Biosecurity

A Systems Perspective

Edited by Susan M. Hester, Lucie M. Bland, Edith Arndt, Sana Bau, James S. Camac, Evelyn Mannix, Raphaël Trouvé and Andrew P. Robinson

First published 2024

ISBN: 978-1-032-18168-4 (hbk)
ISBN: 978-1-032-18169-1 (pbk)
ISBN: 978-1-003-25320-4 (ebk)

Chapter 6

Detect: Designing Post-Border Surveillance Schemes

DOI: 10.1201/9781003253204-9

The funder for this chapter is
University of Melbourne, School of Biosciences, Centre of Excellence for Biosecurity Risk Analysis (CEBRA), Australia

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

6 Detect
Designing Post-Border Surveillance Schemes

James S. Camac

ABSTRACT

Pre-border and border controls reduce (but do not eliminate) the risk of biosecurity threats entering a country, so regulators must prepare for the eventuality of pests and disease incursions. Post-border surveillance is the primary tool used to detect new outbreaks, delimit and manage existing outbreaks, declare eradication success, and provide evidence to trading partners that a threat is absent to gain or maintain market access. This chapter outlines the three broad types of post-border surveillance (active, general, and passive) and reviews their pros and cons. General and passive surveillance are useful sources of first detections but are of limited use for inferring the likelihood of threat absence, due to issues with unknown surveillance reliability and effort. Active surveillance can be used to inform multiple surveillance objectives, but its cost restricts its use to small geographic areas and high-risk threats. Overall, the amount of surveillance to be implemented depends on the objective of surveillance, the reliability of the surveillance method, and the regulator's tolerance for failing to detect a threat that is present. For all objectives, the surveillance strategy and effort required should represent best value for money (i.e. minimising the costs of surveillance and potential costs associated with the threat).

GLOSSARY

Area freedom Declaration of the absence of a threat from a region (e.g. a production zone) for the purposes of access to international or domestic markets.

Proof of freedom Declaring a threat as absent from a region after eradication measures have been successful.

Active surveillance A deliberate and coordinated surveillance effort designed to detect new or priority pests and diseases. Targeted surveillance is a form of active surveillance that is optimised to detect a particular threat.

General surveillance A semi-coordinated, multi-threat focused, surveillance effort commonly implemented by environmental stakeholders (e.g. park rangers), agricultural stakeholders (e.g. farmers, agronomists, vets, and industry organisations), scientists, and/or citizen science groups.

Passive surveillance The chance detection and reporting of threats by the public. Passive surveillance is the most fortuitous and accidental type of surveillance, with little structured or coordinated surveillance effort or reporting framework.

Sensitivity The probability a single surveillance unit (e.g. survey, trap, or test) will detect a threat assuming it is present. Imperfect sensitivity (<1) increases the likelihood of false negatives (i.e. declaring a threat absent when it is in fact present).

Surveillance effort A measure of the amount of effort undertaken to detect a threat, which could be in terms of the number of traps, survey hours, site revisits, or diagnostic tests.

DOI: 10.1201/9781003253204-9

Tracing An intelligence-gathering exercise that aims to identify an incursion's plausible means of introduction and secondary spread.

Natural detection point The point where the pest or disease becomes self-evident (i.e. 100% probability of detection), even without expenditure on active surveillance or additional passive surveillance.

INTRODUCTION

Pre-border and border controls attempt to reduce the risk of exotic species and diseases entering and establishing in a jurisdiction, but these controls do not eliminate risk entirely. A jurisdiction's biosecurity system reduces risk to an appropriate level of protection (ALOP) that balances trade-offs so that the risk of threat entry and establishment is acceptable by the public, industry, and trading partners (see Chapter 2. Biosecurity Systems and International Regulations). The consequence of not reducing risk to zero is that from time to time, even a well-managed biosecurity system will have post-border incursions that establish and spread. In an era of increasing globalisation (Hulme 2009, Seebens et al. 2017), regulators must plan for this eventuality.

Post-border surveillance is the primary tool regulators use to detect new outbreaks before they spread so widely that they become infeasible to eradicate and/or cause significant economic, social, and environmental impacts. It is also used to infer confidence that a threat is absent from a region of interest, which is important for both maintaining and regaining market access for some commodities. Post-border surveillance also plays a role in informing on-the-ground biosecurity response strategies.

This chapter describes the various objectives of post-border surveillance (namely area freedom, early detection, delimitation, and monitoring) and the surveillance methods that are most appropriate to achieving each. These methods (active, general, and passive surveillance) can all play an important role in detecting biosecurity threats. The practical considerations in selecting a method, including where to undertake surveillance, how to infer absence from surveillance data, and how much to spend on surveillance, are also discussed.

OBJECTIVES OF POST-BORDER SURVEILLANCE

Post-border surveillance provides the necessary evidence to inform four objectives: area freedom, early detection, incursion delimitation, and progress towards post-incursion management objectives (e.g. eradication or containment).

Surveillance for Market Access (Area Freedom)

To mitigate exposure to high-impact biosecurity threats, many countries (and some jurisdictions within countries) impose restrictions on the movement and trade of plants, animals, and associated goods. To export these items across international borders and to secure or maintain access to premium export markets, governments and industries are required to provide evidence to trading partners that their region or production zones are free from agricultural threats. This evidence of absence, referred to as area freedom, typically involves various forms of post-border surveillance complemented by other sources of information, such as scientific publications, research data, field observations, and other non-survey data (IPPC 2017). The quality and quantity of such evidence is ultimately governed by the requirements of the trading partner, the potential impact of a threat, and the international standards imposed by the World Trade Organisation (see Chapter 2. Biosecurity Systems and International Regulations). The globalisation of human movement and trade has resulted in countries becoming more exposed to new pests and diseases (Hulme 2009;

Seebens et al. 2017, 2021), so trading partners are increasingly requiring more evidence to support claims of area freedom. Data derived from post-border surveillance programs, particularly ongoing active surveillance programs, are often seen as the gold standard of evidence for area freedom.

Surveillance for Early Detection

Early detection is one of the main lines of defence against the widespread establishment and spread of exotic threats. Early detection surveillance is a form of ongoing monitoring that often complements surveillance for area freedom. However, unlike area freedom, the implementation of surveillance for early detection is not governed by the requirements of trading partners or international standards. Surveillance for early detection is underpinned by the central theory that incursions are an inevitability and that to minimise impacts and maximise the feasibility and cost-effectiveness of containment and eradication, regulators must detect new threats when populations are small and geographically restricted (Ahmed et al. 2022; Leung et al. 2002). Because this form of surveillance is not a mandate set by a trading partner or international body, governments and industry contend with the issue of whether to invest resources (e.g. infrastructure, people, and diagnostics) in the early detection of a potential future outbreak or to only deploy resources when an incursion is detected. This trade-off between prevention and reaction is governed by three factors: (1) the likelihood of an incursion; (2) its potential environmental, economic, and/or social impacts; and (3) the feasibility of containment and eradication (see Chapter 7. Prepare, Respond, and Recover).

Surveillance for Delimiting the Extent of an Outbreak

When an incursion occurs, determining the extent of the outbreak is critical. Delimiting an outbreak quickly and accurately can reduce the likelihood of further spread and maximise eradication success through targeted control measures. Initial detections can come from area freedom or early detection surveillance programs, industry stakeholders (e.g. farmers and agronomists), or the public. For example, outbreaks of exotic fruit fly (e.g. the oriental fruit fly *Bactrocera dorsalis*) can be detected by sophisticated pheromone lure traps, industry members, and citizens who notice their fruit tree has become infested.

Delimitation surveillance is a reactive but necessary process that occurs once an outbreak has been detected. Once a detection is made, biosecurity agencies undertake intelligence-gathering activities, commonly referred to as tracing, to identify plausible means of introduction and secondary spread (Leung, Cacho, and Spring 2010; Potts et al. 2013). Typically, these activities involve detailed discussions with landowners in the immediate vicinity of the initial detection (which may or may not be the point of introduction), expanding to other locations based on this information. This local intelligence gathering is used to construct a network of likely spread movements among properties, which can then be used in models that simulate the likely extent of post-border spread (IPPC 2016b). These data and models are ground-truthed by conducting threat-specific surveillance (i.e. targeted or active surveillance) to determine the true extent of the outbreak. Examples of formal tracing schemes include Australia's National Livestock Information System and New Zealand's National Animal Identification and Tracing (MAF 2009).

