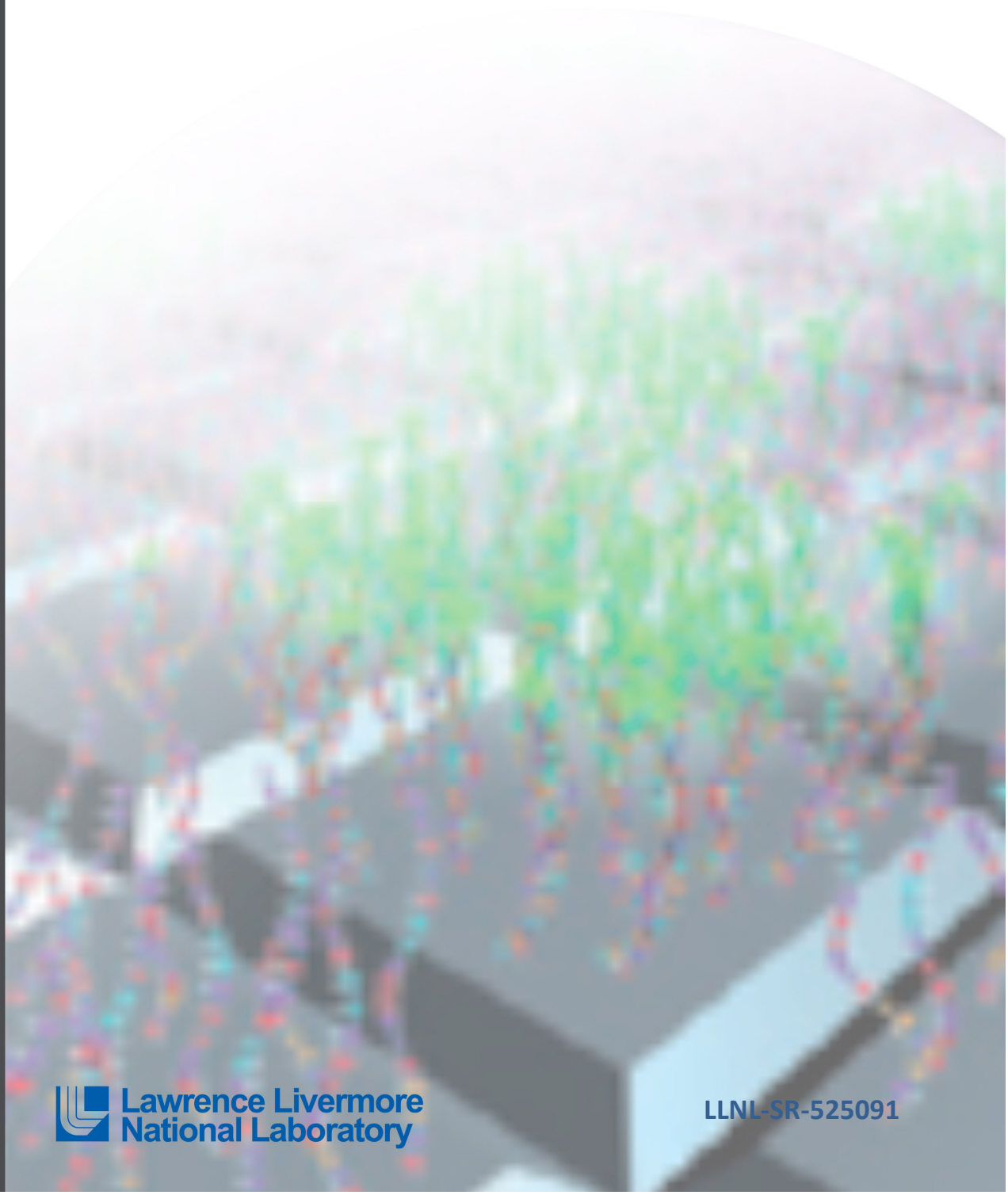
Exploring the Possible Use of Information Barriers for future Biological Weapons Verification Regimes

S. John Luke



Lawrence Livermore National Laboratory

LLNL-SR-525091

This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344

Executive Summary

This report describes a path forward for implementing information barriers in a future generic biological arms-control verification regime. Information barriers have become a staple of discussion in the area of arms control verification approaches for nuclear weapons and components. Information barriers when used with a measurement system allow for the determination that an item has sensitive characteristics without releasing any of the sensitive information. Over the last 15 years the United States (with the Russian Federation) has led on the development of information barriers in the area of the verification of nuclear weapons and nuclear components. The work of the US and the Russian Federation has prompted other states (e.g., UK and Norway) to consider the merits of information barriers for possible verification regimes.

In the context of a biological weapons control verification regime, the dual-use nature of the biotechnology will require protection of sensitive information while allowing for the verification of treaty commitments. A major question that has arisen is whether—in a biological weapons verification regime—the presence or absence of a weapon pathogen can be determined without revealing any information about possible sensitive or proprietary information contained in the genetic materials being declared under a verification regime.

This study indicates that a verification regime could be constructed using a small number of pathogens that spans the range of known biological weapons agents. Since the number of possible pathogens is small it is possible and prudent to treat these pathogens as analogies to attributes in a nuclear verification regime.

This study has determined that there may be some information that needs to be protected in a biological weapons control verification regime. To protect this information, the study concludes that the Lawrence Livermore Microbial Detection Array may be a suitable technology for the detection of the genetic information associated with the various pathogens. In addition, it has been determined that a suitable information barrier could be applied to this technology when the verification regime has been defined.

Finally, the report posits a path forward for additional development of information barriers in a biological weapons verification regime. This path forward has shown that a new analysis approach coined as Information Loss Analysis *might need to be pursued so that a numerical understanding of how information can be lost in specific measurement systems can be achieved.*

Introduction

Most—if not all—weapons control treaties or agreements that involve technical verification demand some sort of protection of the data that could be obtained in the measurement process. [1, 2] In most of these agreements, the methodology to safeguard the possible sensitive data relied upon physical control of the data that has been obtained. In the late eighties and early nineties it was envisaged that protection of sensitive data could go beyond simple administrative controls. It was conceived that a methodology could be developed to use hardware and software controls, in addition to administrative controls, to protect sensitive information. This systems-level thinking led to the concept of the information barrier.

An information barrier is an integrated system that protects information that has been determined to be sensitive by a host party from an inspecting party, while also providing the inspecting party with certain agreed upon, nonsensitive information. Traditionally, the system provides a *green*, *red,* or *yellow* light that qualitatively supplies verification information without releasing any sensitive technical details. The various *lights* indicate whether the verification measurement is consistent with, inconsistent with, or indeterminate with the declaration of the monitored party, respectively.

A challenge for the next generation of arms-control verification regimes is to determine the nature—and the necessity—of information barriers that might be used as part of a verification measurement regime. Information barriers must be produced in the context of measurements and a specific regime.

A possible misapprehension* is that an information barrier is a generic—for lack of a better term—device that can be placed upon a measurement system to protect some generic sensitive data; much like a shroud† applied to an object to prevent its visual examination. In practice, the characteristics of an information barrier depend strongly on the specific regime, type of information that is being protected, and how the measurement is being performed. Designing an effective information barrier requires:

- A detailed understanding of the information that is contained in the measurement data.
- An assessment of risk associated with the loss of any possible sensitive data.
- A detailed loss analysis to understand the associated sensitive information loss mechanisms for each specific measurement.
- Development of an information barrier methodology that mitigates each loss mechanism.
- A comprehensive red team assessment of the developed measurement system with information barrier.

Establishing an information barrier for a biological weapons verification regime is in some respects premature because the details of a strict verification regime have yet to be defined. The text of the original BWC dealt little with verification or compliance related to an agreement on verification. However, in the 2nd Review Conference for the BWC there was some discussion concerning the Declaration of past activities in offensive and/or defensive biological research and development programmes (CBM F) [2] This consideration as well as recent discussion of the possible compliance regime in the 7th Review Conference [3], indicates that the time might be ripe for discussion of a comprehensive verification regime that could resemble the CWC regime.[1]

Much of the discussion considered in this report is forward thinking and speculative. However, by considering the possible details and configuration of a regime beforehand, it may help guide policy

---

* This issue is addressed in an upcoming paper S. John Luke, *Information Barriers 201: Challenges to Conventional IB Thinking*, in press.

† The idea of a shroud for data is much like the concept of data blinding that has been suggested for data obtained under the CTBT. This approach may be very difficult to implement to the satisfaction of treaty partners.

makers (and technology providers) as to how the technical basis of a verification regime might be constructed. This report assumes that a verification regime will be entered into *voluntarily* by at least two state parties. In addition, this report assumes that one of the participants in the verification regime has declared that it has performed research and development using one of a set of *subject* pathogens. These *subject* pathogens are contained in a schedule of genetic materials that have the capability to be used as an offensive (or defensive) biological weapon.

A possible verification regime would be for a monitoring party to monitor the presence of various pathogens that a monitored party—say a research laboratory—is using for legitimate research. The charge of the monitoring party is to ensure that only certain malicious pathogens are present, which the monitored party has voluntarily declared. [4] The monitoring party has the right—under a verification protocol—to confirm that the inspected party is indeed using the *controlled* pathogens but has no right to ascertain how the pathogen is being used in the legitimate research and development in order to protect sensitive or proprietary information.

Implementation of Information Barriers in a Verification Regime

The protection of sensitive host party information from a monitoring party, during a verification measurement, is the primary purpose of an Information Barrier. The determination of the identity of sensitive information is governed by the host party and may take many forms, from information that is of importance to the national security to proprietary information with intellectual property value. An information barrier is a combination of hardware, software, controls, and procedures that offers assurance to the host party that its sensitive data are being securely held. Ideally, the implementation of an information barrier incorporates a layered approach instead of a monolithic one. With an effective layered approach, it is possible for the host party to ensure that data are protected even if a single layer might fail.

In general, the host party implements the measurement instrumentation within its own facility, and is in control of the measurement equipment at all times. The measurement system that includes the information barrier must conform to the environmental, safety, health, and security requirements of all facilities in the host country. The monitoring party (or sometimes the *inspecting party*, depending on the nature of the agreement that controls the measurement process) is present to ensure that measurements of the subject materials are consistent with declarations and/or agreements. The monitoring party—depending on the nature of agreement—may have little or no control of the measurement system after it has been implemented. Therefore, a very important issue for the monitoring party is authentication of the measurement system. This gives the monitoring party high confidence that the measurements being performed behind the information barrier are consistent with the design specifications. In other words, the monitoring party must have confidence that the host party is not spoofing the measurement outcome by some sort of hidden switch or similar operation.

The design of the measurement system that includes an information barrier must be certified before use in the host's facilities, and ensure high-fidelity measurements without operator interaction, to minimize both false positives and false negatives. False negatives may lead to a situation where the monitoring party does not trust the declaration of the host party, and false positives call into question the integrity of the measurement process.

Meeting these distinct host-party and monitoring-party constraints requires a great deal of cooperation and negotiation in establishing the proper information barrier methodology for any regime. It is clear that an acceptance of the information barrier by the monitoring party must require a combination of joint development and joint experimentation on known samples to ensure that the information barrier can be trusted from the point of view of the monitoring party.

Host Party Point of View

From the perspective of the host party, the overriding information barrier requirement is that its sensitive information *must* be protected at any cost. There cannot—and should not—be any compromise in this position. Any regime that a host party enters into voluntarily will have to satisfy its concerns in this regard. While the most direct way to prevent access to sensitive information during a measurement would be to allow no measurement at all, this would not satisfy the requirement to provide the monitoring party with some adequate basis for confidence in the declaration of the host party. Confidence building procedures—such as measurements—are almost certain to be required for any arms control regime.

