تحقيق المتانة والمرونة في العمليات اللوجيستية ضمن بيئة معلومات متدهورة

دون سنايدر (Don Snyder)، إليزابيث بودين بارون (Elizabeth Bodine-Baron)،
مهيار إيه. أموزيغار (Mahyar A. Amouzegar)، كريستين أف. لينش (Kristin F. Lynch)،
ماري لي (Mary Lee)، جون جي . درو (John G. Drew)

للحصول على مزيدٍ من المعلومات حول هذا المنشور، الرجاّء زيارة الموقع الإلكتروني
https://www.rand.org/t/RR2015

نشرته مؤسسة RAND، سانتا مونيكا، كاليفورنيا
© حقوق الطبع والنشر لعام 2017 محفوظة لمؤسسة RAND
RAND® هي علامة تجارية مسجّلة.

حقوق الطبع والنشر الإلكتروني محدودة

هذه الوثيقة والعلامة (العلامات التجارية) الواردة فيها محمية بموجب القانون. يتوفر هذا التمثيل للملكية الفكرية الخاصة بمؤسسة RAND للاستخدام لأغراض غير تجارية حصريًا. يحظر النشر غير المصرَّح به لهذا المنشور عبر الإنترنت. يصرح بنسخ هذه الوثيقة للاستخدام الشخصي فقط، شريطة أن تظل مكتملة بدون إجراء أي تعديل عليها. يلزم الحصول على تصريح من مؤسسة RAND لإعادة إنتاج أو إعادة استخدام أي من الوثائق البحثية الخاصة بنا، بأي شكل كان، لأغراض تجارية. للمزيد من المعلومات حول تصاريح إعادة الطباعة والربط على المواقع الإلكترونية، الرجاء زيارة صفحة التصاريح في موقعنا الإلكتروني:
www.rand.org/pubs/permissions

مؤسسة RAND مؤسسة بحثية تُعِدّ حلولًا للتحديات التي تواجه السياسات العامة، للمساهمة في جعل المجتمعات حول العالم أكثر أمانًا وسلامةً وصحة وازدهارًا. تعَدّ مؤسسة RAND مؤسسة غير ربحية وحيادية وملتزمة بالصالح العام.

لا تعكس منشورات مؤسسة RAND بالضرورة آراء عملاء ورعاة الأبحاث الذين يتعاملون معها.

ادعم مؤسسة RAND
وتبرع بمساهمة خيرية معفاة من الضريبة على
www.rand.org/giving/contribute

www.rand.org

تمهيد

تعتمد العمليات اللوجستية على المعلومات الدقيقة. فاتخاذ القرارات بالاستناد إلى معلوماتٍ غير دقيقة قد يؤدي إلى تعارض عمليات الدعم مع النتائج المرجوّة ما قد يؤثر سلبًا على العمليات القتالية. فحتى الأخطاء الصغيرة نسبياً في أنظمة الدعم تترك أثرًا كبيرًا على العمليات في بعض الأحيان. ولكن حدوث الأخطاء أمر محتّم، لذلك يجب أن تمتلك العمليات اللوجيستية المتانة اللازمة لمواجهة الأخطاء، سواء أكانت عشوائية أم نتيجة هجوم إلكتروني متعمّد وموجّه.

طلبت القوات الجوية الأمريكية من مشروع RAND للقوات الجوية تحديد المواضع التي يمكن أن تستثمر فيها القوات الجوية جهودها في إحداث تغييرات على الأساليب والتقنيات والإجراءات وذلك بهدف تحسين قدرة الطيار على اكتشاف أي تلف كبير في البيانات اللوجيستية وتقييمه والتخفيف منه. والهدف من ذلك هو معالجة الأخطاء الموجودة في البيانات قبل أن تترك أثرًا سلبيًا بالغًا في العمليات القتالية.

أُنجز العمل بوصفه جزءًا من مشروع يعود إلى السنة المالية 2016 تحت عنوان "قدرة العمليات اللوجيستية على الصمود والاستمرار بعد التعرّض لهجوم إلكتروني"، وذلك برعاية مدير تحقيق التكامل بين الموارد وتحت قيادة نائب قائد القوات الجوية الأمريكية للشؤون اللوجيستية والهندسة وحماية القوات، وبرعاية مشتركة من مدير الشؤون اللوجيستية والهندسة وحماية القوات في قيادة الضربة الشاملة في القوات الجوية. وأجري العمل ضمن برنامج إدارة الموارد لمشروع RAND للقوات الجوية. هذه الدراسة يجب أن تُهم العاملين في مجالي اللوجيستيات والعمليات في القوات الجوية.

مشروع RAND للقوات الجوية

مشروع RAND للقوات الجوية (PAF) هو القسم في مؤسسة RAND الذي يمثل مركز البحث والتطوير للدراسات والتحليل الممول فدراليًا من القوات الجوية الأمريكية. يقوم هذا المشروع بتزويد القوات الجوية بتحليلات مستقلة لبدائل السياسات التي تؤثر على التطوير والتوظيف والجاهزية القتالية ودعم القوات الجوية والفضائية والإلكترونية الحالية والمستقبلية. ويُجرى البحث ضمن أربعة برامج: تحديث القوات والتوظيف؛ والقوى العاملة والموظفين والتدريب؛ وإدارة الموارد؛ والاستراتيجيات والعقيدة. أُعدّت الدراسة الحالية بموجب العقد رقم FA7014-16-D-1000. للمزيد من المعلومات حول مشروع RAND للقوات الجوية يرجى زيارة: www.rand.org/paf

المحتويات

التمهيد iii
الأشكال والجداول vi
ملخص vii
شكر وعرفان xiii
اختصارات xiv
1. تحليل المشكلة 1
الدافع 1
هدف التقرير ونطاقه 2
المنهجية 4
السياق 4
إطار العمل 6
2. التحديات التي تواجه عملية الاكتشاف 7
سرعة الاكتشاف 7
عناصر عملية الرصد والاكتشاف 7
قدرة العميل على الاطّلاع على البيانات 8
الحالات الشاذة في البيانات 9
خبرة القوى العاملة 10
الدافع للتبليغ 11
ملخص التحديات التي تواجه عملية الاكتشاف 12
3. توصيات لتحسين عملية الاكتشاف 13
تحسين السرعة 13
الإجراءات على مستوى الأفراد 13
الإجراءات على مستوى المؤسسة 14
تجاوز عقبة العمليات الآلية 14
قانون بينفورد (Benford) 15
تقنيات أخرى 18
التأقلم مع ظروف الحرب 19
التدريب على عملية الاكتشاف 21
تحفيز عملية الاكتشاف 24
بناء ثقافة التبليغ والحفاظ عليها 24
آليات تحفيز الأفراد 26
تحفيز العاملين لاكتشاف البيانات الشاذة 28
نتائج ونقاش 29
التوعية والتدريب ورسائل القيادة 29
الوضعية 31
الأدوات 31

4. التقييم 32
حاجات عمليات التبليغ والتقييم 32
التبليغ 32
التقييم 33
قنوات التبليغ الحالية وحدودها 35
هيكل مقترح للاستجابة لعمليتي الإبلاغ والتقييم 37
العمليات اللوجيستية 37
العمليات الإلكترونية 39
ملخص 40
5. ترتيب الجهود من حيث الأولوية 41
ما الذي يجب أن تتضمنه عملية تحديد الأولويات 41
استراتيجية لتحديد الأولويات 42
الوقت 42
الهجمات الاحتمالية 45
الملخص 45
6. نقاش ونتائج 47
المراجع 49

الأشكال والجداول

الشكل S.1 هيكل الاستجابة المقترح لعملية التبليغ والتقييم.....x
الشكل 1.1 رسم بياني يوضح التوازن بين مقدار الثقة والشك.....5
الشكل 3.1 بيانات تسعير من D200A التي تتبع قانون بينفورد.....16
الشكل 3.2 بيانات قطع الغيار القابلة للإصلاح من D200A، والتي لا تتبع قانون بينفورد (Benford).....17
الشكل 3.3 تحليل عملية التحكم بالعمليات الإحصائية لطلبات المستودع.....19
الشكل 4.1 هيكل الاستجابة المقترح لعمليتي الإبلاغ والتقييم 38
الشكل 5.1 الأطر الزمنية المتنافسة للتأثير على العمليات القتالية والاستجابة.....43

الجدول 3.1 ملخص إطار العمل التحفيزي.....27

ملخص

لحماية قدرة القوات الجوية الأمريكية على إبراز قوتها، يجب أن يكون الدعم اللوجيستي متينًا ومرنًا ليستوعب طيفًا من التهديدات، بما في ذلك الهجمات الإلكترونية[1] وأحد أنواع هذه الهجمات هو الإتلاف المتعمّد للبيانات. عندما تكون البيانات تالفة، فإنّ الاعتماد عليها في أي إجراء يمكنه إعاقة سير العمليات اللوجيستية، مما قد يؤثر سلبًا على العمليات القتالية. ولكن الهجمات الإلكترونية المتعمدة ليست المسبب الوحيد لتلف البيانات، فقد ينتج ذلك أيضًا عن بعض الأخطاء الروتينية.

في عام 2015، وفي جزء من مبادرة تحت عنوان "قدرة العمليات اللوجيستية على الصمود والاستمرار"، قدمت قيادة العمليات اللوجيستية للقوات الجوية ثلاث خطوات للاستجابة لحالات الاشتباه بوقوع تلف في البيانات، وهي: (1) الاكتشاف (والإبلاغ) عن أي خطأ مشبوه؛ (2) تقييم ما إذا كانت بالفعل أخطاءً أم لا، وإن كانت كذلك، تحديد ما إذا كانت مجرد أخطاءٍ أم نتيجة لهجوم متعمّد؛ ومن ثم (3) العمل على التخفيف من أية مشاكل تواجه العمليات اللوجيستية ناتجة عن أخطاء حقيقية. الهدف من هذا التقرير هو تعزيز متانة العمليات اللوجيستية ومرونتها في حالة وقوع تلف كبير للبيانات. ويدرس التقرير ما يمكن أن يقوم به القائمون على الشؤون اللوجيستية لتحسين رصد تلف البيانات وتقييم مستوى التلف والإبلاغ عنه وإعطاء الأولوية للاستجابة، وذلك لضمان استمرار العمليات على نحو مُرضٍ. ولا يتطرق التقرير إلى التدابير التي يمكن أن يتخذها القائمون على أمن المعلومات أو إلى تدابير محددة تقلل من الهجمات الإلكترونية التي تستهدف الوحدات اللوجيستية.

اكتشاف تلف البيانات

بعد دراسة الخطوات اللازمة للنجاح في اكتشاف أي تلف في البيانات ضمن إطار عمل عالي المرونة، حددنا خمسة مجالات مهمة تعتبر واعدة أكثر من غيرها في تعزيز القدرة على كشف تلف البيانات:

1. يجب أن تتم عملية الاكتشاف بسرعة كافية. يمكن تحقيق هذه السرعة من خلال الجمع بين أفراد يقومون بالرصد والإبلاغ عن وجود بيانات تالفة بسرعة، والاكتشاف المبكر لتلف البيانات ضمن سلسلة الحفظ.
2. تمثل العمليات ذات الدرجة العالية من التشغيل الآلي، التي لا يرى الأفراد خلالها البيانات في العمليات العادية، تحديًا كبيرًا أمام عملية رصد أي خلل في البيانات. يتطلب التشغيل الآلي آليةً خاصة للمساعدة في اكتشاف التلف.
3. تزداد أهمية اكتشاف تلف البيانات في الحروب، ولكن الحالات الشاذة تكون أقل وضوحًا خلال الحروب بالمقارنة مع أوقات السلم، فالحرب بحد ذاتها حالةٌ شاذة. لذلك ثمة حاجة لوجود آليات لتعديل آليات الرصد من ظروف السلم إلى ظروف الحرب.
4. لكي يتمكّن العاملون (من طيارين ومدنيين ومتعاقدين) من اكتشاف البيانات الشاذة، عليهم أن يخضعوا جميعًا للتدريب لفهم النمط الأساسي المتوقع، كما ينبغي أن يكونوا متيقظين بشكل متواصل عند تفحّص البيانات.

---

1 يعني مصطلح "*متين*" القدرة على امتصاص هجومٍ ما والحفاظ على مستوى مقبول من التشغيل، أما *المرونة* فتشير إلى القدرة على العودة للعمل بسرعة كافية بعد التعرض لهجوم.

5. يجب أن تتيح القيادة بيئة تشجع العاملين على الإبلاغ عن البيانات الشاذة المشبوهة.

لمواجهة هذه التحديات، نقدم ثلاث توصيات أساسية:

أولاً، نوصي في إطار السياسة اللوجيستية، بتحديد التدابير التي يجب أن يتخذها العاملون في المجال اللوجيستي للاستجابةِ لمستوى كل حالة من حالات العمليات الخاصة بالمعلومات (INFOCON).[2] من بين جميع التوصيات في هذا التقرير، نعتقد أن هذا الإجراء هو أكثرها ترجيحًا لتحقيق نتائج إيجابية ملموسة بأقل قدر من الموارد. فهذه التدابير تركز على استمرار العمليات اللوجيستية أكثر من تركيزها على تأمين المعلومات. وسيتم تحديد الإجراءات ضمن المجال اللوجيستي لموازاة الإجراءات الحالية الخاصة بأنظمة تكنولوجيا المعلومات. لكل مستوى حالة من حالات العمليات الخاصة بالمعلومات، يجب تحديد تدابير احترازية في كل مجال وظيفي لزيادة المتانة والمرونة. يبدأ العمل بهذه التدابير مع ازدياد مستوى الخطورة لمطابقة الموارد التي أنفقت مع بيئة الخطر (وكذلك الكفاءة مقارنة بالتكلفة). وكما هو الحال عند التعامل مع مستويات حالة حماية القوات، تتميز التدابير التي ينبغي اتخاذها بكونها محددة ومخصصة، وتكون مدرجة ضمن تعليمات القوات الجوية الأمريكية.

ثانيًا، نوصي بتبنّي نهج بسيط للكشف عن تلف البيانات من خلال عمليات آلية بالكامل (لا يستطيع فيها البشر "رؤية" البيانات خلال العمليات العادية) تُستخدم بشكل روتيني للكشف عن عمليات الاحتيال. يُعد قانون بينفورد (Benford) (الذي سنتحدث عنه بشكل مفصّل في الفصل الثالث) إحدى الطرق السهلة نسبيًا للتحقق من صحة البيانات، لكن يمكن استخدام طرق معيارية أخرى. ويجب تحديد إلى أي مدى يمكن استخدام هذه التقنيات بالاعتماد على مستوى الخطر الإلكتروني (مستوى كل حالة من حالات العمليات الخاصة بالمعلومات) من أجل تقليل كمية العمل المطلوب. ولكن لا تعد هذه الأدوات حلاً بحد ذاتها، بل يمكن استخدامها للإبلاغ عن البيانات التي من المرجح أن تكون إشكالية وبالتالي إخضاعها للمزيد من المراجعة من قبل معنيين.

ثالثًا، نوصي بتعزيز تعليم جميع أعضاء المؤسسة وتدريبهم بشأن الخطر الذي يشكله تلف البيانات (وتشكله الهجمات الإلكترونية بشكل عام) على العمليات. فيما يلي، الأهداف الرئيسية لهذا التدريب:

- توعية جميع العاملين على جميع المستويات بأن *كل* أنظمة البيانات عرضة للتلف والهجمات الإلكترونية، ولذلك، فإن اليقظة مطلوبة تجاه جميع الأنظمة والعمليات.
- إرساء ثقافة لدى القوى العاملة تؤكد أنّ لكل فرد عامل في المؤسسة اللوجيستية حصة في الأمن الإلكتروني، وليس فقط أصحاب تخصصات معينة في الأمن الإلكتروني.

على كل مستويات القيادة (من رأسها حتى هيئات الإشراف) أن تقوم بدور في نشر هذه الرسائل. ويجب على من يشغلون المناصب العليا (من ضباط علم وضباط ميادين بشكل عام) أن يضعوا الإبلاغ عن المخاوف المتعلقة بالأمن الإلكتروني في أعلى سلّم أولوياتهم. ولتحقيق ذلك، يجب حماية الأشخاص الذين يقومون بالإبلاغ عن أية عمليات انتقامية، واعتماد سياسة تضمن سهولة القيام بالإبلاغ وتوفر توجيهات واضحة. يهدف ذلك إلى تغيير الثقافة السائدة لزيادة يقظة العاملين عند التبليغ عن احتمال وجود بيانات تالفة وغيرها من المخاوف الإلكترونية، بقدر يقظتهم حيال

[2] قريبًا سيتم الاستعاضة عن نظام مستوى حالة العمليات الخاصة بالمعلومات (INFOCON) بنظام حالة الفضاء الإلكتروني (CYBERCON). فمستويات النظام الأول شاملة يحددها القائد أو القيادة الإستراتيجية الأمريكية. ولكن بإمكان القادة على جميع المستويات أن يحددوا محليًا مستويات لحالات العمليات تكون أكثر صرامة للأنظمة التي يتولّون قيادتها (رئيس هيئة الأركان المشتركة الأمريكية 6510.01F، 9 شباط (فبراير) 2011، يبدأ العمل بالتوجيه الحالي اعتبارًا من 9 حزيران (يونيو) 2015; وفقًا لتوجيهات القيادة الاستراتيجية 1-527، 27 كانون الثاني (يناير) 2006).

السيطرة على الضرر الذي تلحقه الأجسام الغريبة بخطوط الطيران وغيرها من المخاوف المتعلقة بالسلامة. وحاليًا، يتوفر القليل من المراجع، إن وجدت، حول سلامة البيانات أو الأمن الإلكتروني في الإصدارات اللوجيستية.[3]

يجب على أصحاب الرتب القيادية الأدنى (الضباط الأعوان وكبار ضباط الصف غير المفوضين) أن يطوّروا توجيهات واضحة ومحددة للعاملين بشأن أنواع البيانات الشاذة الواجب عليهم الإبلاغ عنها وفقًا للمعرفة التي يملكونها حول حاجات العمليات.

يجب أن يتم تعميم الرسائل على جميع العاملين، بما في ذلك الطيارين والمدنيين والمتعاقدين. يجب أن يستمر تعميم هذه الرسائل بشكل دائم. بالنسبة للطيارين، يجب أن يبدأ ذلك من المدرسة التقنية ويستمر خلال التدريب العملي والتمارين. بالإضافة إلى ذلك، يجب تطبيقها بأكبر قدر ممكن ضمن بيئة العمل من خلال اختبار أمثلة حقيقية، ويجب أن تركز على العواقب المحتملة التي تترتب على الفشل في اكتشاف البيانات الشاذة والإبلاغ عنها.

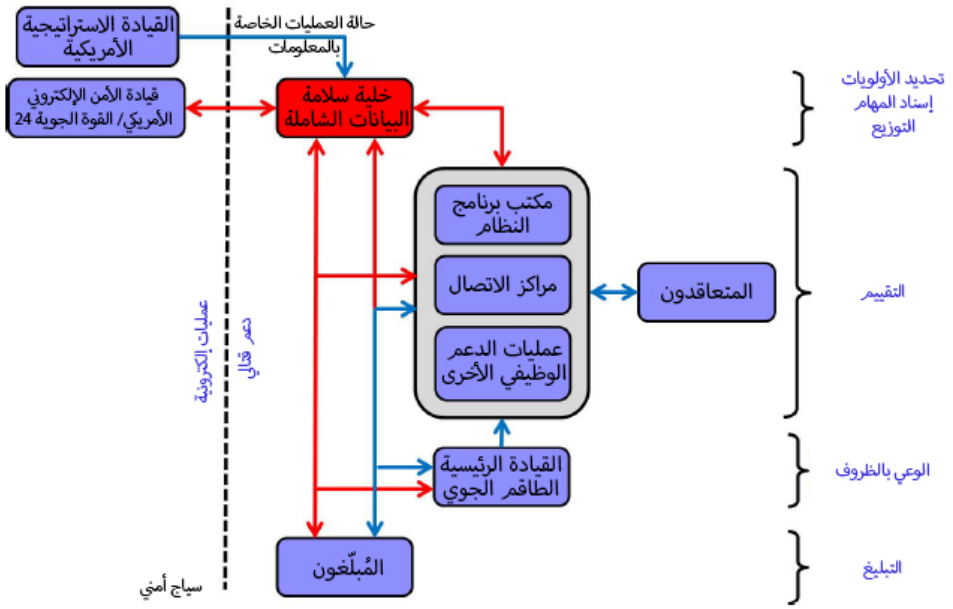
الإبلاغ والتقييم

ثمة العديد من أوجه القصور في الآليات الحالية للإبلاغ والتقييم لدى القوات الجوية الأمريكية. ولم يتم تصميم أي منها بهدف الحد من الهجمات الإلكترونية. لذلك نوصي باستكمال آليات الإبلاغ والتقييم الحالية مع بعض آليات وعمليات الإبلاغ الإضافية وإنشاء خلية تنسيق. المخطط الكامل المقترح موضح في الشكل S.1.

في الشكل S.1، تكون العناصر البنيوية الحالية (قنوات ومنظمات الإبلاغ) موضّحة بالأسود والأزرق أما العناصر البنيوية المقترحة حديثًا فتكون موضحة باللون الأحمر. عند قراءة الشكل من أسفل إلى أعلى، يبلّغ الطيارون والمدنيون والمتعاقدون (المشار إليهم في المربع المعنوَن "المُبلّغون") عن البيانات التي يشتبهون بتعرّضها للإتلاف . أما الخط الأسود فيمثّل قنوات الإبلاغ العديدة الموجودة (مثل مكاتب المساعدة والتقارير المبنية على النموذج 22 والطلبات 107). تصل هذه التقارير إلى منظمات مختلفة كي تخضع لشكل من أشكال التقييم (مثل مكاتب البرامج ومراكز الاتصال ووكالة لوجيستيات الدفاع) وغالبًا ما يتم توجيهها إلى منظمات أخرى بهدف نشر الوعي بشأن الظروف المحتمل مواجهتها (مثل موظفي قيادة رئيسية)، كما هو موضح في المربع الموجود على يمين القوس بعنوان "الوعي بشأن الظروف المحتملة". بعد انتهاء عملية التقييم، عادةً ما تُرسل بعض الملاحظات إلى الأفراد الذين رفعوا التقرير. وفي حالات قليلة، قد تؤدي هذه الملاحظات إلى تغيير السياسة أو التوعية أو التدريب، إلّا أنه لا يتم تطبيق أي من هذه الحلول بشكل منتظم حاليًا.

[3] على سبيل المثال، سياسة المؤسسة لصيانة الطائرات، تعليمات القوات الجوية 21-101، 2015، لا تتضمن هذه الرسائل.

الشكل .S.1 هيكل الاستجابة المقترح لعملية الإبلاغ والتقييم



ملاحظات: تشير الخطوط الزرقاء إلى القنوات الموجودة. أما الخطوط والمربعات الحمراء فتشير إلى القنوات والكيانات الجديدة. GLODIC (Global Data IntegrityCell) تعني خلية سلامة البيانات الشاملة، وتعني MAJCOM (major command) قيادة رئيسية، وتشير SPO (system programoffice) إلى مكتب برنامج النظام، أما USCYBERCOM (U.S. CyberCommand) فهي تعني قيادة الفضاء الإلكتروني الأمريكية، وUSSTRATCOM (U.S.Strategic Command) تعني القيادة الاستراتيجية الأمريكية.

لا توجد سلطة مطّلعة على جميع التقارير المرفوعة حاليًا بهدف تقييمها لمعرفة ما إذا كان هناك هجوم منسق قد يحدث أم لا. كما لا توجد سلطة مركزية تتحمّل مسؤولية تحديد السبب وراء أي تلف كبير يصيب البيانات الحساسة ونشر معلومات حول كيفية معالجته.

بالتالي، نقترح إنشاء هيئة مركزية جديدة تحت اسم "*خلية سلامة البيانات الشاملة*" (Global DataIntegrity Cell GLODIC)، والتي ستحصل على نسخ من جميع هذه التقارير. سوف تحافظ هذه الخلية على قدر من الوعي بالظروف على مستوى المؤسسة بجميع التقارير الموجودة. ونظرًا إلى أنّه تم اتخاذ إجراءات بشأن هذه التقارير من قبل القائمين على عملية التقييم، وتم تحديدها في السياسات التي تحكم آليات الإبلاغ الحالية، سيكون الجزء الأكبر من الدور الرئيسي لهذه الخلية تجاه هذه التقارير هو البحث عن الاتجاهات والهجمات المنسقة المتوقعة واستخلاص الدروس مع الوقت والقيام بدور مركز لتبادل المعلومات حول هذه الدروس المستقاة. ويجب ألّا يقتصر عمل الخلية على هذه الأنشطة، بل يجب أن يمتدّ لتتبع المسائل اللوجيستية الأخرى التي تتعلق بالفضاء الإلكتروني. كما يمكن لها أن تكون منظمة موجودة ذات مسؤوليات أوسع شاملة لهذه الأنشطة، مع زيادة الموارد بما يتناسب مع حجم المسؤوليات الملقاة على عاتقها.

أما النشاط الداعم الثاني المقترح فيتمثل في إجراء تقييم لمعرفة ما إذا كان قد وقع هجوم إلكتروني أم لا. ويجب أن يتم التقييم من قبل أصحاب الخبرة وليس بالضرورة من قبل منظمة مركزية. أما بالنسبة لأنظمة الأسلحة، قد تكمن الخبرة في قيادة الإمدادات في القوات الجوية. أما أنظمة تكنولوجيا المعلومات المتصلة بالشبكة، فتكمن الخبرة المطلوبة للتعامل معها في القوة الجوية رقم أربع وعشرين. ولكن مع وجود خلية سلامة البيانات الشاملة GLODIC، ستحتاج

بعض المنظمات إلى تشكيل وجهة نظر خاصة بالمؤسسة وأرشفة الحوادث وتعميم الإرشادات. وقد تشمل الإرشادات إما وجوب عزل النظام عن الشبكة وتغيير الإجراءات وإغلاق الأنظمة من أجل الأدلة الجنائية أم لا. ويمكن لقيادة الفضاء الإلكتروني الأمريكية والقوة الجوية الرابعة والعشرين تأدية هذه المهام.

تحديد الأولويات

إن حل هذه المشاكل في جميع الأنظمة والوظائف التي تدعمها سيشكل عبئًا كبيرًا. وللحصول على استجابة مثلى، يجب إعطاء الأولوية لإجراءات وقائية والتبليغ عن أحداث دون غيرها. ويجب تحديد إطار زمني للاستجابة للحوادث من أجل تقييمها والعمل على الحد منها. الهدف من ترتيب الأولويات هو ترتيب مستويات الخطورة وليس تقييمها. ويتمثل أحد العناصر الأساسية لتحديد الأولويات في فهم العلاقة بين المتانة المتأصلة لأي عملية (الوقت الذي يستغرقه الهجوم للتأثير على العمليات القتالية) ومقدار مرونة الاستجابة بعد التعرض للهجوم (الوقت اللازم للكشف عن الهجوم والإبلاغ عنه وتقييمه والتخفيف من آثاره والتعافي منه). تُعطى أولوية الاستجابة للعمليات الهشة ومن ثم العمليات المتينة. ويشكّل كل من الوقت، الذي ينظر إليه باعتباره عاملاً تنافسيًا، واحتمال التعرّض لهجوم ما بُعدين مهمين لمستوى الخطورة يعدّان عاملين أساسيين في اقتراحنا لتحديد الأولويات. وبذلك يمكن وضع استراتيجية لتحديد الأولويات بالترتيب الآتي:

1. وضع قائمة بالمهام (التي قد تبلغ العشرات) والوظائف التي تُنجز ضمن المجال اللوجيستي. يعتمد مستوى الدلالة في تفصيل المهام على عملية الاكتشاف التي تتم خلال الخطوات اللاحقة.
2. لكل مهمة، يجب تحديد هذه الأنظمة للبيانات التي تتحكم بالعملية أو أرشفة البيانات الموثوقة التي تُبنى عليها الإجراءات أو القرارات.
3. تصنيف مستوى الاشتباه في هذه الأنظمة للبيانات تلك بناءً على الأمن النسبي لمستضيفي هذه الأنظمة.
4. إذا اتُّخذت إجراءات بناءً على بيانات خاطئة في أي من هذه الأنظمة للبيانات، يجب تقدير الوقت الذي سيستغرقه ظهور الآثار السلبية على العمليات القتالية (ساعات أو أيام أو أسابيع أو شهور أو سنوات).
5. إذا اتُّخذت إجراءات بناءً على بيانات خاطئة في أي من أنظمة البيانات هذه، يجب تقدير وقت الاستجابة على وجه التقريب، والذي قد يحكمه الوقت اللازم للتعافي من الهجوم (ساعات أو أيام أو أسابيع أو شهور أو سنوات).
6. مقارنة هذه الأوقات ومن ثم ترتيب المهام بناء على ذلك.
7. التخطيط للهامش الزمني للمهام تبعًا لمستوى الاشتباه في أنظمة البيانات المرتبطة بها.
8. تحديد الأولويات من خلال البدء بأزواج المهام التي تملك أقصر هامش زمني والتي تكون أنظمة بياناتها أكثر قابلية للتأثر وصولاً إلى تلك التي تملك أطول هامش زمني وأنظمة بياناتها هي الأقل قابلية للتأثر.

