الجـزء الرابع
لماذا لا تستطيع التكنولوجيات المحسنة إنقاذنا؟

فشل النظم التكنولوجية

يقول المؤلف إن النظم التكنولوجية هى نظم متكاملة توفر لنا الماء والغذاء والطاقة، وبواسطتها نستطيع التنقل من مكان إلى آخر، وكذلك تسمح لنا بالاتصال بعضنا البعض وتحدد كافة الأنشطة الجسمانية والاجتماعية التى تعتمد عليها حياتنا. وكثير منا لا يمكنه فهم كيفية تشغيل هذه الأنظمة المعقدة ! فليس من الضرورى معرفة عمل هذه النظم من أجل استعمالها والاستفادة منها ، وفى أغلب الأمور لا نحتاج إلى تفاصيل فنية لمعرفة كيف نصون ونصلح هذه التكنولوجيات. على سبيل المثال ، نحن نستخدم السيارات والأمر لا يحتاج إلى مهندس أو عالم إلكترونيات وكيمياء أو ميكانيكا لديه المعرفة الكاملة لصيانة هذه السيارات. كل ما نحتاجه هو معرفة الأجزاء المكونة للسيارات وكيفية عمل كل جزء لإصلاحة واستبداله. وعمومًا للتكنولوجيات قدرات هائلة، ولكن هناك دائمًا حدودًا لهذه القدرات. وصلاحية النظم التكنولوجية تعتمد على مدى التعقيد فى المكونات الأساسية لهذا النظام. وهذا يعنى اعتماد الأجزاء المختلفة وتفاعلها بعضها البعض. فكلما ازداد عدد الأجزاء المكونة للنظام، أصبح النظام أكثر تعقيدًا وبالتالى تقل صلاحيتها. فى هذه النظم تتوفر طرق مختلفة لحدوث الخطأ التكنولوجى. فالأجزاء الداخلية مثلاً ترتبط ببعضها عن طريق وسائل الربط، وفشل النظام التكنولوجى عادة يكون لخلل ناتج عن زيادة الحمولة فى هذه الوسائل. ويقول المؤلف إن أنظمة الأقمار الاصطناعية التى تحدد دقة عملها من لحظة الإطلاق إلى تحديد المسار وتثبيتها فى مدارات حول الأرض، وكذلك كفاءة وسائل الاتصال مع المحطات الأرضية تكون غاية التعقيد. وفى أحيان كثيرة لا يمكن إصلاح الأعطال التكنولوجية التى تحدث بهذه الأقمار الاصطناعية عن طريق الاستشعار عن بعد بواسطة محطات التحكم الأرضية. ولذلك نشاهد اليوم تراكم أعداد هائلة من هذه النظم فى

الفضاء عبر السنوات الماضية، مما يشكل ازدحامًا قد يؤدى إلى حوادث تصادم مع الأقمار الجديدة الأخرى، مما يكلف البشرية مبالغ طائلة .

وفى مجال البحث والتطوير قد لا يمكننا تجنب التعقيد فى النظم التكنولوجيا التى تستطيع إنجاز المهمة. ويحتاج الأمر إلى تصميمات وإجراءات تشغيل غاية التعقيد. ولكن فى المقابل ترتفع كفاءة الأداء ودقته بالإضافة إلى توفير الوقت وقلة التكاليف بالمقارنة بالنظم المناظرة البسيطة. هذا التعقيد يجعل احتمال حدوث الخطأ أكبر.

ويقول « دوماس» إنه فى مجال صناعة الطائرات الحربية، لا توجد تقريبًا طائرة واحدة يمكنها الطيران أكثر من ٧٢ دقيقة متصلة دون عطب فى أجهزتها الداخلية، وتحتاج هذه الطائرات إلى عمليات إصلاح مستمرة بمعدل ١,٦ لكل رحلة طيران وبمتوسط ٧٠٪ من الرحلات[٩٦-٩٧].