Surveillance for Threat Monitoring and Management Success (Proof of Freedom)

Once an outbreak has been detected and its extent has been determined, biosecurity practitioners are faced with deciding how to manage the infestation (see Chapter 7. Prepare, Respond, and Recover). Three management options are possible: (1) attempt eradication; (2) contain (i.e. prevent further spread); or (3) do nothing and shift resources to mitigating and adapting to impacts. If the decision is made to do nothing, there is little need for surveillance, as resources are allocated towards mitigation and adaptation strategies (see Chapter 7. Prepare, Respond, and Recover).

If eradication or containment is the objective, then surveillance becomes a critical tool for evaluating the effectiveness of control measures (see Chapter 10. Monitoring, Evaluation, and Reporting). For containment and eradication purposes, targeted surveillance will typically be positioned within the delimited area of infestation and in surrounding areas (IPPC 2016b). Surveillance within the outbreak area is focused on both monitoring and evaluating the success of control treatments and to provide evidence that the threat has been successfully eradicated. By contrast, surveillance surrounding an outbreak is focused on determining whether the outbreak is contained and not spreading outside the area of treatment. Both forms of surveillance are an essential requirement for declaring a threat has been successfully contained or eradicated (commonly referred to as proof of freedom).

How long such surveillance is maintained depends on the management objective. If the focus is eradication, then it will remain in place until a desired level of statistical confidence is reached such that proof of freedom can be declared (Ramsey, Parkes, and Morrison 2009; Rout 2017; Rout, Salomon, and McCarthy 2009). Alternatively, if eradication is deemed infeasible and containment is the goal, then surveillance may be ongoing, with management focusing on maintaining low numbers and reducing spread.

TYPES OF POST-BORDER SURVEILLANCE

A range of surveillance methods can be used to facilitate the early detection of new outbreaks, monitor and manage existing outbreaks, or provide evidence of eradication success or area freedom. Surveillance methods fall on a continuum that ranges from the deliberate and coordinated use of sophisticated surveillance methods that maximise the detection of a particular threat, to surveillance methods that attempt to benefit from chance detections and reporting made by the public (Hester and Cacho 2017). This continuum is categorised into three main types of surveillance: active surveillance, general surveillance, and passive surveillance (Figure 6.1).

Active Surveillance

Active surveillance (also referred to as targeted surveillance) is the deliberate and coordinated effort to detect new or managed pests and diseases. It is typically implemented by biosecurity regulators to meet specific objectives, such as to provide evidence of area freedom to trading partners, to delimit and contain an incursion, or to monitor the performance of an eradication or containment program.

Active surveillance uses sophisticated tools and survey methods that are highly effective in detecting a specific threat. For animal and plant diseases, this often involves planned regular surveys of hosts for signs of illness, coupled with routine sampling for diagnostics such as polymerase chain reaction (PCR) tests and antibody (i.e. serology) tests. For non-disease threats (e.g. invasive vertebrates, invertebrates, and weeds), active surveillance includes repeated site surveys using visual observations and tools such as pheromone lure traps, animal traps, acoustic monitoring, field cameras, seed bank analyses, or detector dogs. New technologies are increasingly used to enhance detection rates, including environmental DNA (eDNA) methods for detecting invasive species in ballast water and freshwater systems, drones and remote sensing, and machine learning for rapid and automated identification of priority threats (see Chapter 13. Profiling and Automation).

Data derived from active surveillance are the most reliable for inferring the presence or absence of a threat. Not only do active surveillance tools and methods have known likelihoods of detection (i.e. sensitivity) and known false positives (i.e. specificity), but they are also implemented by highly trained staff using proven protocols. These detailed protocols describe how and where surveillance should be implemented, what data should be collected (e.g. threat presence/absence and measures of surveillance effort), and how these data can be used to infer threat absence.

Active surveillance is the most resource intensive and costly form of surveillance (Anderson et al. 2017). As such, it is commonly used to delimit and contain outbreaks and to declare eradication

Surveillance continuum

Purposeful ⟷ **Opportunistic**

Surveillance Types	**Active surveillance**	**General surveillance**	**Passive surveillance**
Objectives	Early detection. Area freedom (market access). Incursion response (i.e. delimitation, monitoring containment/ eradication success).	First detection. Supplementary data for incursion responses (i.e. delimitation & management).	First detections of known & unexpected threats. Supplementary data for incursion responses (i.e. delimitation & management).
Methods	Detailed surveillance protocols. Typically threat-specific. Sophisticated monitoring & diagnostic tools.	Formal & informal surveillance protocols of varying detail. Typically multi-threat focused. Some industry/organisation guidelines.	No formal surveillance protocols. Any species/threat. Reliant on opportunistic chance encounters.
Data collectors	Biosecurity regulators (highly trained staff)	Industry & environmental stakeholders with variable training (e.g. farmers, agronomists, veterinarians, park rangers, scientists, conservation groups).	General public (little to no training)
Reliability (Sensitivity & Specificity)	High sensitivity & specificity.	Unknown or highly variable among individuals/groups. Expected to be greater for threats with impacts relevant to reporter/group.	Unknown. Expected to be greater for threats with visible/distinctive features or impacts.
Reporting	Detailed formal reporting protocols. Surveillance effort known.	Variable formal reporting protocols. Variable reporting likelihoods among industries. Dependent on incentives vs costs to individual. Surveillance effort rarely reported.	No formal reporting protocols. No incentives to report. Reporting occurs across many platforms Surveillance effort rarely reported.
Where (Extent & effort)	Most constrained extent. Production zones (*area freedom*) High risk locations (*early detection*) Within & surrounding outbreaks (*monitoring*)	Moderate geographic extent. Expected to be higher in areas where the impacts of incursion are likely to be greatest.	Greatest potential geographic extent. Concentrated in/near human population centres/roads.
Cost	Most expensive. Regulator-incurred expense, with occassional co-investment from industry.	Moderate expense. Regulator & industry co-investment (e.g. agricultural threats). Regulator-incurred expense (e.g. environmental/society threats).	Least expensive. Regulator-incurred expenses for collating reports, verification, communication plans.

FIGURE 6.1 Characteristics of active, general, and passive surveillance.

success (i.e. proof of freedom). Because of its expense, it is also the most geographically and temporally constrained method, with most effort occurring within and surrounding known outbreaks and only persisting for as long as it takes to meet the required burden of evidence to declare proof of freedom. If active surveillance for a particular threat is expected to provide high value for money compared to other risk-reducing activities, it may be used on an ongoing basis to either facilitate the early detection of incursions or to support claims of area freedom for market access. In these cases, ongoing active surveillance can be positioned near high-risk points of entry (e.g. ports), in areas of high establishment potential, or within high-value production zones.

General Surveillance

General surveillance is a semi-coordinated surveillance effort implemented by environmental stakeholders (e.g. park rangers), agricultural stakeholders (e.g. farmers, agronomists, vets, and industry organisations), scientists, or citizen science groups (Hester and Cacho 2017). General surveillance is more opportunistic than active surveillance, in that it capitalises on the interests and motivations of various groups to conduct the surveillance necessary to protect their own assets or the community (Kruger, Ticehurst, and van der Meer Simo 2022). Biosecurity regulators play a lesser role in implementing general surveillance, but regulators sometimes co-invest in such programs if they can improve early detection and bolster existing active surveillance programs (Hester and Cacho 2017).

Because general surveillance is implemented by multiple stakeholders, with costs and logistics being shared among these groups, it can be implemented over a greater geographic extent compared to active surveillance. However, biosecurity regulators face multiple challenges in using and interpreting data from general surveillance. While reported detections can be verified and acted upon by regulators, estimating the reliability of general surveillance in detecting threats is challenging because the reliability of different groups is unknown and likely to be highly variable. Each group implements general surveillance based on their own objectives and threats of interest, and as such, they might utilise different taxon expertise, training resources, and surveillance methods at varying levels of effort, which may or may not be documented. Without knowing a method's sensitivity or the survey effort undertaken, regulators cannot quantify the reliability of general surveillance, and thus, cannot solely rely on it to estimate the likelihood a threat is absent from a region.