Two general approaches have been taken for measurement systems employing information barriers:

- *Attribute measurements*: a measurement system is designed to determine the value of some particular attribute (or attributes), which is compared to an agreed-on nonsensitive threshold or falls within an agreed, nonsensitive range. In this case, the measurement system employing an information barrier can provide a simple yes/no indication to the monitoring party.
- *Template measurements*: a measurement system is constructed that compares data from measurement of a monitored item not to pre-agreed attribute threshold values but rather to internally stored templates that have been derived in advance from measurements of known items. As in the attribute-based approach, the template-matching approach would provide to the monitoring party only a yes/no answer, not the underlying sensitive data that would remain behind the information barrier. Such a scheme would clearly have to be regime (and item) dependent.

The other major host party requirement is the need to certify all equipment to be used in its facilities. The host party certification process* is why, in general, any equipment used in a host party facility is most likely to be developed by and provided by the host. The host party can expedite the certification process by designing the information barrier equipment and/or software to be as simple as possible, with the caveat that *simple*† is a dynamic term and should be considered on a case-by-case basis. It is clear, however, that if a system is designed to be easily certifiable, it is in general much easier to be accepted by the facility for use (and possibly easier to be authenticated by the monitoring party).

Monitoring Party Point of View

In direct contrast to the information-protection mind-set of the host party, the priority of the monitoring party is to obtain enough information to gain reasonable confidence in the host-party declaration. Ideally, the monitoring party would like unfettered access to the item under consideration to verify the nature of the declared item. However, this desire cannot be accommodated because of the requirement imposed by the host party to ensure that the monitoring party cannot access information that has been deemed sensitive. Therefore the monitoring party must rely upon confidence-building measures to confirm the declaration of the host party. By nature these confidence-building measures do not provide certainty; they simply provide a degree of confidence as to the veracity of the host party declaration. The confidence level may be increased if the monitoring party is granted necessary access so that the authentication requirements of the system can be established and is allowed to be involved in acceptance testing of the verification system.

The idea of authentication has a long history in the area of nonproliferation. There is a large breadth of opinion on the nature of authentication of equipment (both software and hardware) and on how to implement the authentication process. It is clear, however, that it is in the best interest of the monitoring

* Certification is the analog of the authentication process of the monitoring party, described below.

† It behooves the host party to design a system to be as simple as possible because any complexity makes the pseudo-tractable problem of authentication intractable.

party to have a solid approach to authentication that is commensurate with the level of confidence required for the type and context of agreement. In general, from an authentication point of view—as was the case for certification by the host party—it is necessary that the information barrier system be as simple as possible.

Authentication is important at several stages in the development and implementation process. Ideally both parties participate in designing the system that does not contain any functionality that is not consistent with the operation for which the information barrier system was designed. This process can be very time consuming, given that the idea of an information barrier is rather dynamic. Authentication also is an issue during evaluation and acceptance testing of information barrier system performance, where the entire dynamic range of the information barrier is tested against known standards, which have the same characteristics of the agreement relevant item and have been certified and agreed upon by both parties. The extent that the information barrier system is exercised during the course of a regime is open to negotiation. However, the information barrier system must be exercised fully before it is accepted.

Acceptance testing provides the baseline for any future evaluation of the information barrier system. Ideally, from a monitoring party point of view, acceptance testing would be jointly performed by both of the parties. Acceptance testing would allow for measurements to be made both without and with the use of the information barrier to assure the monitoring party of the veracity of the measurement process. In acceptance testing, the dynamic range of the measurement system would be exercised fully in that all of the possible permutations of the information barrier would be completely determined.

Short History of Information Barrier Thinking

Most information barrier implementation over the last 20 years has been initiated by the US and the Russian Federation.* The short history of information barrier thinking presented here has been written from the perspective of the United States. Other activities, such as a U.K.-Norway-VERTIC project, have not been included because it was a simulated exercise and did not involve *real* sensitive information.†

In addition, the history concentrates on US-Russian Federation interactions because it is in those interactions that the majority of information barrier contemplation has resided. A timeline, presented in **Figure 1**, shows the development of various measurement systems that have employed some sort of information barrier approaches.

The early discussion of information barriers [5-8] for use in nuclear verification centered around two approaches:

- Attribute measurements that involve determining specific characteristics of items under consideration.
- Template measurements that involve determining global characteristics of items under consideration.

These different approaches were championed by different experts and applied in the various projects described below.

---

* Over the last 5 years, the United Kingdom has shown an increased interest in developing information barriers for some of their measurement systems.

† The protection of *real* sensitive information makes the parties of various agreements very nervous and somewhat paranoid. This concept has been dubbed *The Gollum Principle* after the character in the Hobbit and Lord of the Rings. What the character Gollum teaches us is that there is extreme behavior when one seeks to protect *precious data*. The act in protecting precious data can—and usually does—change the parties involved in the protection of the information.

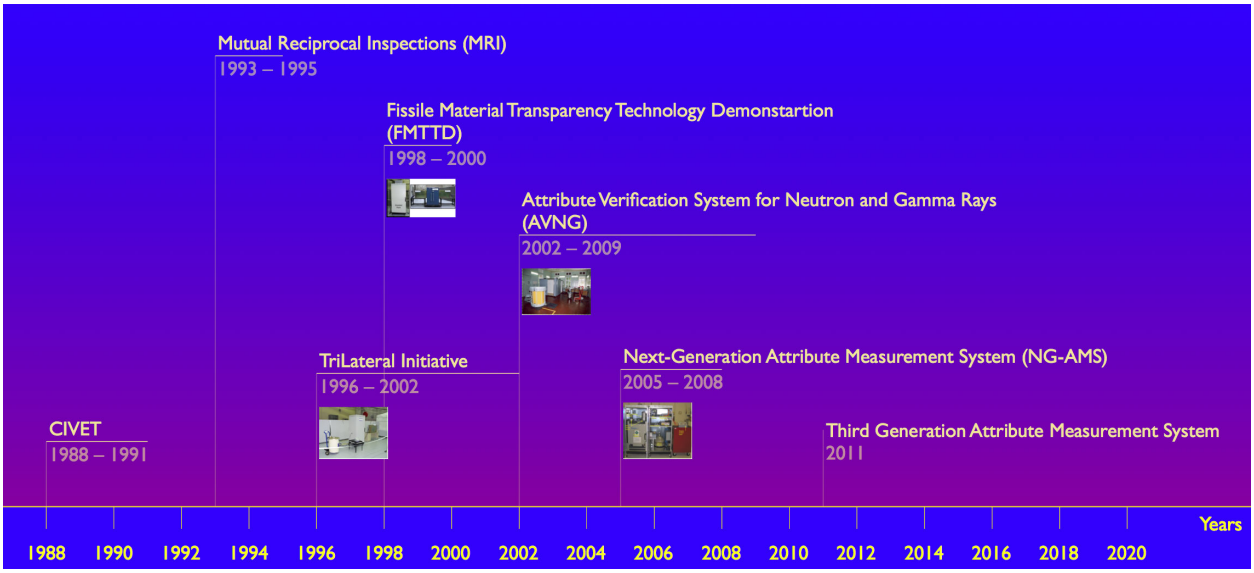


Figure 1. Timeline for information barrier development.

Controlled Intrusiveness Verification Technology System (CIVET)

The earliest technical solution to the protection of sensitive information in the nuclear weapons arena was CIVET [9, 10]. CIVET was developed at BNL and was in many ways very forward thinking CIVET was a single-function multichannel analyzer (MCA) that could be used with a high-purity germanium detector to determine the value of enrichment of a sample of uranium. The idea was visionary but suffered from at least two shortcomings. The first shortcoming was that the instrument was designed without the benefit of being designed for a specific regime. As will be discussed below, the design of a measurement system with an information barrier, but without a specific regime, is in many ways counterproductive. Second, the technology available at the time was not conducive to designing an instrument that could be authenticated. Clearly the chipset count in the instrument would make the authentication process difficult. The technology when CIVET was conceived could not support the vision of its implementation. However, as technology progressed, what CIVET envisioned could be implemented.

Mutual Reciprocal Inspections (MRI)

The JOINT STATEMENT ON INSPECTION OF FACILITIES CONTAINING FISSILE MATERIALS REMOVED FROM NUCLEAR WEAPON, which was agreed to by Secretary Hazel O'Leary and Minister Viktor Mikhailov, established the framework for the interaction involving technical experts from the United States and the Russian Federation to consider the measurement of the characteristics of weapons-quality plutonium [11, 12]. These cooperative experiments were instigated to understand what measurements could be made jointly between the United States and Russian Federation and how these measurements could be implemented in an agreement between the two parties. These interactions, however, did not lead to development of an information barrier. The joint measurements were important because these interactions did test some ideas that would be considered later in the history of the development of information barriers. Two of the major ideas that were tested were the limitation on how much data are taken during a gamma ray spectrometry measurement and smearing out the resolution in an imaging measurement. The first of these approaches has been used in several areas, mainly in developing the measurement process known is Pu600. The imaging approach has not been considered as yet, and this is not likely to be a productive direction because the sensitive information can be protected. In addition, it is always beneficial to make the best possible measurements and avoid possible incorrect conclusions.

Tri Lateral Initiative (Tri LAT)

The Tri Lateral Initiative [13-18] was initiated by a joint statement by the United States, Russian Federation, and the International Atomic Energy Agency (IAEA) in 1996 to investigate technical, legal, and financial issues associated with IAEA verification of weapon-origin fissile material in the Russian Federation and the United States. Under a bilateral agreement with the IAEA, experts from the United States developed a system for the measurement of various characteristics of plutonium that could be put under IAEA Safeguards. This system was demonstrated to experts from the IAEA and the Russian Federation to prove that measurements of fissile material could be made behind an information barrier.

The Tri-lateral Initiative (Tri Lat) was important in the short history of information barriers. The Tri Lat was the first time that a measurement system was developed for an actual agreement. During the course of developing the system, attributes for plutonium were chosen and in some ways canonized the thresholds associated with these characteristics. Finally, the measurement system developed during the Tri Lat indicated that it was possible to make high-quality measurements behind an information barrier, as well as exercise novel hardware solutions for information barriers that were the basis of future information barrier designs.

Fissile Material Technology Transparency Demonstration (FMTTD)

The Fissile Material Transparency Technology Demonstration (FMTTD) [19-24], performed at Los Alamos National Laboratory on August 14-17, 2000, had two major objectives. The first was to demonstrate to the Russian delegation that a six-attribute measurement system with information barrier (AMS/IB) could be built with sufficient protection to allow measurement of classified components without revealing classified information. The second was to construct this AMS/IB in such a manner as to convince the Russian delegation that it would be possible for a monitoring party to fully authenticate the operation of the system. The six attributes that were chosen for this demonstration were:

- Presence of plutonium.
- Presence of weapons-grade plutonium.
- Plutonium mass.
- Plutonium age.
- Absence of plutonium oxide.
- Symmetry of the plutonium source.

The demonstration was successful in showing that measurements could be made on sensitive items without the release of any sensitive information. However, the demonstration did not lead to the use of the technology developed in a verification regime between the United States and Russian Federation.