ويستطرد المؤلف قائلاً ، أنه كلما ازداد النظام تعقيدًا لا يستطيع القائمون على تصنيعها وتصميمها وتشغيلها معرفة ما يحدث من أخطاء، ويحتاجون إلى أجهزة دقيقة للقياس لتحديد الأعطال، وكذلك معدات خاصة للإصلاح، مما يدعو فى أغلب الأحيان إلى أخطاء فى تشخيص الأعطال وفى جميع الأجزاء. فى هذا الشأن سرد المؤلف قصة نجاح وكالة الفضاء الأمريكية (ناسا) فى ٢٤ إبريل عام ١٩٩٠، فى إطلاق تليسكوب هابل الفضائى. وبعد شهر من إطلاق التليسكوب إلى الفضاء اكتشف العلماء عيوبًا فنية عديدة حالت دون تشغيل التليسكوب بكفاءة. وكذلك عجزت المحطات الأرضية فى القيام بأعمال الإصلاح خاصة فى الأنظمة البصرية وعدساته العملاقة ، مما تسبب فى ضياع عشرة سنوات كاملة دون الاستفادة من المعلومات التى يوفرها هذا التليسكوب الهائل. وفى عام ١٩٩٣م، أمكن إصلاح هذا التليسكوب بتكلفة قدرها ١,٦ بليون دولار أمريكى واستغرق الأصلاح مدة عام كامل وتم بواسطة رواد الفضاء فى رحلة تاريخية لمكوك الفضاء « شاتل ». ومنذ عام ١٩٩٩م، يعانى التليسكوب من مشاكل جديدة متمثلة فى تعطيل أمد الجيروسكوبات الستة وهى من المكونات الأساسية للتليسكوب .

ويتحدث المؤلف عما يسمى بـ « النظم المعاونة » التى تجعل النظام ككل أكثر أمنًا من أى من مكوناته المنفردة كل على حدة. إلا أنه أحيانًا ما تفشل

هذه النظم المعاونة ، مما يجعل دائمًا إمكانية لحدوث الخطأ . ويسترشد بحادثة توقف ثلاثة من أجهزة الأمان المصممة لمنع تسرب المواد الكيميائية الخطرة، تسبب هذا الحادث فى كارثة مدينة باهوبال الهندية عام ١٩٨٤م. وكذلك فشل بعض الأجهزة المعاونة للأمان المسئولة عن الكوارث النووية فى مفاعلات ثرى ميل أيلاند عام ١٩٧٩ وتشرنوبيل عام ١٩٨٦م.

وفى ٢٠ ديسمبر عام ١٩٨٩م ، فشلت أجهزة التوجيه فى إحدى طائرات البوينج المدنية وعلى متنها ٣٩١ راكبًا مما أدى إلى انحراف الطائرة من المسار، وطيرانها فى اتجاه مخالف لمسافة ١٢٠٠ كيلو متر دون أن يكتشف ملاحو الطائرة الخطأ [٩٨].

ففى حالة اعتماد الأجزاء الأساسية بالنظام على وحدة تحكم واحدة، هذا يجعل قابلية حدوث الخطأ كبيرة فى حالة أى عطل يصيب هذه الوحدة. على سبيل المثال، عندما يتعطل مولد الطاقة فى إحدى المستشفيات عن العمل، سوف يصيب جميع أقسام المستشفى بالتوقف عن العمل تمامًا، وبالتالى يصبح الغرض من استعمال المولد عديم الفائدة. هذا ما حدث أيضًا فى المحطة النووية فى مدينة رانكوسيكو فى يوم ٢٠ مارس ١٩٧٨م، عندما استبدل أحد العاملين مصباح الإنذار فى غرفة التحكم الآلى بالمحطة. نتج عن هذه العملية حدوث « قفلة كهربائية » أوقفت عمل معدات التحكم فى نظام تغذية التبريد المائى ، مما كاد أن يتسبب فى كارثة نووية مروعة[٩٩]. وكذلك احتراق الطائرة الجامبو طراز دى سى١ يوم ٢٩ يوليو ١٩٨٩م، وهى تابعة للخطوط الجوية المتحدة. وكان على متنها ٣٠٠ راكب أثناء إقلاعها من مطار مدينة سبوكسى بأيوا . ونتج عن الحادث مقتل ١١٢ راكبًا. اتضح بعد ذلك أن سبب الحادث توقف ثلاثة من النظم الهيدروليكية بالطائرة [١٠٠]. ويعزو المؤلف هذه الحوادث إلى أخطاء فى التصميم.

ففى حالة القاذفة ب ـ ٢ ، اكتشف عام ١٩٩٥م (بعد ١٤ عامًا من دخولها الخدمة و٦ أعوام من الاختبارات) أن أنظمة الأمان بالطائرة لم تختبر كاملاً، على الرغم من إنفاق ٢ بليون دولار فى تصنيع هذه الطائرة. وتبين أن هناك مشاكل فنية عديدة تعانى منها الطائرة خاصة عند سقوط الأمطار. وقد ورد تقرير صادر عن القوات الجوية الأمريكية يفيد أن رادار الطائرة لا يمكنه التمييز بين قطرات المطر أو أى أجسام أخرى[١٠١]. والجدير

بالذكر أن هذه الطائرة استعملت لأول مرة أثناء قذف قوات حلف الناتو ليوغوسلافيا عام ١٩٩٩م[١٠٢].

