14

Verification and advanced co-operative security

Nancy Gallagher

The security circumstances confronting the world today are fundamentally different from those which shaped the theory and practice of Cold War arms control. Then, the central problem was to deter a massive nuclear or conventional attack while using arms control to stabilise deterrence and prevent proliferation. Now, the United States and its allies have little reason to fear a deliberate large-scale attack. Instead, the most troublesome security problems involve smaller-scale, more diffuse dangers driven by key trends associated with globalisation.[1] Various developments, including the information revolution, the emergence of global markets and transnational networks, widespread access to dual-use materials and sophisticated technologies, and growing economic inequalities, have magnified the threats posed by angry individuals, disaffected groups and weak states. They have also multiplied the destruction that could occur from natural causes, accident, inadvertence or other unintended consequences of 'business as usual' in a tightly connected high-technology world.

The Advanced Methods of Cooperative Security Program at the University of Maryland is exploring conceptual issues and operational techniques for co-operative responses to new global security problems.[2] The goal is to promote interdisciplinary research and discussion about applications that exemplify emerging security problems and embody elements of potential solutions. The current focus is on research with dangerous pathogens, space activities and fissile material controls. This chapter presents the basic concept of advanced co-operative security and explores the role for verification in advanced co-operative security systems. It also provides a brief illustration of advanced co-operative security in practice, using the example of biotechnology.

These concepts are at an early stage of development and far removed from current practice. This essay seeks to spark further research and discussion in order to broaden the array of options available for serious consideration.

The challenges of global security

The central problem for global security today is not balancing competing alliance systems but building inclusive arrangements which let co-operative states and non-state actors pursue diverse interests without causing major unintended problems and which organise the vast majority of willing co-operators to deal more effectively with a relatively small number of hostile players. This involves a reduced emphasis on deterrence and contingency response, and an increased emphasis on reassurance and systematic prevention. In the nuclear arena, for example, numbers now matter less than operational practices. Any country's residual need for deterrence can be satisfied with a much smaller stockpile of weapons. The most worrying scenarios all involve some type of irresponsible behaviour, such as lax security at storage sites, or loose talk about 'usable' nuclear weapons that promotes proliferation and weakens the nuclear taboo. Reducing such nuclear dangers requires agreement on operational practices that minimise the potential for misperception, mistakes, uncontrollable escalation or opportunistic action by hostile third parties.

The incentives for a reorientation of security policy from deterrence and secrecy towards reassurance and transparency were evident by the mid-1980s, when the 35 members of the Conference on Security and Co-operation in Europe (CSCE) sought to reduce risk of conventional war by changing European security concepts and operational practices. The 1986 Stockholm Accord provided for modest information exchanges, on-site inspections and constraints on major military activities. The 1990 Conventional Armed Forces in Europe (CFE) Treaty and the associated agreement on personnel (the 1992 CFE-IA Agreement), as well as the series of Vienna Documents (1990, 1992, 1994 and 1999) that followed the Stockholm Accord and the 1992 Open Skies Treaty, have included tighter behavioural constraints, detailed data-reporting requirements, extensive verification mechanisms and institutional arrangements which are integral to a more co-operative European security system.[3]

Initial attempts to elaborate the concept of co-operative security reflected this dramatic shift in East–West security relations. The original approach focused on

setting agreed standards for the size, concentration, configuration and operations of national militaries. The goal was to permit defence of the homeland but preclude large-scale external attacks, and to facilitate effective and legitimate multilateral military responses to external aggression or civil conflict. Compliance was to be verified through extensive transparency around weapons and operations, including increased sharing of national intelligence and international technical monitoring. Some inspection of key defence programmes was also considered necessary. Proponents argued that co-operative security systems should be inclusive and equitable, and should rely when possible on positive inducements and other forms of co-operative compliance management. They recognised, however, that a comprehensive co-operative security system would need tougher enforcement mechanisms, including economic sanctions and multilateral military responses.[4]

The example that comes closest to co-operative security from outside the European conventional force context is probably the nuclear threat reduction programmes in the former Soviet Union. In the mid-1990s, changed security circumstances and altered threat perceptions convinced the American and Russian leaders that they had a mutual interest in ensuring the safe and secure handling of nuclear weapons and material from the former Soviet arsenal. A variety of American-funded projects have helped Russia eliminate nuclear launchers under the Strategic Arms Reduction Treaty (START I); removed nuclear weapons from other former Soviet states; and reduced the likelihood that nuclear weapons, material or know-how would proliferate to hostile states or terrorist groups.