In practice, the sensitivity of general surveillance is assumed to be lower than that of active surveillance. Because of its opportunistic nature, general surveillance tends to be multi-threat focused and not optimised to detect any single threat. In contrast, active surveillance is often optimised to detect a specific threat, and it relies on specialist equipment and survey techniques that maximise the likelihood of detection. While estimates of sensitivity and effort are difficult to quantify, it may be assumed that both will be greater in regions where the potential impacts of incursions are greatest. For instance, farmers are likely to have higher expertise in detecting pests and diseases that pose significant threats to their produce, and they are more likely to invest in detection effort in areas most exposed to a threat. The same farmers may be less capable of detecting and less inclined to search for a pest or disease that does not pose a threat to their own assets.

Despite these challenges, general surveillance has been a significant contributor to first detections in various agricultural industries (Hammond et al. 2016), and there is a strong desire by regulators and industry to make better use of general surveillance data by integrating those with other methods to infer likelihoods of threat absence (Martin et al. 2017).

Passive Surveillance

Passive surveillance is the chance detection and reporting of threats by the public. Passive surveillance is the most fortuitous and accidental of all types of surveillance (Hester and Cacho 2017), and it differs from active and general surveillance in that there is little coordinated surveillance effort or reporting framework. Detections arise purely by chance, often based on random encounters coupled with individual curiosity. Passive surveillance can be described as "the threat comes to you" whereas active surveillance and to a lesser degree, general surveillance, can be described as "you go to the threat". Much like general surveillance, public reportings have been a significant source of first detections for many invasive species (Hester and Cacho 2017).

Reporting of passive surveillance occurs on a variety of formal and informal platforms such as biosecurity hotlines, online citizen science databases (e.g. iNaturalist, the Global Biodiversity Information Facility, and the Atlas of Living Australia), and social media platforms. Individuals making chance detections do so with no underlying objective, and often, with variable capability to identify what they have found, let alone to whom it should be reported. Public detections often go unreported, and when they are reported, can be prone to false positives (i.e. a report being misidentified as a threat of concern).

While governments and regulators have little direct costs associated with implementing passive surveillance, there are many indirect costs associated with using such data, including the cost of verifying and collating records from multiple platforms. As with general surveillance, passive surveillance data have unknown sensitivity and survey effort. Detection likelihoods will also vary across space and taxa. Public recordings tend to be geographically biased towards regions of high human population density (e.g. in and around metropolitan areas) or along roads or walking tracks (Figure 6.2; Dodd et al. 2015). Public detections are also more likely for threats with highly

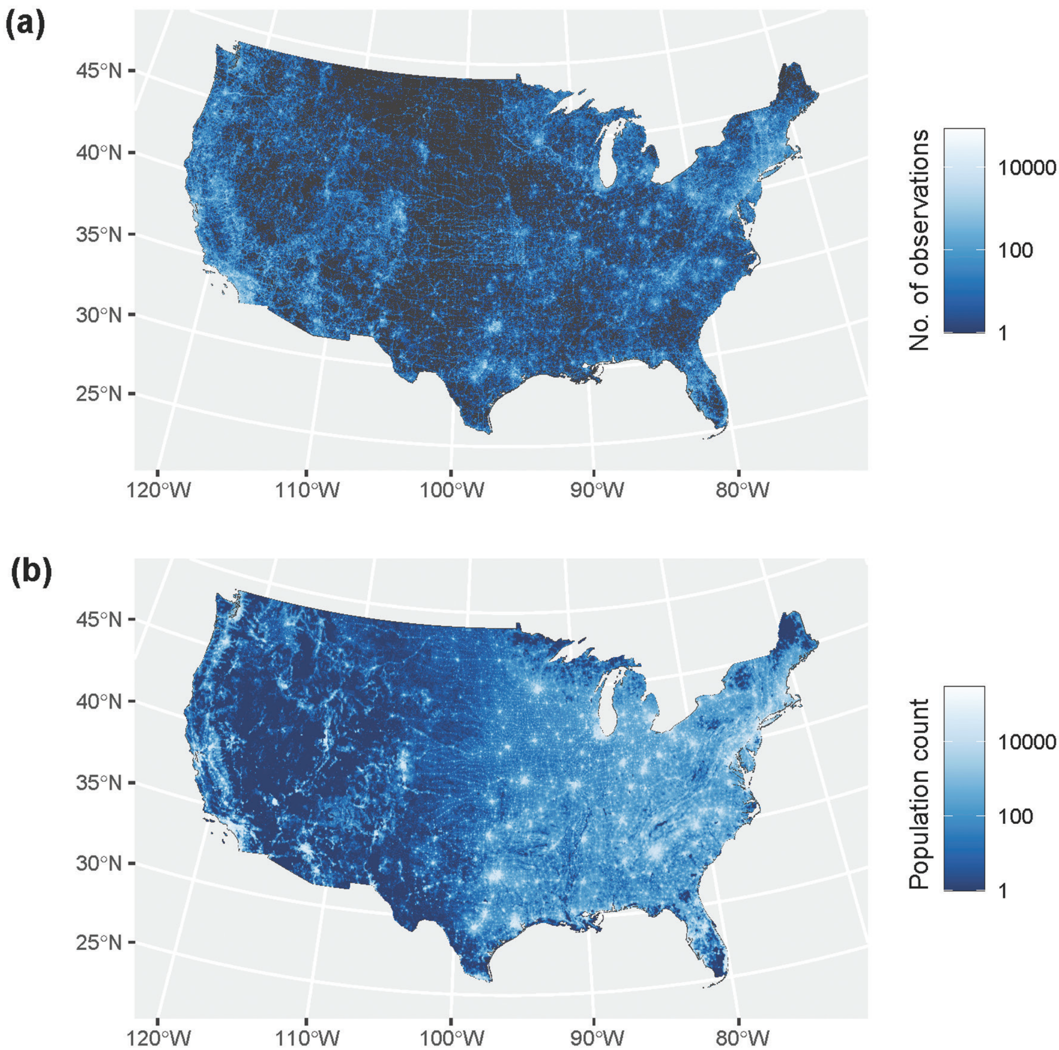

FIGURE 6.2 (a) The number of observations of plant taxa and (b) human population count in the contiguous United States. Note the highest densities of occurrences typically correspond to areas with high human population counts (i.e. close to metropolitan areas and along major road networks). Plant taxa data were extracted from the global biodiversity information facility on 14 December 2021 (GBIF Org 2021) and human population count data for the year 2020 were obtained from Columbia University's Centre for International Earth Science Information Network (CIESIN 2022). Both layers were projected to the USA Albers Equal Area Conic coordinate system (ESRI:102003) and aggregated to a 5-km raster grid.

visible impacts or striking physical attributes (Box 6.1), and reportings generally occur when a threat reaches its natural detection point (e.g. when it has established and reached a population size, extent, or impact that makes encounters with the public more likely; Kompas et al. 2019).

PRACTICAL CONSIDERATIONS IN POST-BORDER SURVEILLANCE

A range of practical considerations must be considered when designing a post-border surveillance system, including:

- Selecting the type(s) of surveillance to use under each objective.
- For early detection, determining where to conduct surveillance.
- For area freedom or proof of freedom, inferring threat absence from surveillance data.

Selecting Surveillance Type(s) for an Objective

A fundamental challenge faced by biosecurity regulators is deciding which surveillance type to prioritise and fund under different surveillance objectives. Each surveillance type (active, general, and passive) has advantages and disadvantages, and each type differs in terms of cost, reliability, and capacity to infer likelihoods of absence (Figure 6.1).