من بين هذه التوصيات، نعتقد أن التوصيتين الواعدتين أكثر من غيرهما ستشكلان مقدمة للسياسة اللوجيستية للاستجابات لمختلف مستويات حالات العمليات الخاصة بالمعلومات (INFOCON) ولإيصال المسؤوليات التي قمنا بتحديدها إلى منظمة نسمّيها "خلية سلامة البيانات الشاملة" (GLODIC). وقد تكون هذه المنظمة منظمة موجودة بالفعل، ويمكنها كذلك تأدية مهام أخرى مرتبطة بالعمليات الإلكترونية بالإضافة إلى التعامل مع تلف البيانات.

وبما أن تلف البيانات هو أحد أنواع الهجمات الإلكترونية، طوّرنا الحجج الرئيسية في هذا التقرير قدر الإمكان لتكون عامة بما يكفي لمواجهة أكبر قدر ممكن من الهجمات الإلكترونية. يمكن توسيع مخطط تحديد الأولويات بسهولة

ليشمل مجموعة كاملة من الهجمات الإلكترونية. وإن الأفكار المتعلقة بتحسين عملية الاكتشاف ليست بالأهمية نفسها بالنسبة لجميع الهجمات، فبعض الهجمات تكون في غاية الوضوح مثل تدمير البيانات وحظر الوصول إليها، ولكن يمكن لهذه الأفكار أن تكون مفيدة في الاكتشاف المبكر عن هجمات أقل وضوحًا. وتجدر الإشارة إلى أن الطرق التي نوصي باتباعها عند الإبلاغ وتقييم البلاغات تجدي نفعًا في جميع أنواع الهجمات الإلكترونية ولا يجب أن تقتصر على فقط على تلف البيانات.

شكر وعرفان

نتقدم بالشكر إلى كل من لاري كينغسلي (Larry Kingsley) ولورنا استيب (Lorna Estep) لإشرافهما ودعمهما خلال الدراسة. نشكر أيضًا العديد من أفراد القوات الجوية الذين ساعدونا ودعمونا، وهم كثر إلى درجة يصعب ذكرهم جميعًا بالأسماء. ولكن لا من غنى عن أفكارهم وانتقاداتهم.

نقدم شكرًا خاصًا للزملاء في مؤسسة RAND الذين ساهموا في المناقشات وهم بات بورين (Pat Boren)، وليونيل غالوي (Lionel Galway) وسارة نواك (Sarah Nowak) ولورين كيندريك (Lauren Kendrick) ومارك بوزارد (Marek Posard) وجيم باورز (JimPowers) ومارك روبينز (Marc Robbins) ولارا شميت (Lara Schmidt)

كما نشكر كلاً من دان غونزاليس (Dan Gonzales) ودانييل طرّاف (Danielle Tarraf) لمراجعتهما المسودة الأولى من هذا التقرير.

ما تلقيناه من مساعدة وآراء من الأشخاص المذكورين أعلاه لا يعني أنهم يتفقون مع الآراء الواردة في هذه الدراسة. فنحن وحدنا مسؤولون عن المضمون، بما فيه من أخطاء أو نواقص.

اختصارات

AFMC/EN	مديرية الهندسة والإدارة التقنية التابعة لقيادة الإمدادات في القوات الجوية
ASRS	نظام تقرير سلامة الطيران
CYBERCON	حالة الفضاء الإلكتروني
FPCON	حالة حماية القوات
GLODIC	وحدة سلامة البيانات الشاملة
INFOCON	حالة العمليات الخاصة بالمعلومات
LogATSO	قدرة العمليات اللوجيستية على الصمود والاستمرار
MAJCOM	القيادة الرئيسية
MICAP	القدرة على أداء المهمة
NIPRNet	شبكة موجّه بروتوكول الإنترنت غير الآمنة
PAF	مشروع القوات الجوية
PKI	بنية تحتية رئيسية عامة
SPO	مكتب برنامج النظام
USCYBERCOM	قيادة الفضاء الإلكتروني الأمريكية
USSTRATCOM	القيادة الاستراتيجية الأمريكية

1. تحليل المشكلة

الدافع

بإمكان القوات الجوية الأمريكية إبراز قدر كبير من القوة الجوية في أي مكان في العالم وخلال وقت قصير. تشكل هذه القوة تحديات كبيرة أمام أي خصم يفكر في شن هجمات مباشرة. تتطلب القوات الجوية دعمًا لوجيستيًا آنيًا[4]، ولذلك قد يختار الخصم شن هجمات غير مباشرة ضد القوات الجوية من خلال استهداف دعمها اللوجيستي. الهدف من وراء هذه الهجمات هو عرقلة القوات الجوية الأمريكية من خلال تقويض أساساتها. وقد يتراوح الأثر المرجو من هذه الهجمات بين إبطاء القوات الجوية أو إعاقة قدرتها على شن عمليات استطلاعية، ربما ما يكفي من الوقت ليتمكّن الخصم من تحقيق النتائج التي يصبو إليها، لإيقاف جميع العمليات القتالية من خلال إصابة العمليات اللوجيستية بالشلل.

لحماية القدرة على إبراز قوتها، يجب أن تتأكد القوات الجوية من قدرة عملياتها اللوجيستية على امتصاص أي هجوم (المتانة) واستعادة وظائفها بشكل مرضٍ بعد ذلك (المرونة).[5] تتخذ الهجمات التي تستهدف العمليات اللوجيستية أشكالاً متعددة، ومن الأشكال التقليدية للهجمات تلك التي تستهدف القدرة الحركية، وأحد الأمثلة البارزة على ذلك تفجير المدارج. وبالرغم من أن الأقسام اللوجيستية ليست مسؤولة عن حماية مدارج الطائرات بشكل مباشر، فإنها مسؤولة عن إصلاحه بسرعة لاستعادة القدرة على شن العمليات. وهناك العديد من الأمثلة المشابهة، وتتمتع القوات الجوية الأمريكية بقدرة كبيرة على الحفاظ على مستوى مقبول من الدعم اللوجيستي بالرغم من أية هجمات قد تستهدف قدرتها الحركية (بما في ذلك الهجمات الكيميائية والبيولوجية النووية).

يمثل الفضاء الإلكتروني مجالاً جديدًا نسبيًا لشن الهجمات. وكما هي الحال مع أغلب الهجمات التي تعطّل الحركة، فإن الأقسام اللوجيستية غير مسؤولة بشكل مباشر عن حماية أنظمتها الإلكترونية من هذه الهجمات، ولكنها تكون مسؤولة عن امتلاك القدرة على تجاوز هذه الهجمات والتعافي منها.[6] وتتخذ العمليات الإلكترونية أشكالاً متعددة، فقد يسعى الخصم إلى نقل المعلومات بشكل غير مشروع لأغراض استخباراتية، أو قد يشن هجومًا شرسًا عبر تدمير بيانات أو تلفها أو حظر الوصول إليها أو السيطرة على العمليات. وتشكل كل هذه الأشكال للعمليات الإلكترونية خطرًا على العمليات اللوجيستية.

تقوم بالعمليات اللوجيستية في القوات الجوية الأمريكية أقسام عدة، منها تلك المسؤولة عن صيانة الطائرات وعمليات المطارات والهندسة المدنية والتخطيط اللوجيستي وإدارة الذخائر وقوات الأمن وعمليات سلسلة الإمداد. وللقيام بهذه المهام، طُوّرت المئات من أنظمة تكنولوجيا المعلومات لتخزين البيانات ونشرها ولإدارة عملية جرد

---

[4] يُستخدم مصطلح *لوجيستيات* في هذا التقرير بمفهومه الأوسع، كما تم تعريفه في المنشور المشترك 1-02 ، 2016: بعنوان "تخطيط وتنفيذ حركة القوات ودعمها". تكون المفاهيم عامة بما فيه الكفاية إلى درجة تنطبق بالتساوي على *اللوجيستيات والدعم القتالي*. وتُعرف الأخيرةُ في وثيقة عقيدة القوات الجوية 4-0، 2013، "بالقدرة الأساسية والشاملة على منح المرونة والدعم للقوات الجوية والحفاظ عليها واعتمادها كأساس للبناء في نطاق العمليات العسكرية".

[5] انظر على سبيل المثال، مجلس علوم الدفاع، 2015.

[6] هناك نوع من أنواع التوازي مع ضوابط السلامة، يكون فيه الوعي والاجتهاد والاستجابة لازمين على كل فرد. سنناقش هذه السمات في الفصلين الثاني والثالث.

المخزون والتحكم بالعمليات ونشر وعي بالظروف المحتملة لدعم عملية اتخاذ القرار. تُستخدم أنظمة المعلومات بشكل مستمر في جميع أرجاء العالم في مقرات القوات الجوية الأمريكية في السلم والحرب. ويتسم العديد من هذه الأنظمة بالارتباط بالشبكات، وبالرغم من أن معظمها خاصٌ بالقوات الجوية إلا أن بعضها أصبح في متناول الأوساط المشتركة والشركاء العاملين في القاعدة الصناعية. فمعظمها موجودة ضمن شبكة موجّه بروتوكول الإنترنت غير الآمنة (NIPRNet).

تعتمد العمليات اللوجيستية بشكل كبير على البيانات والمعلومات في هذه الأنظمة،[7] وفي غياب البيانات الموثوقة، تتوقف العديد من العمليات الأساسية. التعقيد والحجم الهائل لشبكة التوريد يفرض متطلبات معرفة مدى تطابق القطع وحجم المخزون ومواقع القطع والعديد من البيانات الأخرى تفوق القدرات البشرية. وتتطلب هذه العمليات أنظمة بيانية للعمل؛ وبدون هذه البيانات ستتوقف العمليات الجوية في نهاية المطاف. وتُعد صيانة الطائرات مثالاً آخر. حيث إن الطائرات الحديثة في غاية التعقيد ولا يمكن صيانتها دون الاعتماد على البيانات التقنية ومعدات التشخيص الآلية.

لا بُدّ بالطبع من حدوث الأخطاء، فهي تقع بشكل روتيني. ومع ذلك، فإن معظم الأخطاء التي تقع بشكل يومي لا تترك أثرًا سلبيًا كبيرًا على العمليات، كما تطورت الأنظمة اللوجيستية والعمليات لتتمكن من التعامل مع هذا النوع من الأخطاء. ومع أنّ العشوائية التي تتميز بها الأخطاء الروتينية تجعل من احتمال تسببها بمشكلة تشغيلية أساسية ضئيلاً للغاية، فإن هناك احتمال بتسببها بأثر كبير، كما أثبتت التجارب. ومن الأمثلة الحديثة على ذلك، إرسال قطعة صالحة من النظام التشغيلي للأسلحة ليتم نزعها وتنفيذ أمر تقني محدد بوقت زمني غير صحيح على أسطول من الطائرات.

قد يقوم خصمٌ ماهر ذو تصميم ومعرفة بإلحاق ضرر بالغ ومتعمد بالبيانات التي قد يصعب اكتشاف أنها بيانات شاذة، إلا أنها تؤثر بشكل كبير وسلبي على العمليات. وقد يلجأ الخصم لهذا النوع من الهجمات المتعمدة الذي يؤدي إلى تلف البيانات أو يحظر الوصول إليها ليُطيل التوغل في الأنظمة وليخفي السبب وراء تلفها. لكن سواءً أكان تلف البيانات ناتجًا عن التعرض لهجوم أو وقوع خطأ عشوائي، يجب أن يكون الدعم اللوجيستي قويًا ومرنًا بشكلٍ كافٍ لاستيعاب تلف البيانات والاستمرار في تقديم القدر الكافي من الدعم للعمليات القتالية.

هدف هذا التقرير ونطاقه

يبحث هذا التقرير في سبل تحسين استمرارية العمليات اللوجيستية عند تعرض البيانات اللوجيستية للتلف. ويقصد بتلف البيانات تغيّر البيانات بشكل كافٍ ليؤثر سلبًا على سير العمليات. من الأمثلة على ذلك، تغيّر وجهة الشحن لقطع غيارٍ مهمة ووجود بيانات تقنية خاطئة حول إجراءات إصلاح الطائرات وتشخيص خاطئ من أحد أدوات الفحص الآلية ووصول أمر خاطئ بإعادة توزيع بعض قطع الغيار وغيرها الكثير. لن نتطرق في هذا التقرير إلى تصنيف هذه الهجمات الإلكترونية حسب خطورتها على العمليات اللوجيستية.

[7] في أغلب الأحيان، يُستخدم مصطلح البيانات لوصف الأعداد والرموز الأولية في قواعد البيانات، وتُستخدم المعلومات لوصف المعنى المستخرج من البيانات لاتخاذ القرارات. لأغراض التبسيط، يستخدم هذا التقرير مصطلح "البيانات" بمعناها العام الذي يتضمن المعلومات أيضًا.

تمثل وحدة الأمن الإلكتروني خط الدفاع الأول ضد هذه التهديدات. لكن في حال فشل التدابير الأمنية في التصدي لهذه التهديدات، تتولى وحدة اللوجيستيات مسؤولية العمل للتعافي من الهجمة دون وقوع أي أثر سلبي على العمليات القتالية. وقد اقتصر نطاق هذه الدراسة على الإجراءات التي يمكن أن تقوم بها *وحدة الخدمات اللوجيستية* (وليس وحدة الفضاء الإلكتروني) لجعل العمليات مرنة. يتمثل العائق الأخير في تجنب الحلول المكلفة ماديًا والتي تستغرق سنوات من التنفيذ. ولذلك، اقتصر النقاش والحلول المحتملة على حلول اقتصادية سهلة التنفيذ نسبيًا وضمن نطاق وحدة الخدمات اللوجيستية.

قبل تحديد النهج الذي سنتبعه لحل مشكلة تلف البيانات، سنذكر بعض الافتراضات بشكل واضح. من البديهي أن تكون *جميع* البيانات عرضةً للتلف *وجميع* أنظمة البيانات عرضة للهجمات. وتمتد هذه الفرضية إلى ما هو أبعد من الأنظمة التجارية وشبكات تكنولوجيا المعلومات لتشمل الأنشطة التي تدعم منظومة أنظمة الأسلحة ومنظومة الأسلحة نفسها. توجد العديد من أنظمة تكنولوجيا المعلومات التي تدعم الخدمات اللوجيستية ضمن شبكات غير آمنة نسبيًا، وتتبادل البيانات مع العديد من الجهات التجارية التي لا تخضع قدرتها الأمنية للقوات الجوية الأمريكية. ولكن حتى الأنظمة غير المتصلة بشكل نسبي بالشبكات الخارجية تتبادل البيانات مع جهات خارجية، وهي أيضًا عرضة للهجوم.

إنّ جميع هذه الأنظمة موجودة ضمن شبكات غير آمنة نسبيًا، لذا لا نقوم بأي محاولة لتقييم مدى ضعفها في التصدي للهجمات الإلكترونية. لكن من أجل تطوير العمليات اللوجيستية القوية والمرنة، يجب اعتبار جميع الأنظمة في خطر. وبما أنه لا توجد قاعدة آمنة تمامًا من الهجمات الحركية، كذلك لا يوجد نظام آمن تمامًا من الهجمات الإلكترونية. لن نتعمق في هذه النقطة لأن التجربة أثبتت أن أكثر الأنظمة أمانًا قابلة للاختراق. أثناء إعداد هذه الدراسة، صادفنا العديد من الأفراد داخل المؤسسة اللوجيستية للقوات الجوية يعتقدون أن أنظمة البيانات التي يستخدمونها منيعة ضد أي هجوم. لكن هذه الثقة المفرطة تشكل حاجزًا أمام تحسين قوة ومرونة جميع العمليات، وستتم مناقشة هذه النقطة في فصول لاحقة.

كما نفترض أن الهدف الأساسي من هذه الدراسة هو ضمان إنجاز مهمة العمليات القتالية (مثل جيل الطليعة). إن استمرار العمليات اللوجيستية أمرٌ في غاية الأهمية إلى درجة التأثير في العمليات القتالية. أما الافتراض الأخير فهو أن عدد المجالات الوظيفية والأنظمة البيانية المعرضة للتلف أكبر من أن يتم التعامل معها بشكل فوري. كما أنّ محدودية الموارد تعني الحاجة لتحديد الأولويات لتحقيق التوازن مع العوامل التي تؤثر على القوة والمرونة، وسنتحدث عن هذا الموضوع في الفصل الخامس.[8]

[8] انظر Snyder et al., 2015

المنهجية

السياق

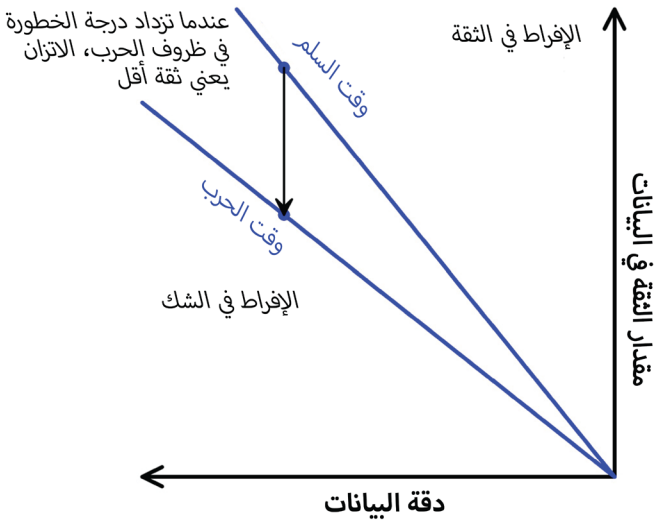
إنّ البيانات وأنظمة الحاسوب التي تقدم وعيًا بالظروف المحتملة وتتحكم في العمليات تعمل أيضًا على تعزيز القدرات اللوجيستية. وقد تطورت العديد من العمليات الضخمة والمعقدة وأصبحت تعتمد على البيانات ولم يعد بإمكان الأفراد السيطرة عليها بالفاعلية نفسها. فإما أن يثق المسؤولون عن العمليات في البيانات أو في معرفتهم وقدراتهم المحدودة وهم بذلك يخاطرون باحتمال ارتكاب الأخطاء. لكن قد تحتوي البيانات والمعلومات على الأخطاء، كما قد تحتوي الخوارزميات التي تقدم وعيًا بالظروف وتتحكم بالعمليات على أخطاء وقد تفشل في بعض الأحيان. وبالتالي يجب أن تتناسب ثقة المسؤولين عن العمليات بالتكنولوجيا مع مقدار دقة البيانات ومصداقيتها.

يصور الشكل 1.1 التوازن المثالي بين الثقة والشك في البيانات. يمثل المحور **س** مدى دقة البيانات (في الواقع) والمحور **ص** مدى ثقة العاملين في البيانات (موقف العاملين). تشير الخطوط الزرقاء إلى أن مستوى الثقة الموزون في البيانات يتناسب مع دقتها؛ مستوى ثقة منخفض في البيانات منخفضة الدقة، ومستوى ثقة عالٍ في البيانات الدقيقة. يشير أحد الخطين إلى مستوى الثقة الموزون في وقت السلم والآخر في وقت الحرب، وذلك حين يزيد احتمال حدوث تلفٍ للبيانات. الجزء العلوي الأيسر من الشكل يمثل العاملين الذين يفرطون في ثقتهم في البيانات، وهؤلاء معرضون لارتكاب الأخطاء نتيجة اتباع البيانات التي تحتوي على الأخطاء دون تفكير. من الأمثلة على النوع الأول من الأخطاء، هو البدء بسلسلة من مناورات الطيران الخطيرة لأن الطيار وثق بشكل خاطئ بمؤشر سرعة طيارة معطل وتوصل إلى استنتاج خاطئ بأن طائرته بدأت بالهبوط لكنها في الواقع تطير بشكل طبيعي.[9] أما الجزء السفلي الأيمن من الرسم فيمثل العاملين الذين يفرطون في الشك في صحة البيانات. وهؤلاء العمال هم عرضة لارتكاب الأخطاء بسبب الاعتماد على أحكامهم الشخصية ومهاراتهم المحدودة للحصول على بيانات أكثر دقة، مما قد يؤدي إلى بطء العمليات. ومن الأمثلة على ذلك، اصطدام طائرتين بسبب اعتماد طيار إحدى الطائرتين على حكم بشري خاطئ بدلاً من الاعتماد على نظام التشغيل الآلي الذي يتجنب الاصطدامات.[10]

[9] Croft, 2016.

[10] Bennett, 2004.

الشكل .1.1 رسم بياني يوضح التوازن بين مقدار الثقة والشك



ملاحظة: هذا المنظور مستوحى من لي (Lee) وسي (See)، 2004، ص 55، الشكل 2.

لأن درجة الثقة اللازمة للحصول على استجابة موزونة تعتمد على دقة البيانات، فإنّها تختلف باختلاف النظام وتختلف أيضًا لنظام واحد باختلاف الوقت. ومن المتوقع أن تزداد التهديدات التي تؤثر على سلامة البيانات لنظامٍ معين في أوقات الحروب (أو الأوضاع التي تؤدي للحروب) مقارنة بأوقات السلم. ومع ازدياد خطر التعرض للهجمات خلال الأوضاع التي تؤدي إلى وقوع الحرب، على العاملين أن يعيدوا النظر في ثقتهم لتتناسب مع احتمال وجود بيانات تالفة. وإنّ قيام العاملين بإعادة النظر في ثقتهم بالبيانات قد يضعهم في خانة "العاملين المفرطين بالشك"، في الشكل 1.1، لدى ترقبهم لمصادفة بيانات تالفة عند الانتقال لحالة الحرب. ويؤدي ذلك إلى ظهور الحاجة لتوخي الحذر لتجنب الأخطاء الذاتية التي يسببها الشك المفرط في البيانات.

ليتمكن العاملون من وضع الثقة المناسبة في البيانات التي بين أيديهم، عليهم فهم محوري الرسم البياني في الشكل 1.1. كما عليهم فهم البيانات التي يتعاملون معها حتى يتمكنوا من تقييم درجة دقتها، بالإضافة إلى الوعي بحدود المعرفة التي يمتلكونها.[11] لفهم مدى دقة البيانات، عليهم أولاً أن يُسلّموا بحقيقة احتمال تلف البيانات بقدر يتخطى الأخطاء الروتينية التي تقع بشكل يومي والتي يتعاملون معها في أغلب الأحيان. كما عليهم فهم أنّ البيانات *قد* تكون معرضة للهجوم، وأنّ إنكار احتمال وجود أخطاء في البيانات يعرضهم للانجراف نحو حالة "الإفراط في الثقة" في الشكل 1.1.، التي لن يتمكنوا فيها من اكتشاف الأخطاء الكبيرة عند وقوعها وقبل وقوع أثرها السلبي.

لكن يجب أن يكون العاملون على اطلاعٍ بالإجراءات الواجب اتباعها عند تقييم البيانات. عليهم فهم المعلومات وحدود الخبرة التي يملكونها. فإذا بالغوا في تقدير ما يعرفون، سيقعون ضمن فئة "العاملين الذين يفرطون بالشك" كما هو موضح في الشكل 1.1، وبالتالي سيتعرضون إلى ارتكاب الأخطاء أو المبالغة في الإبلاغ عن البيانات التي يشتبه في تلفها. أما في حال قللوا من شأن معرفتهم، فإنهم يقعون ضمن فئة "الذين يفرطون في الثقة" من خلال عدم الإبلاغ عن البيانات التي يشتبه في تلفها.

[11] انظر Lee and Moray, 1992

في الفصل الثالث، سنناقش بتفصيل أكبر الطرق التي تمكن العاملين من وضع الثقة المناسبة في البيانات.

إطار العمل

تتطلب الاستجابة الفعالة لأي اضطراب في سير العمليات وجود ملاحظات دقيقة وإيصالها للأشخاص المخولين بأخذ الإجراءات اللازمة وأخذ القرارات لإجراء التعديل اللازم على سير العمليات. في عام 2015، وفي جزء من مباردة تُدعى قدرة الخدمات اللوجيستية على الاستمرار والعمل وتُعرف باسم (LogATSO)، قدمت قيادة العمليات اللوجيستية للقوات الجوية ثلاث خطوات للاستجابة وهي: (1) اكتشاف أي خطأ محتمل؛ (2) تقييم الأخطاء لمعرفة ما إذا كانت خطأً حقيقيًا، ومن ثم تحديد ما إذا كانت نتيجة خطأ غير مقصود أم هجمة متعمدة؛ ومن ثم (3) العمل على التخفيف من المشاكل التي تؤثر على العمليات اللوجيستية والتي نتجت عن وقوع الأخطاء الحقيقية. تشكل هذه الخطوات الملاحظات ومراحل اتخاذ القرار للاستجابة الديناميكية، وسنتخذها إطارًا للعمل.

يعد هذا التقرير تجسيدًا لإطار عمل حملة قدرة الخدمات اللوجيستية على الاستمرار والعمل (LogATSO) للاستجابة لتلف البيانات. من أهداف هذا العمل ما يلي: (1) زيادة قوة العمليات القتالية من خلال زيادة قوة العمليات اللوجيستية للتصدي لتلف البيانات، (2) تحسين مستوى الأمن الإلكتروني الشامل للقوات الجوية الأمريكية من خلال تقليل أثر الهجمات على الخدمات اللوجيستية، (3) ردع الخصوم من الشروع في شن أي هجمات، وذلك بوجود آلية استجابة فعّالة وإظهارها لهم. يركز هذا التقرير على الهيكل العام للكيفية التي تمكّن القوات الجوية من الحفاظ على قوة العمليات اللوجيستية ومرونتها لمواجهة تلف البيانات. حيث يجب أن تقوم القوات الجوية بتحديد أولوياتها في هذا المجال وأفضل طريقة للكشف عن البيانات الشاذة وطريقة التقييم التي ستتبعها لوضع آلية مناسبة لتخفيف من الأضرار على مستوى المؤسسة. بالرغم من أن تحديد تدابير التخفيف المحتملة ليس موضوع هذا التقرير، سنقدم بعض التدابير التي ظهرت أثناء إجراء هذا التقرير حول اكتشاف تلف البيانات وتقييمه.

في الفصول الثلاثة القادمة، سنناقش بالتفصيل عمليات الاكتشاف والتبليغ والتقييم. في الفصل الخامس سنبحث في توجيه الجهود ضمن بيئة محدودة الموارد حيث تشكل البيانات موضع قلق. ولذلك، علينا تحديد المسائل التي سنوجه جهودنا نحوها أولًا والمواضع التي يُمكن المخاطرة بها. وسنخوض في مسألة تحديد الأولويات في الفصل السادس من خلال نقاش موجز وعميق حول التهديدات الإلكترونية وكيفية تحسين مستوى قوة العمليات اللوجيستية ومرونتها.

2. التحديات التي تواجه عملية الاكتشاف

تُعد عملية اكتشاف الخطأ الخطوة الأولى الضرورية التي تسبق أي إجراء من شأنه التخفيف من أثر الخطأ. ومن أجل تحسين عملية اكتشاف البيانات الشاذة، علينا أن نفهم المنعطفات التي يجب أن يتم الاكتشاف عندها لتجنب وقوع العواقب السلبية، كما يجب فهم الإجراءات التي يجب اتخاذها لنجاح عملية الاكتشاف. في هذا الفصل، سنقوم بتحليل هذه المواضيع والتوصل للائحة من المجالات الأساسية التي من شأنها أن تحسن عملية اكتشاف تلف البيانات. في الفصل الثالث، سنقدم توصيات لتحسين عملية الاكتشاف في هذه المجالات الأساسية.

سرعة الاكتشاف

قبل تنفيذ أي تقييم أو إجراء تصحيحي للاستجابة للبيانات التالفة، يجب اكتشاف البيانات الشاذة. ويمكننا القول أنّه إن كان تلف البيانات سيؤثر سلبًا في العمليات فسيتم اكتشافه في النهاية. من الملاحظات الرئيسية المذكورة في الفصل الأخير، إن لم يتم اكتشاف تلف البيانات إلا بعد توقف العمليات، مثل جيل الطليعة، حينها يكون الأوان قد فات. لذلك من المهم أن يتم اكتشاف وجود تلف البيانات الذي قد يؤثر سلبًا في العمليات القتالية في وقتٍ مبكر للاستجابة له قبل أن يؤثر على العمليات القتالية.

ثمة طريقتان تمثلان فرصًا لزيادة سرعة الاكتشاف، هما: (1) زيادة قدرة الأفراد على الاكتشاف بشكل أسرع من خلال تعزيز قدراتهم على الانتباه، و (2) الاكتشاف المبكر عن تلف البيانات ضمن سلسلة التتبع للبيانات، مثل اكتشاف وجود شذوذ في البيانات التقنية من خلال مكتب البرنامج قبل أن يتمكن المشرف من رؤيتها واكتشافها. كلما كان اكتشاف الحالات الشاذة أسرع ضمن سلسلة التتبع، قلّت الحاجة إلى الاعتماد على الأفراد في عملية الاكتشاف.

عناصر عملية الاكتشاف

لتحليل عملية الاكتشاف، علينا أن نقوم أولاً بتعريف ماهية *الاكتشاف*، ما هي الأحداث التي يجب أن تقع حتى تحدث عملية الاكتشاف. يجب تلبية عدد من الشروط لاكتشاف البيانات الخاطئة، أولاً، يجب أن يتوفر شخص أو شيء ليلعب دور (*العميل*) ويكون مطلعًا على البيانات الخاطئة. ثانيًا، يجب أن يكون الخطأ أمرًا شاذًا، أي أنه يختلف عن النمط الأساسي المتوقع. ثالثًا، يجب أن يمتلك العميل قدرًا كافيًا من الخبرة ليتمكن من التمييز بين ما هو شاذ والنمط الأساسي المتوقع. رابعاً، إذا تولى الأفراد مهمة الاكتشاف (الاستشعار)، فيجب أن يكون لديهم دافع للكشف والإبلاغ عن بيانات الحالات الشاذة، أو على الأقل، يجب ألا يكون لديهم أي دافع لإخفاء الحالات الشاذة وعدم الإبلاغ عنها. سنناقش هذه الحالات في القسم التالي.

