحماية أنظمة التخزين، وتقييد عمليات التصدير والنسخ، واستخدام وسائل التعة التخزين، وآليات الاسترجاع مناسبة تمنع استعادتها دون تصريح، مع مراعاة أي متطلبات تتعلق بحفظ إجراءات تضمن المحافظة على أصل التسجيل وسلامته، وتوثيق عملية التصدير، ومن قام بها، ووقت حدوثه إلى حماية متكاملة تضمن سريتها وسلامتها وتوافرها. كما يجب تنظيم الاحتفاظ بها وحذفها وتصديرها وفق على المراقبة بصورة مستمرة أو التي تمثل فيها التسجيلات مصدرًا أساسيًا للمعلومات الأمنية. وينبغي ألا تقتصر الخطة على إنشاء نسخ احتياطية، بل يجب أن تشمل تحديد البيانات المهمة، المصرح به إلى النظام، أو إداريًا من خلال يتم العبث تقنيًا من خلال الدخول غير المصرح به إلى النظام، أو تغيير الإعدادات، أو تعطيل التسجيل، أو الحسابات، وتقييد الصلاحيات، وتسجيل العمليات، ومراقبة الأنشطة غير المعتادة، وبيانات الإدارة. ولذلك فإن أمن الشبكة يمثل جزءًا لا يتجزأ من أمن المراقبة.

أولًا: عزل شبكة المراقبة

يُعد فصل منظومة المراقبة عن الشبكات الأخرى، أو تقسيمها منطقيًا وفق احتياجات المنشأة، من الإجراءات التي يمكن أن تقلل من انتشار التهديدات وتحد من الوصول غير الضروري.

ويُعرف هذا الاتجاه ضمن ممارسات أمن الشبكات بالتقسيم أو Network Segmentation. (11)

ثانيًا: التحكم في الاتصالات

ينبغي ألا تكون جميع الاتصالات بين مكونات الشبكة مفتوحة بصورة غير مقيدة، وإنما ينبغي تحديد الاتصالات الضرورية بين الكاميرات والخوادم ومحطات الإدارة ومكونات الشبكة الأخرى.

ويمكن استخدام الجدران النارية وقواعد التحكم في الوصول للحد من الاتصالات غير الضرورية(12) .

ثالثًا: حماية الاتصالات

عند نقل البيانات عبر الشبكات، ينبغي استخدام آليات حماية مناسبة للاتصالات، ولا سيما عندما تمر البيانات عبر شبكات غير موثوقة.

وتساعد تقنيات التشفير وبروتوكولات الاتصال الآمنة على تقليل مخاطر التنصت أو التلاعب بالبيانات أثناء النقل.

رابعًا: تحديث معدات الشبكة

تحتاج معدات الشبكة إلى إدارة مستمرة للتحديثات والثغرات الأمنية، لأن وجود جهاز شبكة غير محدث قد يمثل نقطة ضعف تؤثر في بقية المنظومة.

وينبغي أن تكون عملية التحديث منظمة، ومبنية على تقييم المخاطر، وأن تراعي اختبار التحديثات قبل تطبيقها في البيئات الحساسة.

خامسًا: مراقبة الشبكة

تساعد مراقبة الشبكة في اكتشاف السلوك غير المعتاد ومحاولات الوصول غير المصرح به، وتوفر معلومات يمكن استخدامها في الاستجابة للحوادث.

وتزداد أهمية هذه المراقبة عندما تكون منظومة المراقبة متصلة بشبكات المؤسسة أو بالإنترنت.

المبحث الرابع: حماية أجهزة التسجيل

تمثل أجهزة التسجيل والخوادم مركزًا بالغ الأهمية في منظومة المراقبة، لأنها تستقبل التسجيلات وتخزنها وتوفرها للمستخدمين والأنظمة المصرح لها.

ومن ثم فإن اختراق جهاز التسجيل أو تعطيله قد يؤدي إلى فقدان جزء كبير من الوظيفة الأمنية للمنظومة.

أولًا: الحماية المادية

ينبغي وضع أجهزة التسجيل في أماكن مقيدة الوصول، ومناسبة من حيث درجة الحرارة والطاقة والحماية من المخاطر البيئية.

كما ينبغي منع الوصول غير المصرح به إلى المنافذ والأقراص ووسائط التخزين.

ثانيًا: تأمين نظام التشغيل

يجب تأمين نظام التشغيل الذي يعمل عليه جهاز التسجيل، وتطبيق التحديثات المناسبة، وتعطيل الخدمات غير المطلوبة، واستخدام حسابات إدارية محمية.

ويجب أن تكون إدارة الجهاز جزءًا من برنامج إدارة الأصول والتحديثات الأمنية في المنشأة.

ثالثًا: حماية واجهات الإدارة

تحتاج واجهات الإدارة المحلية أو الشبكية إلى حماية مناسبة، بما يشمل المصادقة القوية، وتحديد المستخدمين المصرح لهم، وتقييد الوصول الإداري.

رابعًا: مراقبة العمليات

ينبغي الاحتفاظ بسجلات مناسبة للعمليات الحساسة التي تتم على أجهزة التسجيل، مثل الدخول الإداري، وتغيير الإعدادات، وحذف البيانات أو تصديرها، متى كان النظام يدعم ذلك.

خامسًا: تقليل نقاط الضعف

ينبغي تقليل الخدمات والمنافذ والحسابات التي لا تحتاج إليها أجهزة التسجيل، لأن كل خدمة غير ضرورية يمكن أن تزيد من سطح الهجوم.

المبحث الخامس: حماية التسجيلات

تعد التسجيلات المرئية من أهم الأصول التي تنتجها منظومة المراقبة، وقد تكون ذات قيمة تشغيلية أو تحقيقية أو قانونية. ولذلك فإن حمايتها ينبغي أن تشمل السرية والسلامة والتوافر، بالإضافة إلى ضمان إمكانية إثبات مصدرها وسلامتها عند الحاجة.

أولًا: سرية التسجيلات

تتطلب سرية التسجيلات منع الاطلاع عليها من الأشخاص غير المصرح لهم.

ويتحقق ذلك من خلال التحكم في الصلاحيات، وحماية أنظمة التخزين، وتقييد عمليات التصدير والنسخ، واستخدام وسائل التشفير المناسبة حيثما كان ذلك ملائمًا.

ثانيًا: سلامة التسجيلات

تعني سلامة التسجيلات ضمان عدم تغيير محتواها أو العبث بها دون اكتشاف ذلك.

وتكتسب هذه المسألة أهمية خاصة عندما تستخدم التسجيلات لأغراض التحقيق أو الإجراءات القانونية.

وتتطلب سلامة البيانات استخدام ضوابط مناسبة لمنع التعديل غير المصرح به، وتوثيق عمليات الوصول والتصدير، والمحافظة على النسخ الأصلية وفق السياسات المعتمدة.

ثالثًا: توافر التسجيلات

لا تكفي حماية التسجيلات من التعديل إذا لم تكن متاحة عند الحاجة.

ومن ثم ينبغي تحديد متطلبات الاحتفاظ، وسعة التخزين، وآليات الاسترجاع، والضوابط التي تمنع فقدان البيانات بسبب الأعطال أو الحذف غير المقصود.

رابعًا: الاحتفاظ والحذف

ينبغي ألا يُنظر إلى الاحتفاظ بالتسجيلات على أنه عملية تخزين مفتوحة المدة، بل يجب أن تحدد المنشأة مدة الاحتفاظ وفق احتياجاتها الأمنية والتشغيلية والمتطلبات النظامية والتنظيمية ذات الصلة.

وعند انتهاء المدة ينبغي التخلص من البيانات بطريقة مناسبة تمنع استعادتها دون تصريح، مع مراعاة أي متطلبات تتعلق بحفظ الأدلة أو التحقيقات الجارية(13) .

خامسًا: تصدير التسجيلات

عند تصـــدير تســـجيلات لأغراض التحقيق أو المشـــاركة الرســـمية، ينبغي اســـتخدام إجراءات تضمن المحافظة على أصل التسجيل وسلامته، وتوثيق عملية التصدير، ومن قام بها، ووقت حدوثها، والنسخة التي تم استخراجها.

وقد خصص NIST إرشادات فنية لتصدير الفيديو الرقمي بهدف تعزيز قابلية استخدام التسجيلات وحفظ خصائصها المهمة(14) .

المبحث السادس: النسخ الاحتياطي واستمرارية الخدمة

لا تقتصـــر حماية منظومة المراقبة على منع الاختراق، بل تشـــمل أيضًـــا قدرتها على الاستمرار في العمل واستعادة التسجيلات والخدمات بعد الأعطال أو الحوادث.
وتزداد أهمية ذلك في المنشـآت التي تعتمد على المراقبة بصـورة مسـتمرة أو التي تمثل فيها التسجيلات مصدرًا أساسيًا للمعلومات الأمنية.

أولًا: مفهوم النسخ الاحتياطي

يقصـــد بالنســـخ الاحتياطي إنشـــاء نســـخة إضـــافية من البيانات يمكن اســـتخدامها لاستعادتها عند فقدان البيانات الأصلية أو تلفها أو عدم إمكانية الوصول إليها.
ولا ينبغي أن يقتصـر النسـخ الاحتياطي على التسـجيلات وحدها في جميع الحالات؛ فقد تكون هناك حاجة أيضًـــا إلى حماية إعدادات الأنظمة وقواعد البيانات والمعلومات اللازمة لإعادة بناء المنظومة.

ثانيًا: استراتيجية النسخ الاحتياطي

ينبغي أن تحدد المنشأة:

- البيانات التي يجب نسخها.
- دورية النسخ.
- موقع النسخ.
- مدة الاحتفاظ بالنسخ.
- آلية استعادة البيانات.
- المسؤوليات المتعلقة بإدارة النسخ.

وتوصي ممارسات استمرارية الأعمال والأمن السيبراني باختبار عمليات الاستعادة بدل افتراض أن النسخ الاحتياطية ستعمل تلقائيًا عند الحاجة(15) .

ثالثًا: النسخ المنفصل

ينبغي، بحسب مستوى المخاطر، الاحتفاظ ببعض النسخ في بيئة منفصلة عن النظام التشغيلي الأساسي، بحيث لا يؤدي اختراق النظام الأصلي إلى فقدان جميع النسخ.

وتكتسب هذه الممارسة أهمية خاصة في مواجهة الهجمات التي تستهدف حذف البيانات أو تشفيرها.

رابعًا: استمرارية الخدمة

تعني استمرارية الخدمة قدرة منظومة المراقبة على الاستمرار في أداء وظائفها الأساسية رغم الأعطال أو الحوادث.

ويمكن تحقيق ذلك من خلال إجراءات تشمل:

- توفير مصادر طاقة احتياطية.
- استخدام مكونات احتياطية عند الحاجة.
- وجود بدائل مناسبة للتخزين أو التسجيل.
- خطط لاستعادة الخدمة.
- إجراءات واضحة للتعامل مع الأعطال.

خامسًا: اختبار الاستعادة

لا يمكن اعتبار خطة النسخ الاحتياطي ناجحة دون اختبار فعلي لقدرة المنشأة على استعادة البيانات والخدمات.

ولهذا ينبغي إجراء اختبارات دورية للتحقق من صلاحية النسخ، وسلامة البيانات، والمدة اللازمة للاستعادة.

المبحث السابع: مخاطر العبث والتلاعب

يمثل العبث والتلاعب أحد أخطر التهديدات التي يمكن أن تتعرض لها منظومة المراقبة، لأن نجاح المعتدي في تعطيل الكاميرات أو تغيير الإعدادات أو حذف التسجيلات قد يؤدي إلى إضعاف قدرة المنشأة على الكشف والتوثيق والتحقيق.

وقد يكون العبث ماديًا مباشرًا، أو تقنيًا من خلال الوصول غير المصرح به إلى النظام، أو إداريًا من خلال إساءة استخدام الصلاحيات.

أولًا: العبث المادي

يشمل العبث المادي:

١. تحريك الكاميرا من موضعها.

٢. تغطية العدسة.

٣. قطع الطاقة أو الاتصال.

٤. إتلاف الجهاز.

٥. الوصول إلى أجهزة التسجيل أو التخزين.

وتتطلب مواجهة ذلك إجراءات مادية مناسبة، ومراقبة حالة الأجهزة، ووضع الكاميرات والمعدات الحساسة في مواقع تقلل احتمالات العبث بها.

ثانيًا: العبث التقني

قد يتم العبث تقنيًا من خلال الدخول غير المصرح به إلى النظام، أو تغيير الإعدادات، أو تعطيل التسجيل، أو حذف البيانات، أو تعديل صلاحيات المستخدمين.

وتتطلب مواجهة ذلك حماية الحسابات، وتقييد الصلاحيات، وتسجيل العمليات، ومراقبة الأنشطة غير المعتادة، وتطبيق ضوابط أمن الشبكات.

ثالثًا: التلاعب بالتسجيلات

يعد التلاعب بالتسجيلات من أخطر أشكال العبث؛ لأنه قد يؤدي إلى فقدان القيمة الإثباتية للتسجيل أو التشكيك في سلامته.

ولهذا ينبغي تطبيق ضوابط تمنع التعديل غير المصرح به، وتوثيق عمليات الوصول والتصدير، والحفاظ على النسخ الأصلية وفق الإجراءات المعتمدة.

رابعًا: اكتشاف العبث

لا ينبغي أن تقتصر الحماية على منع العبث، بل يجب أن تشمل القدرة على اكتشافه.

ومن الوسائل الممكنة:

- التنبيه عند فقد الاتصال.
- مراقبة حالة الكاميرات.
- تسجيل تغييرات الإعدادات.
- مراقبة عمليات الدخول.
- مراجعة السجلات.
- التنبيه عند حدوث سلوك غير معتاد.

خامسًا: الاستجابة لحوادث العبث

عند اكتشاف عبث أو تلاعب، ينبغي وجود إجراء واضح يحدد:

١. كيفية اكتشاف الحادث والإبلاغ عنه.
٢. كيفية عزل المكون المتأثر عند الحاجة.
٣. كيفية المحافظة على الأدلة والسجلات.
٤. كيفية استعادة الخدمة.
٥. كيفية تحديد سبب الحادث.
٦. كيفية منع تكراره.

ويتوافق ذلك مع مبادئ إدارة الحوادث الأمنية التي تؤكد أهمية الاستعداد والكشف والاستجابة والتعافي والتحسين المستمر(16) .

المبحث الثامن: الضوابط التنظيمية والإجرائية

لا تقتصر حماية منظومة المراقبة على الإجراءات التقنية المتعلقة بالكاميرات والشبكات وأجهزة التسجيل، وإنما تمتد إلى مجموعة من الضوابط التنظيمية والإجرائية التي تحدد كيفية تشغيل المنظومة، والمسؤوليات المرتبطة بها، وحدود استخدامها، وآليات الوصول إلى التسجيلات والتعامل معها. فحتى المنظومة التي تتمتع بمستوى مرتفع من الحماية التقنية قد تتعرض للخطر إذا غابت السياسات الواضحة، أو لم تحدد المسؤوليات والصلاحيات، أو لم توجد إجراءات منظمة للتعامل مع الحوادث والتسجيلات.

وتؤكد الأطر المهنية الحديثة في إدارة أمن المعلومات والخصوصية أهمية الجمع بين التدابير التقنية والتنظيمية، بحيث لا ينظر إلى أمن النظام باعتباره وظيفة للأجهزة والبرمجيات وحدها، وإنما باعتباره نتيجة لتكامل السياسات والإجراءات والمسؤوليات والضوابط التقنية .كما توصي الإرشادات المتخصصة في أنظمة المراقبة المرئية بتحديد المسؤول عن إدارة النظام وتشغيله، وأغراض استخدام المراقبة، ومدة الاحتفاظ بالتسجيلات، ومن يحق له الوصول إليها، وإجراءات التعامل مع الحوادث وطلبات الحصول على التسجيلات Eedpb.europa.eu+1 .

ومن ثم، فإن الضوابط التنظيمية والإجرائية تمثل الإطار الذي يحول الحماية التقنية من مجموعة من الإجراءات المتفرقة إلى نظام مؤسسي قابل للإدارة والرقابة والمراجعة والمساءلة.

أولًا: مفهوم الضوابط التنظيمية والإجرائية

يمكن تعريف الضوابط التنظيمية والإجرائية في منظومة المراقبة بأنها:

مجموعة السياسات والقواعد والإجراءات والمسؤوليات التي تنظم تشغيل منظومة المراقبة، وإدارة الوصول إليها، واستخدام بياناتها، وحمايتها، والتعامل مع الحوادث المرتبطة بها، بما يضمن استخدامها وفق الأهداف الأمنية والتنظيمية المعتمدة.

وتشمل هذه الضوابط الجوانب المتعلقة بمن يملك صلاحية تشغيل النظام، ومن يحق له مشاهدة التسجيلات أو تصديرها، وكيفية التعامل مع الأعطال والحوادث، وكيفية الاحتفاظ بالتسجيلات والتخلص منها، وكيفية مراجعة أداء المنظومة ومدى الالتزام بالسياسات المعتمدة. وتؤكد الإرشادات الأوروبية الخاصة بأجهزة الفيديو أهمية وجود سياسات وإجراءات تحدد المسؤوليات، وأغراض المراقبة، وفترات الاحتفاظ، والتدريب، وصلاحيات الوصول، وإجراءات الحوادث والاستعادةEedpb.europa.eu .

ثانيًا: أهمية الضوابط التنظيمية والإجرائية

تكتسب الضوابط التنظيمية والإجرائية أهميتها من كونها توفر الإطار الذي يحدد كيفية استخدام المنظومة وليس مجرد كيفية تشغيلها .ويمكن بيان أهميتها في الآتي:

1. تحديد المسؤوليات

تحدد الضوابط الجهة أو الأشخاص المسؤولين عن إدارة منظومة المراقبة وتشغيلها وصيانتها ومراجعة استخدامها.

2. تنظيم الصلاحيات

تحدد من يملك صلاحية المشاهدة أو الإدارة أو التصدير أو حذف التسجيلات، وبأي حدود.

3. الحد من الاستخدام غير المشروع

تسهم السياسات الواضحة في منع استخدام التسجيلات لأغراض لا تتفق مع الغرض الأمني المحدد للمنظومة.

4. توحيد الإجراءات

تضمن وجود طريقة موحدة للتعامل مع الحوادث والأعطال وطلبات التسجيلات وحفظ الأدلة.

5. تعزيز المساءلة

تجعل القرارات والإجراءات قابلة للتتبع والمراجعة، وتحدد المسؤولية عند حدوث مخالفة أو إساءة استخدام.

وتنسجم هذه المبادئ مع أطر إدارة الخصوصية والأمن التي تركز على الحوكمة، وإدارة المخاطر، وإدارة الهويات والصلاحيات، وحماية البيانات، والمراجعة المستمرة . NNIST+1

ثالثًا: السياسات الواجب توافرها

ينبغي أن تستند منظومة المراقبة إلى مجموعة من السياسات المكتوبة، ومن أهمها:

- سياسة استخدام منظومة المراقبة: تحدد أهداف استخدام النظام ونطاقه والأنشطة المسموح بها.
- سياسة إدارة المستخدمين والصلاحيات: تحدد مستويات الوصول وآليات منح الصلاحيات وسحبها.
- سياسة الاحتفاظ بالتسجيلات: تحدد مدد الاحتفاظ وفق الأهداف الأمنية والمتطلبات القانونية والتنظيمية.
- سياسة الوصول إلى التسجيلات: تحدد الحالات التي يجوز فيها الاطلاع على التسجيلات أو نسخها أو مشاركتها.
- سياسة التعامل مع الحوادث: تحدد الإجراءات الواجب اتباعها عند حدوث اختراق أو عبث أو فقدان للتسجيلات.
- سياسة الصيانة والتحديث: تنظم صيانة الأجهزة والبرمجيات وإدارة التحديثات.
- سياسة النسخ الاحتياطي والاستعادة: تحدد آليات النسخ الاحتياطي واختباره واستعادة الخدمة.
- سياسة التدريب والتوعية: تحدد متطلبات تدريب العاملين على تشغيل النظام وحماية بياناته.

ويؤكد دليل EDPB الخاص باستخدام أجهزة الفيديو ضرورة أن تتضمن سياسات المراقبة موضوعات مثل المسؤولية عن النظام، والغرض والنطاق، والاستخدامات المسموحة والمحظورة، ومدة التسجيل، والتدريب، وصلاحيات الوصول، والإجراءات

التشـــغيلية، والتعـامـل مع طلبـات الحصـــول على التســـجيلات، وإدارة الحوادث والاستعادةEedpb.europa.eu .

رابعًا: الإجراءات التشغيلية

لا تكفي الســـياســـات العامة وحدها، بل يجب تحويلها إلى إجراءات عملية قابلة للتطبيق. ومن أهم الإجراءات:

1. إجراءات بدء التشغيل

وتشـــمل التحقق من حالة الكاميرات وأجهزة التســـجيل والشـــبكات والأنظمة المرتبطة بها.

2. إجراءات المراقبة

وتحدد كيفية متابعة الشاشات والتعامل مع التنبيهات وتوثيق الأحداث المهمة.

3. إجراءات التعامل مع الحوادث

وتحدد كيفية اكتشـــاف الحادث، والإبلا غ عنه، وحفظ التســـجيلات ذات الصـــلة، وتصعيده إلى الجهة المختصة.

4. إجراءات تصدير التسجيلات

وتحدد من يملك صلاحية تصدير التسجيل، وكيفية توثيقه وحفظه، ومنع إجراء تغييرات غير مصرح بها عليه.

5. إجراءات الأعطال

تحدد كيفية التعامل مع تعطل الكاميرات أو أجهزة التســجيل أو الشـبكة، وآلية الإبلا غ عن الأعطال وإصلاحها.

6. إجراءات إنهاء صلاحية المستخدم

تتضـــمن إلغاء حســـابات المســـتخدمين الذين لم تعد لديهم حاجة وظيفية إلى النظام، خصوصًا عند تغيير الوظيفة أو انتهاء العلاقة الوظيفية.

خامسًا: التدريب والتوعية

يمثل العنصر البشري جزءًا أساسيًا من أمن منظومة المراقبة. ولذلك ينبغي ألا يقتصر التدريب على كيفية تشغيل الأجهزة، وإنما يشمل أيضًا:

- حماية بيانات الدخول.
- الاستخدام الصحيح للصلاحيات.
- التعامل مع التسجيلات.
- حماية سرية المعلومات.
- إجراءات الإبلاغ عن الحوادث.
- التعامل مع طلبات الحصول على التسجيلات.
- الالتزام بسياسات الخصوصية.
- مخاطر مشاركة التسجيلات أو نسخها خارج الإجراءات المعتمدة.

وتشير أطر NIST المتعلقة بالخصوصية إلى أهمية إدماج الوعي والتدريب ضمن حوكمة مخاطر الخصوصية، إلى جانب السياسات والإجراءات والمراقبة والمراجعةNNIST .

سادسًا: المراجعة والتدقيق

ينبغي مراجعة الضوابط التنظيمية والإجرائية بصورة دورية للتأكد من استمرار ملاءمتها للمنظومة والمخاطر القائمة.

وتشمل عملية المراجعة:

- مراجعة حسابات المستخدمين.
- مراجعة الصلاحيات.
- مراجعة سجلات الدخول والاستخدام.
- مراجعة الحوادث الأمنية.
- مراجعة مدة الاحتفاظ بالتسجيلات.
- مراجعة إجراءات النسخ الاحتياطي والاستعادة.
- تقييم مدى الالتزام بالسياسات.

- تحديث الإجراءات عند تغير المخاطر أو التقنية أو المتطلبات التنظيمية.

وتدعم أطر NIST هذا الاتجاه من خلال التركيز على الحوكمة، وإدارة المخاطر، والمراقبة والمراجعة المستمرة، بدل التعامل مع الضوابط باعتبارها إجراءات ثابتة لا تحتاج إلى تحديث NNIST+1 .

سابعًا: مبدأ الفصل بين المهام

من الضوابط المهمة عدم ترك جميع الصلاحيات في يد مستخدم واحد دون رقابة. ولذلك يستحسن، بحسب حجم المنشأة وطبيعة المخاطر، الفصل بين بعض الوظائف، مثل:

- إدارة النظام.
- المراقبة التشغيلية.
- إدارة المستخدمين.
- تصدير التسجيلات.
- مراجعة سجلات الاستخدام.
- التحقيق في الحوادث.

ويهدف هذا الفصل إلى تقليل احتمالات إساءة استخدام الصلاحيات، كما ينسجم مع مبادئ أقل قدر من الصلاحيات والفصل بين المهام التي ترد في أطر الأمن والخصوصية الحديثة NNIST Publications .

المراجع:

(1) European Data Protection Board, *Guidelines 3/2019 on processing of personal data through video devices*, Final Version, 30 January 2020، ولا سيما الجزء المتعلق بالضوابط التنظيمية والتقنية في أنظمة المراقبة بالفيديو Eedpb.europa.eu+1 .

(2) National Institute of Standards and Technology, *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management*, Version 1. 0, 2020. NNIST Computer Security Resource Center+1

(3) European Data Protection Board, *Guidelines 3/2019*, Section 9.3. 1، بشأن سياسات وإجراءات أنظمة المراقبة بالفيديو . Eedpb.europa.eu

(4) National Institute of Standards and Technology, *NIST Privacy Framework*, Core، وخاصة مجالات الحوكمة وإدارة السياسات والوعي والتدريب والمراقبة والمراجعة NNIST .

(5) National Institute of Standards and Technology, *NIST Privacy Framework*, PR.AC-P، بشأن إدارة الهويات والصلاحيات ومبدأ أقل قدر من الصلاحيات والفصل بين المهام NNIST Publications .

المبحث التاسع: الخصوصية والمسؤولية المهنية

تعد الخصوصية من أكثر القضايا حساسية في منظومة المراقبة، لأن تشغيل الكاميرات يؤدي بطبيعته إلى جمع ومعالجة معلومات يمكن أن ترتبط بالأفراد بصورة مباشرة أو غير مباشـــرة. ومن ثم، فإن تحقيق الهدف الأمني للمراقبة لا ينبغي أن يكون منفصـــلًا عن حماية حقوق الأفراد ومراعاة الحدود المهنية والقانونية لاستخدام المنظومة.

ولا يعني ذلك أن وجود كاميرات المراقبة يمثل في ذاته انتهاكًا للخصـــوصـــية، وإنما تتحدد مشـــروعية الاســـتخدام ومدى قبوله وفق الغرض من المراقبة، ونطاقها، ومكانها، وطريقة تشغيلها، والبيانات التي تجمعها، ومدة الاحتفاظ بها، والجهات التي تستطيع الوصول إليها.

وتؤكد المبادئ الدولية والإرشـــادات المهنية الخاصـــة بالمراقبة بالفيديو أهمية تحديد الغرض المشـــروع، وتقليل البيانات إلى القدر اللازم، والشـــفافية، وتقييد الوصـــول إلى التســـجيلات، وتحديد مدد الاحتفاظ، واتخاذ تدابير تقنية وتنظيمية لحماية البيانات.

كما يقدم إطار NIST للخصوصية منهجًا قائمًا على إدارة مخاطر الخصوصية بدل النظر إليها باعتبارها مسألة قانونية منفصلة عن إدارة المخاطر المؤسسية NNIST+1 .

أولًا: مفهوم الخصوصية في منظومة المراقبة

يمكن تعريف الخصوصية في سياق المراقبة الأمنية بأنها:

حق الأفراد في ألا تخضـــع معلوماتهم الشـــخصـــية أو صـــورهم أو أنماط حركتهم وممارساتهم للمراقبة أو الجمع أو الاستخدام أو الإفصاح بصورة تتجاوز الغرض الأمني المشروع أو الحدود النظامية والمهنية المقررة.

وتتخذ الخصوصية في أنظمة المراقبة أبعادًا متعددة، من أهمها:

- خصوصية المكان.
- خصوصية الأشخاص.
- سرية التسجيلات.

- التحكم في الوصول إلى المعلومات.
- الحد من استخدام التسجيلات خارج الغرض المحدد.
- حماية التسجيلات من الإفشاء أو الاستخدام غير المصرح به.

وتتعامل إرشادات EDPB مع بيانات الفيديو بوصفها قد تتضمن بيانات شخصية، وتتناول مسائل المشروعية والشفافية والإفصاح للغير والبيانات الحساسة واستخدام التقنيات الذكية في المراقبةEedpb.europa.eu .

ثانيًا: مبدأ الغرض المحدد

من أهم الضوابط المهنية أن يكون للمراقبة غرض محدد ومشروع وواضح.

فعلى سبيل المثال، إذا أنشئت منظومة مراقبة لحماية منشأة ومنع الدخول غير المصرح به، فلا ينبغي تحويل التسجيلات تلقائيًا إلى أغراض أخرى لا ترتبط بالغرض الأصلي، إلا في الحدود التي يسمح بها النظام القانوني والسياسات المعتمدة.

ويؤكد EDPB أن استخدام المراقبة يجب أن يرتبط بغرض واضح، وأن المنظمة ينبغي أن تحدد الغرض والنطاق والاستخدامات المسموحة والمحظورة ضمن سياساتها وإجراءاتهاEedpb.europa.eu .

ثالثًا: مبدأ التناسب وتقليل التدخل

لا ينبغي أن يكون الهدف من حماية المنشأة مبررًا لاستخدام مراقبة أوسع من الحاجة الفعلية. ولذلك ينبغي تحقيق التوازن بين:

الحاجة الأمنية ← مستوى المراقبة ← أثر المراقبة على الخصوصية.

ويعني ذلك أن اختيار أماكن الكاميرات ونطاق التصوير ومستوى التحليل ومدة الاحتفاظ بالتسجيلات ينبغي أن يرتبط بالمخاطر والأهداف الأمنية الفعلية.

وتبرز إرشادات EDPB أهمية اختبار الضرورة والتناسب عند استخدام المراقبة، بحيث لا تستخدم المراقبة إذا كان الهدف الأمني يمكن تحقيقه بطريقة أقل تدخلاً، وبحيث يقتصر جمع البيانات على ما يلزم للغرض المحددEedpb.europa.eu+1 .

رابعًا: المناطق التي تتطلب عناية خاصة

تتطلب بعض الأماكن مستوى أعلى من الحذر بسبب طبيعتها وارتباطها المباشر بالخصوصية.

ومن أمثلتها:

- دورات المياه.
- غرف تبديل الملابس.
- الأماكن المخصصة للخصوصية الشخصية.
- بعض الأماكن الطبية.
- بعض الأماكن المخصصة للراحة الشخصية.

ولا ينبغي أن يكون تركيب الكاميرات في هذه الأماكن إجراءً اعتياديًا، بل يجب إخضاعه لأعلى درجات التقييم القانوني والمهني، وقد يكون محظورًا بحسب النظام القانوني المطبق.

كما ينبغي تجنب توجيه الكاميرات إلى مناطق لا تدخل ضمن الحاجة الأمنية للمنشأة، متى كان بالإمكان تحقيق الهدف الأمني دون ذلك.

خامسًا: الشفافية والإعلام

تتطلب الممارسة المهنية الرشيدة إعلام الأشخاص بوجود المراقبة عندما يكون ذلك مطلوبًا قانونًا أو مناسبًا وفق طبيعة المنشأة.

وتشمل الشفافية، بحسب السياق القانوني والتنظيمي:

- بيان وجود المراقبة.
- تحديد الغرض منها.
- توضيح الجهة المسؤولة عنها.
- بيان كيفية التعامل مع البيانات.
- توضيح مدة الاحتفاظ متى كان ذلك مطلوبًا.
- توفير المعلومات المتعلقة بحقوق الأفراد وفق القانون المطبق.

وتعد الشفافية من المبادئ الأساسية في إرشادات EDPB الخاصة بأجهزة الفيديو، كما ترتبط ضمن إطار NIST للخصوصية بإدارة المخاطر والتواصل مع الأفراد والجهات المعنية1+Eedpb.europa.eu .

سادسًا: حماية التسجيلات من الاستخدام غير المشروع

لا تنتهي مسؤولية الخصوصية بمجرد تسجيل الصورة، وإنما تمتد إلى كل دورة حياة التسجيل، بما في ذلك:

١. الجمع.
٢. النقل.
٣. التخزين.
٤. المشاهدة.
٥. النسخ.
٦. التصدير.
٧. المشاركة.
٨. الأرشفة.
٩. الحذف.

ومن ثم يجب حماية التسجيلات من الوصول غير المصرح به أو التعديل أو الفقد أو الاستخدام خارج الغرض المحدد.

وتؤكد الإرشادات الأوروبية الخاصة بالمراقبة أن أمن النظام يتطلب حماية مادية لمكونات النظام، وسلامة النظام ومقاومته للتدخل، وضبط الوصول، إلى جانب حماية سرية البيانات وسلامتها وتوافرهاEedpb.europa.eu .

سابعًا: الوصول إلى التسجيلات والإفصاح عنها

يجب ألا يكون الوصول إلى التسجيلات متاحًا لجميع العاملين في المنشأة، وإنما ينبغي أن يخضع لمبدأ الحاجة إلى المعرفة والصلاحيات المحددة.

وينبغي تنظيم:

- من يحق له مشاهدة التسجيلات.
- من يحق له تصديرها.
- الحالات التي يجوز فيها مشاركتها.
- الجهات التي يمكن تزويدها بالتسجيلات.
- طريقة توثيق طلبات التسجيل.
- آلية رفض الطلبات غير المصرح بها.
- تسجيل عمليات الوصول والتصدير.

وتشير الإرشادات المتخصصة إلى ضرورة تحديد من يمكنه الوصول إلى التسجيلات ولأي أغراض، وكذلك وضع إجراءات للتعامل مع طلبات الحصول على التسجيلات من الجهات الخارجيةEedpb.europa.eu .

ثامنًا: مدة الاحتفاظ بالتسجيلات

تمثل مدة الاحتفاظ أحد أهم عناصر إدارة خصوصية التسجيلات.

فليس من الممارسة الرشيدة الاحتفاظ بكل التسجيلات إلى أجل غير محدد دون مبرر، كما أن تقليل مدة الاحتفاظ لا ينبغي أن يؤدي إلى فقدان تسجيلات ضرورية لتحقيق هدف أمني مشروع أو التحقيق في حادث وقع بالفعل.

ومن ثم ينبغي أن تحدد مدة الاحتفاظ وفق:

- الغرض من التسجيل.
- طبيعة المخاطر.
- المتطلبات القانونية والتنظيمية.
- طبيعة المنشأة.
- الحاجة إلى التحقيق في الحوادث.
- إمكانية تمديد الاحتفاظ بالتسجيل المرتبط بحادث أو إجراء رسمي.

وتؤكد الإرشادات المتخصصة ضرورة تحديد مدة الاحتفاظ بالتسجيلات، مع وضع ترتيبات خاصة للتسجيلات المرتبطة بالحوادث الأمنية عند الحاجة .
Eedpb.europa.eu

تاسعًا: المسؤولية المهنية للعاملين
لا تقتصر المسؤولية المهنية على الإدارة العليا أو الجهة المالكة للنظام، وإنما تشمل كل شخص يشارك في تشغيل منظومة المراقبة أو الوصول إلى بياناتها.
وتشمل المسؤولية المهنية للعاملين:
1. السرية
عدم إفشاء التسجيلات أو المعلومات المتعلقة بها إلى غير المصرح لهم.
2. النزاهة
عدم تعديل التسجيلات أو حذفها أو التلاعب بها خارج الإجراءات المقررة.
3. الالتزام
العمل وفق السياسات والإجراءات المعتمدة.
4. الحياد
عدم استخدام التسجيلات لتحقيق أغراض شخصية أو غير مهنية.
5. المساءلة
تحمل المسؤولية عن الأفعال التي تقع ضمن نطاق الصلاحيات الممنوحة للمستخدم.
6. الإبلاغ
الإبلاغ عن أي حادث أو إساءة استخدام أو محاولة للوصول غير المصرح به.
وتنسجم هذه المبادئ مع متطلبات إدارة الهوية والصلاحيات والمساءلة الواردة في الأطر الأمنية والخصوصية، التي تؤكد أهمية إدارة الحسابات والاعتمادات والصلاحيات ومراجعتها وتدقيقها1+NIST Publications N .