Recent Work

Attribute Verification System Neutrons Gammas (AVNG)

The AVNG attribute measurement system [25-30] was designed and built at the All Russian Scientific Institute of Experimental Physics (VNIIEF) in Russia to make measurements of potentially classified plutonium items and display previously agreed upon characteristics of the item in an unclassified form. Detailed measurements of an item under consideration were made behind an information barrier, and unclassified *attributes* based on these measurements were displayed outside the information barrier. The attributes were derived by comparing measurement results to thresholds, and only reporting whether the result was above or below the threshold (e.g., mass of plutonium> 2kg). A measurement system such as the AVNG could be used to verify a declaration made concerning a treaty-limited plutonium item. A monitoring party could use displayed attributes as well as any procedures before, during, or after the

measurement to gain confidence that the item's properties were consistent with the declared properties. A primary design criterion of an AVNG-like system is that classified information cannot be released. This criterion is often in conflict with the desire of monitoring party to obtain as much information as possible for authentication of the system and measurements.

Next Generation Attribute Measurement System

The goal of the Next Generation Attribute Measurement System (NG-AMS) was to develop a system that was designed from the ground up to be both certifiable and authenticatable [31-33]. The NG-AMS was developed and built exclusively at Los Alamos National Laboratory (LANL). The attribute measurement system could make measurements on sealed canisters of plutonium. As designed, the NG-AMS system determined the value of three attributes from the detection of neutrons and gamma rays emitted from a sample. These three attributes are the mass of the plutonium, the $^{240}Pu/^{239}Pu$ ratio, and the date on which the ^{241}Am was last separated from the plutonium. The system was designed with enough flexibility to allow for the determination of different attributes as might be needed in the future.

The development of the NG-AMS sought to understand the issues that affect authentication. The major issue that the developers discovered—as others had—is the limited information displayed due to the restriction of potentially sensitive measurements. This is the driving force for continued development of information barriers, and cannot be relaxed, restricting the LANL developers to conclude that certification of the AMS is paramount for the host party; just as authentication is of the utmost importance to the monitoring party. The conclusion is important because it indicates that joint development may ease the concerns of both parties.

Third Generation Attribute Measurement System (3G-AMS)

In 2011, the NNSA instituted the development of the Third Generation Attribute Measurement System. The purpose of this effort is to design and build a modular system capable of identifying attributes of a nuclear weapon or weapon components. The effort is being coordinated between the national laboratories and PANTEX Corporation. The Third Generation Attribute Measurement System differs from previous attribute measurement system development by defining three unique goals that govern the design of the system.

1. Authentication – for the first time the designers are attempting to take into account the authentication of the system as a design constraint.
2. Measurement on a full warhead – most of the previous attribute measurement systems focused mainly on determining the attributes of weapons components.
3. Demonstration performed in a nuclear weapons facility, which is challenging technology providers to produce an instrument that is ready for prime-time, rather than a pieced-together laboratory system.

This project is still in the very early stages of development, so there is little documentation available at this time. However, the emphasis of the DOE on this project indicates the commitment by the DOE to continue work in the advancement of information barrier thinking.

Implications of attribute v. template discussion on information barrier thought

In an attribute measurement approach, the measurement system focuses on determining specific characteristics of the item under consideration. In the case of a nuclear measurement regime, these attributes might be plutonium mass, plutonium isotopics, uranium enrichment, etc. Template measurements focus on determining a global characteristic of an item under consideration and comparing that global characteristic with a measurement that was obtained on a *control item*.

At the conclusion of these initial discussions, it was determined that templates would be appropriate in a monitoring regime that involved the measurement of numerous items of the *same* type, while attribute

measurements would be most appropriate if the regime involved items not of the same type but with *similar* features.* Attribute measurement systems allow for the development of measurement systems that are more general in nature, without the necessity to store sensitive information as part of the measurement system. Advocates of the attribute measurement approach concluded that attributes, in general, had fewer concerns with sensitive data because no sensitive data would be stored with the system. However, this concept may be incorrect because the existence of *transient* sensitive data presents an information security threat that is at least equivalent to the risk associated with *permanent* sensitive data.

One of the design constraints of any measurement system is that the false alarm rate must be kept to a minimum. False alarms contribute to the peril of the yellow light† in a measurement system. In an attribute measurement system the last thing that either party wants is a yellow light. Red lights can be accounted for and treated in the protocol; yellow lights are difficult to deal with because there can be many situations that contribute to a yellow light. In practical matters all yellow lights are added to the red light for the system. When the red light rate is too high it calls into question the appropriateness of the measurement system.

Measuring attributes allows for the design of measurement systems that can be as good as can be designed [34, 35]. This is an advantage for the attribute measurement approach in that it allows for the best possible measurements to be performed—from the point of view of experimental error—so that statistical variations of the measurements are kept to a minimum. These *optimal* measurements, along with appropriately chosen threshold values, allow for the false alarm rates to be kept to as low as possible.

In the case of a template measurement approach, defining the false alarm rate is a little trickier. There has been little work done on how to quantify the false alarm rate—from a statistical point of view—in a template measurement scenario. Clearly, the false alarm rate is a function of the overall fit to the template. However, the constraint on the goodness of the fit has $n - 1$ parameters, and there is no assurance that the goodness of fit is reflective of a poor measurement. The difficulty in quantifying false alarm rates was one of the reasons contributing to the outcome that attribute measurements were considered more appropriate for a verification regime.

Information Barriers in a Biological Weapons Control Regime

The use of an information barrier in a measurement system relevant for biological weapons has not been seriously broached to date. The reasons are twofold. First, a verification regime has not been defined for the BWC (or for a BWC-like treaty) that requires the protection of any sensitive information. Second, the exact nature of what could be considered sensitive information in a biological weapons verification regime has yet to be defined. However, recent discussions about the importance of the dual-use *dilemma* [36-41] in biotechnology indicates that use of an information barrier on a measurement system in a biological weapons verification regime may be inevitable.

The dual-use aspects of biotechnology could make verification under a biological weapons control regime daunting from the point of view of protecting sensitive information. The issue revolves around—as it usually does—the amount of information that may be shared in a verification regime versus assurance of the veracity of a measurement of the nature of a treaty-relevant item.

---

* For example, a set of items that contain plutonium.

† In most measurement systems with information barriers, there is only a binary result. A green light is indicated when the result is consistent with the declaration; while red light indicates that the result is inconsistent with the declaration. If the false alarm rate is too high for a system, which would lead to more results that are inconsistent with the declaration, this is not desirable from the point of view of the host party.

The application of information barriers to a biological weapons regime can be regarded as somewhat parallel to their use in a nuclear weapons control regime. The elements of biological weapons truly have dual-use concerns. These dual-use issues center on the fact that techniques and genetic building blocks that are used for the development of biological weapons have direct uses in various nonweapons applications. In addition, attenuated strains of biological agents may be used as vaccines or as controls for diagnostics development. This is less the case in nuclear weapons development. There are fewer defined uses of special nuclear materials and technology that might be found in nuclear weapons. These similarities and differences will need to be considered as the development of information barriers in a biological weapons regime matures.

Though differences exist between the science (and engineering) aspects surrounding the development and implementation of a measurement system for nuclear and biological weapons, there are some parallels that may be useful for the design of a verification regime. The pros and cons of using attribute and template measurement information barrier systems, as discussed earlier in this paper with respect to nuclear weapons, could also be considered for the case of biological weapons.

As mentioned in the introduction, a possible verification regime would be for a monitoring party to monitor the presence of various pathogens that a monitored party has a use for in legitimate biotechnological research. The mission of the monitoring party would be to ensure that only certain malicious pathogens are present, which have been *voluntarily* declared by the monitored party.[4]

Given complete access to an item that is declared by a monitored party it is possible in principle to fully map out the DNA sequence of that item. However, given the usual access and time constraints associated with any verification regime, this is probably not the most prudent avenue to be considered. Some of the information obtained from a complete genetic analysis of an item could be regarded as sensitive or proprietary depending on the nature of the regime. Knowledge of the complete sequence of a biological sample is analogous to having all the information about a nuclear weapon. The possession of this information by the monitoring party could pose a definite risk to the monitored party; the extent of this risk depends on the nature of the measurement process and the nature of the inspection regime.*

It is clear that a detailed sequence could in theory be determined for each *item*† that could be voluntarily declared in a regime. The sequencing information of the declared item could be regarded as the equivalent of a template in a nuclear regime. The obtained sequence could be compared to all of the possible sequences of all the possible biological agents that could be present in the verification regime to determine whether or not the declared item was consistent with the declaration. A disadvantage of a measurement system if designed in this manner is that highly detailed and potentially sensitive information would exist within the system that would need to be rigorously protected from disclosure.

It is therefore wise to search for a measurement methodology that would not require the storage of potentially sensitive information with (or on) the measurement system because it makes the implementation of an information barrier much more straightforward. One possible approach would be to seek the equivalent of attributes in the biological realm. This could be accomplished by looking only at portions of the genetic material available for measurement, portions that still would give sufficient confidence that presence of the declared material is being confirmed. This methodology is the equivalent of producing an attribute measurement system in a nuclear verification regime. This approach limits the amount of possible sensitive information that needs to be protected and allows for the seamless implementation of an information barrier.

---

* An overview of how the risk analysis for a biological regime might be performed will be introduced below.

† *Item* is used as a parallel to items in a nuclear weapons verification regime. Items in a biological weapons control could be one several classes of biological agents. In the definition of a verification regime it is necessary to choose a limited set of agents that defines the regime.

Examination of Observables

In the age of recombinant DNA research, it is impossible to fully span the space of possible pathogens that could be considered as a biological weapon. However, if one is defining a verification regime that is *voluntarily* entered into by two (or more) parties, it is possible to define a limited set of biological agents that could be included in a verification regime. For the purposes of this discussion, the items listed in **Table 1** could be chosen for the initial biological agents to be considered for a biological weapons control regime.[42]

Table 1. Possible biological items for a biological weapons control regime.

Bacillus anthracis (Anthrax)	Burkholderia mallei (Glanders)
Brucella melitensis (Brucellosis)	Chlamydia psittaci (Ornithosis)
Burkholderia pseudomallei (Melioidosis)	Clostridium perfringens
Clostridium botulinum (Botulism)	Enterohaemorrhagic Escherichia coli
Coxiella burnetti (Q fever)	Rickettsia mooseri (Typhus)
Francisella tularensis (Tularemia)	Rickettsia rickettsii (Rocky Mountain spotted fever)
Rickettsia prowasecki (Typhus)	Salmonella typhi (Typhoid)
Rickettsia tsutsugamushii (Scrub typhus)	Vibrio cholerae (Cholera)
Shigella dysenteriae (Dysentery)	Yersinia pestis (Plague)

In this initial statement of possible malicious biological agents, only bacterial species are identified as those to be considered for the initial items for a verification regime. The purpose of this exercise is to form a hypothetically agreed set of pathogens that defines a biological weapon* so that we can evaluate possible technologies that could be used to determine the nature of the items that are being considered. The *natures of the items* are the observables that define the biological agents under consideration. These observables—more than likely—will be genetic sequences to be determined that establish the item under consideration as confirming its declaration.

The genomes that define the pathogens are somewhat well known and well characterized so that they can be determined with relative ease. The advantage of limiting the original regime to a small set of observables is that a thorough risk and consequence analysis can be performed on any measurement approaches. There has been considerable advancement in the area of biological agent detection so that *almost real-time* measurements can be achieved with a little more work.

Possible Technologies for a Verification Regime

The characteristics that are important for a detector of biological weapons are presented in Ivnitski et al. [43] Their characteristics are modified and are presented in **Figure 2**.

* The assumption is that the treaty parties could agree on a limited set of pathogens to be subject to declaration and verification.