قدرة العميل على الاطلاع على البيانات

إذا لم يتمكن العميل من رؤية البيانات الشاذة، فلن يتم اكتشافها. قد يتمثل الاطلاع على البيانات في قدرة العميل على رؤيتها خلال الأنشطة العادية (الاكتشاف التفاعلي) أو من خلال تحري العميل عن البيانات الشاذة (الاكتشاف الاستباقي). يمكن أن يكون العملاء من الأفراد (الطيارين والمدنيين والمتعاقدين) أو أجهزة الحاسوب (الخوارزميات). نحرص على بقاء عمل الأفراد الذين يقومون بدور المكتشف ضمن نطاق الأسئلة التي يجيب عنها هذا التقرير، كما هو مطلوب. في الفصل التالي، سنناقش طريقة واحدة يمكن للخوارزميات أن تساعد فيها في عملية الاكتشاف، لكن فقط في السياق الذي يشمل توفر الأدوات لتعزيز مهارات الاكتشاف لدى الأفراد.

يتفاوت اطلاع الأفراد على البيانات بطرق مهمة ضمن هذا السياق. في بعض الحالات، يتمكن الأفراد من رؤية البيانات بشكل منتظم. وفي معظم الحالات، يكون الهدف من البيانات هو توجيه أفعال الأفراد. من الأمثلة على ذلك، استخدام البيانات التقنية لإرشاد عمال الصيانة عند إجراء صيانة للطائرات. بالنسبة لعمال الصيانة الخبراء الذين يتبعون البيانات التقنية التي طبقوها آلاف المرات في الماضي، من المنطقي أن نتوقع اكتشاف بعض الحالات الشاذة. إذا اعتاد عامل الصيانة على ضبط عزم الدوران عند درجة معينة، يجب أن يكون لدى العمال الجدد الخبرة الكافية لاكتشاف أي حالة شاذة، وإذا ما كان هناك تغير مفاجئ وغير ظاهر بمقدار الضعف في العزم. لكن قد لا يتمكن شخص مبتدئ يقوم بهذه المهمة لأول مرة من اكتشاف ذلك، فقد لا يستطيع شخصٌ مبتدئ تمييز الأنماط الشاذة لأنه لا يعرف الأنماط الأساسية المتوقعة.

في حالات أخرى، قد يملك الفرد القدرة على الاطلاع على البيانات الشاذة دون أن يُتوقع منه أن يميزها، لأنه لا يملك المعرفة الكافية ضمن السياق أيًا كان مستوى خبرته. على سبيل المثال، إذا كان هناك قطعة لطائرة من نوع مستخدم حاليًا وضمن قاعدة بيانات التوريد ووُجد أنّ هناك (خطأ) في هذه القطعة ويجب نزعها، لا يمكننا أن نتوقع من العمال الذين ينفذون هذه المهمة أن يعرفوا أنّ عليهم تخزين هذه القطعة وليس نزعها. هذا المستوى من المعرفة يوجد ضمن المستويات العليا في المنظمة، ويمكن توقع اكتشاف هذا النوع من الأخطاء عندما تصبح المعرفة متاحة. في بعض الحالات، تكون المعرفة المطلوبة لاكتشاف خطأ ما خارج القوات الجوية (مثل قاعدة الصناعة الدفاعية).

إنّ الحالات التي يكون فيها مستوى المعرفة للعاملين أقل من القدر الذي يُتوقع عنده تحديد الحالات الشاذة هي في ازدياد ولا يُتوقع أن تقل في المستقبل. والأنظمة، مثل F-35A، هي معقدة للغاية والعاملون في التوريد والصيانة يعتمدون على تكنولوجيا المعلومات لتشخيص العمليات الموكلة إليهم وإدارتها وتنفيذها. هذا الاعتماد هو نتيجة طبيعية لتعقيد الأنظمة وقدرة تكنولوجيا المعلومات الحديثة. رافق هذه التغييرات انحدارٌ في قدرات الأفراد والخبرات المباشرة في التعامل مع البيانات. حيث يعتمد الميكانيكي في العصر الحديث على أجهزة الحاسوب للكشف عن الأعطال ولا يعتمد على الخبرة وحدها، كالاستماع لصوت المحرك أو على اللمس. وبسبب هذا الاعتماد، تراجع مستوى مهارات القوى العاملة التي تمكنهم من تشخيص الأعطال دون الاعتماد على الحاسوب. هذه الظاهرة التي تبعت التطور التكنولوجي أثرت أيضًا على العمليات اللوجيستية.

في حالات أخرى، لا يمكن للأفراد رؤية البيانات خلال العمليات الطبيعية. وعدم تعرض الأفراد لأي نوع من الأخطاء يعني أنهم لن يتمكنوا من تمييزها. وإنّ جزءًا كبيرًا من العمليات ضمن سلسلة التوريد آلية، لدرجة أن العديد من المعاملات لا تخضع لرقابة الأفراد.

لامتلاك عمليات لوجيستية قوية ومرنة يمكنها مواجهة تلف البيانات، يُعد وجود آلية اكتشاف فعالة أمرٌ ضروريٌ لكل حالة من هذه الحالات الثلاث. أكثر هذه الحالات تحديًا التي يتعرض لها العميل هي تلك التي لا يطلع فيها الأفراد على البيانات خلال العمليات العادية. سنناقش الحالة التي يتمكن فيها الأفراد الذين لا يملكون الخبرة من رؤية البيانات لاحقًا في هذا الفصل تحت عنوان الخبرة. أما الحالة التي يرى فيها العاملون الخبراء البيانات فيشكل الدافع فيها تحديًا وسنناقشه لاحقًا ضمن هذا الجزء.

الحالات الشاذة للبيانات

إن لم يكن تلف البيانات مختلفًا بشكل ملحوظ عن النمط الأساسي، أي إن لم تكن شاذة، لن يتمكن الأفراد من تمييزها. في هذا السياق، ثمة ثلاثة عوامل يمكنها إخفاء البيانات الشاذة وزيادة صعوبة اكتشافها.

أولًا، تكون بعض مجموعات البيانات على درجة عالية من الاختلاف، لذلك يتطلب اكتشاف البيانات الشاذة فيها وجود انحراف كبير جدًا في البيانات عن النمط الأساسي المتوقع. أي أنّ هناك قدرًا كبيرًا من الفوضى في البيانات في وضعها الطبيعي حيث تصعب ملاحظة وجود أي شيء مختلف. ربما تُعد سلسلة التوريد أوضح مثال على التنوع الكبير للبيانات. العديد من القطع يكون الطلب عليها عرضيًا، وتختلف الوجهات التي تُشحن إليها بالإضافة إلى ضخامة عمليات سلسلة التوريد. لذلك، ينطوي النمط الأساسي للعمليات العادية على الكثير من التقلبات، ويكون حجم البيانات الذي يُعتمد عليه لتحديد الحالات الشاذة مهولاً. هذه الخصائص تخفي الحالات الشاذة، وقد يستغل الخصوم هذه الخصائص لإخفاء الهجمات التي تسبب تلف البيانات.

هناك جانب إيجابي لهذه الخصائص، فبسبب اختلاف أنماط البيانات بدرجة عالية تطورت عمليات سلسلة التوريد لتزداد قوة في التصدي للأخطاء على مستوى معين. تقع الأخطاء الصغيرة بشكل يومي في عمليات سلسلة التوريد. وبالتالي قد يصعب تحديد البيانات الشاذة الصغيرة، لكن أثرها على العمليات القتالية بسيط. يمكن لعمليات سلسلة التوريد العادية أن تستوعب الأخطاء الصغيرة دون أن يكون لها أي أثر كبير على العمليات.

لكن قد تترك بعض الأخطاء الصغيرة أثرًا بالغًا وتؤدي إلى ظهور عاملٍ ثانٍ: البيانات التي أصيبت بالتلف نتيجة التعرض لهجوم إلكتروني من قبل أحد الخصوم تمثل نمطًا شاذًا مختلفًا عن الأخطاء التي اعتاد العاملون على رؤيتها. يتم تصميم الهجمات المستهدفة لتترك أكبر أثر سلبي ممكن على العمليات وذلك بأصغر التغييرات. في أغلب الأحيان، يختلف نمط الهجمات المتعمدة عن نمط الأخطاء اليومية العادية في نظام البيانات، والتي تملك طابعًا عشوائيًا في أغلب الأحيان. كما يستحيل تقريبًا التنبؤ بنمط تلف البيانات نتيجة التعرض لهجوم ما وذلك بسبب الكم الهائل من البيانات المعرضة للتلف. على الأغلب، ستختلف البيانات الشاذة عن البيانات المعروفة من خبرات سابقة أو عمليات التحليل. من الجدير بالذكر أن النمط الأساسي يختلف خلال الحروب مما يزيد من صعوبة عملية الاكتشاف.

ينشأ العامل الثالث الذي يساعد في إخفاء الأخطاء بسبب أنّ النمط الأساسي للبيانات الذي يعرفه العاملون لتمييز البيانات الشاذة ناتجٌ عن الأنشطة الروتينية للعمليات الثابتة والمستقرة (كالعمليات التي تحدث وقت السلم). هذا النمط الأساسي يختلف للعمليات ذات التواتر السريع (كالعمليات في وقت الذروة أو أنشطة النشر أو قمة جيل الطليعة). ويعد سيناريو الحرب هو الأكثر خطورة، فقد تكون الهجمات مزعجة في وقت السلم إلا أنها غالبًا لا تترك أثرًا

خطيرًا على العمليات القتالية. في الحقيقة، إن كان للهجمات وقت السلم أثرٌ بالغ على العمليات القتالية، فقد يؤدي ذلك إلى الانتقال لوضع حالة الحرب. لذلك يكون التركيز على الهجمات الإلكترونية ومقدماتها أكبر في وقت الحرب من أي وقت آخر.

على سبيل المثال، إرسال قطع غيار مهمة لطائرة F-22 لقاعدة لا تملك هذا النوع من الطائرات قد يلفت الانتباه في وقت السلم. أما خلال نشر قوات التدخل السريع، قد لا يتم الاعتراض على هذه الشحنة، فقد يفترض العاملون أنه سيتم توريد F-22 لهذا الموقع ولكن لم يتم إعلامهم بذلك. تختلف الأنشطة التي تتم خلال عملية نشر قوات التدخل السريع بطبيعتها عن تلك التي اختبرها العاملون من قبل، وإن كانوا من الجنود القدامى في عمليات التدخل السريع السابقة.

تعمل هذه العوامل الثلاثة على إخفاء البيانات التالفة من خلال إخفاء خصائصها الشاذة وتشكل جميعها تحديًا لعملية الاكتشاف. ولأن فترات الحرب المختلفة تشهد أكبر قدر من القلق من الهجمات الإلكترونية، يتمثل التحدي الأخطر بالعامل الثالث الذي يقوم بإخفاء البيانات الشاذة، وهو اكتشاف الحالات الشاذة في حالة الحرب عند امتلاك خبرة بالنمط الأساسي في وقت السلم. أي أنّ أكثر المشكلات تحديًا وصعوبة في الحاجة للكشف عن السلوكيات الشاذة هو تحديد ما يشكل السلوك الشاذ خلال أكثر الأوقات خطورة - العمليات الحربية- حيث يشكل النمط الأساسي بحد ذاته شذوذًا.

خبرة القوى العاملة

حتى عند تعرض القوى البشرية لبيانات شاذة، فإنهم بحاجة لقدرٍ كافٍ من الخبرة لفهم المدى المتوقع من البيانات، وفي حال ملاحظة سلوك خارجٍ عن المألوف للبيانات معرفة هل هو كافٍ للتأثير بشكل سلبي على العمليات. على العاملين أن يمتلكوا المهارات اللازمة لإدراك وجود الحالات الشاذة والحكم بما إذا كان هناك حاجة للتبليغ عنها لمستوى أعلى (مشرف أو مركز الاتصالات إلخ). كما تحدثنا سابقًا، كلما كان شذوذ البيانات التالفة أقل وضوحًا، تطلب اكتشافها خبرة أكبر. تُكتسب الخبرة من خلال التدريب والتعليم والتجربة، لكن يمكن للخبرة أن تكون فاعلة عندما يواظب العاملون على مراقبة البيانات ودراسة الأنماط العادية و ربط العواقب الحقيقية بالبيانات الخاطئة المقابلة. على العاملين أن يحافظوا على *تركيزهم*، أي عليهم تفحص العمليات الجارية، والعمل على تحسين فهمهم للعمليات بشكل مستمر، وأن يكونوا على استعدادٍ دائم لما يتحدى توقعاتهم.[12] يكمن التحدي الذي يقف أمام الخبرة في امتلاك ثقافة اليقظة وتطويرها والمحافظة عليها، بحيث تسود بيئة العمل، وذلك بدءًا من التدريب وحتى المدرسة الفنية وفي العمل. كما يجب أن يمتد هذا المبدأ ليشمل الطيارين والمدنيين والمتعاقدين.

[12] انظر Weick and Sutcliffe، 2001، ص42

وجود دافع للتبليغ

العاملون الذين يملكون الخبرة الكافية للكشف عن تلف البيانات، ويتعرضون للبيانات التالفة التي تصنف ضمن الحالات الشاذة يواجهون تحديًا آخر: وهو الحاجة لوجود ما يدفعهم للتبليغ عن تلف البيانات، أو على الأقل، يجب ألا يكون هناك ما يردعهم عن ذلك. بعض الأفراد لا يميلون في بطبيعتهم لمخالفة الدوافع المرغوبة للتبليغ عن البيانات الشاذة. يعتقد بعض العاملين أن التبليغ عن وجود بيانات شاذة هو إشارة لاحتمال وجود مشاكل في العمليات التي يقومون بها. وقد لا يرغبون بالكشف عنها للمشرفين عليهم حتى يبدو كل شيء تحت السيطرة. قد يؤدي هذا الاعتقاد إلى تأخر التبليغ عن البيانات الشاذة المكتشفة وبالتالي إلى تفاقم المشكلة وتحولها إلى أزمة تفوق قدرة العامل على السيطرة، حينها يكون الأوان قد فات للتخفيف من أثر الهجمة. في هذه الحالة، يتحول الخطأ الصغير إلى حادث. قد توجد هذه الظاهرة على مستوى الوحدات التنظيمية، فقد ترغب الوحدة في الاحتفاظ بمشاكلها وحلها ضمن الوحدة وتتردد في الإبلاغ عن المشاكل التي تواجهها لهذا السبب نفسه.

من المؤكد أنّ هذا التوجه يزداد انتشارًا في الأوقات الحرجة، مثل العمليات التي تتم في أوقات الحرب. خلال الحرب، يحتاج القادة ويتوقعون من العاملين أن يؤدوا أعمالهم دون الشكوى من المشاكل التي يواجهونها. في هذه الأوقات، يقع القادة تحت الضغط الذي يفرضونه على أنفسهم، والعاملون تحت إشرافهم يدركون ذلك وقد يخشون أن يتلقى القادة خبر الشك في تلف البيانات بشكل سيء. ما هو الوقت المناسب للتبليغ؟ هل سيغضب القادة في حال تم التبليغ عن وجود حالات شاذة ليتضح لاحقًا أنها ليست كذلك؟ هل سيبدو العامل وكأنه يؤخر سير العمليات بكثرة التشكيك بدلاً من أن ينجز عمله؟ كيف يمكن للعاملين أن يشعروا بحرية التساؤل حول البيانات والمعلومات التي أعطيت إليهم؟

تشكل هذه الظاهرة مشكلة وبالأخص بالنسبة لهجمة منسقة ضد نظامٍ للسلاح. لنفترض أن إحدى منظومات الأسلحة تعرضت لهجوم من خلال إفساد بيانات صيانة نظام الأسلحة ونظام التوريد ونظام نقل القطع التي تم توريدها وقاعدة دعم العمليات حيث يقع نظام الأسلحة. قد تبدو كل واحدة من هذه الهجمات صغيرة بالنسبة للمجالات الفاعلة، وقد لا تصنف ضمن الهجمات، بل مجرد مشكلة شاذة. من أجل تشكيل وجهة نظر على مستوى المؤسسة والبحث في الوضع وتقييمه وتصنيفه على أنه هجوم منسق، يجب أن يتم تحفيز العاملين في جميع هذه المجالات للتبليغ عن ملاحظاتهم، ليتمكن شخصٌ ذو نظرةٍ أوسع من تقييم الوضع.

مع ازدياد الأنظمة تعقيدًا وازدياد حجم البيانات وازدياد المهام التي أصبحت تُنجَز آليًا، يتم تدريب العمال على زيادة ثقتهم في البيانات. لكن المهمة المطلوبة هنا هي عرض البيانات بمستوى معين من الشك. هذا التضارب حول مسألة الثقة واحتمال انعدام الثقة في البيانات يؤدي إلى حالة من التوتر يجب التغلب عليها من خلال وضع قدر أكبر من الثقة المتبادلة بين العاملين وقادتهم.

يحتاج العمال أيضًا إلى قنوات رسمية معروفة على نطاق واسع للإبلاغ عن البيانات. تُعد هذه القنوات للتبليغ جزءًا مهمًا من عملية التقييم. هذه الحاجة إلى دمج قنوات التبليغ مع آليات التقييم، ستكون السبب في نقاشنا حول قنوات التبليغ في الفصلين الثالث والرابع.

يتطلب حل مشكلة الدافع تغيير الثقافة السائدة، فمن أجل تعزيز عملية الاكتشاف والتبليغ لا بد من ترسيخ ثقافة الثقة، ليؤمن الطيارون والمدنيون والمتعاقدون بأن أفعالهم تعود بالنفع على سير المهام وأنه لن يتم فرض أي عقاب عند القيام بالتبليغ.

ملخص التحديات التي تواجه عملية الاكتشاف

هناك خمسة مجالات رئيسية أظهرت القدرة على تعزيز عملية اكتشاف تلف البيانات:

- يجب أن تتم عملية الاكتشاف بسرعة كافية. يمكن تحقيق هذه السرعة من خلال الجمع بين عاملين هما، وجود أفراد يقومون بالاكتشاف عن تلف البيانات والتبليغ عنه بسرعة، بالإضافة إلى الاكتشاف المبكر لتلف البيانات ضمن سلسلة التتبع.
- تمثل العمليات الآلية البحتة – التي لا تُمكن الأفراد من رؤية البيانات خلال العمليات العادية -تحديًا كبيرًا أمام عملية الاكتشاف. يتطلب التشغيل الآلي آليةً خاصة للمساعدة في اكتشاف التلف.
- تزداد أهمية اكتشاف تلف البيانات في الحروب، لكن الحالات الشاذة تكون أقل وضوحًا خلال الحروب بالمقارنة مع أوقات السلم، فالحروب نفسها حالةٌ شاذة، وتكمن أهمية الآليات في ضبط آليات الاكتشاف من وقت السلم إلى وقت الحرب.
- كي يتمكن العاملون (طيارون، ومدنيون، ومتعاقدون) من اكتشاف وجود بيانات شاذة، عليهم أن يخضعوا جميعًا لتدريب حول فهم النمط الأساسي المتوقع، كما ينبغي أن يكونوا متيقظين عند تفحص البيانات.
- يجب أن تقوم القيادة بخلق بيئة تشجع العاملين على الإبلاغ عن البيانات الشاذة المشبوهة.

في الفصل التالي، سنقترح بعض الطرق التي تقلل ولو جزئيًا من هذه التحديات الحرجة وتشجع تغيير الثقافة المرتبطة بها لتسهيل اكتشاف الحالات الشاذة.

3. توصيات لتحسين عملية الاكتشاف

هناك الكثير من الإجراءات التي تعالج التحديات التي تواجه عملية اكتشاف تلف البيانات. تتراوح بين توصيات مفصلة نسبيًا للأفراد على مستوى العمل وسياسات وتوجيهات للقادة من أجل التغيير. سنناقش هذه التوصيات بشكلٍ موازٍ لنقاشنا للتحديات في الفصل السابق. سيتضح لاحقًا أن بعض توصياتنا الفردية تتطرق لمواجهة أكثر من تحدي ولو جزئيًا، وأن أفضل الطرق لمواجهة التحديات الفردية تكون من خلال إجراءات متعددة الاتجاهات.

تحسين السرعة

يمكن زيادة سرعة عملية الاكتشاف على مستويين: على مستوى الأفراد من خلال تغير سلوكيات العاملين، وعلى مستوى المؤسسة من خلال اكتشاف الأخطاء مبكرًا أثناء المعالجة وتمرير البيانات بدلاً من فعل ذلك قبل اتخاذ الإجراءات المبنية على البيانات مباشرة.

الإجراءات على مستوى الأفراد

تتوفر البيانات من أجل اتخاذ قراراتٍ مستنيرة، وتُتخذ القرارات من أجل تنفيذ الإجراءات. وبالتالي، فإن وجود خطأ في البيانات يشكل خطرًا لاتخاذ قرار سيء، مما يؤدي بدوره إلى اتخاذ إجراء يخالف أهداف العمليات. من المهم أن يكتشف الأفراد وجود أي بيانات شاذة بشكل كبير قبل اتخاذ أي إجراء. هناك ثلاثة عوامل لها دورٌ بارز في زيادة سرعة الأفراد على اكتشاف البيانات الشاذة.

أولاً، إذا كان متوقعًا من العامل أن يكتشف وجود البيانات الشاذة ويبلغ عنها في مرحلة مبكرة (أي قبل اتخاذ أي إجراء بالاستناد إلى هذه البيانات)، فيجب أن يطّلع العامل على هذه البيانات في وقت مبكرٍ أيضًا. أما إذا كان العامل يرى البيانات مباشرة قبل (أو أسواء من ذلك، فيراها بعد) اتخاذ الإجراءات، فعلى الأرجح أن يكون الأوان قد فات لتقييم وقوع الأثر السلبي على العمليات وتخفيفه وتجنبه. لكن اطّلاع العاملين على البيانات بصورة روتينية قبل أن يتمكنوا من رؤيتها خلال أنشطتهم العادية سيكون مرهقًا وقد يؤدي إلى إبطاء سير العمليات اللوجستية على نحو لا يطاق. مع ذلك، قد تفرض الظروف نفسها في بيئة عالية الخطورة (مثل الحروب) عند وجود مجال ذو أولوية عالية (والتي تم تحديدها ضمن العملية الموضحة في الفصل الخامس) سيكون من المفيد أن يقوم العاملون الذين تلقوا التعليمات بفحص بيانات هذا المجال في وقت مبكر عن المعتاد. وسنناقش هذه الفكرة لاحقًا في هذا الفصل عند مناقشة التأقلم مع وقت الحرب.

ثانيًا، يقوم القادة بتسهيل عمليات الاكتشاف والتبليغ السريعة من خلال التوقع من القوى العاملة القيام بالاكتشاف والتبليغ عن البيانات التي يشتبه بتلفها. يعد هذا تغيرًا في الثقافة يشبه التغير في ثقافة التبليغ عن مخاوف السلامة، وهو ما يعد ضروريًا لمواجهة العديد من التحديات التي تعوق عملية الاكتشاف، وسنناقشها بتفصيلٍ أكبر عند التحدث عن دوافع الاكتشاف لاحقًا في هذا الفصل.

أما العامل الثالث فهو تسهيل عملية التبليغ عن البيانات التي يشتبه بتلفها. الكثير من المؤلفات تؤكد أن من أكثر ما يساهم في دفع الأشخاص إلى القيام بأمر ما هو جعل القيام بذلك الأمر في غاية السهولة.[13] إلى جانب اطّلاع العاملين على البيانات بشكل أكبر، قد لا يكون هناك العديد من الطرق لجعل كشف البيانات الشاذة أسهل بشكل كبير بالنسبة للعاملين. لكن يمكن جعل عملية التبليغ عن البيانات المشبوهة أسهل بالنسبة لهم من خلال توفير آليات تبليغ سهلة ومعروفة بالنسبة لهم. سنتحدث عن آليات التبليغ في الفصل الرابع.

الإجراءات على مستوى المؤسسة

تنتقل العديد من البيانات من منظمة إلى أخرى قبل استخدامها في أخذ القرارات. مثل البيانات التقنية لعمليات الصيانة، قد تنشأ في مكتب أحد البرامج، ومن ثم تنتقل إلى القيادة الرئيسية، ثم إلى كادر العامل في الجناح أو المجموعة قبل أن تصل إلى عامل الصيانة الذي سيعتمد على البيانات لتنفيذ الإجراء المطلوب منه. يُسمى هذا التدفق للبيانات *بسلسلة التتبع*. وبوضوح، كلما تم اكتشاف الأخطاء في وقت مبكر ضمن سلسلة التتبع سيقل الوقت اللازم للاستجابة، وستزداد مرونة العلميات. الاستمرار بتحديد الأخطاء الموجودة في البيانات في وقت مبكر ضمن سلسلة التتبع يتطلب مشاركة المؤسسة بأكملها، بما في ذلك الطيارين والمدنيين والمتعاقدين. من الأفضل اكتشاف وجود خطأ في بيانات تقنية في مكتب برنامج من اكتشافها في خط للطيران، ومن الأفضل اكتشاف وجود خطأ في التزويد خلال الشحن من اكتشافه أثناء النقل. فعندما يترك الخطأ ليكتشفه آخر شخص في سلسلة التتبع، لن يحد ذلك فقط من الوقت المتاح للاستجابة للخطأ بل أغلب الظن أن ذلك الشخص لن يملك المعرفة المطلوبة لتمييز ما هو شاذ. لذلك، فإن جميع التوصيات الأخرى في هذا الفصل تنتفع من أكبر عدد ممكن من التطبيقات عبر المؤسسة لتصل للطيارين والمدنيين والمتعاقدين.

تجاوز عقبة العمليات الآلية

تمثل العمليات اللوجيستية الحديثة شراكة معقدة بين القوى البشرية والتكنولوجيا. في بعض الأحيان تقود التكنولوجيا هذه الشراكة. وتعد عمليات سلسلة التوريد أحد هذه المجالات. وبالأخص في الجزء الذي يقع تحت إدارة وكالة الدفاع اللوجستية، صممت سلسلة التوريد لتحتوي على العديد من العمليات التي تكاد تعد آلية بالكامل، مع وجود تدخل بسيط للقوى البشرية دون وجود أي دور للقوى البشرية في هذه العمليات. في هذه الحالات، تصدف فرصٌ ثمينة ونادرة يتمكن فيها العاملون من اكتشاف أخطاء البيانات قبل تنفيذ أي إجراء بالاستناد إليها. مؤخرًا، أصبحت هذه الحالات أكثر انتشارًا مع ازدياد تعقيد العمليات اللوجيستية والسعي للحصول على كفاءة أعلى. يتطلب التشغيل الآلي وسائل أخرى بالإضافة تختلف عن الإحساس البشري للكشف عن الأخطاء.

إن الفكرة التي سنتوصل إليها في هذا القسم هي شكلٌ آخر من أشكال اكتشاف البيانات من قبل الإنسان بمساعدة الأدوات-الطرق المتبعة لتحديد نوع محدد من تلف البيانات. هناك عدد مهول من الطرق لاكتشاف البيانات الشاذة. سيقتصر نقاشنا على التقنيات البسيطة ومنخفضة التكلفة في تنفيذها. جميع الطرق التي نتحدث عنها تستغل حقيقة وجود أنماط للبيانات المفيدة. حيث يصعب إنتاج هذه الأنماط عند تلف البيانات، مما يجعل تزييف البيانات أمرًا

[13] Thaler and Sunstein, 2008.

صعبًا بعض الشيء.[14]

قانون بينفورد (Benford)

تعتمد إحدى الطرق الأكثر استخدامًا للكشف عن التزوير على أحد أكثر الأنماط انتشارًا للبيانات ويعرف باسم قانون بينفورد (Benford).[15] الأرقام[16] الأولى ضمن مجموعات ضخمة للبيانات ليست موزعة بالقدر نفسه. فالرقم 1 يتردد بنسبة أكبر من الرقم 2، والرقم 2 يتردد بنسبة أكبر من 3، وهكذا، وبالتالي الرقم 9 يتردد بأقل نسبة كأول رقم من عدد ضخم. إذا قمنا بتسمية الرقم الأول من عدد ضخم بـ D، حيث d يمثل أي عدد بين(1،2،3...9). قانون بينفورد (Benford) للأرقام الأولى هو[17]

$$\text{احتمال } (D = d) = \text{لوغاريتم}_{10}\left(1 + \frac{1}{d}\right)$$

تخضع مجموعات البيانات التي تتبع هذا النمط في التوزيع هذا تخضع لقانون بينفورد (Benford). إذا اتبعت مجموعة من البيانات قانون بينفورد (Benford)، وفقًا لهذه المعادلة يوجد احتمال بنسبة 30 بالمئة أن يكون الرقم الأول ضمن أي قاعدة بيانات يساوي 1، و18 بالمئة أن يكون 2، وهكذا وبذلك يكون هناك احتمال بنسبة 4.5 بالمئة أن يكون الرقم الأول من عدد ضخم هو 9. عند تغير هذه الأرقام بطريقة احتيالية، تنحرف بيانات بينفورد (Benford) عن هذا النمط، ويستند إلى هذه الحقيقة للكشف عن تزييف البيانات.[18]

ثمة مجموعة كبيرة جدًا من أنواع البيانات تتبع قانون بينفورد (Benford). وتتنوع هذه البيانات لتشمل الثوابت الفيزيائية، ومعدلات الاضمحلال الإشعاعي، وملفات خدمة الإيرادات الداخلية، وبعض بيانات سوق الأوراق المالية، وغيرها الكثير.[19] متي يمكن توقع اتباع البيانات لقانون بينفورد (Benford)؟ لا يوجد جوابٌ واضح لهذا السؤال حتى الآن. لكن، يمكن إثبات ذلك رياضيًا، فأخذ أي توزيع للبيانات وضربه أو قسمته بشكلٍ متكرر على عدد عشوائي أو رفعه لأي أُس لعدد لا نهائي من المرات فالناتج سيكون تابعًا لقانون بينفورد (Benford). فإذا كان توزيع البيانات يخضع لقانون بينفورد (Benford) فإنه سيبقى كذلك بعد الضرب والقسمة وبعد رفعه لأي أس (النطاق وقاعدة الثبات).[20] في الحقيقة، فإن التوزيع الذي يشكل نطاقًا ثابتًا يكون خاضعًا لقانون بينفورد (Benford). هذا الثبات يعني إن كان هناك توزيع للبيانات يتبع لقانون بينفورد (Benford) عند التعبير عنه بمجموعة واحدة من الوحدات، سيبقى توزيع البيانات تابعًا لبينفورد (Benford) وإن تم التعبير عنه بأي وحدة.