عاشرًا: استخدام تقنيات التحليل الذكي والبيانات الحساسة

أدى التطور التقني إلى إدخال تقنيات أكثر تقدمًا في منظومات المراقبة، مثل التعرف على الوجوه وتحليل السلوك والتعرف الآلي على الأشخاص أو المركبات.

وتزداد الحساسية المهنية والخصوصية عند استخدام هذه التقنيات؛ لأنها قد تنتج معلومات أكثر تفصيلًا عن الأفراد مقارنة بالتسجيل المرئي التقليدي.

ولهذا ينبغي قبل استخدامها تقييم:

- الغرض من التقنية.
- ضرورتها لتحقيق الهدف الأمني.
- مستوى دقتها.
- مخاطر النتائج الخاطئة.
- نوع البيانات التي تنتجها.
- الجهات التي تستطيع الوصول إليها.
- مدة الاحتفاظ بها.
- المخاطر المحتملة على حقوق الأفراد.

وتتناول إرشادات EDPB بصورة خاصة التقنيات الذكية للمراقبة والمعالجة المرتبطة بالبيانات الحساسة، بما يؤكد أن الانتقال من التسجيل التقليدي إلى التحليل الآلي يرفع مستوى الحاجة إلى التقييم والضبط Eedpb.europa.eu+1 .

حادي عشر: تقييم أثر الخصوصية

عندما تكون منظومة المراقبة أو طريقة استخدامها مرجحة لإحداث مخاطر مرتفعة على حقوق الأفراد، ينبغي إجراء تقييم مناسب لأثر الخصوصية وفق الإطار القانوني المطبق.

وتتمثل قيمة هذا التقييم في أنه يسمح بتحديد:

1. السرية

عدم إفشاء التسجيلات أو المعلومات المتعلقة بها إلى غير المصرح لهم.

تحمل المسؤولية عن الأفعال التي تقع ضمن نطاق الصلاحيات الممنوحة للمستخدم.

6. الإبلاغ

الإبلاغ عن أي حادث أو إساءة استخدام أو محاولة للوصول غير المصرح به.

وتنسجم هذه المبادئ مع متطلبات إدارة الهوية والصلاحيات والمساءلة الواردة في الأطر الأمنية والخصوصية، التي تؤكد أهمية إدارة الحسابات والاعتمادات والصلاحيات ومراجعتها وتدقيقها.

عاشرًا- التقني إلى إدخال تقنيات أكثر تقدمًا في منظومات المراقبة، مثل التع تكون منظومة المراقبة أو طريقة استخدامها مرجحة لإحداث مخاطر مرتفعة على حقوق الأفراد،وصية تبدأ من تحديد الغرض من المراقبة، وتمتد إلى اختيار مواقع الكاميرات، وتقليل نطاق التصوير، وتنظيم الوصول إلى التسجيلات، وتحديد مدة الاحتفاظ نفسه، مع تدقيق المراجع وتوحيد المصطلحات والأسلوب الأكاديمي في: استخدام تقنيات التحليل الذكي والبيانات الحساسة

أدى التطور التقني إلى إدخال تقنيات أكثر تقدمًا في منظومات المراقبة، مثل التعرف على الوجوه وتحليل السلوك والتعرف الآلي على الأشخاص أو المركبات.

وتزداد الحساسية المهنية والخصوصية عند استخدام هذه التقنيات؛ لأنها قد تنتج معلومات أكثر تفصيلًا عن الأفراد مقارنة بالتسجيل المرئي التقليدي.

ولهذا ينبغي قبل استخدامها تقييم:

- الغرض من التقنية.
- ضرورتها لتحقيق الهدف الأمني.
- مستوى دقتها.
- مخاطر النتائج الخاطئة.
- نوع البيانات التي تنتجها.
- الجهات التي تستطيع الوصول إليها.
- مدة الاحتفاظ بها.
- المخاطر المحتملة على حقوق الأفراد.

وتتناول إرشادات EDPB بصورة خاصة التقنيات الذكية للمراقبة والمعالجة المرتبطة بالبيانات الحساسة، بما يؤكد أن الانتقال من التسجيل التقليدي إلى التحليل الآلي يرفع مستوى الحاجة إلى التقييم والضبط.

- طبيعة البيانات التي ستجمع.
- الغرض من جمعها.
- المخاطر المحتملة.
- الأشخاص المتأثرين.
- وسائل تقليل المخاطر.
- مدى ضرورة النظام وتناسبه.
- الضوابط التقنية والتنظيمية المطلوبة.

ويشير إطار NIST للخصوصية إلى أهمية تحديد مخاطر الخصوصية وإدارتها ضمن عملية إدارة مخاطر مؤسسية، كما تتطلب أطر قانونية معينة، مثل GDPR في نطاق تطبيقه، تقييم أثر حماية البيانات في حالات محددة مرتفعة المخاطرNNIST+1 .

ثاني عشر: التوازن بين الأمن والخصوصية

لا ينبغي النظر إلى الأمن والخصوصية على أنهما هدفان متعارضان بصورة مطلقة؛ إذ يمكن تصميم منظومة تحقق مستوى مناسبًا من الحماية الأمنية مع تقليل التدخل غير الضروري في خصوصية الأفراد.

ويتحقق ذلك من خلال:

ثاني عشر: التوازن بين الأمن والخصوصية

لا ينبغي النظر إلى الأمن والخصوصية على أنهما هدفان متعارضان بصورة مطلقة؛ إذ يمكن تصميم منظومة تحقق مستوى مناسبًا من الحماية الأمنية مع تقليل التدخل غير الضروري في خصوصية الأفراد.

ويتحقق ذلك من خلال:

- تحديد الغرض الأمني بدقة.

- اختيار أقل وسائل المراقبة تدخلاً متى كانت كافية.
- تحديد نطاق التصوير.
- تقييد الوصول.
- تقليل مدة الاحتفاظ.
- حماية التسجيلات.
- توثيق الاستخدام.
- مراجعة النظام بصورة دورية.
- تقييم مخاطر الخصوصية قبل إدخال التقنيات الجديدة.

وبذلك تصبح الخصوصية جزءًا من تصميم المنظومة وليس إجراءً لاحقًا يضاف بعد تشغيلها.

المراجع:

خلاصة الفصل الرابع

يتضح من دراسة أمن منظومة المراقبة وحمايتها أن أمن الكاميرات لا يمكن اختزاله في حماية الأجهزة من السرقة أو التلف، بل يمثل عملية متكاملة تشمل المكونات والأشخاص والشبكات وأجهزة التسجيل والبيانات والنسخ الاحتياطية واستمرارية الخدمة.

وقد أظهر الفصل أن حماية مكونات المنظومة تمثل نقطة البداية، إلا أنها لا تكفي بمفردها؛ إذ إن الحسابات والصلاحيات تمثل أحد المسارات المهمة التي يمكن من خلالها الوصول إلى النظام، ولذلك فإن تطبيق مبدأ أقل قدر من الصلاحيات، وإدارة الحسابات، والمصادقة المناسبة، وتسجيل الأنشطة، يمثل جزءًا أساسيًا من الحماية.

كما تبين أن الشبكة التي تربط مكونات المنظومة تحتاج إلى حماية مستقلة، من خلال التقسيم والتحكم في الاتصالات وحماية البيانات أثناء النقل وتحديث مكونات الشبكة ومراقبتها.

وأظهر التحليل كذلك أن أجهزة التسجيل والتخزين تمثل أصولًا عالية القيمة، وأن حمايتها ينبغي أن تجمع بين الحماية المادية والتقنية. كما أن التسجيلات نفسها تحتاج إلى حماية تضمن السرية والسلامة والتوافر، مع تنظيم عمليات الاحتفاظ والحذف والتصدير.

ويمثل النسخ الاحتياطي واستمرارية الخدمة عنصرًا مكملًا للحماية، إذ لا يكفي منع الحوادث، وإنما يجب أن تكون المنشأة قادرة على استعادة البيانات والخدمات عند وقوع الأعطال أو الحوادث.

وأخيرًا، فإن مخاطر العبث والتلاعب تؤكد أن أمن المنظومة يجب أن يقوم على ثلاث حلقات مترابطة: الوقاية، والكشف، والاستجابة.

ويمكن صياغة النموذج المتكامل لأمن منظومة المراقبة على النحو الآتي:

حماية المكونات ← إدارة الهوية والصلاحيات ← حماية الشبكات ← حماية التسجيل ← النسخ الاحتياطي واستمرارية الخدمة ← اكتشاف العبث ← الاستجابة والتعافي

ومن ثم فإن السؤال الأمني الصحيح لا ينبغي أن يكون : هل منظومة المراقبة محمية؟ وإنما :إلى أي مدى تستطيع المنظومة المحافظة على سرية التسجيلات وسلامتها وتوافرها واستمرارية وظائفها في مواجهة الأخطاء والاختراقات والعبث والأعطال؟

أهم نتائج الفصل الرابع

١. أمن منظومة المراقبة يتجاوز الحماية المادية للك ameras والأجهزة.
٢. جميع مكونات المنظومة تمثل جزءًا من سطح الحماية.
٣. الكاميرات الشبكية تحتاج إلى ضوابط أمنية باعتبارها أجهزة متصلة بالشبكة.
٤. إدارة المستخدمين والصلاحيات عنصر أساسي في حماية المنظومة.
٥. ينبغي تطبيق مبدأ أقل قدر من الصلاحيات.
٦. الحسابات الفردية تعزز المساءلة وتتبع الأنشطة.
٧. حماية الشبكة جزء لا يتجزأ من حماية منظومة المراقبة.
٨. تقسيم الشبكة يمكن أن يقلل نطاق انتشار التهديدات.
٩. أجهزة التسجيل والتخزين تمثل أصولًا عالية القيمة.
١٠. التسجيلات تحتاج إلى حماية السرية والسلامة والتوافر.
١١. ينبغي تنظيم الاحتفاظ بالتسجيلات وحذفها وتصديرها.
١٢. النسخ الاحتياطي ضروري لمواجهة فقدان البيانات.
١٣. اختبار الاستعادة عنصر أساسي في التحقق من فعالية النسخ الاحتياطي.
١٤. استمرارية الخدمة تتطلب الاستعداد للأعطال والحوادث.
١٥. العبث قد يكون ماديًا أو تقنيًا أو إداريًا.
١٦. يجب أن تشمل الحماية القدرة على اكتشاف العبث وليس منعه فقط.
١٧. إدارة حوادث العبث ينبغي أن تشمل الوقاية والكشف والاستجابة والتعافي.
١٨. حماية منظومة المراقبة عملية مستمرة وليست إجراءً لمرة واحدة.

أسئلة التفكير والتقييم للفصل الرابع

أولًا: أسئلة معرفية

١. ما المقصود بأمن منظومة المراقبة؟
٢. ما أهم مكونات منظومة المراقبة التي تحتاج إلى الحماية؟
٣. لماذا تحتاج الكاميرات الشبكية إلى حماية سيبرانية؟
٤. ما المقصود بمبدأ أقل قدر من الصلاحيات؟
٥. ما أهمية إدارة حسابات المستخدمين؟
٦. ما المقصود بتقسيم شبكة المراقبة؟
٧. لماذا تعد أجهزة التسجيل من الأصول الحساسة؟
٨. ما المقصود بسرية التسجيلات وسلامتها وتوافرها؟
٩. ما أهمية النسخ الاحتياطي؟
١٠. ما المقصود باستمرارية الخدمة؟
١١. ما صور العبث بمنظومة المراقبة؟
١٢. ما المقصود بالتلاعب بالتسجيلات؟

ثانيًا: أسئلة تحليلية

١. حلل العلاقة بين حماية المكونات وأمن المنظومة ككل.
٢. لماذا لا تكفي حماية الكاميرات ماديًا لتحقيق أمن المنظومة؟
٣. حلل أهمية مبدأ أقل قدر من الصلاحيات في منظومات المراقبة.
٤. كيف يمكن أن يؤدي اختراق حساب مستخدم إلى تهديد التسجيلات؟
٥. حلل أهمية تقسيم شبكة المراقبة.
٦. لماذا تمثل أجهزة التسجيل هدفًا مهمًا للمهاجم؟
٧. حلل العلاقة بين سرية التسجيلات وسلامتها وتوافرها.
٨. لماذا ينبغي اختبار النسخ الاحتياطية بدل الاكتفاء بإنشائها؟
٩. حلل مخاطر العبث المادي والتقني بمنظومة المراقبة.
١٠. لماذا ينبغي أن تجمع حماية المنظومة بين الوقاية والكشف والاستجابة؟

ثالثًا: أسئلة تطبيقية

١. اختر منشأة تعرفها، وحدد أهم مكونات منظومة المراقبة التي تحتاج إلى الحماية.
٢. صمم سياسة لإدارة المستخدمين والصلاحيات في منظومة مراقبة أمنية.
٣. ضع تصورًا لتقسيم شبكة منظومة المراقبة عن الشبكات الأخرى.
٤. صمم إجراءات لحماية أجهزة التسجيل.
٥. ضع سياسة لحماية التسجيلات والاحتفاظ بها وتصديرها.
٦. صمم خطة للنسخ الاحتياطي واستعادة التسجيلات.
٧. ضع خطة لاستمرارية خدمة منظومة المراقبة عند انقطاع الطاقة أو تعطل أجهزة التسجيل.
٨. صمم إجراءً لاكتشاف العبث بإحدى الكاميرات.
٩. ضع سيناريو للتعامل مع حذف تسجيلات أمنية بصورة غير مصرح بها.
١٠. صمم إطارًا متكاملًا لحماية منظومة المراقبة من العبث والتلاعب.

الباب الرابع:
تقييم الفاعلية والتطبيقات

الفصل الأول: فاعلية منظومة كاميرات المراقبة

تمهيد الفصل

تمثل فاعلية منظومة كاميرات المراقبة المرحلة التي تنتقل فيها الدراسة من تحليل مكونات المنظومة ووظائفها التشغيلية إلى الحكم على مدى إسهامها الفعلي في تحقيق الأهداف الأمنية للمنشأة .فوجود عدد من الكاميرات، أو ارتفاع دقة التسجيل، أو استمرار عمل أجهزة التسجيل، لا يكفي منفردًا للحكم بأن المنظومة فعالة؛ إذ إن الحكم على الفاعلية يتطلب الربط بين الأهداف الأمنية المحددة، والمتطلبات الوظيفية، وقدرات المنظومة الفنية والتشغيلية، والنتائج التي تتحقق في بيئة الاستخدام الفعلية. ويؤكد منهج NIST في تحديد متطلبات جودة الفيديو أهمية البدء بحالة الاستخدام والمهمة المراد إنجازها قبل تحديد متطلبات جودة الصورة ومكونات النظام NNIST+1 .

كما أن معيار IEC 62676-4:2025 يعالج منظومات المراقبة بالفيديو من منظور دورة حياتها، بما يشمل التخطيط والتصميم والتركيب والاختبار والتشغيل والصيانة، وهو ما يدعم النظر إلى الفاعلية باعتبارها نتيجة لتكامل عناصر متعددة، لا نتيجة لمواصفة فنية منفردة IIEC Webstore .

وتؤكد الأدلة التطبيقية كذلك أن أثر المراقبة بالفيديو لا يكون متجانسًا في جميع البيئات أو الأهداف؛ فقد وجدت مراجعات منهجية أن أثر CCTV على الجريمة يختلف باختلاف نوع الجريمة، ودرجة التغطية، والمراقبة النشطة، ومدى اقترانه بتدخلات أمنية أخرى. ولذلك ينبغي تجنب التعامل مع "الفاعلية" بوصفها خاصية ثابتة للكاميرا نفسها Ccollege.police.uk+1 .

وعليه، يتناول هذا الفصل مفهوم الفاعلية، ويميز بينها وبين مجرد وجود المنظومة وكفاءتها الفنية والتشغيلية، ثم يعرض مؤشرات قياسها، وعوامل نجاحها، وأسباب انخفاضها، وينتهي بمنهجية عملية لتقييم الأداء الفعلي، مع إدخال أبعاد قانونية واقتصادية وتحليلية تساعد على تكوين حكم أكثر شمولًا.

المبحث الأول: مفهوم الفاعلية

لا يمكن تقييم فاعلية منظومة كاميرات المراقبة قبل تحديد المقصود بالفاعلية وتحديد علاقتها بالأهداف الأمنية التي أنشئت المنظومة من أجل تحقيقها. فالفاعلية لا تعني مجرد عمل الأجهزة، وإنما ترتبط بالنتائج الأمنية التي تتحقق بالفعل.

أولًا: مفهوم الفاعلية الأمنية

يمكن تعريف الفاعلية الأمنية لمنظومة كاميرات المراقبة بأنها:

مدى إسهام المنظومة، في ظروف التشغيل الفعلية، في تحقيق الأهداف الأمنية المحددة للمنشأة من خلال الوقاية والكشف ودعم الاستجابة والتوثيق والتحقيق، وفق مستوى الأداء المطلوب.

وهذا التعريف يمثل صياغة تحليلية إجرائية للباحث، وليس تعريفًا معياريًا منسوبًا حرفيًا إلى معيار بعينه.

ويستند هذا التصور إلى مبدأ عام في قياس الأداء الأمني يتمثل في ربط القياسات بالأهداف والنتائج المطلوبة، واستخدام البيانات الكمية والنوعية للحكم على مدى كفاية الضوابط الأمنية وأدائها NNIST+1 .

ثانيًا: الفاعلية باعتبارها علاقة بين الأهداف والنتائج

يمكن فهم الفاعلية من خلال العلاقة الآتية:

الأهداف الأمنية ← المتطلبات ← قدرات المنظومة ← الأداء الفعلي ← النتائج الأمنية

فإذا كان الهدف هو حماية مدخل حساس، فلا يكفي إثبات وجود كاميرا عند المدخل؛ بل يجب التحقق من أن الكاميرا توفر المعلومات المطلوبة للتعرف أو الكشف، وأن التسجيل متاح عند الحاجة، وأن المشغل يستطيع استخدامه، وأن المعلومات الناتجة تسهم في الاستجابة أو التحقيق.

ومن ثم، فإن الفاعلية ترتبط بالسؤال:

إلى أي مدى تحققت النتيجة الأمنية المطلوبة؟

وليس بالسؤال:

هل توجد معدات تعمل؟

ثالثًا: أنواع الفاعلية

أقسام فاعلية منظومة المراقبة إلى خمسة أبعاد رئيسية:

1. الفاعلية الوقائية

وهي مدى إسهام المنظومة في تقليل فرص وقوع بعض الأحداث الأمنية، بما في ذلك أثر المراقبة الظاهرة أو استخدامها ضمن منظومة أمنية أوسع.

ولا يجوز افتراض أن وجود الكاميرات يؤدي حتمًا إلى منع الجريمة؛ فالأدلة التجريبية تشير إلى تفاوت أثر CCTV باختلاف البيئة ونوع الجريمة وطريقة التشغيل . Ccollege.police.uk

2. الفاعلية الكشفية

وهي مدى قدرة المنظومة على توفير المعلومات اللازمة لاكتشاف الأحداث أو الأنشطة ذات الدلالة الأمنية في الوقت المناسب.

3. الفاعلية الاستجابية

وهي مدى إسهام المعلومات التي توفرها المنظومة في دعم اتخاذ القرار وتوجيه الاستجابة المناسبة.

4. الفاعلية التوثيقية

وهي مدى قدرة المنظومة على إنتاج تسجيلات قابلة للاسترجاع والاستخدام في المراجعة والتحليل والتحقيق.

5. الفاعلية التحقيقية

وهي مدى إسهام التسجيلات والمعلومات المرتبطة بها في إعادة بناء الأحداث ودعم إجراءات التحقيق، مع مراعاة متطلبات سلامة البيانات والإجراءات القانونية المعمول بها.

وتدعم الأدلة المهنية في مجال الفيديو الجنائي أهمية تأمين التسجيلات وفهرستها وتخزينها والمحافظة على سلامتها وقيمتها الإثباتية Office of Justice O . Programs+1

رابعًا: الفاعلية ليست قيمة مطلقة

لا يصح وصف منظومة بأنها "فعالة" بصورة مطلقة دون تحديد:

- الهدف الأمني.
- نوع المنشأة.
- طبيعة المخاطر.
- المنطقة محل التقييم.
- الفترة الزمنية.
- مستوى الأداء المطلوب.
- الموارد البشرية المتاحة.
- الأنظمة الأمنية المرتبطة بها.

وبالتالي، فإن منظومة قد تكون مناســـبة لتحقيق هدف معين، لكنها غير كافية لتحقيق هدف آخر.

المبحث الثاني: الفرق بين وجود المنظومة وكفاءتها

يمثل الخلط بين وجود المنظومة وفاعليتها أحد أكثر مصـــادر الخطأ في تقييم أنظمة المراقبة. فقد تكون المنظومة مكتملة من الناحية المادية، ولكنها تعاني من قصـــور في الأداء أو التغطية أو التشغيل.

أولًا: وجود المنظومة

يقصد بوجود المنظومة توافر مكوناتها الأساسية وتركيبها في المواقع المحددة، مثل:

- الكاميرات.
- أجهزة التسجيل.
- الشبكات.
- شاشات العرض.
- البرمجيات.
- مصادر الطاقة.
- وسائل التخزين.
- التجهيزات المساندة.

ويمثل ذلك شـــرطًا أوليًا للتشـــغيل، لكنه لا يمثل دليلًا بذاته على تحقيق الأهداف الأمنية.

ثانيًا: الكفاءة الفنية

يقصـــد بالكفاءة الفنية قدرة المكونات على أداء وظائفها الفنية وفق المتطلبات المحددة، مثل:

١. جودة الصورة.
٢. دقة التسجيل.
٣. التغطية البصرية.
٤. الأداء في ظروف الإضاءة المختلفة.
٥. سلامة الاتصال.
٦. قدرة التخزين.

٧. استقرار الأجهزة.

ويولي NIST أهمية كبيرة لمطابقة جودة الفيديو مع المهمة المراد تنفيذها؛ فالجودة المطلوبة ليست قيمة مجردة، وإنما تتحدد بما يحتاج إليه المستخدم من معلومات لإنجاز المهمة المطلوبةNNIST+1 .

ثالثًا: الكفاءة التشغيلية

تتجاوز الكفاءة التشغيلية سلامة الأجهزة إلى قدرة المنظومة على العمل بصورة مناسبة في بيئة التشغيل الفعلية، بما يشمل:

- انتظام التشغيل.
- سرعة الوصول إلى المعلومات.
- قدرة العاملين على الاستخدام.
- الالتزام بالإجراءات.
- الصيانة.
- معالجة الأعطال.
- إدارة التسجيلات.
- الاستجابة للتنبيهات.

رابعًا: الفاعلية الأمنية

تمثل الفاعلية الأمنية المستوى الأعلى في هذا التسلسل؛ لأنها تسأل عن النتيجة الأمنية النهائية.

ويمكن تمثيل العلاقة على النحو الآتي:

وجود المنظومة ← الكفاءة الفنية ← الكفاءة التشغيلية ← الوظيفة الأمنية ← النتيجة الأمنية

وهذه العلاقة نموذج تحليلي مقترح في هذه الدراسة، وليست معادلة معيارية.

خامسًا: مثال توضيحي

إذا كانت المنشأة تمتلك عشر كاميرات عند مداخلها، فقد يكون ذلك دليلًا على وجود المنظومة.

لكن إذا كانت خمس كاميرات لا تعمل، أو كانت الإضـــاءة تمنع التعرف، أو كانت زاوية التصوير لا تغطي نقطة العبور المطلوبة، أو لم يستطع المشغل استرجاع التسجيل عند الحاجة، فإن وجود الكاميرات لا يتحول تلقائيًا إلى فاعلية أمنية.

المبحث الثالث: الفرق بين الكفاءة الفنية والفاعلية الأمنية

تعد جودة الأداء الفني عنصـــرًا مهمًا في منظومة المراقبة، لكنها لا تمثل وحدها معيارًا للحكم على النجاح الأمني. فقد تحقق المنظومة مســتويات فنية مرتفعة دون أن تحقق الهدف الأمني المطلوب.

أولًا: الكفاءة الفنية

تشمل الكفاءة الفنية مجموعة من المؤشرات، منها:

- جودة الصورة.
- الدقة.
- معدل الإطارات.
- جودة العرض.
- جودة التسجيل.
- الأداء في الإضاءة المنخفضة.
- استقرار الشبكة.
- قدرة التخزين.

ونوضـح أن متطلبات جودة الفيديو ينبغي أن تنطلق من حالة الاسـتخدام والمهمة، مثل التعرف على شخص أو قراءة لوحة مركبة أو اتخاذ قرار تكتيكي.

ثانيًا: الفاعلية الأمنية

تتعلق الفاعلية الأمنية بقدرة المنظومة على اســتخدام هذه الإمكانات لتحقيق نتيجة أمنية.

فعلى ســبيل المثال، قد تمتلك الكاميرا دقة عالية، ولكن إذا كان موقعها لا يتيح رؤية الوجه في نقطة العبور، فإن ارتفاع الدقة لا يعوض سوء التصميم.

ثالثًا: أمثلة على الفصل بين الكفاءة والفاعلية

الفاعلية الأمنية	الكفاءة الفنية	الحالة
منخفضة	مرتفعة	صورة عالية الجودة لمنطقة غير مهمة
منخفضة	منخفضة تشغيليًا	كاميرا مناسبة ولكنها متوقفة

الفاعلية الأمنية	الكفاءة الفنية	الحالة
قد تكون محدودة	جيدة	تغطية جيدة مع ضعف التشغيل البشري
مرتفعة نسبيًا	جيدة	صورة مناسبة مع استجابة سريعة
محدودة	جيدة جزئيًا	تسجيل جيد لكن يصعب استرجاعه

رابعًا: العلاقة بين الجودة والنتيجة

لا ينبغي النظر إلى جودة الصورة باعتبارها هدفًا نهائيًا، وإنما باعتبارها وسيلة لتحقيق مهمة أمنية محددة.

ومن هنا يمكن صياغة العلاقة:

الجودة الفنية المناسبة للمهمة + التغطية المناسبة + التشغيل الفعال + الاستجابة المناسبة = إمكانية أعلى لتحقيق النتيجة الأمنية

وهذه صياغة تحليلية وليست علاقة حسابية معيارية.

خامسًا: أثر المراقبة النشطة

ونشير من خلال الممارسة العملية الى أن بعض برامج كانت أكثر فاعلية عندما اقترنت بالمراقبة النشطة، كما ارتبطت الفاعلية بدرجة التغطية واستخدام مع تدخلات أمنية مكملة. ولا يعني ذلك أن هذه النتائج تنطبق بصورة آلية على كل منشأة، وإنما توضح أهمية السياق وطريقة التنفيذ .

المبحث الرابع: مؤشرات الفاعلية

لا يمكن إصـدار حكم موضـوعي على الفاعلية دون تحديد مؤشـرات قابلة للملاحظة والقياس والمقارنة. ولذلك ينبغي بناء نظام قياس يرتبط بالأهداف الأمنية ويجمع بين المؤشرات الفنية والتشغيلية والنتائجية.

وتشـير منهجية NIST الخاصـة بقياس الأداء إلى أهمية ربط القياسـات بالأهداف، وجمع البيانات وتحليلها واستخدامها في دعم القرارات وتحسين الأداءNNIST+1 .

أولًا: مؤشرات التغطية

تشمل:

- نسبة المناطق ذات الأولوية التي تغطيها الكاميرات.
- عدد النقاط العمياء.
- نسبة نقاط الدخول والخروج المغطاة.
- نسبة المناطق الحساسة المغطاة.

مؤشر مقترح لنسبة التغطية

نسبة التغطية = (عدد المناطق ذات الأولوية المغطاة ÷ إجمالي المناطق ذات الأولوية) × ١٠٠

وهذه معادلة قياس مقترحة في هذه الدراسة، وليست معادلة مفروضة في IEC.

ثانيًا: مؤشرات جودة المعلومات

تشمل:

- وضوح الصورة.
- إمكانية التعرف.
- إمكانية التمييز بين الأشخاص أو الأشياء.
- جودة التسجيل في ظروف الإضاءة المختلفة.
- استقرار الصورة.
- قابلية العرض والاسترجاع.

وتتوافق هذه الفكرة مع منهج VQiPS الذي يربط جودة الفيديو بالمهمة التي يتعين على المشاهد إنجازها1+NNIST .

ثالثًا: مؤشرات التوافر والاستمرارية

تشمل:

- نسبة التوافر.
- عدد الأعطال.
- مدة الانقطاع.
- متوسط زمن إصلاح الأعطال.
- نسبة الأنظمة الاحتياطية العاملة.

مؤشر مقترح للتوافر

نسبة التوافر = (زمن التشغيل الفعلي ÷ الزمن المطلوب للتشغيل) × ١٠٠

ويجب تحديد فترة القياس مسبقًا، مثل يوم أو شهر أو ربع سنة، حتى تكون المقارنة ذات معنى.

رابعًا: مؤشرات الكشف

يمكن قياسها من خلال:

- نسبة الأحداث التي اكتشفتها المنظومة.
- زمن اكتشاف الحدث.
- نسبة الإنذارات الصحيحة.
- معدل الإنذارات الكاذبة.
- نسبة الأحداث التي تم التعرف عليها وفق مستوى المعلومات المطلوب.

مؤشر مقترح لمعدل الكشف

معدل الكشف = (عدد الأحداث التي اكتشفتها المنظومة ÷ عدد الأحداث المعروفة التي كان ينبغي اكتشافها) × ١٠٠

ولا ينبغي استخدام هذا المؤشر دون وجود وسيلة موثوقة لتحديد "الأحداث التي كان ينبغي اكتشافها"، وإلا أصبح الناتج مضللًا.

خامسًا: مؤشرات الاستجابة

تشمل:

- زمن انتقال المعلومة.
- زمن اتخاذ القرار.
- زمن وصول فريق الاستجابة.
- نسبة الأحداث التي تم التعامل معها وفق الإجراء المحدد.

متوسط زمن الاستجابة

متوسط زمن الاستجابة = مجموع أزمنة الاستجابة ÷ عدد الأحداث المقاسة

ومن المهم تحديد نقطة بداية الزمن ونقطة نهايته بدقة.

سادسًا: مؤشرات التوثيق والتحقيق

تشمل:

- نسبة التسجيلات المتاحة عند الطلب.
- زمن استرجاع التسجيل.
- نسبة التسجيلات القابلة للاستخدام.
- اكتمال بيانات الوقت والمصدر.
- سلامة ملفات التصدير.

وتؤكد إرشادات وزارة العدل الأمريكية أهمية تأمين الفيديو وفهرسته وتخزينه والمحافظة على قيمته وسلامته عند استخدامه كدليل OOffice of Justice Programs . كما يركز NISTIR 8161 Rev.1تحديدًا على متطلبات تصدير وتبادل تسجيلات الفيديو الرقمي والبيانات الوصفية المرتبطة بها، ولذلك ينبغي استخدامه في هذا السياق المحدد لا كمصدر عام لكل جوانب التوثيقNNIST .

مؤشر مقترح لقابلية الاسترجاع

نسبة التسجيلات المسترجعة بنجاح = (عدد طلبات الاسترجاع الناجحة ÷ إجمالي طلبات الاسترجاع) × ١٠٠

سابعًا: مؤشرات التشغيل والإدارة

تشمل:

- نسبة العاملين المدربين.
- نسبة الالتزام بالإجراءات.
- انتظام الاختبارات.
- انتظام الصيانة.
- زمن معالجة البلاغات الفنية.
- مستوى توثيق الحوادث والأعطال.

ثامنًا: مؤشرات التكامل

تشمل:

- نسبة الأنظمة المرتبطة فعليًا.
- نجاح انتقال التنبيهات.
- زمن انتقال الحدث بين الأنظمة.
- نسبة الأحداث التي يتم التعامل معها آليًا أو شبه آلي وفق الإجراءات.
- قدرة مركز القيادة على الحصول على المعلومات المطلوبة.

تاسعًا: مؤشر مركب للفاعلية

يمكن للباحث، عند الحاجة إلى مؤشر مركب، استخدام النموذج الآتي:

درجة الفاعلية الكلية = مجموع (درجة المؤشر × الوزن النسبي للمؤشر)

على أن:

مجموع الأوزان = ١٠٠%

ولا يمثل هذا النموذج معيارًا دوليًا، وإنما أداة بحثية مقترحة لتجميع نتائج المؤشـــرات المختلفة .

المبحث الخامس: عوامل نجاح المنظومة

لا تنتج الفاعلية من عنصر واحد، وإنما من تفاعل مجموعة من العوامل الفنية والبشرية والتنظيمية والتشغيلية. ولذلك فإن معالجة قصور الفاعلية تتطلب تحديد العامل الذي يؤثر في النتيجة بدل الاكتفاء باستبدال الأجهزة.

أولًا: التخطيط الأمني

يبدأ نجاح المنظومة من تحديد:

- الأصول المراد حمايتها.
- المخاطر.
- الأهداف الأمنية.
- المناطق ذات الأولوية.
- المهام التي يتعين على الفيديو دعمها.

ونؤكد أهمية البدء بحالات الاستخدام والمهام قبل تحديد متطلبات الفيديو .

ثانيًا: التصميم المناسب

يشمل التصميم:

- اختيار مواقع الكاميرات.
- تحديد مجالات الرؤية.
- تحديد متطلبات الجودة.
- دراسة الإضاءة. الفكرة مع منهجيات إدارة الاستمرارية وتحسين الأداء وقف نجاح المنظومة على مجموعة مترابطة من العوامل تبدأ بالتخطيط وتنتهي بالتقييم والتحسين. ويظل البعد ختلاف الولاية القضائية، ولذلك يجب الرجوع إلى التشريعات الوطنية ينشأ انخفاض الفاعلية عادة من تفاعل عوامل فنية وبشرية وتنظيمية واقتصادية وقانونية. ولذلك ينبغي أن يعتمد تقييم القصور على تحليل الأسباب الجذرية بدل الاكتفاء بملي المرحلة التي تتحول فيها المؤشرات والمفاهيم السابقة إلى عملية تقييم منظمة. ولا بتحديد الأهداف وينتهي بإعادة القياس. ويجب أن يجمع التقييم بين البيانات الفنية والتشغيلية والأمنية، وأن يميز

بين مستوى الأداء وبين أهمية الوظيفة المتأثرة. كما ينبغي ألا تقتصر عملية التقييم على التشخيص، بل تمت فني، مثل متطلبات التخطيط والتصميم والاختبار أو مبادئ جودة الفيديو. وقد أُسند إلى لا يُفهم من الإحالة المرجعية أن المصدر الأجنبي الإصدار الحالي، و NIST SP 800-55 Rev.1لم يعد المرجع الأحدث للقياس.

- تحديد قدرات التخزين.
- تصميم الشبكة.
- تحديد متطلبات الاعتمادية.