These programmes have improved Russian security standards and practices. New monitoring technologies are being developed to demonstrate that co-operative obligations have been met, without revealing other sensitive information. By developing industrial partnerships with Russian entities, American government agencies and firms have learned about Russian nuclear operations and gained experience working on nuclear problems with their Russian counterparts. However, despite these practical benefits, deeper co-operation has been impeded by suspicions and resistance on both sides. American access to sensitive Russian sites is restricted; Russia does not gain reciprocal access and auditing rights that come as a condition of American funding; and individual co-operative projects have not been embedded in a larger strategic framework of mutual accommodation and restraint. In short,

ad hoc threat reduction co-operation may be a step in the right direction, but it falls far short of comprehensive co-operative security.[5]

Meanwhile global trends are generating new types of security problem that cannot be addressed effectively through unilateral action, traditional arms control or ad hoc co-operation. For example, biotechnology has the potential to cure life-threatening illnesses or to create more virulent pathogens which could cause devastation that would rival the results of nuclear attack and against which defence would be equally difficult. Research involving especially dangerous pathogens, such as smallpox and Ebola, cannot be banned without foreclosing opportunities for protection and forgoing other public health benefits. Export controls, access controls and the classification of weapons-related information cannot provide reliable protection because everything needed to make deadly diseases is available in nature, in worldwide scientific laboratories and pharmaceutical firms, from mail-order companies, or on the Internet. Since large amounts of bio-agents could be grown quickly from a small sample of a virulent organism, quantitative limits are not an effective way to differentiate between legitimate and illegitimate activities. In short, the national security and arms control tools that have helped to prevent nuclear proliferation are not well suited for preventing the misuse of biology without impeding beneficial research.

Addressing such security challenges requires the development of more advanced co-operative security concepts and practices. They would have much in common with their predecessors, including the basic premise that most states and non-state actors do not want to threaten others' security and would benefit from shared standards of behaviour and mechanisms of reassurance; but the concept of advanced co-operative security differs from its predecessors in ways that reflect key trends in global security. Potential threats no longer arise primarily from dangerous configurations of military capabilities, but increasingly from the misapplication of dual-use technologies that are dispersed throughout society. Thus, advanced co-operative security arrangements cannot be mainly between national military establishments but must include scientists, commercial interests and non-governmental organisations.

If massive aggression is now less likely than asymmetrical attacks or dispersed interactions that coalesce into catastrophe, then the dividing line between legitimate

and illegitimate activities can no longer turn on quantitative thresholds or qualitative distinctions, such as rules about how large a purely defensive military can be and what types of weaponry it should or should not have. Instead, striking the right balance between promoting the beneficial uses of potentially dangerous technology while preventing misapplications will require expert judgements based on detailed information about who is doing what, why and how. This means that compliance cannot be verified primarily through exchanges of national intelligence, remote sensing, passive on-site monitoring or adversarial inspections. It will require unprecedented sharing of sensitive information, sophisticated systems for handling large volumes of data, and extensive protection against the misuse of information that was disclosed for protective purposes.

The role for verification in advanced co-operative security

Verification—one of the most controversial and time-consuming aspects of Cold War arms control—has been attacked from both the political left and the political right as largely unnecessary and often counterproductive in the new, more co-operative security environment. The administration of President George W. Bush in the US appropriated a stance that had long been popular with the disarmament movement by declaring that a strategic arms agreement could be reached quickly, without lengthy negotiation of detailed verification provisions, because verification would only institutionalise mistrust. As for agreements that include not only rivals-turned-friends but also countries of concern, some people are using the changed nature of the threat as evidence that verification could diminish national security and prosperity. For example, the Bush administration withdrew US support for the negotiation of a verification protocol to the 1972 Biological and Toxin Weapons Convention (BWC) on the grounds that the types of multilateral transparency measure that were under consideration could not reliably detect clandestine work with small amounts of deadly pathogens, yet would reveal information about US national security and commercial activities that could aid potential attackers or business competitors.

These attempts to dismiss verification as an outmoded relic of the Cold War are based on a narrow, often politically motivated, conception of verification as an adversarial process that should provide nearly complete confidence that every militarily significant violation by a devious enemy will be detected, identified and

attributed in time for a response before national security is harmed.[6] This conception neither reflects the full range of past verification approaches and accomplishments nor illuminates the role that verification should play in advanced co-operative security systems.

