THE ECONOMICS OF SECURITY

WILLIAM ARTHURS
CHAIRMAN, THE INTERNATIONAL COMMISSION ON ECONOMICS AND SECURITY

The International Commission on Economics and Security (ICOES) is a project of the Transatlantic Institute.

(c) The Transatlantic Institute, registered charity number 1108682
London, UK
April 2005

Abstract:

Traditionally, security has been understood in terms of technological advances. This paper argues that security is a subjective concept, and that problems of security can best be understood using simple economic concepts. Economics offers a wide range of tools and models to understand individual actors' decisions about security and the interaction that takes place during the emergence of a collective decision. Once security problems are understood as problems of resource allocation and incentives, behaviours usually characterised as perverse can be readily explained.

1. Introduction

This paper discusses modes of analysis that can be applied to security.

Security should properly be understood as a holistic concept encompassing spectra of different types of threats to social groups and of types of responses to those threats. Threats to social groups can originate from economic, social and environmental influences, as well as from terrorism or conventional military action. Social groups can respond to a given threat in a range of different ways: they can learn to live with it and do nothing; attempt to address or control it directly; address it indirectly by building capabilities to handle the threat, should it crystallise; disengage from activities which give rise to the threat; or structure their response so as to pass on the risk to others outside the group.

Perceptions of threats, and possible responses to them, are inevitably mediated through the political process, in which (whatever the formal structure of government) a single leader or small group of leaders persuades a rather larger group of politically-engaged followers to set out an agenda of perception and response which the public will regard as legitimate or at any rate not worth contesting. Such agendas can vary in quality from the finely-reasoned, balanced and exhaustive (for example, the Federalist Papers), to the delusional (the fascist and communist ideologies of the twentieth century).

Today's concerns about security appear disparate compared to the single shadow of mutually assured destruction cast by the Cold War. Anxieties about terrorism, health and safety scares (for example, genetically modified organisms, carcinogens in foods, dangerous public transport, environmental degradation), and generalised threats to established ways of life (attributed to the weakening of national sovereignty, population movements, and globalisation) have little in common apart from the mode of analysis that is customarily applied to them.

2. Two different modes of analysis for security issues

But how should issues of security be analysed? What I call the "security conundrum" is the puzzling persistence of the naive view that issues of security should primarily be understood in terms of technological progress and regress. This naive view is no straw man: it is the standard mode of analysis in popular discourse. Often, security breaches are blamed on deficiencies in technology for which the remedy is more advanced technology: for example, identity tokens to be carried by citizens of democracies, and linked to central databases: or more technologically-advanced security systems to protect information and communications technology facilities used by the government or the financial markets. Conversely, some threats are blamed on advanced technology, and the proposed remedy

is to discard that technology (genetic modification; preservatives in food; the entertainment and communications infrastructure which, by way of “cultural imperialism”, allows American entertainment products to be distributed around the world).

Set out like this, the naive view is incoherent in its ambivalence toward technological progress. Looked at another way, however, the naive view is bound up in a complex of attitudes toward the assessment of the costs and benefits of particular courses of action. Uncosted demands for more and better technology go hand in hand with uncosted demands for the abandonment of technologies that, according to the naive view, have fallen from favour. Technological development exists in a vacuum and the desired new technologies emerge as dei ex machina, while the undesired technologies are developed for short-sighted or callous commercial motives.

The naive view is essentially an irresponsible view characterised by ignorance of economics and of the commercial and military driving forces behind technological development. It has no explanatory power: behaviour which, under this view, is characterised as perverse, is imputed to, and also serves as conclusive evidence of, a third party’s moral failings or weakness of character. This is simply a circular argument.

The better view is the economic view of security. Security is inherently subjective (contrary to the naive view in which security is objectified as an attribute of technology), and problems of security can best be understood using simple economic concepts. Economics offers a wide range of tools and models to understand individual actors’ decisions about security and the interaction that takes place during the emergence of a collective decision. Once security problems are understood as problems of resource allocation and incentives, behaviours characterised as perverse by the naive view can be readily explained.

For example, consider the ability of Western political elites to insulate themselves from security problems in the current climate of concern about terror and crime rates, while passing the risk onto the populace. This illustrates an important aspect of the design of incentives: they will be ineffective, or less effective than they could have been, if the persons who are in a position to address a threat do not suffer unduly if the threat crystallizes.