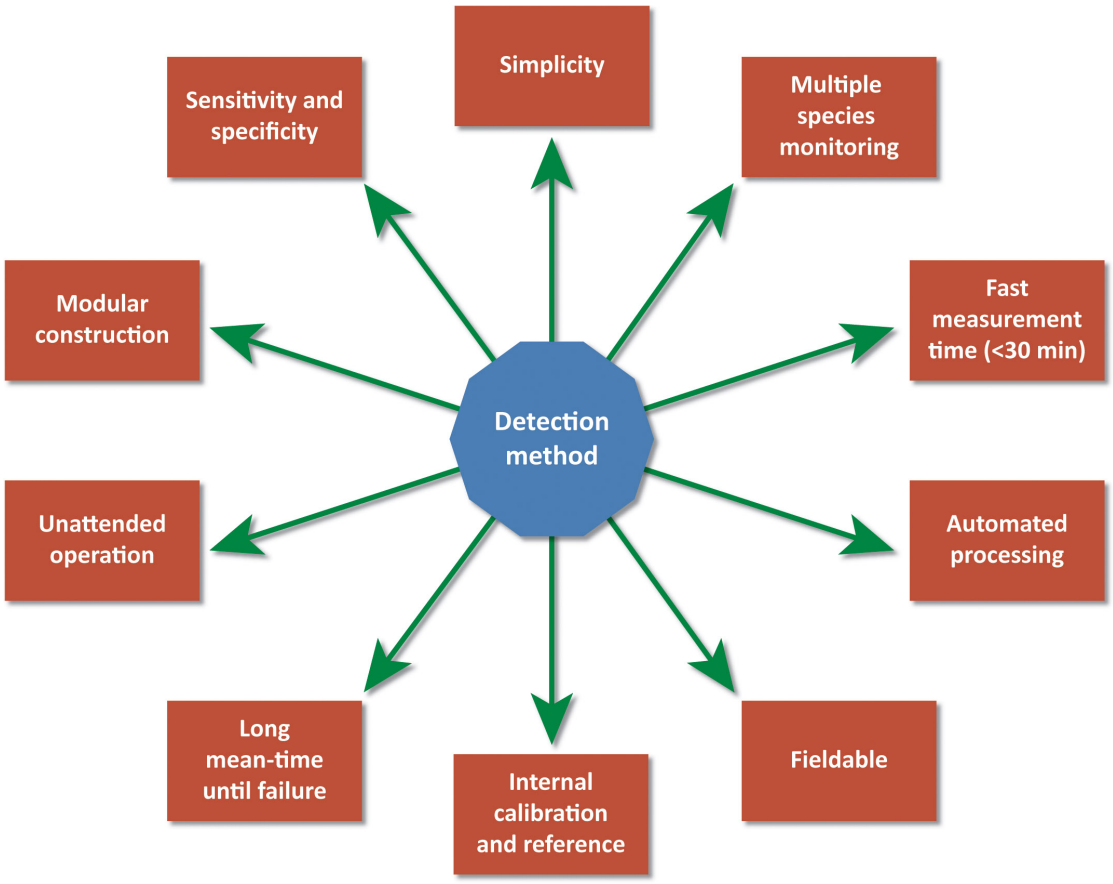


Figure 2. Characteristics of good detection systems.

The characteristics in Figure 2 are important, but an additional characteristic that is not usually considered in the development of a measurement system is authentication. This will not be considered until the discussion below.* Though all ten of the characteristics of an ideal measurement system shown in the figure are important; two characteristics are *not vital* for a measurement system that is used in a verification regime, namely unattended operation and fieldablity†. There will little need for a measurement system to be operated in an unattended fashion; in fact, it would not be prudent for a measurement system to have this characteristic because of the opportunity for deception.

There are then eight remaining characteristics of a biological weapons detection system that need to be considered when down-selecting an appropriate technology.

- Sensitivity and Specificity – are required so that the best possible measurement can be made. False alarm rates increase when the measurement sensitivity is reduced and if the instrument does not detect the species of interest. This is one of the areas where a biological regime is distinct from a nuclear regime because the detection of a *specific* biological component is required. The consequences of yellow lights, from a policy point of view, are difficult to negotiate, particularly if the false alarm rate is too great.

* The discussion of authentication of biological measurement methodology will be considered in the section on future development of information barriers for a biological weapons regime.

† The need for the system to be fieldable is important from a technology provider point of view. If the system is designed to be fieldable there is a higher probability that the system will function properly in a non-laboratory environment.

- Simplicity – the system has to be simple to operate with a very simple interface and operating procedure.
- Multiple species monitoring – the measurement system should be able to detect all species that are included as part of the regime.
- Measurement time – the time to perform a complete analysis must be significantly less than an hour. A time of 15 minutes is probably ideal, with a time of 30 minutes being reasonable. This, however, may not be possible with the present technology in the case of biological measurements. In the biological realm, time to perform an acceptable experiment is a strong function of how much material is available for testing.* Time must always be balanced against the quality of measurement.
- Automated processing – all of the data analysis after introduction of the sample needs to be performed automatically, and most likely electronically. Although a desired quality for arms control measurements, this may be questionable in the case of biological weapons because of the constraints of sample preparation.
- Internal calibration – all of the calibration should be internal to the measurement instrument with the possible exception of authentication sources that might be necessary to make sure that the measurement system operates as designed.
- Long mean time until failure – monitoring events are in most cases rare events, so the mean time until failure must be long because the measurement systems will be unused much of the time.†
- Modular construction – this makes it easier to swap out spare components when something goes wrong with the instrument.

In addition, technologies that are able to determine the sequence of a specific pathogen may require a preliminary step, *amplification*‡ of the genetic signatures. Amplification of the signatures proceeds as shown in **Figure 3**.§ The three major steps for amplification are:

1. Selection of the sequence of the gene(s) or other region(s) of interest.
2. Preparation of the sequences for replication via specific primers.
3. Replication of the selected sequences.

Details of each of these steps depend on the analysis method that is chosen, but the overall description is instructive because it brings up issues that will have to be considered in detail as a follow-on to this work.

---

* If the amount of material is *large enough* the time for analysis can be greatly reduced because the amplification step (see below) can be eliminated. The definition of *large enough* will have to be determined on a case-by-case basis for each biological species being considered.

† This is a particularly tricky proposition in the case of biological measurements because of the need for reagents in sample preparation. In addition, the use of reagents in the amplification and hybridization process leads to possibility of creating false alarms (see below).

‡ The ensuing discussion describes what could be called *target-specific* amplification of the *region(s) of interest.* There are some applications, particularly in the case of microarrays, where random or whole genome amplification is employed. This is a case if the DNA analysis is highly multiplexed. This process has drawbacks as well, because if the detection of *too many* pathogens is sought, there is a real possibility that there may be interactions between the various primers that are necessary for the specific pathogens. The degree of multiplexing needs to be considered; however, for a small set of target pathogens this may not be an issue.

§ This figure has been modified from Griffiths *et al.* p. 341.

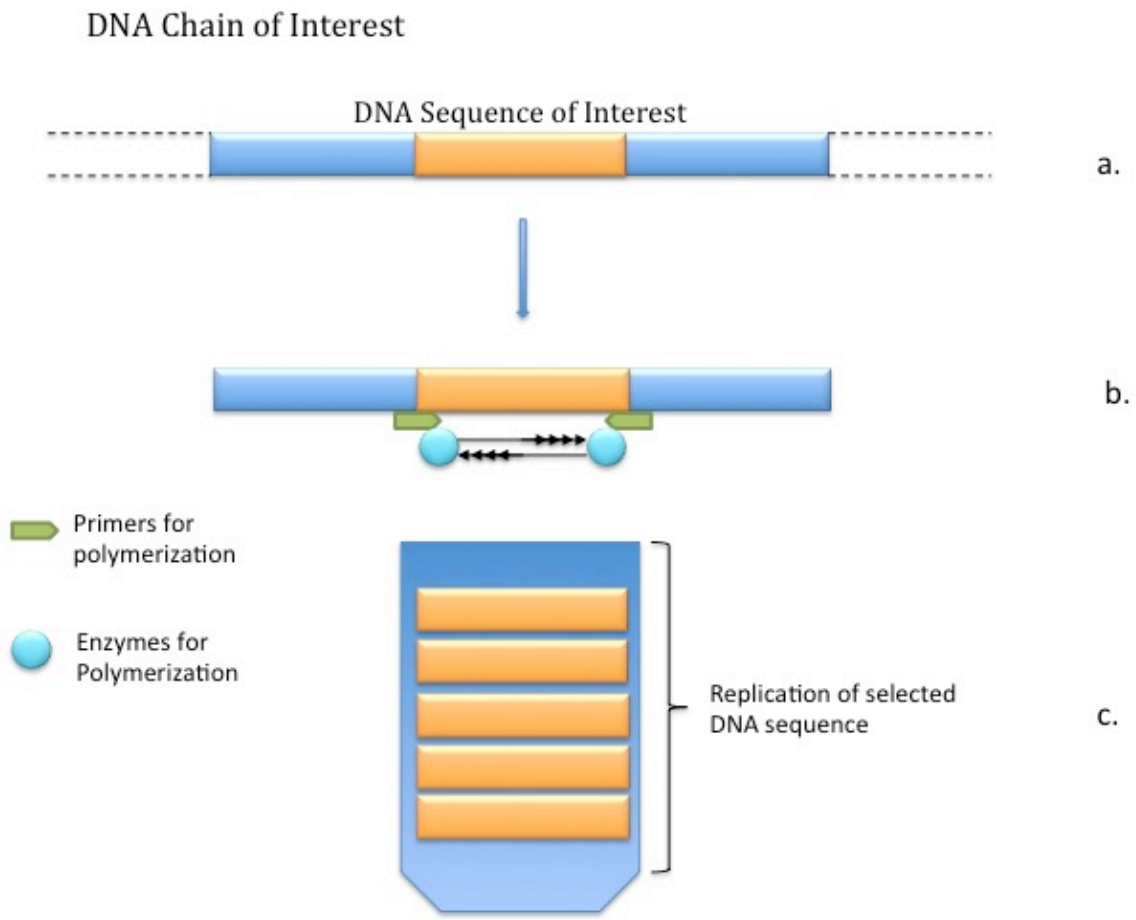


Figure 3. Amplification of DNA signatures.

In step (a) in Figure 3 the specific sequence to be amplified is selected. This will have to be determined via bioinformatics analyses for each pathogen under consideration. In some sense, this is analogous to cutting the DNA sequence out of the entire DNA sequence of the pathogen. In step (b), a suitable pair of primers to cut the sequence under consideration is chosen. These primers define the endpoints of the sequence by binding to the ends of the sequence under consideration. The primers then function to guide the replication of the DNA sequence. [44] Within step (b), enzymes are attached to the DNA sequence under consideration that allow for the replication of the DNA. Finally, in step (c) the sequence under consideration is allowed to replicate exponentially. The number of generations necessary in step (c) is a function of the detection methodology.

Steps (b) and (c) are important from the point of view of the negotiation of a verification regime because in these two steps continuity of knowledge (COK) of the original sample can be compromised. The introduction of primers of DNA polymerization and enzymes for the replication of the DNA sequence could call into question whether the sample that will be analyzed later has any relation to the original sample. The *amount* of loss of continuity of knowledge depends on the nature of the agreement. If the verification regime were constructed like the CWC and there were a list of pathogens such as that given in Table 1 that were subject to random detection, the COK of the sample is less of an issue. If, however, a monitored party declared a sample to contain a certain pathogen, the COK issue is now forefront for step (b). The issues involved with the COK in this case will have to be considered in detail as the work on information barriers for biological weapons agreements continues. Similarly, step (c) introduces

continuity of knowledge issues. It is not clear if the level of uncertainty is a function of the number of replication cycles.* This will have to be considered in the future.