Verification, broadly defined, refers to any process that is used to assess compliance with co-operative obligations. It can be implicit and purely unilateral, as was the case with the 1963 Limited Test Ban Treaty (also known as the Partial Test Ban Treaty, the PTBT) which does not mention verification because the superpowers' own monitoring systems would provide evidence of a nuclear test in a prohibited environment. It can be part of an adversarial 'game' with monitoring rules and inspection rights in which opponents try to uncover information about the other side's treaty compliance and 'collateral issues' while protecting their own sensitive information, as was largely the case with superpower nuclear arms control. It can also take more co-operative forms, as with the European conventional security agreements mentioned above or the safeguard agreements used to confirm that non-nuclear weapon state parties to the 1968 Nuclear Non-Proliferation Treaty (NPT) are not diverting nuclear energy from peaceful uses into weapon programmes. The reasons for pursuing verification can also be diverse. States can press for intrusive and exacting verification arrangements in order to gain high confidence in compliance or to stymie negotiations. Likewise, they can favour only modest measures, such as voluntary data exchanges, because they care more about reaching an agreement than they do about compliance; because they want to protect their own secrets more than they care to know what others are doing; or because they have no real interest in agreements that constrain their own military options.

The trends shaping global security have reduced the importance of some of the factors that made verification important and controversial during the Cold War. At the same time, they have intensified other factors that make the exchange and analysis of compliance information likely to be even more essential and contentious than it was before, regardless of whether the process is called verification or something else. Despite recurrent American attempts to depict verification as a technical adjunct to the substantive limits placed on the superpowers' military capabilities, both sides in the Cold War recognised that information revealed, obtained or concealed during the verification process had intrinsic national security value.

Cold War concerns about verification could be somewhat muted, however, because the co-operative constraints left each side with such large residual capabilities that low-level cheating or collateral information collection was unlikely to have a significant effect on the bilateral strategic balance.

Addressing the most pressing global security problems will require more comprehensive and reliable obligations and verification arrangements among a diverse group of states and non-state actors. The stakes will be as high as they were during the Cold War, but it will be harder to tolerate sloppiness in any part of a security system. No amount of residual military capability can compensate for problems such as major intelligence failures, lax safety practices in work with dangerous pathogens, imprecise accounting standards that lose track of fissile material, or enforcement systems that can only handle egregious violations.

Given the ease with which dangers can cross national borders, homeland security will require not only tougher domestic regulatory arrangements but also high standards and rates of compliance among global neighbours. The complexity of the issues, the diversity of interests, the high stakes and low tolerance for mistakes mean that formal legal agreements with clear obligations, accountability measures and methods of protection will be necessary at both the national and the international levels. Everyone will want to know that the overall system is working as intended, but in the information age the adage that 'knowledge is power' is truer than ever. Thus, it is crucial to think carefully about what compliance information is really necessary, how it should be gathered, who should have access to raw data and analysis, and how assessments of compliance should be made.

The shift in emphasis of co-operative security from deterrence and contingency response to reassurance and systematic prevention calls for a corresponding reorientation in the ends and means of verification. If in a co-operative security regime one is less concerned about deliberate aggression by any of the main players and more concerned either that they might engage in inadvertently dangerous behaviour or that a minor player (small state or terrorist group) might misbehave, then more emphasis can be placed on reassurance than was true of traditional American approaches to verification. The deterrence and detection functions do not disappear, but the normal mode of verification can assume that most participants will try to comply because they share the underlying goals and understand the reasons behind

the rules, not because they fear punishment. Verification is no longer seen as a zero-sum game between hiders and finders. Instead, the presumption is that most participants will be willing to exchange detailed information in the interests of mutual reassurance and protection so long as they have confidence that the information will be handled carefully and used appropriately. With reassurance as the primary objective, it makes no sense to differentiate between 'substantive' obligations and verification mechanisms because disclosure is an integral and intrinsically valuable part of an advanced co-operative security system.

Reconceptualising verification to emphasise the co-operative exchange of information for mutual benefit can increase international support for a robust cooperative security system. During the Cold War, representatives of the non-aligned countries often dismissed the superpowers' use of mutually incompatible, but equally adversarial, approaches to verification as evidence that neither side was really serious about co-operation. In more recent multilateral negotiations, verification has sometimes been seen as a Western construct to which developing countries might acquiesce in return for other forms of technical, scientific or financial assistance, not as something that directly increases the security of all participants.[7] But if verification information is used not just to catch the 'bad guys' but also to help the 'good guys' benefit safely from dual-use technologies, then verification is less likely to be seen as a Western obsession that offers little but trouble for the rest of the world.