Another example relating to incentives illustrates their role in job roles and career paths. Consider the level of salience of the threat posed by Al Qaeda as perceived by the US administration during the years leading up to 9/11. US responses to Al Qaeda’s attacks on US facilities can be seen, in retrospect, as having sent a powerful signal that the USA was reluctant to take aggressive and effective action against this threat: Osama bin Laden notoriously characterised the USA as a “weak horse”. Imagine the career prospects of a US state functionary (a civil servant or intelligence officer) who foresaw the need to take effective action and therefore decided to challenge the consensus that the terror threat was best dealt with via the legal process. If he were proved wrong, that would have ended his career. If he were proved right, he would still get a reputation as a maverick. Now imagine, for the purposes of comparison, the career prospects of this maverick’s colleague who adheres to the consensus view. If she is proved wrong, she was wrong in good company, including the company of many people senior to her, and is therefore very unlikely to be singled out for dismissal. (If she is proved right, so much the better for her, and she will not earn a reputation as a maverick.) In a bureaucracy with an established consensus view and well-defined career paths, incentive structures militate against the surfacing of intellectual challenge. The extent to which the standard solutions to this well-known problem depend on anonymous, external channels for maverick concerns to be

escalated up the hierarchy, rather than on changes to the design of career paths and incentives within the organisation itself, shows the difficulty posed by this problem and the need for further research in the design of organisational structures and incentives.

3. A comparison with the economics of law

The economics of security, as a discipline of applied economics, can be compared with the economics of law. In a system of voluntary market exchanges, it is easy to characterise the contractual terms under which economic agents enter into transactions, and the enforcement mechanisms and litigation processes relating to those transactions, as subject to the overall discovery process of the market. The extension of this principle to cover those situations outside contractual relationships in which economic agents find themselves affected by the actions of others, but nevertheless can take decisions about their own welfare, or may choose to enter into contractual relationships with other parties, enabled the whole of common law to be analysed in economic terms, and permitted bold, unifying conjectures such as Posner's (that the common law could be shown to be economically efficient).

Similarly, consideration of security from an economic point of view enables a diverse range of security problems across different technical disciplines to be understood using similar analytical tools. In addition, it should be noted that security interacts with law in that so many decisions, whether taken by individuals or groups, about risk and security are taken or constrained within a legal framework. Such a legal framework typically combines tort law with statute defining particular duties of care (or conversely, in some cases, denying a duty of care on the part of state agents who have immunity for actions carried out in their official capacity) or particular procedural rules for legal action; alternatively the legal framework may define new categories of crimes along with procedural rules. Posner and other legal theorists have offered no arguments as to why we should expect that such statutes should be economically efficient or welfare-maximising.

4. Examples of the economic view of security issues

4.1 Identity cards: does more technology add to security?

Identity cards are a paradigm case of a technological proposal to solve a security problem. The problem in this case is one for the state, how to identify citizens and others with valid immigration status so as to be able to distinguish them from interlopers. Proponents of ID cards argue that solutions to this problem will help in the fight against terrorism, although the 9/11 bombers all held valid visas and the Madrid bombers all held valid Spanish identity cards. The identity card solution, as proposed in the UK, differs from other ID card schemes currently in force in Western Europe. It takes the form of a card embodying security features, to be carried by the subject, which is linked to a record on a central database containing identifying data and other personal data, maintained by the state or its agents. In this solution, unique biometric data are recorded on the card and at the central data repository, in order to tie the card to a single legitimate cardholder. Identity cards are common in continental Europe and have in recent years been proposed in several English-speaking countries, but at the time of writing are a serious legislative proposal only in the UK.

The immediate outcome of this solution is that the multiple overlapping paper-based documentary proofs of identity which have been relied on hitherto (birth certificate, passport, driving licence, bank statements, educational credentials; which, taken together,

establish an identity by “placing” an individual), will be superseded by the single proof of identity offered by the ID card. The process of verifying the identity claimed by the cardholder will require technology to check the biometric measures, rather than the cross-referencing and consistency-checking of multiple paper documents.

From the point of view of anyone wishing to compromise the ID card system and to establish a false identity, the costs of attack differ from those incurred under the previous system. Multiple low-value identity documents are replaced by a single, high-value technological device. This device, and the central database, are single points on which attackers can concentrate their efforts: for example, compare the likely modest salary of a data input clerk or a database administrator at the central data repository with the amount that employee’s services, if corrupted, could be worth to a hostile party. Once forged or compromised, false identities will be easier to pass than under the existing system precisely because the credence generally placed in technology will lull users into a false sense of security.

The identity card, if introduced, is certain to be ineffective, and likely to be counterproductive, for any purpose currently proposed. It has however been offered to the electorate as a solution to threats of terrorism and uncontrolled immigration, on the basis that “something must be done” and that politicians have to be seen to take action however unlikely it is to be effective. Opposition to such measures is undertaken by small activist groups who are prepared to research the issues and often already have substantial background knowledge in the technological aspects. It is not likely to be economically rational for individual voters to research such issues in sufficient depth to be able to form a view. Given this, Wildavsky suggested that citizens should pool their energies by forming study groups to research such public policy issues collectively.