Active surveillance is almost always used as the primary tool to delimit and monitor an outbreak, and it is increasingly required by trading partners for declaring area freedom. When using active surveillance, regulators can easily coordinate and quantify surveillance effort within and surrounding an outbreak or production zone. Reliability (i.e. sensitivity and specificity) in detecting a threat is known, hence data from active surveillance can be used to infer the likelihood a threat is absent and inform when to declare eradication success (i.e. proof of freedom) or area freedom for market access.

In contrast, regulators have limited capacity to coordinate passive and general surveillance. Regulators can conduct awareness campaigns in and around outbreak zones to increase public and stakeholder detection and reporting, but the efficacy of such programs is difficult to quantify. Even with awareness campaigns, the reliabilities of passive and general surveillance are often unknown, because sensitivity and survey effort data are not commonly collected. Passive and general surveillance are therefore rarely used in statistical models to infer likelihoods of absence or eradication success. Instead, detections derived from these forms of surveillance act as supplemental data to identify new outbreaks, support existing evidence of absence, and position active surveillance resources (IPPC 2016a).

Active surveillance is also the gold standard for early detection, but its high cost often restricts its use to threats posing the highest risk to a jurisdiction (i.e. where the benefits of earlier detection outweigh increases in surveillance cost; see Chapter 9. Resource Allocation). Active surveillance for early detection is undertaken when a trading partner requires its use in informing area freedom declarations. For example, active surveillance networks using pheromone lure traps are implemented in the United States, Australia, and New Zealand for both area freedom and early detection of exotic fruit fly threats such as the Mediterranean fruit fly (*Ceratitis capitata*) and the Oriental fruit fly (*B. dorsalis*). These species feed on many hosts, have significant impacts on horticultural yield and quality, and they are difficult to eradicate and can disrupt access to premium export markets. As such, there is an incentive for countries to detect these threats early to minimise impacts.

For most threats, where the costs of active surveillance are not expected to provide good value for money, regulators rely on both general and passive surveillance for first detections. While neither is truly optimised for early detection, the implicit assumption is that both general and passive surveillance will detect threats early enough so that they can be contained or eradicated. However, this assumption requires scrutiny. In Australia, detection of the non-descript Russian wheat aphid (*Diuraphis noxia*; Figure 6.3c) relied on general and passive surveillance systems. The species remained undetected until 2016, by which time it was widespread in cereal cropping regions across the south-east and was deemed infeasible to control or eradicate (Yazdani et al. 2018).

To reduce the chance of incursions being detected at a point where it is infeasible to control or eradicate, regulators must consider:

- How the attributes of the threat (e.g. size and morphology) influence the reliability of passive and general surveillance (Box 6.1).
- Where general and/or passive surveillance effort is greatest (Figure 6.2), and how this compares to where a threat is most likely to establish.
- Whether the costs of active surveillance provide good value for money in terms of earlier detection.

BOX 6.1. SPECIES-SPECIFIC FACTORS INFLUENCE THE PROBABILITY OF DETECTION

An analysis of citizen reports of beetles (Coleoptera) and true bugs (Hemiptera) in the Atlas of Living Australia found that the probability of reporting by a member of the public (and by implication, the probability of detection) was strongly influenced by the physical attributes of a species (Caley, Welvaert, and Barry 2019). Species with large body size, large geographic range, or striking colour patterns or morphological features had a significantly higher annual probability of being reported by a member of the public. The black pine sawyer beetle (*Monochamus galloprovincialis*; Figure 6.3a) and the Colorado potato beetle (*Leptinotarsa decemlineata*; Figure 6.3b), two relatively large (>10 mm) beetles with distinctive morphological features, had average annual detection probabilities of 0.91 and 0.76, respectively. At the other end of the spectrum, the small (<5 mm) and non-descript Russian wheat aphid (*D. noxia*; Figure 6.3c) and the generic-looking mountain pine beetle (*D. ponderosae*; Figure 6.3d) had citizen detection probabilities of 0.03 and 0.02, respectively.

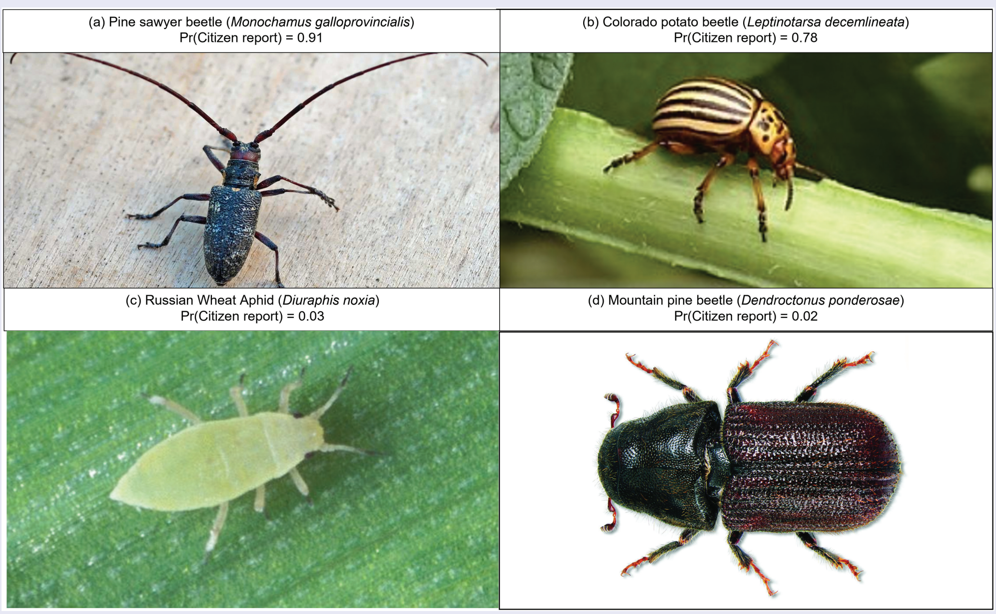

FIGURE 6.3 Probabilities of citizen reporting four threats in Australia. Note that pests with less distinctive features have lower reporting rates (From Caley et al. 2019).

Determining Where to Conduct Surveillance for Early Detection

There is often a clear geographic disconnect between where general surveillance effort is concentrated and where initial establishment events are most likely to occur. Most successful exotic threats have generalist attributes and enter and spread via human movement and trade. Propagule pressure and establishment potential for most threats will therefore be greatest in regions with highest human activity, such as points of entry (i.e. airports and ports) and populated areas where people and goods are most likely to disperse (i.e. cities and urban areas). In contrast, general surveillance for most agricultural and environmental biosecurity threats tends to be concentrated in sparsely populated areas where the potential impacts of incursions are greatest (e.g. production zones and national parks), but where propagule pressure and establishment potential may be low.

While passive surveillance is expected to be concentrated in areas of high human activity or establishment potential (Figure 6.2), its ability to inform regulators of new incursions in a timely manner depends on the attributes of the threat (Box 6.1). A threat could establish in an urban area and remain undetected until it has reached its natural detection point, by which time it may have spread far and wide, making control and eradication infeasible.

Active surveillance can be labour intensive and costly to maintain and is rarely implemented uniformly across geographic space. Rather, it should be concentrated in regions expected to have high entry or establishment potential. The establishment potential of an exotic threat is governed by three spatial factors (Camac, Baumgartner, Hester, et al. 2021, Camac, Baumgartner, et al. 2020, Catford, Jansson, and Nilsson 2009), where all three factors must be met for establishment to occur:

- Can the threat reach the location of interest (i.e. propagule pressure)?
- Are abiotic conditions suitable (e.g. climate suitability)?
- Are biotic conditions suitable (e.g. presence of host or food)?

Based on these factors, two approaches are commonly used to inform early detection surveillance. Pathway models estimate contamination or leakage rates reaching a country's border or points of entry (Camac, Baumgartner, Garms, et al. 2021; also see Chapter 9. Resource Allocation), while species distribution models identify areas of suitable environment that may be conducive for establishment. Both approaches provide critical information for where to prioritise surveillance and are outlined in Chapter 14. Map.