ويضع IEC 62676-4:2025 التخطيط والتصميم والتركيب والاختبار والتشغيل والصيانة ضمن دورة حياة نظام المراقبة بالفيديوIIEC Webstore .

ثالثًا: جودة التنفيذ والاختبار

لا يكفي تصميم المنظومة؛ بل يجب اختبارها بعد التنفيذ والتحقق من مطابقة الأداء للمتطلبات.

ومن أمثلة ذلك:

- اختبار التغطية.
- اختبار جودة الصورة.
- اختبار التسجيل.
- اختبار الإنذارات.
- اختبار الاسترجاع.
- اختبار التكامل.

رابعًا: العنصر البشري

يمثل العاملون عنصرًا حاسمًا في تحويل القدرة التقنية إلى نتيجة تشغيلية.

وتشمل متطلبات العنصر البشري:

- التدريب.
- وضوح المسؤوليات.

- إجراءات التشغيل.
- التدريب على الطوارئ.
- التدريب على استرجاع التسجيلات.
- التدريب على التعامل مع الإنذارات.

خامسًا: الصيانة والإدارة

تحتاج المنظومة إلى:

- صيانة دورية.
- مراقبة مستمرة.
- معالجة الأعطال.
- تحديثات مناسبة.
- اختبارات دورية.
- إدارة التغيير.

سادسًا: التكامل مع المنظومات الأخرى

تزداد القيمة الأمنية المحتملة عندما تعمل الكاميرات ضمن منظومة متكاملة مع:

- التحكم في الدخول.
- الإنذار.
- الاتصالات.
- أنظمة السلامة.
- مركز القيادة والتحكم.

لكن التكامل لا ينبغي أن يقاس بمجرد وجود وصـــلة تقنية؛ وإنما بمدى نجاحها في دعم المهمة الأمنية.

سابعًا: التقييم والتحسين المستمر

تحتاج المنظومة إلى دورة تحسين مستمرة:

قياس ← تحليل ← تصحيح ← إعادة قياس

وتتفق هذه الفكرة مع منهجيات إدارة الاستمرارية وتحسين الأداء التي تقوم على المراقبة والمراجعة والتحسين المستمرIISO .

ثامنًا: البعد الاقتصادي

ينبغي ألا يقتصـــر تقييم نجاح المنظومة على أدائها الفني، بل يجب النظر إلى موارد المنشأة والتكلفة الكلية للملكية، وتشمل:

- تكلفة الشراء.
- تكلفة التركيب.
- تكلفة الشبكات والتخزين.
- تكلفة الصيانة.
- تكلفة التدريب.
- تكلفة التحديث.
- تكلفة التوقف والأعطال.

ولا يعني ذلك أن أقل منظومة تكلفة هي الأفضـــل؛ وإنما ينبغي البحث عن التوازن بين مستوى الحماية المطلوب والتكلفة الكلية لتحقيقه.

تاسعًا: مصفوفة عوامل النجاح

العامل	السؤال التقييمي
التخطيط	هل حددت الأهداف والمخاطر؟
التصميم	هل يتوافق التصميم مع المهام الأمنية؟
التنفيذ	هل اختبرت المنظومة بعد التركيب؟
العنصر البشري	هل العاملون مؤهلون؟
الصيانة	هل توجد صيانة واختبارات دورية؟
التكامل	هل التكامل يدعم النتائج الأمنية؟
التقييم	هل تقاس النتائج بصورة دورية؟
الاقتصاد	هل تتناسب التكلفة مع مستوى الحماية المطلوب؟

المبحث السادس: أسباب انخفاض الفاعلية

قد تنخفض فاعلية منظومة المراقبة رغم وجود تجهيزات متقدمة، وذلك نتيجة عوامل منفردة أو متداخلة. ومن ثم فإن تقييم القصور ينبغي أن يبحث عن السبب الجذري لا عن المظهر الفني للمشكلة فقط.

أولًا: قصور التغطية

يظهر عندما:

- توجد مناطق عمياء.
- لا تغطي الكاميرات النقاط الحرجة.
- تتغير طبيعة الموقع دون تحديث التغطية.
- تتعارض زاوية التصوير مع المهمة المطلوبة.

وتشير الأدلة التجميعية إلى وجود ارتباط بين ارتفاع مستوى التغطية وبعض النتائج الإيجابية في برامجCCTV ، مع ضرورة مراعاة اختلاف السياقات . Ccollege.police.uk

ثانيًا: ضعف جودة المعلومات

قد ينتج عن:

- ضعف الإضاءة.
- سوء الموقع.
- الحركة السريعة.
- الانعكاسات.
- ضعف الإعدادات.
- الضغط المفرط للبيانات.
- عدم ملاءمة الجودة للمهمة.

ثالثًا: الأعطال وانقطاع الخدمة

تشمل:

- تعطل الكاميرات.

- فشل الشبكة.
- توقف التسجيل.
- نقص التخزين.
- انقطاع الطاقة.
- فشل أنظمة العرض.

وهنا تظهر أهمية قياس التوافر بدل الاكتفاء بالتحقق من وجود الجهاز.

رابعًا: القصور البشري

قد ينشأ عن:

- ضعف التدريب.
- الإرهاق.
- سوء توزيع المسؤوليات.
- ضعف الالتزام بالإجراءات.
- سوء التعامل مع التنبيهات.
- عدم القدرة على الاسترجاع السريع.

خامسًا: القصور التنظيمي

مثل:

- عدم وضوح السياسات.
- ضعف إجراءات التشغيل.
- غياب إجراءات الطوارئ.
- ضعف إدارة الصلاحيات.
- عدم تحديد مسؤوليات الصيانة.
- عدم وجود نظام لتوثيق الأعطال والحوادث.

سادسًا: ضعف التكامل

قد تعمل كل منظومة بصورة مستقلة دون أن تتحول المعلومات إلى استجابة منسقة.

وهذا يؤدي إلى وجود:

كاميرا + إنذار + تحكم دخول

دون وجود:

معلومة مشتركة + قرار منسق + استجابة متكاملة.

سابعًا: الاعتماد المفرط على التقنية

لا ينبغي اعتبار التقنية بديلًا عن:

- التخطيط.
- العامل البشري.
- الحماية المادية.
- الإجراءات.
- الاستجابة.

وتؤكد الأدلة التجميعية الخاصة بـــ CCTV أن النتائج تختلف باختلاف طريقة التنفيذ والســـياق، وأن الجمع بين CCTV وتدخلات أمنية مكملة قد يكون أكثر فاعلية من الاعتماد على الكاميرات وحدها في بعض البيئاتCcollege.police.uk .

ثامنًا: القصور القانوني والخصوصية

قد تنخفض القيمة العملية للمنظومة إذا لم تكن إجراءات الجمع والتخزين والوصـــول والاستخدام متوافقة مع القوانين واللوائح المعمول بها.

ويختلف هذا الجانب باختلاف الولاية القضائية، ولذلك يجب الرجوع إلى التشريعات الوطنية والمحلية الخاصة بالخصوصية والأدلة وحماية البيانات عند إجراء تقييم ميداني.

تاسعًا: القصور الاقتصادي

قد ينشأ القصور عن: تقليل الاستثمار في الصيانة. / اختيار حلول أقل من المتطلبات. / إهمال تكاليف التشـــغيل المســـتقبلية. / عدم توفير قطع الغيار. / ضـــعف التخطيط للاستبدال والتحديث.

المبحث السابع: تقييم الأداء الفعلي

يمثل تقييم الأداء الفعلي المرحلة التي تتحول فيها المؤشـــرات والمفاهيم الســـابقة إلى عملية تقييم منظمة. ولا ينبغي أن يقتصـــر التقييم على الفحص الفني، بل ينبغي أن يقارن بين الأداء الفعلي والمتطلبات والأهداف الأمنية.

أولًا: تحديد أهداف التقييم

تبدأ عملية التقييم بتحديد الغرض، مثل:

- التحقق من تحقيق الأهداف الأمنية.
- اكتشاف مناطق القصور.
- قياس التحسن.
- دعم قرارات الاستثمار.
- تحديد احتياجات التحديث.
- التحقق من جاهزية الاستجابة.

ثانيًا: تحديد نطاق التقييم

يشمل تحديد:

- المنشأة.
- المناطق.
- الكاميرات.
- الفترة الزمنية.
- الأحداث محل الدراسة.
- الوظائف التي سيتم تقييمها.

ثالثًا: تحديد معايير القياس

يجب تحديد:

- المؤشر.
- طريقة الحساب.

- مصدر البيانات.
- فترة القياس.
- المستوى المقبول.
- المسؤول عن القياس.

وتشير أدلة NIST المتعلقة بقياس الأداء إلى أهمية استخدام مقاييس مرتبطة بالأهداف والنتائج، وجمع البيانات وتحليلها لاستخدامها في اتخاذ القرارات وتحسين الأداء . NNIST+1

رابعًا: جمع البيانات

يمكن جمع البيانات من:

- سجلات النظام.
- سجلات الأعطال.
- سجلات الصيانة.
- التسجيلات الفعلية.
- اختبارات التغطية.
- اختبارات جودة الصورة.
- سجلات الإنذارات.
- سجلات الاستجابة.
- مقابلات العاملين.
- اختبارات الاسترجاع.
- اختبارات التكامل.

خامسًا: تحليل البيانات

يمكن تصنيف النتائج إلى:

- نقاط قوة.
- نقاط قصور.
- مخاطر حرجة.

- تحسينات ضرورية.
- تحسينات اختيارية.

سادسًا: مصفوفة تقييم الفاعلية

المؤشر	طريقة القياس	المجال	النتيجة	الدرجة المرجحة	الوزن
نسبة التغطية	اختبار ميداني	التغطية	—	—	20%
ملاءمة الصورة للمهمة	اختبار عينة	جودة المعلومات	—	—	15%
نسبة التوافر	سجلات النظام	التوافر	—	—	15%
معدل الكشف	تحليل أحداث	الكشف	—	—	15%
متوسط زمن الاستجابة	سجلات الأحداث	الاستجابة	—	—	15%
قابلية الاسترجاع	اختبارات استرجاع	التوثيق والتحقيق	—	—	10%
الالتزام بالإجراءات	تدقيق	التشغيل والإدارة	—	—	5%
نجاح التكامل	اختبار	التكامل	—	—	5%
		الإجمالي			100%

وتستخدم هذه المصفوفة كأداة بحثية مقترحة، ويمكن تعديل الأوزان والمؤشرات وفق طبيعة المنشأة.

سابعًا: مصفوفة الأولويات التصحيحية

مستوى القصور	الإجراء	وصف الحالة
حرج	معالجة فورية	يؤثر في هدف أمني أساسي
مرتفع	معالجة عاجلة	يؤثر في وظيفة أمنية مهمة
متوسط	خطة تحسين	يؤثر في الأداء دون تعطيل جوهري
منخفض	متابعة دورية	أثر محدود

ثامنًا: دراسة حالة تطبيقية افتراضية

لنفترض منشأة تحتوي على:

- 100منطقة ذات أولوية.
- 92منطقة مغطاة.
- زمن مطلوب للتشغيل قدره ٧٢٠ ساعة خلال فترة التقييم.
- زمن تشغيل فعلي قدره ٧٠٥ ساعات.
- 50حدثًا معروفًا كان ينبغي اكتشافها.
- اكتشفت المنظومة ٤٤ حدثًا.
- 30طلب استرجاع للتسجيلات، نجح منها ٢٧ طلبًا.

وفق المؤشرات المقترحة:

نسبة التغطية = ٩٢ ÷ ١٠٠ × ١٠٠ = ٩٢%

نسبة التوافر = ٧٠٥ ÷ ٧٢٠ × ١٠٠ ≈ ٩٧٫٩%

معدل الكشف = ٤٤ ÷ ٥٠ × ١٠٠ = ٨٨%

نسبة نجاح الاسترجاع = ٢٧ ÷ ٣٠ × ١٠٠ = ٩٠%

هذه النتائج لا تعني تلقائيًا أن المنظومة "فعالة بنسبة ٩١. ٥٪"، لأن المؤشرات تقيس أبعادًا مختلفة، ولأن تجميعها يحتاج إلى أوزان مبررة. فإذا استخدمت المصفوفة السابقة، يمكن إدخال النتائج في نموذج الدرجة المرجحة بعد توحيد المقاييس.

وهذا المثال افتراضي لأغراض شرح منهجية القياس وليس نتيجة ميدانية أو دليلًا على أداء منشأة بعينها.

تاسعًا: تحليل فجوة الأداء

يمكن تمثيل الفجوة بالصيغة:

فجوة الأداء = المستوى المستهدف – المستوى الفعلي

فإذا كان الهدف المحدد للتوافر ٩٩٪ وكان الأداء الفعلي ٩٧٫٩٪:

فجوة التوافر = ٩٩ – ٩٧٫٩ = ١٫١ نقطة مئوية

ولا ينبغي اعتبار حجم الفجوة وحده كافيًا لتحديد الأولوية؛ إذ ينبغي النظر أيضًا إلى خطورة الوظيفة الأمنية المتأثرة.

عاشرًا: التقييم الاقتصادي

يمكن إدخال البعد الاقتصادي من خلال مقارنة:

- التكلفة الكلية للملكية.
- مستوى المخاطر.
- مستوى الفاعلية.
- تكلفة البدائل.
- تكلفة القصور أو الانقطاع.

ولا يلزم أن يستخدم الباحث مؤشرًا ماليًا واحدًا للحكم على المنظومة؛ فقد تكون بعض الوظائف الأمنية حرجة بحيث لا يمكن تقييمها على أساس التكلفة وحدها.

حادي عشر: التقييم القانوني

يجب أن يتضمن التقييم الميداني مراجعة:

- الأساس القانوني للمراقبة.
- حدود جمع البيانات.
- سياسات الاحتفاظ.
- ضوابط الوصول.
- استخدام التسجيلات.
- مشاركة البيانات.
- متطلبات الخصوصية.

- الإجراءات الخاصة باستخدام التسجيلات كأدلة.

وهذا الجانب يعتمد على النظام القانوني للدولة والقطاع والمنشـــأة، ولذلك لا يجوز استبدال النصوص القانونية المحلية بإحالة عامة إلى معيار دولي.

ثاني عشر: الإجراءات التصحيحية

بعد تحديد الفجوات، يمكن تصنيف الإجراءات إلى:

إجراءات فنية

- تعديل مواقع الكاميرات.
- تحسين الإضاءة.
- رفع جودة التسجيل عند الحاجة.
- زيادة التغطية.
- معالجة الأعطال.

إجراءات تشغيلية

- إعادة توزيع المشغلين.
- تحسين إجراءات الاستجابة.
- رفع كفاءة الاسترجاع.
- إجراء اختبارات دورية.

إجراءات تنظيمية

- تحديث السياسات.
- تحديد المسؤوليات.
- ضبط الصلاحيات.
- توثيق الحوادث والأعطال.

إجراءات استثمارية

- استبدال المكونات المتقادمة.
- توسيع التخزين.
- تعزيز الاعتمادية.

- تحسين التكامل.

ثالث عشر: إعادة القياس

لا ينتهي التقييم بمجرد إصـــدار التقرير، بل ينبغي إعادة القياس بعد تنفيذ الإجراءات التصحيحية للتحقق من تحقق التحسن.

ويمكن تمثيل دورة التقييم على النحو الآتي:

تحديد الأهداف ← تحديد المؤشـــرات ← جمع البيانات ← قياس الأداء ← تحليل الفجوات ← تحديد الأولويات ← تنفيذ الإجراءات التصـــحيحية ← إعادة القياس ← التحسين المستمر

وهـذا يتســـق مع النهج القـائم على القيـاس والتحليـل والتحســـين في إدارة الأداء والاستمرارية ISO+1 .

رابع عشر: النموذج المتكامل لفاعلية منظومة المراقبة

يمكن صياغة النموذج العام للفصل على النحو الآتي:

الأهداف الأمنية

↓

تحديد المخاطر والمتطلبات

↓

التصميم والتنفيذ

↓

الكفاءة الفنية

↓

الكفاءة التشغيلية

↓

الوظيفة الأمنية

↓

النتائج الفعلية

↓

القياس والتقييم

↓

تحليل الفجوات

↓

الإجراءات التصحيحية

↓

إعادة القياس والتحسين المستمر

ويمثل هذا النموذج إطارًا تحليليًا للباحث يجمع بين العناصر التي تناولها الفصل، ولا ينبغي تقديمه باعتباره نموذجًا معياريًا صادرًا عن IEC أو NIST.

خامس عشر: مصفوفة القرار النهائية

الإجراء	المجال	النتيجة	الأهمية الأمنية	الأولوية
تحسين النقاط الحرجة	التغطية	مرتفعة	عالية	عالية
معالجة جودة الصورة	جودة المعلومات	متوسطة	عالية	عالية
تعزيز الصيانة	التوافر	مرتفعة	متوسطة	متوسطة
تقليل الإنذارات الكاذبة	الكشف	مرتفعة	عالية	عالية
تقليل زمن الاستجابة	الاستجابة	متوسطة	عالية	عالية
تحسين الاسترجاع	التوثيق	مرتفعة	متوسطة	متوسطة
تدريب العاملين	التشغيل	منخفضة	عالية	عالية
اختبار التكامل	التكامل	متوسطة	عالية	عالية

وهذه المصفوفة توضح أن درجة المؤشر وحدها لا تكفي لتحديد الأولوية؛ فالمؤشر المتوسط في وظيفة أمنية حرجة قد يكون أكثر إلحاحًا من مؤشر منخفض في وظيفة أقل أهمية.

خلاصة الفصل الحادي عشر

أظهر التحليل أن فاعلية منظومة كاميرات المراقبة لا يمكن اختزالها في عدد الكاميرات أو مواصفاتها الفنية أو مجرد استمرارها في العمل. فالفاعلية مفهوم يرتبط بمدى إسهام المنظومة في تحقيق الأهداف الأمنية المحددة لها في البيئة الفعلية للمنشأة.

وقد تبين وجود تمييز منهجي بين وجود المنظومة، والكفاءة الفنية، والكفاءة التشغيلية، والفاعلية الأمنية .فوجود المكونات يمثل مستوى أوليًا، بينما تعكس الكفاءة الفنية قدرة المكونات على أداء وظائفها، وتعكس الكفاءة التشغيلية قدرة المنظومة على العمل في

بيئة الاستخدام، أما الفاعلية الأمنية فتتعلق بالنتيجة التي تتحقق من استخدام هذه الإمكانات.

كما أمكن التمييز بين خمسة أبعاد للفاعلية :الفاعلية الوقائية، والكشفية، والاستجابية، والتوثيقية، والتحقيقية .ويسمح هذا التمييز ببناء مؤشرات أكثر دقة، لأن نجاح المنظومة في الكشف مثلًا لا يعني بالضرورة نجاحها في دعم التحقيق، كما أن جودة التسجيل لا تعني بالضرورة سرعة الاستجابة.

وأظهر التحليل كذلك أن تقييم الفاعلية يحتاج إلى مؤشرات متعددة تشمل التغطية، وجودة المعلومات، والتوافر، والكشف، والاستجابة، والتوثيق والتحقيق، والتشغيل، والتكامل. ويمكن تحويل عدد من هذه المؤشرات إلى مقاييس كمية تساعد على المقارنة، مع ضرورة التمييز بين المعادلات المقترحة لأغراض البحث وبين المتطلبات أو المنهجيات التي تنص عليها المعايير بصورة مباشرة.

كما تبين أن نجاح المنظومة يتأثر بالتخطيط والتصميم والتنفيذ والعنصر البشري والصيانة والتكامل والتقييم المستمر، وأن انخفاض الفاعلية قد ينتج عن قصور في أي من هذه العناصر أو عن تفاعلها معًا.

وأظهر التحليل أهمية إدخال البعدين القانوني والاقتصادي في عملية التقييم؛ فالمنظومة الأمنية لا تعمل في فراغ قانوني، كما أن القرارات المتعلقة بالتحديث والاستثمار تحتاج إلى موازنة مستوى الحماية المطلوب مع التكلفة الكلية للملكية والمخاطر المرتبطة بالقصور.

ح النموذج المتكامل للفاعلية

أولاً: ما المقصود بهذا النموذج؟

هذا النموذج يمثل خارطة طريق منهجية توضح كيف تنتقل منظومة المراقبة من مجرد الفكرة إلى النتيجة الأمنية القابلة للقياس والتحسين .وهو ليس مجرد تسلسل خطي، بل هو دورة مستمرة تعيد تغذية نفسها في كل مرحلة.

بمعنى آخر: هو الإطار النظري الذي يربط بين جميع عناصر الفاعلية، ويوضح أن الفاعلية ليست حدثاً لحظياً، بل عملية متدرجة ومستمرة.

ثانيًا: شرح كل مرحلة بالتفصيل

المرحلة ١: الأهداف الأمنية

السؤال الجوهري: ما الذي نريد تحقيقه أمنيًا؟

المقصود: تحديد النتائج الأمنية المرجوة من المنظومة، مثل:

- حماية الأرواح.
- حماية المعلومات.
- حماية الأصول.
- حماية المحيط.
- دعم التحقيق.

الأهمية: هذه المرحلة هي نقطة الانطلاق؛ فبدون أهداف واضحة لا يمكن الحكم على فاعلية أي منظومة.

المرحلة ٢: المتطلبات والمخاطر

السؤال الجوهري: ما المخاطر التي تواجهنا؟ وما المتطلبات اللازمة لمواجهتها؟

المقصود: تحليل المخاطر (احتمالها × أثرها)، وتحديد المتطلبات الفنية والتشغيلية اللازمة لمواجهتها.

الأهمية: هذه المرحلة هي التي تربط الأهداف بالواقع؛ فالأهداف بدون تحليل مخاطر تظل طموحات غير قابلة للتحقيق.

المرحلة ٣: التصميم والتنفيذ

السؤال الجوهري: كيف نصمم المنظومة وننفذها وفق المتطلبات؟

المقصود: تصميم المنظومة (توزيع الكاميرات، العدسات، الارتفاعات، الشبكات، التخزين)، ثم تنفيذها (التركيب، الضبط، الاختبار).

الأهمية: هذه المرحلة هي ترجمة المتطلبات إلى واقع مادي؛ فالتصميم السيئ يُفشل أفضل المتطلبات.

المرحلة ٤ : الكفاءة الفنية

السؤال الجوهري : هل تعمل المنظومة كما ينبغي تقنيًا؟

المقصود : قياس الأداء الفني للمكونات: جودة الصورة، استقرار الشبكة، سلامة التسجيل، دقة التوقيت، استمرارية الطاقة.

الأهمية : هذه المرحلة هي الأساس التقني الذي تُبنى عليه الفاعلية الأمنية.

المعادلة : الكفاءة الفنية = (عدد المكونات العاملة ÷ إجمالي المكونات) × ١٠٠%

المرحلة ٥ : الكفاءة التشغيلية

السؤال الجوهري : هل تُشغَّل المنظومة بصورة صحيحة؟

المقصود : قياس الأداء التشغيلي: كفاءة المشغلين، الالتزام بالإجراءات، سرعة الاستجابة، انتظام الصيانة.

الأهمية : هذه المرحلة هي الجسر بين التقنية والأمن؛ فمنظومة فنية ممتازة قد تفشل بسبب سوء التشغيل.

المعادلة : الكفاءة التشغيلية = (المهام المنفذة وفق المتطلبات ÷ إجمالي المهام) × ١٠٠%

المرحلة ٦ : الوظيفة الأمنية

السؤال الجوهري : هل تؤدي المنظومة وظائفها الأمنية؟

المقصود : قياس الوظائف الأمنية: الكشف، التحقق، الاستجابة، التوثيق، دعم التحقيق.

الأهمية : هذه المرحلة هي جوهر الفاعلية؛ فكل ما سبق كان ممهداً لهذه الوظائف.

المرحلة ٧ : النتائج الفعلية

السؤال الجوهري : ما النتائج الأمنية التي تحققت فعليًا؟

المقصود :قياس النتائج الفعلية: عدد الأحداث المكتشفة، سرعة الاستجابة، جودة التوثيق، دعم التحقيق.

الأهمية :هذه المرحلة هي الحكم النهائي على المنظومة من حيث النتائج.

التمييز المهم:

- الوظيفة الأمنية =ما يفترض أن تؤديه المنظومة.
- النتائج الفعلية =ما تحقق فعليًا.

المرحلة ٨: القياس والتقييم

السؤال الجوهري :كيف نقيس النتائج ونقيّمها؟

المقصود :استخدام مؤشرات الأداء ونظام الدرجات وبطاقة التقييم للحكم على مستوى الأداء.

الفرق بين القياس والتقييم:

- القياس :إنتاج قيمة (مثل: نسبة الكشف ٨٥٪).
- التقييم :إصدار حكم (هل ٨٥٪ كافية؟).

المرحلة ٩: تحليل الفجوات

السؤال الجوهري :ما الفرق بين الوضع الحالي والوضع المستهدف؟

المقصود :تحليل الفجوات :الفجوة = المستوى المستهدف – المستوى الحالي، مع تحليل السبب الجذري.

الأهمية :هذه المرحلة هي التي تحوّل التقييم إلى خطة عمل.

المرحلة ١٠: الإجراءات التصحيحية

السؤال الجوهري :ما الإجراءات اللازمة لسد الفجوات؟

المقصود :تحديد الإجراءات التصحيحية، والمسؤوليات، والمواعيد، ومؤشرات النجاح.

الأهمية :هذه المرحلة هي ترجمة التقييم إلى عمل ملموس.

المرحلة ١١ : إعادة القياس والتحسين المستمر
السؤال الجوهري :هل نجحت الإجراءات التصحيحية؟
المقصـود :إعادة القياس بعد تنفيذ الإجراءات، والتحقق من تحسـن الأداء، والبدء في دورة جديدة من التحسين.
الأهمية :هذه المرحلة هي التي تجعل التقييم عملية مستمرة وليس حدثاً لمرة واحدة.

ثالثًا: لماذا هذا النموذج مهم؟
.1يمنع التسرع في الحكم
فبدلاً من القول "المنظومة جيدة" أو "المنظومة سيئة" بناءً على انطباع، يفرض النموذج المرور بجميع المراحل قبل إصدار الحكم.
.2يربط التقنية بالأمن
يوضح النموذج أن الكفاءة الفنية ليست كافية، بل يجب أن تُترجم إلى كفاءة تشغيلية ثم إلى وظيفة أمنية ثم إلى نتائج فعلية.
.3يجعل التقييم قابلاً للقياس
كل مرحلة في النموذج قابلة للقياس بمؤشرات محددة، مما يجعل التقييم موضوعيًا.
.4يضمن التحسين المستمر
النموذج دائري، وليس خطيًا؛ فبعد إعادة القياس، تعود الدورة للبدء من جديد.

رابعًا: مثال تطبيقي للتوضيح

لنفترض أن منشأة لديها ٤٨ كاميرا:

المرحلة	الوضع في المثال
الأهداف الأمنية	حماية الأرواح، المعلومات، الأصول، المحيط
المتطلبات والمخاطر	7مخاطر، ٣ عالية، ٢ متوسطة، ٢ منخفضة
التصميم والتنفيذ	48كاميرا موزعة على ١٢ منطقة
الكفاءة الفنية	85%الكاميرات تعمل( )
الكفاءة التشغيلية	52%التدريب والصيانة ضعيفة( )
الوظيفة الأمنية	الكشف ٧٠٪، الاستجابة ٦٠%
النتائج الفعلية	15حدثًا مكتشفًا من ٢٠
القياس والتقييم	56%ضعيف( )
تحليل الفجوات	فجوة ٢٤٪ عن المستهدف(80%)
الإجراءات التصحيحية	18إجراءً
إعادة القياس	بعد ٦ أشهر

خامساً: الخلاصة

النموذج المتكامل للفاعلية هو إطار منهجي شامل يجمع بين:

- التخطيط الأمني (الأهداف والمخاطر).
- التنفيذ التقني (التصميم والكفاءة الفنية).
- التشغيل البشري (الكفاءة التشغيلية).
- النتائج الأمنية (الوظيفة والنتائج الفعلية)
- التقييم والتحسين (القياس والفجوات والإجراءات).

وهو بذلك يمثل جوهر الكتاب، لأنه يربط جميع فصـــوله في رؤية واحدة متكاملة :أن فاعلية منظومة المراقبة لا تُقاس بالتقنية وحدها، بل بقدرتها على تحقيق نتائج أمنية قابلة للقياس والتحسين المستمر.

ومن ثم فإن السؤال المنهجي الصحيح في تقييم منظومة كاميرات المراقبة ليس:
"كم كاميرا تم تركيبها؟"
وإنما:
"إلى أي مدى تحقق المنظومة الأهداف الأمنية المحددة لها في الواقع، وبأي مستوى من الكفاءة والفاعلية، وما الفجوات التي تحول دون تحقيق المستوى المطلوب؟"

أهم نتائج الفصل الأول

١. فاعلية منظومة كاميرات المراقبة ترتبط بتحقيق الأهداف الأمنية الفعلية.
٢. وجود المنظومة لا يعني بالضرورة كفاءتها أو فاعليتها.
٣. الكفاءة الفنية تختلف عن الكفاءة التشغيلية والفاعلية الأمنية.
٤. يمكن تحليل الفاعلية إلى وقائية وكشفية واستجابية وتوثيقية وتحقيقية.
٥. جودة الصورة ينبغي أن تقاس في ضوء المهمة الأمنية المطلوبة.
٦. التغطية عنصر مهم في تقييم الفاعلية، لكنها ليست المؤشر الوحيد.
٧. التوافر والاستمرارية من العناصر الأساسية لاستدامة الوظيفة الأمنية.
٨. يمكن استخدام مؤشرات كمية لقياس جوانب مختلفة من الأداء.
٩. المعادلات المقترحة في هذا الفصل أدوات بحثية وليست معايير دولية ملزمة.
١٠. المؤشر المركب للفاعلية يحتاج إلى أوزان مبررة ومحددة مسبقًا.
١١. نجاح المنظومة يتأثر بالتخطيط والتصميم والتنفيذ والتشغيل والصيانة.
١٢. العنصر البشري يمثل عاملًا مهمًا في تحويل القدرات الفنية إلى نتائج أمنية.
١٣. التكامل مع الأنظمة الأمنية الأخرى يمكن أن يعزز قيمة المنظومة في بعض البيئات.
١٤. الاعتماد على التقنية وحدها لا يكفي لتحقيق الفاعلية الأمنية.
١٥. أسباب انخفاض الفاعلية قد تكون فنية أو بشرية أو تنظيمية أو اقتصادية أو قانونية.
١٦. ينبغي أن يتضمن التقييم الفعلي تحليلًا للفجوة بين الأداء المستهدف والأداء المحقق.
١٧. لا ينبغي تحديد أولويات المعالجة بالاعتماد على درجة المؤشر وحدها، بل يجب مراعاة أهمية الوظيفة الأمنية.
١٨. البعد القانوني عنصر لازم عند تقييم استخدام التسجيلات والوصول إليها والاحتفاظ بها.

١٩. البعد الاقتصادي يساعد في اتخاذ قرارات الاستثمار والتحديث، لكنه لا يحل محل تقييم المخاطر.
٢٠. إعادة القياس بعد تنفيذ الإجراءات التصحيحية ضرورية للتحقق من التحسن.
٢١. التحسين المستمر يمثل الحلقة الأخيرة في دورة تقييم الفاعلية.
٢٢. الحكم على المنظومة ينبغي أن يستند إلى النتائج الأمنية لا إلى عدد الأجهزة وحده.

أسئلة التفكير والتقييم للفصل الأول

أولًا: أسئلة معرفية

١. ما مفهوم الفاعلية الأمنية لمنظومة كاميرات المراقبة؟
٢. ما الفرق بين وجود المنظومة والكفاءة الفنية؟
٣. ما الفرق بين الكفاءة الفنية والكفاءة التشغيلية؟
٤. ما المقصود بالفاعلية الأمنية؟
٥. ما أنواع الفاعلية التي يمكن تمييزها؟
٦. ما أهم مؤشرات فاعلية المنظومة؟
٧. كيف تحسب نسبة التغطية؟
٨. كيف تحسب نسبة التوافر؟
٩. ما المقصود بمعدل الكشف؟
١٠. ما المقصود بمتوسط زمن الاستجابة؟
١١. ما المقصود بفجوة الأداء؟
١٢. ما مراحل تقييم الأداء الفعلي؟

ثانيًا: أسئلة تحليلية

١. لماذا لا يكفي عدد الكاميرات للحكم على فاعلية المنظومة؟
٢. حلل العلاقة بين الكفاءة الفنية والفاعلية الأمنية.
٣. لماذا قد تكون منظومة مرتفعة الجودة الفنية منخفضة الفاعلية؟
٤. حلل أثر العنصر البشري في الفاعلية.

٥. لماذا تختلف مؤشرات الفاعلية باختلاف طبيعة المنشأة؟
٦. حلل العلاقة بين التغطية والكشف.
٧. كيف يمكن أن يؤثر التكامل في الفاعلية؟
٨. لماذا ينبغي التمييز بين الفاعلية الوقائية والكشفية والاستجابية؟
٩. حلل أثر الأعطال في الفاعلية الأمنية.
١٠. لماذا لا يكفي مؤشر واحد لتقييم المنظومة؟
١١. حلل العلاقة بين الفاعلية والتكلفة الكلية للملكية.
١٢. كيف يؤثر الإطار القانوني في تقييم المنظومة؟
١٣. لماذا ينبغي إعادة القياس بعد الإجراءات التصحيحية؟

ثالثًا: أسئلة تطبيقية

١. اختر منشأة، وحدد أهدافها الأمنية ثم صمم مؤشرات لقياس فاعلية منظومة المراقبة فيها.
٢. احسب نسبة التغطية لمنشأة من اختيارك.
٣. احسب نسبة التوافر خلال فترة زمنية محددة.
٤. صمم مؤشرًا لقياس سرعة استرجاع التسجيلات.
٥. صمم مصفوفة أوزان لتقييم منظومة في منشأة حيوية.
٦. طبق نموذج الفاعلية على سيناريو افتراضي.
٧. حدد أسباب انخفاض الفاعلية في منظومة افتراضية.
٨. صمم خطة إجراءات تصحيحية لمعالجة مواطن القصور.
٩. صمم مصفوفة قرار تحدد أولويات التحسين.
١٠. صمم برنامجًا لإعادة القياس بعد تنفيذ الإجراءات التصحيحية.
١١. قارن بين منظومتين تختلفان في الكفاءة الفنية والفاعلية الأمنية.
١٢. حلل التكلفة الكلية للملكية في مشروع افتراضي لكاميرات المراقبة.
١٣. ضع قائمة بالمتطلبات القانونية التي ينبغي مراجعتها قبل استخدام التسجيلات لأغراض التحقيق.

قائمة المصادر والمراجع الأساسية للفصل الحادي عشر

أولًا: المعايير الدولية

١. International Electrotechnical Commission (IEC). *IEC 62676-4:2025: Video Surveillance Systems for Use in Security Applications — Part 4: Application Guidelines*. 2nd ed. Geneva: IEC, 2025.
يغطي المعيار التخطيط والتصميم والتركيب والاختبار والتشغيل والصيانة لمنظومات المراقبة بالفيديو IIEC Webstore.