There are three possible approaches for the presence of regime-relevant pathogens in a declared sample: Polymerase Chain Reaction (PCR), sequencing, and microarrays. [45] The diagram† in **Figure 4** shows a pictorial representation of the strengths of these three methods as a function of cost and time to obtain results. As this diagram indicates there are certain areas of application space where each of these methods could be applied. Clearly any one of these techniques *could* be used in a verification regime, but each of these methods has limitations that prevent their consideration for a measurement technology. These will be discussed below.

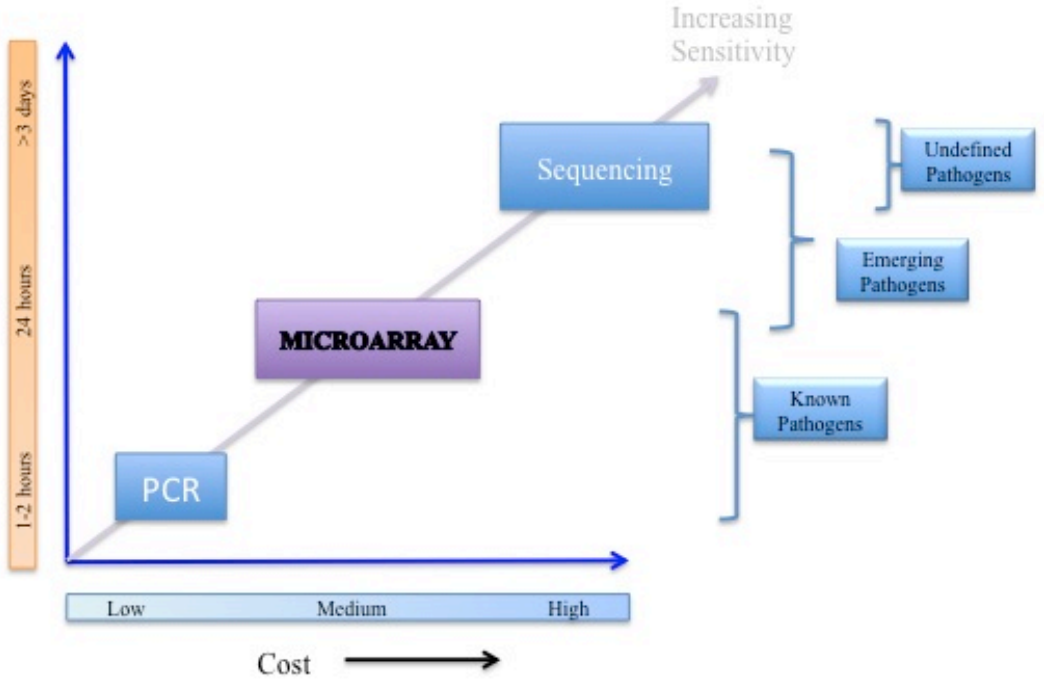


Figure 4. Three methods for the determination of DNA signatures.

Polymerase Chain Reaction (PCR)

The PCR methodology (alone‡) [46-50] from a standpoint of verification regime has some very positive attributes, such as low cost and fairly rapid turnaround§. The sensitivity of the methodology may relegate the method as less useful in a bioweapons regime. The other shortfall of this method is the limited application of the method to a wide number of pathogens at one time. However, given that a perceived verification regime only focuses on at the most 20 pathogens, this methodology might be applied. However, since it is desirable to have a number of signatures (say six to reduce the false positives) for

---

* At first sight it seems that the level of uncertainty is independent of the number of DNA amplifications. However, this is unknown at this time.

† See C. Jiang.

‡ The PCR methodology is also used within the MDA (see below) to amplify the original sample of DNA if the amount of material is sufficiently small. The necessity for PCR as an amplification process also has some issues for the authentication issues. There is a possibility for loss of continuity of knowledge in this process. This will be discussed in detail below.

§ Time of measurement in some sense is the most vital constraint in a verification regime. In any monitoring regime the time for individual measurements must be on the order of an hour or less.

each bacterial pathogen the number of signals clearly stretches the capabilities of this methodology. That being said, it is not clear that even for a small number of pathogens being considered that PCR alone will be a suitable solution for the measurement approach. This is unfortunate because the PCR approach is the gold standard for pathogen detection in terms of sensitivity, particularly if the amount of material to be examined is small.

The PCR methodology in essence is a means to amplify the amount of DNA that is being analyzed so that the signal might be increased. The general features of the amplification process were described above. The polymerase primers are chosen specifically for the genome sequence that is being measured. This process is not usable in the case of unknown biological agents, but in the case of determining whether something known is present in the sample. This approach is quite feasible. The problem arises because the primers are very species-specific and will require multiplexing reactions if many species are being considered. [45] Again this is not a showstopper, but there are limits to optimize the reaction process if identification of large numbers of pathogens is being sought. After the amplification has been accomplished, the resultant DNA is tagged* so that the sequences can be determined by a suitable spectral method. Determination of the sequence involves analysis of the spectral data and the identification of which signatures are present by several possible methodologies.

DNA Sequencing

Clearly the best way to determine the nature of a declared pathogen under a bioweapons verification regime is the complete sequencing [51, 52] of all of the genetic material in a sample. This methodology has at least four shortcomings. The first is the time it would take to perform the analysis itself. The time involved would be at least on the order of days. This timescale is not acceptable for a verification regime. Second, the cost would be prohibitive for any kind of realistic measurement scenario. Even though the time and cost of this analysis is decreasing rapidly, there still is no fully automated sample-in/analysis-out sequencer available at this time. Third, it would be difficult to assure continuity of knowledge of the sample during the analysis process. Fourth, measurement (e.g., sequence analysis) protocols would have to be constructed very carefully. The procedures may need to be so detailed that they might reveal information about the items under consideration.

The approach to *complete* DNA sequencing of a purified microbial organism is somewhat similar to the PCR process described above. The entire DNA chain is *cut* into pieces. Amplification of the DNA is employed using random primers, and the procedure is completed as above. The fragments are all analyzed, and a sequence is constructed,† a process that is rather time and computationally expensive. An even more complex case is the *metagenomic sequencing* of a complex (nonpurified) sample that might contain DNA from a very large number of organisms. Typically the DNA fragments from this kind of sequencing cannot be re-assembled, but instead each short DNA read is mapped to known genomes. Determining what organisms are likely present is a complex (and as-yet not fully solved) research problem, as many genes are common across wide swaths of bacterial organisms.

Microarrays

The microarray detection approach[45, 53-63] takes advantage of random amplification and uses specific templates (called *probes*) for the target sequence. Basically, the microarrays lay out the complementary sequences to the sequences that are being sought. DNA from the sample is fragmented and optionally may be amplified using either specific or random amplification, depending on how many total genomic regions are being targeted. The fragments from the specific pathogens that are present (if present) attach

* It is actually the individual bases that are tagged so that each base (A, T, C, G) of the DNA sequence possesses, for example, a distinct color.

† The reconstruction of the original chain is daunting, but it is not intractable. The reconstruction is helped by specific chemical details about how each base pair is attached to each other, which is beyond the scope of this present work.

themselves to probes on the array that have been designed for the specific regions of interest. An artist's rendition of this process is shown in **Figure 5**.[45]

The array is analyzed and compared to the analysis of all potential genomes being exposed to the array to determine which genetic species have bound themselves to the array. The array can be constructed for any number of specific regions of any number of specific pathogens so that it is a very sensitive methodology for the detection of a set of possible pathogens.

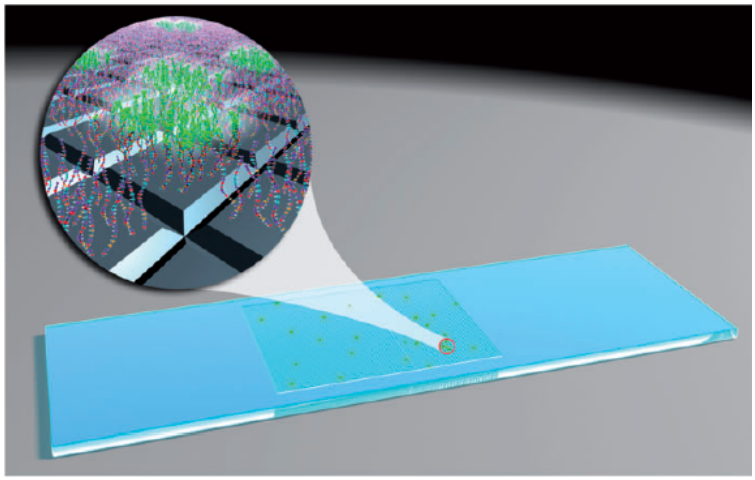


Figure 5. Artist's rendition of DNA strands attached to an MDA.

Microbial Detection Array as a Possible Solution

As was indicated above, MDA techniques [45, 53-63] could be a solution to the determination of attributes analogous to nuclear weapons. It would be possible to construct an array* that was sensitive to all eighteen pathogens indicated in Table 1. McLoughlin [45] discusses several approaches that might be ways to design arrays that might be used for a possible regime.

In the first step, the complements to the samples to be considered are laid out on a blank array. It is this array that is used for detection of the specific sequences. The sample is processed by random amplification, if amplification is necessary. The genetic material is extracted and labeled (usually) with fluorescent dye, and the labeled genetic material is allowed to interact with the array (hybridization). The genetic material with specific characteristics matching the probes on the array is bound to its complements on the target array. The array is placed in a fluorescence scanner, and the resultant signal is recorded. The image is analyzed and compared to both a control and a combination of all possible pathogens. This analysis may prove to be rather involved if the number of pathogens (or targets) for the regime grows too large. Development of the analysis methodology may require joint development by all parties involved in the verification regime.[28]

The description by McLoughlin [45] of the Lawrence Livermore microbial detection array (LLMDA) [45, 57-59] indicates that it might be a solution to consider as part of a future instrument for a biological weapons regime. The design of the LLMDA is more than adequate for a regime that is considering only 19 pathogens. The necessity for only a having known pathogens makes the design of the array itself much simpler than a generic *detection* array. The analysis is simplified, as well, since all of the possible results for all 19 pathogens could be local. The analysis is somewhat analogous to template analysis in the discussion above. As opposed to the nuclear case, information about the sequences of the 19 pathogens would not be sensitive. Any sensitive material in all likelihood would have been stripped off during the probe design process, so it could not be detected via the microarray.

* The current version of the LLMDA is sensitive to 900 sequenced bacteria and over 2200 sequenced viruses. Due to the large number of targets (>350,000) the LLMDA methodology employs random amplification to limit the primer interaction discussed in footnote ‡ on page 16. If the regime is confined to a small number of pathogens, it may be possible to use specific amplification because of the small number of primers needed (<100).

Risk Assessment

In defining the biological weapons control verification regime, it is useful to remember that a risk factor must be assigned for the information being protected. In the case of nuclear weapons—at least from the point of view of the United States—the information being protected is defined under The Atomic Energy Act of 1954 and Executive Order 12958. This is still being defined for a biological regime. The value of the information must be considered on a case-by-case basis. For the sake of argument, assume that a proprietary backbone exists in the genome that is declared under the agreement. The genetic backbone would be discovered if the genetic material from the declared material were fully sequenced. The risk associated with the loss of this information depends on the preciousness factor of the information. More than likely, in the case of biological weapons this preciousness factor would be based on financial loss. There may be proprietary methods that involve BW-significant materials that are used by the companies that have a legitimate need to possess questionable pathogens. Defining the preciousness factor will have to be determined for each regime and for each material to be declared.