Inferring Threat Absence from Surveillance Data

A fundamental problem with declaring an exotic threat absent from a region based only on a lack of detections is that this assumes the surveillance program has perfect sensitivity. That is, if the threat is present, the surveillance program will always detect it. In practice, post-border surveillance programs never have perfect sensitivity. The complication of imperfect sensitivity means that a lack of detections from a surveillance program can arise from one of two processes: (1) the threat is truly absent; or (2) the threat is present, but the surveillance program failed to detect it (i.e. a false negative). While imperfect specificity leading to false positives can be cross-checked, it is impossible to be certain a threat is truly absent.

Given the issue of not being able to definitively determine the absence of a threat, scientists and biosecurity practitioners use statistical approaches to quantify the likelihood of threat absence. Which approach to use largely depends on the decision context and the data at hand. If the focus is to determine the success of an eradication program, models can be used to quantify the certainty of pest absence as a function of a time series of sightings or detections, detailed information on the number of individuals removed during an eradication program, and/or management effort over time (for a detailed summary of approaches see Rout 2017). By contrast, if the focus is to determine pest absence without an outbreak, such as for the purposes of early detection or area freedom, then negative observations (i.e. the number of non-detections) from surveillance programs can be used to inform likelihoods of absence (Barrett et al. 2010).

Irrespective of the approach used, three fundamental questions must be answered to estimate likelihoods of absence:

- What is the target prevalence or population size of the threat to be detected?
- What is the sensitivity of the surveillance method for the threat?
- What is the tolerance for being wrong?

Determining the Target Prevalence or Population Size of the Threat

In addition to the unit of area one wishes to infer absence for, estimating the likelihood of absence requires a clear definition of the minimum prevalence (i.e. design prevalence) of the threat to be detected or, in the case of non-disease threats, the population size to be detected. In a biosecurity context, prevalence could be the proportion of infected individuals or sites within a pre-defined sampling unit (e.g. a herd or a region).

When determining the minimum prevalence and/or population size to be detected, the answer will be a trade-off between being high enough to detect the threat and low enough that it can still be controlled or eradicated—a maximum tolerable level (Martin et al. 2017; Whittle et al. 2013). A design prevalence of 1% or 0.1% is commonly set for screening consignments at the border (see Chapter 5. Screen). This prevalence rarely translates to the post-border context as the surveillance unit changes from consignments to susceptible individuals or locations. Post-border, prevalence should be set by first considering the number of susceptible units (e.g. individuals or sites) in an area and then determining what number of undetected infected individuals would be tolerable. If a regulator optimised post-border surveillance effort to be 95% confident of detecting a 1% prevalence of a citrus disease in an area containing 1,000,000 susceptible host trees, the post-border surveillance system will be optimally designed to detect an outbreak containing more than 10,000 infected trees. A question the regulator should ask is whether 10,000 possible undetected infections is tolerable.

For pests, minimum population size may be more relevant and tractable than prevalence. Larger populations are generally more easily detectable, but they are also more difficult to control and eradicate. The sensitivity of a surveillance unit is typically measured in terms of the probability of detecting a single individual at a site and/or for a certain period of time. For many threats, detection probabilities will be extremely low, so sensitivity may be re-scaled such that it becomes the probability of detecting at least one individual from a population of *N* individuals. The size of this population is governed by the probability of detecting the threat and the probability of containing or eradicating it.

Estimating Surveillance Sensitivity

Surveillance programs never have perfect sensitivity, and estimating surveillance sensitivity is difficult because it can vary substantially among species and is influenced by multiple factors, including species traits (see Box 6.1), surveillance effort (e.g. the number of surveys, tests, or traps and survey time (Garrard et al. 2008; Hauser and McCarthy 2009); the local abundance of the species (McCarthy et al. 2013), site conditions, and observer or surveillance attributes (Bailey, Simons, and Pollock 2004).

Despite these difficulties, information about sensitivity can be obtained in many situations, including by conducting experiments designed to estimate sensitivity under a variety of conditions (Hauser et al. 2016), by using (or estimating) detection rates for species with similar traits (Box 6.1; Caley et al. 2019; Garrard et al. 2012), by conducting meta-analyses, or, when no other data are available, by using expert judgement (see Chapter 12. Elicit).

What is the Tolerance for Being Wrong?

Regardless of the method used to infer threat absence, a regulator will have to define their tolerance for incorrectly concluding the threat is absent when in fact it is present (Figure 6.4). In a biosecurity context, this tolerance is often described in terms of either the likelihood of

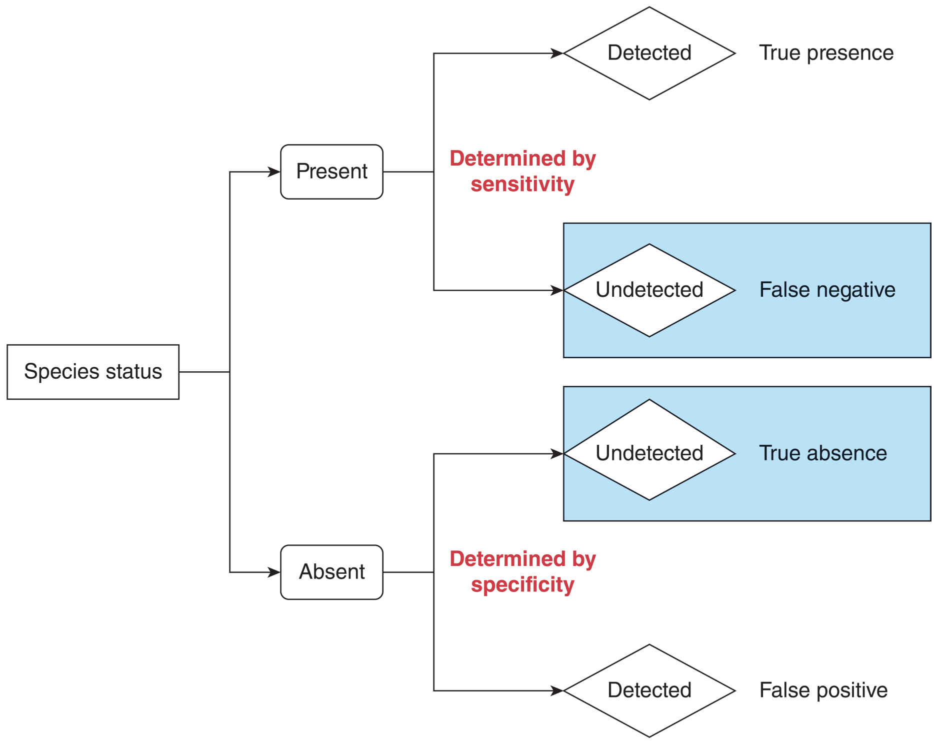

FIGURE 6.4 Scenario tree outlining the two processes leading to absence observations when surveillance sensitivity and specificity are imperfect.

detection failure (i.e. 1 – probability of detection) or likelihood of presence (i.e. 1 – probability of absence) after accounting for zero detections, design prevalence, and surveillance sensitivity and effort.

To declare threat absence, the likelihoods of detection failure or threat presence are set to some tolerable level and are typically governed by rules of thumb coupled with regulatory requirements and a country's ALOP (see Chapter 2. Biosecurity Systems and International Regulations). Commonly, this tolerance is set to 0.05%—we accept that we will incorrectly declare a threat as absent (when in fact it is present) 5% of the time (European Food Safety Authority et al. 2020). However, this tolerance level is somewhat arbitrary and does not consider the cost of surveillance or the potential economic, social, and environmental costs of failing to detect a threat. If the impacts of failing to detect a threat are high and the cost of surveillance is low, then it may be prudent for regulators to lower the tolerance level to reduce the chance of incorrectly declaring absence and maximise the likelihood of avoiding those damages. If the impacts of failed detections are low and the cost of surveillance is high, then a regulator may be more tolerant to failed detections and set a higher tolerance level (Camac, Dodd, et al. 2020;Hauser and McCarthy 2009; Kompas, Chu, and Nguyen 2016).