والمعروف أن مهندسى التصميم يستخدمون برامج خاصة فى تحليل النماذج المختلفة. ودرجة التعقيد للنظم التكنولوجية والتكامل بين أجزائها. وهناك دائمًا قدر لعدم الدقة فى عمل هذه البرامج، قد يكون ضئيلاً، إلا أنه يسمح دائمًا بإمكانية حدوث الخطأ. على سبيل المثال، عند تصميم النظم البصرية فى التليسكوب هابل الفضائى، كان هناك خطأ ضئيل فى مقدار انحناء المرايا الابتدائية والثانوية فى هذا النظام بمقدار $\frac{١}{٥٠} - \frac{١}{١٠٠}$ من الدرجة وهو ما يمثل سمك شعرة الرأس. وفى حقيقة كان من الممكن الكشف عن هذا الخطأ إذا تم اختبار وضع المرآتين معًا، إلا أن هذا الاختبار قد تم فقط عن طريق برامج المحاكاة بالكمبيوتر [١٠٣]. وكان من الصعب رصد مقدار هذا الخطأ. فإن أى كمبيوتر لا يمكنه منح الإجابات الصحيحة أذا لم يسأل الأسئلة الصحيحة !! فهذه الحسابات الآلية لا تملك الأحاسيس عن مدى خطورة التصميم أو معرفة أى الأجزاء يكون مهمًا، وهذا يرجع أولاً وأخيرًا إلى مصممى هذه البرامج. ويحتاج الأمر إلى العناية الدقيقة بالأنظمة المعاونة التى قد تقلل من احتمالات حدوث الأخطاء. ويقول المؤلف إن معظم المفاعلات النووية القديمة تعانى من فشل أنظمتها الإلكترونية، وكذلك فى أنظمة الطائرات ومنصات إطلاق الصواريخ.. إلخ. ويعزو ذلك إلى أن معظم الدوائر المتكاملة المصنوعة من مواد أشباه الموصلات لم تجر عليها اختبارات الجودة والقياس[١٠٤]. وهذا لا يعنى فشل الأنظمة الإلكترونية الحديثة، ولكن يعنى عدم الوثوق بكفاءتها. وهذا الأمر يعود إلى التكاليف الباهظة التى يحتاجها برنامج الاختبارات.

ويركز المؤلف على ضرورة القيام بأعمال الصيانة التى أصبحت من الأمور المهمة لضمان استمرار العمل فى النظم التكنولوجية المتقدمة. فأى من هذه الأنظمة قد يصبح « قطعة من الخردة » دون إجراء الصيانة اللازمة لرفع الكفاءة. وكلما ازداد النظام تعقيدًا، أصبحت تكاليف الصيانة باهظة. ويسترشد المؤلف بتكنولوجيا الفضاء وما يحتاجه ذلك لتوفير الأموال الطائلة من أجل عمليات الصيانة للنظم الفضائية المعقدة، التى تحتاج إلى عناية ودقة فائقة. وحتى الآن لا يوجد أى دليل مقنع على أن الصيانة غير السليمة

تؤدى إلى فشل خطير فى الأنظمة التكنولوجية، فطبيعة هذه الأنظمة وتفاعلها مع قابلية الخطأ البشرى الذى صممها وبناها وقام بصيانتها، لا يوفر الضمانات الكافية لمنع حدوث الكوارث. ولا يوجد أى نوع من التكنولوجيات الخطرة يستثنى من هذه القاعدة .

الكمبيوتر والاصلاح التكنولوجى:

يعتقد الناس أن الكمبيوتر هو أحد الحلول الممكنة لعدم الأمان فى البشرية. فالكمبيوتر لا تشرب أو تتعاطى المخدرات وليس لديها عائلة ومشاكل شخصية ولا تسأم من الأعمال الروتينية. وفى بعض الأوقات وبعض الأعمال يكون الكمبيوتر أكثر أمنًا من الناس ولكنه فى أحيانًا أخرى يكون أقل أمنًا. فهذه الكمبيوترات تفتقر إلى الإحساس المشترك والحكم الجيد والإحساس بالخلود. وهى تضخم ولا تتغلب على الخطأ البشرى. على سبيل المثال عندما أخطأ طيار إحدى الطائرات التابعة للخطوط الجوية الأمريكية (المسافرة إلى كالاى ـ بكولومبيا) فى كتابة الشفرة للكمبيوتر بالطائرة فى ديسمبر ١٩٩٥م ، أخذ الكمبيوتر الطائرة إلى « بوجاتا ».