٢. International Organization for Standardization (ISO). *ISO 22301:2019: Security and Resilience — Business Continuity Management Systems — Requirements*. Geneva: ISO, 2019.
يستخدم في الفصل لدعم مفاهيم الاستمرارية والمراقبة والمراجعة والتحسين، وليس بوصفه معيارًا متخصصًا في CCTV. IISO

٣. International Organization for Standardization (ISO). *ISO 22320:2018: Security and Resilience — Emergency Management — Guidelines for Incident Management*. Geneva: ISO, 2018.
يفيد في الجوانب المرتبطة بإدارة الحوادث والأدوار والمسؤوليات وإدارة الموارد والتنسيق أثناء الاستجابة IISO.

٤. International Organization for Standardization / International Electrotechnical Commission. *ISO/IEC 27035-1:2023: Information Technology — Information Security Incident Management — Part 1: Principles and Process*. Geneva: ISO/IEC, 2023.
يستخدم لدعم مفاهيم الكشف والتقييم والاستجابة والتعلم من الحوادث في الجانب المعلوماتي من المنظومة IISO.

ثانيًا: المصادر الحكومية والفنية

٥. National Institute of Standards and Technology (NIST). *Video Quality in Public Safety (VQiPS): Getting Started*. Gaithersburg, MD: NIST.
يدعم منهج تحديد متطلبات جودة الفيديو انطلاقًا من حالات الاستخدام والمهام المطلوبة NNIST.

٦. National Institute of Standards and Technology (NIST). *VQiPS: Use Cases*. Gaithersburg, MD: NIST.
يدعم الربط بين حالة الاستخدام وجودة الفيديو المطلوبة والمهمة التي يتعين على المشاهد إنجازها NNIST.

٧. National Institute of Standards and Technology (NIST). Chew, Elizabeth, Marianne Swanson, Kevin Stine, Nadya Bartol, Anthony Brown, and Will Robinson. *Performance Measurement Guide for Information Security*, NIST SP 800-55 Rev. 1. Gaithersburg, MD: NIST, 2008.
يستخدم هنا بوصفه مرجعًا منهجيًا تاريخيًا لقياس الأداء وتطوير المؤشرات، مع التنبيه إلى أنه سُحب لاحقًا وحل محله مسار أحدث من منشورات NNIST+1. SP 800-55.

٨. National Institute of Standards and Technology (NIST). *The NIST Cybersecurity Framework (CSF) 2. 0*. NIST Cybersecurity White Paper 29. Gaithersburg, MD: NIST, 2024.
يفيد في ربط القياس بالنتائج الأمنية وإدارة المخاطر، ولا يستخدم بوصفه معيارًا متخصصًا في تقييم CCTV. NNIST

٩. National Institute of Standards and Technology (NIST). Nadel, Lawrence D., Mary T. Laamanen, Michael D. Garris, and Craig S. Russell. *Recommendation: Closed Circuit Television (CCTV) Digital Video Export Profile — Level 0 (Revision 1)*. NISTIR 8161 Rev. 1. Gaithersburg, MD: NIST, 2019.
يستخدم في موضوع تصدير التسجيلات الرقمية وتبادلها والبيانات الوصفية المرتبطة بها، وليس كمصدر عام لكل متطلبات التوثيق NNIST.

١٠. National Institute of Standards and Technology (NIST). Cichonski, Paul, Tom Millar, Timothy Grance, and Karen Scarfone. *Computer Security Incident Handling Guide*. NIST SP 800-61 Rev. 2. Gaithersburg, MD: NIST, 2012.
يستخدم في الجوانب المتعلقة بإدارة الحوادث والاستجابة، مع ملاحظة أن Rev.2 سُحب في ٣ أبريل ٢٠٢٥ وحل محله Rev.3. NNIST Computer Security Resource Center

ثالثًا: مصادر العدالة والأدلة المرئية

١١. U.S. Department of Justice, Bureau of Justice Assistance. *Video Evidence: A Law Enforcement Guide to Resources and Best Practices.* Washington, DC: U.S. Department of Justice, 2014. يدعم الجوانب المتعلقة بجمع الفيديو وتخزينه وتأمينه والحفاظ على سلامته وقيمته الإثباتيةOOffice of Justice Programs .

١٢. College of Policing. *Closed-circuit television (CCTV).* Crime Reduction Toolkit. يستخدم كمصدر تجميعي للأدلة المتعلقة بأثرCCTV ، مع مراعاة اختلاف النتائج باختلاف السياق والتغطية والمراقبة النشطة والتدخلات المكملةCcollege.police.uk .

الفصل الثاني: منهجية تقييم منظومات كاميرات المراقبة

تمهيد الفصل

يمثل تقييم منظومات كاميرات المراقبة مرحلة أساسية في الانتقال من مجرد امتلاك المنظومة وتشغيلها إلى التحقق من قدرتها الفعلية على أداء الوظائف الأمنية التي أنشئت من أجلها. فوجود عدد مناسب من الكاميرات، أو ارتفاع دقة التصوير، أو توافر أجهزة تسجيل متقدمة، لا يكفي بمفرده للحكم على نجاح المنظومة؛ إذ إن الحكم المهني يتطلب فحص مدى توافق مكونات المنظومة ووظائفها وتشغيلها مع الأهداف الأمنية ومتطلبات الاستخدام الفعلي. وتؤكد الإرشادات الدولية الخاصة بأنظمة المراقبة بالفيديو أهمية النظر إلى النظام باعتباره منظومة متكاملة تبدأ من تحديد المتطلبات وتمتد إلى التصميم والتركيب والاختبار والتشغيل والصيانة والتقييم.(1)

ويختلف التقييم عن الفحص الفني البسيط؛ فالفحص قد يقتصر على التحقق من سلامة جهاز أو مكون، في حين يسعى التقييم إلى تكوين حكم منظم بشأن مستوى الأداء والقدرة على تحقيق الأهداف المحددة. ولهذا فإن منهجية التقييم ينبغي أن تربط بين الأهداف الأمنية، والمتطلبات، ومؤشرات القياس، والبيانات الفعلية، ومعايير الحكم، وأولويات التحسين .ويؤكد المختصون في منهجيته الحديثة لقياس الأمن المعلوماتي أهمية تحديد المقاييس واختيارها وترتيب أولوياتها، ثم جمع البيانات وتحليلها واستخدام النتائج في دعم القرارات والتحسين.(2)

ولا ينبغي أن ينظر إلى التقييم بوصفه عملية تهدف إلى منح المنظومة درجة نهائية فحسب، بل بوصفه دورة إدارية وفنية تساعد على اكتشاف نقاط القوة والقصور وتحديد الفجوات وترتيب الإجراءات التصحيحية. ويتفق ذلك مع المنهج القائم على إدارة

المخاطر، الذي يربط بين تحديد المخاطر وتحليلها وتقييمها ومعالجتها ومراقبتها ومراجعتها والتحسين المستمر.(3)

المبحث الأول: أسس التقييم

لا يمكن إجراء تقييم علمي لمنظومة كاميرات المراقبة من دون تحديد الأساس الذي ستبنى عليه عملية التقييم. فالحكم على المنظومة لا ينبغي أن يعتمد على الانطباع الشخصي أو على عدد الأجهزة المركبة، وإنما على معايير محددة ترتبط بالأهداف الأمنية ومتطلبات الاستخدام والنتائج الفعلية.(1)

أولًا: مفهوم تقييم منظومة المراقبة

يمكن تعريف تقييم منظومة كاميرات المراقبة إجرائيًا بأنه :عملية منهجية لجمع وتحليل الأدلة والبيانات المتعلقة بالأداء الفني والتشغيلي والأمني للمنظومة، ومقارنتها بالمتطلبات والمعايير والأهداف المحددة، بهدف إصدار حكم موضوعي بشأن مستوى الأداء وتحديد نقاط القوة والقصور والفجوات وأولويات التحسين .(2)

وهذا التعريف يجمع بين أربعة عناصر رئيسية :القياس، والمقارنة، والحكم، والتحسين .ولا يعني ذلك أن جميع عناصر التقييم يمكن اختزالها في رقم واحد؛ فبعض الجوانب يمكن قياسها كميًا، مثل نسبة التوافر أو زمن الاسترجاع، بينما تحتاج جوانب أخرى إلى تقييم نوعي أو قائم على الأدلة، مثل مدى ملاءمة التصميم الأمني أو جودة الإجراءات التشغيلية.(3)

ثانيًا: الفرق بين القياس والتقييم

ينبغي التمييز بين القياس والتقييم:(4)

العنصر	القياس	التقييم
الوظيفة	إنتاج قيمة أو نتيجة قابلة للملاحظة	إصدار حكم على مستوى الأداء
السؤال	كم؟ أو إلى أي مستوى؟	هل المستوى مناسب؟
المخرج	رقم أو قيمة أو وصف	حكم وتصنيف وأولوية
الأساس	مؤشر أو مقياس	معيار ومتطلب وأهداف
الاستخدام	جمع البيانات	دعم القرار والتحسين

ومن ثم، فإن نسبة توافر قدرها ٩٨٪ تمثل نتيجة قياس، بينما الحكم على كون ٩٨٪ كافية أو غير كافية يمثل عملية تقييم تعتمد على متطلبات المنشأة وطبيعة المخاطر ومستوى الخدمة المطلوب. وقد أكد NIST في منهجيته الحديثة للقياس أهمية التمييز بين المقاييس والنتائج وتحليلها واستخدامها في تقييم كفاية الضوابط والقرارات المرتبطة بالمخاطر.(5)

ثالثًا: مبدأ الارتباط بالأهداف الأمنية

ينبغي أن يبدأ التقييم من سؤال أساسي :ما الهدف الأمني الذي أنشئت المنظومة لتحقيقه؟ فإذا كان الهدف هو مراقبة المداخل، ينبغي أن يركز التقييم على قدرة المنظومة على تحقيق الرؤية المطلوبة عند نقاط الدخول والخروج. وإذا كان الهدف هو اكتشاف الاقتحام، فينبغي أن يركز التقييم على التغطية والكشف والإنذار والاستجابة. وإذا كان الهدف هو دعم التحقيق، فينبغي التركيز على جودة التسجيل وسلامته وإمكانية استرجاعه.(6)

وتنسجم هذه الفكرة مع منهج VQiPS الذي يربط متطلبات جودة الفيديو بحالة الاستخدام والمهمة المطلوب إنجازها، بدلًا من افتراض أن مستوى جودة واحدًا مناسب لجميع الاستخدامات.(7)

رابعًا: مبدأ التقييم القائم على المخاطر

لا تتمتع جميع المناطق والأصول والأحداث بالأهمية نفسها. ولذلك ينبغي أن يراعي التقييم مستوى المخاطر، بحيث تعطى الأولوية للمناطق والأحداث ذات التأثير الأمني الأعلى.(8)

ويمكن التعبير عن أولوية التقييم إجرائيًا بالعلاقة الآتية:

أولوية التقييم = احتمال الخطر × أثر الخطر × أهمية الوظيفة الأمنية

وهذه ليست معادلة معيارية ملزمة، وإنما أداة تحليلية مقترحة لتنظيم أولويات التقييم داخل المنشأة. ويتماشى هذا النهج مع مبادئ ISO 31000 التي تربط إدارة المخاطر

بتحقيق الأهداف، وتدعو إلى تحديد المخاطر وتحليلها وتقييمها ومعالجتها ومراقبتها ومراجعتها بصورة مستمرة.(9)

خامسًا: مبدأ الأدلة القابلة للتحقق

ينبغي أن يستند التقييم إلى أدلة يمكن التحقق منها، مثل:(10)

١. سجلات الأعطال.
٢. سجلات النظام.
٣. اختبارات جودة الصورة.
٤. تقارير الصيانة.
٥. عينات التسجيلات.
٦. نتائج اختبارات الاسترجاع.
٧. سجلات الإنذارات.
٨. سجلات الدخول والصلاحيات.
٩. مقابلات المشغلين.
١٠. الملاحظة الميدانية.
١١. الوثائق والإجراءات المعتمدة.

ولا يكفي أن يقرر المقيم أن المنظومة "جيدة" أو "ضعيفة" من دون تحديد الأساس الذي بني عليه الحكم.

سادسًا: مبدأ القابلية للتكرار

ينبغي أن تكون منهجية التقييم قابلة لإعادة التطبيق بحيث يؤدي استخدام المعايير ذاتها على بيانات مماثلة إلى نتائج متقاربة (١١). ويقتضي ذلك تحديد:

١. المؤشر.
٢. تعريفه.
٣. مصدر بياناته.

٤. طريقة حسابه.
٥. فترة القياس.
٦. معيار الحكم.
٧. المسؤول عن القياس.
٨. مستوى عدم اليقين، عند الحاجة.

سابعًا: مبدأ التحسين المستمر

لا ينبغي أن ينتهي التقييم بمجرد إصدار التقرير؛ فالنتائج ينبغي أن تتحول إلى إجراءات تصحيحية، ثم يعاد القياس للتحقق من أثر هذه الإجراءات (١٢). ويتماشى ذلك مع توجه ISO 31000 نحو المراقبة والمراجعة والتحسين المستمر، ومع منهج NIST الذي ينظر إلى القياس بوصفه برنامجًا مستمرًا وليس نشاطًا منعزلًا.(13)

المراجع:

① International Electrotechnical Commission, *IEC 62676-4:2025, Video surveillance systems for use in security applications – Part 4: Application guidelines*, 2nd ed., (Geneva: IEC, 2025).

.② International Electrotechnical Commission, *IEC 62676-4:2025*

③ Katherine Schroeder, Hung Trinh, and Victoria Pillitteri, *Measurement Guide for Information Security: Volume 1 – Identifying and Selecting Measures*, NIST SP 800-55 Vol. 1, (Gaithersburg, MD: National Institute of Standards and Technology, 2024).

.④ Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 1*

.⑤ Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 1*

.⑥ International Electrotechnical Commission, *IEC 62676-4:2025*

⑦ National Institute of Standards and Technology, *Video Quality in Public Safety (VQiPS): Use Cases*, (Gaithersburg, MD: NIST).

⑧ International Organization for Standardization, *ISO 31000:2018, Risk management – Guidelines*, (Geneva: ISO, 2018).

⑨ ISO, *ISO 31000:2018*.

.⑩ Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 1*

.⑪ Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 1*

⑫ Katherine Schroeder, Hung Trinh, and Victoria Pillitteri, *Measurement Guide for Information Security: Volume 2 – Developing an Information Security Measurement Program*, NIST SP 800-55 Vol. 2, (Gaithersburg, MD: NIST, 2024).

.Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 2*؛ و⑬ ISO, *ISO 31000:2018*

المبحث الثاني: محاور التقييم

يتطلب تقييم منظومة كاميرات المراقبة تقسيمها إلى محاور مترابطة، لأن تقييم جانب واحد لا يعكس بالضرورة الأداء الكلي. فقد تكون المنظومة ذات جودة تصوير مرتفعة، لكنها تعاني ضعفًا في التغطية أو التوافر أو التشغيل أو الاستجابة.(1)
وعليه، يقترح هذا الفصل سبعة محاور رئيسية للتقييم، مع إمكانية تعديلها وفق طبيعة المنشأة.

أولًا: محور التخطيط والتصميم الأمني
يشمل هذا المحور التحقق من مدى توافق المنظومة مع:(2)

- طبيعة المنشأة.
- الأصول التي تتطلب الحماية.
- التهديدات والمخاطر.
- المناطق الحرجة.
- حالات الاستخدام.
- أهداف المراقبة.
- متطلبات الاستجابة والتحقيق.

ولا ينبغي تقييم التصميم بمعزل عن الغرض الأمني من الكاميرا؛ فاختيار المعدات ينبغي أن يتبع المتطلبات لا أن يسبقها. وتؤكد IEC 62676-4 أهمية التخطيط وتحديد المتطلبات ضمن دورة حياة نظام المراقبة.(3)

ثانيًا: محور التغطية وجودة المشهد
يركز هذا المحور على:(4)

- تغطية المناطق ذات الأولوية.
- وجود النقاط العمياء.
- زاوية الرؤية.

- موضع الكاميرا.
- جودة الصورة.
- الإضاءة.
- التفاصيل المطلوبة لحالة الاستخدام.
- جودة المشهد ليلًا ونهارًا.

ولا ينبغي اعتبار الدقة الرقمية وحدها مؤشـــرًا كافيًا؛ إذ إن جودة الفيديو تعتمد على ســـلســـلة النظام من الالتقاط والمعالجة والنقل والتخزين والعرض، كما أن المتطلبات تتحدد وفق المهمة المراد إنجازها.(5)

ثالثًا: محور التوافر والاستمرارية

يتناول:(6)

- نسبة توافر الكاميرات.
- توافر التسجيل.
- توافر الشبكة.
- أعطال الأجهزة.
- الانقطاعات.
- زمن الإصلاح.
- وجود البدائل والتكرار عند الحاجة.

وتزداد أهمية هذا المحور في المنشـــآت التي تتطلب مراقبة مســـتمرة أو التي يمكن أن يؤدي فيها فقدان التسجيل إلى أثر أمني مرتفع.

رابعًا: محور الكشف والتحليل

يتناول:(7)

- قدرة المشغل على اكتشاف الأحداث.
- جودة التنبيهات.

- أداء التحليلات الذكية عند استخدامها.
- معدل الإنذارات الكاذبة.
- معدل الأحداث غير المكتشفة.
- ملاءمة قواعد التحليل للبيئة.
- قابلية التحقق من التنبيه.

خامسًا: محور التشغيل والموارد البشرية

يشمل: (8)

- كفاءة المشغلين.
- التدريب.
- وضوح المسؤوليات.
- الإجراءات التشغيلية.
- إدارة المناوبات.
- متابعة الإنذارات.
- التعامل مع الأحداث.
- الالتزام بإجراءات التوثيق والاسترجاع.

سادسًا: محور التسجيل والاسترجاع والتحقيق

يشمل: (9)

- جودة التسجيل.
- مدة الاحتفاظ.
- دقة التوقيت.
- سلامة التسجيل.
- سرعة الاسترجاع.
- إمكانية التصدير.

- حماية التسجيلات.
- توثيق عمليات الوصول والتصدير.

وتشير NIST إلى أهمية أن يكون الفيديو المعروض قادرًا على دعم مهام مثل التعرف أو اتخاذ القرار، بينما ترتبط قابلية استخدام التسجيل أيضًا بسلامة سلسلة المعالجة والتخزين والعرض.(10)

سابعًا: محور التكامل والأمن السيبراني والحوكمة

يشمل:(11)

- التكامل مع أنظمة التحكم بالدخول.
- التكامل مع الإنذار.
- التكامل مع أنظمة الأمن والسلامة.
- حماية الحسابات.
- إدارة الصلاحيات.
- حماية الشبكات.
- سلامة البيانات.
- إدارة التغيير.
- الإجراءات والسياسات.
- الخصوصية.

وتكتسب هذه الجوانب أهمية خاصة لأن منظومة المراقبة الحديثة تعتمد بدرجات متفاوتة على الشبكات والبرمجيات وتبادل البيانات، وهو ما يجعل حماية المعلومات والأنظمة جزءًا من التقييم الشامل. ويضع ISO/IEC 27001 إطارًا لإدارة مخاطر أمن المعلومات وحماية السرية والسلامة والتوافر.(12)

جدول محاور التقييم

المحور	أمثلة على عناصر القياس
التخطيط والتصميم	ملاءمة التصميم للأهداف والمخاطر
التغطية والجودة	التغطية، النقاط العمياء، جودة المشهد
التوافر والاستمرارية	التوافر، الأعطال، زمن الإصلاح
الكشف والتحليل	الكشف، التنبيهات، الإنذارات الكاذبة
التشغيل	التدريب، الإجراءات، الأداء البشري
التسجيل والتحقيق	الاسترجاع، السلامة، التصدير
التكامل والحوكمة	التكامل، الأمن السيبراني، الصلاحيات والخصوصية

المراجع:

① International Electrotechnical Commission, *IEC 62676-4:2025*.

② IEC, *IEC 62676-4:2025*.

③ IEC, *IEC 62676-4:2025*.

④ National Institute of Standards and Technology, *Video Quality in Public Safety (VQiPS): Getting Started and Use Cases*, (Gaithersburg, MD: NIST).

⑤ NIST, *VQiPS: Getting Started and Use Cases*.

⑥ IEC, *IEC 62676-4:2025*.

⑦ NIST, *VQiPS: Use Cases*.

⑧ Katherine Schroeder, Hung Trinh, and Victoria Pillitteri, *Measurement Guide for Information Security: Volume 1*.

⑨ NIST, *VQiPS: Display* and *VQiPS: Processing*.

⑩ NIST, *VQiPS: Display* and *VQiPS: Processing*.

⑪ International Organization for Standardization and International Electrotechnical Commission, *ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, (Geneva: ISO/IEC, 2022).

⑫ ISO/IEC, *ISO/IEC 27001:2022*.

المبحث الثالث: مؤشرات الأداء

تمثل مؤشرات الأداء الأداة الأساسية لتحويل التقييم من وصف عام إلى عملية يمكن قياس نتائجها ومقارنتها ومتابعتها. وينبغي اختيار المؤشر بحيث يكون مرتبطًا بهدف واضح، وقابلًا للقياس، وله مصدر بيانات معروف، ويمكن تفسير نتيجته.(1)
ويؤكد المختصون أن تطوير المقاييس ينبغي أن يشمل تحديد المقاييس واختيارها وترتيب أولوياتها وتقييمها، مع إمكانية استخدام القياسات الكمية والنوعية.(2)

أولًا: خصائص المؤشر الجيد
يفضل أن يتصف المؤشر بما يأتي:(3)

ثانيًا: مؤشرات التغطية
يمكن استخدام:(4)
نسبة التغطية = (عدد المناطق ذات الأولوية المغطاة بصورة تحقق المتطلب ÷ إجمالي المناطق ذات الأولوية) × ١٠٠

وهذه صيغة تشغيلية مقترحة في هذا الكتاب وليست معادلة إلزامية واردة حرفيًا في معيار بعينه. كما يمكن حساب معدل النقاط العمياء:

معدل النقاط العمياء = (عدد النقاط العمياء ذات الأهمية ÷ إجمالي النقاط التي تتطلب تغطية) × ١٠٠

ثالثًا: مؤشرات جودة المعلومات

يمكن تقييم جودة المعلومات باستخدام مؤشرات مثل:(5)

١. نسبة المشاهد التي تحقق مستوى التفاصيل المطلوب.

٢. نسبة المشاهد الصالحة للتعرف.

٣. نسبة التسجيلات الصالحة للتحقيق.

٤. جودة المشهد في ظروف الإضاءة المختلفة.

وتتحدد قيمة هذه المؤشرات وفق حالة الاستخدام. فمتطلبات التعرف على لوحة مركبة تختلف عن متطلبات مراقبة حركة عامة، وهو ما يتوافق مع منهج VQiPS القائم على ربط جودة الفيديو بالمهمة المراد تنفيذها.(6)

رابعًا: مؤشرات التوافر

يمكن استخدام:(7)

نسبة التوافر = (زمن التشغيل الفعلي ÷ الزمن المطلوب للتشغيل) × ١٠٠

كما يمكن استخدام:

معدل الأعطال = عدد الأعطال ÷ فترة القياس

و:

متوسط زمن الإصلاح = إجمالي زمن الإصلاح ÷ عدد الأعطال

وهذه المؤشرات ينبغي تفسيرها وفق مستوى الخدمة المطلوب وطبيعة المنشأة.

خامسًا: مؤشرات الكشف

يمكن قياس أداء الكشف باستخدام:(8)

معدل الكشـــف = (عدد الأحداث التي اكتشـــفتها المنظومة ÷ إجمالي الأحداث المرجعية المعروفة) × ١٠٠

وعند استخدام نظام تحليل آلي يمكن إضافة:

معدل الإنذارات الكاذبة = (عدد الإنذارات غير الصـــحيحة ÷ إجمالي الإنذارات) × ١٠٠

ويجب الحذر من اســتخدام معدل الكشــف منفردًا؛ لأن ارتفاعه قد يترافق مع ارتفاع كبير في الإنذارات الكاذبة. ولذلك ينبغي تحليل المؤشرين معًا.

سادسًا: مؤشرات الاستجابة

يمكن حساب:(9)

متوسط زمن الاستجابة = مجموع أزمنة الاستجابة ÷ عدد الأحداث

كما يمكن قياس:

نســبة الأحداث المســتجابة ضــمن الزمن المســتهدف = (عدد الأحداث التي تمت الاستجابة لها ضمن الزمن المستهدف ÷ إجمالي الأحداث التي تتطلب استجابة) × ١٠٠

سابعًا: مؤشرات التسجيل والاسترجاع

يمكن استخدام:(10)

نســبة نجاح الاســترجاع = (عدد طلبات الاســترجاع الناجحة ÷ إجمالي طلبات الاسترجاع) × ١٠٠

و:

متوســط زمن الاســترجاع = مجموع الزمن اللازم لتلبية طلبات الاســترجاع ÷ عدد الطلبات

ثامنًا: مؤشرات الالتزام التشغيلي

يمكن استخدام:(11)

نسبة الالتزام بالإجراءات = (عدد الإجراءات المنفذة وفق الإجراء المعتمد ÷ إجمالي الإجراءات التي تم فحصها) × ١٠٠

كما يمكن قياس:

- نسبة الموظفين المدربين.
- نسبة اختبارات الصيانة المنفذة.
- نسبة مراجعات الصلاحيات المنجزة.
- نسبة الحوادث الموثقة بصورة صحيحة.

تاسعًا: مؤشرات التكامل

يمكن تقييم التكامل من خلال: (12)

- نسبة الأنظمة المتكاملة مع المنظومة.
- نسبة الأحداث التي تنتقل بصورة صحيحة بين الأنظمة.
- معدل فشل التكامل.
- زمن انتقال الحدث.
- نسبة التنبيهات المتبادلة بصورة صحيحة.

مصفوفة المؤشرات الأساسية

يمكن قياس فاعلية منظومة المراقبة من خلال مجموعة من المؤشرات التي تغطي جوانب التغطية والتوافر والأعطال والكشف والاستجابة والاسترجاع والتشغيل والتكامل.

ومن أبرز هذه المؤشرات:

أولًا: مؤشرات التغطية

- نسبة التغطية: تقيس مدى تحقيق المناطق التي تمت تغطيتها مقارنة بالمناطق التي يُفترض تغطيتها، وتحسب وفق المعادلة: المناطق المحققة ÷ المناطق المطلوبة × ١٠٠.

- معدل النقاط العمياء: يقيس نسبة النقاط التي لا تحقق فيها المنظومة التغطية المطلوبة، وتحسب وفق المعادلة: النقاط العمياء ÷ النقاط المطلوبة × ١٠٠.

ثانيًا: مؤشرات التوافر والأعطال

- نسبة التوافر: تقيس مدى تشغيل المنظومة فعليًا مقارنة بفترة التشغيل المطلوبة، وتحسب وفق المعادلة: التشغيل الفعلي ÷ التشغيل المطلوب × ١٠٠.
- معدل الأعطال: يقيس تكرار الأعطال خلال فترة زمنية محددة، ويحساب وفق المعادلة: عدد الأعطال ÷ فترة القياس.

ثالثًا: مؤشرات الكشف والإنذارات

- معدل الكشف: يقيس قدرة المنظومة على اكتشاف الأحداث مقارنة بعدد الأحداث المرجعية المعروفة، وتحسب وفق المعادلة: الأحداث المكتشفة ÷ الأحداث المرجعية × ١٠٠.
- معدل الإنذارات الكاذبة: يقيس نسبة الإنذارات غير الصحيحة من إجمالي الإنذارات الصادرة عن النظام، وتحسب وفق المعادلة: الإنذارات غير الصحيحة ÷ إجمالي الإنذارات × ١٠٠.

رابعًا: مؤشرات الاستجابة والاسترجاع

- متوسط زمن الاستجابة: يقيس متوسط الوقت المستغرق للتعامل مع الأحداث منذ اكتشافها وحتى الاستجابة لها، ويحساب وفق المعادلة: مجموع زمن الاستجابة ÷ عدد الأحداث.
- نسبة نجاح الاسترجاع: تقيس قدرة النظام على استرجاع التسجيلات أو المعلومات المطلوبة بنجاح، وتحسب وفق المعادلة: الطلبات الناجحة ÷ إجمالي الطلبات × ١٠٠.

خامسًا: مؤشرات التشغيل والتكامل

- الالتزام بالإجراءات: يقيس مدى التزام العاملين بالإجراءات التشغيلية المعتمدة، وتحسب وفق المعادلة: المهام الملتزمة ÷ المهام المفحوصة × ١٠٠.
- نجاح التكامل: يقيس قدرة مكونات المنظومة والأنظمة المرتبطة بها على العمل معًا بصورة صحيحة، وتحسب وفق المعادلة: العمليات الناجحة ÷ العمليات المختبرة × ١٠٠.

وبذلك توفر هذه المؤشرات صورة متكاملة عن أداء المنظومة؛ إذ لا يقتصر التقييم على جودة المعدات، وإنما يشمل مدى التغطية، واستمرارية التشغيل، ومعدل الأعطال، وقدرة الكشف، ودقة الإنذارات، وسرعة الاستجابة، وإمكانية استرجاع المعلومات، والالتزام بالإجراءات، ونجاح التكامل بين مكونات النظام.

المراجع:

① Katherine Schroeder, Hung Trinh, and Victoria Pillitteri, *Measurement Guide for Information Security: Volume 1 — Identifying and Selecting Measures*, NIST SP 800-55 Vol. 1, (Gaithersburg, MD: NIST, 2024).

.② Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 1*

.③ Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 1*

.④ International Electrotechnical Commission, *IEC 62676-4:2025*

⑤ National Institute of Standards and Technology, *Video Quality in Public Safety (VQiPS): Use Cases*, (Gaithersburg, MD: NIST).

⑥ NIST, *VQiPS: Use Cases*.

.⑦ IEC, *IEC 62676-4:2025*

⑧ NIST, *VQiPS: Use Cases*.

⑨ International Organization for Standardization, *ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements*, (Geneva: ISO, 2019).

⑩ NIST, *VQiPS: Display* and *VQiPS: Processing*.

⑪ Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 2 — Developing an Information Security Measurement Program*, NIST SP 800-55 Vol. 2, (Gaithersburg, MD: NIST, 2024).

.⑫ ISO/IEC, *ISO/IEC 27001:2022*

المبحث الرابع: بطاقة التقييم

تمثل بطاقة التقييم أداة عملية لتحويل محاور التقييم ومؤشـراته إلى نموذج موحد يمكن اسـتخدامه ميدانيًا. ولا يقصـد بالبطاقة أن تكون نموذجًا إلزاميًا لجميع المنشـآت، بل إطارًا يمكن تعديله وفق طبيعة المنشأة ومستوى المخاطر.(1)

أولًا: مكونات بطاقة التقييم

ينبغي أن تتضمن البطاقة:(2)

١. محور التقييم.
٢. العنصر محل التقييم.
٣. المؤشر.
٤. الوزن النسبي.
٥. مصدر البيانات.
٦. النتيجة الخام.
٧. الدرجة.
٨. الملاحظات.
٩. الأدلة.
١٠. الإجراء التصحيحي المقترح.

ثانيًا: النموذج المقترح لبطاقة التقييم

الدرجة المرجحة	الدرجة من ٥	النتيجة	الوزن	المؤشر	المحور
—	—	—	10%	ملاءمة التصميم للأهداف	التخطيط والتصميم
—	—	—	20%	نسبة التغطية وجودة المشهد	التغطية والجودة
—	—	—	15%	نسبة التوافر	التوافر
—	—	—	15%	معدل الكشف والإنذارات	الكشف
—	—	—	10%	الالتزام بزمن الاستجابة	الاستجابة
—	—	—	10%	نجاح الاسترجاع وسلامة التسجيل	التسجيل والتحقيق
—	—	—	10%	الالتزام والتدريب والصيانة	التشغيل
—	—	—	10%	التكامل والأمن والصلاحيات	التكامل والحوكمة
			100%		المجموع

وهذه الأوزان نموذجية مقترحة وليست أوزانًا معيارية مفروضة من IEC أو ISO أو NIST.وينبغي تعديلها وفق طبيعة المنشأة.

ثالثًا: مصادر الأدلة في البطاقة

يمكن تصنيف الأدلة إلى:(3)

- أدلة ميدانية: الملاحظة والاختبارات.
- أدلة تقنية: سجلات الأجهزة والأنظمة.
- أدلة تشغيلية: السجلات والإجراءات.

- أدلة بشرية :المقابلات والاختبارات.
- أدلة وثائقية :المخططات والسياسات والتقارير.

رابعًا: التحقق من جودة البيانات

ينبغي عدم إدخال البيانات في البطاقة بصورة آلية؛ بل يجب فحص:(4)

- مصدر البيانات.
- تاريخها.
- اكتمالها.
- اتساقها.
- دقتها.
- إمكانية التحقق منها.

وتولي منهجية NIST الحديثة أهمية لجودة البيانات وتوثيق القياســـات وتحليلها وعدم اليقين المرتبط بها.(5)

المراجع:

.① International Electrotechnical Commission, *IEC 62676-4:2025*

② Katherine Schroeder, Hung Trinh, and Victoria Pillitteri, *Measurement Guide for Information Security: Volume 1*.

.③ Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 1*

.④ Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 1*

.⑤ Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 1*

المبحث الخامس: نظام الدرجات

يساعد نظام الدرجات على تحويل نتائج القياس المختلفة إلى مقياس موحد يسمح بالمقارنة بين المجالات. غير أن تحويل النتائج إلى درجات ينبغي أن يتم وفق قواعد معلنة حتى لا تتحول عملية التقييم إلى حكم شخصي.(1)

أولًا: مقياس الدرجات المقترح

نقترح اعتماد مقياس من خمس درجات لتقييم مدى تحقق المتطلبات والمؤشرات. ويُعد هذا المقياس منهجًا مقترحًا في الكتاب، ولا يمثل تصنيفًا صادرًا عن معيار دولي. وتُفسَّر الدرجات على النحو الآتي:

الدرجة ٥ – ممتاز:

تعني أن المتطلب يتحقق بدرجة عالية، مع مستوى أداء يفي بالتوقعات بدرجة قوية.

الدرجة ٤ – جيد جدًا:

تعني أن المتطلب يتحقق بدرجة جيدة جدًا، مع وجود قصور محدود لا يؤثر بصورة جوهرية في مستوى الأداء.

الدرجة ٣ – مقبول:

تعني أن المتطلب يحقق الحد العملي المقبول، مع وجود بعض الجوانب التي تحتاج إلى تحسين أو تطوير.

الدرجة ٢ – ضعيف:

تعني وجود قصور مؤثر في تحقيق المتطلب، ويحتاج هذا القصور إلى معالجة واضحة لتحسين مستوى الأداء.

الدرجة ١ – حرج:

تعني عدم تحقق المتطلب أو وجود قصور جوهري يؤثر بصورة كبيرة في تحقيق الهدف المطلوب.

ثانيًا: تحويل المؤشرات الكمية إلى درجات

يمكن تحويل المؤشرات الكمية إلى درجات من خلال وضع حدود أو نطاقات داخلية لكل مؤشر، بما يتناسب مع طبيعة الخدمة ومتطلباتها ومستوى المخاطر المرتبطة بها.