Broadening the objectives of verification to include positive purposes beyond reassurance can be controversial. When information from a verification system is also used to accomplish some unrelated, but unquestionably benign, objective, as occurs with earthquake data from the seismic sensors for the 1996 Comprehensive Nuclear Test Ban Treaty (CTBT), the only real concern is that the secondary purpose might detract attention and resources from the primary mission. The situation is more problematic when the same information could be used for co-operative or competitive purposes: for instance, technical assistance to increase the reliability of commercial satellite launches could also help ballistic missile development. Globalisation makes the national security strategy of restricting access to dual-use information increasingly difficult to sustain because there are so many incentives and opportunities to share powerful information with foreign business associates,

academic colleagues, fellow activists or partners in crime. It is wiser to work with, rather than against, this trend by making the exchange of dual-use information conditional on the acceptance of appropriate arrangements to document that it is being used for agreed purposes.[8]

The design of verification arrangements will differ depending on issue area, both in order to focus the most scrutiny on the most serious security concerns and in order to leverage maximum verification benefit from information being gathered or exchanged in that field for other purposes. In general, each advanced co-operative security system would include:

- reporting and other disclosure requirements whereby participants would document their own compliance with co-operative obligations;
- routine cross-checks whereby authorities would collect information to confirm or question the accuracy and completeness of disclosed information; and
- increasingly intrusive investigative powers allowing authorities to request additional information, conduct inspections, and take other steps to clarify suspicious situations and, if necessary, provide the evidence of non-compliance needed for an effective response.

Relevant concepts, practices and technologies can be found not only in previous arms control agreements but also in other types of international agreement, in various national regulatory regimes, in voluntary transparency and review arrangements, and even in surprising places, such as inventory tracking systems for global business. One review of global governance across a wide range of issues identified a diverse array of verification tools and some important general lessons, such as the need for verification to determine not only whether a violation has occurred but why it has happened, so that informed choices can be made to promote compliance.[9] The novel aspect of verification for advanced co-operative security lies not in any individual component. Rather, it rests in the creative synthesis of diverse sources of information, many of which exist now but are underutilised, for the purpose of providing participants with a clearer picture of activity in realms of behaviour that were previously shielded from outside scrutiny.

As other authors have noted, globalisation and the information revolution are creating new incentives and opportunities for small states, the private sector and

civil society to be active in the verification process.[10] Recent writing shows that global civil society shares the interest of advanced co-operative security in setting behavioural norms and promoting transparency. The decentralised nature of many global security problems makes non-coercive 'regulation by revelation' attractive, especially as governments, businesses and private-sector groups should be both regulators and regulated—that is, be more transparent about their own operations and use public information to pressure others to behave appropriately.[11]

Contrary to some writing about transparency, however, the advanced methods of co-operative security approach does not assume that all compliance information could come from open sources or that it should be made public. Once a clear picture has been obtained of the types of information needed to verify compliance with a particular set of co-operative obligations, one should first determine how much of that information is already in the public domain or in other accessible data sets. Then one needs to determine how much of the other necessary information should be encouraged or required to be made public, and how much is truly sensitive for national security or commercial reasons and thus needs to be kept within the system under special access and use rules. The computer technology exists to mine vast quantities of open-source data and to integrate compliance information from diverse sources into very powerful controlled-access databases. The more difficult challenge is deciding what needs to be known, who should know it and how that knowledge should be used to enhance co-operation.

Participants in a co-operative security regime will be more forthcoming with information about their activities if they are not worried about confusing regulations, unachievable standards, false accusations or criminal penalties for unintentional errors. If compliance concerns arise during the verification process, they should be handled, at least initially, through co-operative mechanisms. These would include procedures to clarify ambiguous rules and resolve disputes about the rules' applicability to specific cases. They could incorporate technical, financial and legal assistance to increase capacity for compliance. They could involve a range of positive incentives to encourage compliance. They would also include strategies to change how participants think about co-operation, such as providing more complete and accurate information to influence cost–benefit calculations or promoting norms to alter underlying values.[12] These mechanisms would be a relatively constructive, low-

cost way to resolve compliance problems that arise from ignorance, incapacity or inadvertence. If, however, the verification process yields evidence of deliberate and egregious violations, then there would be a need to have more adversarial investigation and enforcement tools available, either within the co-operative security system itself or through another national or international body.