Note that this question is almost exactly analogous to one currently being faced by those charged with regulating *Select Agents* in the United States: What, exactly, defines the difference between a Select Agent and an organism that is similar, but not subject to, the same regulation? The current Select Agent definition is organism-based and is clearly inadequate for the 21st century. (Modern genetic engineering could put all the nasty bits of a pathogen into a nonpathogen chassis.) A recent National Academy panel examined the question of what scientific advances are needed to turn this definition into one based on gene-resolution instead of organism-resolution. It is likely advisable to ensure that the mechanism used to implement information barriers for BWC compliance verification be congruent with the evolution path of Select Agent legal definition.[64]

When considering the risk of loss of information, it is necessary to understand the consequences of loss of the information by the host party. This issue is similar to the broader issue of *dual-use* in biotechnology and was addressed in an NRC report in 2004.[39] In this report the authors examined three important questions to be considered before releasing information to the public domain. [39]

- What categories of genome data present the greatest concern?
- What are the pros and cons of unlimited vs. restricted access to such data, including threats posed to the scientific community or to national security?
- What are some options for making decisions about release to the public domain?

These three questions are also important to risk analysis of information in any treaty regime. The first of these questions must be answered when a regime has been defined. However, as was discussed above, there is undoubtedly proprietary information based on how the pathogens have been prepared and how they are used in legitimate applications. Genomics has become significantly advanced so that a great deal of information can be obtained from a complete genetic sequence. To define the effect of loss of proprietary information, there will need to be coordination among several governmental agencies and interaction among the companies involved in the production of the various genetic materials. The model for this might be something like the Chemical Weapons Convention, but the problem is less defined than the CWC schedule of chemicals. In fact, there is some probability that a schedule of genetic backbones may be sensitive as well. However, this would have to be worked out within the structure of any agreement with the full cooperation of the companies involved. Such a public/private interaction would be rather unprecedented.

The national security portion of the second of these questions is more than likely not a concern in this discussion. However, as work continues in this realm, national security aspects of any of the pathogens being considered may become more important. The release to the scientific community, in general, has some interesting aspects. One of the most important aspects is the peaceful use of questionable pathogens

in, say, the pharmaceutical regime. These issues will have to be considered on a case-by-case basis as they arise in the future.

The last of the three questions is interesting, but has no bearing to the risk assessment of the loss of material. The disclosure of the use of dangerous pathogens in peaceful applications may cause more stir than anything risky.

Several approaches to risk assessment have been described in many different venues [65-71]. The bottom line of these approaches is that there has not been*

> *"… found a single formula or application that will cover the security needs of all organizations for all situations."*

This statement can be extended to verification regimes as well. There is no single solution for all possible biological regimes. By definition risk assessment is†

> *"… a formal and systematic analysis to identify or quantify frequencies or probabilities and the magnitude of losses to recipients due to hazards (physical, chemical, or microbial agents) from failures …"*

To understand if and how an information barrier may be applied to a measurement system, it is necessary to understand how, with what probability, and with what consequence the loss of information can occur. These considerations are related to the three questions that Kaplan et al. [72] pose concerning risk analysis:

1. What can happen?
2. How likely is it that this will happen?
3. If it does happen, what are the consequences?

In terms of the present discussion, these questions are translated to the following three questions:

1. What information can be lost?
2. What is the probability of loss?
3. What – if any – are the consequences of the loss of information?

The most important point of contention is to understand what information can be lost and, as a caveat, where that information can be lost in the measurement process. This is clearly a function of the nature of the type of data being considered and the measurement system itself. The nature of the data is important because it defines how the data are handled. Examples of the characteristics of the data might be as follows:

- Are the data under consideration in scalar or vector format?
- Are the raw data relevant, or is only the processed data of importance?

These questions must be considered when determining how data might be lost. The importance of the measurement system is that it defines how the information is handled. In addition, it defines how design features might be implemented to control the possible loss of information.

---

* Broder, p. xvi.

† Modarres, p. 7.

It should be noted that even when these questions are considered fully, some individuals might express the following opinion:*

> *"A risk analysis is essentially a listing of scenarios. In reality, the list is infinite. Your analysis, and any analysis, is perforce finite, hence incomplete. Therefore no matter how thoroughly and carefully you have done your work, I am not going to trust your results. I'm not worried about the scenarios you have identified, but about those you haven't thought of. Thus I am never going to be satisfied."*

This viewpoint was expressed when risks were evaluated during development of information barriers for several demonstrations involving nuclear weapons and components. However, it is important to distinguish between the idea of uncertainty of loss of information and the consequences of loss of information. In the development of information barriers, and after all risks have been considered, there remains a vanishingly small probability† that information will be lost, and that small probability of loss may be unacceptable to some individuals.

The idea of information loss analysis is analogous to standard probabilistic risk analysis (PRA). Kaplan and his collaborators [72] discuss PRA in terms of a *set of triplets* where the triplets *are* s_i, p_i, *and* x_i that correspond to the scenario, probability p_i that scenario s_i will occur, and the consequence x_i of scenario s_i. This formalism allows for the determination of the risk of each event (scenario) and allows for the construction of the total risk for a given system. This approach takes advantage of the opportunity to understand and define each scenario completely. The probability of the occurrence can be individually determined, so a probability for the absolute risk can be assigned based on Bayesian formulation.

The understanding of information loss is distinct from classical PRA because the assessment of any information loss must be determined **before** the system can be built. In principle, if the measurement system is made up of components, the information loss probability could be assessed for each component. However, there is some *gestalt* aspect to the performance of a system of components. This being the case, the idea of a joint probability of occurrence and consequence must be contemplated. This implies that designers of the measurement system and information barrier need to work in concert to understand the probability and consequence of occurrence of information loss at any point of the measurement process. In many ways, this will be more of an art than empirically based. How this methodology will be applied to the idea of an information barrier in a biological weapons regime will have to be studied in detail as a measurement protocol for such a regime has been defined.

To construct an appropriate information barrier, an analysis of information loss would proceed in an analogous manner to PRA:‡

1. Level 1, systems analysis.
2. Level 2, systems plus consequence analysis.
3. Level 3, systems, consequence, and containment analysis.

In the level 1 analysis, the overall nature of the measurement system and protocol would need to be considered. At this level of analysis the nature and the mechanism for information loss would need to be

* Kaplan, S. and B.J. Garrick, p. 14.
† The probability of loss approaching zero.
‡ Bedford and Cooke, p. 11.

determined. This is what Kaplan *et al.* [72] call the scenarios. How these scenarios might be described and determined in a biological weapons regime is introduced in the next section entitled Loss Analysis.*

Level 2 analyses involve understanding the consequences of information loss within the confines of the protocol being considered. It is clear that when the nature of the information that could be lost is determined, the consequences must also be determined. Analysis levels 2 and 3 are reversed in information loss analysis versus PRA. The reason for this is evident because, though information might be lost, there may not be any consequences that matter to any of the parties in a given agreement. If there are no *grave* consequences to loss of material, then it is not necessary to perform a level 3 analyses for that particular event. In PRA all events have some consequences that matter to the system as a whole. Therefore, mitigation of events must be considered before consequences are defined. A qualitative measure of the *preciousness* for loss of information must be defined at this point in the analysis. In the case of nuclear information, the qualitative *preciousness* factors are defined in the various classification guides developed by the DOE and DOD. The *preciousness factors* for information that is not explicitly stated in the guides must be derived at the highest levels of the Interagency. It is not clear that analogous guidance exists for biological information. Data need to be systemized before an information barrier for a measurement system can be considered.

If the consequences of the loss of information warrant mitigation, then a level 3 analyses must be performed on the event to understand how to contain that information loss. This is the point that the information barrier is actually conceived for the system under consideration. This analysis will necessarily involve the developers of the measurement system, representatives of the agencies involved in the development of the agreement, and representatives of the private sector with vested interest in the information being considered.

The scientific basis for Information Loss Analysis (ILA) is at its infancy. A great deal of work needs to be performed in this area as the need for the development of information barriers increases.

Loss Analysis

Where and how information can be lost in the measurement process depends greatly on the measurement system being considered and the information that is being obtained. In general, there will be multiple potential points of information loss for a given piece of data. The determination of loss points aids in the understanding how an information barrier may be implemented. Since, in the present discussion, a regime and/or measurement system has not been defined, it is useful to consider a simple example of what a measurement procedure might look like for a biological weapons verification regime.

In a measurement regime, two kinds of losses are important:

- The actual loss of information, which is directly related to the information barrier.
- Loss of information concerning the fidelity of the sample. Though this is not directly related to the information barrier, it is important in understanding the fidelity of the measurement process. This is really the expression of the loss of continuity of knowledge of the sample's identity in the measurement process.

Both of these issues are important in the construction of any kind of measurement system. Even though the second issue is not directly related to data protection, it is important in constructing a measurement system that is useful for the performance of a measurement system.

---

* In principle, that discussion could have taken place in this section, but it was separated from the general risk analysis discussion to call attention to the fact that it is vital for any discussion of information barriers to determine where and how information can be lost.

To understand where information can be lost within a measurement system, the system must be thoroughly studied. In a generic sense, this is nearly impossible to accomplish. It is useful to look at a concrete example to understand the possible areas where information can be compromised. Consider the model measurement system shown in Figure 6.

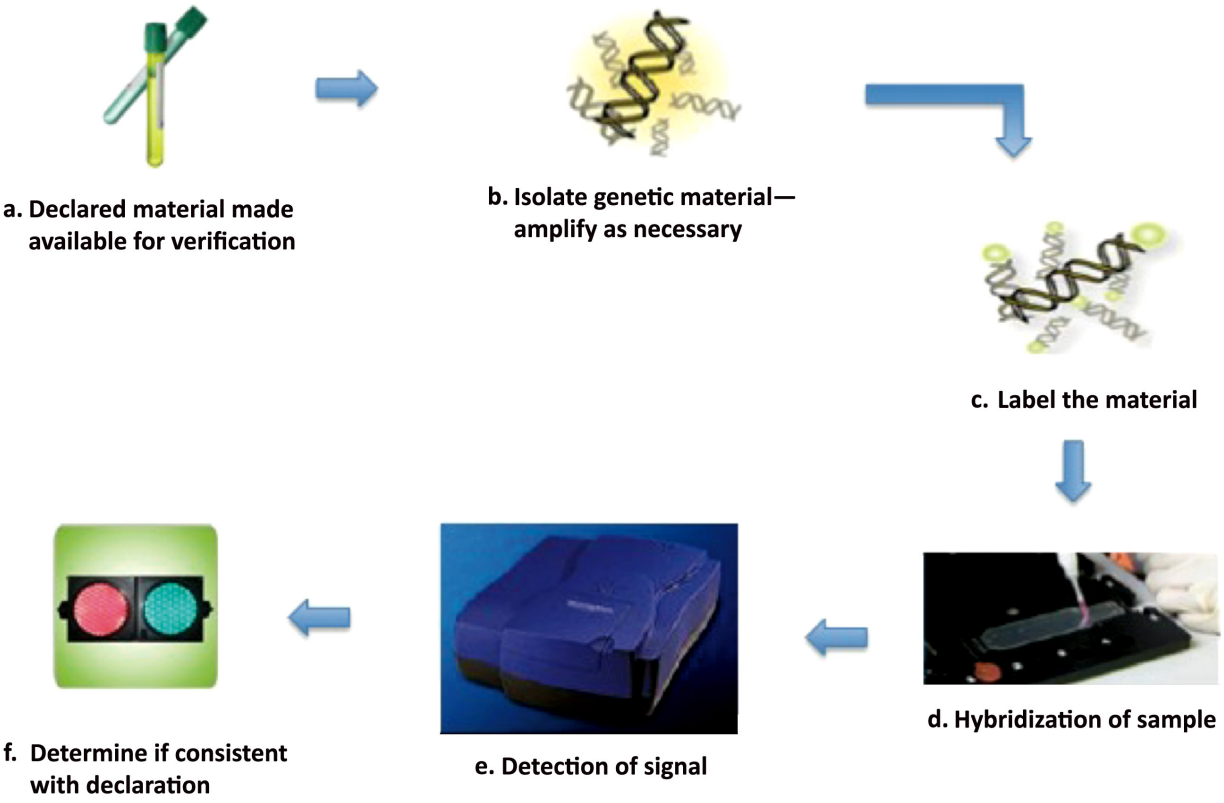


Figure 6. Example of a measurement that could be used in a verification regime.