فعلى سبيل المثال، إذا كان الهدف المحدد لنسبة التوافر هو 99%، فيمكن للمنشأة أن تضع، لأغراض التقييم الداخلي، نطاقات للدرجات على النحو الآتي:

- الدرجة ٥ :عندما تبلغ نسبة التوافر ٩٩٪ فأعلى.
- الدرجة ٤ :عندما تتراوح نسبة التوافر بين ٩٨٪ وأقل من ٩٩.%
- الدرجة ٣ :عندما تتراوح نسبة التوافر بين ٩٧٪ وأقل من ٩٨.%
- الدرجة ٢ :عندما تتراوح نسبة التوافر بين ٩٥٪ وأقل من ٩٧.%
- الدرجة ١ :عندما تكون نسبة التوافر أقل من ٩٥.%

وتُعد هذه الحدود مثالًا تطبيقيًا فقط لتوضيح آلية تحويل المؤشرات الكمية إلى درجات، ولا ينبغي اعتبارها حدودًا معيارية أو تعميمها على جميع المنشآت. إذ ينبغي لكل منشأة أن تحدد حدود التقييم الفعلية وفقًا لمتطلبات الخدمة، ومستوى الأداء المستهدف، وطبيعة المخاطر، والظروف التشغيلية ذات الصلة.

وبذلك يصبح مقياس الدرجات أداة مرنة يمكن تكييفها مع مختلف المؤشرات، بحيث لا تقتصر عملية التقييم على الحكم الوصفي، وإنما تسمح أيضًا بتحويل النتائج الكمية إلى درجات موحدة تسهّل المقارنة والمتابعة واتخاذ إجراءات التحسين.

ثالثًا: تحويل المؤشرات النوعية

في بعض الحالات لا توجد قيمة رقمية مباشرة، مثل ملاءمة التصميم أو كفاية الإجراءات. وهنا يمكن استخدام أسئلة تقييم محددة، مثل:(4)

- هل توجد سياسة معتمدة؟
- هل تطبق السياسة؟
- هل توجد أدلة على التطبيق؟
- هل تراجع السياسة دوريًا؟
- هل توجد مسؤوليات محددة؟

ثم تحول الإجابات إلى درجة وفق قاعدة معلنة.

رابعًا: التعامل مع البيانات غير المتاحة

لا ينبغي منح درجة افتراضية للعنصر الذي لا تتوافر بيانات كافية عنه (٥). ويستخدم أحد التصنيفات الآتية:

- غير مقاس.
- بيانات غير كافية.
- غير منطبق.

ويجب عدم الخلط بين "غير منطبق" و"لم يتم القياس."

خامسًا: التعامل مع المؤشرات الحرجة

قد تؤدي الدرجة الكلية المرتفعة إلى إخفاء قصور حرج في عنصر أمني بالغ الأهمية. ولذلك ينبغي استخدام قاعدة الحد الأدنى، بحيث يمكن أن يمنع وجود قصور حرج في عنصر محدد تصنيف المنظومة باعتبارها "ممتازة" مهما كان المتوسط العام.(6)

وهذه القاعدة مهمة خصوصًا عندما يتعلق القصور بـ:

- مناطق حرجة.
- التسجيل.
- الوصول غير المصرح به.
- انقطاع الخدمة.
- سلامة الأدلة.

المراجع:

.① Katherine Schroeder, Hung Trinh, and Victoria Pillitteri, *Measurement Guide for Information Security: Volume 1*

.② Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 1*

.③ Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 1*

.④ Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 1*

.⑤ Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 2*

.⑥ Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 1*

المبحث السادس: حساب مستوى الكفاءة

بعد تحديد المؤشـــرات والدرجات والأوزان، تأتي مرحلة تجميع النتائج بهدف تكوين صـــورة كلية عن مســـتوى أداء المنظومة. غير أن هذا التجميع ينبغي أن يكون واضـــحًا وقابلًا لإعادة الحســـاب، مع التمييز بين الكفاءة الفنية والتشـــغيلية وبين الفاعلية الأمنية (1).

أولًا: حساب الدرجة المرجحة

يمكن حساب الدرجة المرجحة لكل محور بالصيغة: (2)

الدرجة المرجحة = درجة المحور ÷ ٥ × الوزن النسبي

وبذلك تكون النتيجة النهائية:

النتيجة الكلية = مجموع الدرجات المرجحة لجميع المحاور

وتتراوح النتيجة بين ٠ و١٠٠%.

ثانيًا: تصنيف المستوى العام

نقترح التصنيف الآتي: (3)

لتفسير نتائج مؤشرات الأداء، يمكن تصنيف النتائج ضمن خمسة مستويات رئيسية، بحيث يعكس كل مستوى درجة الفاعلية المحققة:

١. متقدم 90–100%: يدل على مستوى مرتفع جدًا من الأداء والفاعلية.
٢. جيد جدًا 80–89%: يشير إلى أداء قوي مع وجود بعض الجوانب المحدودة التي يمكن تحسينها.
٣. جيد 70–79%: يعكس مســـتوى أداء مقبولًا وفعالًا، مع الحاجة إلى بعض التحسينات.
٤. مقبول 60–69%: يشير إلى تحقيق الحد الأدنى من المستوى المطلوب، مع وجود فجوات تستدعي المعالجة.

٥. أقل من ٦٠٪: ضـــعيف —يدل على انخفاض مســـتوى الفاعلية ووجود حاجة واضحة إلى إجراءات تصحيحية وتحسينات جوهرية.

وبذلك تُستخدم النتيجة المئوية ليس فقط لقياس الأداء، وإنما أيضًا لتحديد مستوى الفاعلية وتوجيه إجراءات التحسين والتصحيح.

وهذا التصنيف أداة داخلية مقترحة وليس تصنيفًا معياريًا دوليًا.

ثالثًا: مثال تطبيقي

إذا حصلت المنظومة على النتائج الآتية:(4)

تقييم منظومة المراقبة من ١٠٠%، لكن ليس كل جانب له نفس الأهمية.

لدينا 8جوانب نقيّمها، وكل جانب له وزن ودرجة من ٥:

- التصميم :أهميته ١٠٪، ودرجته ٤ من ٥ .
- التغطية والجودة :أهميتها ٢٠٪، ودرجتها ٤ من ٥ .
- التوافر :أهميته ١٥٪، ودرجته ٥ من ٥ .
- الكشف :أهميته ١٥٪، ودرجته ٣ من ٥ .
- الاستجابة :أهميتها ١٠٪، ودرجتها ٣ من ٥ .
- التسجيل :أهميته ١٠٪، ودرجته ٤ من ٥ .
- التشغيل :أهميته ١٠٪، ودرجته ٤ من ٥ .
- التكامل :أهميته ١٠٪، ودرجته ٣ من ٥ .

كيف نحسب النتيجة؟

ببساطة، درجة ٥ تعني ١٠٠٪، ودرجة ٤ تعني ٨٠٪، ودرجة ٣ تعني ٦٠.%

ثم نحسب مساهمة كل جانب حسب وزنه.

مثلاً:

التصميم:

درجته ٤ من ٥ = ٨٠%

ووزنه ١٠%

إذن مساهمته.8% =

التغطية والجودة:

4من ٥ = ٨٠%

ووزنها ٢٠%

إذن مساهمتها.16% =

ونفعل الشيء نفسه مع باقي المحاور.

النتيجة النهائية

بعد جمع جميع المساهمات، تكون النتيجة:

الفاعلية الكلية للمنظومة = ٧٤٪ تقريبًا.

وبحسب التصنيف الذي وضعناه سابقًا:

= 74%مستوى "جيد."

- النتيجة : أن المنظومة تعمل بشـــكل جيد، لكنها تحتاج إلى تحســـين بعض الجوانب، خصوصًا الكشف والاستجابة والتكامل.

بمعنى أبســـط جدًا: نقيّم كل جانب من ٥ → نحوله إلى نســـبة → نراعي أهمية كل جانب → نجمع النتائج → نحصل على مستوى فاعلية المنظومة.

- طريقة التقييم

نحن نقيم المنظومة من 100%، ونقســـم هذه النســـبة على عدة جوانب، لأن بعض الجوانب أهم من غيرها.

كل جانب نعطيه درجة من ٥:

- إذا حصل على 5من ٥ ←فهو ممتاز ويأخذ كامل النسبة المخصصة له .
- إذا حصل على 4من ٥ ←فهو جيد ويأخذ ٨٠٪ من النسبة المخصصة له .
- إذا حصل على 3من ٥ ←فهو متوسط ويأخذ ٦٠٪ من النسبة المخصصة له .

وبعد تقييم جميع الجوانب، نجمع النتائج.

في حالتنا كانت النتيجة النهائية .76%

وهذا يعني ببساطة:
المنظومة مستواها جيد، لكنها تحتاج إلى بعض التحسينات حتى تصل إلى مستوى أعلى.
أي أننا لا نقول إن المنظومة ممتازة لمجرد أنها تعمل، بل ننظر إلى التصميم، والتغطية، والتوافر، والكشف، والاستجابة، والتسجيل، والتشغيل، والتكامل، ثم نخرج بحكم عام على مستوى المنظومة.

- وبحسب التصنيف المقترح، يقع الأداء في مستوى جيد .لكن هذا الحكم لا يعني أن جميع جوانب المنظومة جيدة؛ فقد يكون محور الكشف والاستجابة أقل من بقية المحاور، ولذلك ينبغي الانتقال إلى تحليل الفجوات.

رابعًا: حساب مؤشرات الكفاءة الأساسية
يمكن أيضًا حساب مؤشرات مستقلة:(5)
كفاءة التشغيل = (المهام المنفذة وفق المتطلبات ÷ إجمالي المهام المفحوصة) × ١٠٠
كفاءة الاسترجاع = (طلبات الاسترجاع الناجحة ÷ إجمالي الطلبات) × ١٠٠
كفاءة التكامل = (عمليات التكامل الناجحة ÷ إجمالي عمليات الاختبار) × ١٠٠

خامسًا: عدم مساواة الكفاءة بالفاعلية الأمنية
ينبغي التأكيد على أن النتيجة الكلية لا تمثل تلقائيًا "الفاعلية الأمنية" (٦). فقد تكون المنظومة:

- عالية الكفاءة الفنية، ولكن منخفضة الفاعلية الأمنية بسبب سوء التغطية.
- عالية التوافر، ولكن ضعيفة في الكشف.
- ممتازة في التسجيل، ولكن ضعيفة في الاستجابة.
- جيدة في جميع الجوانب التقنية، ولكن غير متوافقة مع الهدف الأمني الأصلي.

ولهذا ينبغي أن يستخدم التقييم الكلي باعتباره أداة مساعدة للحكم لا بديلًا عن التحليل الأمني.

المراجع:

① Katherine Schroeder, Hung Trinh, and Victoria Pillitteri, *Measurement Guide for Information Security: Volume 1*.

② Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 1*.

③ Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 1*.

④ Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 1*.

⑤ Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 1*.

⑥ Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 2*.

المبحث السابع: تحديد نقاط القوة والقصور

لا تكتمل قيمة التقييم بمجرد استخراج النتيجة النهائية؛ إذ إن الغرض العملي هو معرفة المجالات التي تؤدي فيها المنظومة بصورة جيدة، والمجالات التي تعاني قصورًا، ومدى أهمية هذا القصور.(1)

أولًا: تحديد نقاط القوة

تحدد نقطة القوة عندما يحقق العنصر نتيجة مرتفعة مع وجود أدلة موثوقة على استقرار الأداء (٢). ومن أمثلتها:

- ارتفاع نسبة التوافر.
- انخفاض الأعطال.
- نجاح استرجاع التسجيلات.
- ارتفاع جودة المشهد في المناطق الحرجة.
- التزام المشغلين بالإجراءات.
- فعالية التكامل.

ثانيًا: تحديد نقاط القصور

يمكن تصنيف القصور إلى:(3)

أ. قصور فني

مثل: ضعف جودة الصورة، سوء الإضاءة، النقاط العمياء، ضعف التخزين، ضعف الشبكة.

ب. قصور تشغيلي

مثل: تأخر الاستجابة، ضعف التدريب، عدم الالتزام بالإجراءات، ضعف متابعة الإنذارات.

ج. قصور تنظيمي

مثل: غياب السياسات، عدم وضوح المسؤوليات، عدم مراجعة الصلاحيات، ضعف إجراءات التغيير.

د. قصور أمني

مثل: عدم تغطية منطقة حرجة، ضعف الكشف، عدم القدرة على توثيق حدث، ضعف التكامل مع أنظمة الأمن.

ثالثًا: ترتيب القصور

لا ينبغي معالجة جميع أوجه القصور بالطريقة نفسها. ويقترح تصنيف القصور إلى (4):

لتحديد أهمية المشكلات أو نقاط الضعف في منظومة المراقبة، يمكن تصنيفها إلى أربعة مستويات حسب تأثيرها على الأمن:

- حرج: مشكلة خطيرة جدًا قد تؤدي إلى فقدان وظيفة أمنية أساسية أو تعرض أصل مهم للخطر، ولذلك تحتاج إلى معالجة فورية.
- مرتفع: مشكلة تؤثر بشكل كبير في الأداء الأمني، وتحتاج إلى معالجة بأولوية عالية.
- متوسط: مشكلة تؤثر في الأداء، ولكن يمكن السيطرة عليها أو احتواؤها، وتكون أولويتها متوسطة.
- منخفض: مشكلة تأثيرها محدود ويمكن التعامل معها ضمن أعمال التحسين والصيانة الدورية، ولذلك تكون أولويتها منخفضة.

وباختصار:

حرج → نعالجه فورًا

مرتفع → نعالجه بأولوية عالية

متوسط → نعالجه عند توفر الإمكانية

منخفض → نعالجه ضمن التحسين الدوري

رابعًا: ربط القصور بالمخاطر

ينبغي أن يسأل المقيم: ما الخطر الناتج عن هذا القصور؟ فمثلًا: (5)

ضعف تغطية مدخل رئيسي ← احتمال عدم اكتشاف دخول غير مصرح به ← أثر أمني مرتفع.

وبذلك يصبح التقييم أداة لإدارة المخاطر وليس مجرد قائمة بالملاحظات.

المراجع:

① Katherine Schroeder, Hung Trinh, and Victoria Pillitteri, *Measurement Guide for Information Security: Volume 1*.

② Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 1*.

③ Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 1*.

④ International Organization for Standardization, *ISO 31000:2018, Risk management – Guidelines*, (Geneva: ISO, 2018).

⑤ ISO, *ISO 31000:2018*.

المبحث الثامن: تحليل الفجوات

يمثل تحليل الفجوات المرحلة التي تنتقل فيها عملية التقييم من تحديد الوضع الحالي إلى تحديد الفرق بين الوضع القائم والوضع المستهدف. وهو من أهم المراحل التي تسمح بتحويل نتائج التقييم إلى خطة تحسين عملية.(1)

أولًا: مفهوم تحليل الفجوة

يمكن تعريف فجوة الأداء بأنها: الفرق بين المستوى الحالي للأداء والمستوى المستهدف الذي تحدده الأهداف أو المتطلبات أو المعايير المعتمدة .(2)ويمكن تمثيلها بصورة مبسطة:

الفجوة = المستوى المستهدف – المستوى الحالي

وإذا كان المؤشر من النوع الذي تكون فيه القيمة الأقل أفضل، مثل زمن الاستجابة أو معدل الإنذارات الكاذبة، فإن تفسير الفجوة ينعكس وفق طبيعة المؤشر.

ثانيًا: مستويات الفجوة

يمكن تصنيف الفجوات إلى:(3)

١. فجوة متطلبات.
٢. فجوة تصميم.
٣. فجوة تنفيذ.
٤. فجوة تشغيل.
٥. فجوة صيانة.
٦. فجوة بشرية.
٧. فجوة أمنية.
٨. فجوة تكامل.
٩. فجوة حوكمة.

ثالثًا: نموذج تحليل الفجوات

ما المقصود بتحليل الفجوات؟

تحليل الفجوات يعني ببساطة أن نسأل:

أين نحن الآن؟ وأين نريد أن نصل؟ وما الذي يمنعنا من الوصول؟

ثم نحدد أهمية المشكلة وما الذي يجب فعله لمعالجتها.

مثال مبسط على النموذج

1. التغطية:

الوضع الحالي هو 82%، بينما المستوى المطلوب هو 95%.

إذن هناك نقص قدره 13%.

والسبب هو سوء توزيع الكاميرات، ولذلك تعتبر المشكلة ذات أولوية عالية وتحتاج إلى المعالجة.

2. التوافر:

الوضع الحالي هو 97%، بينما المطلوب 99%.

إذن هناك فرق بسيط قدره 2%.

والسبب هو تكرار الأعطال، ولذلك تعتبر المشكلة متوسطة الأولوية.

3. الاسترجاع:

الوضع الحالي هو 80%، بينما المطلوب 95%.

إذن هناك فجوة قدرها 15%.

والسبب هو ضعف فهرسة التسجيلات، ولذلك تعتبر المشكلة عالية الأولوية.

4. التدريب:

الوضع الحالي هو 70%، بينما المطلوب 100%.

إذن هناك فجوة كبيرة قدرها 30%.

والسبب هو نقص البرامج التدريبية، ولذلك تعتبر المشكلة عالية الأولوية.

الخلاصة

الفكرة ببساطة هي:

الوضع الحالي → الوضع المطلوب → الفرق بينهما → سبب الفرق → أهمية المشكلة.

وفي هذا المثال، فإن أكبر فجوة هي التدريب بنسبة ٣٠%، ثم الاسترجاع بنسبة ١٥%، ثم التغطية بنسبة ١٣%، وأخيرًا التوافر بنسبة ٢.%

وهذا يساعد المسؤول على معرفة ما الذي يجب إصلاحه أولًا وما الذي يمكن تأجيله.

رابعًا: تحليل السبب الجذري

لا ينبغي أن يقتصر التقرير على القول إن هناك فجوة، بل ينبغي البحث عن سببها.(4)

مثال :المشكلة :ضعف جودة التسجيل. قد يكون السبب:

- اختيار غير مناسب للكاميرا.
- إعدادات غير صحيحة.
- ضغط مفرط.
- ضعف الشبكة.
- تخزين غير كافٍ.
- عطل في جهاز التسجيل.

ومن ثم ينبغي معالجة السبب الجذري وليس العرض فقط.

خامسًا: ترتيب الفجوات

يمكن استخدام مصفوفة تجمع بين:(5)

أثر الفجوة × احتمال وقوع الخطر × صعوبة المعالجة

لتحديد أولويات التدخل.

سادسًا: تحويل الفجوة إلى إجراء تصحيحي

ينبغي أن يرتبط كل قصور بإجراء محدد:(6)

الفجوة	الإجراء	المسؤول	المدة	مؤشر النجاح
ضعف التغطية	إعادة تصميم بعض النقاط	إدارة الأمن/الفني	30 يومًا	تغطية ≥ ٩٥%
ضعف الاسترجاع	تحسين الفهرسة والتخزين	تقنية المعلومات	20 يومًا	نجاح الاسترجاع ≥ ٩٥%
ضعف التدريب	برنامج تدريبي	إدارة الأمن	45 يومًا	اجتياز ١٠٠٪ من المشغلين

وهذه الآلية تتفق مع المنهج القائم على استخدام القياسات لتحديد أوجه القصور وتوجيه الموارد نحو المجالات التي تحتاج إلى تحسين.(7)

المراجع:

.① Katherine Schroeder, Hung Trinh, and Victoria Pillitteri, *Measurement Guide for Information Security: Volume 1*

.② Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 1*

.③ Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 1*

.④ Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 1*

⑤ International Organization for Standardization, *ISO 31000:2018*.

.⑥ Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 2*

⑦ Shirley M. Radack, *Using Performance Measurements to Evaluate and Strengthen Information System Security*, ITL Bulletin, (Gaithersburg, MD: National Institute of Standards and Technology, 2008).

المبحث التاسع: إعداد تقرير التقييم

يمثل تقرير التقييم المخرج النهائي للعملية، وينبغي ألا يكون مجرد قائمة فنية بالأعطال، بل وثيقة إدارية وفنية وأمنية تساعد متخذ القرار على فهم مستوى الأداء، ومواطن القوة والقصور، والمخاطر، والإجراءات المطلوبة.(1)

أولًا: أهداف التقرير

يهدف التقرير إلى:(2)

- توثيق نتائج التقييم.
- بيان مستوى الأداء.
- تحديد نقاط القوة.
- تحديد أوجه القصور.
- تحديد المخاطر المرتبطة بالقصور.
- ترتيب أولويات المعالجة.
- تحديد الإجراءات التصحيحية.
- دعم قرارات الإدارة.

وتشير منهجية NIST الحديثة إلى أهمية توثيق المقاييس والنتائج وتحليل البيانات واستخدامها في إعداد التقارير ودعم القرارات المتعلقة بالأمن.(3)

ثانيًا: الهيكل المقترح لتقرير التقييم

يقترح أن يتكون التقرير من:(4)

1. صفحة التعريف
   - اسم المنشأة.
   - اسم المنظومة.
   - تاريخ التقييم.
   - الجهة المنفذة.

- فترة القياس.

2. الملخص التنفيذي
   - المستوى العام.
   - أهم نقاط القوة.
   - أهم أوجه القصور.
   - المخاطر الحرجة.
   - التوصيات ذات الأولوية.
3. نطاق التقييم
   - المناطق المشمولة.
   - الأنظمة المشمولة.
   - الفترة الزمنية.
   - العناصر المستثناة.
4. منهجية التقييم
   - المحاور.
   - المؤشرات.
   - مصادر البيانات.
   - طريقة القياس.
   - نظام الدرجات.
   - طريقة حساب النتيجة.
5. النتائج التفصيلية

تعرض النتائج حسب كل محور.

6. مصفوفة المخاطر والفجوات
   - الملاحظة.
   - الخطر.
   - مستوى الخطورة.

- سبب المشكلة.
- الإجراء المطلوب.

7. خطة التحسين

- الإجراء.
- المسؤول.
- الأولوية.
- المدة.
- التكلفة التقديرية عند الحاجة.
- مؤشر النجاح.

ثالثًا: نموذج مختصر للملخص التنفيذي

يمكن أن يقدم التقرير ملخصًا على النحو الآتي: (5)

أظهرت نتائج التقييم أن مستوى الأداء العام لمنظومة المراقبة بلغ ٧٦%، وهو ما يصنف المنظومة ضمن مستوى جيد.

وكان التوافر هو أقوى محور في المنظومة، مما يعني أن النظام يعمل بدرجة جيدة من الاستمرارية والاعتمادية.

أما الاستجابة فكانت أضعف محور، مما يشير إلى الحاجة إلى تحسين سرعة وكفاءة التعامل مع الأحداث والتنبيهات الأمنية.

كما أظهر التقييم وجود فجوة حرجة تتمثل في تغطية منطقة ذات أولوية، وهي فجوة تحتاج إلى معالجة لضمان تحقيق المستوى المطلوب من الحماية.

وبناءً على ذلك، تم تحديد أولويات التحسين على النحو الآتي:

١. الأولوية الأولى: معالجة مشكلة التغطية، وخاصة تغطية المناطق ذات الأولوية الأمنية.

٢. الأولوية الثانية: تحسين الاستجابة، من خلال رفع سرعة وكفاءة التعامل مع التنبيهات والحوادث.

٣. الأولوية الثالثة: رفع مستوى التدريب، لضمان قدرة العاملين على استخدام المنظومة والتعامل مع الأحداث بصورة صحيحة.

وبصورة مختصرة، فإن المنظومة جيدة بشكل عام، ولكن تحسين التغطية والاستجابة والتدريب سيؤدي إلى رفع مستوى فاعليتها الأمنية.

رابعًا: ضوابط جودة التقرير

ينبغي أن يتصف التقرير بـ:(6)

- الموضوعية.
- الوضوح.
- قابلية التحقق.
- التمييز بين الحقيقة والاستنتاج.
- توثيق الأدلة.
- تحديد حدود التقييم.
- عدم المبالغة في النتائج.

خامسًا: التمييز بين النتيجة والتفسير والتوصية

ينبغي ألا تختلط النتيجة بالتوصية.(7)

النتيجة :أظهرت الاختبارات أن نسبة نجاح استرجاع التسجيلات بلغت ٨٢.%

التفسير :تشير النتيجة إلى وجود قصور في القدرة على الاسترجاع مقارنة بالمستوى المستهدف البالغ ٩٥.%

التوصية :يوصى بمراجعة آلية الفهرسة والتخزين وإجراء اختبار استرجاع شامل بعد المعالجة.

وهذا الفصل بين البيانات والتفسير والتوصية يعزز موضوعية التقرير.

سادسًا: إعادة التقييم

لا تنتهي دورة التقييم بإصـــدار التقرير؛ بل ينبغي إعادة القياس بعد تنفيذ الإجراءات التصـــحيحية، للتحقق من انخفاض الفجوة وتحســـن الأداء (٨). ويمكن تمثيل الدورة على النحو الآتي:

التقييم الأولي ← تحديد الفجوات ← الإجراءات التصـــحيحية ← إعادة القياس ← المقارنة ← التحسين المستمر

ويتوافق هذا النهج مع مفهوم التحسين المستمر في نظم الإدارة وإدارة المخاطر والقياس الأمني.(9)

المراجع:

.① Katherine Schroeder, Hung Trinh, and Victoria Pillitteri, *Measurement Guide for Information Security: Volume 1*

.② Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 1*

.③ Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 1* and *Volume 2*

.④ Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 1*

.⑤ Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 1*

.⑥ Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 1*

.⑦ Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 1*

.⑧ Schroeder, Trinh, and Pillitteri, *Measurement Guide for Information Security: Volume 2*

ISO, *ISO 22301:2019*.و؛ ⑨ International Organization for Standardization, *ISO 31000:2018*

خلاصة الفصل الثاني

أظهر هذا الفصل أن تقييم منظومات كاميرات المراقبة لا ينبغي أن يقتصر على التحقق من وجود الأجهزة أو سلامتها الفنية، وإنما ينبغي أن يمثل عملية منهجية تربط بين الأهداف الأمنية، ومتطلبات الاستخدام، والمخاطر، والمؤشرات، والبيانات الفعلية، ومعايير الحكم، والإجراءات التصحيحية.

وقد تبين أن أول خطوة في التقييم هي تحديد الأساس الذي سيبنى عليه الحكم، مع التمييز بين القياس والتقييم. فالقياس ينتج قيمة أو نتيجة، في حين يستخدم التقييم هذه النتائج لإصدار حكم مقارن بالمتطلبات والأهداف.

كما تبين أن التقييم الشامل ينبغي أن يتناول سبعة محاور، تشمل التخطيط والتصميم، والتغطية وجودة المشهد، والتوافر والاستمرارية، والكشف والتحليل، والتشغيل البشري، والتسجيل والاسترجاع، والتكامل والحوكمة والأمن السيبراني.

وأظهر الفصل أهمية بناء مؤشرات كمية ونوعية يمكن استخدامها بصورة قابلة للتكرار، مثل نسبة التغطية، ونسبة التوافر، ومعدل الكشف، ومعدل الإنذارات الكاذبة، ومتوسط زمن الاستجابة، ونسبة نجاح الاسترجاع، ونسبة الالتزام بالإجراءات.

وقد جرى التأكيد على أن المعادلات التشغيلية المقترحة في هذا الفصل ليست معايير دولية إلزامية، وإنما أدوات قياس يمكن للمنشأة تعديلها وفق طبيعة أهدافها ومخاطرها ومستوى الخدمة المطلوب.

كما قدم الفصل بطاقة تقييم تجمع بين المحور والمؤشر والوزن والنتيجة والدرجة والدليل، ثم اقترح نظامًا للدرجات يسمح بتحويل النتائج المختلفة إلى مقياس موحد. وتم كذلك وضع نموذج لحساب النتيجة المرجحة، مع التأكيد على أن النتيجة الرقمية لا ينبغي أن تحجب قصورًا أمنيًا حرجًا.

وانتقل الفصل بعد ذلك إلى تحديد نقاط القوة والقصور وتصنيفها وفق مستوى الأولوية، ثم إلى تحليل الفجوات بين الوضع الحالي والمستوى المستهدف، وربط الفجوات بأسبابها الجذرية وإجراءات المعالجة.

وأخيرًا، جرى تحديد مكونات تقرير التقييم، بحيث لا يكون التقرير مجرد قائمة فنية، وإنما وثيقة تجمع بين النتائج والأدلة والتحليل والمخاطر والتوصيات وخطة التحسين وإعادة القياس.

وبذلك يمكن صياغة منهجية التقييم المتكاملة في النموذج الآتي:

الأهداف الأمنية ← تحديد المخاطر والمتطلبات ← تحديد محاور التقييم ← اختيار مؤشرات الأداء ← جمع الأدلة والبيانات ← القياس والتحقق ← إسناد الدرجات والأوزان ← حساب مستوى الأداء ← تحديد نقاط القوة والقصور ← تحليل الفجوات والأسباب الجذرية ← تحديد الأولويات ← الإجراءات التصحيحية ← إعادة القياس ← التحسين المستمر

ومن ثم فإن السؤال المركزي في تقييم منظومة كاميرات المراقبة لا ينبغي أن يكون: كم عدد الكاميرات الموجودة؟ ولا حتى: هل تعمل الكاميرات؟ بل ينبغي أن يكون:

إلى أي مدى تحقق منظومة المراقبة الأهداف الأمنية المحددة لها، وبأي مستوى من الأداء الفني والتشغيلي والفاعلية الأمنية، وما الفجوات التي تحول دون الوصول إلى المستوى المستهدف؟

أهم نتائج الفصل الثاني

١. تقييم منظومة كاميرات المراقبة عملية منهجية وليست حكمًا انطباعيًا.
٢. ينبغي التمييز بين القياس والتقييم.
٣. يجب أن يرتبط التقييم بالأهداف الأمنية وحالات الاستخدام.
٤. ينبغي أن تراعي عملية التقييم مستوى المخاطر.
٥. يجب الاعتماد على أدلة قابلة للتحقق.
٦. ينبغي أن تكون منهجية التقييم قابلة للتكرار.
٧. يتكون التقييم الشامل من سبعة محاور فنية وتشغيلية وأمنية وتنظيمية.
٨. جودة الصورة تمثل عنصرًا من عناصر التقييم وليست معيارًا وحيدًا.
٩. التوافر والاستمرارية عنصران أساسيان في تقييم المنظومة.
١٠. العنصر البشري يمثل جزءًا من الأداء الفعلي للمنظومة.

١١. التسجيل والاسترجاع عنصران أساسيان في الوظيفة التحقيقية.
١٢. التكامل والأمن السيبراني والحوكمة أصبحت عناصر مهمة في التقييم الحديث.
١٣. ينبغي اختيار مؤشرات الأداء وفق الأهداف وحالات الاستخدام.
١٤. يمكن استخدام مؤشرات كمية مثل التغطية والتوافر والكشف والاسترجاع.
١٥. ينبغي عدم اعتبار المعادلات التشغيلية المقترحة معايير دولية إلزامية.
١٦. بطاقة التقييم تساعد على توحيد عملية جمع وتحليل النتائج.
١٧. ينبغي توثيق مصدر كل نتيجة في بطاقة التقييم.
١٨. يمكن استخدام نظام درجات موحد لتسهيل المقارنة.
١٩. لا ينبغي السماح للمتوسط العام بإخفاء قصور أمني حرج.
٢٠. لا تساوي الكفاءة الفنية الفاعلية الأمنية.
٢١. ينبغي تحديد نقاط القوة والقصور بصورة منفصلة.
٢٢. يجب ترتيب أوجه القصور وفق مستوى المخاطر والأولوية.
٢٣. يمثل تحليل الفجوات حلقة الوصل بين التقييم والتحسين.
٢٤. ينبغي البحث عن الأسباب الجذرية للقصور.
٢٥. يجب ربط كل فجوة بإجراء تصحيحي ومسؤول وموعد ومؤشر نجاح.
٢٦. ينبغي أن يكون تقرير التقييم قابلًا للتحقق والمراجعة.
٢٧. يجب التمييز في التقرير بين النتيجة والتفسير والتوصية.
٢٨. ينبغي إعادة التقييم بعد تنفيذ الإجراءات التصحيحية.
٢٩. يمثل التحسين المستمر المرحلة النهائية لدورة التقييم.
٣٠. القيمة الحقيقية للتقييم تتمثل في قدرته على دعم القرار وتحسين الفاعلية الأمنية.

أسئلة التفكير والتقييم للفصل الثاني

أولًا: أسئلة معرفية

١. ما المقصود بتقييم منظومة كاميرات المراقبة؟
٢. ما الفرق بين القياس والتقييم؟
٣. ما المقصود بالتقييم القائم على المخاطر؟
٤. ما أهم محاور تقييم منظومة المراقبة؟
٥. ما خصائص مؤشر الأداء الجيد؟
٦. كيف تحسب نسبة التغطية؟
٧. كيف تحسب نسبة التوافر؟
٨. ما الفرق بين معدل الكشف ومعدل الإنذارات الكاذبة؟
٩. ما مكونات بطاقة التقييم؟
١٠. ما أهمية نظام الدرجات؟
١١. كيف تحسب الدرجة المرجحة؟
١٢. ما المقصود بالفجوة؟
١٣. ما أنواع الفجوات؟
١٤. ما مكونات تقرير التقييم؟

ثانيًا: أسئلة تحليلية

١. لماذا لا يكفي عدد الكاميرات للحكم على مستوى المنظومة؟
٢. لماذا ينبغي ربط المؤشرات بالأهداف الأمنية؟
٣. كيف يمكن أن تكون المنظومة ذات كفاءة فنية مرتفعة ولكن ذات فاعلية أمنية محدودة؟
٤. لماذا ينبغي عدم الاعتماد على مؤشر واحد؟
٥. كيف يمكن للمتوسط العام أن يخفي قصورًا أمنيًا حرجًا؟
٦. لماذا يعد تحليل السبب الجذري مهمًا في تقييم المنظومة؟
٧. ما العلاقة بين تحليل الفجوات وإدارة المخاطر؟
٨. كيف يؤثر العامل البشري في نتيجة التقييم؟
٩. لماذا ينبغي إعادة التقييم بعد تنفيذ الإجراءات التصحيحية؟

ثالثًا: أسئلة تطبيقية

١. اختر منشأة حقيقية أو افتراضية وحدد أهدافها الأمنية.
٢. حدد سبعة محاور لتقييم منظومة المراقبة في المنشأة.
٣. اختر عشرة مؤشرات مناسبة للتقييم.
٤. صمم بطاقة تقييم متكاملة.
٥. ضع أوزانًا نسبية لمحاور التقييم مع تبريرها.
٦. احسب مستوى الأداء باستخدام نموذج الدرجات المرجحة.
٧. حدد ثلاث نقاط قوة وثلاث نقاط قصور.
٨. أعد مصفوفة لتحليل الفجوات.
٩. حدد الأسباب الجذرية لثلاث فجوات.
١٠. ضع خطة إجراءات تصحيحية.
١١. أعد ملخصًا تنفيذيًا لتقرير التقييم.
١٢. أعد اختبار إعادة تقييم بعد تنفيذ الإجراءات التصحيحية.

قائمة المصادر والمراجع الأساسية للفصل الثاني

أولًا: المعايير الدولية

١. International Electrotechnical Commission. *IEC 62676-4:2025, Video surveillance systems for use in security applications – Part 4: Application guidelines*. 2nd ed. Geneva: IEC, 2025.

٢. International Organization for Standardization. *ISO 31000:2018, Risk management – Guidelines*. Geneva: ISO, 2018.

٣. International Organization for Standardization. *ISO 22301:2019, Security and resilience – Business continuity management systems – Requirements*. Geneva: ISO, 2019.

٤. International Organization for Standardization. *ISO 22320:2018, Security and resilience – Emergency management – Guidelines for incident management*. Geneva: ISO, 2018.

٥. International Organization for Standardization and International Electrotechnical Commission. *ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. Geneva: ISO/IEC, 2022.