Advanced co-operative security in practice

The 2002 anthrax attacks in the United States raised a host of questions about access to dangerous pathogens and revealed a remarkable lack of information and oversight of research involving virulent disease agents in academia, in industry, among defence contractors and in government national security laboratories. Much of the ensuing debate has focused on finding the right balance between science and security—trying to leave the 'good guys' alone as much as possible while preventing the 'bad guys' from gaining access to dangerous pathogens or learning from the open literature how to make deadly diseases.

Advanced co-operative security offers an alternative approach to promoting beneficial uses of biotechnology while preventing its misapplication—one in which systematic disclosure and independent peer review are used to make science and security mutually supportive. This section previews the basic elements of the prototype Biological Research Security System (BRSS) that is being developed as part of the Advanced Methods of Cooperative Security Program.[13]

A comprehensive research oversight system that covers both legitimate scientists and potential miscreants is needed for several reasons. To begin with, the most objective and effective way to draw proactive distinctions between the 'good guys' and the 'bad guys' is to define disclosure and review requirements for everybody doing legitimate work with dangerous pathogens, so that anyone who refuses stands out. Furthermore, the system needs to address not only the deliberate misuse of biotechnology but also various ways in which legitimate science could cause inadvertent destruction. Lax safety and security standards could prove disastrous even in a laboratory devoted solely to bio-defence or vaccine development.[14] Cutting-edge research could produce unexpectedly dangerous results.[15] Knowledge generated by benign research could be used by someone else for hostile purposes.[16] Finally, a diffuse problem such as that presented by dangerous pathogens requires a decen-

tralised solution that is primarily designed and implemented by a worldwide network of legitimate scientists.

Many international agreements and domestic regulations cover some aspect of work with dangerous pathogens, but few address basic research.[17] The BWC prohibits states parties from developing, producing, stockpiling, or otherwise acquiring or retaining biological agents or toxins 'of types and in quantities that have no justification for prophylactic, protective or other peaceful purposes' but does not list research among its prohibitions. Neither the BWC nor subsequent review conferences have provided much guidance for differentiating between peaceful and hostile purposes, and some people argue that almost any activity could be justified in the name of 'threat assessment'.[18] During work on the BWC verification protocol a partial, indirect attempt was made to define activities that should be the focus of additional verification efforts by generating lists of dangerous agents, criteria for relevant facilities and requirements for declaring particular kinds of work. The logic behind constructive proposals was to concentrate on types and quantities of agents and equipment that seemed most likely to be used by a state in an offensive military programme. The politics of the protocol negotiations, however, combined conflicting preferences for secrecy and security into a compromise draft text in which the thresholds and exemptions of the transparency arrangements were so important that the net effect of going only that far might well have been to increase suspicions rather than to reduce them.[19]

Much attention is currently concentrated on strengthening national systems for controlling dangerous pathogens as an alternative or a supplement to future international efforts. In the US a patchwork of regulations and recommendations have some relevance for basic research with dangerous pathogens but focus primarily on the later stages of testing, producing and packaging biotechnology products. The three most relevant areas are probably new legislation mandating reports on the possession of designated pathogens; bio-safety recommendations to promote the safe handling of pathogens that pose varying degrees of risk; and review procedures for recombinant DNA (rDNA) research at institutions that receive funding for that purpose from the National Institutes of Health (NIH). The new federal legislation does not require any information about the research being done with the designated pathogens. Bio-safety reviews and most rDNA reviews are done at

the local (institutional) level with varying degrees of rigour. Much research with dangerous pathogens could be done with no external reporting or review whatsoever, especially if it does not involve a listed pathogen or is conducted at an institution that does not receive NIH funding. Concerns about what might be going on behind closed laboratory doors are likely to grow as funding for bio-defence work expands, more work is done on a classified basis, and pressures increase for the publication of potentially dangerous research results to be restricted.

An advanced co-operative security approach to balancing the benefits and risks of biotechnology research seeks to make science and security work together through the twin mechanisms of systematic disclosure and independent peer review. One can envisage the establishment of a BRSS with objectives, standards and operational procedures that are shared globally yet implemented largely on the local and national levels. The fundamental objective would be to provide reassurance that legitimate research involving dangerous pathogens was being done in such a way that its benefits for global society outweighed the risks of deliberate misuse or inadvertent danger. The system would be based on agreed standards for assessing the level of danger posed by different lines of research and for assigning appropriate operational standards for work at each danger level.