Multiple model types can be applied to infer the absence of a biosecurity threat, and which one to use will depend on how surveillance sensitivity and effort are measured and whether spatial information on the likelihood of threat presence is available. Here, we outline two of the simplest models used to infer threat absence: the binomial model and Bayes theorem (Box 6.2). For alternative models and a more comprehensive discussion of their assumptions and limitations, see Chapter 5. Screen and Hester, Hauser, and Kean (2017).

BOX 6.2. INFERRING THREAT ABSENCE WITH THE BINOMIAL MODEL AND BAYES THEOREM

Binomial Model

The binomial model is the most commonly used approach to estimate the likelihood of threat absence. The model is based on the confidence of rejecting the null hypothesis that the threat is present, where confidence is defined as the probability a surveillance program detects the threat. This is estimated as a function of the sensitivity (S) of a surveillance unit (e.g. diagnostic test, trap, or survey) at threat prevalence (p) and a given amount of surveillance effort (N_{effort}; e.g. the number of tests or traps). The probability of detection is expressed as:

$$\Pr(\textit{Detection}) = 1 - (1 - p \times S)^{N_{\text{effort}}} \tag{Eq. 6.1}$$

Absence is inferred if no detection is recorded and the confidence of detection, $\Pr(\textit{Detection})$, is at or above a pre-defined level. If tolerance for being wrong is 0.05, then confidence would need to be 0.95 or higher to reject the null hypothesis that the threat is present (i.e. declare the threat absent). This model can be further expanded to account for other technical considerations, such as clustered sampling (see Chapter 5. Screen). While this approach provides a measure of confidence in threat absence, it does so solely as a function of surveillance sensitivity at a pre-defined prevalence and the amount of surveillance effort. The method ignores potential differences in the likelihood of pest establishment across space or time: confidence of absence may be overestimated in places where establishment likelihood is high and underestimated in areas where establishment likelihood is low (see Chapter 14. Map).

Bayes Theorem

Compared to the binomial model, which quantifies the conditional probability of detection assuming the threat is present, Bayes theorem uses a more logical measure of pest absence—the probability of pest absence (Barrett et al. 2010; McArdle 1990). Another advantage of the Bayesian approach is that it can directly incorporate additional sources of information, using a model parameter known as the prior (McCarthy 2007). In the context of estimating likelihoods of threat absence, the prior describes the belief a threat is present at a location, $\Pr(\textit{Presence})$. The probability of threat absence is given by:

$$\Pr(\textit{Absence}) = 1 - \frac{(1 - \Pr(\textit{Detection})) \times \Pr(\textit{Presence})}{(1 - \Pr(\textit{Presence})) + (1 - \Pr(\textit{Detection})) \times \Pr(\textit{Presence})} \tag{Eq. 6.2}$$

$$\text{where } \Pr(\textit{Detection}) = 1 - (1 - Pr(S))^{N_{\text{effort}}} \tag{Eq. 6.3}$$

Because the Bayesian approach can explicitly account for information on differential risk across space and/or time, it is less susceptible to over- or under-estimation of the likelihood of absence. The Bayesian approach can also identify regions that require greater surveillance effort based on estimated likelihoods. The prior probability of threat presence can be informed using a variety of data sources, such as expert elicitation (see Chapter 12. Elicit), a map of establishment likelihood (see Chapter 14. Map), or data from past surveillance programs or incursions. If no prior knowledge is available, the prior can be set at 0.5 (i.e. a 50% chance of the threat being present) and the posterior probability of absence will be driven solely by surveillance records (Rout 2017).

VALUE FOR MONEY IN SURVEILLANCE PLANNING

As surveillance effort increases, so too does the confidence that a threat is absent. Higher confidence implies lower chances of incorrectly claiming absence and, thus, lower chances of incurring additional surveillance and market costs (e.g. time out of market and re-eradication costs). However, this confidence comes at the cost of investing in surveillance methods with higher sensitivity and/or investing in more surveillance effort (e.g. additional people, time, or money). The optimal amount of surveillance is the one that minimises surveillance costs and the expected costs of incorrectly claiming absence (Box 6.3).

Irrespective of the objective, the surveillance strategy and effort required should be determined by what represents the best value for money (see Chapter 9. Resource Allocation). When surveillance occurs for early detection, delimiting the extent of an outbreak, or for threat monitoring and management, surveillance requirements are set by the regulator. When the objective of surveillance is market access, trading partners typically set surveillance requirements. However, the cost of implementing those requirements may outweigh the benefit of market access, so regulators should still minimise net expected costs.

Practitioners should also understand that a given budget could be used to survey any number of pests simultaneously, so they should consider whether an investment into surveillance for one pest gives better value than surveillance for other pests, rather than considering each pest in isolation. The "value for money" premise holds regardless of whether budget allocations are being made for a single threat, across a number of threats, or indeed at different stages of the biosecurity continuum (see Chapter 9. Resource Allocation). Allocating a surveillance budget across pests and diseases will depend on the difficulty (cost) of detection and eradication of each pest, and the avoided damages from preventing or removing the pest. Deciding where best to locate surveillance, and over which time period, has important budgetary implications. Finally, surveillance activities do not occur in isolation, they are one of a suite of activities undertaken to manage pest and disease risks (e.g. research, control, treatment, and community engagement) and thus should not be considered in isolation (see Chapter 7. Prepare, Respond, and Recover).

BOX 6.3. DETERMINING OPTIMAL SURVEILLANCE EFFORT

The optimal surveillance effort (n) of a threat can be estimated by minimising the total costs of surveillance and the costs of failing to detect the threat, using the following equation:

$$Total\ costs(n) = Cost_{Surveillance}(n) + \Pr(Wrong \mid n) \times Cost_{Wrong} \qquad \text{(Eq. 6.4)}$$

The first term ($Cost_{Surveillance}$) captures the costs associated with implementing n units of surveillance effort (e.g. infrastructure, diagnostics, and logistics). The probability of being wrong given with n surveillance units, $\Pr(Wrong \mid n)$, is either the probability of failing to detect the threat ($1 - \Pr(Detection)$) derived from the binomial model or the estimated probability of presence ($1 - \Pr(Absence)$) derived from the Bayesian approach (Box 6.2). The cost of being wrong, $Cost_{Wrong}$, is the cost associated with incorrectly declaring a threat is absent, which may include immediate costs (e.g. containment and eradication protocols) and damages that accrue over time (e.g. agricultural yield losses, time out of market, and the cost and time required to declare eradication success). Optimal surveillance effort can be identified by calculating total cost for a range of surveillance efforts, with optimal surveillance effort being the point where total cost is minimised.

In the theoretical scenario plotted in Figure 6.5, we assume that:

- If the threat is wrongly thought to be absent and allowed to spread, the damages would be worth \$10 million ($Cost_{Wrong}$).
- The threat is to be detected at a prevalence of 1% using a surveillance method with a unit sensitivity S of 0.2.
- The cost of each surveillance unit (e.g. hardware and logistical costs) is \$5,000 and scales linearly with the number n of surveillance units added (blue line).

Using the binomial model defined in Box 6.2, the probability of being wrong given n surveillance units $\Pr(Wrong \mid n)$ is $1 - \Pr(Detection)$. Total costs are estimated using Eq. 6.4. Under this scenario, the total cost is U-shaped (black line), meaning that increasing surveillance effort decreases total costs, up until a point where high surveillance costs outweigh the benefits of avoiding damages. Note that very high surveillance levels (>1,960 surveillance units) result in greater surveillance expenditure relative to the overall damages to be avoided (\$10 million).

In this scenario, the optimal amount of surveillance is 693 units at a cost of about \$3.5 million (where total cost is lowest), with a $\Pr(Detection)$ of 0.75. The optimal amount of surveillance is lower than the 1,449 samples (\$7.3 million) that would traditionally be required to meet the arbitrary confidence threshold of 0.95. These surveillance costs translate to total costs (cost of surveillance + cost of incorrectly declaring absence) of \$5.7 million for the optimal scenario and \$7.8 million for the traditional confidence threshold scenario, translating into a saving of \$2.1 million.