وضع الباحثون بعض الخصائص التي تشير لكون مجموعة البيانات تتبع قانون بينفورد (Benford). بالرغم من أن وجود هذه الخصائص لا يضمن اتباع البيانات لقانون بينفورد (Benford):[21]

---

[14] انظر Hill, 1999

[15] قانون بينفورد (Benford) هو في الواقع نمط منتشر بشكل ملحوظ، وليس قانونًا.

[16] أول *رقم ذو دلالة* في أي عدد هو أول رقم ليس صفرًا عند قراءة العدد من اليسار إلى اليمين. على سبيل المثال، أول رقم دال في 218.81 هو 2، أما أول رقم ذو دلالة في 0,0375 فهو 3. الرقم الدال الأول لا يكون صفرًا أبدًا، أما الرقم الثاني أو ما بعده، فيمكن أن يكون صفرًا. مثلًا إنّ الرقم الدال الثاني في 0.102 هو 0.

[17] إذا افترضنا أنّ D_n هو عدد دال ترتيبه n من اليسار إلى اليمين. حينها يكون قانون بينفورد العام هو

$$\text{احتمال } (D_1 = d_1, D_2 = d_2, \dots, D_m = d_m) = \text{لوغاريتم}_{10}\left(1 + \left(\sum_{j=1}^{m} 10^{m-j} d_j\right)^{-1}\right)$$

[18] Durtschi, Hillison, and Pacini, 2004; Nigrini, 2012; Berger and Hill, 2015, Chapter 10.

[19] Berger and Hill, 2015, pp. 4–5.

[20] Boyle, 1994; Hill. 1995; Berger and Hill, 2015.

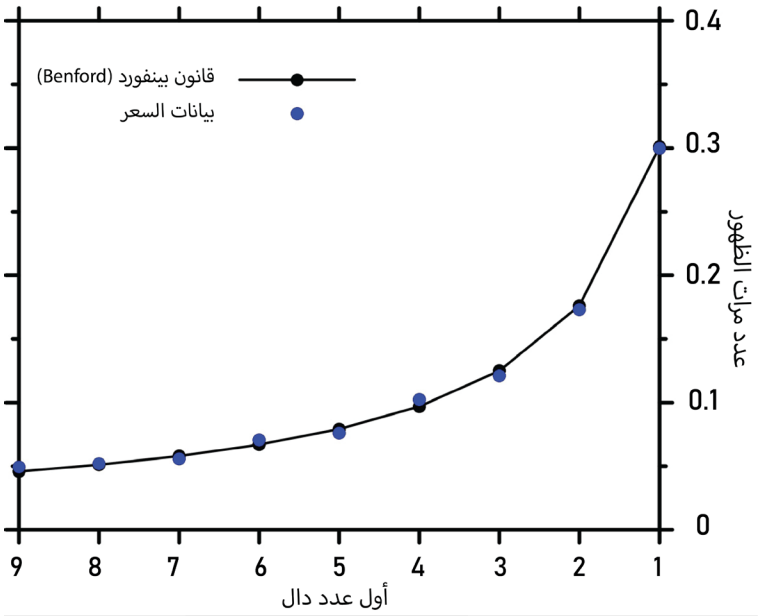
[21] انظر Durtschi, Hillison, and Pacini, 2004

- الأرقام الناتجة عن مجموعات رياضية لأرقام أخرى (مثل نواتج الأرقام المتعلقة بالمنتجات، كحاصل ضرب السعر بالكمية)
- البيانات على مستوى المعاملات (على خلاف البيانات المجمعة)
- مجموعة كبيرة من البيانات تمتد قيمها لدرجات متعددة
- البيانات التي يكون فيها المتوسط أكبر من الوسيط والانحراف يكون موجبًا (ذيل طويل باتجاه اليمين)
- نطاق الثبات.

من بين مجموعات البيانات التي يقل ترجيح توافقها مع قانون بينفورد (Benford) تلك التي تتكون من أرقام تسلسلية (مثل أرقام الهاتف)، والبيانات التي تتأثر بالعوامل النفسية (مثل الأسعار التي تحدد بـ19.99$)، والبيانات التي تحتوي على عدد كبير من الأرقام الخاصة بالشركة (الحسابات المحددة لتسجيل الأموال المستردّة لسعر ثابت، إلخ)، أو البيانات المحدودة بسقف أدنى وأعلى. أما البيانات الممثلة بنسب مئوية بدلاً من قيم أساسية فعلى الأغلب لن تتوافق مع قانون بينفورد (Benford)، وكذلك البيانات التي تتكوّن من عدد ثابت من الأرقام (مثل رقم بطاقة التعريف الوطنية الذي يتكوّن من تسعة أرقام).

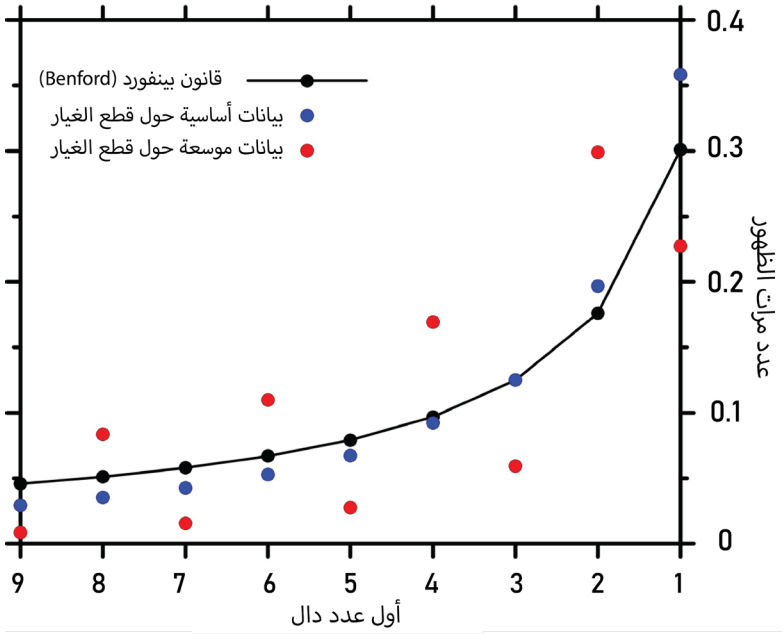
في بحث عن البيانات التي تتوافق مع قانون بينفورد (Benford)، أجرينا فحصًا غير رسمي لمجموعة من البيانات اللوجيستية ووجدنا أنّ بعضها يتبع قانون بينفورد (Benford). ومن الأمثلة على ذلك بيانات التسعير من نظام متطلبات المواد الثانوية، الذي غالبًا ما يشار إليه بمحدد نظام البيانات، D200A. يوضح الشكل 3.1 هذه البيانات بالمقارنة مع توزيع بينفورد (Benford) المثالي. فتبدو البيانات قريبة جدًا من أن تكون بيانات بينفورد (Benford). ويوجد العديد من المؤشرات التي تؤكد على توافق هذه البيانات مع قانون بينفورد (Benford) بالإضافة إلى اختبارات إحصائية أخرى.

الشكل 3.1 بيانات تسعير من D200A التي تتوافق مع قانون بينفورد (Benford).



لم تتوافق العديد من البيانات التي فحصناها مع قانون بينفورد (Benford)، بما في ذلك بعض البيانات الأخرى من D200A. أحد الأمثلة على ذلك، بيانات D200A الخاصة بطلبات قطع غيار الطائرات القابلة للإصلاح في السنوات المالية 2008-2013. تتوافق هذه البيانات مع معظم شروط ملاءمة قانون بينفورد (Benford) في القسم أعلاه، كحجم مجموعات البيانات (تقريبًا 118,000 سجل) الذي يتخذ مستويات متعددة، ومتوسطه أعلى من الوسيط مع انحراف إيجابي. وبعد فحصٍ وثيق، فشل حجم هذه البيانات في بعض الاختبارات الإحصائية شديدة الدقة. ووقد كشف أحد الاختبارات بشكل خاص أنّ حجم البيانات ثابت المقياس. يُبيّن الشكل 3.2 بيانات D200A الأصلية (البيانات الخام)، ثم حاصل ضربها بالعدد 2 (بيانات موسّعة)، وقانون بينفورد.[22] وكما هو واضح، يتغيّر توزيع البيانات بشكل كبير بعد ضربها بالعدد 2 لذلك لا يعد غير مرتبط بمقياس، بالتالي فإنها لا تتوافق مع قانون بينفورد (Benford).

الشكل 3.2 بيانات قطع الغيار القابلة للإصلاح من D200A، والتي لا تتوافق مع قانون بينفورد.



في الاختبارات التي تستعمل بيانات صورية تتوافق مع قانون بينفورد (Benford) وحيث تم تلقائيًا تعديل نقاط عشوائية لتصبح غير متوافقة مع قانون بينفورد (Benford)، وجدنا أنه بإمكاننا تحديد متى تم تغيير ما يقارب 9 بالمئة أو أكثر من البيانات باستخدام اختبارات مختلفة لحُسن المطابقة. بالتالي، نتوقّع أنه إذا قام أحد الخصوم بتغيير أكثر من 9 بالمئة من البيانات ضمن المجموعة المتوافقة مع قانون بينفورد (Benford)، يمكن للتقنيات الإحصائية أن ترصد هذا المستوى من التلف.[23] في المقابل، سيكون من الصعب أو من المستحيل اكتشاف التلف الذي يقل عن 9 بالمئة من البيانات باستخدام هذه الطريقة.

[22] انظر Berger and Hill, 2015, p. 73، لمعرفة كيفية تطبيق هذا الاختبار القياسي.

[23] انظر Nigrini، 2012 لمراجعة جيدة لهذه الاختبارات.

تقنيات أخرى

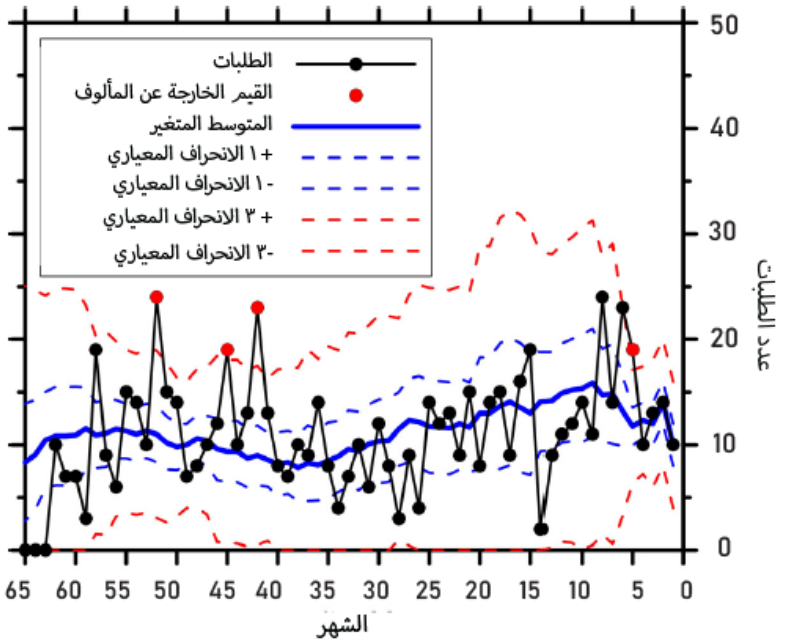
حتى لو لم تتوافق مجموعة البيانات مع قانون بينفورد (Benford)، غالبًا ما ستُظهر نمطًا متّسقًا طيلة وقت توزيع الأرقام الدالّة. فإذا كان هذا النمط معروفًا من عملية تحديد العينات قبل حدوث أي تلاعب في البيانات، يمكن للمحلل أن يقارن البيانات المشتبه بها مع هذا النمط المعروف. تشبه هذه المقاربة كثيرًا طريقة قانون بينفورد (Benford) التي شرحناها سابقًا، باستثناء مقارنة البيانات مع توزيع معروف وليس مع توزيع بينفورد (Benford). ولكن الميزة الإضافية لقانون بينفورد (Benford) هي أنّ الباحثين السابقين أسسوا تقنيات إحصائية لرصد تلف البيانات. لذلك فإنّ تقييم ما إذا أُجري تغيير كبير على مجموعة بيانات بينفورد (Benford)، يمكن أن يصبح إجراءً روتينيًا باستخدام أدوات قائمة ولا يتطلب امتلاك المحلل لأي مهارات خاصة. أما إذا كانت مجموعة البيانات لا تتوافق مع قانون بينفورد (Benford)، فإنه بالاعتماد على طبيعة أنماط الأرقام الدالّة، قد تكون هناك حاجة إلى طرق إحصائية مخصصة وستتطلب بالتالي من المحلل امتلاك مهارات متقدمة وتطوير اختبارات خاصة بكل مجموعة بيانات.

لا بد من الإشارة إلى وجود اختبار إحصائي إضافي هو "*التحكم بالعملية الإحصائية*". فبدلاً من تفحّص مجموعة البيانات ككل بحثًا عن التلف، تفحص هذه الطريقة كل معلومة في مجموعة البيانات باعتبارها حالة شاذة محتملة. تعد هذه الطريقة مفيدة جدًا للتسلسل الزمني للبيانات، مثل طلبات قطع الغيار. مع مرور الوقت، تقيس هذه الطريقة الاستثناءات في أي توزيع مستقر لقيم خاصة بنوع معين من البيانات. تقوم الفكرة الرئيسية على الحفاظ على مسار إحصائي معين (مثلاً المتوسط المتغير لعدد من الطلبات) مع مرور الوقت، بالإضافةِ إلى أي اختلاف يطرأ على الإحصاءات (مثل الانحراف المعياري أو الانحراف المطلق). بالتالي، تخلق هذه الطريقة لوحة مراقبة تُظهر ما إذا كانت أية بيانات "خارجة عن المألوف" بشكل ما. تتألف لوحة المراقبة من ثلاثة خطوط تدل على الوقت: الخط المركزي (عادةً يمثل المتوسط)، والحد الأعلى للمراقبة والحد الأدنى للمراقبة. والحد الأعلى والحد الأدنى للمراقبة يمثلان ثلاثة انحرافات معيارية شائعة تقع فوق المتوسط وتحته. عندما لا تتبع البيانات توزيع غاوس (Gaussian distribution)، تستخدم معايير أخرى لهذه الحدود، مثل قيم النّسب المئويّة الـ95 والـ5. وتقدم الحدود طريقةً لرصد كل ما هو خارج عن المألوف أو يشكل استثناءً.

يُظهر الشكل 3.3 مثالاً على هذه الطريقة في طلبات من مجموعة أوغدن (Ogden) للخدمات اللوجيستية الخاصة بالطائرات لحلقات دائرية (NIIN 013313891) خلال 65 شهرًا، بدءًا من كانون الثاني (يناير) 2011 وحتى أيار (مايو) 2016. وهذه الطلبات مسجّلة في قاعدة بيانات التوزيع الاستراتيجي. تظهر الطلبات الحقيقية باللون الأسود. أما الخط الأزرق المتصل فيعرض المتوسط المتغير من 12 شهرًا الماضية (باستثناء كانون الثاني (يناير) 2011 حتى كانون الأول (ديسمبر) 2011، وهو المتوسط المتغير الموجود منذ الأشهر الماضية من البيانات التي تبدأ من كانون الثاني (يناير) 2011). تمثل الخطوط الحمراء المتقطعة الانحرافات المعيارية المتغيرة الثلاثة للبيانات ذاتها. تُشير النقاط الحمراء إلى القيم الشاذة التي تقع خارج حدود الانحرافات المعيارية الثلاثة. توجد قيمة شاذة في فترة مبكرة، عند الشهر الخامس التي يمكن تجاهلها لأن البيانات المدخلة والمستخدمة في حساب المتوسط والانحراف المعياري عند تلك النقطة قليلة جدًا. توجد ثلاث قيم شاذة في الأشهر 42 و45 و52، استجابةً لطلبات حزيران (يونيو) 2014، وأيلول (سبتمبر) 2014، ونيسان (أبريل) 2015 حيث كانت أرقام الطلبات 23 و19 و24 على التوالي. استُثنيت هذه القيم الشاذة من الحسابات التي أجريت لاحقًا للمتوسط المتغير والانحراف المعياري. تقع هذه القيم خارج حدود الانحرافات المعيارية الثلاثة من

الأشهر 12 الماضية وقد تتطلب المزيد من التحقيقات لاحقًا. يمكن لمثل هذا النهج أن يساعد في تمييز القيم الشاذة ولكنه قد يتطلب جدولاً زمنيًا أقصر مما هو موضح في هذا الرسم.

الشكل 3.3 تحليل عملية مراقبة العمليات الإحصائية لطلبات المستودع



نلاحظ أنّ جميع هذه التقنيات تلفت الانتباه لاحتمال وجود بيانات شاذة عندما لا يتمكن الأفراد من رؤية البيانات الشاذة أو عندما تكون البيانات الشاذة مخبأة في مجموعة بيانات كبيرة وفوضوية. يُبلّغ عن هذه البيانات المهمة لإجراء مزيد من التحقيقات حولها، لتحديد ما إذا كانت هذه الحالة الشاذة إشكالية. بالتالي هذه الطريقة *ترصد* الحالات الشاذة لكن لا تقيّمها.

التأقلم مع ظروف الحرب

ليست الحرب فقط الوقت الأهم لامتلاك تدابير فعّالة للتصدي لحالات تلف البيانات الناتجة عن الهجمات الإلكترونية، ولكنها تشكل أيضًا تحديًا للعاملين باختلافها عن بيئة السلم التي اعتادوا عليها. بالنسبة لرصد تلف البيانات، فالاختلاف الأساسي بين ظروف السلم وظروف الحرب هو أنّ ما قد يبدو حالةً شاذةً يختلف في ظروف السلم عن ظروف الحرب في بعض الأحيان. ولكن درجة الاختلاف هذه تتفاوت باختلاف المجالات الوظيفية. ففي حين لا يطرأ تغيير على البيانات الخاصة بعمليات الصيانة في حالة الحرب، يطرأ في المقابل تغيير كبير على البيانات الخاصة بالتوريد والنقل خلال الحرب عما كانت عليه في السلم. يزيد هذا التغيير الذي يطرأ على خط الأساس المعياري من صعوبة اكتشاف الأخطاء الحقيقية في هذه المجالات خلال الحرب، حيث يكون احتمال وجود أخطاء هو الأكبر.

تحتاج المجالات الوظيفية كالتوريد والنقل للتكيّف مع بيئة الحرب لتتمكن من رصد تلف البيانات بفعالية. لكن ما هي التعديلات التي يمكن إدخالها؟ مقارنة مع ظروف السلم، يكون خطر التعرض للهجمات الإلكترونية في ظروف الحرب

أكبر، بالإضافة إلى العواقب التي تترتّب على اتخاذ إجراءات مبنية على بيانات خاطئة. هذا التغير في درجة الخطورة يقترح طريقة واحدة لمواجهة هذا التحدي: بالنسبة للمجالات الوظيفية التي يحتمل أن تشهد قدرًا كبيرًا من الانحراف في أنماط العمليات عند الانتقال من حالة السلم إلى الحرب، فيجب عليها أن تطبق تدابير استجابة بشكل تدريجي لرصد تلف البيانات.

تكون الاستجابة التدريجية مشابهةً لمستويات حالة حماية القوات (FPCON) التي تُستَخدم في قبول المخاطر التي تهدد أمن المنشأة وتخفيفها. بالاعتماد على درجة الخطر، تحدد وزارة الدفاع خمس زيادات تدريجية في مستويات حالة حماية القوات (FPCON) والتدابير الوقائية المرتبطة بها، وهي: المستوى الطبيعي وألفا وبرافو وتشارلي وأعلى مستوى وهو دلتا.[24] تُحدد هذه المستويات وتتغير بصورة ديناميكية. لكل مستوى في حالة حماية القوات (FPCON)، تدابير وقائية محددة مصممة لمواجهة الخطر، دون أن تفرض عبئًا عاليًا غير ضروري على العمليات الأساسية أو أفراد قوات الأمن.

قد يتبع الاكتشاف عن تلف البيانات وضعه المتدرج تصاعديًا بناءً على حالة العمليات الخاصة بالمعلومات (INFOCON) المُقيّمة بشكل منفصل.[25] ونظرًا للطبيعة المترابطة للفضاء الإلكتروني، تحدد حالة العمليات الخاصة بالمعلومات (INFOCON) بالاعتماد على الحالة العالمية وليس المحلية. والنقطة التي نرغب في التأكيد عليها هي أنّ حالة حماية القوات (FPCON) وحالة العمليات الخاصة بالمعلومات (INFOCON) تصفان التدابير المحددة التي يتوجب اتخاذها، بناءً على مستوى الخطر المحدد. تُفرض تدابير حالة حماية القوات (FPCON) على القوات الأمنية، بينما تُفرض تدابير حالة العمليات الخاصة بالمعلومات (INFOCON) على قوات الدفاع الإلكترونية ومديري الشبكات.

نوصي الأوساط اللوجيستية بتحديد سياسة تشمل التدابير التي يجب أن تتخذها بناءً على مستوى حالة العمليات الخاصة بالمعلومات (INFOCON). تهدف هذه التدابير إلى استمرار العمليات اللوجيستية أكثر من ضمان المعلومات. ولكن تحديد ما هي هذه التدابير بالضبط وأي منها تطبّق في كلٍ من المجالات الوظيفية يتطلب دراسة منفصلة. فيما يلي، بعض الأمثلة على الإجراءات التي يمكن اتخاذها:

- قبل اتخاذ أي إجراء حاسم قد يتطلب التعافي منه وقتًا طويلاً إن بُني على خطأ، تحققوا من البيانات من خلال التواصل مع السلطات المناسبة كلّ على حدة وذلك لتأكيد الإجراء المطلوب (مثل، الاتصال بمكتب البرنامج للتحقق من الجزء المتعلق بنزع السلاح).
- تحققوا من البيانات من وقت لآخر وتأكدوا بشكل نشيط من سلامتها بأساليب استباقية أخرى (للاستعاضة عن الاكتشاف السلبي السائد خلال العمليات العادية).
- انسخوا البيانات تكرارًا بطرق تجعل من الصّعب مهاجمتها، مثل طباعة بيانات معيّنة (كجرد محتويات المخزن ومواقع المستودعات، والأوامر التقنية) ونسخها على وسائط معزولة (مثل الأقراص المدمجة).
- راجعوا الإجراءات اليدوية وتلك التي لا تتعلق بتكنولوجيا المعلومات، وطبقوها تكرارًا.

---

[24] تعليمات وزارة الدفاع 2000. 16، 2006.

[25] قريبًا ستتم الاستعاضة عن نظام مستوى حالة العمليات الخاصة بالمعلومات (INFOCON) بنظام حالة الفضاء الإلكتروني (CYBERCON). فمستويات النظام الأول شاملة ويحددها القائد أو القيادة الاستراتيجية الأمريكية. ولكن بإمكان القادة على جميع المستويات أن يحددوا محليًا مستويات لحالات العمليات أكثر صرامة للأنظمة التي يتولّون قيادتها (رئيس هيئة الأركان المشتركة الأمريكية 6510.01F، 9 شباط (فبراير) 2011، يبدأ العمل بالتوجيه الحالي اعتبارًا من 9 حزيران (يونيو)، 2015; وفقًا لتوجيهات القيادة الاستراتيجية 1-527، 27 كانون الثاني (يناير)، 2006).

ندرك أنّ الانتقال إلى الاستجابة التدريجية سيبطئ سير العمليات بشكل ما خلال وجود خطر إلكتروني كبير، إلا أنه سيقدم وقاية ضد أي تأخير أطول أو ضد حالات توقّف التشغيل التي قد تنتج عن هجوم ناجح. أحيانًا قد يكون توقّف التشغيل ضروريًا لرصد البيانات رصدًا دقيقًا. وتستخدم القوات الجوية أنظمة تكنولوجيا المعلومات والبيانات وتعتمد عليها أكثر فأكثر من أجل تقليل العبء على العاملين. وليس من المستغرب أن تُبين الأبحاث أنه كلما زاد عبء العمل والضغط على العاملين، زاد اعتمادهم على البيانات وقل احتمال أن يشكوا أو يرصدوا أي خطأ فيها.[26] عند التعامل مع ضغط عمل كبير، يميل العاملون إلى زيادة درجة ثقتهم ليصبحوا ضمن فئة العاملين الذين "يفرطون في الثقة" كما هو موضح في الشكل 1.1. ينطبق الأمر ذاته عند زيادة أساس حالة حماية القوات (FPCON)، حيث يتم التضحية ببعض الكفاءات لزيادة مستوى الأمن.

من شأن الاستجابةِ التدريجية أن تقلل الحاجة إلى تبديد الموارد خلال الأوقات التي يكون فيها مستوى الخطر منخفضًا وتكون العواقب المترتبة على اتخاذ إجراءات مبنيّة على بيانات خاطئة منخفضة نسبيًا أيضًا. وتغيير إجراءات الوحدة اللوجيستية وفقًا لحالة العمليات الخاصة بالمعلومات (INFOCON) سيكون بمثابة رادع لأي هجوم. فسيدرك الخصوم أنّ القوة أقل عرضة للهجمات الإلكترونية نظرًا لتبنّيها تدابير أكثر متانة ومرونة.

التدريب على عملية الاكتشاف

تعتمد الدرجة التي يثق بها الأفراد في البيانات والتشغيل الآلي على خبراتهم السابقة بمدى دقة البيانات وفائدة التشغيل الآلي. فكلما شعروا أنه يمكنهم الاعتماد أكثر على البيانات والتشغيل الآلي، زادت ثقتهم وقلّ احتمال شكّهم بإمكانية وجود مشكلات وبالتالي قلّت إمكانية رصدهم له وكشفها عن طريق الاستدلال.[27] ويكون العاملون الذين يثقون كثيرًا في البيانات معرضين لخطر التصرف بالاستناد إلى البيانات دون تفحّصها والانجراف نحو حالة "الإفراط في الثقة" الموضحة في الشكل 1.1. وبينما يكون العاملون الذين يضعون قدرًا قليلاً من ثقتهم في البيانات، معرّضين للانجراف نحو حالة "الإفراط في الشك" الموضحة في الشكل 1.1 وبالتالي اتخاذ إجراءات تخالف التعليمات المبنيّة على بيانات صحيحة (كاستبدال التوجيهات الصوتية من البيانات بأحكامهم الشخصية أو تجاهل إنذار حقيقي بسبب سماع العديد من الإنذارات الخاطئة).

بالرجوع مجددًا إلى الشكل 1.1، لتحقيق أكبر قدر من الفعالية في رصد تلف البيانات، على العاملين أن يبقوا عند خط "الثقة الموزونة"، حيث يعبّرون عن مستوى مناسب من الثقة بالنظر إلى البيئة الواقعية. ونظرًا إلى أنّ الدقة المحتملة للبيانات ستختلف باختلاف بيئة التهديد، والتي تقدرها حالة العمليات الخاصة بالمعلومات (INFOCON)، يحتاج العاملون إلى ضبط تصوّراتهم (ثقتهم في البيانات) بناءً على ذلك للحفاظ على توازن ثقتهم مع البيئة. لكن معظم تصورات العاملين في مجال اللوجيستيات تنشأ من تدريبهم وتجاربهم اليومية، وليس من تجارب الحرب أو الهجمات.

بشكل عام، من غير المرجح أن يمثل هذا التدريب ولا التجارب اليومية، بدقّة ما يمكن أن يحدث في حالة الحرب التي تشمل التعرّض للهجوم. ونظرًا إلى أنه من غير المرجح أن تكون القوات الجوية الأمريكية قد تعرضت للهجوم الأعنف في الفضاء الإلكتروني، فإن العاملين لم يختبروا جميع الهجمات المحتملة. فالتدريب والتجارب حصلا بتأثيرات

[26] Endsley, 1995; Parasuraman and Riley, 1997.

[27] Lee and Moray, 1992; Parasuraman and Riley, 1997; Madhaven, Wiegmann, and Lacson, 2006; Merritt and Ilgen, 2008; Hoff and Bashir, 2015; de Vries, van den Berg, and Midden, 2015.