The BRSS should be based on a definition of dangerous research that is understandable for both scientists and lay people and is flexible enough to match rapid advances in biotechnology. The three features of a pathogen that are most relevant are its transmissibility, its infectivity and its pathogenicity. In other words, to assess the risk posed by research with a particular pathogen, one needs to know three things about the organism that the researcher will start or end up with. Could it spread easily from person to person or be widely disseminated in some other way? How many of the people that it encounters will become sick? And how many sick people will die? (Natural pathogens reflect evolutionary trade-offs along these dimensions. For example, pathogens that kill their hosts too quickly have less opportunity to spread.) Smallpox is considered to be among the most dangerous pathogens because it is moderately contagious, low-level exposure can lead to infection, and 30 per cent or more of infected individuals will die unless vaccinated before symptoms appear.[20] Smallpox that was genetically engineered to be more contagious or vaccine-resistant would be much worse.

One could define extremely dangerous research (EDR) loosely to cover work with pathogens whose combined danger factors are comparable to or worse than those associated with smallpox, the pathogen for which research is currently most tightly controlled.[21] Moderately dangerous research (MDR) would include work with pathogens such as anthrax that could pose very serious public health problems but do not have the same mass destruction potential as would be seen in a self-sustaining epidemic of smallpox or highly virulent influenza. Potentially dangerous research (PDR) would cover experiments that start with relatively benign pathogens and involve techniques that might produce a more dangerous pathogen or provide knowledge that could be applied to another, more dangerous pathogen with potentially devastating results. One of the first tasks in creating the BRSS would be to decide whether these conceptual categories should be operationalised narrowly, to minimise the amount of research subject to each level of oversight, or broadly, to reduce the likelihood of dangerous research receiving inadequate supervision.

Each level of danger would have corresponding disclosure and review requirements. Since EDR, if mishandled, might have dire global consequences, the very small amount of research that might be done in this realm should be subject to strict international control. For example, scientists would need a special license to conduct EDR; they would be required to submit regular activity reports and to secure approval from an international body of experts for each proposed EDR experiment, all of which would be conducted only at approved facilities under international supervision; and the results of all experiments would be handled according to special dissemination procedures. In terms of moderately dangerous research, internationally agreed standards and procedures for licensing, routine reporting, research proposal review and dissemination would be applied by national authorities with oversight from the international agency. Most biological research would either be low-risk, and thus could continue without new oversight requirements, or fall into the PDR category, which would be subject to more systematic local oversight and independent review with national oversight using world-class standards.

The BRSS would include two different types of verification. Much of the reassurance in the system would be a natural by-product of following the appropriate licensing, reporting, review and publication procedures, all of which would be designed with a presumption in favour of transparency or, if necessary, systematic disclosure of

sensitive information under agreed access and use conditions. There would need to be additional means to ensure that information provided to the system was detailed, accurate and complete enough to enable reliable judgements about the research activities in question. Some of this could be done by relatively neutral, technical methods, such as auditing annual reports for internal consistency, cross-checking information provided by one laboratory with submissions from others with which it interacted, or comparing research proposal review records with findings published in academic journals and patent applications for biomedical products.

Some tough political choices will be unavoidable, though, especially for moderately dangerous research involving information that is sensitive for reasons of national security, proprietary interests or other intellectual property rights. The preferred approach would be to require thorough reporting and review at the national level, with the most sensitive details being kept confidential but made available on request to the appropriate international authorities under agreed access and use rules. The less willing laboratories and national authorities are to disclose sensitive information through co-operative procedures, the more necessary it would be to resort to challenge inspections and other adversarial forms of verification.

The underlying purpose of the BRSS is to buttress the negative norm against the destructive use of life science embodied not only by the 1925 Geneva Protocol and the BWC, but also by the Hippocratic Oath and universal ideas of human decency. However, the fact that the proposed system builds on specific positive, process-oriented obligations has important implications for verification. To begin with, it is easier to confirm a positive than to prove a negative. Moreover, the appropriate standard for this verification system is not whether it can detect every significant clandestine biological weapons-related activity; that standard is both too broad for a research-focused system and impossible for any prevention-oriented approach to meet. A more appropriate standard would ask whether the BRSS verification arrangements (a) do more good than harm—whether the benefits of increased confidence that the power of biological research is not being misused outweigh whatever inconvenience and intrusion occurs at each level of research; and (b) make a net contribution to global security when combined with other national and international tools for detecting, deterring and redressing deliberately destructive misuses of biotechnology.