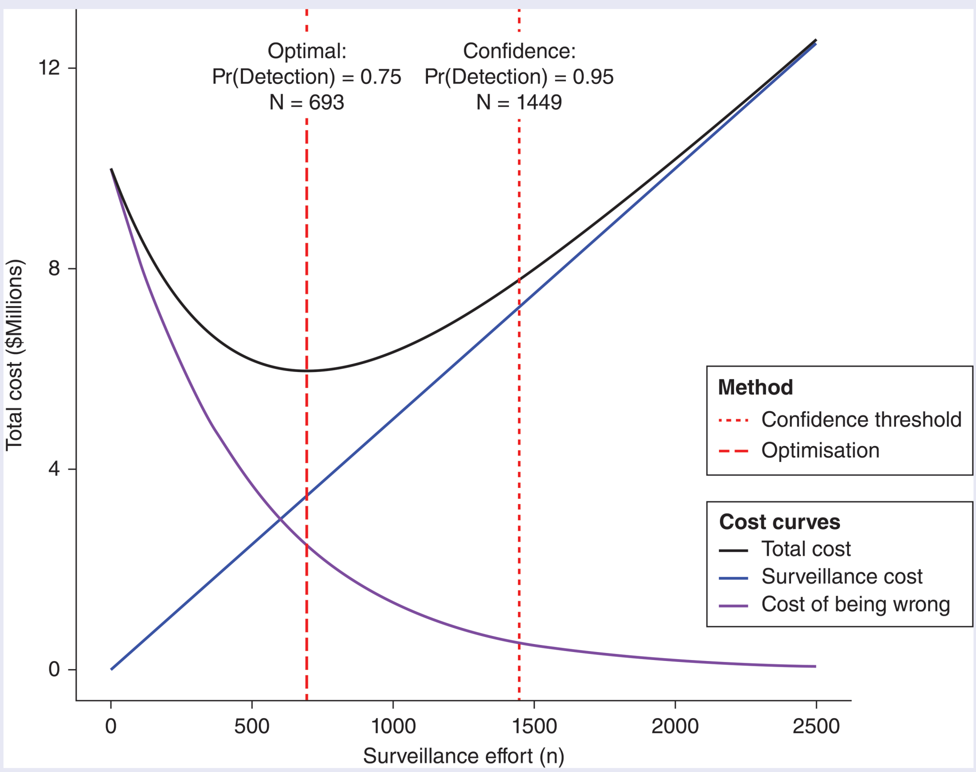

FIGURE 6.5 Theoretical example of the cost of surveillance and the cost of potential damages as surveillance effort (n) increases.

IN A NUTSHELL

- Post-border surveillance can be used to meet four objectives: (1) claiming area freedom, (2) early threat detection, (3) outbreak delimitation, and (4) threat monitoring and management (including declaring proof of freedom).
- Surveillance methods range from the deliberate and coordinated use of sophisticated surveillance tools (i.e. active surveillance), to those that attempt to benefit from detections made by stakeholders (i.e. general surveillance) or the public (i.e. passive surveillance).
- Early detection surveillance should be prioritised in areas where the risk of establishment is greatest.
- Due to variable reliability of the data, significant care should be taken when using data from general and passive surveillance to make claims of threat absence.
- How much surveillance is required depends on the objective of surveillance, the tolerance for being wrong and the magnitude of the cost and benefits (avoided damages) of surveillance.

REFERENCES

Ahmed, D. A., E. J. Hudgins, R. N. Cuthbert, M. Kourantidou, C. Diagne, P. J. Haubrock, B. Leung, C. Liu, B. Leroy, S. Petrovskii, A. Beidas, and F. Courchamp. 2022. “Managing Biological Invasions: The Cost of Inaction.” *Biological Invasions*:1–20. https://doi.org/10.1007/s10530-022-02755-0.

Anderson, C., S. Low-Choy, P. Whittle, S. Taylor, C. Gambley, L. Smith, P. Gillespie, H. Löcker, R. Davis, and B. Dominiak. 2017. “Australian Plant Biosecurity Surveillance Systems.” *Crop Protection* 100:8–20. https://doi.org/10.1016/j.cropro.2017.05.023.

Bailey, L. L., T. R. Simons, and K. H. Pollock. 2004. “Estimating Site Occupancy and Species Detection Probability Parameters for Terrestrial Salamanders.” *Ecological Applications* 14 (3):692–702. https://doi.org/10.1890/03-5012.

Barrett, S., P. Whittle, K. Mengersen, and R. Stoklosa. 2010. “Biosecurity Threats: The Design of Surveillance Systems, Based on Power and Risk.” *Environmental and Ecological Statistics* 17 (4):503–519. https://doi.org/10.1007/s10651-009-0113-4.

Caley, P., M. Welvaert, and S. C. Barry. 2019. “Crowd Surveillance: Estimating Citizen Science Reporting Probabilities for Insects of Biosecurity Concern.” *Journal of Pest Science* 45:1–8. https://doi.org/10.1007/s10340-019-01115-7.

Camac, J., J. Baumgartner, B. Garms, A. Robinson, and T. Kompas. 2021. Estimating trading partner exposure risk to new pests or diseases. Technical Report for CEBRA project 190606. Centre of Excellence for Biosecurity Risk Analysis.

Camac, J., J. Baumgartner, S. Hester, R. Subasinghe, and S. Collins. 2021. Using edmaps & Zonation to inform multi-pest early-detection surveillance designs. Technical Report for CEBRA project 20121001. Centre of Excellence for Biosecurity Risk Analysis.

Camac, J., J. Baumgartner, A. Robinson, and J. Elith. 2020. Developing pragmatic maps of establishment likelihood for plant pests. Technical Report for CEBRA project 170607. Centre of Excellence for Biosecurity Risk Analysis.

Camac, J., A. Dodd, N. Bloomfield, and A. Robinson. 2020. Sampling to support claims of area freedom: Technical report for the Department of Agriculture. Centre of Excellence for Biosecurity Risk Analysis.

Catford, J. A., R. Jansson, and C. Nilsson. 2009. “Reducing Redundancy in Invasion Ecology by Integrating Hypotheses into a Single Theoretical Framework.” *Diversity and Distributions* 15 (1):22–40. https://doi.org/10.1111/j.1472-4642.2008.00521.x.

CIESIN. 2022. “Center for International Earth Science Information Network.” accessed 14 December 2021. http://www.ciesin.org/.

Dodd, A. J., M. A. McCarthy, N. Ainsworth, and M. A. Burgman. 2015. “Identifying Hotspots of Alien Plant Naturalisation in Australia: Approaches and Predictions.” *Biological Invasions* 18 (3):631–645. https://doi.org/10.1007/s10530-015-1035-8.

European Food Safety Authority, E. Lázaro, S. Parnell, A. V. Civera, J. Schans, M. Schenk, J. C. Abrahantes, G. Zancanaro, and S. Vos. 2020. “General Guidelines for Statistically Sound and Risk-Based Surveys of Plant Pests.” *EFSA Supporting Publications* 17 (9):1919E. https://doi.org/10.2903/sp.efsa.2020.EN-1919.

Garrard, G. E., S. A. Bekessy, M. A. McCarthy, and B. A. Wintle. 2008. “When Have We Looked Hard Enough? A Novel Method for Setting Minimum Survey Effort Protocols for Flora Surveys.” *Austral Ecology* 33 (8):986–998. https://doi.org/10.1111/j.1442-9993.2008.01869.x.

Garrard, G. E., S. Ramula, M. A. McCarthy, N. S. G. Williams, S. A. Bekessy, and B. A. Wintle. 2012. “A General Model of Detectability Using Species Traits.” *Methods in Ecology and Evolution* 4 (1):45–52. https://doi.org/10.1111/j.2041-210x.2012.00257.x.

GBIF Org. 2021. “Occurrence Download.” The Global Biodiversity Information Facility. https://www.gbif.org/occurrence/download/0079039-210914110416597.

Hammond, N. E. B., D. Hardie, C. E. Hauser, and S. A. Reid. 2016. “Can General Surveillance Detect High Priority Pests in the Western Australian Grains Industry?” *Crop Protection* 79:8–14. https://doi.org/10.1016/j.cropro.2015.10.004.