ثانيًا: المصادر الحكومية والتقنية

٦. Schroeder, Katherine, Hung Trinh, and Victoria Pillitteri. *Measurement Guide for Information Security: Volume 1 — Identifying and Selecting Measures*. NIST SP 800-55 Vol. 1. Gaithersburg, MD: National Institute of Standards and Technology, 2024.

٧. Schroeder, Katherine, Hung Trinh, and Victoria Pillitteri. *Measurement Guide for Information Security: Volume 2 — Developing an Information Security Measurement Program*. NIST SP 800-55 Vol. 2. Gaithersburg, MD: National Institute of Standards and Technology, 2024.

٨. Radack, Shirley M. *Using Performance Measurements to Evaluate and Strengthen Information System Security*. ITL Bulletin. Gaithersburg, MD: National Institute of Standards and Technology, 2008.

٩. National Institute of Standards and Technology. *Video Quality in Public Safety (VQiPS): Getting Started*. Gaithersburg, MD: NIST.

١٠. National Institute of Standards and Technology. *Video Quality in Public Safety (VQiPS): Use Cases*. Gaithersburg, MD: NIST.

١١. National Institute of Standards and Technology. *Video Quality in Public Safety (VQiPS): Display*. Gaithersburg, MD: NIST.

١٢. National Institute of Standards and Technology. *Video Quality in Public Safety (VQiPS): Processing*. Gaithersburg, MD: NIST.

الفصل الثالث: الاتجاهات المستقبلية للتطور التقني ومستقبل المراقبة الأمنية

تمهيد الفصل

شـــهدت أنظمة المراقبة بالفيديو خلال العقود الأخيرة تحولًا جوهريًا تجاوز حدود الانتقال من الكاميرات التناظرية إلى الكاميرات الرقمية والشبكية. فقد انتقلت المنظومة تدريجيًا من كونها وسيلة لالتقاط الصور وتسجيلها واسترجاعها عند الحاجة، إلى كونها مكوّنًا من مكونات البنية التحتية الأمنية الرقمية، قادرًا على جمع البيانات المرئية، ومعالجتها، واســتخراج مؤشــرات منها، وربطها بمصــادر أخرى للمعلومات، وإنتاج تنبيهات تســاعد العاملين في الأمن على اكتشــاف الأحداث والتعامل معها في وقت أقرب. ويواكب هذا التحول تطور تقنيات الشــبكات، والتخزين، والحوســبة الطرفية، والرؤية الحاسوبية، والتعلم الآلي، والذكاء الاصطناعي، فضلًا عن تطور معايير التكامل والتشغيل البيني بين مكونات منظومة الأمن المادي[1] .

وقد أصبح هذا التحول أكثر أهمية مع التوسع الكبير في عدد الكاميرات وحجم البيانات المرئية الناتجة عنها؛ إذ لم يعد من العملي الاعتماد على المراقبة البشــرية المســتمرة لجميع التدفقات المرئية، خصــوصًــا في المنشــآت والمواقع واســعة النطاق. وتشــير الأدبيات العلمية إلى أن تحليل الفيديو الذكي ظهر استجابةً جزئية لهذه المشكلة، من خلال اســتخدام خوارزميات قادرة على اكتشــاف الأشــخاص والمركبات والأجســام والأفعال والأحداث غير الاعتيادية داخل المشــاهد المرئية. [٢] كما أصــبح البحث الذكي في الفيديو وتتبع الأشـخاص عبر كاميرات متعددة من مجالات البحث والتطوير المتقدمة في أنظمة المراقبة الأمنية[3] .

ولا يعني ذلك أن التطور التقني ســيؤدي إلى إلغاء الدور البشــري في الأمن. فالوظيفة الأســاســية للتقنيات الحديثة ينبغي أن تُفهم في إطار تعزيز القدرة الأمنية البشــرية لا استبدالها بصورة مطلقة. فالخوارزمية قد تكتشف نمطًا بصريًا أو حدثًا غير اعتيادي، لكنها لا تمتلك بالضــرورة الســياق الكامل الذي يحتاج إليه القرار الأمني، كما أن أداء نماذج الذكاء الاصطناعي قد يتأثر بظروف الإضاءة، وزاوية التصوير، وكثافة المشهد، وطبيعة البيئة، واختلاف البيانات التي دُرّبت عليها النماذج عن البيئة التي تُســتخدم

فيها فعليًا. وقد أكدت دراسات حديثة أن الانتقال من الأداء المختبري إلى الاستخدام التشغيلي يظل مرتبطًا بتحديات مثل انحياز البيانات، واختلاف المجال التطبيقي، والقيود الحوسبية، وضعف بعض مقاييس التقييم التشغيلية[4] .

ومن ثم فإن مستقبل المراقبة الأمنية لا ينبغي أن يُقاس بعدد وحدات التصوير أو بارتفاع الدقة البصرية وحدها، وإنما بقدرة المنظومة المتكاملة على تحقيق سلسلة أمنية مترابطة تبدأ من الرصد وجمع البيانات، ثم التحليل واكتشاف المؤشرات، ثم التحقق والتقييم، ثم دعم القرار والاستجابة، ثم حفظ الأدلة والمعلومات اللازمة للتحقيق اللاحق.

وفي هذا السياق، أصبحت المعايير الدولية أكثر اهتمامًا ليس فقط بمتطلبات الصورة والتسجيل، وإنما أيضًا بأداء التحليلات الذكية، والتشغيل البيني، وتبادل البيانات الوصفية والأحداث بين الأنظمة. ويُظهر إصدار IEC 62676-6:2026 ، على سبيل المثال، اتجاهًا واضحًا نحو تقييم أداء أنظمة تحليل محتوى الفيديو الذكية بصورة معيارية، بما يشمل تصنيف الأجسام، واكتشاف أنشطتها، والكشف عن سيناريوهات مركبة مثل التسلل، والتسكع، وسقوط الأشخاص، والتتبع غير المصرح به، والأجسام المتروكة[5] .

وبناءً على ذلك، يناقش هذا الفصل الاتجاهات المستقبلية للمراقبة الأمنية من منظور يجمع بين التطور التقني والوظيفة الأمنية، مع التركيز على التحول الرقمي، والتحليلات الذكية، والذكاء الاصطناعي، وتحليل الفيديو، والأتمتة، والتكامل بين الأنظمة، ثم ينتقل إلى فرص التطور والمخاطر والتحديات التي ينبغي أخذها في الاعتبار عند تصميم وتشغيل منظومات المراقبة المستقبلية.

الاتجاهات المستقبلية للتطور التقني
ومستقبل المراقبة الأمنية
Future Operatiens Center

المبحث الأول: التحول الرقمي

يمثل التحول الرقمي الأســـاس الذي بُنيت عليه معظم الاتجاهات الحديثة في أنظمة المراقبة الأمنية. فقد انتقلت المنظومات تدريجيًا من البنية التناظرية القائمة على الإشارة المرئية التقليدية إلى البنية الرقمية المعتمدة على كاميرات الشـــبكات، وبروتوكولات الاتصال، والخوادم، وأجهزة التخزين، ومنصات إدارة الفيديو.

ولا ينبغي فهم التحول الرقمي على أنه مجرد استبدال الكاميرا التناظرية بكاميرا شبكية؛ فالتحول الحقيقي يحدث عندما تتحول منظومة المراقبة من نظام تسـجيل مسـتقل إلى منظومة معلومات أمنية مترابطة يمكنها تبادل البيانات والأحداث مع بقية مكونات البيئة الأمنية.

فالكاميرا الشبكية الحديثة لا تؤدي وظيفة التقاط الصورة فقط، وإنما يمكن أن تتضمن وظائف للضـــغط والترميز، ومعالجة الصـــورة، واكتشـــاف الحركة، وإنتاج البيانات الوصـفية، وإرسـال الأحداث إلى نظام إدارة الفيديو أو إلى تطبيقات أمنية أخرى. وتوفر مواصـــفاتONVIF ، مثلProfile T ، إطارًا للتوافق في عدد من وظائف الفيديو المتقدم، بما في ذلك H.264 وH.265، وإعدادات التصـــوير، وأحداث الحركة والعبث، وتدفق البيانات الوصفية، وبعض وظائف التحكم والصوت OONVIF .(2)

وتزداد أهمية المعايير المفتوحة في بيئات المراقبة واســعة النطاق؛ لأن الاعتماد الكامل على مورد واحد قد يؤدي إلى ارتفاع تكلفة التوسع والاستبدال والصيانة، كما قد يحد من قدرة المؤسسة على إدخال تقنيات جديدة. وتوضح ONVIF أن التوافق وفق ملفاتها المعتمدة يوفر أســـاسًـــا للتحقق من إمكانية التشـــغيل البيني بين الأجهزة والعملاء المتوافقة، مع بقاء مسؤولية التحقق من المتطلبات الفنية والتنظيمية على عاتق المصمم والمستخدم والمُكامل OONVIF .(3)

ومن الناحية المعمارية، يتجه التحول الرقمي إلى توزيع المعالجة بين ثلاثة مســـتويات رئيسية:

١. المعالجة على مســـتوى الكاميرا أو الحافة (Edge Processing): حيث تنفذ بعض عمليات التحليل داخل الكاميرا نفسها.

٢. المعالجة المحلية أو المركزية : حيث تتم معالجة الفيديو والتحليلات على خوادم أو أجهزة مخصصة داخل المنشأة.

٣. المعالجة السحابية أو الهجينة : حيث تستفيد المنظومة من موارد سحابية أو مراكز بيانات خارج الموقع، مع إمكانية الإبقاء على بعض الوظائف الحساسة محليًا.

ويتيح هذا التوزيع للمصمم اختيار البنية التي تحقق التوازن بين زمن الاستجابة، وعرض النطاق، والخصوصية، والاعتمادية، والتكلفة.

ففي المواقع التي تتطلب استجابة آنية، مثل مداخل المنشآت الحساسة أو المناطق عالية الخطورة، قد تكون المعالجة على الحافة أكثر ملاءمة؛ لأنها تقلل الحاجة إلى إرسال جميع تدفقات الفيديو إلى خادم مركزي. أما في البيئات التي تحتاج إلى تجميع وتحليل أعداد كبيرة من الكاميرات، فقد تكون المعالجة المركزية أو الهجينة أكثر كفاءة.

ومن هنا يمكن القول إن التحول الرقمي أعاد تعريف العلاقة بين الكاميرا والشبكة والخادم والتخزين والتحليل والمستخدم .فلم تعد هذه المكونات تعمل بصورة منفصلة، بل أصبحت أجزاء من منظومة واحدة، ويؤثر ضعف أي عنصر منها في القيمة الأمنية للنظام كله.

الأثر الأمني للتحول الرقمي

يمكن للتحول الرقمي أن يعزز الأمن من خلال:

- تحسين سرعة الوصول إلى الصور والأحداث.
- إتاحة المراقبة المركزية للمواقع المتعددة.
- تسهيل البحث في التسجيلات بدل مراجعتها بصورة يدوية كاملة.
- دعم التنبيهات والأحداث الآلية.
- تسهيل تكامل الفيديو مع أنظمة التحكم بالدخول والإنذار.
- توفير إمكانات أكبر للتحليل واستخراج البيانات الوصفية.
- دعم الإدارة المركزية للحسابات والصلاحيات والإعدادات.

- تحسين القدرة على التوسع مقارنة ببعض البنى التقليدية.

لكن هذه المزايا يقابلها توسع في سطح الهجوم السيبراني؛ فكل كاميرا أو خادم أو واجهة إدارة أو حساب مستخدم أو اتصال شبكي قد يمثل نقطة ينبغي تأمينها. ولذلك فإن الرقمنة لا تعني تلقائيًا زيادة الأمن؛ بل قد تؤدي إلى زيادة المخاطر إذا نُفذت دون هندسة أمنية مناسبة.

ويتعين لذلك إدخال الأمن السيبراني في مرحلة التصميم، بما يشمل تقسيم الشبكة، وإدارة الهوية والصلاحيات، وتحديث البرمجيات، وتأمين واجهات الإدارة، ومراقبة السجلات، وحماية الاتصالات والبيانات. ويقدم إطار NIST CSF 2. 0 أساسًا عامًا لإدارة مخاطر الأمن السيبراني، ولا يقتصر على قطاع بعينه .(4) NNIST CSRC

المراجع:

① Cherilyn Pascoe, Stephen Quinn, Karen Scarfone, *The NIST Cybersecurity Framework (CSF) 2. 0*, (Gaithersburg, MD: National Institute of Standards and Technology, 2024)، صـ. ١ وما بعدها NNIST .

② ONVIF, *Profile T – Advanced Video Streaming*, ONVIF، ينظر في مواصفات Profile T ووظائف بث الفيديو والبيانات الوصفية والأحداث الأمنية OONVIF .

③ ONVIF, *ONVIF Profiles*, ONVIF، ينظر في مفهوم ملفات التوافق وأهميتها في التشغيل البيني بين أجهزة وأنظمة الأمن المادي . OONVIF

④ National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2. 0*, NIST CSWP 29, (Gaithersburg, MD: NIST, 2024). NNIST CSRC

المبحث الثاني: التحليلات الذكية

تمثل التحليلات الذكية إحدى أهم مراحل التطور في أنظمة المراقبة الأمنية؛ إذ تنقل النظام من مجرد عرض وتسجيل ما حدث إلى محاولة اكتشاف ما يستحق انتباه المشغل أثناء حدوثه.

والتحليلات الذكية هي مجموعة من الخوارزميات والوظائف البرمجية التي تستخرج معلومات أو أحداثًا ذات دلالة أمنية من تدفق الفيديو. وقد تشمل هذه الوظائف اكتشاف الحركة، واكتشاف الأشخاص والمركبات، وتتبع الأجسام، واكتشاف الدخول إلى مناطق محددة، ومراقبة العبور عبر خطوط افتراضية، واكتشاف التجمهر أو البقاء غير المعتاد، واكتشاف العبث بالكاميرا، وغيرها من الوظائف بحسب النظام وحالة الاستخدام.

والفرق الجوهري بين التسجيل التقليدي والتحليل الذكي أن الأول يحتفظ بالمعلومة، بينما يحاول الثاني تفسير جزء من المعلومة وتحديد ما إذا كان يستحق توليد حدث أو تنبيه.

ومن الناحية التشغيلية، يمكن تمثيل دورة التحليل الأمني على النحو الآتي:

فيديو ← كشف ← تصنيف ← تتبع ← تطبيق قاعدة ← توليد حدث ← تقييم ← تنبيه ← استجابة.

ولا يعني وجود التحليل الذكي أن جميع النتائج صحيحة؛ إذ تظل الخوارزميات عرضة للأخطاء الناتجة عن الإضاءة، والازدحام، وزوايا التصوير، والعوائق، والطقس، وجودة الصورة، واختلاف البيئة عن البيانات التي صُمم أو دُرّب عليها النظام.

ولهذا ينبغي ألا يقاس نجاح التحليل الذكي بالسؤال: «هل يستطيع النظام اكتشاف الأشياء؟»، وإنما بمجموعة من الأسئلة الأكثر دقة:

- ما معدل الكشف الصحيح؟
- ما معدل الإنذارات الكاذبة؟
- ما معدل الإخفاق في اكتشاف الأحداث الحقيقية؟
- في أي ظروف تتراجع الدقة؟
- ما زمن الاستجابة؟

- هل يستطيع المشغل فهم سبب التنبيه؟
- هل يمكن اختبار أداء النظام دوريًا؟
- ما الإجراء الذي سيترتب على التنبيه؟

وهنا تظهر أهمية التمييز بين الدقة التقنية والقيمة الأمنية .فقد يكون نظام ما عالي الدقة في تصنيف الأشخاص والمركبات، ولكنه ضعيف القيمة الأمنية إذا كانت التنبيهات كثيرة إلى درجة تجعل المشغل يتجاهلها. وبالعكس، قد يكون تحليل محدود الوظائف أكثر فائدة إذا صُمم لمعالجة خطر محدد وكانت تنبيهاته قليلة وذات دلالة عالية.

ومن ثم ينبغي أن يبدأ اختيار التحليلات من تقييم المخاطر الأمنية، لا من قائمة الوظائف المتاحة في كتالوج الشركة.

التحليلات القائمة على الأحداث

أحد الاتجاهات المهمة هو الانتقال من التسجيل المستمر إلى الإدارة القائمة على الأحداث. ففي النظام التقليدي قد يتم تسجيل آلاف الساعات من الفيديو دون أن يكون معظمها ذا قيمة تحقيقية. أما التحليل الذكي فيستطيع إضافة بيانات وصفية للأحداث، بحيث يصبح البحث قائمًا على خصائص محددة، مثل نوع الجسم أو الموقع أو الزمن أو اتجاه الحركة.

وتؤدي البيانات الوصفية دورًا مهمًا في جعل الفيديو قابلًا للبحث الآلي، وهي من الوظائف التي تدعمها بعض معايير التشغيل البيني الحديثة في أنظمة الفيديو الشبكية (5). OONVIF

التحليلات عند الحافة

يتزايد الاتجاه نحو تنفيذ جزء من التحليل بالقرب من مصدر البيانات، أي داخل الكاميرا أو جهاز حوسبة قريب منها. ويتيح ذلك تقليل كمية البيانات التي يجب إرسالها إلى المركز، وتسريع الاستجابة لبعض الأحداث، وتقليل الاعتماد على الاتصال المستمر بمركز المعالجة.

إلا أن المعالجة على الحافة لا تلغي الحاجة إلى التصميم المركزي؛ إذ تحتاج المؤسسة إلى إدارة نماذج التحليل، وتحديث البرمجيات، ومراقبة صحة الأجهزة، وتوحيد الإعدادات، وتقييم الأداء.

التحليلات التكيفية

من الاتجاهات المســـتقبلية المهمة تطوير تحليلات أكثر قدرة على التكيف مع البيئة. فالخوارزمية التي تعمل بكفاءة في موقف معين قد تتراجع كفاءتها في موقع آخر بسبب اختلاف الإضاءة أو الخلفية أو كثافة الحركة أو طبيعة الأشخاص والمركبات.

ولهذا ينبغي أن تصبح عملية المراقبة المستمرة لأداء التحليل جزءًا من إدارة النظام، لا مجرد مرحلة اختبار تسبق التشغيل.

المراجع:

المبحث الثالث: الذكاء الاصطناعي

يعد الذكاء الاصطناعي من أكثر الاتجاهات تأثيرًا في مستقبل المراقبة الأمنية، لكنه في الوقت نفسه من أكثر المجالات التي تتطلب حذرًا منهجيًا؛ لأن استخدام خوارزميات التعلم الآلي في بيئة أمنية يعني أن القرار التقني قد يتأثر بجودة البيانات، ونطاق التدريب، وظروف التشغيل، وطريقة تفسير النتائج، وإجراءات المشغلين.

وتتمثل القيمة الأساسية للذكاء الاصطناعي في قدرته على معالجة كميات ضخمة من البيانات المرئية واستخراج أنماط يصعب على الإنسان متابعتها بصورة مستمرة. ومن تطبيقاته المحتملة: تصنيف الأجسام، والكشف عن السلوكيات أو الأحداث، وتحليل الكثافات، وتتبع الأجسام، ودعم البحث الجنائي في الفيديو، وربط الأحداث عبر كاميرات متعددة.

غير أن الاستخدام الأمني للذكاء الاصطناعي يجب ألا يقوم على افتراض أن الخوارزمية «ترى الحقيقة»؛ فالخوارزمية تنتج تقديرًا أو تصنيفًا احتماليًا ينبغي تفسيره في سياق الاستخدام.

ولهذا يوصي إطار NIST لإدارة مخاطر الذكاء الاصطناعي بالنظر إلى مجموعة متكاملة من خصائص الثقة، من بينها الصلاحية والموثوقية، والسلامة، والأمن والمرونة، والمساءلة والشفافية، والقابلية للتفسير، وتعزيز الخصوصية، والعدالة مع إدارة التحيز الضار AAIRC+1. (6)

وتكتسب هذه المبادئ أهمية خاصة في المراقبة الأمنية؛ لأن الخطأ في النظام لا يكون دائمًا خطأً تقنيًا محدود الأثر. فقد يؤدي التنبيه الخاطئ إلى إرسال فريق أمني إلى موقع غير صحيح، أو إلى تعطيل حركة طبيعية، أو إلى اتهام شخص بصورة غير صحيحة، بينما قد يؤدي عدم اكتشاف حادث حقيقي إلى تفويت فرصة التدخل المبكر.

الذكاء الاصطناعي والإنسان

من الخطأ تصور مستقبل المراقبة الأمنية على أنه استبدال المشغل البشري بالكامل بالذكاء الاصطناعي. والأكثر واقعية هو ظهور نموذج الإنسان المدعوم بالتحليل الذكي.

في هذا النموذج يتولى النظام معالجة الحجم الكبير من البيانات وتحديد الأحداث المحتملة، بينما يحتفظ الإنسان بدور التحقق والتفسير واتخاذ القرار، خصوصًا في الأحداث ذات الأثر العالي.

ويؤكد المختصون أن إدارة مخاطر الذكاء الاصطناعي ينبغي أن تمتد عبر دورة حياة النظام، وأن تشمل الحوكمة والتحديد والقياس والإدارة، مع تقييم الأداء والمخاطر بصورة مستمرة AAIRC+1 .(7)

وبالتالي ينبغي أن تتضمن منظومة المراقبة المستقبلية آليات واضحة للتدخل البشري، وعدم الاعتماد على مخرجات الذكاء الاصطناعي بصورة آلية في القرارات التي تترتب عليها آثار أمنية أو قانونية كبيرة.

الذكاء الاصطناعي والأمن السيبراني

يمثل الذكاء الاصطناعي نفسه مكونًا ينبغي حمايته. فالنظام لا يعتمد فقط على الكاميرا، وإنما على النماذج والبرمجيات والبيانات والبنية الحاسوبية وواجهات التكامل.

وتشير NIST إلى أن أنظمة الذكاء الاصطناعي تواجه مخاطر تتصل بسرية البيانات وسلامتها وإتاحتها، إضافة إلى مخاطر خاصة مثل الهجمات على النماذج والبيانات أو استغلال نقاط النهاية AAIRC+1 .(8)

ومن ثم فإن تأمين أنظمة المراقبة المستقبلية يجب أن يتعامل مع الأمن السيبراني للكاميرا والنظام، والأمن السيبراني للتحليلات والذكاء الاصطناعي، وأمن البيانات الناتجة عنهما باعتبارها طبقات مترابطة.

المراجع:

المبحث الرابع: تحليل الفيديو

يُعد تحليل الفيديو أحد المجالات التي ستتغير فيها وظيفة غرفة المراقبة بصورة جوهرية. ففي النموذج التقليدي يعتمد المشغل على مراقبة شاشات متعددة، وهي مهمة محدودة بسبب القدرة البشرية على الانتباه المستمر.

أما في النموذج المتقدم، فتتحول غرفة المراقبة من مكان لمشاهدة الشاشات إلى مركز لإدارة الأحداث الأمنية .ويصبح الفيديو مصدرًا للبيانات، بينما تتولى التحليلات تحديد المقاطع والأحداث التي تحتاج إلى تدخل بشري.

وتتمثل إحدى أهم مزايا تحليل الفيديو في تقليص الزمن اللازم للوصول إلى المعلومة. فبدل البحث اليدوي في ساعات طويلة من التسجيل، يستطيع المشغل استخدام معايير البحث للوصول إلى الأحداث ذات الخصائص المطلوبة.

وتزداد قيمة هذه الوظيفة في التحقيقات اللاحقة للحوادث، حيث يمكن الربط بين: الوقت + الموقع + الكاميرا + نوع الجسم + اتجاه الحركة + الحدث + المقطع المسجل.

وبذلك يتحول الفيديو من مادة خام إلى سجل زمني للأحداث.

غير أن جودة التحليل تعتمد أساسًا على جودة الصورة. فلا يمكن لخوارزمية متقدمة أن تعوض بصورة كاملة عن كاميرا ذات موقع سيئ أو إضاءة غير مناسبة أو مجال رؤية غير كافٍ. ولذلك يظل التصميم الفيزيائي للكاميرات، والعدسة، وزاوية الرؤية، والإضاءة، والارتفاع، والتباين، وجودة الشبكة والتخزين، عوامل أساسية في نجاح التحليل.

وهذه نقطة منهجية مهمة :الذكاء الاصطناعي لا يلغي هندسة المراقبة؛ بل يجعلها أكثر أهمية.

المبحث الخامس: الأتمتة

تتجه أنظمة المراقبة الأمنية إلى زيادة الاعتماد على الأتمتة، بحيث لا يقتصر دور النظام على إنتاج تنبيه، وإنما يمكن أن يؤدي التنبيه إلى سلسلة من الإجراءات المحددة مسبقًا.

فإذا اكتشفت المنظومة دخولًا غير مصرح به إلى منطقة محظورة، يمكن — وفق تصميم النظام وسياساته — أن ينتج عن ذلك تسجيل الحدث، وإرسال تنبيه إلى غرفة

العمليات، وإظهار الكاميرا المرتبطة بالحدث، وربط الحدث بنظام التحكم بالدخول أو الإنذار، ثم تسجيل إجراءات المشغل.

وتكمن أهمية الأتمتة في تقليل الزمن بين الاكتشاف والاستجابة.

لكن الأتمتة الكاملة ليست دائمًا الخيار الأفضل. ففي بعض الحالات يمكن أن يؤدي خطأ التحليل إلى تنفيذ إجراء غير مناسب. ولذلك ينبغي تحديد مستويات الاستقلالية وفق درجة خطورة الحدث.

ويمكن تصور ثلاثة مستويات:

١. تنبيه فقط: يكتشف النظام الحدث ويترك القرار للمشغل.

٢. استجابة مساعدة: ينفذ النظام إجراءات منخفضة المخاطر تلقائيًا، مع إبقاء القرار النهائي للإنسان.

٣. استجابة آلية: ينفذ النظام الإجراء بصورة تلقائية عندما تكون القاعدة واضحة والمخاطر محدودة والإجراء قابلًا للعكس أو مضبوطًا ضمن سياسة معتمدة.

والقاعدة المهنية هنا هي أن مستوى الأتمتة ينبغي أن يتناسب مع موثوقية الكشف وحجم الضرر المحتمل الناتج عن الخطأ.

المبحث السادس: التكامل المتقدم

يتجه مستقبل أنظمة المراقبة إلى تجاوز التكامل بين الكاميرا وجهاز التسجيل نحو التكامل مع منظومة الأمن المادي بأكملها.

ومن أهم الأنظمة التي يمكن أن تتكامل معها منصة إدارة الفيديو:

- أنظمة التحكم بالدخول.
- أنظمة كشف التسلل.
- أنظمة الإنذار.
- أنظمة إدارة المباني.
- أنظمة إدارة الزوار.
- أنظمة الحماية المحيطية.
- أنظمة الاتصال والطوارئ.

- منصات إدارة الحوادث.
- أنظمة الأمن السيبراني ومراقبة الشبكات.

ويؤدي هذا التكامل إلى بناء صورة تشغيلية مشتركة بدل التعامل مع كل نظام بصورة مستقلة.

وتكتسب معايير التشغيل البيني أهمية متزايدة في هذه البيئة. وقد طورت ONVIF مجموعة من الملفات التي تدعم جوانب مختلفة من التشغيل البيني في منتجات الأمن المادي، ومنها ملفات لأنظمة الفيديو وإدارة البيانات الوصفية والأحداث .(9) OONVIF

كما أعلنت ONVIF في عام ٢٠٢٥ توجهها إلى إنهاء دعم Profile S والتوصية باستخدام Profile T بوصفه البديل الأحدث، وهو مثال واضح على أن التشغيل البيني نفسه يتطور استجابةً لمتطلبات الأمن السيبراني الحديثة .(10) OONVIF

ومن منظور التصميم الأمني، ينبغي ألا يكون التكامل هدفًا في حد ذاته؛ بل يجب أن يخدم سيناريو أمنيًا واضحًا. فتكامل عشرات الأنظمة دون تحديد كيفية استخدام البيانات قد يؤدي إلى التعقيد بدل تحسين الأمن.

المبحث السابع: فرص التطور

يفتح التطور التقني مجالًا واسعًا لتحسين أداء أنظمة المراقبة الأمنية، ويمكن تحديد أبرز فرص التطور المستقبلية في عدد من الاتجاهات.

أولًا: الانتقال من المراقبة إلى التنبؤ

يمكن للتحليلات المتقدمة أن تساعد في اكتشاف الأنماط غير المعتادة، بما يسمح بالانتقال تدريجيًا من الاستجابة للحوادث إلى دعم الوقاية منها.

ومع ذلك ينبغي التفريق بين اكتشاف مؤشرات الخطر والتنبؤ المؤكد بوقوع الجريمة أو الحادث؛ فالأول ممكن تقنيًا في حدود معينة، بينما الثاني يتطلب حذرًا بالغًا من التحيز والإنذارات الكاذبة.

ثانيًا: الحوسبة الطرفية

ستزداد أهمية معالجة الفيديو بالقرب من مصدره، خصوصًا مع ارتفاع أعداد الكاميرات وزيادة الحاجة إلى الاستجابة السريعة وتقليل نقل البيانات.

ثالثًا: المنصات الهجينة

من المرجح أن تجمع الأنظمة المستقبلية بين المعالجة المحلية والسحابية بدل الاعتماد المطلق على أحدهما.

رابعًا: البحث الدلالي في الفيديو

بدل البحث التقليدي بالزمن والكاميرا فقط، ستتطور واجهات البحث لتسمح للمحقق بالوصول إلى الأحداث وفق أوصاف أكثر تعقيدًا، مع بقاء جودة النتائج مرتبطة بجودة البيانات الوصفية والنماذج المستخدمة.

خامسًا: إدارة الفيديو بوصفه أصلًا معلوماتيًا

ستصبح سياسات الاحتفاظ بالفيديو، وتصنيفه، وحمايته، وضبط الوصول إليه، وتحديد دورة حياته، جزءًا من حوكمة المعلومات الأمنية.

سادسًا: زيادة قابلية التشغيل البيني

كلما توسعت المنظومة الأمنية، ازدادت الحاجة إلى معايير تسمح بإدخال أجهزة وبرمجيات من مصادر مختلفة دون فقد الوظائف الأساسية.

سابعًا: رفع موثوقية الأدلة الرقمية

ستزداد أهمية إثبات مصدر الفيديو وسلامته وعدم العبث به، ولا سيما عندما يستخدم التسجيل في التحقيقات أو الإجراءات القانونية.

المبحث الثامن: المخاطر والتحديات المستقبلية

رغم الإمكانات الكبيرة للتطور التقني، فإن مستقبل المراقبة الأمنية يواجه مجموعة من المخاطر التي ينبغي إدارتها منذ مرحلة التصميم.

1. مخاطر الاعتماد المفرط على الذكاء الاصطناعي

قد يؤدي الإفراط في الثقة بنتائج التحليل الآلي إلى تقليل دور المشغل وإضعاف التحقق البشري. ولذلك يجب التعامل مع نتائج الذكاء الاصطناعي بوصفها مدخلًا لاتخاذ القرار لا حقيقة مطلقة.

2. الإنذارات الكاذبة

كلما زادت حساسية النظام دون ضبط مناسب، زادت احتمالية الإنذارات الكاذبة. وإذا تكرر ذلك بصورة كبيرة فقد ينشأ ما يسمى إرهاق التنبيهات، بحيث يفقد المشغل قدرته على التمييز بين الأحداث المهمة وغير المهمة.

3. الأمن السيبراني

توسع الاتصال الشبكي يزيد عدد النقاط التي يجب تأمينها. ومن ثم فإن الكاميرات المستقبلية ينبغي أن تعامل باعتبارها أجهزة شبكية كاملة، وليست أجهزة تصوير فقط.

4. الخصوصية وحماية البيانات

تتزايد أهمية الخصوصية كلما انتقل النظام من مجرد التسجيل إلى التحليل والتصنيف والتتبع. ولذلك ينبغي تحديد الغرض من جمع البيانات، وفترة الاحتفاظ بها، والصلاحيات، وآليات الوصول والمشاركة، وفق القوانين واللوائح المعمول بها في الدولة والقطاع.

5. التحيز الخوارزمي

قد تختلف نتائج النماذج باختلاف ظروف التصوير والبيانات التي طُورت عليها. ولهذا فإن اختبار النظام في بيئة الاستخدام الفعلية أمر ضروري، ولا يكفي الاعتماد على نتائج المورد في بيئة اختبار مختلفة.

ويؤكد المختصون أن صلاحية وموثوقية أنظمة الذكاء الاصطناعي ينبغي تقييمهما بصورة مستمرة، مع توثيق حدود قابلية تعميم النظام خارج الظروف التي جرى تطويره أو اختباره فيها AAIRC. (11).

6. مخاطر الاعتماد على مورد واحد

يمكن أن يؤدي الاعتماد الكامل على منصة أو مصنع واحد إلى مخاطر تتعلق بالتكلفة، والاستمرارية، والتوافق، وتحديثات البرمجيات، والقدرة على الانتقال إلى بدائل مستقبلية.

7. تقادم التكنولوجيا

سرعة التطور تجعل بعض الأجهزة والبرمجيات عرضة للتقادم. ولذلك يجب عند التصميم النظر إلى دورة الحياة الكاملة وليس تكلفة الشراء الأولية فقط.

8. مخاطر التخزين

كلما ارتفعت الدقة ومعدلات الإطارات وعدد الكاميرات وفترة الاحتفاظ، ارتفعت متطلبات التخزين والشبكة. ويجب النظام المتقدم الذي يفقد الاتصال أو الطاقة أثناء الحادث قد يكون أقل قيمة من نظام أبسط لكنه أكثر اعتمادية. ولهذا ينبغي دمج مصادر الطاقة الاحتياطية، وتصميم الشبكات بصورة مرنة، ووضع ألا ينظر إلى التخزين باعتباره مساحة قرص فقط، بل باعتباره عنصرًا من عناصر استمرارية الأدلة الرقمية.

9.انقطاع الشبكة أو الطاقة

النظام المتقدم الذي يفقد الاتصال أو الطاقة أثناء الحادث قد يكون أقل قيمة من نظام أبسط لكنه أكثر اعتمادية. ولهذا ينبغي دمج مصادر الطاقة الاحتياطية، وتصميم الشبكات بصورة مرنة، ووضع خطط للتشغيل عند فشل بعض المكونات.

10.الفجوة بين التقنية والإجراءات

قد تمتلك المؤسسة أفضل الكاميرات وأحدث خوارزميات الذكاء الاصطناعي، لكنها لا تحقق مستوى الأمن المطلوب إذا لم تكن لديها إجراءات واضحة للتعامل مع التنبيهات، وتوثيق الحوادث، وحفظ الأدلة، وإدارة الصلاحيات، والصيانة، والتدريب.

وهنا تظهر قاعدة أساسية في هندسة الأمن:

لا تحقق التقنية وحدها الأمن؛ وإنما يتحقق الأمن من تكامل التقنية مع التصميم والإجراءات والأفراد والحوكمة.

خلاصة الفصل

يتضح من تحليل الاتجاهات المستقبلية أن أنظمة المراقبة الأمنية تمر بمرحلة انتقال جوهرية من أنظمة تسجيل الفيديو إلى منصات ذكية لإدارة المعلومات والأحداث الأمنية.

ويتمثل جوهر هذا التحول في خمسة انتقالات مترابطة:

من التسجيل إلى التحليل، ومن التحليل إلى الفهم، ومن الفهم إلى التنبيه، ومن التنبيه إلى الاستجابة، ومن الاستجابة إلى إدارة المخاطر.