محلية محدودة، مما سمح للوحدات بالوصول إلى الوحدات الأخرى للحصول على الدعم. إلّا أنه في حال وقوع هجوم واسع النطاق، قد تكون جميع الوحدات في خطر وقد لا تملك أيٌ منها القدرة على الوصول إلى الوحدات الأخرى للحصول على مساعدة. وهذا النقص في الخبرة الواقعية يحد من قدرة العاملين في الوحدة اللوجيستية على تصوّر ما قد يكون هجومًا إلكترونيًا موجّهًا ومنسّقًا من قبل دولة قادرة. لذلك يجب أن يسدّ التدريب هذه الفجوة.

لم نجرِ مسحًا ممنهجًا، ولكن ملاحظتنا السردية المبنية على العديد من الاجتماعات مع العاملين في المجال اللوجيستي وصولًا إلى القيادة الرئيسية والرتب كافة، بدءًا من طياري الدرجة الأولى إلى ضباط الميادين، جميعها تؤكد وجود نقصٍ في الوعي في هذه المسألة. ففي كل مجموعة قابلناها كان هناك أفراد يراودهم الشك أنّ النظام الذي يستخدمونه قد يتعرض لهجوم أو قد يقوم أحدهم بتبديل البيانات التي يستخدمونها. في المقابل كان هناك العديد من العاملين على ثقة كبيرة بقدرة خبراء أمن الحواسيب في القوات الجوية الأمريكية على حماية بياناتهم من أي تلف قد يلحقه الخصوم بها. وهذه التصورات لا تعكس المخاطر الحقيقية بدقة.[28]

من ناحية أخرى، يتلقّى العاملون، وبالأخص الطيارون منهم، العديد من الإحاطات حول السلامة بعضها يتعلق بحياتهم الشخصية (مثل ركوب الدراجة) وبعضها يتعلق بمكان عملهم. وتتراوح الأخيرة بين تدريبات عامة حول كيفية حمل غرض معين بشكل آمن إلى تدريبات متخصصة حول تجنّب الإصابة عند القيام بعملية صيانة معينة. تجري العديد من تدريبات السلامة على يد أحد المشرفين في مكان العمل وتوضّح (بشكل تصويري أحيانًا) عواقب عدم اتباع بروتوكولات السلامة. يتعدّى تدريب السلامة المتلقى المجالات العامة ويقوم العاملون والمشرفون بتوثيقه بشكل خاص ومنتظم باستخدام نموذج القوات الجوية الأمريكية رقم 55.

في المقابل، لا يوجد تدريب مواز في مجال الأمن الإلكتروني في مكان العمل. في الواقع، معظم العاملين الذين صادفناهم لم يخضعوا لأي تدريب حول الأمن الإلكتروني أبعد من إحاطة حول كيفية تشغيل حاسوب المكتب. وهذا الأمر يترك لدى العاملين انطباعًا أنّ الأمن الإلكتروني يطبّق على بيئة المكتب أما مكان العمل (مثل، أنظمة صيانة الطائرات) فآمن ولذلك لا يحتاجون لأي تدريب خاص بالأمن الإلكتروني لمكان العمل.

بدون توعية حول المخاطر الإلكترونية الحقيقية، يقل احتمال رصد العاملين للبيانات المشكوك في تلفها والتبليغ عنها. لذلك، فالتوصية الرئيسية للتدريب هي تثقيف جميع العاملين (طيارين ومدنيين ومتعاقدين) حول إمكانية وجود تلف البيانات وبالتالي وجوب توخّي الحذر فيما يتعلق بهذه الحالات الشاذة.

قد يتطلّب وضع منهج كامل لما قد يبدو عليه هذا النظام التعليمي والتدريبي، دراسة منفصلة. ولكن نتصوّر أن تقوم خطوطه العريضة على الدمج بين التعليم والتدريب بعد توجيه العاملين فيما يتعلق بالسلامة. فيما يلي، الأهداف الرئيسية للتعليم والتدريب:

- الإشارة إلى أنّ جميع أنظمة البيانات عرضة لتلف البيانات والهجمات الإلكترونية، وبالتالي، فإنّ اليقظة مطلوبة عند التعامل مع جميع الأنظمة والعمليات.
- التأكيد على أنّ لكل فرد عامل في المؤسسة اللوجيستية حصة في الأمن الإلكتروني، وليس فقط أصحاب تخصصات معينة في الأمن الإلكتروني.

[28] انظر على سبيل المثال، Batey، 2016.

- يجب أن يستمر التعليم والتدريب طوال المسيرة المهنية، بدءًا من المدرسة التقنية وخلال التدريب العملي والتمارين. كما يجب أن يتم تتبعه بسجل منفصل، يشبه الطريقة التي تستخدم في تدريب السلامة ونموذج القوات الجوية رقم 55.
- يجب أن يطبق التعليم والتدريب، بأكبر قدر ممكن من العملية في بيئة العمل من خلال اختبار أمثلة حقيقية، ويجب أن يركز على العواقب المحتملة التي تترتب على الفشل في اكتشاف البيانات الشاذة المشكوك فيها التبليغ عنها.
- يجب أن يشمل التعليم والتدريب جميع العاملين من طيارين ومدنيين ومتعاقدين.
- يجب أن يصف الإجراء الذي ينبغي اتخاذه بشكل متسلسل من خلال حالة العمليات الخاصة بالمعلومات (INFOCON)، ضمن إطار ما ذكر في القسم السابق، ولكن بتفصيل أكبر.

كما في تدريبات السلامة، كلما كانت الرسالة أقل غموضًا، والإجراءات المطلوبة من العاملين والعواقب المترتبة على عدم اتخاذ هذه الإجراءات أكثر واقعية، كانت النتائج أكثر فعالية. ولكن ثمة عقبة أمام القيام بذلك في مجال الأمن الإلكتروني، وهي الحاجة إلى حجب معلومات عن العاملين غير المخولين الاطلاع عليها. مما لا شك فيه، أنه كلما زادت التفاصيل المتوفرة، أصبح العاملون على قدرٍ أكبر من الاطلاع. ولكن حتى أكثر التعليمات عمومية وهي أنّ جميع أنظمة البيانات معرضة للهجمات الإلكترونية لم يتم نشرها بفعالية، بالرغم من أنها ستعود بالنفع على المؤسسة. ومن شأن تقديم أمثلة محددة لما قد يحدث بالإضافة إلى عواقب ذلك أن يساعد في تعزيز الرسالة، إلا أنّ هذه الأمثلة قد تكون افتراضية.

ثمة ملاحظة أخيرة حول التعليم والتدريب، وهي أنّ بعض الأبحاث تخلص إلى أنّ فئة العاملين الأكثر شبابًا تتعامل مع البيانات والتشغيل الآلي بطريقة مختلفة عن فئة العاملين الأكبر سنًا. على ما يبدو تؤثر هذه الاختلافات على درجة الثقة التي تبديها كل فئة عمرية تجاه البيانات. وتؤكد الكثير من الأبحاث أنّ العمر عامل مؤثر في درجة الثقة في البيانات، إلا أنّ كيفية تأثيره تعتمد على السياق.[29] قد يكون من المفيد تصميم دورات التعليم والتدريب في الأمن الإلكتروني حسب الفئات العمرية، بشكل عام (ولرصد تلف البيانات بشكل خاص). للأسف، لا توجد أبحاث قوية حول أثر العمر ولا تقود هذه الأبحاث حتى الآن إلى أية تعميمات محددة حول كيفية إرشاد الفئات العمرية المختلفة.

حتى عندما يكتشف العاملون نوعًا من الأخطاء في البيانات، لا يحصلون على أي ردة فعل على ما حدث وسبب حدوثه أو قد يحصلون على ردة فعل ضئيلة. هل كان الخطأ عشوائيًا؟ وإن كان كذلك، فكيف حدث؟ هل كان نتيجة هجوم؟ في غياب الإجابات، يفتقد العاملون إلى معلومات أساسية ضرورية لتحديد درجة ثقتهم. من المعروف أنّ لهذا النوع من الملاحظات دورًا مهمًا في مجال السلامة، لبناء ثقافة سلامة مُرضية.[30] عند اختبار حالة قريبة من الفوضى أو عند وقوع حادث، تتجمع التقارير الرسمية وتقيّم المعلومات وتنشر الدروس المستفادة للعاملين من خلال التقارير والتدريب المعدل، والآليات الأخرى. تبرز أهمية ردود الأفعال والآراء حول الأداء للمراقبة الفعالة.[31] وتتطلب ردود الأفعال الفعالة وجود قوى عاملة تملك الدافع لكتابة التقارير مع توفر آليات رسمية للتبليغ، وامتلاك قدرة على إجراء تقييم سريع

[29] Hoff and Bashir، 2015، والمراجع الموجودة داخله.

[30] Reason, 1998; Woods, 2006; Dekker, 2006. 90-802, 2013. انظر تعليمات القوات الجوية 90-802، 2013

[31] Parasuraman and Riley, 1997.

لاستخراج الدروس المستفادة، بالإضافة إلى توفر طرق لنشر هذه الدروس المستفادة بين القوى العاملة. سنتناول موضوع تحفيز القوى العاملة في القسم التالي. وسنعالج مواضيع أخرى بدرجات متفاوتة من التفصيل، في الفصل التالي.

تحفيز عملية الاكتشاف

يعتبر نطاق البحوث التي تتحدث عن كيفية تحفيز العاملين واسعًا، ومن الواضح أنه لا يوجد وصفة واضحة تنطبق على جميع الظروف. ونركز هنا على بعض الإضاءات الرئيسية من أبحاث في علم النفس وعلم الاجتماع تتعلق بشكل خاص بمسألة تحفيز العاملين للتبليغ عن أي اشتباه في وجود خطأ ما في البيانات. عند إدارة دوافع القوى العاملة، يحتاج القادة إلى الإجابة عن سؤالين. السؤال الرئيسي الأول هو: ما هي الدوافع التي يريد القادة أن يمتلكها العاملون؟ أما السؤال الثاني فهو: ما هي الآلية الأكثر فعالية في تحفيز العاملين، وفقًا للنتائج المرجوّة؟[32] سنجيب عن السؤال الأول من رؤية أوسع وهي تغيير الثقافة السائدة بين العاملين. وسيتبع النقاش كيفية تطوّر ثقافة السلامة ولكن ليس بالطريقة نفسها التي تطوّر بها الأمن الإلكتروني.[33] بالنظر إلى هذه التوجهات المؤسسية الواسعة، سُنناقش آليات تحفيز الأفراد لتحقيق هذه الأهداف.

بناء ثقافة التبليغ والحفاظ عليها

كما هو الحال مع السلامة، هناك حاجة عامة لبناء *ثقافة* الأمن الإلكتروني التي تشجع العاملين على جميع المستويات على الإبلاغ عن البيانات الشاذة والمشبوهة والحفاظ عليها. يحاجج شين (Schein) بأنه:

> يمكن تعريف *الثقافة* بأنها (a) نمط من الافتراضات الأساسية، (b) اخترعته أو اكتشفته أو طورته مجموعة من الأشخاص، (c) أثناء تعلمهم كيفية التعامل مع المشاكل التي تواجههم أثناء التكيّف الخارجي والتكامل الداخلي، (d) وحقق نتائج جيدة بما يكفي ليعتبر صالحًا، ولذلك (e) يتم تعليمه للأعضاء الجدد (f) باعتباره الطريقة الصحيحة للإدراك والتفكير والشعور فيما يتعلق بهذه المشاكل. وبالتالي، تشير قوة التماسك الداخلي للثقافة ودرجته إلى استقرار المجموعة، وطول الفترة التي عاشتها، وكثافة التجارب التعليمية التي مرت بها، والآليات التي تعلمت من خلالها. (على سبيل المثال، التعزيز الإيجابي أو تجنب التكيّف)، كما تشير أيضًا إلى قوة الافتراضات التي وضعها مؤسسو المجموعة وقادتها ووضوحها.[34]

بالنسبة لمشكلة بناء ثقافة الاكتشاف والتبليغ عن الأخطاء المشتبه بها في البيانات، تقودنا هذه الحجة إلى وجود حاجة إلى (1) قيادة قوية، (2) حماية العاملين الذين يقومون بالتبليغ، (3) مشاركة ردود الفعل حول الأداء، و(4) إرشادات واضحة حول الإجراءات التي يجب اتخاذها. سنناقش التوصيات لكل نقطة بمزيد من التفصيل.

القيادة. على القادة في الوحدة اللوجيستية وضع سلامة البيانات في قمة سلم أولوياتهم وعليهم جعلها أولوية للعاملين. فالقيادة مطلوبة على جميع المستويات. فعند المستويات الأدنى، يجب أن يبيّن القادة أهمية التبليغ بالنسبة

---

[32] Higgins, 2012, especially Chapter 12.

[33] Reason, 1998; Woods, 2006.

[34] Schein, 1990, p. 111. النص الأصلي بالخط المائل.

لهم وبالنسبة للمشرفين عليهم. أما عند المستويات العليا، فيجب أن يؤكد القادة على أهمية سلامة البيانات التي تتطلب الاكتشاف والتبليغ عن كل ما يثير الشك. وحقيقة أنّ معظم الأخطاء في البيانات تحدث نتيجة أخطاء بشرية، تثبط دافع التبليغ عن الأخطاء. والسبب هو ميل الأفراد والمؤسسات إلى عدم التبليغ عن الأخطاء التي يرتكبونها، ومحاولة حل أي مشكلة قبل رفعها لأي شخص آخر خارج المؤسسة. فإذا نتجت البيانات الشاذة عن خطأ بشري فإن ذلك يعد رادعًا للتبليغ. كما أنّ التبليغ عن المشاكل التي يشتبه بها في البيانات وتقييمها سيؤدي إلى إبطاء سير العمل. وكل هذه الأمور تعد من الآثار السلبية المحتملة للتبليغ عن الأخطاء. لذلك من المهم أن يدرك العاملون أنّ القادة يدعمونهم.

يجب أن يؤكد القادة على أنّ جميع أعضاء المؤسسة مشاركون بحصة في الأمن الإلكتروني بشكل عام، والاكتشاف عن تلف البيانات بشكل خاص. فلطالما كان مقبولاً أن يلعب جميع أعضاء المؤسسة دورًا في السلامة. فوجود السلامة أو عدمه، ينتج من الأعمال الجماعية لجميع أعضاء المؤسسة، فهي ليست مسؤولية مجموعة خاصة من خبراء السلامة ضمن منظمة رائدة. تعد هذه إحدى ميزات الأمن الإلكتروني. لذلك، فالأمن الإلكتروني للمنظمة هو نتيجة السلوك الجماعي لجميع أعضائها. ولا يمكن تغيير هذه الثقافة إلا بوجود قيادة فعالة.

الحماية. يجب توفير الحماية للعاملين من أية عمليات انتقامية جراء قيامهم بالتبليغ.[35] قد يتطلب تحقيق الحماية قيام القادة بإصدار سياسات تحمي من يقوم بالتبليغ بشكل صريح، أو تحافظ على سرية هويته، أو كلاهما. فالسرية عنصر أساسي في العديد من أنظمة التبليغ الناجحة في مجال السلامة منها نظام الإبلاغ عن سلامة الطيران (ASRS)،[36] الذي يعد أحد أكثر أنظمة السلامة نجاحًا، والذي يسجّل له على نطاق واسع مستوى السلامة الاستثنائي للطيران التجاري. فمع بداية استخدام نظام الإبلاغ عن سلامة الطيران، شهد الطيران التجاري انخفاضًا كبيرًا في عدد الحوادث.[37] عند التبليغ عن المشاكل داخل قطاع الطيران التجاري، تكون سرية هوية المُبلغ محمية بموجب القانون (ما لم يفصح المبلغ عن سلوك غير قانوني). وبوصفها نتيجة طبيعية لتحقيق الحماية، قد يكون من الجيد في بعض الحالات فرض عقاب أو إنذار للعاملين الذين لا يبلغون عن الأخطاء المهمة على الرغم من علمهم بها.

ردود الفعل. يحتاج العاملون إلى معرفة ردود الفعل حول أدائهم في الرصد والتبليغ، وتكمن أهمية ذلك في مساعدة العاملين على تعلم ضبط مستوى ثقتهم في البيانات بشكل أفضل كما تحفزهم على تحسين أدائهم الوظيفي. وفي إطار عملنا، تعد ردود الفعل جزءًا من عملية التقييم وسنناقشها بمزيد من التفصيل في الفصل التالي.

الإرشاد. يجب أن يكون لدى العاملين إرشادات واضحة حول الإجراءات المتوقعة منهم. ما المناسب للإبلاغ عنه، ومتى؟ ولمن؟ يحتاج العاملون لعملية واضحة وقنوات رسمية للتبليغ، كما يجب أن تكون عمليات الإبلاغ عن البيانات التي يشتبه في سلامتها سهلة وتشبه عمليات الإبلاغ الأخرى قدر الإمكان.[38] وينبغي أن تكون حدود ما يمكن فعله واضحة للعاملين. على سبيل المثال، إنّ تشخيص المشكلة وإصدار تعليمات حول كيفية التخفيف من أثرها، هو من

---

[35] Weick and Sutcliffe, 2001, Chapter 5.

[36] Reynard et al., 1986; see ASRS, undated.

[37] Dijkstra, 2006.

[38] Thaler and Sunstein, 2008.

مسؤولية مجموعة أو مجموعات التقييم وليس العاملين. سنناقش بعض هذه العمليات في الفصل التالي.

بالنظر إلى التغييرات المطلوبة في الثقافة، ما هي التوجيهات التي توفرها الأبحاث لتحفيز الأفراد العاملين في هذا السياق؟

آليات تحفيز الأفراد

تشير بعض الأبحاث الحديثة في علم النفس إلى أنّ فعالية الآليات المختلفة لتحفيز الناس تعتمد على درجة التطابق بين وجهة آلية التحفيز والطريقة التي يؤدي بها العامل مهمة معيّنة.[39] فلا توجد أداة واحدة تحقق جميع الأهداف، مثل تقديم الحوافز (الثواب أو العقاب) التي تحفز العاملين بشكل فعّال. تنتج آلية التحفيز الفعالة من التوافق المتبادل بين حالة العامل والمهمة المراد إنجازها والآليات المتبعة لتحفيز ذلك العامل. لفهم التفكير الأكاديمي في هذا المجال من التحفيز، من الضروري امتلاك خلفية عن الموضوع.

يحدد علماء النفس حالتين للعاملين في هذا الإطار: *التركيز التنظيمي من جهة ووضع التنظيم الذاتي* من جهة ثانية. لنتحدث أولاً عن نوعي التركيز التنظيمي: *التعزيز والمنع*.[40] في المدرسة، الطالب الذي يركز على تعزيز أدائه سيطمح للحصول على درجة A التي ينظر إليها على أنها إنجاز. أما الطالب الذي يركز على منع الأداء السلبي فسيشعر بمسؤولية الحصول على الدرجة A لأنه يشعر أنّ عليه أن يحصل عليها ويخشى الحصول على أي درجة أخرى. إن التركيز على التعزيز يؤكد على التقدم والإنجاز وتحقيق أهداف جديدة. أما التركيز على المنع فيُعنى بالسلامة والأمن وتجنّب الخسارة والحفاظ على المكتسبات وعلى الوضع الراهن.[41]

على الرغم من أنّ الأفراد بشكل عام يميلون إما إلى التركيز على التعزيز أو المنع، فقد يميل عامل واحد للتركيز على التعزيز في وضع معيّن ومن ثم على المنع في وضع آخر. فإذا رأى العامل أنّ الوضع الراهن في مهمة معينة غير مقبول، قد يوجه تركيزه نحو التعزيز. فإذا كانت المهمة هي تنظيف مكان العمل، على سبيل المثال، سيعتبر العامل أنّ الوضع غير مقبول، وسيسعى جاهدًا لتحسين مكان العمل، وبذلك يكون العامل قد وجه تركيزه نحو التعزيز. من جهة أخرى، إذا رأى العامل أنّ الوضعَ الراهن جيد وأنّ هناك خطر في تعكيره، قد يوجّه تركيزه نحو المنع. قد يكون هذا هو الحال إذا كان أحد عمال الصيانة مترددًا في ضبط جهاز يبدو أنه يعمل بشكل جيد.

يمكن التلاعب بنوع التركيز التنظيمي الذي قد يتبناه العامل (يستفيد المعلنون من هذه الحقيقة). وتشير التجارب إلى أنه يمكن تغيير التركيز التنظيمي للشخص بمجرد تغيير الطريقة التي ينظر بها إلى المشكلة. ومثال على ذلك، أظهر الذين أُبلغوا في إحدى الدراسات أنّ إنجاز جزء معيّن من مهمة ما بشكل صحيح سيؤهلهم للحصول على مهمة ثانية

[39] معظم البراهين الواردة في هذا القسم مستمدة من Higgins، و2012 Cesario Higgins, and Scholer، 2008. انظر أيضًا Tyler and Blader 2005.

[40] Higgins, 1996.

[41] Crowe and Higgins, 1997.

ممتعة (مكافأة)، ميلاً إلى التركيز على التعزيز. أما الذين أُبلغوا أنّ إنجاز جزء معيّن من مهمة ما بشكل خاطئ سيؤدي إلى توليهم مهمة ثانية مملة (عقاب)، فقد أظهروا ميلاً نحو التركيز التنظيمي على المنع.[42]

الحالة الثانية للعمال هي أسلوب التنظيم الذاتي. فأساليب التنظيم الذاتي هي استراتيجيات يتم اختيارها بما يتناسب مع التركيز. *فالتقييم* هو أسلوب يريد فيه الفرد تقييم جميع البدائل المتاحة قبل الالتزام بأي إجراء، حتى لو أدى ذلك إلى تأخير اتخاذ الإجراء. فهنا يكون الشخص يقظًا وتحليليًا ويريد أن "يؤدي المهام الموكلة إليه بشكل صحيح". أما أسلوب *التحرّك* فيرغب فيه الفرد في اتخاذ إجراء، حتى لو كان ذلك يعني عدم النظر في جميع البدائل المتاحة له. وهنا يكون الشخص متلهّفًا ومتحمسًا ويريد "إنجاز المهام الموكلة إليه".[43] تتناسب استراتيجية التحرّك *بشكل تنظيمي* مع التركيز على التعزيز، وتتناسب استراتيجية التقييم بشكل تنظيمي مع التركيز على المنع.[44]

تكون قوة انخراط الفرد أكبر في الحالات التي يكون فيها التنظيم متناسبًا مع أهداف المهمة الموكلة إليه.[45] تقودنا هذه الملاحظة إلى كيفية تحفيز العاملين بالشكل الأكثر فعالية. *فيجب أن تتلاءم آليات التحفيز مع التركيز التنظيمي المرغوب وأسلوب التنظيم الذاتي ويجب أن يتم تأطيرها بطريقة تدفع العاملين إلى التركيز التنظيمي المرغوب فيه، في ضوء أهداف العمل*. يمكن توضيح هذه النقطة من خلال مثالين، الجدول 3.1. أدناه يلخص هذا النقاش.

الجدول 3.1. ملخص إطار العمل التحفيزي

	المجال	البيئة A	البيئة B
الأهداف الإدارية	الأهداف	الجودة	الكمية
		"إنجاز المهمة بالشكل الصحيح"	"إنجاز المهمة"
		تفكير، تحليل	إنتاج
		يقظة	اتخاذ إجراء
	التركيز التنظيمي	منع	تعزيز
	اسلوب التركيز الذاتي	تقييم	تحرّك
كيفية التحفيز	الحوافز	مكافات لعدم تكبّد خسائر	كسب المكافات
		عقوبات	
	رسائل القيادة	التزامات	اعتزاز
		مسؤولية	حماسة
	البيئة	جدّي	متعة
	ردود فعل فعّالة	سلبي	إيجابي

المصدر: مُلخص من هيغينز (Higgins) 2012.

[42] Roney, Higgins, and Shah, 1995

[43] Higgins, 2012, pp. 130–133.

[44] Higgins, 2012, p. 87.

[45] Higgins, 2012, p. 87.

يقدم المثال الأول، البيئة A في الجدول 3.1 – دراسة لمهمة تقدّم الجودة على الكمية. في هذه الحالة يجب على العاملين إظهار قدرة على التفكير والتحليل واليقظة. وعليهم "إنجاز مهمة بشكل صحيح". وهذا الوضع يلائم التركيز التنظيمي للمنع، كما أنّ أسلوب التنظيم الذاتي المناسب هو التقييم. ولتحفيز العمال في هذه الحالة، يجب أن تتناسب آليات التحفيز تنظيميًا مع هذه الأهداف.[46] إذا تم استخدام الحوافز، فمن الأفضل تقديمها في قالب عدم الخسارة وليس كمكافأة يجب كسبها. وهذا يعني إخبار العاملين أنهم سيحصلون على مكافأة من نوع ما طالما *لم يفشلوا* في *إنجاز المهمة* بدلاً من إخبارهم أنهم سيحصلون على مكافأة إذا *نجحوا* في *إنجاز مهمة ما*. كما أنّ العقوبات أيضًا تعد مناسبة من ناحية تنظيمية، لكن قد تعيق الحافز إذا تم النظر إليها على أنها غير عادلة. وبالإضافة إلى الحوافز، يمكن لرسائل القادة أن تكون مناسبة إذا قُدّمت في قالب التزامات ومسؤوليات بدلاً من قالب يستفزّ الاعتزاز والحماسة.[47] تتناسب البيئة العامة مع التنظيم الذاتي إذا اتسمت بالجدية بدلاً من المتعة. وأخيرًا، تكون ردود الفعل والآراء ملائمة بشكل أفضل إذا كانت سلبية (الإبلاغ عن حالات الفشل) بدلاً من كونها إيجابية (الإبلاغ عن النجاحات).[48]

يقدم المثال الثاني، البيئة B في الجدول 3.1 -دراسة لمهمة تقدم الكمية على الجودة. في هذه الحالة، يجب على العاملين التركيز على الإنتاج واتخاذ الإجراءات؛ وعليهم "إنجاز المهام الموكلة إليهم". وهذا الوضع يلائم التركيز التنظيمي للتعزيز، ووضع التنظيم الذاتي المناسب هو التحرك. ولتحفيز العمال في هذه الحالة، يجب اتباع الأساليب التي تخالف الحالة الأولى. فإذا استخدمت الحوافز، من الأفضل تقديمها على شكل مكافأة يمكن الحصول عليها بدلاً من شكل عدم الخسارة. أما أسلوب العقوبات فهو أسلوب غير مناسب ويجب تجنّبه. وبالإضافة إلى الحوافز، يمكن لرسائل القادة أن تكون مناسبة إذا اتسمت بالنشاط وطُرحت بطرق تشجع الاعتزاز والحماسة، ولا تتخذ شكل الالتزامات والمسؤوليات. والبيئة العامة تكون مناسبة أكثر إذا كانت مرحة بدلاً من أن تكون جدية. وأخيرًا، تكون ردود الفعل ملائمة أكثر إذا كانت إيجابية (الإبلاغ عن النجاحات) بدلاً من أن تكون سلبية (الإبلاغ عن حالات الفشل).[49]

تحفيز العاملين لاكتشاف البيانات الشاذة

ماذا يعني هذا في سياق تحفيز اكتشاف البيانات الشاذة في المجال اللوجيستي؟ في ضوء أهداف هذه الدراسة، يجب أن يُحفّز العاملون في مجال اللوجيستيات في القوات الجوية الأمريكية من طيارين ومدنيين ومتعاقدين لتقديم عمليات لوجيستية متينة ومرنة وللإبلاغ عن أية أخطاء يكتشفونها في البيانات قد تلحق ضررًا بالعمليات اللوجيستية. تتوافق هذه الأهداف مع قوة عاملة مُنتبهة ومتبصّرة ويقظة تقدّم الدقة على كمية الإنتاج، وقد تحمل شعار "إنجاز المهام بالشكل الصحيح". لذلك، من أجل تحفيز القوة العاملة، يجب أن تقدم الحوافز في صورة مكافآت لعدم الخسارة، ويجب أن تتخذ الرسائل شكل الالتزامات والمسؤوليات، وأن تكون نبرة الرسائل وبيئة العمل اللتان يضعهما المشرفون جدية، ويجب أن تكون ردود الفعل والآراء حول حالات الإخفاق في التبليغ.

---

[46] Higgins, 2012, pp. 239–242.

[47] 2008 Cesario, Higgins, and Scholer, 2008.

[48] Higgins, 2012.

[49] Higgins, 2012.

ليس اتّباع هذه المبادئ صيغة سحرية لتعزيز الاكتشاف عن البيانات الشاذة، إنما هي اتجاهات تظهرها البحوث حول ما قد يحفز الأفراد. والأنماط التي يلخصها الجدول 3.1 راسخة في الأبحاث والتجارب العملية. وأي غموض في تطبيقها هو درجة تدفع العاملين إما لتبني التركيز على التعزيز أو المنع. أظهرت أساليب القيادة التي تتوسط في التركيز التنظيمي لأتباعها نتائج متباينة في مجال السلامة.[50] فتبيّن أنّ كلاً من التعزيز والمنع يعززان السلامة. يشجع التركيز على التعزيز على التفكير الاستباقي لتجنب الحوادث وتحسين العادات ولكنه يقلل من معدلات الامتثال لقواعد السلامة. أما التركيز على المنع فيقود إلى نتائج مضادة. وينبغي رصد نتائج تطبيق هذه المبادئ على اكتشاف البيانات وتعديل الطرق المتبعة وفقًا لما هو مناسب.