Conclusion

The pathogens application illustrates some of the ways in which security co-operation and verification need to change to reflect the altered circumstances of global security. In contrast to the Cold War, when threatening military capabilities and arenas for security co-operation existed apart from most citizens' normal existence, many new threats and the opportunities for co-operation are now spread throughout routine scientific, economic and social interactions. Biotechnology research is a diffuse, knowledge-driven, collaborative activity of increasing importance to the health and economic welfare of every country in the world. Any security strategy that ignores these fundamental facts is bound to fail. Any approach that recognises new types of threats but responds using traditional national security and law enforcement tools will impose unnecessarily high costs—including increased suspicion, threat assessment activities that erode constraints on the destructive uses of biotechnology, draconian prohibitions on experimentation or publication that impede scientific advance, and infringements on civil liberties—all for little or no net gain to world security.

Working out the details of a Biological Research Security System, or any other advanced co-operative security solution for comparable problems in other fields, will require a tremendous amount of creative thinking by scientists, arms control experts, information technology specialists, lawyers and industry representatives from around the world. This is a long-term vision; no one expects a full-blown version of this system to be in place at any time soon. But as the problem becomes more urgent the number of people working on incremental improvements to existing national and international arrangements will grow exponentially. Thinking now about where we might want to be headed can make the difference between counterproductive confusion and slow, steady progress in the right direction.

Nancy Gallagher is Associate Director for Research at the Center for International and Security Studies at Maryland, University of Maryland. She is the author of *The Politics of Verification*, Johns Hopkins University Press, Baltimore, MD, 1999, and the editor of *Arms Control: New Approaches to Theory and Policy*, Frank Cass, London, 1998.

Endnotes

[1] For a fuller analysis, see John Steinbruner, *Principles of Global Security,* Brookings Institution Press, Washington, DC, 2000.

[2] See the website of the Center for International and Security Studies at Maryland (CISSM) at www.puaf.umd.edu/CISSM/Projects/AMCS/AMCS.htm for more information about the Advanced Methods of Cooperative Security Program.

[3] On the role of arms control in managing the end of the Cold War and creating more co-operative norms of behaviour in Europe, see Stuart Croft, *Strategies of Arms Control,* Manchester University Press, Manchester, 1996.

[4] One of the earliest discussions of the concept of co-operative security was Ashton B. Carter, William J. Perry and John D. Steinbruner, *A New Concept of Cooperative Security,* Brookings Occasional Papers, Brookings Institution, Washington, DC, 1992. The fullest treatment of the earlier approach is Janne Nolan (ed.), *Global Engagement: Cooperation and Security in the 21st Century,* Brookings Institution, Washington, DC, 1994.

[5] Rose Gottemoeller, 'Arms control in a new era', *Washington Quarterly,* vol. 25, no. 2, spring 2002, pp. 45–58.

[6] For an analysis of competing approaches to verification and their effects on decisions about co-operation, see Nancy W. Gallagher, *The Politics of Verification*, Johns Hopkins University Press, Baltimore, MD, 1999.

[7] Trevor Findlay, 'Introduction: the salience and future of verification', in Trevor Findlay (ed.), *Verification Yearbook 2000*, The Verification Research, Training and Information Centre (VERTIC), London, December 2000, p. 17.

[8] This parallels the Cold War experience: the development of satellites, seismic monitoring and other remote sensing technology made it increasingly difficult for the Soviet Union to maintain tight secrecy about its nuclear weapons development. This increased its incentives to negotiate with the West about how such technology could be used to verify compliance with arms control agreements.

[9] P.J. Simmons and Chantal de Jonge Oudraat, *Managing Global Issues*, Carnegie Endowment for International Peace, Washington, DC, 2001, esp. pp. 693–698. This study found four techniques to be especially important in assessing compliance with co-operative agreements, all of which fit well with the advanced co-operative security approach: the use of independent experts and data; transparency and open review; mechanisms to protect sensitive information; and uniform standards of evaluation and trusted analysis.

[10] See, for example, Andrew Rathmell, 'The information revolution and verification', in *Verification Yearbook 2000,* pp. 215–228.