The process for the measurement has six distinct steps:*

a. The material to be considered by the inspecting party is declared by the inspected party. In most cases this is just a formal step undertaken by the inspected party because in a vast majority of cases the measurement system is under host control. The inspecting party in this step ensures that the container, which contains the agreement relevant material, is consistent with the declaration. It is not clear what this means in the context of a biological weapons verification regime. There are no preliminary tests that the inspecting party can perform to ensure the hint of compliance by the inspected party. This step will need to be negotiated on a case-by-case basis by the agreement partners.

b. The material that is given over for verification is isolated and amplified as necessary by some sort of PCR process. If the number of required signatures is small, then specific PCR amplification can be applied. This limits the possible primer-primer interactions that occur when a large number of signatures is considered. This step has inherent issues concerning data integrity.

* It is generally prudent to keep the number of steps in a measurement as low as possible because each step is a point of vulnerability. In an actual verification regime these steps might be able to combined; however, allowing them to be separate in this exercise allows for a detailed understanding of how the analysis might proceed.

Figure 7 shows a sketch of a system that could avoid these issues. This step allows for the breaking down of the initial material under consideration. In addition, the step can involve amplification of the genetic material. The amplification and isolation of genetic material involves the introduction of other agents (primers and enzymes) that allow for this step to be completed. Care must be taken that the inspecting party understands the intimate details of this process because continuity of knowledge may be compromised. The detailed information involved in this step indicates that joint development may be prudent.

c. This step involves the introduction of additional material to the materials that are being verified. This is an authentication nightmare. The process is somewhat sublime because the step simply involves the attachment of a label to the individual bases. These markers are relatively standard; however, the nature of the labeling molecules will have to be understood by all the parties involved in the agreement.

d. This step involves the hybridization of the labeled sample so that it can be allowed to attach itself to the suitable MDA array. Though not considered explicitly in this discussion, the DNA arrays will have to be authenticated by the inspecting party. This could possibly be done by the use of pathogen standards. Once again, the sample is subjected to external stimuli that allows for the material to be prepared for further use.

e. This step involves exposure of the MDA array to the suitable photonic sources, collection of the scattered light data on a suitable detector—typically some CCD—and analysis of the image. The analyzed image results are compared to all of the signals that could be obtained if there were any of the pathogens or a combination of any of the pathogens present in the sample.

f. Results of analysis are given as a red light/green light response to the presence of any of the pathogens that might be present in the sample. It is important remember that there only be a red light/green light response to the measurement.* Whether the result is consistent with the declaration will be outside the privy of the measurement system.

Without a detailed study of the measurement procedure, it seems that steps (b) and (e) are the points of the measurement process that have the highest probability for the release of sensitive information. Even though in step (b) a specific portion of the DNA has been targeted for amplification, there is a chance that information about the entire sequence might be lost. This could arise from the type of primers and enzymes chosen for the process. If all of these materials are shared among all of the agreement partners, the monitoring party may be able to ascertain some of the details about the entire sequence of the genetic material.

In addition, there is a chance that some information could be lost in step (e). The image of the MDA exposed to a suitable photonic source has more information than just the sequence information about the pathogens under consideration. If the image were analyzed fully, it could reveal more information about the original sequence.

It is clear that a great deal of work is needed to understand the measurement process when a technology has been chosen and a verification regime has been defined. This work will lead to quantities similar to the p_i in PRA that defines the probability for the release of information. It may also be possible to construct a *probability of information loss*. Whether this can occur or not will depend on continued work.

* It is not clear if the goal to only have a red light/green light process to a measurement in a biological regime is tractable. This will need to be addressed experimentally when a regime has been determined and a measurement system has been developed.

Path Forward for Information Barrier Development

The Microbial Detection Array may be a way to implement a biological weapons control verification regime. Some work still needs to be done however. The first is to decrease the time for the PCR process from hours to minutes. The second is that the time for hybridization must be decreased as well if possible because it is the *rate-determining* step in the analysis process. Recent work by Wheeler *et al.* [50] addresses a methodology that has reduced PCR to the minute timeframe, but this implementation is still not usable for a verification regime. However, increasing the rate of the hybridization process has not been addressed. In addition, a great deal of work needs to be done in the design of suitable MDAs for a verification regime that involves all of the pathogens considered in Table 1.

The suggested path forward for information barrier development in a biological weapons regime is as follows:

1. Systemization of what information is regarded as sensitive. In addition, what are the categories of genetic information that might be considered sensitive? For example, what is the genetic starting material that is considered sensitive?
2. Continued development of PCR technology that drives the time of amplification down to the minute timeframe with instrumentation that is fieldable in a verification regime context. Fieldable in a *verification regime* has a multi-faceted meaning. The system must be self-contained. All of the analysis must be able to be performed in the presence of the monitoring party. The system should be, at most, a tabletop system. In addition, the system must be as simple as possible and authenticatable
3. Considerable work needs to be done to understand the degree of amplification versus false alarm rate for a given measurement and for each pathogen under consideration.
4. Continued development of MDA arrays that can be used with the small set of pathogens considered in this paper.
5. Continued development of reducing the time of array hybridization from hours to minutes.
6. Integration of the latest PCR technology with the appropriate MDA arrays to understand system performance issues and information loss mechanisms.
7. Examination of the authentication issues related to the integrated instrumentation.
8. Development of databases that can be used locally for analysis of the sequencing data.
9. Development of a single-purpose electronics package that could result in analysis on a chip.*

Finally, an instrument like the one shown in Figure 7, conceived by Jaing in [58], might prove to be an ideal technical foundation for the measurement system in a biological weapons verification regime.

* Although this does not exist at present, such development needs to be included in all discussions.

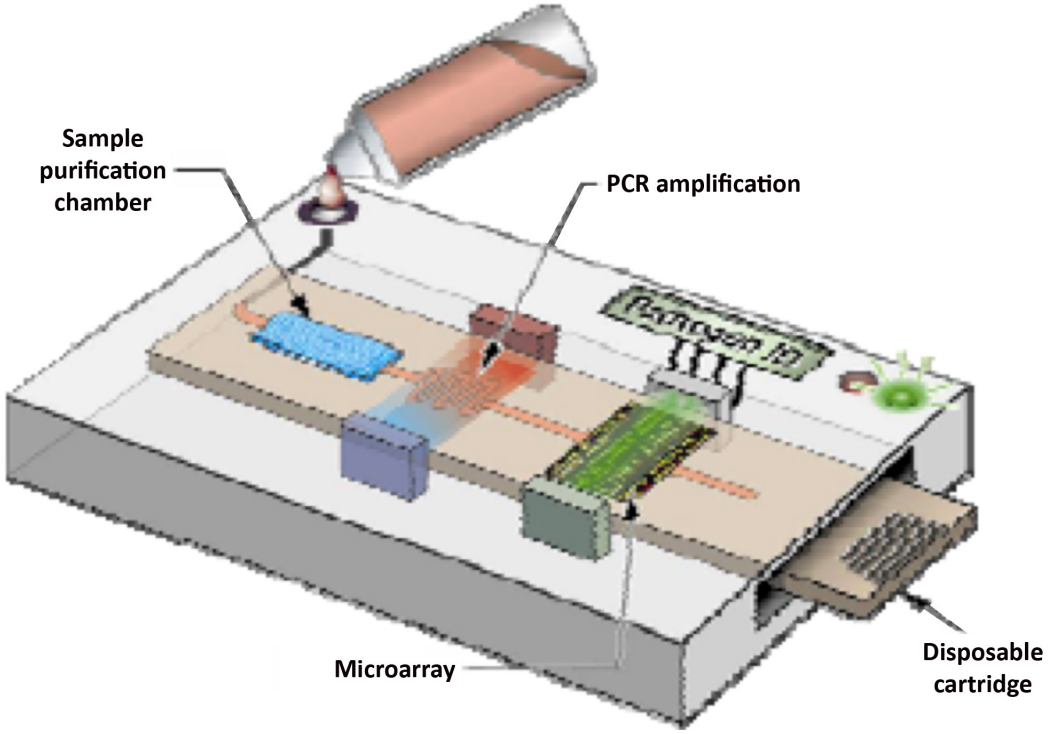


Figure 7. Sketch of a possible instrument for biological weapons verification.

Summary

Information barriers may play a vital role in any future biological-weapons-control verification regime. There is sufficient evidence that sensitive and/or proprietary information exists in the biotechnology associated with the determination of the genetic structure of weapons pathogens. This information could be either in the area of financial loss or national security. The nature of the information will have to be determined as details of a verification regime unfold.

The Lawrence Livermore Microbial Detection Array (LLMDA) is a possible technical solution to any future verification regime that requires measurement of a small set of pathogens related to biological weapons. A great deal of progress has been made in PCR reaction processing, which makes real-time determination of the presence of defined pathogens a reality.

This report provides a path forward for the development of information barriers in a biological weapons control regime. The report has defined a methodology by which information barriers might be implemented using biological detection. The report introduces the idea of Information Loss Analysis (ILA) that could be thought of as an analogy to Probabilistic Risk Analysis. The formulation of ILA will occur as the mathematical basis for information loss is pursued. Continued work in the development of information barriers will be greatly helped with a detailed understanding of ILA.

Finally, the examination of information barriers in different contexts is very important. This discussion will become more fruitful as the verification regimes become more defined. The use and necessity of information barriers in a future biological weapons regime seems likely but will be crystalized when a biological weapons verification regime has been established.