يلاحظ أيضًا أنّ هذه الأهداف لا تتوافق مع قوة عاملة تركز على معدلات الإنتاج المرتفعة والنشاط المستمر الموجّه نحو عائدات الإنتاج، باختصار، قوة عاملة ترفع شعار "إنجاز المهام". وهذين الشعارين للقوى العاملة، "إنجاز المهام بالشكل الصحيح" و"إنجاز المهام"، مطلوبان في الوحدات اللوجيستية في القوات الجوية الأمريكية، لكنهما يثيران توترًا بين القوى العاملة. جميع الأمور الأخرى متساوية، من المتوقع أن تتيح بيئة تقوم على مبدأ "إنجاز المهام بالشكل الصحيح" تحقيق نتائج أكثر دقة في التبليغ عن البيانات الشاذة. كما أنها تتفق مع إطار الاستجابة المتدرج لحالة التهديد الإلكتروني لمستويات حالة العمليات الخاصة بالمعلومات (INFOCON) التي يتقدم فيها الأمن على الكفاءة. من جهة أخرى، من المتوقع أن تمنع بيئة تقوم على مبدأ "إنجاز المهام" حدوث مثل هذا الإبلاغ. لذلك سيرغب قادة القوات الجوية في تكييف آليات التحفيز المستخدمة مع حالة اكتشاف البيانات الشاذة، أو على الأقل، توخّي الحذر من عدم التدخل في الحالات حيث الأفضلية للتركيز على التعزيز.

نقاش ونتائج

تتكرر العديد من التوصيات المقترحة في هذا الفصل عند مناقشة كيفية التعامل مع التحديات المتعددة. لترتيب هذه التوصيات بشكل أكثر تنظيمًا، سنقوم في هذا القسم بجمع التوصيات الرئيسية في قائمة واحدة وترتيبها وفقًا للأهمية بشكل تقريبي وحسب الفئة العامة.

التعليم والتدريب ورسائل القيادة

أول توصية حسب تقييمنا هي تعليم جميع أعضاء المؤسسة وتدريبهم. وتكون العناصر الرئيسية للرسالة هي كما يلي:

- توعية العاملين على جميع المستويات أنّ جميع أنظمة البيانات عرضة لتلف البيانات وللهجمات الإلكترونية، مما يجعل اليقظة ضرورية على صعيد جميع الأنظمة والعمليات.
- إرساء ثقافة في القوى العاملة أنّ لكل فرد في المؤسسة اللوجيستية دورًا في الأمن الإلكتروني، وليس فقط أصحاب تخصصات معينة في الأمن الإلكتروني.

[50] Kark, Katz-Navon, and Delegach, 2015; Aryee and Hsiung, 2016.

يجب أن يقوم كل مستوى من مستويات القيادة (القيادة والإشراف) بدور في نشر هذه الرسائل. ويجب على من يشغلون المناصب العليا (من ضباط علم وضباط ميادين بشكل عام) أن يضعوا التبليغ عن المخاوف المتعلقة بالأمن الإلكتروني في أعلى سلّم أولوياتهم. ولتحقيق ذلك، يجب توفير الحماية للأشخاص الذين يقومون بالتبليغ من أية عمليات انتقامية واعتماد سياسة تضمن سهولة القيام بالتبليغ وتوفر توجيهات واضحة. يهدف ذلك إلى تغيير الثقافة السائدة، لزيادة يقظة العاملين عند التبليغ عن احتمال وجود بيانات تالفة وغيرها من المخاوف الإلكترونية، بقدر يقظتهم حيال السيطرة على الضرر الذي تلحقه الأجسام الغريبة بخطوط الطيران وغيرها من المخاوف المتعلقة بالسلامة. وحاليًا،يتوفر القليل فقط من المراجع، إن وجدت، حول سلامة البيانات أو الأمن الإلكتروني في الإصدارات اللوجيستية.[51]

يجب على أصحاب الرتب القيادية الأدنى (ضباط السرايا وكبار ضباط الصف) أن يضعوا توجيهات واضحة ومحددة للعاملين بشأن أي نوع من البيانات الشاذة عليهم إبلاغهم عنها وفقًا للمعرفة التي يملكونها حول حاجات العمليات.

يجب أن يتم تعميم الرسائل على جميع العاملين، بما في ذلك الطيارين والمدنيين والمتعاقدين. ويجب أن يستمر تعميم هذه الرسائل بشكل دائم. بالنسبة للطيارين، يجب أن يبدأ ذلك من المدرسة التقنية ويستمر خلال التدريب العملي والتمارين. بالإضافة إلى ذلك، يجب تطبيقها بأكبر قدر ممكن ضمن بيئة العمل من خلال اختبار أمثلة حقيقية، ويجب أن تركز على العواقب المحتملة التي تترتب على الفشل في اكتشاف البيانات الشاذة والتبليغ عنها.

إنّ أفضل طريقة لإيصال هذه الرسائل إلى جميع المستويات هي تقديمها باعتبارها التزامات ومسؤوليات للكشف والتبليغ. وبدلاً من وضع مكافآت للكشف الدقيق والإبلاغ الفوري، يجب وضع مكافآت لعدم الفشل في تحقيق النجاح ووضع العقاب المناسب في حالات الإخفاق في الإبلاغ. من الأفضل نشر هذه الرسائل في جو عمل جاد وليس في جو من المرح. وستكون الآراء حول الأداء الجماعي للعاملين في الاكتشاف والإبلاغ أكثر فعالية عند التركيز على الإخفاقات وعواقبها أكثر من النجاحات.

يمكن استخدام مجال السلامة نموذجًا لتوضيح كيفية تطبيق التوعية والتدريب. تتشارك هذه التحديات والتوصيات المقترحة في العديد من السمات مع السلامة. تعتبر السلامة مصدر قلق في جميع البيئات. فكل العاملين لديهم حصة في السلامة، وليس فقط العاملين في المنظمات المسؤولة عن السلامة. وهي أيضًا في أعلى سلّم أولويات القادة على جميع المستويات. ويخضع جميع العاملين لجلسات توعية وتدريب حول السلامة طيلة حياتهم المهنية. وتكون التوجيهات محددة قدر الإمكان. وتستخدم أمثلة حقيقية تسلّط الضوء على النتائج السلبية في حال عدم اتباع إجراءات السلامة. ويكون الإبلاغ عن المخاوف والمخالفات المتعلقة بالسلامة هو الأمر المتوقع ويتم تشجيعه. وفي كثير من الأحيان، تُمدد السرية. وقد تبيّن نجاح منح مكافآت على عدم الفشل في تحقيق النجاح والمعاقبة على الفشل. يمكن للأمن الإلكتروني أن يتقدم بشكل كبير من خلال اتباع هذه العادات. ولنكن واضحين: نحن لا نوصي بدمج السلامة والأمن الإلكتروني، بل نوصي باستخدام بعض الحلول الناجعة للتعامل مع تحديات مماثلة في كلا المجالين.

[51] على سبيل المثال، سياسة التأسيس لصيانة الطائرات، تعليمات القوات الجوية 21-101،2015 لا تتضمن هذه الرسائل.

الوضعية

نوصي وحدة الخدمات اللوجيستية بتحديد سياسة خاصة بالتدابير التي ينبغي اتخاذها استجابة لكل مستوى من مستويات حالة العمليات الخاصة بالمعلومات (INFOCON). من بين جميع التوصيات في هذا التقرير، نعتقد أنّ هذا الإجراء هو أكثرها ترجيحًا لتحقيق نتائج إيجابية ملموسة بأقل قدر من الموارد. فهذه التدابير تركز أكثر على استمرار العمليات اللوجيستية منه على تأمين المعلومات. وسيتم تحديد الإجراءات ضمن المجال اللوجيستي لموازاة إجراءات حالية خاصة بأنظمة تكنولوجيا معلومات. لكل مستوى حالة من حالات العمليات الخاصة بالمعلومات يجب تحديد تدابير احترازية في كل مجال وظيفي لزيادة المتانة والمرونة. يبدأ العمل بهذه التدابير مع ازدياد مستوى التهديد لمطابقة الموارد التي أنفقت (والكفاءة مقارنة بالتكلفة) مع بيئة التهديد. كما هو الحال عند التعامل مع مستويات حالة حماية القوات (FPCON)، تتميز التدابير التي ينبغي اتخاذها بكونها محددة ومخصصة، وتكون مدرجة ضمن تعليمات القوات الجوية الأمريكية. تتضمن بعض الأمثلة على الإجراءات التي يمكن اتخاذها ما يلي:

- قبل اتخاذ أي إجراء حاسم قد يتطلب التعافي منه وقتًا طويلاً إن بني على خطأ، تحققوا من البيانات من خلال التواصل مع السلطات المناسبة كلّ على حدة وذلك لتأكيد الإجراء المطلوب (مثل، الاتصال بمكتب البرنامج للتحقق من الجزء المتعلق بنزع السلاح).
- تحققوا من البيانات من وقت لآخر وتأكدوا بشكل نشيط من سلامتها بأساليب استباقية أخرى (للاستعاضة عن الاكتشاف السلبي السائد خلال العمليات العادية).
- انسخوا البيانات تكرارًا بطرق تجعل من الصّعب مهاجمتها، مثل طباعة بيانات معيّنة (كجرد محتويات المخزن ومواقع المستودعات والأوامر التقنية) ونسخها على وسائط معزولة (مثل الأقراص المدمجة).
- راجعوا الإرشادات والإجراءات التي لا تتعلق بتكنولوجيا المعلومات، وطبقوها تكرارًا.

الأدوات

يجب أن تفكّر القوات الجوية الأمريكية، إلى الحد الممكن عمليًا، في استخدام التقنيات القياسية المستخدمة في اكتشاف عمليات الاحتيال عند اكتشاف تلف بيانات ضمن المجموعات التي لا يراها الأفراد أثناء العمليات العادية. من الأفضل استخدام هذه الأدوات في الوظائف والبيانات المصنّفة باعتبارها أولويات وفقًا لإطار العمل الموضح في الفصل الخامس. يعتبر قانون بينفورد (Benford) أحد الطرق السهلة نسبيًا للتحقق من البيانات، ولكن يمكن استخدام طرق قياسية أخرى. يجب تحديد مدى استخدام هذه التقنيات بحسب حالة التهديد الإلكتروني من أجل تخفيف عبء العمل.

4. التقييم

حال الاشتباه باكتشاف خطأ في البيانات، يجب إبلاغ الشخص الذي يمكنه تقييم الخطأ. هل هو خطًأ حقًا؟ إذا كان كذلك، هل هو خطأ طبيعي، أم هجوم خبيث؟ عند هذه الخطوة توجد مرحلتان رئيسيتان. أولاً، يحتاج العاملون إلى قنوات وعمليات قياسية للتبليغ. وقد تحدثنا عن ذلك في الفصل السابق وسنتحدث عنه بشكل أوسع في هذا الفصل. ثانيًا، تحتاج المؤسسة إلى منظمة تستلم البلاغات وتفسرها وتنشر النتائج التي تتوصل إليها. فتقييم الخطأ له أدوار وآثار على جميع العمليات اللوجيستية والعمليات الإلكترونية.

في هذا الفصل، سنحدد حاجات المؤسسات الخاصة بعمليات التبليغ والتقييم. ثم نقارنها بالعمليات والمؤسسات القائمة داخل القوات الجوية الأمريكية ونبحث في آلية توظيفها في معالجة مشكلة متانة العمليات اللوجيستية ومرونتها في مواجهة الهجمات الإلكترونية. وأخيرًا، سنخلص إلى تحديد الثغرات في عمليات التبليغ والتقييم الحالية واقتراح بعض التعديلات البسيطة على العمليات والمؤسسات القائمة التي من شأنها تعزيز متانة العمليات اللوجيستية ومرونتها في وجه البيانات التي تم اختراقها.

حاجات عمليات التبليغ والتقييم

التبليغ

يصف كل من الفصل الثاني والثالث الخصائص الأساسية المرغوبة لإجراءات التبليغ. يجب أن تكون عملية التبليغ (1) شاملة و(2) آنيّة و(3) سهلة و(4) في متناول جميع العاملين و(5) محمية من الاتهامات المضادة التي قد تنشأ عن التبليغ.

يجب أن تمتد العملية أو العمليات لتشمل جميع احتمالات تلف البيانات. تعد آليات التبليغ الخاصة بأنواع معينة من البيانات ضمن مجال وظيفي محدد مفيدة للغاية. ولكن يجب أن تتوفّر آلية للتبليغ لأي عامل يلاحظ وجود تلف في البيانات في أية قاعدة بيانات.

يجب أن تتم العملية في الوقت المناسب. ويتطلب ذلك اتخاذ إجراءات فورية بالنيابة عن مقدم البلاغ ونقلها بشكل سريع عبر قنوات التبليغ. إذا كان لا بد من المرور بمستويات بيروقراطية متعددة، بشكل يتطلب الحصول على موافقة عدة مستويات في سلسلة القيادة على سبيل المثال، سيضيع جزءٌ من الوقت في كل خطوة. وفي كل خطوة هناك إمكانية لأن يماطل شخص ما أو يعترض عملية التبليغ سواء بقصد أو بغير قصد. يجب أن يمر التقرير مباشرة بالشخص المعني بالتقييم، وأن يجري إعلام الآخرين فقط من أجل نشر الوعي بالظروف.

يجب أن تكون العملية سهلة. فالعاملون يميلون إلى تأخير أو تجنّب المهام الشاقة التي قد تمر من دون أن يلاحظها أحد في حال الإخفاق في أدائها. ومن شأن التبليغ الشاق سواء على العامل أو على أي شخص في قناة الإرسال وصولاً إلى المسؤولين عن التقييم، تأخير الاستجابة. يمكن أن تكون عملية التبليغ شاقة بعدة طرق. فقد تتطلب الكثير من العمل الورقي من طرف العامل، أو قد تشكل عبئًا معرفيًا كبيرًا على العامل، على سبيل المثال مطالبة العامل بالاختيار من بين العديد من أنظمة التبليغ أو امتلاك معرفة مسبقة بالمؤسسة الأفضل لتقييم البلاغ. وستبدو آثار عبء الإبلاغ كبيرة في

الأوقات التي يكون فيها ضغط العمل كبيرًا، كما خلال العمليات سريعة الإيقاع، حين يكون ثمة احتمال وقلق أكبر من وقوع هجوم ما. وأفضل طريقة للتبليغ تكون بأقل قدر ممكن من العمل الورقي وبتعليمات بسيطة وباتباع عملية مألوفة بالنسبة للمعنيين (على سبيل المثال، تقليد عمليات مماثلة).

يجب أن تكون العملية فعّالة وفي متناول جميع العاملين. ولأنّ الأخطاء في البيانات قد تقع في أي مكان، فإنّ الشخص الذي يكون في وضع أفضل للكشف عن الأخطاء والإبلاغ عنها يحتاج إلى نظام إبلاغ في متناول يده. ويجب أن يكون نظام الإبلاغ الواحد ملائمًا للطيارين والمدنيين والمتعاقدين.

يجب أن توفر هذه العملية الحماية إلى مقدم البلاغ. فمن المحتمل أن يكون مقدم البلاغ هو الوحيد الذي يملك المعرفة اللازمة لتقديم البلاغ، لذا فإنّ فشله في فعل ذلك لن يعرضه لأي خطر في هذه الحالات. من ناحية أخرى، إذا كان لدى العاملين خوف من التعرّض لعمليات انتقامية بسبب تقديمهم أي بلاغ، فعلى الأغلب أنّ العديد منهم لن يقدموا على فعل ذلك. يثبط هذا التناقض عزيمة العاملين عن القيام بالإبلاغ. لذلك يجب أن يضع القادة الحماية من الانتقام ضمن أولوياتهم ورسائلهم. وكما ناقشنا في الفصل الأخير، سوف تنتج هذه التغييرات من التعديلات على الثقافة السائدة في مكان العمل. ولكن لأنّ مقدم البلاغ قد يكون طيارًا أو مدنيًا أو متعاقدًا وكل منهم يعمل تحت رقابة مختلفة تمامًا، فقد تكون هناك حاجة إلى السرية لضمان قدر كافٍ من حرية الإبلاغ. تستخدم بعض أنظمة الإبلاغ الخاصة بالسلامة سرية إعداد التقارير باعتبارها عنصرًا أساسيًا في جمع التقارير الحساسة.[52]

التقييم

تنطوي عملية التقييم على العديد من الأنشطة، أبرزها (1) ترتيب أولويات تقييم الحوادث وتحديد مقدار السرعة اللازمة لإنجاز كل منها؛ (2) إيكال كل حادثة إلى مُقيّم أو مجموعة من المقيّمين؛ (3) توزيع الحوادث على المقيّمين وأية منظمات أخرى بغرض التوعية بالظروف؛ (4) تقييم الحوادث. (5) نشر نتائج التقييم؛ (6) جمع الدروس المستفادة وحفظها في الأرشيف ونشرها. يجب القيام بكل نشاط من هذه الأنشطة في مجال الدعم اللوجيستي (الدعم القتالي) وفي مجال العمليات الإلكترونية. سنركّز في معظم نقاشنا على المكان الذي يمكن فيه القيام بهذه الأنشطة في مجال الخدمات اللوجيستية (الدعم القتالي) وكيفية ذلك.

ترتيب الأولويات. في أي نظام تبليغ، سيستلم المقيّمون العديد من الحوادث ويكون عليهم أن يعطوا الأولوية لتقييم بعضها قبل غيرها. فكل تقييم في حد بذاته سيلزم إنجازه في إطار زمني معيّن، ويفضل أن يتم ذلك قبل أن يتخذ المسؤولون عن التشغيل أي قرار حاسم بالاستناد إلى البيانات. لذلك، ينبغي تجهيز المؤسسة الأولى المسؤولة عن استلام البلاغات بشكل يمكّنها من تحديد سرعة تقييم حادث ما وترتيب الأولوية في تقييم الحادث. يمكن الحكم على درجة الإلحاح والأولوية بالاستناد إلى إطار العمل الموضّح في الفصل الخامس. وحين يكون حجم التقارير كبيرًا، قد نجد أنّ بعضها يسهل الحكم عليه بالفحص الأوّلي وأنه لا يستحق تقييمًا مفصلاً بسبب الازدواج الكامل أو الجزئي في خط التقييم أو بسبب غياب واضح للأهمية.

[52] يعد نظام تقرير سلامة الطيران (ASRS) مثالاً على ذلك.

من المهم أن تكون المؤسسة التي تعمل على تحديد أولويات الحوادث، سلطة مركزية. فقط عندما تنظر مؤسسة واحدة في جميع التقارير يمكنها أن تحكم بشكل مناسب بشأن الأولوية النسبية. والسبب الآخر لأهمية وجود كيان مركزي، هو امتلاك منظور واسع يتيح اكتشاف ارتباطات محتملة بين المسائل المبلّغ عنها. لنأخذ على سبيل المثال أنّ هجومًا منسقًا وقع ضد أحد أنظمة السلاح أدى إلى تعرّض جميع المجالات المرتبطة بهذا النظام لهجوم صغير ولكنه مهم: صيانة خطوط الطيران، ودعم سلسلة الإمداد، وعمليات القاعدة المحلية، ودعم النقل. فبدون سلطة مركزية، يمكن تقييم كل من هذه الهجمات الصغيرة على أنها مصدر إزعاج غير منطقي. ولكن من وجهة نظر مركزية، سينظر إليها باعتبارها اعتداءً منسقًا على نظام سلاح واحد. لذلك تحتاج السلطات التي تضع خطة للاستجابة والتخفيف من آثار الهجمات إلى امتلاك هذا المنظور الواسع.

إيكال المهام. بعد تحديد الأولويات وتحديد السرعة المطلوبة لإجراء التقييم، يجب إيكال كل بلاغ إلى مجموعة تملك خبرة ذات صلة لتقييم الحادث. يجب أن يكون لدى المؤسسة التي توزّع هذه المهام المعرفة الكافية لتحديد الجهة التي ستتعامل مع الحادث ويجب أن يكون لديها السلطة والتفويض بذلك.

التوزيع. بعد ذلك، يجب توزيع التقرير حول الحادث ومستوى أولويته والإطار الزمني للتقييم، على المؤسسة (المؤسسات) المسؤولة عن التقييم وعلى أي مؤسسة يجب أن تكون على دراية بهذا الحادث لنشر الوعي بالظروف.

التقييم. يتطلب إجراء التقييم قدرًا من المعرفة الفنية في المجال الوظيفي. ويتم نشر هذه المعرفة في العديد من المؤسسات المنضوية تحت لواء المؤسسة الكبرى، بما في ذلك مكاتب البرنامج والعمليات الوظيفية ووكالة لوجيستيات الدفاع والمتعاقدين وغيرها الكثير. ومن ثم، سيتعيّن توزيع التقييمات. ولكل حادثة، سيتم إيكال إجراءات التقييم إلى مؤسسة تملك المعرفة اللازمة. ثم تحدد المؤسسة المعنية بإجراء التقييم ما إذا كانت البيانات خاطئة حقًا. يتطلب هذا الجزء من التقييم وجهتي نظر لوجيستية وإلكترونية، وبالتالي ينقسم إلى جزئين في هذه المرحلة.

من ناحية لوجيستية، سيحتاج المقيّمون أولاً إلى تحديد ما إذا كان الحادث المبلغ عنه هو خطأ بالفعل. على سبيل المثال، قد يلاحظ أحد المبلغين تغييرًا في بيانات فنية أو بيانات تتعلق بوجهة قطعة غيار ويشك في وجود تلف فيها. ومع ذلك، قد يكتشف المُقيِّم بعد بعض التحقيق أنّ البيانات كانت دقيقة في واقع الأمر أو يقرر أن الخطأ كان في إدخال البيانات أو نتيجة خطأ روتيني آخر.[53] إذا تم تقييم البيانات على أنها تالفة ولم يكن هناك أي تفسير واضح، عندها سيتم مشاركة الحادث مع أحد المقيّمين في العمليات الإلكترونية لتحديد ما إذا كان هذا التلف ناتجًا عن هجوم إلكتروني أم لا.

[53] تحتوي العديد من قواعد البيانات على سجلات تدوّن معلومات المستخدم الذي قام بإجراء تغيير على البيانات وفي أي وقت فعل ذلك. ومن المهم أن يفهم المُقيِّم أيضًا أنّ أي تغيير يجري بواسطة حساب مرخّص يمكن أن يعد بيانات تالفة ناتجة عن هجوم إلكتروني وليس خطأ روتينيًا. يتمثل جزء أساسي من التقييم في تحديد السبب الرئيسي لتلف البيانات، ويتطلّب ذلك عادة التحدث إلى العاملين المعنيين، وعدم الاكتفاء بالسجل على أنه صحيح. فيمكن لكيان إلكتروني متطور تغيير معلومات السجل بمجرد وصوله إلى قاعدة البيانات.

من ناحية العمليات الإلكترونية، بعد أن يحدد المقيّمون ما إذا كان الحادث يبدو أنه نتيجة هجوم إلكتروني، عليهم تقييم ما إذا كان هذا الحادثُ مرتبطًا بأية حوادث أخرى وتحديد الإجراءات التي يجب اتخاذها لمعالجة آثار الهجوم. عندما يتأكد هذا المُقيِّم من أنّ الحادث هو الخطأ، وأنّ الخطأ وقع نتيجة التعرض لهجوم إلكتروني متعمّد، قد تقيّد المخاوف بشأن أمن العمليات نشر هذا التقييم بعدد محدود من الأفراد المصرّح لهم الاطلاع عليه. ستقيّد هذه الحاجة الأمنية بالتالي حلقة ردود الفعل لمقدم البلاغ. ومع ذلك، قد يوزّع المُقِّيم تعليمات بعزل المعدات الحاسوبية أو إطفاء الأنظمة من أجل الحفاظ على الأدلة الجنائية أو قد يتخذ إجراءات أخرى.

//نشر. بعد ذلك، يجب إرسال التقييمات إلى السلطة المركزية، وهي السلطة نفسها التي قامت بإيكال مهمة التقييم.

//جمع. يجب أن تقوم بعض المؤسسات بجمع الدروس المستفادة من هذه الحوادث وحفظها في الأرشيف ونشرها. فإذا تسببت بعض الأخطاء الشائعة في حدوث أخطاء متعددة في البيانات، يمكن الاستفادة من هذه الدروس لتعديل السياسات والتدريب والإجراءات بهدف الحد من وقوع أخطاء في البيانات في المستقبل.

قنوات التبليغ الحالية وحدودها

خلال العمليات العادية، تقع أنواع مختلفة من الأخطاء في بيانات كل وظيفة لوجيستية. وبالتالي، طوّرت كل وظيفة لوجيستية طريقة واحدة أو أكثر لأداء بعض أنشطة الإبلاغ والتقييم. سنعرض بإيجاز بعض هذه الأنشطة لمعرفة ما يمكن توظيفه لخدمة متانة العمليات اللوجيستية ومرونتها، وتحديد القدرات الإضافية اللازمة لتعزيز قنوات الإبلاغ الحالية وعمليات التقييم.

إحدى أكثر آليات الإبلاغ استخدامًا، وأوسعها انتشارًا، هي التي تتخذ شكل مكتب مساعدة أو مركز اتصال. وهي مؤسسات يمكن التواصل معها، عادة عن طريق البريد الإلكتروني و/أو الهاتف، لحل التفاوت في البيانات والشكاوى الأخرى. غالبًا ما تتوفر هذه الخدمات خلال ساعات العمل الاعتيادية وأحيانًا تتوفر على مدى 24 ساعة في اليوم و7 أيام في الأسبوع، لمعالجة المسائل الطارئة والعاجلة. تمتلك معظم أنظمة تكنولوجيا المعلومات الرسمية مكاتب مساعدة أو مراكز اتصال. كما أنّ المجالات الوظيفية تعتمد إجراءات مشابهة، خصوصًا في مجال معالجة التفاوت في البيانات. على سبيل المثال، تملك أقسام الإمداد عملية تبليغ رسمية عن تقارير تتضمن تفاوتًا في الإمداد خلال النموذج المعياري رقم 364.[54] أما المجال الوظيفي الخاص بالوقود فلديه مكتب مساعدة للإبلاغ عن مشاكل نظام المعلومات الآلي.[55] وهناك العديد من الأمثلة الأخرى.

بالإضافة إلى مكاتب المساعدة ومراكز الاتصال، طورت بعض المجالات الوظيفية مثل صيانة الطائرات إجراءات متعددة للإبلاغ عن الأخطاء المشبوهة في البيانات التقنية والتحقق منها. يمكن لعاملي الصيانة الذين يشككون في البيانات التقنية تقديم بلاغ حول التناقضات إلى مكاتب البرامج باستخدام النموذج رقم 22.[56] يوجه العامل هذه البلاغات، عبر الجناح إلى القيادة الرئيسية، ثم إلى المؤسسة الناشئة المسؤولة عن المسألة التقنية التي بلّغ عنها العامل (مثل مكتب

[54] تعليمات القوات الجوية 23-101، 2016. القسم 5.9.9.5؛ تعليمات القوات الجوية 21-201، 2015، القسم 7.9.3.

[55] تعليمات القوات الجوية 23-201، 2014، القسم 6.10.

[56] الدليل التقني TO 00-51-1، 2014، القسم 9.

البرنامج).[57] حين لا تتعامل بيانات النظام التقني مع مشكلة ما بشكل مناسب، يتعين على عمال الصيانة القيام بإجراء منفصل يتمثل في إرسال طلبات المساعدة التقنية إلى الأفراد الذين يملكون خبرة هندسية، ولهذا الإجراء اسم غير رسمي هو "طلبات 107"، وسميت بذلك وفقًا للنظام التقني المرتبط بها.[58] تُعدّ كلتا الآليتين من آليات التبليغ رسمية ومألوفة لجميع عمال الصيانة، كما أنها تقدم وسائل إبلاغ عن مخاوف محددة متعلقة بسلامة البيانات.

يمكننا التعميم أنه كلما كانت خطورة الخطأ المحتمل في البيانات أكبر، كانت آليات الإبلاغ والتقييم الخاصة في المجالات الوظيفية اللوجيستية الفردية أكثر رسمية وتطورًا. وفي مجال الإمداد والنقل، والذي تكون فيه الأخطاء الفردية شائعة نسبيًا وبشكل عام لا تترك أثرًا فوريًا على العمليات، تقتصر آليات الإبلاغ وإجراءات التقييم بشكل رئيسي على مراكز الاتصال والتواصل المباشر مع الأطراف المعنية بالعملية. في عمليات الصيانة والتخلص من الذخائر المتفجرة، والذي تكون فيه البيانات التقنية دقيقة ومحددة لتجنّب وقوع أية عواقب وخيمة، تم تطوير آليات متعددة. وتشكل هذه الآليات إجراءات محددة بشكل رسمي مع آلية مساءلة واضحة.

غالبًا ما تتضمن آليات الإبلاغ الخاصة بالمجالات التي قد تؤثر أخطاء البيانات فيها على سلامة الطيران أو توفّر الطائرات، مثل البيانات التقنية الخاصة بصيانة الطائرات وقطع الطائرات، شكلاً من تحديد الأولويات والمدة الزمنية المتوقعة لإيجاد حل لها. على سبيل المثال، تُعطى طلبات قطع الغيار رموز تأثير المهمة وتحمل محددًا في نظام البلاغات يتيح وضع إشارة على القطع التي تنطبق عليها حالة القدرة على أداء المهمة (MICAP) وإعطائها الأولوية.[59] وتصنّف بلاغات النموذج رقم 22، وفقًا لمستوى الأولوية بين حالات طارئة أو ملحّة أو روتينية. وكذلك طلبات 107 قد تصنّف حالات روتينية أو ملحّة أو فوريّة أو طارئة. وتساعد هذه التصنيفات في ترتيب البلاغات من حيث أولوية التقييم وغالبًا من حيث المدة اللازمة للاستجابة.