[11] Ann Florini, 'The end of secrecy', *Foreign Policy,* no. 111, summer 1998, pp. 61–62. See also Ann Florini (ed.), *The Third Force: The Rise of Transnational Civil Society,* Japan Center for International Exchange and Carnegie Endowment for International Peace, Tokyo and Washington, DC, 2000.

[12] On co-operative versus coercive compliance strategies, see Ronald B. Mitchell, 'International control of nuclear proliferation: beyond carrots and sticks', *Nonproliferation Review,* fall 1997, pp. 40–52; and Abram Chayes and Antonia Handler Chayes, *The New Sovereignty: Compliance with International Regulatory Agreements,* Harvard University Press, Cambridge, Mass., 1995.

[13] Since this is a work in progress, readers are encouraged to visit www.puaf.umd.edu/CISSM/Projects/AMCS/Pathogens.htm for more information about the Controlling Dangerous Pathogens Project and a fuller description of the proposed system.

[14] For example, a review by the US Department of Energy's Inspector General found that experiments with botulism, plague, anthrax and other lethal pathogens were being conducted at national laboratories without appropriate oversight—both violating requirements and carrying out activities which should have required oversight but did not—and without rigorous safety procedures. The Inspector General at the US Department of Agriculture found that unauthorised individuals could easily gain access to laboratories where deadly

biological agents were stored without adequate security. US Department of Energy, Office of the Inspector General, Office of Inspections, 'Inspection of Department of Energy activities involving biological select agents', February 2001, available at www.ig.doe.gov; and Reuters, 'Report finds easy lab access to deadly pathogens', 7 May 2002.

[15] The mousepox experiment in Australia has become a classic example of this problem. Other worrying examples include an experiment at Imperial College in London where researchers hoping to develop a vaccine for hepatitis C and eliminate the need for animal testing planned to combine hepatitis C with dengue fever, which could have created a lethal hybrid virus for which there is neither vaccine nor treatment. The experiment was stopped by the UK's Health and Safety Executive because serious safety violations at the laboratory had been reported in the past and it was attempting to proceed without a follow-up inspection. Ronald J. Jackson *et al.,* 'Expression of mouse interleukin-4 by a recombinant ectromelia virus suppresses cytolytic lymphocyte responses and overcomes genetic resistance to mousepox', *Journal of Virology*, February 2001, pp. 1205–1210; and Charles Arthur, 'Scientists made virus "more lethal than HIV"', *The Independent,* 24 July 2001.

[16] Recent examples of publications that contain dangerous information include a report on the synthesis of the polio virus using publicly available genetic information and short segments of mail-order DNA, and another paper identifying camelpox as smallpox's closest cousin. Jeronimo Cello *et al.*, 'Chemical synthesis of poliovirus cDNA: generation of infectious virus in the absence of natural template', *Science*, vol. 297, no. 5583, 9 August 2002, pp. 1016–1018; and 'The sequence of camelpox virus shows it is most closely related to variola virus, the cause of smallpox', *Journal of General Virology,* no. 83, 2002, pp. 855–872.

[17] For details of international agreements and domestic regulations, see Elisa D. Harris, 'International and domestic efforts to prevent dangerous uses of biological pathogens: a preliminary assessment', CISSM working paper, forthcoming; and Stacy Gunther, 'Federal regulation of scientific research', CISSM working paper, December 2001, available at www.puaf.umd.edu/CISSM/Publications/AMCS/AMCS.htm.

[18] The Third BWC Review Conference in 1991 did note that experiments involving the open-air release of dangerous pathogens had no justification for peaceful purposes, but no other similarly concrete distinctions have been elaborated between legitimate and illegitimate experiments. On attempts to differentiate between offensive and defensive research related to biological weapons, see Milton Leitenberg,'Distinguishing Offensive from Defensive Biological Research',*Critical Reviews in Microbiology,* (forthcoming 2003).

[19] John Steinbruner, Nancy Gallagher and Stacy Gunther, 'A tough call', *Arms Control Today,* vol. 31, no. 4, May 2001, pp. 23–24.

[20] Donald A. Henderson *et al.*, 'Smallpox as a biological weapon', *Journal of the American Medical Association,* vol. 281, no. 22, 9 June 1999, pp. 2127–2137.

[21] Stacy Gunther, 'Smallpox: oversight of a dangerous pathogen', CISSM working paper, forthcoming at www.puaf.umd.edu/CISSM/Publications/AMCS/AMCS.htm.