غير أن هذا التطور لا يعني أن التقنية أصبحت قادرة على الاستغناء عن التصميم الأمني أو العنصر البشري. بل على العكس؛ فكلما أصبحت المنظومة أكثر ذكاءً وتعقيدًا،

ازدادت الحاجة إلى الحوكمة، والاختبار، والتحقق، والأمن السيبراني، وإدارة المخاطر، وحماية الخصوصية.

ويجب لذلك أن يقوم التصميم المستقبلي لأنظمة المراقبة على مبدأ الأمن بالتصميم (Security by Design)، بحيث تؤخذ المخاطر الأمنية والتقنية والسيبرانية والخصوصية في الاعتبار منذ المراحل الأولى للمشروع.

كما ينبغي أن يخضع الذكاء الاصطناعي لمبدأ الثقة المقيسة لا الثقة المفترضة؛ أي أن أداء النظام يجب أن يقاس ويختبر ويراقب بصورة مستمرة، وأن تكون حدوده معروفة للمستخدمين. ويؤكد إطار NIST لإدارة مخاطر الذكاء الاصطناعي أن إدارة المخاطر عملية مستمرة تمتد عبر دورة حياة النظام، وأن وظائف الحوكمة والتحديد والقياس والإدارة ينبغي أن تكون مترابطة AAIRC+1. (12)

ومن ثم فإن مستقبل المراقبة الأمنية الأكثر نضجًا لن يكون بالضرورة المستقبل الذي يحتوي على أكبر عدد من الكاميرات أو أكثر الخوارزميات تعقيدًا، وإنما المستقبل الذي يستطيع تحقيق أفضل توازن بين:

الدقة الأمنية، وسرعة الاستجابة، والاعتمادية، والأمن السيبراني، وقابلية التشغيل البيني، والتكلفة، والخصوصية، والحوكمة.

وبهذا المعنى، تصبح كاميرات المراقبة جزءًا من منظومة أمنية أوسع، يكون هدفها النهائي ليس «رؤية كل شيء»، وإنما رؤية ما يهم، وفهم ما يحدث، واكتشاف الخطر في الوقت المناسب، ودعم القرار الأمني، والمحافظة على الأدلة، وتقليل احتمالية وقوع الضرر وآثاره.

المراجع:

⑨ ONVIF, *ONVIF Profiles*, ONVIF، ينظر في ملفات التشغيل البيني لأنظمة الأمن المادي، بما فيها أنظمة الفيديو والبيانات الوصفية والأحداث OONVIF .

⑩ ONVIF, *ONVIF to End Support for Profile S; Recommends Profile T as Replacement*, 9 October 2025. OONVIF

⑪ National Institute of Standards and Technology, *AI RMF Core*, ينظر في متطلبات قياس صلاحية وموثوقية النظام وتوثيق حدود قابليته للتعميم AAIRC .

⑫ Elham Tabassi, *Artificial Intelligence Risk Management Framework (AI RMF 1. 0)*, NIST AI 100-1, (Gaithersburg, MD: National Institute of Standards and Technology, 2023)، وينظر في وظائف الحوكمة والتحديد والقياس والإدارة لإدارة مخاطر الذكاء الاصطناعي.

المبادئ الأساسية لفاعلية منظومة المراقبة

يمكن اختزال المنهج المتكامل للفاعلية في مجموعة من المبادئ الأساسية:

1. مبدأ الغرض الأمني

ينبغي أن يكون لكل عنصر في المنظومة غرض أمني محدد يمكن تفسيره وقياس مدى تحقيقه.

2. مبدأ المخاطر أولًا

يجب أن يوجه مستوى الحماية إلى مستوى المخاطر، بحيث تحصل المناطق والأصول الأكثر تعرضًا للتهديد على الأولوية المناسبة.

3. مبدأ الوظيفة قبل المواصفة

لا ينبغي اختيار الكاميرا بناءً على الدقة أو عدد الميجابكسل فقط، وإنما بناءً على الوظيفة التي ستؤديها والظروف التي ستعمل فيها.

4. مبدأ التغطية الفعالة

وجود مجال رؤية لا يعني بالضرورة وجود تغطية أمنية فعالة؛ إذ يجب أن تكون الصورة مناسبة للمهمة المطلوبة، مع مراعاة الزوايا والمسافات والإضاءة والعوائق.

5. مبدأ جودة الصورة القابلة للاستخدام

المعيار النهائي لجودة الصورة هو قدرتها على دعم القرار الأمني، والكشف، والتعرف، والتوثيق، والتحقيق بحسب الوظيفة المطلوبة.

6. مبدأ الاستمرارية

ينبغي تصميم وتشغيل المنظومة بما يضمن استمرار الخدمة، بما في ذلك الطاقة، والتخزين، والشبكات، والصيانة، والتعامل مع الأعطال.

7. مبدأ سلامة الأدلة

يجب حماية التسجيلات من الفقد والتعديل والوصول غير المصرح به، مع المحافظة على دقة التوقيت وإجراءات الحفظ والاسترجاع والتوثيق.

8. مبدأ أقل صلاحية

ينبغي منح كل مستخدم الصلاحيات التي يحتاج إليها لأداء عمله فقط، مع استخدام حسابات فردية وسجلات وصول ومراجعة دورية للصلاحيات.

.9مبدأ قابلية القياس

ينبغي أن تكون عناصر التقييم قابلة للقياس أو التحقق، وأن تكون النتيجة قابلة للتفسير وإعادة الاختبار.

.10مبدأ التحسين المستمر

لا ينبغي اعتبار تقييم المنظومة إجراءً لمرة واحدة، وإنما دورة مستمرة:

تحديد الأهداف ← تحليل المخاطر ← التصميم والتقييم ← تحديد الفجوات ← المعالجة ← إعادة التقييم ← التحسين المستمر.

- الدروس المستفادة

تكشف الدراسة المتكاملة لمنظومات المراقبة عن عدد من الدروس العملية المهمة.

أول هذه الدروس أن الاستثمار في التكنولوجيا لا يضمن وحده تحقيق الأمن .فقد تكون الكاميرات حديثة وعالية الدقة، بينما يؤدي سوء التوزيع أو ضعف الإضاءة أو قصور التخزين أو ضعف التشغيل إلى انخفاض القيمة الأمنية للمنظومة.

والدرس الثاني أن أكبر الأخطاء تبدأ عادة من مرحلة التخطيط .فإذا لم تحدد المنشأة أهدافها الأمنية ومناطق المخاطر والوظائف المطلوبة للصورة منذ البداية، فإن معالجة المشكلات بعد التركيب قد تصبح أكثر تكلفة وتعقيدًا.

أما الدرس الثالث فهو أن المنظومة ينبغي أن تُقيّم ككل مترابط .فلا يصح تقييم الكاميرات بمعزل عن العدسات والإضاءة والشبكة والتسجيل والتخزين والمشغلين والصيانة والأمن السيبراني.

والدرس الرابع أن الكمية لا تعوض سوء التوزيع .إضافة كاميرات جديدة إلى منظومة تعاني من سوء التصميم قد تزيد عدد الأجهزة دون أن تعالج المشكلة الأساسية.

والدرس الخامس أن الأدلة الموضوعية أكثر قيمة من الانطباعات .فبدل القول إن منطقة ما "تبدو جيدة"، ينبغي تحديد سبب الحكم: نسبة التغطية، أو نتيجة اختبار جودة الصورة، أو مستوى كثافة البكسلات المناسب للوظيفة، أو نسبة التسجيل المتاح، أو زمن استرجاع التسجيل.

والدرس السادس أن نقاط الضعف يجب أن ترتبط بالمخاطر .فليس كل قصور فني متساويًا في أهميته الأمنية، ولذلك ينبغي أن يوجه ترتيب المعالجة وفق أثر القصور في المخاطر ذات الأولوية.

والدرس السابع أن العنصر البشري لا يقل أهمية عن العنصر التقني .فالمنظومة تحتاج إلى مشغلين مؤهلين، وإجراءات واضحة، ومناوبات مناسبة، وتدريب مستمر، وآلية للتعامل مع الأعطال والأحداث.

والدرس الأخير أن التقييم الناجح هو الذي يؤدي إلى تغيير قابل للقياس .فإذا انتهى التقييم إلى قائمة طويلة من الملاحظات دون خطة تنفيذ وإعادة اختبار، فإن قيمته الإدارية والأمنية تظل محدودة.

- التوصيات

استنادًا إلى الإطار المتكامل الذي تناولناه، يمكننا تقديم التوصيات الآتية:

١. اعتماد منهج قائم على المخاطر عند تصميم أو إعادة تقييم منظومات المراقبة.
٢. تحديد الوظيفة الأمنية المطلوبة لكل منطقة قبل اختيار الكاميرا ومواصفاتها.
٣. إجراء مسح ميداني شامل قبل التصميم أو إعادة التوزيع، يشمل المداخل والمخارج والممرات والمناطق الحساسة والمحيط الخارجي وظروف الإضاءة والعوائق.
٤. استخدام معايير قابلة للقياس في تقييم جودة الصورة بدل الاعتماد على الدقة الاسمية للكاميرا وحدها.
٥. التحقق ميدانيًا من الأداء النهاري والليلي وفي ظروف الإضاءة الصعبة.
٦. إجراء حسابات التخزين بناءً على معدل البت ونمط التسجيل ومدة الاحتفاظ الفعلية، مع مراعاة هامش مناسب للاعتمادية والتوسع.
٧. وضع سياسة واضحة للاحتفاظ بالتسجيلات وفق المتطلبات الأمنية والقانونية والتنظيمية للمنشأة.
٨. تطبيق حسابات مستخدمين فردية وصلاحيات مبنية على الأدوار ومنع استخدام الحسابات المشتركة.

٩. فصل منظومة المراقبة عن الشبكات غير الضرورية وتطبيق الضوابط المناسبة لحماية الاتصالات والأجهزة والتسجيلات.

١٠. وضع برنامج صيانة وقائية موثق يشمل الكاميرات وأجهزة التسجيل والشبكات ومصادر الطاقة والتخزين.

١١. تطوير برامج تدريب دورية للمشغلين تشمل تشغيل النظام، واكتشاف الأحداث، والاستجابة، واسترجاع التسجيلات، وإجراءات الطوارئ.

١٢. مراجعة ملاءمة نظام المناوبات وعدد العاملين بما يحقق تغطية تشغيلية مستدامة دون الاعتماد على ساعات عمل تؤدي إلى إرهاق المشغلين.

١٣. إنشاء إجراءات واضحة للتعامل مع الأعطال والحوادث تتضمن الإبلاغ والتصعيد والاستجابة والتوثيق والإغلاق.

١٤. تطبيق آليات مناسبة لحماية التسجيلات المهمة وضمان سلامتها وإمكانية استخدامها عند الحاجة.

١٥. إجراء تقييم دوري شامل للمنظومة بدل انتظار حدوث حادث أمني لاكتشاف أوجه القصور.

١٦. ربط نتائج التقييم بخطة تحسين رسمية تتضمن الأولوية والمسؤولية والمدة والتكلفة ومؤشر النجاح.

١٧. إعادة التقييم بعد تنفيذ الإجراءات التصحيحية للتأكد من أن المشكلة قد عولجت فعليًا، وليس فقط تسجيل إتمام الإجراء إداريًا.

١٨. عدم اعتبار أي نسبة تقييم نهائية دون بيان منهج احتسابها، بما في ذلك الأوزان ومقياس الدرجات والأدلة المستخدمة.

- آفاق التطوير

تشهد منظومات المراقبة تحولًا متسارعًا من الأنظمة التقليدية التي تركز على التسجيل والمشاهدة إلى منظومات أكثر تكاملًا وذكاءً. ومن المتوقع أن تتجه عملية التطوير خلال السنوات المقبلة إلى عدة مسارات.

أول هذه المسارات هو التحليلات المرئية الذكية التي تساعد في اكتشاف الأحداث والأنماط غير المعتادة وتقليل العبء الواقع على المشغلين. غير أن إدخال هذه التقنيات

ينبغي ألا يكون هدفًا بحد ذاته، بل يجب أن يرتبط باحتياج أمني واضح، وأن يخضع لضوابط الدقة والخصوصية والإشراف البشري.

وثانيها هو التكامل بين منظومة المراقبة وبقية الأنظمة الأمنية، مثل التحكم في الدخول، وأنظمة الإنذار، وإدارة الزوار، وأنظمة إدارة المباني والطوارئ. ويسمح هذا التكامل بالانتقال من مجرد تسجيل الأحداث إلى دعم الاستجابة لها.

وثالثها هو تطور تقنيات التصوير والمعالجة والتخزين، بما يتيح الحصول على تفاصيل أفضل واستخدام أكثر كفاءة للموارد، مع ضرورة تقييم هذه التقنيات وفق احتياجات المنشأة الفعلية وليس وفق حداثة المنتج.

ورابعها هو ازدياد أهمية الأمن السيبراني لمنظومات المراقبة نتيجة توسع اتصال الكاميرات وأجهزة التسجيل بالشبكات. وبالتالي سيصبح تقييم أمن المنظومة جزءًا أساسيًا من أي تقييم شامل لفاعليتها.

وخامسها هو الانتقال نحو التقييم المستمر القائم على البيانات، بحيث لا ينتظر المسؤول إجراء تقييم سنوي لاكتشاف المشكلات، بل تعتمد المنشأة على مؤشرات أداء مستمرة مثل توفر الكاميرات، ونسبة التسجيل، وأزمنة الأعطال، وجودة الصورة، وأداء التخزين، ونتائج الاختبارات الدورية.

كما ستزداد أهمية الحوكمة والخصوصية والاستخدام المسؤول للبيانات المرئية، خصوصًا مع اتساع استخدام التحليلات الذكية والتعرف الآلي. وهذا يفرض تحقيق توازن بين متطلبات الأمن وبين حماية حقوق الأفراد والالتزام بالأنظمة واللوائح ذات الصلة.

المبحث الخامس: الأتمتة

أولًا: مفهوم الأتمتة الأمنية

الأتمتة هي نقل بعض الإجراءات المتكررة من التنفيذ اليدوي إلى التنفيذ الآلي وفق قواعد ومعايير محددة مسبقًا.

وفي منظومات المراقبة يمكن أن تبدأ الأتمتة من اكتشاف حدث معين، ثم توليد تنبيه، ثم ربطه بالكاميرات ذات الصلة، ثم توجيهه إلى المشغل أو النظام المختص.

ثانيًا: الأتمتة ودورة الاستجابة

يمكن تمثيل دورة الأتمتة الأمنية على النحو الآتي:

اكتشاف ← تصنيف أولي ← تنبيه ← تحقق ← تصعيد ← استجابة ← توثيق.

وتختلف درجة الأتمتة المناسبة بحسب مستوى المخاطر.

ففي حدث منخفض المخاطر يمكن أن تكون الاستجابة آلية بدرجة أكبر، بينما تتطلب الأحداث عالية التأثير مستوى أعلى من التحقق البشري.

ثالثًا: مزايا الأتمتة

تتمثل أهم فوائدها في:

- تقليل زمن الاستجابة.
- تقليل الأعمال المتكررة.
- تحسين الاتساق في تنفيذ الإجراءات.
- تسريع الوصول إلى البيانات ذات الصلة.
- تقليل العبء التشغيلي.
- تحسين توثيق الأحداث.

رابعًا: مخاطر الأتمتة

الأتمتة ليست مرادفًا للكفاءة دائمًا.

فإذا كانت القاعدة غير صحيحة أو كانت البيانات غير موثوقة، فقد يؤدي تنفيذ الإجراء بصورة آلية إلى تكرار الخطأ بسرعة وعلى نطاق واسع.

ومن هنا ينبغي تطبيق مبدأ:

أتمتة ما يمكن التحقق منه، وإبقاء القرارات الحساسة تحت إشراف بشري مناسب.

المراجع:

①ينظر NIST : ، *Artificial Intelligence Risk Management Framework*، فيما يتعلق بإدارة المخاطر والاختبار والإشـــراف البشـــري في الأنظمة الذكية NNIST AI .
Resource Center+1

المبحث السادس: التكامل المتقدم

أولًا: من الأنظمة المنفصلة إلى البيئة الأمنية الموحدة

كان من الشائع أن تعمل كاميرات المراقبة والتحكم في الدخول وأنظمة الإنذار بصورة منفصلة، بحيث يدير كل نظام بياناته وأحداثه.

أما الاتجاه الحديث فيسعى إلى زيادة التكامل بين هذه الأنظمة بحيث يصبح الحدث الأمني قابلًا للربط عبر أكثر من مصدر.

ثانيًا: التكامل مع التحكم في الدخول

يمكن ربط حدث الدخول بسجل الكاميرا في المنطقة نفسها، بحيث يصبح بالإمكان معرفة:

- من قام بالدخول.
- متى حدث الدخول.
- أين حدث.
- ماذا سجلت الكاميرا في اللحظة نفسها.

وهذا يزيد من قيمة كل نظام من خلال الاستفادة من بيانات النظام الآخر.

ثالثًا: التكامل مع أنظمة الإنذار

يمكن ربط الإنذار بالكاميرات القريبة بحيث يتحول الحدث من مجرد رسالة:

"حدث إنذار"

إلى:

"حدث إنذار في موقع محدد، وهذه هي المشاهد المرتبطة به".

وهذا يوفر للمشغل معلومات أفضل للتحقق قبل اتخاذ إجراء.

رابعًا: قابلية التشغيل البيني

يمثل التشغيل البيني عنصرًا أساسيًا في البيئات متعددة الموردين.

وتوفر ONVIF ملفات تعريف تحدد مجموعات من الوظائف التي يجب أن تدعمها الأجهزة والعملاء المتوافقة، بهدف تسهيل التوافق بين المنتجات المختلفة. كما تشمل المنظومة ملفات تعريف مرتبطة بالفيديو والبيانات الوصفية والأحداث والتخزين والتكامل (1) .

ومن المهم هنا التمييز بين وجود شعار أو ادعاء بالتوافق وبين التحقق الفعلي من المطابقة؛ إذ تشير ONVIF إلى أن قاعدة بيانات المنتجات المتوافقة هي المرجع الرسمي للتحقق من المطابقة OONVIF (2) .

خامسًا: الاتجاه نحو السحابة

يمثل الفيديو السحابي أو Video Surveillance as a Service اتجاهًا متناميًا، ويسعى ONVIFحاليًا إلى تطوير Profile V لتوحيد جوانب من البث والتسجيل والإشعارات في أنظمة المراقبة السحابية، مع التركيز على التشفير والتكامل وعدم الارتباط بمورد واحد OONVIF (3) .

وهذا الاتجاه قد يوفر مرونة في التوسع والإدارة، لكنه يفرض أسئلة إضافية حول:

- مكان تخزين البيانات.
- الاعتماد على الاتصال الخارجي.
- أمن الحسابات.
- التوافر.
- الخصوصية.
- التكاليف طويلة الأجل.
- سياسات الاحتفاظ والحذف.

سادسًا: التحدي المستقبلي للتكامل

كلما زادت الأنظمة المتكاملة، زادت قيمة المنظومة، ولكن زادت أيضًا نقاط الفشل والاعتماد المتبادل.

ومن ثم ينبغي ألا يكون هدف التصميم هو أكبر قدر ممكن من التكامل، بل التكامل الذي يضيف قيمة أمنية قابلة للقياس دون خلق تعقيد غير ضروري.

المراجع:

ONVIF ① ، *ONVIF Profiles* ، حول مفهوم ملفات التعريف والتوافق بين الأجهزة والعملاء OONVIF .

ONVIF — *Standardizing IP Connectivity for Physical Security*. OONVIF ،② ONVIF

Profile V — Release Candidate: For Cloud Video Streaming, Recording and Event Notifications. OONVIF ،③ ONVIF

المبحث السابع: فرص التطور

لا ينبغي النظر إلى التطور التقني على أنه زيادة في تعقيد المنظومة فقط، بل بوصفه فرصة لإعادة تعريف القيمة الأمنية للمراقبة بالفيديو.

أولًا: تحسين الكشف المبكر

تتيح التحليلات الذكية والذكاء الاصطناعي إمكانية اكتشاف بعض الأحداث أو الأنماط غير المعتادة بصورة أسرع من الاعتماد الكامل على المراقبة البشرية.

لكن ينبغي التعامل مع ذلك باعتباره قدرة على دعم الكشف وليس ضمانًا لاكتشاف جميع المخاطر.

ثانيًا: تحسين كفاءة المشغل

يمكن للأنظمة الذكية تقليل كمية المعلومات التي يحتاج المشغل إلى مراجعتها يدويًا، من خلال إعطاء الأولوية للأحداث الأكثر أهمية.

وبذلك يصبح دور المشغل أكثر تخصصًا، ويتحول من مراقب للشاشات إلى محلل ومتحقق ومدير للاستجابة.

ثالثًا: تسريع التحقيقات

يتيح البحث الذكي الوصول إلى المعلومات ذات الصلة بصورة أسرع، وهو ما قد يقلل الوقت المطلوب لمراجعة التسجيلات.

وتظهر القيمة بصورة أكبر في المنشآت التي تحتوي على أعداد كبيرة من الكاميرات ومعدلات تسجيل مرتفعة.

رابعًا: رفع كفاءة الموارد

يمكن للتقنيات التحليلية أن تساعد المنشأة في الحصول على قيمة أكبر من البنية التحتية القائمة، بدل أن يكون الحل في جميع الحالات هو زيادة عدد الكاميرات.

ومن منظور اقتصادي وأمني، فإن السؤال الصحيح هو:

هل يمكن زيادة القيمة الأمنية للمنظومة قبل زيادة حجمها؟

خامسًا: دعم القرارات الأمنية

يمكن للبيانات المتراكمة أن تساعد في تحديد:

- المناطق ذات النشاط المرتفع.

- أوقات زيادة الحركة.
- تكرار الحوادث.
- الأعطال المتكررة.
- المناطق التي تحتاج إلى إعادة تصميم.
- الاحتياجات المستقبلية للتوسع.

وهنا تتحول بيانات المراقبة من سجل تاريخي إلى مصدر يدعم التخطيط الأمني.

سادسًا: دعم الصيانة التنبؤية

يمكن الاستفادة من بيانات النظام وسجلات الأعطال لاكتشاف مؤشرات قد تسبق بعض الأعطال، بما يساعد على الانتقال تدريجيًا من الصيانة التصحيحية إلى الصيانة الوقائية والتنبؤية حيثما كانت البيانات والتقنية تسمح بذلك.

المراجع:

① ينظر IEC : ، *IEC 62676-4:2025*، فيما يتعلق بدورة حياة أنظمة المراقبة والتخطيط والتصميم والاختبار والتشغيل والصيانة IIEC Webstore .

المبحث الثامن: المخاطر والتحديات المستقبلية

أولًا: الأمن السيبراني

كلما أصبحت الكاميرات أكثر اتصالًا بالشبكات والأنظمة الخارجية، أصبحت جزءًا من سطح الهجوم السيبراني للمنشأة.

ولذلك يجب أن تشمل إدارة المخاطر:

- إدارة الحسابات والصلاحيات.
- تحديث البرمجيات.
- حماية الشبكة.
- مراقبة النشاط غير المعتاد.
- حماية واجهات الإدارة.
- إدارة دورة حياة الجهاز.
- التعامل مع انتهاء الدعم البرمجي.

وتؤكد إرشادات NIST الحديثة الخاصة بأمن أجهزة إنترنت الأشياء أهمية النظر إلى أمن الجهاز منذ مرحلة التصميم والاقتناء وحتى الدعم وما بعد البيع NNIST (1) .

Computer Security Resource Center+1

ثانيًا: الخصوصية وحماية البيانات

تتزايد حساسية الخصوصية كلما انتقلت المنظومة من التسجيل إلى التعرف والتحليل والاستدلال.

فالكاميرا التقليدية تسجل المشهد، بينما تستطيع الأنظمة التحليلية الحديثة استخراج خصائص ومعلومات إضافية منه.

وهذا يفرض ضرورة تحديد:

- الغرض من الجمع.
- نطاق الاستخدام.
- الأشخاص المخولين بالوصول.
- مدة الاحتفاظ.

- قواعد مشاركة البيانات.
- آليات الحذف.
- متطلبات حماية البيانات.

ثالثًا: الانحياز والأخطاء الخوارزمية

قد تختلف دقة نماذج الذكاء الاصطناعي باختلاف البيئة والبيانات وظروف التصوير.

لذلك لا ينبغي اعتماد النتيجة الخوارزمية دون معرفة مستوى أدائها في البيئة التي تستخدم فيها.

ويؤكد المختصون أن صلاحية وموثوقية أنظمة الذكاء الاصطناعي تتطلب الاختبار والقياس والمراقبة المستمرة، وأن إدارة المخاطر يجب أن تراعي طبيعة الاستخدام وشدة النتائج المحتملة للخطأ NNIST AI Resource Center+1 (2) .

رابعًا: الإنذارات الكاذبة وإرهاق المشغل

يمكن أن تؤدي زيادة التحليلات إلى زيادة عدد التنبيهات.

وإذا لم تتم معايرة النظام بصورة مناسبة، فقد يتحول التنبيه من أداة مساعدة إلى عبء تشغيلي.

وهنا تصبح جودة النظام مرتبطة ليس فقط بقدرته على اكتشاف الأحداث، وإنما بقدرته على تمييز الأحداث المهمة عن الأحداث غير المهمة.

خامسًا: التقادم التقني

تتميز تقنيات المراقبة بسرعة التطور، ولذلك قد تصبح بعض الأجهزة أو البرمجيات قديمة قبل انتهاء عمرها المادي.

ولهذا ينبغي عند التصميم مراعاة:

- قابلية التحديث.
- قابلية التوسع.
- التوافق مع المعايير.
- توفر قطع الغيار.
- الدعم البرمجي.

- أمن الجهاز خلال دورة حياته.
- إمكانية استبداله دون إعادة بناء المنظومة بالكامل.

وتظهر أهمية هذه المسألة في التطورات الحالية لمعايير التشغيل البيني؛ فعلى سبيل المثال أعلنت ONVIF في ٢٠٢٥ عن إنهاء دعم Profile S تدريجيًا والتوصية بـــ Profile Tبوصفه البديل، وربطت ذلك بتطور متطلبات الأمن السيبراني (3) .

سادسًا: الاعتماد على البنية التحتية

لا تستطيع التقنيات المتقدمة العمل بكفاءة إذا كانت البنية التحتية ضعيفة.

وتشمل عناصر الاعتماد:

- الطاقة الكهربائية.
- الشبكة.
- التخزين.
- الحوسبة.
- التبريد.
- الاتصالات.
- النسخ الاحتياطي.
- أنظمة استعادة الخدمة.

وبالتالي فإن الاستثمار في التحليلات المتقدمة دون الاستثمار في البنية الأساسية قد يؤدي إلى منظومة مرتفعة التكلفة منخفضة الاعتمادية.

سابعًا: نقص الكفاءات

التقنيات الحديثة لا تحتاج فقط إلى مشغل يعرف كيفية مشاهدة الفيديو، وإنما إلى كوادر قادرة على:

- إدارة نظام إدارة الفيديو.
- فهم الشبكات.
- إدارة التخزين.
- ضبط التحليلات.

- تفسير التنبيهات.
- إدارة الصلاحيات.
- التعامل مع الأعطال.
- فهم المخاطر السيبرانية.
- تقييم أداء الخوارزميات.

ومن ثم يصبح الاستثمار في الموارد البشرية جزءًا من الاستثمار في التقنية نفسها.

ثامنًا: مخاطر الاعتماد المفرط على التقنية

من أكبر المخاطر المستقبلية أن تتحول التقنية من أداة لدعم القرار إلى بديل عن التفكير الأمني.

فقد يؤدي الاعتماد المفرط على النظام إلى تجاهل الملاحظة البشرية، أو قبول نتائج الخوارزمية دون تحقق، أو افتراض أن وجود الكاميرات يعني وجود حماية كافية.

والقاعدة الأساسية هنا:

التكنولوجيا تعزز القدرة الأمنية، لكنها لا تلغي الحاجة إلى التقييم البشري وإدارة المخاطر والتخطيط والاستجابة.

تاسعًا: مخاطر المورد الواحد

يمكن أن يؤدي الاعتماد الكامل على مورد واحد إلى ما يسمى بالارتباط بالمورد، بحيث تصبح عملية التوسع أو الاستبدال مكلفة أو معقدة.

ولهذا تزداد أهمية:

- التشغيل البيني.
- المعايير المفتوحة.
- توثيق الواجهات.
- قابلية نقل البيانات.
- التخطيط للخروج من التقنية عند الحاجة.

عاشرًا: حوكمة الذكاء الاصطناعي

مع زيادة استخدام الذكاء الاصطناعي في المراقبة، ينبغي إنشاء إطار حوكمة يحدد:

- لماذا يستخدم النظام؟
- ما القرارات التي يمكنه دعمها؟
- ما القرارات التي لا يجوز أن يتخذها منفردًا؟
- كيف تقاس دقته؟
- كيف تتم مراجعة الأخطاء؟
- من يتحمل المسؤولية؟
- كيف تحمى البيانات؟
- كيف يتم إيقاف النظام أو تعديله عند ظهور مشكلة؟

ويؤكد إطار NIST أن خصائص الذكاء الاصطناعي الجدير بالثقة مترابطة، وأن تحقيق خاصية واحدة لا يكفي وحده لضمان موثوقية النظام؛ كما يؤكد أهمية الموازنة بين الدقة والأمن والخصوصية والتفسير وغيرها وفق سياق الاستخدام (4) .

المراجع:

① Michael Fagan et al., *Foundational Cybersecurity Activities for IoT Product Manufacturers*, NISTIR 8259 Rev. 1، Gaithersburg: National Institute of Standards and Technology، ٢٠٢٦. NNIST Computer Security Resource Center

②ينظر NIST : ، *AI Risk Management Framework — AI Risks and Trustworthiness*. NNIST AI Resource Center

③ ONVIF، *ONVIF to End Support for Profile S; Recommends Profile T as Replacement*، October ٩، 2025. OONVIF

④ Elham Tabassi، *Artificial Intelligence Risk Management Framework (AI RMF 1. 0)*، NIST AI 100-1، NNIST ٢٠٢٣.

المبحث التاسع: النموذج المستقبلي لمنظومة المراقبة الأمنية

يمثل هذا المبحث إضافة تحليلية مهمة للفصل؛ إذ لا يكفي عرض التقنيات المستقبلية بصورة منفصلة، وإنما ينبغي جمعها في نموذج يوضح كيف يمكن أن تتكامل داخل المنظومة الأمنية.

أولًا: طبقة الاستشعار

تتكون من:

١. الكاميرات.

٢. العدسات.

٣. الإضاءة.

٤. المستشعرات المرتبطة.

٥. مصادر البيانات الأخرى.

ووظيفتها جمع البيانات من البيئة.

ثانيًا: طبقة الاتصال

تشمل:

١. الشبكات.

٢. بروتوكولات الاتصال.

٣. نقل الفيديو.

٤. أمن الاتصالات.

٥. إدارة الأجهزة.

ووظيفتها نقل البيانات بصورة موثوقة وآمنة.

ثالثًا: طبقة المعالجة

تشمل:

١. الحوسبة الطرفية.

٢. الخوادم.

٣. أنظمة إدارة الفيديو.

٤. التخزين.

٥. محركات التحليل.

ووظيفتها تحويل البيانات الخام إلى بيانات قابلة للاستخدام.

رابعًا: طبقة التحليل

تشمل:

١. التحليلات التقليدية.

٢. التعرف على الأحداث.

٣. الذكاء الاصطناعي.

٤. البحث الذكي.

٥. تحليل الأنماط.

ووظيفتها استخراج المعلومات ذات القيمة الأمنية.

خامسًا: طبقة القرار

تشمل:

١. التنبيهات.

٢. تحديد الأولويات.

٣. التحقق البشري.

٤. إجراءات التصعيد.

٥. دعم القرار الأمني.

سادسًا: طبقة الاستجابة

تشمل:

١. المشغلين.

٢. الدوريات.

٣. فرق الاستجابة.

٤. أنظمة الإنذار.

٥. التحكم في الدخول.

٦. إجراءات الطوارئ.

سابعًا: طبقة التقييم والتحسين

تستخدم نتائج التشغيل والحوادث والأعطال والتحليلات لإعادة تقييم المنظومة وتحسينها.

وبذلك يمكن تمثيل المنظومة المستقبلية بالصيغة:

استشعار → اتصال → معالجة → تحليل → قرار → استجابة → تعلم وتحسين.

وهذه الدورة أكثر تعبيرًا عن مستقبل المراقبة من تصورها باعتبارها:

كاميرا → شاشة → تسجيل.

المبحث العاشر: الاتجاه الاستراتيجي لمستقبل المراقبة

يمكن استخلاص عدد من الاتجاهات الاستراتيجية التي يتوقع أن تشكل مستقبل المجال.

1. من زيادة عدد الكاميرات إلى زيادة القيمة الأمنية

لن تكون زيادة عدد الكاميرات الحل الأمثل في جميع الحالات، بل ستزداد أهمية تحسين مواقعها وجودة صورها وقدرتها التحليلية.

2. من التسجيل إلى التحليل

ستتحول قيمة التسجيل من كونه أرشيفًا يُراجع بعد الحادث إلى مصدر يمكن البحث والتحليل فيه بصورة أسرع.

3. من التحليل إلى التنبّه

ستصبح الأنظمة أكثر قدرة على اكتشاف الأنماط والمؤشرات التي تستدعي الانتباه، مع بقاء الحاجة إلى التحقق البشري.

4. من النظام المنفصل إلى المنظومة المتكاملة

ستزداد أهمية ربط الفيديو بالتحكم في الدخول والإنذار وأنظمة إدارة الأحداث.

5. من التشغيل اليدوي إلى التشغيل المدعوم بالأتمتة

ستتولى الأنظمة جزءًا أكبر من المهام المتكررة، بينما يزداد تركيز الإنسان على التحقق واتخاذ القرار.

6. من الأمن المادي إلى الأمن المادي الرقمي المتكامل

ستصبح حماية الكاميرات والشبكات والبيانات جزءًا من مفهوم الأمن المادي نفسه.

7. من الاعتماد على المورد إلى قابلية التشغيل البيني

ستصبح القدرة على دمج المنتجات وتبديلها وتطويرها عاملًا مهمًا في استدامة الاستثمار.

8. من التقنية إلى الحوكمة

ستصبح الأسئلة المتعلقة بالخصوصية والمسؤولية والشفافية وإدارة الخوارزميات جزءًا من تصميم المنظومة، وليس موضوعًا قانونيًا منفصلًا عنها.

القراءة التحليلية للفصل

يمكن اختصار التحول التاريخي للمراقبة الأمنية في السلسلة الآتية:

المراقبة البشـرية ← التسـجيل الرقمي ← المراقبة الشـبكية ← التحليلات الذكية ← الذكاء الاصطناعي ← الأتمتة والتكامل ← المنظومة الأمنية القائمة على البيانات.

لكن هذا المسار لا يعني أن الإنسان سيخرج من المنظومة؛ بل إن دوره سيتغير.

ففي النموذج التقليدي كان الإنسان يقوم أساسًا بـ:

المشاهدة.

أما في النموذج المتقدم فسيتولى:

التحقق ← التفسير ← التقييم ← القرار ← إدارة الاستجابة.

ومن هنا فإن التطور التقني الناجح ليس الذي يقلل وجود الإنسـان إلى أدنى حد، وإنما الذي يجعل الإنسـان أكثر قدرة على اسـتخدام المعلومات واتخاذ القرار المناسـب في الوقت المناسب.