ومعظم النظم العسكرية الحديثة تعتمد بشدة على الكمبيوترات التى تتحكم فى المعدات وفى استعمال الأسلحة ونوعية أجهزة التحكم، ويعتبر من وجهة النظر العسكرية أن الكمبيوتر هو الجندى المثالى بالقوات المسلحة، حيث يتبع الأوامر دون تردد ودون طرح الأسئلة . . والبرامج ما هى إلا مجموعة من الأوامر تنفذ آليا ، ومن ناحية أخرى تعمل هذه البرامج أحيانًا على تغيير عمل الكمبيوتر بطريقة غير .مرغوبة (مثل الفيروسات). والكمبيوتر يفعل ما يأمر به المبرمج، عندئذ تصبح المشكلة لدى الإنسان وليس الكمبيوتر [١٠٥]. ولا يمكن تفادى حدوث خلل عند كتابة البرامج المعقدة، مما يجعل إمكانية لحدوث تفاعلات مختلفة بالنظام، حيث من الممكن تركيب الأحداث بطرق مختلفة، تؤدى فى بعض الأحيان إلى حدوث كوارث ولا يمكن بسهولة التعرف عليه.

والجدير بالذكر أن مثل هذا الخلل أدى أثناء حرب الخليج عام ١٩٩١ إلى تراكم الخطأ فى التوقيت بمقدار ١ مليون جزء من الثانية، مما تسبب فى فشل صواريخ باتريوت من التصدى لصواريخ سكود العراقية، والتى دمرت أحد المعسكرات الأمريكية فى مدينة الظهران بالسعودية [١٠٦].

ويقول المؤلف إن « الذكاء الاصطناعى » هو أحد مجالات علوم الحاسب التى بدأت فى الخمسينيات من القرن العشرين، ومنذ الثمانينيات أصبح هذا المجال من أهم وسائل نظم الدفاع الاستراتيجى الأمريكى، خاصة بعد أن اقترح الرئيس الأمريكى الأسبق « رونالد ريجان » استخدام أساليب الذكاء الاصطناعى من أجل إعادة بناء الصواريخ النووية المتقادمة وإدخال نظم حديثة للاستشعار عن بعد ومعدات التوجيه السريع. ومن المعروف أن نظم الذكاء الاصطناعى تتكون من قسمين، هما : قسم التنقيب ، ويعتنى بالتحليل والإرشاد ، وقسم التشخيص الذى يحتوى على مجموعة من «البرامج المنطقية » تمكن الكمبيوتر من معالجة الحالات المعقدة والحالات الفرعية التابعة، ومن ثم عليه أن يقرر ماذا نفعل ؟ وهناك محاولات دؤوبة من قبل الشركات المتخصصة من أجل جعل الكمبيوتر قادرًا على القيام بجميع أعمال الإنسان، خاصة الأعمال الشاقة اعتمادًا على أساليب الذكاء الاصطناعى.

فيروسات الكمبيوتر :

أحيانًا، يتعرض الكمبيوتر إلى هجوم فيروس، يجعله عديم الفائدة. والفيروس هو « برنامج مدمر » يعدى باقى البرامج عن طريق استنساخ ذاته بطريقة آلية. وفى حالة إصابة الكمبيوتر بالفيروس، فإنه ينصاع إلى جميع الأوامر التى يضعها الفيروس.

ومن المعروف أن لفيروسات الكمبيوتر أنواعًا عديدة منها فيروسات غير مؤذية ولا تسبب مشاكل جادة، والبعض الأخر فيروسات خبيثة تسبب أضراراً جسيمة مثل تخريب الملفات والنتائج أو تشويه بعض البرامج الأساسية وكذلك تدمير البعض منها أو تعديلها. ومن الصعب التحكم فى هذه الفيروسات والحد منها أو القضاء عليها، حيث إنها تعمل على تهديد برامج التشغيل فى أنظمة الكمبيوتر الشخصى أو الشبكات المتصلة.

وهناك كما يقول المؤلف ، ثلاث استراتيجيات أساسية للدفاع عن أنظمة الكمبيوتر ضد الإصابة بالفيروسات، هى :

١ ـ الوقاية ومنع التعرض للإصابة.