References

1. United States. Arms Control and Disarmament Agency., *Convention on the Prohibition of the Development, Production, Stockpiling, and Use of Chemical Weapons and on Their Destruction*1993, Washington, DC: U.S. Arms Control and Disarmament Agency : For sale by the U.S. G.P.O., Supt. of Docs. x, 187 p.
2. UNOG. *Confidence Building Measures*. 2011; Available from: http://www.unog.ch/80256EE600585943/(httpPages)/EC2E2D361ADFEE7C12572BC0032F058?OpenDocument.
3. UNOG. *Seventh Review Conference of the Biological Weapons Convention*. 2011; Available from: http://www.unog.ch/80256EE600585943/(httpPages)/1CD974A1FDE4794C125731A0037D96D?OpenDocument.
4. Walker, J.R. and T. Phillips, *The Biological Weapons Convention and the biopharmaceutical industry: The views of the United Kingdom.* Nature Biotechnology, 1998. **16**(4): p. 310-310.
5. Close, D.A., D.M. MacArthur, and N.J. Nicholas, *Information Barriers - A Historical Perspective*, 2000, Los Alamos National Laboratory: Los Alamos, NM.
6. Fuller, J.L. and J.L. Wolford, *Information Barriers*, 2001, IAEA: Vienna, Austria.
7. Williams, R.B., et al., *Advances in Information Barrier Design*, in *INMM 46th Annual Meeting*2005: Phoenix, Az.
8. Wolford, J.L. and D.W. MacArthur, *Safeguards for Nuclear Material Transparency Monitoring*, 1999, Lawrence Livermore National Laboratory: Livermore, CA.
9. Sastre, C., *CIVET a Controlled Intrusiveness Verification Technology*, 1988, Brookhaven National Laboratory: Upton, NY.
10. Zuhoski, P.B., J.P. Indusi, and P.E. Vanier, *Building a Dedicated Information Barrier System for Warhead and Sensitive Item Verification*, 1999, Brookhaven National Laboratory: Upton, NY.
11. Johnson, M.W. and T.B. Gosnell, *Progress toward Mutual Reciprocal Inspections of Fissile Materials from Dismantled Nuclear Weapons*, in *36th INMM Annual Meeting*1995: Palm Desert, CA.
12. Koenig, Z.M., et al., *Plutonium Gamma-Ray Measurements for Mutual Reciprocal Inspections of Dismantled Nuclear Weapons*, in *36th INMM Annual Meeting*1995: Palm Desert, CA.
13. Hass, E., A. Sukhanov, and J. Murphy, *Trilateral Initiative: IAEA Authentication and National Certification of Verification Equipment for Facilities with Classified Forms of Fissile Material*, 2001, IAEA: Vienna, Austira.
14. Langner, D.G., et al., *Complementary Technologies for Verification of Excess Plutonium*, in *INMM Annual Meeting*1998.
15. Luke, S. J., et al., *Verification of the Presence of Weapon-Quality Plutonium in Sealed Storage Containers for the Trilateral Initiative Demonstration*, 2001, IAEA: Vienna, Austria.
16. Nicholas, N.J., et al., *Nonintrusive verification attributes for excess fissile materials*, 1997.
17. Shea, T.E., *Report on the Trilateral Initiative: IAEA Verification of Weapon-Origin Material in the Russian Federation & the United States.* IAEA Bulletin, 2001. **43**(4): p. 49-53.
18. Shea, T.E., *The Trilateral Initiative: A Model For The Future?* Arms Control Today, 2008.
19. Avens, L.R., J.E. Doyle, and M.F. Mullen, *The Fissile Material Transparency Technology Demonstration*, 2001, Los Alamos National Laboratory: Los Alamos, NM.
20. Johnson, M.W., *Attributes and Thresholds in Measurements for Transparency Initiatives*, in *INNM Annual Meeting*2000: New Orleans, LA.
21. Luke, S.J., et al., *Results of Gamma-Ray Measurements from a Recent Demonstration for Russian Technical Experts*, in *42nd INMM Annual Meetiing*2001: Indian Wells, CA.
22. Roybal, D.G. *Fissile Material Transparency Technology Demonstration*. 2001; Available from: http://www.lanl.gov/orgs/n/n1/FMTTD/index_main.htm.

23. Whitestone, R. and D.M. MacArthur, *Fissile Material Transparency Technology Demonstration Attribute Measurement System with Information Barrier: Functional Requirements*, 2000, Los Alamos National Laboratory: Los Alamos, NM.
24. Wolford, J.K., *Gamma Ray Measurement Information Barriers for the FMTT Demonstration System*, 2000.
25. Budnikov, D., et al., *Progress of the AVNG System - Attribute Verification System with Information Barriers for Mass Isotopics Measurements*, in *46th INMM Annual Meeting*2005: Phoenix, AZ.
26. Kondratov, S., et al., *AVNG System Demonstration*, in *51st INMM Annual Meeting*2010: Baltimore, MD.
27. Kondratov, S., et al., *Testing the AVNG*, in *51st INMM Annual Meeting*2010: Baltimore, MD.
28. Luke, S.J., *AVNG as a Test Case for Cooperative Design*, in *51st INMM Annual Meeting*2010: Baltimore, MD.
29. Modenov, A., et al., *AVNG System Software - Atribute Verification Ssystem with Information Barriers for Mass and Isotopics Measurements*, in *48th INMM Annual Meeting*2005: Phoenix, AZ.
30. Razinkov, S., et al., *The Design and Implementation of the AVNG*, in *51st INMM Annual Meeting*2010: Baltimore, MD.
31. Karpius, P. and R. Williams, *Designing a Minimum-Functionality Neutron and Gamma Measurement Instrument with a Focus on Authentication*, 2008, Los Alamos National Laboratory: Los Alamos, NM.
32. Thron, J., et al., *Next Generation Attribute Measurement System*, 2008, Los Alamos National Laboratory: Los Alamos, NM.
33. Thron, J., et al., *Designing a 3rd Generation, Authenticatable Attribute Measurement System*, 2009, Los Alamos National Laboratory: Los Alamos , NM.
34. Liu, S.P., et al., *Template identification technology of nuclear warheads and components.* Chinese Physics B, 2008. **17**(2): p. 363-369.
35. MacArthur, D.W. and D. Langner, *Attribute Verification Systems: Concepts and Status*, in *ESARDA*2003: Stockholm, Sweden.
36. Atlas, R.M. and M. Dando, *The dual-use dilemma for the life sciences: perspectives, conundrums, and global solutions.* Biosecurity and Bioterrorism-Biodefense Strategy Practice and Science, 2006. **4**(3): p. 276-86.
37. DaSilva, E.J., *Biological warfare, bioterrorism, biodefence and the biological and toxin weapons convention.* EJB Electronic Journal of Biotechnology, 1999. **2**(3).
38. Miller, S., *Ethical and philosophical consideration of the dual-use dilemma in the biological sciences*2008, New York: Springer.
39. National Research Council (U.S.). Committee on Genomics Databases for Bioterrorism Threat Agents. and National Academy of Sciences (U.S.), *Seeking security : pathogens, open access, and genome databases*2004, Washington, D.C.: National Academies Press. 74 p.
40. National Research Council (U.S.). Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology., *Biotechnology research in an age of terrorism*2004, Washington, DC: National Academies Press. xiv, 147 p.
41. Scientists, N.R.C.U.S.C.o.A.F.A.o.L., as a Basis for Biosecurity Education., and National Academy of Sciences (U.S.), *A survey of attitudes and actions on dual use research in the life sciences : a collaborative effort of the National Research Council and the American Association for the Advancement of Science*2009, Washington, DC: National Academies Press.
42. Iqbal, S.S., et al., *A review of molecular recognition technologies for detection of biological threat agents.* Biosensors & Bioelectronics, 2000. **15**(11-12): p. 549-578.
43. Ivnitski, D., et al., *Nucleic acid approaches for detection and identification of biological warfare and infectious disease agents.* Biotechniques, 2003. **35**(4): p. 862-869.
44. Griffiths, A.J.F., *Introduction to genetic analysis*. 10th ed2010, New York, NY: W. H. Freeman and Co.

45. McLoughlin, K.S., *Microarrays for Pathogen Detection and Analysis.* Brief Funct Genomics, 2011.

46. Bej, A.K., et al., *Multiplex PCR amplification and immobilized capture probes for detection of bacterial pathogens and indicators in water.* Mol Cell Probes, 1990. **4**(5): p. 353-65.

47. Hamels, S., et al., *Consensus PCR and microarray for diagnosis of the genus Staphylococcus, species, and methicillin resistance.* Biotechniques, 2001. **31**(6): p. 1364-+.

48. Mullis, K., et al., *Specific Enzymatic Amplification of DNA Invitro - the Polymerase Chain-Reaction.* Cold Spring Harbor Symposia on Quantitative Biology, 1986. **51**: p. 263-273.

49. Vandenvelde, C., M. Verstraete, and D. Vanbeers, *Fast Multiplex Polymerase Chain-Reaction on Boiled Clinical-Samples for Rapid Viral Diagnosis.* Journal of Virological Methods, 1990. **30**(2): p. 215-227.

50. Wheeler, E.K., et al., *Under-three minute PCR: probing the limits of fast amplification.* Analyst, 2011. **136**(18): p. 3707-12.

51. Pettersson, E., J. Lundeberg, and A. Ahmadian, *Generations of sequencing technologies.* Genomics, 2009. **93**(2): p. 105-111.

52. Sanger, F., S. Nicklen, and A.R. Coulson, *DNA Sequencing with Chain-Terminating Inhibitors.* Proc Natl Acad Sci U S A, 1977. **74**(12): p. 5463-5467.

53. Allen, J.E., S.N. Gardner, and T.R. Slezak, *DNA signatures for detecting genetic engineering in bacteria.* Genome Biology, 2008. **9**(3).

54. Chambers, J.P., et al., *A review of molecular recognition technologies for detection of biological threat agents.* Biosensors & Bioelectronics, 2000. **15**(11-12): p. 549-578.

55. DeRisi, J.L., et al., *Viral discovery and sequence recovery using DNA microarrays.* Plos Biology, 2003. **1**(2): p. 257-260.

56. Ehrenreich, A., *DNA microarray technology for the microbiologist: an overview.* Appl Microbiol Biotechnol, 2006. **73**(2): p. 255-73.

57. Gardner, S.N., et al., *A microbial detection array (MDA) for viral and bacterial detection.* BMC Genomics, 2010. **11**: p. 668.

58. Jaing, C. *Microbial Detection Array for Product and Health Safety*. IABS Adventitious Agents 2011; Available from: http://www.iabs.org/index.php/conferences/iabs-conferences/past-iabs-conferences/116-baltimore-2011-slides.

59. Jaing, C., et al., *A Functional Gene Array for Detection of Bacterial Virulence Elements.* Plos One, 2008. **3**(5).

60. Miller, M.B. and Y.W. Tang, *Basic concepts of microarrays and potential applications in clinical microbiology.* Clin Microbiol Rev, 2009. **22**(4): p. 611-33.

61. Reifman, J., et al., *A high-throughput pipeline for designing microarray-based pathogen diagnostic assays.* Bmc Bioinformatics, 2008. **9**.

62. Schena, M., et al., *Quantitative Monitoring of Gene-Expression Patterns with a Complementary-DNA Microarray.* Science, 1995. **270**(5235): p. 467-470.

63. Wang, D., et al., *Microarray-based detection and genotyping of viral pathogens.* Proc Natl Acad Sci U S A, 2002. **99**(24): p. 15687-92.

64. Council, C.o.S.M.f.t.D.o.a.G.-S.-B.C.S.f.t.O.o.S.A.N.R., *Sequence-Based Classification of Select Agents:A Brighter Line*2010, Washington D.C.: The National Academies Press.

65. Bedford, T. and R.M. Cooke, *Probabilistic risk analysis : foundations and methods*2001, Cambridge, UK ; New York, NY, USA: Cambridge University Press. xx, 393 p.

66. Broder, J.F., *Risk analysis and the security survey*. 3rd ed2006, Amsterdam ; Boston: Butterworth-Heinemann. xviii, 371 p.

67. Collins, M., *SciAm Perspectives Acceptable Risks for Arms Control.* Scientific American, 2009. **300**(3): p. 25-25.

68. Koller, G.R., *Risk assessment and decision making in business and industry : a practical guide*. 2nd ed2005, Boca Raton, FL: Chapman & Hall/CRC. 326 p.

69. Modarres, M., *Risk analysis in engineering : techniques, tools, and trends*2006, Boca Raton: Taylor & Francis. 401 p.

70. Otway, H.J. and D. Vonwinterfeldt, *Beyond Acceptable Risk - on the Social Acceptability of Technologies.* Policy Sciences, 1982. **14**(3): p. 247-256.

71. Participants, A.P.S.S.G., et al., *Report to the American Physical Society by the study group on light-water reactor safety.* Reviews of Modern Physics, 1975. **47**(S1): p. S1-S123.

72. Kaplan, S. and B.J. Garrick, *On The Quantitative Definition of Risk.* Risk Analysis, 1981. **1**(1): p. 11-27.