الخلاصة

يتضح من دراسة الاتجاهات المستقبلية أن أنظمة المراقبة بالفيديو تتجه نحو تحول عميق من أنظمة تركز على التقاط الصور وتسجيلها إلى منظومات رقمية متكاملة تعتمد على التحليل والذكاء الاصطناعي والأتمتة والتكامل.

وقد أتاح التحول الرقمي تطوير قدرات المنظومة في إدارة البيانات ونقلها وتخزينها، بينما أتاحت التحليلات الذكية تحويل الفيديو إلى أحداث قابلة للاكتشاف والفرز. ثم جاء الذكاء الاصطناعي ليضيف قدرات أكثر تقدمًا في التعرف على الأنماط والبحث والتحليل، في حين سمحت الأتمتة بتقليل زمن الانتقال بين الاكتشاف والتنبيه والاستجابة.

وفي الوقت نفسه، يتيح التكامل بين الكاميرات وأنظمة التحكم في الدخول والإنذار وغيرها بناء صورة أكثر اكتمالًا للأحداث الأمنية. وتدعم معايير التشغيل البيني هذا الاتجاه من خلال تحديد وظائف مشتركة بين الأجهزة والعملاء، بينما تعكس التطورات الحديثة في ONVIF أهمية مواكبة متطلبات الأمن السيبراني والتحديث التقني (1) .

غير أن هذه الفرص لا تخلو من مخاطر. فزيادة الاتصال تعني زيادة التعرض للمخاطر السيبرانية، وزيادة التحليل تعني زيادة متطلبات الخصوصية وحوكمة البيانات، وزيادة الاعتماد على الذكاء الاصطناعي تعني الحاجة إلى اختبار الموثوقية والانحياز وقابلية التفسير والإشراف البشري. وقد أصبح مفهوم "الذكاء الاصطناعي الجدير بالثقة" في الأطر المهنية الحديثة قائمًا على مجموعة متكاملة من الخصائص، لا على الدقة وحدها NNIST+1 (2) .

ومن ثم فإن مستقبل المراقبة الأمنية لا ينبغي أن يفهم باعتباره سباقًا نحو امتلاك أحدث الأجهزة، وإنما باعتباره انتقالًا نحو منظومات أكثر قدرة على جمع المعلومات وتحليلها وربطها والاستجابة لها، مع المحافظة على الأمن والخصوصية والموثوقية والمسؤولية البشرية.

ويمكن التعبير عن هذا الاتجاه في المعادلة المفاهيمية الآتية:

القيمة المستقبلية للمراقبة = جودة البيانات × جودة التحليل × سرعة الاستجابة × التكامل × الحوكمة.

ولا يقصد بهذه العلاقة أنها معادلة رياضية لقياس الأداء، وإنما نموذج تحليلي يوضح أن التقنية لا تحقق قيمتها الأمنية إذا انفصلت عن التشغيل والاستجابة والحوكمة.

أهم نتائج الفصل

١. لم يعد تطور المراقبة بالفيديو مقتصرًا على زيادة دقة الكاميرات، وإنما أصبح مرتبطًا بإدارة البيانات وتحليلها وربطها.
٢. يمثل التحول الرقمي انتقالًا من الكاميرا بوصفها جهازًا منفردًا إلى الكاميرا بوصفها عنصرًا في منظومة معلومات أمنية.
٣. تساعد التحليلات الذكية على تقليل الاعتماد على المشاهدة المستمرة وتوجيه انتباه المشغل إلى الأحداث الأكثر أهمية.
٤. لا تستطيع التحليلات الذكية تعويض التصميم السيئ للكاميرا أو الإضاءة أو مجال الرؤية.
٥. يمثل الذكاء الاصطناعي فرصة كبيرة لتحسين التحليل والبحث والكشف، لكنه لا ينبغي أن يعامل بوصفه مصدرًا معصومًا للحقيقة.
٦. ينبغي أن ترتبط التطبيقات الحساسة للذكاء الاصطناعي بالاختبار والقياس والمراجعة والإشراف البشري.
٧. يتيح تحليل الفيديو المتقدم تحويل التسجيلات من أرشيف سلبي إلى مصدر معلومات قابل للبحث والاستفادة الأمنية.
٨. ترفع الأتمتة سرعة الاستجابة، لكنها تحتاج إلى قواعد صحيحة ومستويات واضحة من التحقق والتفويض.
٩. يمثل التكامل بين الفيديو والتحكم في الدخول والإنذار وغيرها أحد أهم اتجاهات تطوير المنظومات الأمنية.
١٠. تعد قابلية التشغيل البيني عنصرًا مهمًا في استدامة المنظومة وتقليل الارتباط بمورد واحد.
١١. يؤدي التوسع في استخدام الشبكات والأنظمة المتصلة إلى جعل الأمن السيبراني جزءًا من الأمن المادي للمنظومة.

١٢. تزداد أهمية حماية الخصوصية كلما انتقلت المنظومة من التسجيل إلى التحليل والتعرف والاستدلال.
١٣. لا ينبغي قياس نجاح التحليلات بعدد التنبيهات، وإنما بجودة التنبيهات وقابليتها للاستخدام الأمني.
١٤. تمثل جودة البيانات والصورة شرطًا أساسيًا لفاعلية التحليلات والذكاء الاصطناعي.
١٥. تحتاج التقنيات المستقبلية إلى كوادر بشرية قادرة على تشغيلها وتحليل نتائجها وإدارة مخاطرها.
١٦. ينبغي أن يراعى في التصميم المستقبلي قابلية التوسع والتحديث والتكامل والاستبدال.
١٧. لا يعني تطور الأتمتة والذكاء الاصطناعي الاستغناء عن الإنسان، وإنما نقل دوره من المراقبة المستمرة إلى التحقق والتفسير واتخاذ القرار.
١٨. مستقبل المراقبة الأمنية يتجه من التسجيل إلى التحليل، ومن التحليل إلى دعم القرار، ومن الأنظمة المنفصلة إلى المنظومات المتكاملة.
١٩. لا تكفي التقنية وحدها لتحقيق الأمن؛ فالفاعلية النهائية تعتمد على تكامل التقنية مع التصميم والتشغيل والصيانة والاستجابة والحوكمة.
٢٠. الاتجاه الأكثر نضجًا هو بناء منظومة تجعل التقنية مضاعِفًا للقدرة الأمنية البشرية لا بديلًا عنها.

المصادر والمراجع الأساسية للفصل

- IEC، *IEC 62676-1-1:2013, Video Surveillance Systems for Use in Security Applications – Part 1: System Requirements – General*، International Electrotechnical Commission، ٢٠١٣. IIEC Webstore
- IEC، *IEC 62676-1-2:2013, Video Surveillance Systems for Use in Security Applications – Part 1: System Requirements – Performance Requirements for Video Transmission*، International Electrotechnical Commission، ٢٠١٣. IIEC Webstore
- IEC، *IEC 62676-4:2025, Video Surveillance Systems for Use in Security Applications – Part 4: Application Guidelines*، International Electrotechnical Commission، ٢٠٢٥. IIEC Webstore

- ONVIF. OONVIF ،*ONVIF Profiles* ،ONVIF
- *Profile V – Release Candidate: For Cloud Video Streaming, Recording and Event* ،ONVIF ONVIF. OONVIF ،*Notifications*
- .٢٠٢٥ ،*ONVIF to End Support for Profile S; Recommends Profile T as Replacement* ،ONVIF OONVIF
- Fagan, Michael et al., *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*, NIST SP 800-213، National Institute of Standards and Technology، ٢٠٢١. NNIST Computer Security Resource Center
- Fagan, Michael et al., *Foundational Cybersecurity Activities for IoT Product Manufacturers*, NISTIR 8259 Rev. 1، National Institute of Standards and Technology، ٢٠٢٦. NNIST Computer Security Resource Center
- NIST AI ،Tabassi, Elham, *Artificial Intelligence Risk Management Framework (AI RMF 1. 0)* 100-1، National Institute of Standards and Technology، ٢٠٢٣.

خاتمة

بعد تناول منظومات المراقبة بالكاميرات من جوانبها المفاهيمية والفنية والأمنية والتشغيلية والتقييمية، يتضح أن فاعلية هذه المنظومات لا ترتبط بمجرد عدد الكاميرات أو ارتفاع دقتها، وإنما تتحدد بمدى قدرتها على تحقيق أهداف أمنية واضحة، ومعالجة المخاطر الفعلية، وتوفير صورة قابلة للاستخدام، وتسجيل الأحداث والمحافظة عليها، وضمان استمرارية التشغيل وحماية مكونات المنظومة نفسها.

وقد سعى هذا الكتاب إلى الانتقال من النظرة التقليدية إلى منظومة المراقبة باعتبارها مجموعة من الأجهزة التقنية، إلى النظر إليها باعتبارها منظومة أمنية متكاملة تتفاعل فيها عناصر التخطيط، وتحليل المخاطر، والتصميم، والتقنية، والتشغيل، والصيانة، والحماية، والتقييم والتحسين المستمر.

أولًا: أهم الاستنتاجات

يمكن استخلاص مجموعة من الاستنتاجات الرئيسية من مجمل ما تناولته فصول الكتاب:

١. فاعلية منظومة المراقبة تبدأ من الهدف الأمني وليس من اختيار الكاميرا. فقبل تحديد نوع الكاميرا أو دقتها أو عددها، ينبغي تحديد ما الذي يراد حمايته، وما التهديدات المحتملة، وما الوظيفة الأمنية المطلوبة من الصورة.

٢. تحليل المخاطر يمثل الأساس المنطقي لتوزيع الكاميرات. ولا ينبغي توزيع الكاميرات بصورة متساوية أو اعتمادًا على المساحات فقط، بل ينبغي إعطاء الأولوية للمناطق التي تجمع بين ارتفاع قيمة الأصول، واحتمالية التهديد، وشدة الأثر المحتمل.

٣. عدد الكاميرات ليس مؤشرًا كافيًا على جودة المنظومة. فقد تمتلك المنشأة عددًا كبيرًا من الكاميرات، ومع ذلك تظل مناطق مهمة غير مغطاة أو تعاني من مناطق عمياء أو زوايا غير مناسبة.

٤. جودة الصورة مفهوم وظيفي وليست مجرد رقم للدقة. فالدقة، وعدد البكسلات، ومعدل الإطارات، والإضاءة، والعدسة، والمجال

الديناميكي، والضغط، والمسافة، وزاوية التصوير، كلها عوامل تؤثر في قابلية الصورة لتحقيق الوظيفة الأمنية المطلوبة.

٥. تختلف متطلبات الصورة باختلاف الوظيفة الأمنية. فمتطلبات المراقبة العامة تختلف عن متطلبات الكشف، ومتطلبات التعرف تختلف عن متطلبات التحقق من الهوية أو قراءة لوحات المركبات. ولذلك لا يصح اعتماد معيار واحد لجميع الكاميرات والمواقع.

٦. التسجيل لا يحقق قيمته الأمنية إلا إذا كان قابلًا للاسترجاع والاستخدام. فوجود التسجيل وحده لا يكفي، بل يجب أن تتوافر مدة احتفاظ مناسبة، وتوقيت دقيق، وسلامة للبيانات، وآلية فعالة للبحث والاسترجاع والتصدير والحفظ.

٧. حساب سعة التخزين يجب أن يستند إلى معطيات تشغيلية فعلية. ويشمل ذلك عدد الكاميرات، والدقة، ومعدل البت، ومعدل الإطارات، ونمط التسجيل، وساعات التشغيل، ومدة الاحتفاظ، وطريقة الضغط، وهوامش السعة والاعتمادية. ومن ثم فإن الاعتماد على تقدير عام دون بيان افتراضاته قد يؤدي إلى نتائج مضللة.

٨. العنصر البشري جزء أساسي من المنظومة. فالمشغل غير المدرب، أو المناوبة المرهقة، أو غياب إجراءات التصعيد والاستجابة، يمكن أن يقلل من قيمة منظومة تقنية متقدمة.

٩. الصيانة الوقائية شرط لاستمرارية الفاعلية. وتظهر أهمية ذلك خصوصًا في الكاميرات الخارجية، ومكونات الشبكة، وأجهزة التسجيل، ومصادر الطاقة، ووحدات التخزين، والأنظمة التي تعتمد عليها المنظومة في عملها.

١٠. حماية منظومة المراقبة نفسها أصبحت جزءًا من الأمن. فالمنظومة المتصلة بالشبكة يمكن أن تكون هدفًا للوصول غير المصرح به أو العبث أو تعطيل الخدمة أو سرقة التسجيلات، ولذلك يجب أن تشمل الحماية الحسابات والصلاحيات والشبكات والأجهزة والبيانات.

١١. التقييم الجيد يجب أن يكون قائمًا على الأدلة. فلا يكفي القول إن التغطية "جيدة" أو أن الجودة "متوسطة"، بل ينبغي بيان المعيار المستخدم، والبيانات التي جرى قياسها، وطريقة احتساب النتيجة، والدليل الذي أدى إلى الحكم النهائي.

١٢. التقييم الرقمي وسيلة للمقارنة وليس غاية في ذاته. فالدرجة المئوية لا تصبح ذات قيمة إلا إذا كانت ناتجة عن منهج واضح للأوزان والدرجات، وقابلة للتفسير والمراجعة.

١٣. الأولوية لا تحددها الدرجة وحدها. فقد تكون هناك نقطة ضعف ذات درجة فنية منخفضة لكنها ترتبط بخطر مرتفع جدًا، ومن ثم ينبغي أن تدخل نتائج التقييم الفني وتحليل المخاطر معًا في تحديد أولوية المعالجة.

١٤. التقييم الحقيقي ينتهي بخطة تحسين قابلة للقياس. فالغرض من اكتشاف نقاط الضعف ليس وصف المشكلة فقط، وإنما تحويلها إلى إجراءات محددة، ومسؤوليات، ومدد زمنية، ومؤشرات نجاح، ثم إعادة التقييم للتحقق من التحسن.

١٥. إن منظومة المراقبة الفعالة ليست مجموعة من الكاميرات وأجهزة التسجيل فحسب، وإنما هي منظومة أمنية متكاملة تبدأ بفهم الأصول والمخاطر، وتمر بتحديد الأهداف والوظائف الأمنية، ثم التصميم والاختيار الفني، والتشغيل والصيانة، وحماية البيانات والمنظومة، وتنتهي بالتقييم وإدارة الفجوات والتحسين المستمر.

وتؤكد الدراسة التي قدمناها في هذا الكتاب أن السؤال الصحيح ليس: كم كاميرا نحتاج؟ وإنما:

ما المخاطر التي نريد معالجتها؟ وما الوظيفة الأمنية المطلوبة؟ وهل توفر المنظومة الدليل المناسب في المكان والوقت المناسبين وبالجودة التي تسمح باستخدامه؟

وعلى هذا الأساس، فإن فاعلية المنظومة يمكن النظر إليها بوصفها نتاجًا لتكامل خمسة عناصر رئيسية:

أهداف واضحة + تحليل مخاطر سليم + تصميم فني مناسب + تشغيل وصيانة فعّالان + تقييم وتحسين مستمران.

وإذا اختل أحد هذه العناصـــر، فقد تنخفض القيمة الأمنية للمنظومة مهما بلغت جودة بقية عناصـــرها. أما عندما تعمل هذه العناصـــر ضـــمن إطار موحد قائم على الأدلة والقياس، فإن منظومة المراقبة تتحول من مجرد وســيلة لتســجيل الصــور إلى أداة أمنية قادرة على الوقاية والكشف والتوثيق ودعم الاستجابة والتحقيق.

وبذلك لا يكون نجاح منظومة المراقبة في امتلاك أحدث التقنيات، وإنما في قدرتها المستمرة على تحقيق الغرض الأمني الذي صُـممت من أجله، وإثبات ذلك من خلال نتائج قابلة للقياس والتحقق والتحسين.

تم بحمد الله.

ربنا تقبل منا إنك أنت السميع العليم.

مراجع الكتاب :

أولًا: المعايير والمواصفات الفنية الدولية المعايير والمواصفات الفنية الدولية

١. International Electrotechnical Commission. *IEC 62676-1-1: Video Surveillance Systems for Use in Security Applications – Part 1-1: System Requirements – General*. Geneva: IEC, 2013.

٢. International Electrotechnical Commission. *IEC 62676-4: Video Surveillance Systems for Use in Security Applications – Part 4: Application Guidelines*. Geneva: IEC.

٣. International Electrotechnical Commission. *IEC 60529: Degrees of Protection Provided by Enclosures (IP Code)*. Geneva: IEC.

٤. ONVIF. *ONVIF Profiles*. San Ramon, CA: ONVIF.

٥. ONVIF. *Profile T – Advanced Video Streaming*. San Ramon, CA: ONVIF.

٦. ONVIF. *Profile G – Edge Storage and Retrieval*. San Ramon, CA: ONVIF.

٧. ONVIF. *Profile M – Metadata and Events for Analytics Applications*. San Ramon, *CA: ONVIF.*

٨. *International Electrotechnical Commission (IEC). (2025). IEC 62676-4:2025: Video surveillance systems for use in security applications – Part 4: Application guidelines. 2nd ed., Geneva: IEC.*

٩. *International Organization for Standardization (ISO). (2019). ISO 22301:2019: Security and resilience — Business continuity management systems — Requirements. Geneva: ISO.*

١٠. *International Organization for Standardization (ISO). (2016). ISO/IEC 27035-1:2016: Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management. Geneva: ISO.*

١١. *International Organization for Standardization (ISO). (2012). ISO/IEC 27037:2012: Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva: ISO.*

١٢. *National Fire Protection Association (NFPA). (2019). NFPA 1600: Standard on Continuity, Emergency, and Crisis Management. Quincy, MA: NFPA.*

١٣. *National Institute of Standards and Technology (NIST). (2023). Guide to Operational Technology (OT) Security, NIST Special Publication 800-82 Revision 3. Gaithersburg, MD: NIST.*

١٤. *Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer Security Incident Handling Guide, NIST Special Publication 800-61 Revision 2. Gaithersburg, MD: National Institute of Standards and Technology.*

١٥. *Guttman, B., White, D. R., Williams, S., & Walraven, T. (2022). Digital Evidence Preservation: Considerations for Evidence Handlers, NIST Interagency/Internal Report 8387. Gaithersburg, MD: National Institute of Standards and Technology.*

١٦. *National Institute of Standards and Technology (NIST). Video Quality in Public Safety (VQiPS). Gaithersburg, MD: NIST.*

١٧. *Wickens, C. D., Hollands, J. G., Banbury, S., & Parasuraman, R. (2016). Engineering Psychology and Human Performance. 4th ed., Routledge.*

١٨. *Reason, J. (1990). Human Error. Cambridge: Cambridge University Press..*

١٩. *Parasuraman, R., & Riley, V. (1997). "Humans and Automation: Use, Misuse, Disuse, Abuse." Human Factors, 39(2), 230–253.*

٢٠. *Hancock, P. A., & Desmond, P. A. (Eds.). (2000). Stress, Workload, and Fatigue. Mahwah, NJ: Lawrence Erlbaum Associates.*

٢١. *International Civil Aviation Organization (ICAO). (1993). Human Factors Digest No. 7: Investigation of Human Factors in Accidents and Incidents, Circular 240-AN/144. Montreal: ICAO.*

٢٢. *U.S. Nuclear Regulatory Commission (NRC). (2026). Human-System Interface Design Review Guidelines, NUREG-0700 Revision 4. Washington, DC: U.S. Nuclear Regulatory Commission.*

٢٣. *Association of Chief Police Officers (ACPO). (2012). Good Practice Guide for Digital Evidence. Version 5.0. United Kingdom.*

ثانيًا: الأمن السيبراني وإنترنت الأشياء

٢٣. Stouffer, Keith, Michael Pease, CheeYee Tang, Timothy Zimmerman, Victoria Pillitteri, Suzanne Lightman, Adam Hahn, Stephanie Saravia, Aslam Sherule, and Michael Thompson. *Guide to Operational Technology (OT) Security*. NIST Special Publication 800-82 Rev. 3. Gaithersburg, MD: National Institute of Standards and Technology, 2023.

٢٤. Fagan, Michael, Katerina Megas, Jeffrey Marron, Kevin Brady, Barbara Cuthill, Rebecca Herold, David Lemire, and Brad Hoehn. *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*. NIST Special Publication 800-213. Gaithersburg, MD: National Institute of Standards and Technology, 2021.

٢٥. Boeckl, Kaitlin, Michael Fagan, William Fisher, Naomi Lefkovitz, Katerina Megas, Ellen Nadeau, Ben Piccarreta, Danna Gabel O'Rourke, and Karen Scarfone. *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*. NISTIR 8228. Gaithersburg, MD: National Institute of Standards and Technology, 2019.

٢٦. Lieberman, A. G., D. J. Atkinson, V. J. Pietrasiewicz, and K. E. Junker. *Video Surveillance Equipment Selection and Application Guide*. NIJ Guide 200-98. Gaithersburg, MD: National Institute of Standards and Technology / National Institute of Justice, 1999.

٢٧. Home Office / Biometrics and Surveillance Camera Commissioner. *Surveillance Camera Code of Practice*. Amended 2021; brought into effect on 12 January 2022.

٢٨. Biometrics and Surveillance Camera Commissioner. *Surveillance Camera Code of Practice: A Guide for Local Authorities*. UK Government

٢٩. Norman, Thomas L. Integrated Security Systems Design: A Complete Reference for Building Enterprise-Wide Digital Security Systems. 2nd ed. Oxford: Butterworth-Heinemann/Elsevier, 2014.

٣٠. Smith, Clifton L., and David J. Brooks. Security Science: The Theory and Practice of Security. Butterworth-Heinemann/Elsevier.

٣١. International Organization for Standardization. ISO 22341:2021, Security and Resilience — Protective Security — Guidelines for Crime Prevention through Environmental Design. Geneva: ISO, 2021.

٣٢. European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union, 2016.

٣٣. Welsh, Brandon C., and David P. Farrington. "Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-Analysis." Justice Quarterly 26, no. 4 (2009): 716–745. https://doi.org/10.1080/07418820802506206.

٣٤. Piza, Eric L., Brandon C. Welsh, David P. Farrington, and Amanda L. Thomas. "CCTV Surveillance for Crime Prevention: A 40-Year Systematic Review with Meta-Analysis." Criminology & Public Policy 18, no. 1 (2019): 135–159. https://doi.org/10.1111/1745-9133.12419.

ثالثاً: الدراسات العربية

١. حسوني، آمال عبد الجبار، وجبر، نادية كعب. «كاميرات المراقبة بين دواعي الاستعمال وانتهاك الخصوصية .»مجلة الحقوق، الجامعة المستنصرية، المجلد ١٦، العددان ٢٩–٣٠، ٢٠١٧، ص ١–١٨ .

٢. عثمان، أحمد علي حسن. «الضوابط القانونية لاستخدام أنظمة المراقبة التلفزيونية المغلقة "CCTV" في بيئة العمل: دراسة مقارنة بين القانون الفرنسي والمصري والنظام السعودي .»مجلة البحوث القانونية والاقتصادية، العدد ٩٢، ٢٠٢٥، ص ٢٢٢–٣٨٧ .

٣. خالد بن إبراهيم النفيعي، إدارة أنظمة المراقبة: دراسة تطبيقية .

٤. فهد بن محمد العتيبي، مكونات أنظمة المراقبة بالفيديو .

٥. عبد الله بن حسن الشهري، شبكات نقل الفيديو الأمني .

٦. سعد بن عبد العزيز المطيري، التقنيات الحديثة في أنظمة المراقبة .

٧. محمد عبد الله الأحمدي، الأمن الوقائي: المفاهيم والاستراتيجيات .

٨. الزهراني، العدسات البصرية في كاميرات المراقبة .

٩. عبد الرحمن محمد السالم، «معايير الفعالية في أنظمة المراقبة الأمنية .»

١٠. «الدليل المهني لأنظمة المراقبة الأمنية»، المنسوب إلى وزارة الداخلية السعودية.

م	العنوان	ص
١.	الاهداء	
٢.	دوافع تأليف الكتاب/ أهمية الموضوع/ الفئة المستهدفة /منهج إعداد الكتاب /حدود موضوع الكتاب /كيفية الاستفادة من الكتاب	٢
٣.	**الباب الأول: الإطار العام لمنظومات المراقبة**	٩
٤.	الفصل الأول: مدخل إلى كاميرات المراقبة في المجال الأمني	١٠
٥.	المبحث الأول: مفهوم المراقبة الأمنية	١١
٦.	المبحث الثاني: نشأة وتطور أنظمة المراقبة	٢٢
٧.	المبحث الثالث: تطور كاميرات المراقبة	٣٣
٨.	المبحث الرابع: الانتقال من الكاميرا إلى المنظومة	٣٩
٩.	المبحث الخامس: موقع المراقبة ضمن منظومة أمن المنشآت	٤٧
١٠.	المبحث السادس: حدود دور كاميرات المراقبة	٥٣
١١.	الفصل الثاني: منظومة كاميرات المراقبة ومكوناتها	٦٤
١٢.	المبحث الأول: مفهوم منظومة المراقبة	٦٥
١٣.	المبحث الثاني: الكاميرات	٧٠
١٤.	المبحث الثالث: العدسات	٧٧
١٥.	المبحث الرابع: أجهزة التسجيل	٨٥
١٦.	المبحث الخامس: وسائط التخزين	٩٥
١٧.	المبحث السادس: الشاشات ومراكز المراقبة	١٠٣
١٨.	المبحث السابع: الشبكات والاتصالات	١١١
١٩.	المبحث الثامن: أنظمة الطاقة	١١٩
٢٠.	المبحث التاسع: البرمجيات والتحكم	١٢٣
٢١.	المبحث العاشر: تكامل مكونات المنظومة	١٢٨
٢٢.	الباب الثاني :الأسس الفنية لتصميم منظومة المراقبة	١٣٦
٢٣.	الفصل الأول: أنواع كاميرات المراقبة وخصائصها	١٣٧

م	العنوان	ص
٢٤.	المبحث الأول: التصنيف وفق التقنية	١٣٨
٢٥.	المبحث الثاني: التصنيف وفق الوظيفة	١٤٢
٢٦.	المبحث الثالث: الكاميرات الثابتة	١٤٥
٢٧.	المبحث الرابع: الكاميرات المتحركة	١٤٧
٢٨.	المبحث الخامس: الكاميرات الداخلية والخارجية	١٤٩
٢٩.	المبحث السادس: الكاميرات النهارية والليلية	١٥١
٣٠.	المبحث السابع: الكاميرات المتخصصة	١٥٣
٣١.	المبحث الثامن: معايير اختيار النوع المناسب	١٥٥
٣٢.	الفصل الثاني: تصميم منظومة المراقبة	١٦٥
٣٣.	المبحث الأول: تحديد أهداف المراقبة	١٦٦
٣٤.	المبحث الثاني: تحليل الموقع	١٧١
٣٥.	المبحث الثالث: تحليل المخاطر	١٧٦
٣٦.	المبحث الرابع: تحديد المناطق ذات الأولوية	١٨١
٣٧.	المبحث الخامس: تحديد نقاط المراقبة	١٨٥
٣٨.	المبحث السادس: توزيع الكاميرات	١٨٩
٣٩.	المبحث السابع: زوايا الرؤية والارتفاعات	١٩٣
٤٠.	المبحث الثامن: المناطق العمياء	١٩٧
٤١.	المبحث التاسع: التكامل بين نقاط المراقبة	٢٠١
٤٢.	المبحث العاشر: مراجعة التصميم واختباره	٢٠٥
٤٣.	الفصل الثالث: جودة الصورة والعوامل المؤثرة فيها	٢١٣
٤٤.	المبحث الأول: مفهوم جودة الصورة	٢١٥
٤٥.	المبحث الثاني: الدقة والتفاصيل	٢١٩
٤٦.	المبحث الثالث: العدسات وزوايا الرؤية	٢٢٤
٤٧.	المبحث الرابع: المسافة ومجال الرؤية	٢٢٦
٤٨.	المبحث الخامس: الإضاءة	٢٣٠

م	العنوان	ص
٤٩.	المبحث السادس: الرؤية الليلية	٢٣٤
٥٠.	المبحث السابع: الحركة والظروف المتغيرة	٢٣٨
٥١.	المبحث الثامن: العوامل البيئية	٢٤١
٥٢.	المبحث التاسع: اختيار مستوى الجودة وفق الهدف الأمني	٢٤٤
٥٣.	الفصل الرابع: التسجيل والتخزين وإدارة المعلومات	٢٥٨
٥٤.	المبحث الأول: أهمية التسجيل الأمني	٢٦١
٥٥.	المبحث الثاني: أنماط التسجيل	٢٦٥
٥٦.	المبحث الثالث: جودة التسجيل	٢٧١
٥٧.	المبحث الرابع: سعة التخزين	٢٧٥
٥٨.	المبحث الخامس: مدة الاحتفاظ بالتسجيلات	٢٧٨
٥٩.	المبحث السادس: البحث والاسترجاع	٢٨٢
٦٠.	المبحث السابع: النسخ الاحتياطي	٢٨٦
٦١.	المبحث الثامن: إدارة التسجيلات	٢٨٩
٦٢.	المبحث التاسع: حماية التسجيلات وسلامتها	٢٩٢
٦٣.	الباب الثالث: التشغيل والوظيفة الأمنية	٣٠٣
٦٤.	الفصل الأول: تشغيل وإدارة مراكز المراقبة	٣٠٤
٦٥.	المبحث الأول: مركز المراقبة	٣٠٥
٦٦.	المبحث الثاني: تنظيم العمل	٣١٤
٦٧.	المبحث الثالث: مشغلو أنظمة المراقبة	٣٠٨
٦٨.	المبحث الرابع: التدريب والتأهيل	٣٢٢
٦٩.	المبحث الخامس: إجراءات التشغيل	٣٢٦
٧٠.	المبحث السادس: التعامل مع الأحداث	٣٣٢
٧١.	المبحث السابع: التوثيق والإبلاغ	٣٣٧
٧٢.	المبحث الثامن: الإرهاق والأخطاء البشرية	٣٤١
٧٣.	المبحث التاسع: الصيانة واستمرارية التشغيل	٣٤٥

م	العنوان	ص
٧٤.	الفصل الثاني: كاميرات المراقبة وتعزيز أمن المنشآت	٣٥٤
٧٥.	المبحث الأول: الوظيفة الأمنية للمراقبة	٣٥٦
٧٦.	المبحث الثاني: الوقاية والردع	٣٥٩
٧٧.	المبحث الثالث: اكتشاف الأحداث	٣٦١
٧٨.	المبحث الرابع: دعم الاستجابة الأمنية	٣٦٣
٧٩.	المبحث الخامس: مراقبة المداخل والمخارج	٣٦٥
٨٠.	المبحث السادس: حماية المناطق الحساسة	٣٦٧
٨١.	المبحث السابع: توثيق الوقائع	٣٦٩
٨٢.	المبحث الثامن: دعم الاستدلال والتحقيق	٣٧١
٨٣.	المبحث التاسع: إدارة الأزمات والطوارئ	٣٧٣
٨٤.	المبحث العاشر: حدود الاعتماد على كاميرات المراقبة	٣٧٥
٨٥.	الفصل الثالث: التكامل بين كاميرات المراقبة والمنظومات الأمنية	٣٨٤
٨٦.	المبحث الأول: مفهوم التكامل الأمني	٣٨٦
٨٧.	المبحث الثاني: الربط مع أنظمة التحكم بالدخول	٣٨٨
٨٨.	المبحث الثالث: الربط مع أنظمة الإنذار	٣٩٠
٨٩.	المبحث الرابع: مراكز القيادة والتحكم	٣٩٢
٩٠.	المبحث الخامس: التكامل مع أنظمة الأمن والسلامة	٣٩٤
٩١.	المبحث السادس: إدارة الأحداث المتكاملة	٣٩٦
٩٢.	المبحث السابع: متطلبات نجاح التكامل	٣٩٩
٩٣.	الفصل الرابع: أمن منظومة المراقبة وحمايتها	٤٠٨
٩٤.	المبحث الأول: حماية مكونات المنظومة	٤١٠
٩٥.	المبحث الثاني: إدارة المستخدمين والصلاحيات	٤١٢
٩٦.	المبحث الثالث: حماية الشبكات	٤١٤
٩٧.	المبحث الرابع: حماية أجهزة التسجيل	٤١٦
٩٨.	المبحث الخامس: حماية التسجيلات	٤١٩

م	العنوان	ص
٩٩.	المبحث السادس: النسخ الاحتياطي واستمرارية الخدمة	٤١٩
١٠٠	المبحث السابع: مخاطر العبث والتلاعب	٤٢١
١٠١	المبحث الثامن: الضوابط التنظيمية والإجرائية	٤٢٣
١٠٢	المبحث التاسع: الخصوصية والمسؤولية المهنية	٤٢٩
١٠٣	الباب الرابع: تقييم الفاعلية والتطبيقات	٤٤٣
١٠٤	الفصل الأول: فاعلية منظومة كاميرات المراقبة	٤٤٤
١٠٥	المبحث الأول: مفهوم الفاعلية	٤٤٥
١٠٦	المبحث الثاني: الفرق بين وجود المنظومة وكفاءتها	٤٤٨
١٠٧	المبحث الثالث: الفرق بين الكفاءة الفنية والفاعلية الأمنية	٤٥١
١٠٨	المبحث الرابع: مؤشرات الفاعلية	٤٥٣
١٠٩	المبحث الخامس: عوامل نجاح المنظومة	٤٥٧
١١٠	المبحث السادس: أسباب انخفاض الفاعلية	٤٦١
١١١	المبحث السابع: تقييم الأداء الفعلي	٤٦٤
١١٢	الفصل الثاني: منهجية تقييم منظومات كاميرات المراقبة	٤٨٣
١١٣	المبحث الأول: أسس التقييم	٤٨٤
١١٤	المبحث الثاني: محاور التقييم	٤٨٨
١١٥	المبحث الثالث: مؤشرات الأداء	٤٩٣
١١٦	المبحث الرابع: بطاقة التقييم	٤٩٩
١١٧	المبحث الخامس: نظام الدرجات	٥٠٢
١١٨	المبحث السادس: حساب مستوى الكفاءة	٥٠٥
١١٩	المبحث السابع: تحديد نقاط القوة والقصور	٥١٠
١٢٠	المبحث الثامن: تحليل الفجوات	٥١٣
١٢١	المبحث التاسع: إعداد تقرير التقييم	٥١٧
١٢٢	الفصل الثالث: الاتجاهات المستقبلية للتطور التقني ومستقبل المراقبة الأمنية	٥٢٨
١٢٣	المبحث الأول: التحول الرقمي	٥٣١

م	العنوان	ص
١٢٤	المبحث الثاني: التحليلات الذكية	٥٣٤
١٢٥	المبحث الثالث: الذكاء الاصطناعي	٥٣٧
١٢٦	المبحث الرابع: تحليل الفيديو	٥٣٩
١٢٧	المبحث الخامس: الأتمتة	٥٥١
١٢٨	المبحث السادس: التكامل المتقدم	٥٥٣
١٢٩	المبحث السابع: فرص التطور	٥٥٦
١٣٠	المبحث الثامن: المخاطر والتحديات المستقبلية	٥٥٨
١٣١	المبحث التاسع: النموذج المستقبلي لمنظومة المراقبة الأمنية	٥٦٣
١٣٢	المبحث العاشر: الاتجاه الاستراتيجي لمستقبل المراقبة	٥٦٦
١٣٣	خاتمة	٥٧٢
١٣٤	مراجع الكتاب الرئيسية	٥٧٦