٢ ـ التحصين .

٣ ـ العلاج .

وفى الوقت الحالى تم تطوير برنامج يسمى « فاكسين » يرصد أولاً البرنامج الفيروسى ثم يقضى عليه [١٠٧] ومازال الصراع مستمرًا بين الخير والشر فى عالم الكمبيوتر .

أخطاء الكمبيوتر والتكنولوجيات الخطرة :

يقول المؤلف، إن صنع القرار عند معالجة الأزمات عادة يكون فى غاية الصعوبة، خاصة عندما يتعلق الأمر بالتكنولوجيات الخطرة وإمكانية حدوث الخطأ فى وقت قصير جدًا. وقد يؤدى عجز الكمبيوتر عن أداء وظيفته بكفاءة إلى حدوث كوارث مميتة، فتعطيل جزء فى جهاز الكمبيوتر فى المكان والتوقيت الخاطئ قد يهدد الأمن العالمى أجمعه. ويستشهد المؤلف بما حدث فى مقر قيادة الدفاع النووى الأمريكية، عندما اكتشف فى ٣ يونيو عام ١٩٨٠ تعطل دائرة الكترونية متكاملة فى جهاز الكمبيوتر المسئول عن نظام الإنذار المبكر، وعلى الرغم من أن سعر هذه الدائرة الإلكترونية لا يتعدى نصف دولار، إلا أن إطلاق صفارات الإنذار عن طريق الخطأ والتى تنذر بهجوم نووى عن طريق غواصة سوفينية، وضع القوات الأمريكية النووية على أهبة الاستعداد، مما تسبب فى تكبد مبالغ طائلة فى ذلك الوقت. ويقول المؤلف، هناك دائمًا أعطال مباشرة للكمبيوتر العسكرى فى أنظمة الصواريخ والطائرات، مما يجعل احتمالات حدوث أخطاء كبيرة .

ويسرد المؤلف قصة تدمير سفينة القيادة الإنجليزية « شيفلد» أثناء الحرب بين إنجلترا والأرجنتين عام ١٩٨٢ فى نزاعهما على جزر الفولكلاند فى المحيط الأطلنطى . خلال هذه المعركة أطلقت الأرجنتين أحد الصواريخ البحرية من طراز « اكسوست » فرنسية الصنع على السفينة . وعلى الرغم من رصد أجهزة الرداد للصاروخ أثناء طيرانه بالقرب من سطح البحر ، إلا أن أجهزة الإنذار لم تعمل نظرًا لأن الكمبيوتر كان مصنفًا الصاروخ كصديق! والجدير بالذكر أن الأرجنتين نجحت فى استخدام ستة من هذا الطراز الصاروخى فى تدمير بارجتين وأصابة ثالثة بأضرار جسيمة [١٠٨] .

ويضيف المؤلف أن أحدى أهم القضايا المتعلقة بحماية المعلومات الاستراتيجية لدى وزارة الدفاع الأمريكية، ويكشف عن تقرير قدم عام ١٩٩٦ إلى هيئة الدفاع القومى بالكونجرس الأمريكى، يفيد بمدى صعوبة حماية المعلومات الاستراتيجية، خاصة أن وزارة الدفاع تمتلك أكثر من ٢,١

مليون جهاز كمبيوتر وعشرة آلاف شبكة اتصال عملية ومائة ألف شبكة اتصال دولية. وأورد التقرير حدوث أكثر من ٢٥٠,٠٠٠ (مائتين وخمسين ألف) عملية هجوم على الحاسبات الإلكترونية بهيئة الدفاع، ٦٥٪ منها كان ناجحًا. وتأتى هذه الاختراقات الأمنية من خلال شبكة متقدمة من الجواسيس، التى تحاول الحصول على أسرار تصميم وتصنيع التكنولوجيات الخطرة فى شتى المجالات النووية والكيمائية والبيولوجية. بالإضافة إلى ذلك هناك شبكة من الإرهاب الدولى المنظم، لها أهداف عسكرية تستطيع القيام بالأعمال التخريبية لأنظمة الكمبيوتر، عن طريق تطوير فيروسات الكمبيوتر. ولابد أن نعترف أن الهجوم الفيروسى للحاسبات يهدد بوضوح كفاءة نظم الكمبيوتر فى التحكم والتعامل مع التكنولوجيات الخطرة مما يسمح بإمكانية حدوث الخطأ.