لاحظنا وجود عدد من الآليات التي قد تُساعد في الإبلاغ عن التلف المشتبه فيه بالبيانات. معظم هذه الآليات لا تتطلب جهدًا، ويشكل استخدامها جزءًا من التدريب المعياري. غير أنه لأغراض تتعلق بالعمليات اللوجيستية المتينة والمرنة في مواجهة الهجمات الإلكترونية، لا تستوفي هذه الآليات جميع المعايير المذكورة سابقًا ضمن هذا الفصل. لقد حددنا عددًا من الثغرات في آليات التقييم الحالية.

- لا توفر للعاملين طرقًا شاملة للإبلاغ عن جميع حوادث تلف البيانات المحتملة. كما أنها مقيدة بأنواع بيانات وأنظمة بيانات ومجالات وظيفية محددة.
- تضع العبء على العامل لتحديد آلية الإبلاغ المناسبة لأي حادث.
- ليست في متناول جميع العاملين، حيث إن العديد من هذه الآليات مخصصة للطيارين في وظائف معينة وليست متوفرة لجميع المدنيين والمتعاقدين الذين يتعاملون مع البيانات ويعدّون من مقدمي البلاغات المحتملين.
- لا تُقدم منظورًا على مستوى المؤسسة للمشاكل يتيح رصد هجوم منسّق عابر للمجالات الوظيفية أو المؤسسات.

[57] الدليل التقني TO 00-5-1، 2014 القسم 9.6.

[58] الدليل التقني TO 00-25-107، 2011

[59] تعليمات القوات الجوية 23-101، 2016

- لا تقيّم سبب وقوع الحادثة بشكل كامل، ولا تؤرشف الدروس المستفادة منها ولا تنشر هذه المعلومات بشكل منهجي لمراجعة السياسات والتعليم والتدريب.
- ليست سريعة بشكل عام بما يكفي للرد على جميع أنواع الهجمات المحتملة.
- لا تحدد بشكل شامل أولوية كل حادث ولا مدة الاستجابة اللازمة.
- في بعض الحالات، تفرض عبئًا غير ضروري على العاملين للقيام بالإبلاغ. على سبيل المثال، على العامل الذي يشك في صحة بيانات تقنية مصدرها القوات الجوية أن يملأ طلبًا بناءً على النموذج رقم 22. ولكن إذا كان مصدر هذه البيانات التقنية أحد المتعاقدين، تختلف الإجراءات ويتعيّن على العامل كتابة رسالة عبر القيادة الرئيسية إلى مكتب البرنامج المناسب. تعتمد طبيعة استجابة المتعاقد على اللغة المعتمدة في العقد والتي يعمل بموجبها.[60] يمكن تبسيط هذه العملية من خلال اعتماد آلية واحدة للتبليغ يتبعها جميع العاملين، ووضع عبء توجيه عملية التقييم على مكتب البرنامج (أو على متلق آخر).

هيكل مقترح للاستجابة لعمليتي الإبلاغ والتقييم

يمكن للقوات الجوية الأمريكية الاستفادة من آليات الإبلاغ والتقييم المستخدمة حاليًا والتي وصفنا بعضها في القسم السابق، لدعم الجهد الأوسع الذي من شأنه أن يجعلها أكثر متانة ومرونة. ومن شأن إكمال هذه الآليات بعدد قليل من الإجراءات والمؤسسات الإضافية أن يقضي إلى حد كبير على الثغرات الموجودة في عملية التقييم التي حددناها سابقًا. يبيّن الشكل 4.1 الهيكل العام المقترح، ويرد وصفه في الجزء المتبقي من هذا القسم. نعمل على تقسيم الأدوار والمسؤوليات بين الخدمات اللوجيستية (الدعم القتالي) وعوالم العمليات الإلكترونية، وتحديد المزيد من التفاصيل المتعلقة بالجانب اللوجيستي.

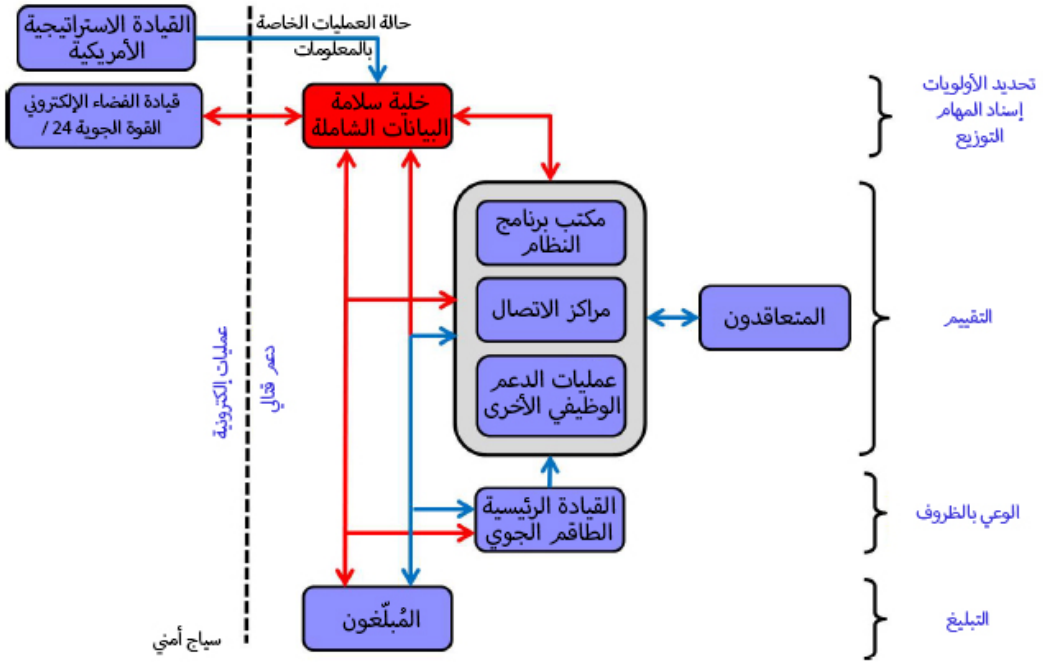
العمليات اللوجيستية

سنبدأ مع الجانب الأيسر للشكل 4.1 الذي يوضح تقييم العمليات اللوجيستية. في هذا الشكل، تظهر العناصر البنيوية الحالية (قنوات ومنظمات التبليغ) بالأسود والأزرق أما العناصر الجديدة المقترحة فباللون الأحمر. عند قراءة الشكل من أسفل إلى أعلى، نرى أنّ الطيارين والمدنيين والمتعاقدين (مشار إليهم في المربع المعنوَن "المُبلّغون") يبلّغون عن البيانات التي يشتبهون بتعرّضها للإتلاف، أما الخط الأسود فيمثّل قنوات التبليغ العديدة الموجودة (مثل مكاتب المساعدة والتقارير بناءً على النموذج 22 والطلبات 107). تصل هذه التقارير إلى منظمات مختلفة كي تخضع لشكل من أشكال التقييم (مثل مكاتب البرامج ومراكز الاتصال ووكالة لوجيستيات الدفاع) وغالبًا ما يتم توجيهها إلى منظمات أخرى بهدف نشر الوعي بالظروف (مثل موظفي قيادة رئيسية)، كما هو موضح في المربع الموجود على يمين القوس بعنوان "الوعي بالظروف". بعد انتهاء عملية التقييم، تُرسل بعض الملاحظات إلى الأفراد الذين رفعوا التقرير. وفي حالات قليلة، قد تؤدي هذه الملاحظات إلى تغيير السياسة أو التوعية أو التدريب، إلّا أنه لا يتم تطبيق أي من هذه الحلول بشكل منتظم حاليًا.

[60] الدليل التقني TO 00-5-1، 2014، القسم 9.

لا توجد سلطة مطلعة على جميع التقارير التي رُفعت حاليًا بهدف تقييمها لمعرفة ما إذا كان هناك هجوم منسق أم لا. كما لا توجد سلطة مركزية تتحمّل المسؤولية عن تحديد السبب وراء أي تلف كبير يصيب بيانات حساسة ونشر معلومات سببية حول كيفية معالجته.

الشكل 4.1 هيكل الاستجابة المقترح لعمليتي الإبلاغ والتقييم



ملاحظات: تشير الخطوط الزرقاء إلى القنوات الموجودة. أما الخطوط والمربعات الحمراء فتشير إلى القنوات والكيانات الجديدة المقترحة. GLODIC (Global Data Integrity Cell) تعني خلية سلامة البيانات الشاملة، وتعني MAJCOM (major command) قيادة رئيسية، وSPO (system program office) تعني مكتب برنامج النظام، أما USCYBERCOM (U.S. CyberCommand) فهي قيادة الفضاء الإلكتروني الأمريكية، وUSSTRATCOM (U.S.Strategic Command) فتعني القيادة الاستراتيجية الأمريكية

بالتالي، نقترح إنشاء هيئة مركزية جديدة تحت اسم "*خلية سلامة البيانات الشاملة*" (Global DataIntegrity Cell GLODIC) التي ستحصل على نسخ من جميع هذه التقارير. سوف تحافظ هذه الخلية على قدر من الوعي بالظروف على مستوى المؤسسة بجميع التقارير الموجودة. ونظرًا إلى أنّه تم اتخاذ إجراءات بشأن هذه التقارير من قبل القائمين على عملية التقييم، وتم تحديدها في السياسات التي تحكم آليات التبليغ الحالية، سيكون الجزء الأكبر من دور هذه الخلية تجاه هذه التقارير هو البحث عن الاتجاهات السائدة والهجمات المنسقة المتوقعة واستخلاص الدروس مع الوقت والقيام بدور مركز لتبادل المعلومات حول الدروس المستقاة.

نظرًا إلى أنّ التقارير الحالية لا تغطي جميع الحوادث المحتملة وليست في متناول جميع العاملين، وبالأخص المتعاقدين، تظهر الحاجة إلى آلية تكميلية لإعداد التقارير لسد هذه الثغرة. سوف تُكرس هذه الآلية للإبلاغ عن تلف

البيانات المشبوهة وغيرها من الهجمات الإلكترونية المحتملة؛ كما هو موضح بالخط الأحمر الذي يربط "المبلّغين" مع خلية سلامة البيانات الشاملة (GLODIC). أول ما ستقوم به الخلية هو الفرز. قد يكون هناك بعض البلاغات الزائفة أو المتكررة، لذلك تعطي الخلية الأولوية للبلاغات التي تجتاز عملية الفرز وتحدد السرعة المطلوبة لتقييمها وتوكلها إلى مقيِّم رئيسي، ومن ثم توزّع البلاغ على منظمة أخرى قد تحتاج إليه من باب الوعي بالظروف. يمكن أن يستفيد القائم على المُقيّم من مجموعة كاملة من المؤسسات التي تملك المعرفة المطلوبة، تشمل مؤسسات القوات الجوية الأمريكية الأخرى والمتعاقدين والوكالات الأخرى (على سبيل المثال وكالة لوجيستيات الدفاع). ويهدف التقييم بشكل رئيسي إلى تحديد ما إذا كان الحادث خطأ حقيقيًا، وإذا كان كذلك، فهل هو خطأ عادي أم هجوم محتمل. هذه هي المعلومات الرئيسية التي يجب على خلية سلامة البيانات الشاملة تتبعها.

لسد أكبر عدد ممكن من الثغرات في عملية التبليغ، يجب أن تكون هذه القناة سهلة الاستخدام، ربما من خلال تصميمها على غرار العملية رقم 107 التي يستعملها عمال الصيانة، كما يجب أن تحافظ على سرية المبلّغ. من شأن النقطة الأخيرة أن تشجع مشاركة المتعاقدين وأعضاء القوات الجوية الأمريكية الذين قد يخشون من عقاب الأفراد الذين يشغلون مناصب قيادية عليا. يمكن للمُقيّم إما إرسال التقييمات بشكل مباشر إلى المبلّغ أو إرسال نسخ إلى خلية سلامة البيانات الشاملة، أو أن تقوم الأخيرة بإرسال التقييم إلى المبلغ.

يجب أن تتمتع خلية سلامة البيانات الشاملة بالخبرة الكافية للقيام بعملية الفرز وتحديد الأولويات وتعيين مُقيّم رئيسي. كما يجب أن يكون لديها معرفة مؤسسية كافية لتعرف أي مؤسسات يجب أن تبلّغ من أجل نشر الوعي بالظروف. وتحتاج إلى أن يكون لديها وضعية تتيح لها تكليف المقيّمين والحصول على استجابات فعالة وفي الوقت المناسب.

لا توجد مؤسسة واحدة تنطبق عليها جميع هذه الخصائص بشكل مثالي، ولكن قد تكون مديرية الهندسة والإدارة التقنية التابعة لقيادة الإمدادات في القوات الجوية (AFMC/EN) الموقع المحتمل لخلية سلامة البيانات الشاملة. نتوقع إجراء معظم عمليات التقييم في مكاتب البرامج التابعة لمركز إدارة دورة حياة القوات الجوية أو في مركز دعم القوات الجوية أو وكالة لوجيستيات الدفاع. إنّ موقع مديرية الهندسة والإدارة التقنية التابعة لقيادة الإمدادات في القوات الجوية مناسب لأول مهمتين. وعلاوة على ذلك، تتركز خبرات الأمن الإلكتروني في نظام الأسلحة التي تساعد في تحديد الأولويات والدروس المستفادة في قيادة الإمدادات في القوات الجوية.

أيًا كانت المنظمة التي ستقوم بدور خلية سلامة البيانات الشاملة، فستحتاج إلى زيادة عدد العناصر فيها. ورغم أنّ تقييم المهارات وتحديد حجم القوى العاملة اللازمة لمثل هذه المؤسسة هما خارج نطاق هذه الدراسة، فإن اتساع نطاق الأنشطة المخصصة لخلية سلامة البيانات الشاملة بالإضافة إلى الوقت اللازم للاستجابة لن يكونا قابلين للإنجاز من خلال إضافة مهام جديدة إلى منظمة موجودة.

لا يبدو أنّ المؤسسات التي تتولى مهامًا إلكترونية خيارًا جيدًا لأنّ دور خلية سلامة البيانات الشاملة موجّه لأداء المهمة وليس إلى أمن المعلومات. فالأولوية تكمن في استمرار المهمة، وليس مجرد تكامل البيانات، ويجب أن تأتي هذه الرؤية من جانب العمليات اللوجيستية. ويتحمّل مدير أمن نظام المعلومات مسؤولية تحسين الأمن الإلكتروني واستعادة العمليات بعد أي فشل إلكتروني.[61] ومع ذلك، فإنّ أمن المعلومات هو جزء أساسي من التقييم. صحيح أنه ليس محور هذا التقرير، ولكن هناك حاجة إلى إجراء نقاش للتأكد من اكتماله.

[61] تعليمات القوات الجوية 33-210، 2008، دمج التغيير 1، 2 تشرين الأول (أكتوبر) 2014؛ الدليل التقني TO 33-1-38، 2015.

عمليات إلكترونية

لا يعتبر نقاشنا هنا حول عملية التقييم من جانب العمليات الإلكترونية مكتملاً بالضرورة. فتركيزنا ينصب على تلك العناصر الضرورية لدعم وظائف خلية سلامة البيانات الشاملة المقترحة بشكل مباشر. ويتمثل النشاط الداعم المقترح الأول في إصدار بيان بحالة العمليات الخاصة بالمعلومات (INFOCON). فصحيح أنّ مستوى حالة هذه العمليات الذي يصدره قائد القيادة الاستراتيجية الأمريكية عالمي، إلا أنه بإمكان القادة أن يحددوا مستويات أكثر صرامة لحالات العمليات للأنظمة التي يتولّون قيادتها. كما هو موضح في الفصل الثالث، يقود مستوى حالة العمليات الخاصة بالمعلومات إلى إنشاء هيكل استجابة متدرج للبلاغات والإطارات الزمنية للتقييم ولإجراءات التخفيف *داخل وحدة الخدمات اللوجيستية*. ستتدفق حالة العمليات الخاصة بالمعلومات إلى داخل خلية سلامة البيانات الشاملة، وبالتالي ستُوزعُ على جميع العاملين. سيحدد كل مجال وظيفي ضمن سياسته كيفية تأقلم عملياته مع كل مستوى من حالة العمليات الخاصة بالمعلومات. ونؤكد هنا أنّ الإجراء الوحيد الذي تتخذه الوحدة الإلكترونية هو تحديد مستوى حالة العمليات الخاصة بالمعلومات؛ بينما تقوم الوحدة اللوجيستية بجميع الإجراءات الأخرى وفقًا للسياسات التي وضعتها الوحدة اللوجيستية حول كيفية الاستجابة لمختلف مستويات حالات العمليات الخاصة بالمعلومات.

يتمثل النشاط المقترح الثاني لدعم وظائف خلية سلامة البيانات الشاملة في تقييم ما إذا حدث هجوم إلكتروني أم لا. ويجب أن يتم التقييم من قبل أصحاب الخبرة وليس بالضرورة من قبل منظمة مركزية. أما بالنسبة لأنظمة الأسلحة، قد تكمن الخبرة في قيادة الإمدادات في القوات الجوية. أما أنظمة تكنولوجيا المعلومات المتصلة بالشبكة، فتكمن الخبرة المطلوبة للتعامل معها في القوة الجوية الرابعة والعشرين. ولكن مع وجود خلية سلامة البيانات الشاملة، ستحتاج بعض المنظمات إلى تشكيل وجهة نظر خاصة بالمؤسسة وأرشفة الحوادث وتعميم الإرشادات. وقد تشمل الإرشادات عزل النظام عن الشبكات وتغيير الإجراءات وإغلاق الأنظمة من أجل الأدلة الجنائية أو عدم القيام بذلك. نسمّي هذه المنظمة *خلية ضمان المعلومات الشاملة* (GLOIAC). لا توجد ضرورة لإرسال جميع البلاغات لهذه المنظمة، بل فقط تلك التي تشير إلى احتمال وجود هجوم إلكتروني.

ملخص

تحترم الهيكلية التي نقترحها للتقييم المعايير الخمسة وهي (1) الشمولية و(2) حسن التوقيت و(3) سهولة الاستخدام و(4) حماية العاملين من الاتهامات المضادة التي قد تنشأ عن التبليغ من خلال السرية و(5) أن تكون في متناول جميع العاملين. من شأن هذه الاقتراحات أن تملأ الثغرات الموجودة في آليات التبليغ والتقييم الحالية بطريقة اقتصادية من خلال العمل على الإضافة إلى العمليات القائمة والمنظمات بإضافات بسيطة، خلية وحدة سلامة البيانات الشاملة، من أجل تحديد الأولويات وإيكال المهام واستخلاص الدروس من الحوادث، بالإضافة إلى قناة سرية صُمِمَت بناءً على طلبات 107 للإبلاغ عن مشاكل إلكترونية مشتبه بها.

5. ترتيب الجهود من حيث الأولوية

نظرًا إلى الكم الهائل من البيانات التي يُحتمل أن تكون خاطئة والعدد الكبير من الوظائف اللوجيستية التي تدعمها هذه البيانات، تحتاج الوحدات اللوجيستية إلى اتباع طريقة معينة لترتيب الجهود من حيث الأولوية للكشف عن البيانات الشاذة وتقييمها والتخفيف من آثارها السلبية المحتملة. في هذا الفصل، نتوجه إلى التساؤل متى يكون الاهتمام بالبيانات الشاذة أكثر حيوية ومتى تكون المخاطرة مقبولة.

ما الذي يجب أن تتضمنه عملية تحديد الأولويات

من المرجّح أنّ ثمة طرقًا موجودة أساسًا للتخفيف من أثر بعض أخطاء البيانات. فقد يطوق العاملون البيانات من خلال الاتصال المباشر مع وحدة أخرى أو مقارنة البيانات بمصدر موثوق آخر، كسجل ورقي. ومن العوامل التي يمكن إدراجها ضمن ترتيب أولويات المخاطر وجود إجراءات تخفيفية وقائية. على سبيل المثال، إذا أُخذت الإجراءات التخفيفية المحتملة بعين الاعتبار عند تحديد الأولويات، فإنّ خطأ محتملاً في البيانات قد يقود إلى آثار سلبية وخيمة على العمليات سيعتبر خطرًا بسيطًا إذا توفرت إجراءات تخفيفية وقائية. في المقابل، فإنه من الممكن استثناء الإجراءات التخفيفية المحتملة من الأولويات ووضعها بعد المخاطر عند معالجة كيفية التخفيف من المخاطر. في هذه الحالة، فإنّ خطأً محتملاً في البيانات قد يقود إلى آثار سلبية كبيرة على العمليات وقد يعد عالي الخطورة حتى لو كان هناك إجراء تخفيفي بديهي.

لدى كل من هاتين المقاربتين إيجابياتها وسلبياتها. فالمطالبة بإدراج الإجراءات التخفيفية المحتملة في عملية تقييم المخاطر سيقلل وعلى الفور من عدد السيناريوهات المثيرة للقلق والتي تعتبرها كلتا المقاربتين حرجة والتي لا تملك إجراءات وقائية واضحة. فالجهود التي تُبذل بهدف لفت الانتباه إلى المخاطر التي ليس لديها حلول لا تعد جهودًا ضائعة.

إلا أنّ هذه المقاربة تنطوي على ثلاثة مخاطر. يكمن الخطر الأول في إتمام تحليل المخاطر وتحديد الأولويات، حيث يجب استكشاف جميع الإجراءات التخفيفية الممكنة. وفي ظل العدد الهائل لأنواع المعلومات والآثار المحتملة لتلفها على العمليات، فإنّ استكشاف جميع الإجراءات التخفيفية الممكنة أمر غير ممكن. أما الخطر الثاني، فيتمثل في أنّ عدم فصل الإجراءات التخفيفية الممكنة عن عملية تقييم المخاطر يفشل في لفت الانتباه إلى حقيقة أنّ الإجراءات التخفيفية التي تجعل المخاطرة مقبولة هي *بحد ذاتها إجراءات تخفيفية حرجة*. ودمج الإجراءات التخفيفية في عملية تقييم المخاطر سيؤدي إلى إخفاء هذه الإجراءات التخفيفية الحرجة. من المهم تحديد هذه الإجراءات وربطها ضمن السياسة بالمخاطر المتعلقة بها بحيث لا تتم إزالتها من دون النظر في دورها في التخفيف من المخاطر المرتبطة بها. أما الخطر الثالث، فهو أنّ ما يبدو أنه إجراء تخفيفي موثوق أثناء عملية التحليل قد يتبيّن أنه غير فعال عند التطبيق. ما لم يتم تطبيق إجراءات التخفيف ضمن سيناريوهات هجوم واقعية، فهناك احتمال أن تكون فعّاليتها مجرد وهم.

لهذه الأسباب، نفصل بين عملية تقييم المخاطر وتحديد أولوياتها عن الإجراءات التخفيفية الممكنة.

استراتيجية لتحديد الأولويات

إنّ الصعوبة الذهنية الرئيسية التي تواجهنا خلال تحديد أولويات الوظائف اللوجيستية للتخفيف من أثر المخاطر وقبولها هي تجاوز حقيقة أنّ جميع الوظائف اللوجيستية ضرورية. فلو لم تكن ضرورية لما وُجدت من الأساس. ولكن الحاجة لجميع هذه الوظائف لا يعني أنّها تتساوى في الأهمية عند إنجاز المهام القتالية. في الأغلب، ليست العمليات اللوجيستية موجودة بشكل مستقل بل لدعم العمليات القتالية. تقترح وجهة النظر المشار إليها مباشرةً معيارًا لتحديد الأولويات حسب الأهمية وهو درجة تأثر العمليات القتالية بتلف البيانات اللوجيستية التي تدعم الوظائف اللوجيستية.[62]

وأخيرًا، هدفنا هو أنه حتى في الحالات التي تتعرض فيها المعلومات اللوجيستية للاختراق، يجب أن تحافظ العمليات القتالية التي تعتمد على هذه المعلومات على متانتها ومرونتها. بعد ذلك، ترتبط درجة حساسية الوظيفة اللوجيستية بمقدار تأثر متانة ومرونة العمليات القتالية بتلف البيانات اللوجيستية. ويُعدّ مفهوم الوقت مركزيًا للمتانة والمرونة.

الوقت

تعتمد متانة ومرونة العمليات القتالية للتصدي لتلف البيانات اللوجيستية على جدولين زمنين متنافسين: (1) زمن الاستجابة بعد إصابة البيانات بالتلف، وهو مجموع الوقت اللازم للكشف عن الهجوم (أو الخطأ العشوائي) وتقييمه والتخفيف من أثره والتعافي منه، و(2) الوقت الذي يستغرقه ظهور الأثر السلبي على العمليات القتالية بعد وقوع الهجوم (أو الخطأ العشوائي) على البيانات اللوجيستية، وهو الوقت الذي يستغرقه تأثر العمليات اللوجيستية بالإضافة إلى الوقت اللازم لتأثير العمليات اللوجيستية على العمليات القتالية. وكلما كان وقت الاستجابة أقصر، كانت العملية أكثر *مرونة*، وكلما طال الوقت اللازم ليؤثر الهجوم على العمليات اللوجيستية والعمليات القتالية، زادت متانة العمليات. إذا أشرنا إلى وقت الاستجابة بـ tr والوقت اللازم للتأثير على العمليات القتالية بـ t_o، فإنّ الهدف هو زيادة *الهامش الزمني* إلى أقصى حد $t_b = t_o - t_r$.

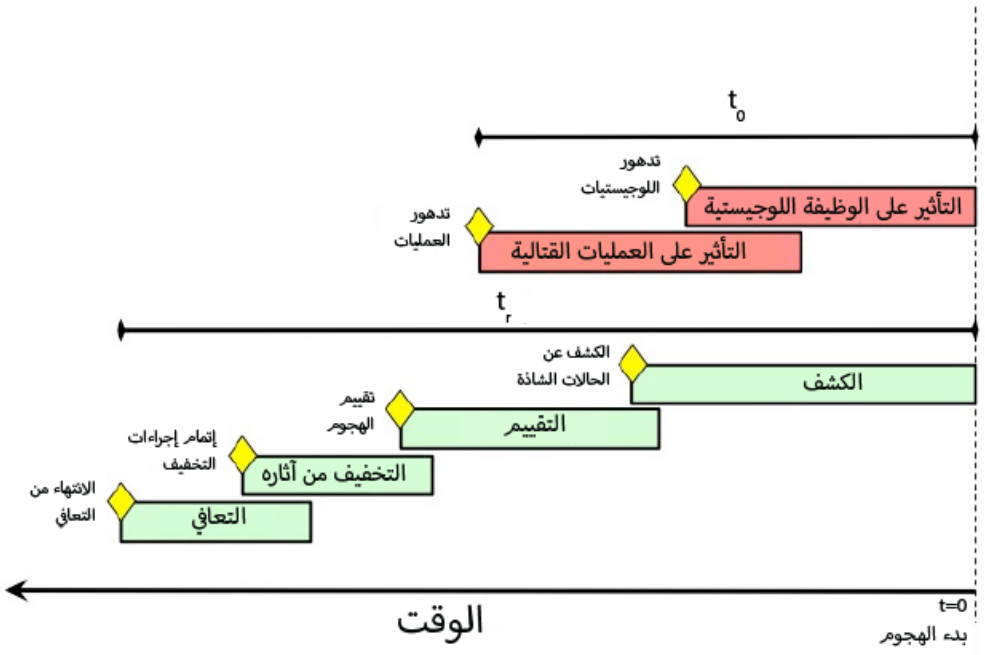
من المفيد عرض ترتيب الأولويات في إطار الهامش الزمني، تحديدًا حيث يمكن تحقيق أقصى قدر من الفعالية والكفاءة. يوضح الشكل 5.1 المفهوم العام. فيحدد في جزئه العلوي تسلسلاً زمنيًا افتراضيًا لأثر العمليات القتالية، يتألف من الوقت اللازم للتأثير على العمليات اللوجيستية ثم الوقت اللازم للتأثير على العمليات القتالية. قد يتداخل هذان المخططان الزمنيان معًا وقد يكونان مترابطين.

لتجسيد هذه المفاهيم، فكر في تلف البيانات في نظام التوريد، التلف البالغ ليوم واحد يؤدي إلى توقف الإمدادات إلى قاعدة العمليات الأمامية أثناء عمليات الطوارئ. ويعني توقف تدفق القطع أنّ هذه الوظائف اللوجيستية تأثرت في يوم واحد. إذا كانت الوحدة تحتوي على مخزون من قطع الغيار في حزمة قطع الغيار الجاهزة، فلن تتأثر العمليات القتالية إلى أن تظهر الحاجة إلى جزء لا تستطيع حزمة قطع الغيار الجاهزة توفيره. إذا استغرق هذا الأمر ثلاثة أسابيع، فإنّ وقت التأثير على العمليات القتالية هو ثلاثة أسابيع. أما إذا كان التأثير الأولي هو عدم توفر قطعة واحدة، فقد يكون التأثير على

[62] في هذا الفصل، سنحلل مكونات وجهة النظر المشار إليها باتباع الأعمال السابقة، 2015، إلى حد كبير ولكن سنوسّع هذا العمل لمعالجة بعض المشاكل المحددة المتعلقة بسلامة البيانات.