Hauser, C. E., and M. A. McCarthy. 2009. “Streamlining ‘search and destroy’: Cost-Effective Surveillance for Invasive Species Management.” *Ecology Letters* 12 (7):683–692. https://doi.org/10.1111/j.1461-0248.2009.01323.x.

Hauser, C. E., J. Weiss, G. Guillera-Arroita, M. A. McCarthy, K. M. Giljohann, and J. L. Moore. 2016. “Designing detection experiments: Three more case studies.” 20th Australasian Weeds Conference, Perth, Western Australia, 11-15 September 2016.

Hester, S. M., and O. J. Cacho. 2017. “The Contribution of Passive Surveillance to Invasive Species Management.” *Biological Invasions* 19 (3):737–748. https://doi.org/10.1007/s10530-016-1362-4.

Hester, S. M., C. E. Hauser, and J. M. Kean. 2017. “Tools for Designing and Evaluating Post-Border Surveillance Systems.” In *Invasive Species: Risk Assessment and Management*, edited by Andrew P. Robinson, Terry Walshe, Mark A. Burgman and Mike Nunn, 17–52. Cambridge: Cambridge University Press.

Hulme, P. E. 2009. “Trade, Transport and Trouble: Managing Invasive Species Pathways in an Era of Globalization.” *Journal of Applied Ecology* 46 (1):10–18. https://doi.org/10.1111/j.1365-2664.2008.01600.x.

IPPC. 2016a. International Standard for Phytosanitary Measures. ISPM No. 6: Guidelines for Surveillance.

IPPC. 2016b. International Standard for Phytosanitary Measures. ISPM No. 9: Guidelines for Pest Eradication Programmes.

IPPC. 2017. International Standard for Phytosanitary Measures. ISPM No. 4: Requirements for the Establishment of Pest Free Areas.

Kompas, T., L. Chu, and H. T. M. Nguyen. 2016. “A Practical Optimal Surveillance Policy for Invasive Weeds: An Application to Hawkweed in Australia.” *Ecological Economics* 130:156–165. https://doi.org/10.1016/j.ecolecon.2016.07.003.

Kompas, T., L. Chu, P. Van Ha, and D. Spring. 2019. “Budgeting and Portfolio Allocation for Biosecurity Measures.” *Australian Journal of Agricultural and Resource Economics* 63 (3):412–438. https://doi.org/10.1111/1467-8489.12305.

Kruger, H., J. Ticehurst, and A. van der Meer Simo. 2022. Guidelines for General Surveillance Programs: Insights and Considerations from Systems Thinking and Nine Case Studies. Canberra: ABARES.

Leung, B., O. J. Cacho, and D. Spring. 2010. “Searching for non-Indigenous Species: Rapidly Delimiting the Invasion Boundary.” *Diversity and Distributions* 16 (3):451–460. https://doi.org/10.1111/j.1472-4642.2010.00653.x.

Leung, B., D. M. Lodge, D. Finnoff, J. F. Shogren, M. A. Lewis, and G. Lamberti. 2002. “An Ounce of Prevention or a Pound of Cure: Bioeconomic Risk Analysis of Invasive Species.” *Proceedings of the Royal Society of London. Series B: Biological Sciences* 269 (1508):2407–2413. https://doi.org/10.1098/rspb.2002.2179.

MAF. 2009. Review of Selected Cattle Identification and Tracing Systems Worldwide: Lessons for the New Zealand National Animal Identification and Tracing (NAIT) Project. Ministry of Agriculture and Forestry.

Martin, T., A. P. Robinson, T. Walshe, M. A. Burgman, and M Nunn. 2017. “Surveillance for Detection of Pests and Diseases: How Sure can We Be of Their Absence?” In *Invasive Species: Risk Assessment and Management*, edited by Andrew P. Robinson, Terry Walshe, Mark A. Burgman and Mike Nunn, 348–384.

McArdle, B. H. 1990. “When Are Rare Species Not There?” *Oikos* 57 (2):276–277. https://doi.org/10.2307/3565950.

McCarthy, M. A. 2007. *Bayesian Methods for Ecology*. Cambridge: Cambridge University Press.

McCarthy, M. A., J. L. Moore, W. K. Morris, K. M. Parris, G. E. Garrard, P. A. Vesk, L. Rumpff, K. M. Giljohann, J. S. Camac, S. S. Bau, T. Friend, B. Harrison, and B. Yue. 2013. “The Influence of Abundance on Detectability.” *Oikos* 122 (5):717–726. https://doi.org/10.1111/j.1600-0706.2012.20781.x.

Potts, J. M., M. J. Cox, P. Barkley, R. Christian, G. Telford, and M. A. Burgman. 2013. “Model-based Search Strategies for Plant Diseases: A Case Study Using Citrus Canker (*Xanthomonas citri*).” *Diversity and Distributions* 19 (5–6):590–602. https://doi.org/10.1111/ddi.12065.

Ramsey, D. S. L., J. Parkes, and S. A. Morrison. 2009. “Quantifying Eradication Success: The Removal of Feral Pigs from Santa Cruz Island, California.” *Conservation Biology* 23 (2):449–459. https://doi.org/10.1111/j.1523-1739.2008.01119.x.

Rout, T. M. 2017. “Declaring Eradication of an Invasive Species.” In *Invasive Species: Risk Assessment and Management*, edited by Andrew P. Robinson, Terry Walshe, Mark A. Burgman and Mike Nunn, 334–347.

Rout, T. M., Y. Salomon, and M. A. McCarthy. 2009. “Using Sighting Records to Declare Eradication of an Invasive Species.” *Journal of Applied Ecology* 46 (1):110–117. https://doi.org/10.1111/j.1365-2664.2008.01586.x.

Seebens, H., S. Bacher, T. M. Blackburn, C. Capinha, W. Dawson, S. Dullinger, P. Genovesi, P. E. Hulme, M. van Kleunen, I. Kühn, J. M. Jeschke, B. Lenzner, A. M. Liebhold, Z. Pattison, J. Pergl, P. Pyšek, M. Winter, and F. Essl. 2021. “Projecting the Continental Accumulation of Alien Species Through to 2050.” *Global Change Biology* 27 (5):970–982. https://doi.org/10.1111/gcb.15333.

Seebens, H., T. M. Blackburn, E. E. Dyer, P. Genovesi, P. E. Hulme, J. M. Jeschke, S. Pagad, P. Pyšek, M. Winter, M. Arianoutsou, S. Bacher, B. Blasius, G. Brundu, C. Capinha, L. Celesti-Grapow, W. Dawson, S. Dullinger, N. Fuentes, H. Jäger, J. Kartesz, M. Kenis, H. Kreft, I. Kühn, B. Lenzner, A. Liebhold, A. Mosena, D. Moser, M. Nishino, D. Pearman, J. Pergl, W. Rabitsch, J. Rojas-Sandoval, A. Roques, S. Rorke, S. Rossinelli, H. E. Roy, R. Scalera, S. Schindler, K. Štajerová, B. Tokarska-Guzik, M. van Kleunen, K. Walker, P. Weigelt, T. Yamanaka, and F. Essl. 2017. “No Saturation in the Accumulation of Alien Species Worldwide.” *Nature Communications* 8 (1):14435. https://doi.org/10.1038/ncomms14435.

Whittle, P. J. L., M. Burgman, R. Stoklosa, S. Barrett, F. C. Jarrad, J. D. Majer, P. A. J. Martin, and K. Mengersen. 2013. “A Method for Designing Complex Biosecurity Surveillance Systems: Detecting non-Indigenous Species of Invertebrates on Barrow Island.” *Diversity and Distributions* 19 (5–6):629–639. https://doi.org/10.1111/ddi.12056.

Yazdani, M., G. Baker, H. DeGraaf, K. Henry, K. Hill, B. Kimber, M. Malipatil, K. Perry, I. Valenzuela, and M. A. Nash. 2018. “First Detection of Russian Wheat Aphid *Diuraphis noxia* Kurdjumov (Hemiptera: Aphididae) in Australia: A Major Threat to Cereal Production.” *Austral Entomology* 57 (4):410–417. https://doi.org/10.1111/aen.12292.