العمليات القتالية بتعطيل طائرة واحدة. ومن ثم، فإنّ الأثر سيكون تدريجيًا إلى حد ما، أو على الأقل لن يعطل الأسطول بأكمله دفعة واحدة. في هذا المثال، يكون وقت التأثير الكلي يومًا واحدًا وثلاثة أسابيع أو 22 يومًا، ويكون التأثير تدريجيًا إلى حد ما.

الشكل 5.1. الأطر الزمنية المتنافسة للتأثير على العمليات القتالية والاستجابة



ليست كل هذه الآثار حتمية. ولكن التزامن ضمن هذا الإطار الزمني بهدف إضعاف العمليات القتالية يمثل الزمن اللازم للاستجابة. والإطار الزمني للاستجابة هو الوقت الذي يستغرقه الاكتشاف عن البيانات الشاذة وتقييم ما إذا كانت تلك الحالة الشاذة خطأً ووضع خطة للتخفيف من أثر هذا الخطأ وتنفيذها وتعافي العمليات من الخطأ. وبالعودة إلى مثال سلسلة التوريد، لنفترض أنّ اكتشاف الخطأ يستغرق يومًا واحدًا وتقييم المشكلة يحتاج إلى يومين والتخفيف من أثرها وتعافي عمليات سلسلة التوريد والعودة إلى حالتها العادية تستغرق أسبوعًا إضافيًا، حينها يكون وقت الاستجابة عشرة أيام.

وبمقارنة هذا الوقت النظري للاستجابة الذي يبلغ عشرة أيام مع وقت التأثير النظري البالغ 22 يومًا، يكون الهامش الزمني إيجابيًا ويترك 12 يومًا إضافيًا احتياطيًا. وبذلك تكون المتانة والمرونة عاليتان بما يكفي لمواجهة التحدي المتمثل في مشكلة سلامة البيانات.[63] إذا استغرق وقت الاستجابة أكثر من 22 يومًا، فإنّ الهامش الزمني سيكون سالبًا ولن يكون النظام قادرًا على استيعاب تلف البيانات والاستجابة له في الوقت المناسب لتجنّب التأثير على العمليات

[63] إذا اعتمدنا مصطلحات أبحاث السلامة والحوادث، يمكننا القول أنه تم تجنب وقوع *حادث* بدلاً من القول إنّ المؤسسة واجهت *حادثًا وشيكًا*.

القتالية. وبهذه الطريقة، يمكن تقدير درجة أهمية سلامة البيانات اللوجيستية وتحديد ترتيبها ضمن الأولويات وفقًا للأولوية التي يتم تعويضها.

بشكل عام، من غير المحتمل أن تكون التقديرات دقيقة بدقة الـ22 يومًا. على الأرجح، أنها ستكون تقريبية وفقًا لحجمها التقريبي، مثل الساعات أو الأيام أو الأسابيع أو الشهور أو السنوات.

بعض عناصر هذه الأطر الزمنية غير ثابت ولكن يمكن تعديلها بدرجات متفاوتة قبل تعرّض البيانات للتلف أو بعد ذلك بشكل ديناميكي. في المثال الافتراضي للتوريد، يحدد مستوى توفر قطع الغيار في الحزمة الجاهزة للقطع مدى متانة التوريد. وكلما طالت المدة التي تستطيع فيها الحزمة الجاهزة للقطع دعم العمليات القتالية حتى وإن توقفت سلسلة التوريد إلى القاعدة، كانت وظيفة التوريد أكثر متانة. فزيادة هذا المخزون بشكل فعال توفر الوقت وتزيد من درجة المتانة. وبالتالي، يمكن إجراء تعديل مسبق على متانة التوريد في مواجهة تلف البيانات من هذا النوع وبشكل فعال على حساب مستويات جهوزية القطع.

بدلاً من ذلك، يمكن زيادة المرونة من خلال تقليل وقت الاستجابة، وذلك من خلال الاكتشاف أو التقييم أو التخفيف من الآثار أو التعافي السريع. ومن الطرق التي تقلل من هذه الأوقات، هي تقديم تدريب وإجراءات قياسية أفضل للاستجابة لتلف البيانات بشكل استباقي، كما هو موضح في الفصول السابقة في هذا التقرير. ولكن يمكن أيضًا ضبط وقت الاستجابة بشكل ديناميكي، بعد تلف البيانات، من خلال إعادة تحديد أولويات توزيع الجهود. إذا كانت إحدى الوظائف متينة نسبة إلى أخرى، يمكن قبول المخاطرة لهذه الوظيفة وإعادة تخصيص الموارد المحررة للوظيفة الأخرى الأقل قوة.

من الملاحظ أنه في بعض الظروف، يكون كلا عنصري الوقت اللازم للتأثير في العمليات القتالية والوقت اللازم للاستجابة هما ثابتين بطبيعتهما. وإذا تدهورت القدرة على صيانة الطائرات، فلا يمكن لعمليات الصيانة السابقة أن تعوّض عن تلك الخسارة. ولأنه من غير الممكن تعديل الإطار الزمني لهذا النوع من الوظائف، فإنّ الأخيرة تعوق القدرة على تنفيذ المهمة بعد حادث أصاب البيانات بالتلف ويجب التخفيف من آثاره بوسائل أخرى.

من العوامل التي تؤثر في وقت الاستجابة وتستحق اهتمامًا خاصًا لأنها قد تستغرق وقتًا طويلاً للغاية، هي: الوقت اللازم للتعافي. تؤثر أخطاء البيانات بطرق مختلفة على الإطار الزمني، وفقًا لطبيعة الإجراءات المتخذة بالاعتماد على البيانات. إذا تم شحن قطعة إلى موقع غير خاطئ، يكون وقت التعافي هو الوقت اللازم لشحن القطعة إلى الموقع الصحيح. ولكن إذا كان الإجراء المتخذ يدمر نوعًا واحدًا من أنواع القطعة بالكامل (بسبب وجود رمز خاطئ في نظام الجرد)، فإنّ وقت التعافي الذي يتكوّن من الوقت اللازم لأداء المهام الإدارية ومهام شراء قطعة جديدة، قد يكون طويلًا إلى حد ما وقد يصل في بعض الأحيان إلى سنة أو أكثر. وتعطى الأولوية للحالات التي يكون وقت التعافي فيها طويلاً بطبيعته، كحالات تدمير القطع، على حساب حالات الشحن إلى موقع خاطئ على سبيل المثال، في حال تساوت جميع العوامل الأخرى.

يقدم هذان الخياران، في المثال، من خلال زيادة الوقت اللازم للتأثير عبر زيادة المخزون المحلي لقطع الغيار وتقليل الوقت اللازم للاستجابة، فضاءً تجاريًا. إذا لم تكن وظيفة لوجيستية معينة متينة بما فيه الكفاية، فقد يتطلب ضمان أدائها استثمارًا لجعلها أكثر مرونة. عندما يكون شراء المتانة خيارًا متاحًا لبعض الوظائف اللوجيستية (مثل الحزم

الجاهزة للقطع وتخزين وقود الطائرات)، قد يكون من الأفضل تخصيص الموارد لتقليل الوقت اللازم للاستجابة للوظائف التي لا تستطيع الاستثمارات البسيطة الزيادة من قوتها (مثل صيانة الطائرات).

الهجمات الاحتمالية

يشكل الوقت بعدًا واحدًا لتحديد الأولويات، ومن المهم أيضًا معرفة مدى احتمال وقوع إحدى وظائف الخدمات اللوجيستية فريسة عطل بسبب تلف البيانات. يتطلب تقدير مدى احتمال تعرض نظام البيانات لهجوم إلكتروني فهم بعض التكوينات المحددة للأنظمة وعادات مشغّلي النظام (يمتد كلاهما للمدى الذي يصله أي متعاقد)، بالإضافة إلى فهم قدرات الخصوم ونواياهم بشكل عام. تتغير هذه العوامل بشكل شبه مستمر، وتقدير العادات التي قد يتبعها المشغّلون في المستقبل لا يمكن الاعتماد عليه على الأغلب. لذلك، فإنّ تقدير الحساسية تجاه الهجمات قد يحتاج إلى موارد مكثفة إلا أنه حافل بالشك في دعم التخطيط. هناك حاجة إلى الوصول لتقدير أبسط يأخذ التصنيف العام للحساسية تجاه الهجوم بعين الاعتبار.

لذلك، نسعى إلى الوصول إلى بديل عن احتمال وقوع هجوم إلكتروني يتلف بيانات أحد أنظمة البيانات. ويهدف ذلك إلى تقدير مدى الحساسية تجاه الهجمات، وليس لقياس قابلية التعرض لهجوم. أي أنّ الهدف هو تصنيف مستوى الحساسية تجاه الهجمات وليس تقييمه. يمكن القيام بالتصنيف وفقًا للوضع الأمني النسبي لنظام تكنولوجيا المعلومات المضيف.[64] على سبيل المثال، يمكن اعتبار نظام على شبكة موجّه بروتوكول الإنترنت الآمنة أقل حساسية من النظام الموجود على شبكة موجّه بروتوكول الإنترنت غير الآمنة (NIPRNet) من عناصر تحكم بنية تحتية رئيسية عامة (PKI). يُعتبر النظام الذي تستضيفه شبكة موجّه بروتوكول الإنترنت غير الآمنة مع عناصر تحكم بنية تحتية رئيسية عامة أقل حساسية تجاه الهجمات مقارنة بنظام تستضيفه شبكة موجّه بروتوكول الإنترنت غير الآمنة من دون عناصر تحكم بنية تحتية رئيسية عامة. سيكون النظام الذي تستضيفه شبكة موجّه بروتوكول الإنترنت غير الآمنة من دون عناصر تحكم بنية تحتية رئيسية عامة أقل حساسية تجاه الهجمات من تلك الأنظمة الموجودة على شبكة الانترنت والتي تتم مشاركتها مع الشركاء العاملين في القاعدة الصناعية، وهكذا.

ملخص

يشكّل الوقت واحتمال التعرّض لهجوم ما بُعدين هامين لمستوى الخطورة، ويُعدّان عاملين أساسيين لتحديد أولويات الجهد. فالوقت يوفر العديد من الخيارات لاحتمال جعل بعض الوظائف اللوجيستية أكثر قوة قبل التعرض لأي حادث إلكتروني. أما احتمال التعرّض لهجمات احتمالية، فتقدّم تصنيفًا بسيطًا للأنظمة للمساعدة في ترتيب الجهود من حيث الأولوية. وبذلك يمكن وضع استراتيجية لتحديد الأولويات بالترتيب الآتي:

- وضع قائمة بالمهام (التي قد تبلغ العشرات) والوظائف التي تُنجز ضمن المجال اللوجيستي. يعتمد مستوى الدلالة في تفصيل المهام على عملية الاكتشاف التي تتم خلال الخطوات اللاحقة.
- لكل مهمة، يجب تحديد أنظمة البيانات الرئيسية التي تتحكم بالعملية أو أرشفة البيانات الموثوقة التي تُبنى عليها الإجراءات أو القرارات.

[64] Snyder et al., 2015.

- تصنيف مستوى حساسية أنظمة البيانات المشار إليها بناءً على الأمن النسبي لمستضيفي هذه الأنظمة.
- إذا اتخذت إجراءات بناءً على بيانات خاطئة في أي من هذه الأنظمة للبيانات، يجب تقدير الوقت الذي سيستغرقه ظهور الآثار السلبية على العمليات القتالية (ساعات أو أيام أو أسابيع أو شهور أو سنوات).
- إذا اتخذت إجراءات بناءً على بيانات خاطئة في أي من هذه الأنظمة للبيانات، يجب تقدير وقت الاستجابة على وجه التقريب، والذي قد يهيمن عليه الوقت اللازم للتعافي من الهجوم (ساعات أو أيام أو أسابيع أو شهور أو سنوات).
- مقارنة هذه الأوقات ومن ثم ترتيب المهام بناءً على ذلك.
- التخطيط للهامش الزمني للمهام تبعًا لمستوى حساسية أنظمة البيانات المرتبطة بها
- تحديد أولويات الجهود من خلال البدء بأزواج المهام التي تملك أقصر هامش زمني والتي تكون أنظمة بياناتها هي الأعلى قابلية للتأثر ووصولاً إلى تلك التي تملك أطول هامش زمني وأنظمة بياناتها هي الأقل قابلية للتأثر.

سنختتم هذا التقرير في الفصل التالي من خلال وضع هذا البحث ضمن السياق العام لتهديد إلكتروني أشمل.

6. نقاش ونتائج

لقد سلطنا في هذا التقرير الضوء على طرق تحسين الاستجابة لتلف البيانات في الأنظمة اللوجيستية. ناقشنا تحديد الأولويات وطرق تعزيز رصد البيانات التي يشتبه بتلفها والإبلاغ عنها، كما قدمنا هيكلاً لتقييم الأحداث والتعلم منها. الهدف المباشر من ذلك هو العمليات اللوجيستية المتينة والمرنة، والهدف النهائي هو العمليات القتالية المتينة والمرنة. ومع القدرة على العمل بصورة مرضية بالرغم من حدوث تلف في البيانات، فتلف البيانات هو مجرد جزء صغير من التهديدات الإلكترونية.

يمكن للبيانات والمعلومات أن تتعرّض للخطر بأساليب عديدة أخرى على يد خصم يتمتع بمهارات عالية: استخراج البيانات وحظر الوصول إليها وتدميرها بشكل كامل. يمكن للخصم أيضًا إحكام السيطرة على العمليات من خلال شن هجوم إلكتروني والتحكّم بها كما يشاء. لذلك، لتكون العمليات اللوجيستية متينة ومرنة بما يكفي للتصدي لأي هجوم إلكتروني (أي المتانة والمرونة اللوجيستية في التصدي للهجوم الإلكتروني)، فإنها تحتاج أيضًا إلى أن تكون متينة ومرنة لطيف كامل من الهجمات الإلكترونية المحتملة. وهذا يعني أنّ النتائج والتوصيات الواردة في هذا التقرير ليست سوى جزءٍ من إطار عمل كبير يهدف لردع الهجمات التي تُشن ضد الوحدات اللوجيستية وصدها. وقد لا تكون الاستجابة لتلف البيانات العنصر الأكثر أهمية في ذلك.

لتحقيق الاستفادة القصوى من توصياتنا، وضعنا الحجج الرئيسية في هذا التقرير قدر الإمكان لتكون عامة بما يكفي لمواجهة جميع أنواع الهجمات الإلكترونية. يمكن توسيع مخطط تحديد الأولويات الوارد في الفصل الخامس بسهولة ليشمل طيف كامل من الهجمات الإلكترونية. والأفكار المتعلقة بتحسين عملية الاكتشاف ليست بالأهمية نفسها بالنسبة لبعض أنواع الهجمات، مثل تدمير البيانات وحظر الوصول إليها، لأن هذه الهجمات في غاية الوضوح. ولكن يمكن لهذه الأفكار أن تكون مفيدة في الاكتشاف المبكر عن هجمات أقل وضوحًا. والطرق التي نوصي باتباعها لتشجيع التبليغ وتقييم البلاغات تجدي نفعًا مع جميع أنواع الهجمات الإلكترونية. ولذلك، نوصي بتطبيق هذه التدابير لطيف كامل من الهجمات الإلكترونية، وألا تقتصر على نطاق ضيق من تلف البيانات.

بالإضافة إلى التوعية والتدريب اللذين يزيدان من احتمال رصد الحوادث الإلكترونية والتبليغ عنها مبكرًا، نؤكد على أهمية تحديد مستوى الخطر الإلكتروني مثل حالة العمليات الخاصة بالمعلومات (INFOCON). تكمن أهمية تحديد مستوى الخطر الإلكتروني في دوره لتحقيق أحد الأهداف الرئيسية للبقاء في الفضاء الإلكتروني، لزيادة صعوبة مهمة الخصم قدر الإمكان باستخدام الحد الأدنى من الموارد. يوجه مستوى الخطر الإلكتروني استجابة تدريجية تحد بشكل استباقي من التأثيرات الإلكترونية السلبية بدلاً من انتظار حدوثها ومن ثم الاستجابة لها، وذلك من خلال جعل مستوى الخطر الإلكتروني معروفًا لدى الخصوم، كما يقوم بردع الهجمات.

العمليات المتينة والمرنة بشكل فعّال تنتج من توفر قوى عاملة مدربة بشكل جيد وتتفهم إمكانية وقوع خلل في العمليات نتيجة التعرض لهجوم إلكتروني، وتمتلك توجيهات واضحة تستند إلى مستوى الخطر الإلكتروني حول كيفية الاستجابة لهذه التهديدات وتملك الدعم من خلال الهيكل لـ 48 للتبليغ والتقييم. من شأن إرسال ردود الأفعال والآراء

على هذه التبليغات ونتائج التقييم إلى العاملين إغلاق هذه الحلقة وتشكيل منظومة للتعلّم تحافظ على المرونة والمتانة مع مرور الوقت.

المراجع

Air Force Doctrine Document 4-0, *Combat Support*, Washington, D.C.: United States Air Force, April 23, 2013.

Air Force Instruction 21-101, *Aircraft and Equipment Maintenance Management*, Washington, D.C.: Secretary of the Air Force, May 21, 2015.

Air Force Instruction 21-201, *Munitions Management*, Washington, D.C.: Secretary of the Air Force, June 3, 2015, certified current February 12, 2016.

Air Force Instruction 23-101, *Air Force Materiel Management*, Washington, D.C.: Secretary of the Air Force, January 29, 2016.

Air Force Instruction 23-201, *Fuels Management*, Washington, D.C.: Secretary of the Air Force, June 20, 2014.

Air Force Instruction 33-210, *Air Force Certification and Accreditation (C&A) Program (AFCAP)*, Washington, D.C.: Secretary of the Air Force, December 23, 2008, Incorporating Change 1, October 2, 2014.

Air Force Instruction 90-802, *Risk Management*, Washington, D.C.: Secretary of the Air Force, February 11, 2013, certified current as of March 23, 2015.

Aryee, Samuel, and Hsin-Hua Hsiung, "Regulatory Focus and Safety Outcomes: An Examination of the Mediating Influence of Safety Behavior," *Safety Science*, Vol. 86, 2016, pp. 27–35.

ASRS—*See* Aviation Safety Reporting System.

Aviation Safety Reporting System, homepage, undated. As of May 31, 2017: http://asrs.arc.nasa.gov/

Batey, Angus, "ALIS on Alert: Experts Warn of Cyber Gaps in F-35 Logistics System," *Aviation Week & Space Technology*, March 14–27, 2016, pp. 56–58.

Bennett, Simon, "The 1st July 2002 Mid-Air Collision Over Űberlingen, Germany: A Holistic Analysis," *Risk Management*, Vol. 6, No. 1, 2004, pp. 31–49.

Berger, Arno, and Theodore P. Hill, *An Introduction to Benford's Law*, Princeton, N.J.: Princeton University Press, 2015.

Boyle, Jeff, "An Application of Fourier Series to the Most Significant Digit Problem," *The American Mathematical Monthly*, Vol. 101, No. 9, November 1994, pp. 879–886.

Cesario, Joseph, E. Tory Higgins, and Abigail A. Scholer, "Regulatory Fit and Persuasion: Basic Principles and Remaining Questions," *Social and Personality Psychology Compass*, Vol. 2, No. 1, 2008, pp. 444–463.

Chairman of the Joint Chiefs of Staff Instruction 6510.01F, *Information Assurance (IA) and Support to Computer Network Defense (CND)*, February 9, 2011, directive current as of June 9, 2015.

Croft, John, "Problematic Probe: Inaccurate Airspeed Readings Due to Ice Crystals Prompted Unnecessary Dives on a United Flight," *Aviation Week & Space Technology*, May 23–June 5, 2016, pp. 32–33.

Crowe, Ellen, and E. Tory Higgins, "Regulatory Focus and Strategic Inclinations: Promotion and Prevention in Decision-Making," *Organizational Behavior and Human Decision Processes*, Vol. 69, No. 2, February 1997, pp. 117–132.

Defense Science Board, *DSB Summer Study Report on Strategic Surprise*, Washington, D.C.: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, July 2015.

Dekker, Sidney, "Resilience Engineering: Chronicling the Emergence of Confused Consensus," in Erik Hollnagel, David D. Woods, and Nancy Leveson, eds., *Resilience Engineering: Concepts and Precepts*, Burlington, Vt.: Ashgate, 2006, pp. 76–92.

Department of Defense Instruction 2000.16, *DoD Antiterrorism (AT) Standards*, October 2, 2006, incorporating Change 2, December 8, 2006.

de Vries, Peter W., Stéphanie M. van den Berg, and Cees Midden, "Assessing Technology in the Absence of Proof: Trust Based on the Interplay of Others' Opinions and the Interaction Process," *Human Factors*, Vol. 57, No. 8, December 2015, pp. 1378–1402.

Dijkstra, Arthur, "Safety Management in Airlines," in Erik Hollnagel, David D. Woods, and Nancy Leveson, eds., *Resilience Engineering: Concepts and Precepts*, Burlington, Vt.: Ashgate, 2006, pp. 183–203.

Durtschi, Cindy, William Hillison, and Carl Pacini, "The Effective Use of Benford's Law to Assist in Detecting Fraud in Accounting Data," *Journal of Forensic Accounting*, Vol. 5, No. 1, 2004, pp. 17–34.

Endsley, Mica R., "Toward a Theory of Situation Awareness in Dynamic Systems," *Human Factors*, Vol. 37, No. 1, 1995, pp. 32–64.

Higgins, E. Tory, "The 'Self-Digest': Self-Knowledge Serving Self-Regulatory Functions," *Journal of Personality and Social Psychology*, Vol. 71, No. 6, 1996, pp. 1062–1083.

Higgins, E. Tory, *Beyond Pleasure and Pain: How Motivation Works*, New York: Oxford University Press, 2012.

Hill, Theodore, P., "A Statistical Derivation of the Significant-Digit Law," *Statistical Science*, Vol. 10, No. 4, 1995, pp. 354–363.

Hill, Theodore P., "The Difficulty of Faking Data," *Chance*, Vol. 12, No. 3, 1999, pp. 27–31.

Hoff, Kevin Anthony, and Masooda Bashir, "Trust in Automation: Integrating Empirical Evidence on Factors That Influence Trust," *Human Factors*, Vol. 57, No. 3, May 2015, pp. 407–434.

Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, Washington, D.C.: Joint Chiefs of Staff, November 8, 2010 (as amended through February 15, 2016).

Kark, Ronit, Tal Katz-Navon, and Marianna Delegach, "The Dual Effects of Leading for Safety: The Mediating Role of Employee Regulatory Focus," *Journal of Applied Psychology*, Vol. 100, No. 5, 2015, pp. 1332–1348.

Lee, John, and Neville Moray, "Trust, Control Strategies and Allocation of Function in Human-Machine Systems," *Ergonomics*, Vol. 35, No. 10, 1992, pp. 1243–1270.

Lee, John D., and Katrina A. See, "Trust in Automation: Designing for Appropriate Reliance," *Human Factors*, Vol. 46, No. 1, 2004, pp. 50–80.

Madhaven, Poornima, Douglas A. Wiegmann, and Frank C. Lacson, "Automation Failures on Tasks Easily Performed by Operators Undermine Trust in Automated Aids," *Human Factors*, Vol. 48, No. 2, Summer 2006, pp. 241–256.

Merritt, Stephanie, and Daniel R. Ilgen, "Not All Trust Is Created Equal: Dispositional and History-Based Trust in Human-Automation Interactions," *Human Factors*, Vol. 50, No. 2, 2008, pp. 194–210.

Nigrini, Mark J., *Benford's Law: Applications for Forensic Accounting, Auditing, and Fraud Detection*, Hoboken, N.J.: John Wiley & Sons, 2012.

Parasuraman, Raja, and Victor Riley, "Humans and Automation: Use, Misuse, Disuse, Abuse," *Human Factors*, Vol. 39, No. 2, 1997, pp. 230–253.

Reason, James, "Achieving a Safe Culture: Theory and Practice," *Work and Stress*, Vol. 12, No. 3, 1998, pp. 293–306.

Reynard, W. D., C. E. Billings, E. S. Cheaney, and R. Hardy, *The Development of the NASA Aviation Safety Reporting System*, NASA Reference Publication 1114, November 1986.

Roney, Christopher J. R., E. Tory Higgins, and James Shah, "Goals and Framing: How Outcome Focus Influences Motivation and Emotion," *Personality and Social Psychology Bulletin*, Vol. 21, No. 11, 1995, pp. 1151–1160.

Schein, Edgar H., "Organizational Culture," *American Psychologist*, Vol. 45, No. 2, 1990, pp. 109–119.

Snyder, Don, George E. Hart, Kristin F. Lynch, and John G. Drew, *Ensuring U.S. Air Force Operations During Cyber Attacks Against Combat Support Systems: Guidance for Where to Focus Mitigation Efforts*, Santa Monica, Calif.: RAND Corporation, RR-620-AF, 2015. As of June 1, 2017:
https://www.rand.org/pubs/research_reports/RR620.html

Strategic Command Directive 527-1, *Department of Defense (DOD) Information Operations Condition (INFOCON) System Procedures*, January 27, 2006, not available to the general public.

Technical Manual TO 00-5-1, *AF Technical Order System*, Washington, D.C.: Secretary of the Air Force, October 1, 2014.

Technical Manual TO 00-25-107, *Maintenance Assistance*, Washington, D.C.: Secretary of the Air Force, August 15, 2011.

Technical Manual TO 33-1-38, *Cybersecurity for Automatic Test Systems and Automatic Test Equipment in FSC*, Washington, D.C.: Secretary of the Air Force, February 28, 2015, not available to the general public.

Thaler, Richard H., and Cass R. Sunstein, *Nudge: Improving Decisions About Health, Wealth, and Happiness*, New Haven, Conn.: Yale University Press, 2008.

Tyler, Tom R., and Steven L. Blader, "Can Business Effectively Regulate Employee Conduct? The Antecedents of Rule Following in Work Settings," *Academy of Management Journal*, Vol. 48, No. 6, 2005, pp. 1143–1158.

Weick, Karl E., and Kathleen M. Sutcliffe, *Managing the Unexpected: Assuring High Performance in an Age of Complexity*, San Francisco, Calif.: Jossey-Bass, 2001.

Woods, David D., "How to Design a Safety Organization: Test Case for Resilience Engineering," in Erik Hollnagel, David D. Woods, and Nancy Leveson, eds., *Resilience Engineering: Concepts and Precepts*, Burlington, Vt.: Ashgate, 2006, pp. 315–325.

تعتمد العمليات اللوجيستية على المعلومات الدقيقة، فحتى الأخطاء الصغيرة نسبيًا في أنظمة الدعم تترك أثرًا كبيرًا على العمليات في بعض الأحيان. ولكن حدوث الأخطاء أمر محتّم، لذلك يجب أن تمتلك العمليات اللوجيستية المتانة اللازمة لمواجهة الأخطاء سواء أكانت عشوائية أم نتيجة هجوم إلكتروني متعمّد وموجّه. طلبت القوات الجوية الأمريكية من مشروع RAND للقوى الجوية تحديد المواضع التي يمكن أن تستثمر فيها القوات الجوية جهودها في إحداث تغييرات على الأساليب والتقنيات والإجراءات، وذلك بهدف تحسين قدرة الطيار على اكتشاف أي تلف كبير في البيانات اللوجيستية وتقييمه والتخفيف من آثاره. وكان الهدف من ذلك هو معالجة الأخطاء الموجودة في البيانات قبل أن تترك أثرًا سلبيًا بالغًا في العمليات القتالية.

تمثل العمليات ذات الدرجة العالية من التشغيل الآلي، التي لا يرى الأفراد خلالها البيانات في العمليات العادية، تحديًا كبيرًا أمام عملية رصد أي خلل في البيانات. فرصد تلف البيانات أمر بالغ الأهمية في الحروب، ولكن الحالات الشاذة تكون أقل وضوحًا خلال الحروب بالمقارنة مع أوقات السلم، فالحرب بحد ذاتها حالةٌ شاذة. لذلك ثمة حاجةٌ لوجود آليات لتعديل آليات الرصد من ظروف السلم إلى ظروف الحرب. ولكي يتمكّن العاملون (من طيارين ومدنيين ومتعاقدين) من اكتشاف البيانات الشاذة، عليهم أن يخضعوا جميعًا للتدريب لفهم النمط الأساسي المتوقع، كما ينبغي أن يكونوا متيقظين بشكل متواصل عند تفحّص البيانات. وبالتوازي، يجب أن تتيح القيادة بيئة تشجع العاملين على الإبلاغ عن البيانات الشاذة المشبوهة.

تشمل التوصيات تحديد التدابير التي يجب أن يتخذها العاملون في المجال اللوجيستي، في إطار السياسة اللوجيستية، للاستجابةِ لمستوى كل حالة من حالات العمليات الخاصة بالمعلومات، وإنشاء كيان مركزي جديد (ربما داخل منظمة موجودة) تحت مسمّى "خلية سلامة البيانات الشاملة"، التي ستتلقّى جميع التقارير بشأن أي خلل مشتبه به في البيانات لنشر الوعي على نطاق المؤسسة.

RAND PROJECT AIR FORCE

www.rand.org

Arabic translation of
"Robust and Resilient Logistics Operations in a Degraded Information Environment"
RR-2015/1-AF