4.2 Will financial transaction reporting detect money flows that finance the greatest security threats?

A similar due diligence measure (that is, a measure that can plausibly be defended in the face of failure, on the grounds that “something had to be done”) is that of the financial reporting carried out as part of the fight against money laundering. Banking technology has enabled the preparation of massive reports of transactions above de minimis limits to be passed regularly by banks to financial regulators. Just as with identity cards, a single point of failure (at the regulator) for the breach of confidentiality has been created. In the fight against terrorism, such regulatory measures are unlikely to be effective in detecting movements of terrorist funding because the amounts of money required to fund a successful terrorist operation are trivial compared with international financial flows: for example, it has been estimated that to mount the 9/11 terror attacks cost a matter of a few hundred thousand dollars. The reader can be certain that the criminals detected by such measures are small or inept, and that professional criminals with large-scale operations will appear to be entirely legitimate.

4.3 Can network economics be used to understand the clash of civilisations?

Another example of an economic concept that can be applied to a security topic is that of network economics, as applied to the “clash of civilisations”. A simple example of a network the value of joining which depends on how many others are members of that network, is the telephone system. If the costs incurred in switching to a different, incompatible network exceed the benefits to the user, that user will be locked in. In such cases, economic theory predicts a market structure with at most a few dominant networks

(some policy analysts have in the past identified the monopolies arising in such markets as natural monopolies which should be run or controlled by the state). The history of competing formats for entertainment media such as video cassettes, and of competing operating systems and application software used in personal computing, show this theory in action. These technologies coalesced around a few de facto standards based on compatibility, interoperability, and (in the case of software) economies of scale in training software developers and users. Another example is that of the rise of English as the international language of commerce.

But these models can also be applied to religions and cultures where religious beliefs exist within social groups with a clear cultural identity. Where such religions promote an ethic of mutual help and solidarity, and where there are barriers to departure to another (or no) religion, these religions can be modelled as networks. Christian culture gave rise historically to a humanist respect for the individual conscience that developed into an Enlightenment secularism which regards religious adherence as a private matter, almost a pastime. The specifically Christian cultural identity was weakened by this philosophical development. Other religions have historically possessed and maintained a stronger cultural identity.

Now, typically a religion makes exclusive claims; that is, it alone is correct and all other religions are false. For such a religion to be successful on its own terms, it must seek to compete effectively in a zero-sum game by checking and containing the advances of its rivals. All religions lose members (at least in this earthly realm) by death, so to maintain and increase their numbers, each religion must operate effective recruitment strategies for new members (such as, being born into the faith, marrying into it, or otherwise converting to it) and erect effective barriers to leaving. The role of the family is thus important in the recruitment strategy, through expectations, reinforced by formal ceremonies, that if an adherent to the faith marries someone outside that faith, then that person will convert to the faith and jointly assume a responsibility to bring their children up within that faith. Barriers to leaving may be socially imposed or, in a theocracy, may be severe legal penalties for apostacy.

Aspects of the above strategies can be seen in the Roman Catholic form of Christianity, and in Islam, numerically very successful religions. An example of a religious group which has failed to take seriously the maintenance of recruitment strategies and barriers to exit, is the Anglican form of Christianity, at least in the West, where a severe decline in numbers and influence has been seen since the 1960s. Anglican cultural identity, once closely related to Englishness and to Anglo-Saxon cultural values, has been attenuated and devalued, as the Anglican church did nothing to counteract, indeed encouraged, the breakdown in social conventions of the 1950s and 1960s on which the recruitment strategies and barriers to exit had depended.

4.4 Who should be held responsible for the actions of terror groups?

In the global war on terror, Anderson explains, using a statistical example of the detection of security weaknesses in a complex information technology system, why, under conditions where conventional enforcement methods are used, attack is easier than defence: the defenders need to be successful all the time while the attackers need to be successful only once. Attackers have a particular interest in identifying one or two security-critical weaknesses to exploit whereas defenders have far less interest in, and resources to, find and plug all security-critical weaknesses. The most efficient solution to this problem may be to combine retribution and deterrence by tackling those who are in the best

position to control the activities of terrorists: that is, the sponsors and hosts of terrorism in rogue or failed states. This approach was proposed as the “Bush Doctrine” shortly after 9/11 (that the US would not distinguish between the terrorists and their state sponsors).

Anderson suggests that the suppression of those terror groups who operate from rogue states may follow a similar course to the suppression of piracy on the high seas from the seventeenth century onwards. Earle’s recent history of the war against piracy draws a series of explicit comparisons with the war on terror. A series of wars took place alongside the development of the current international law on piracy (codified in the 1982 Convention on the Law of the Sea) which, though it restricts the definition of piracy to exclude any acts carried out with state authority or with political intent, is exceptional in that it disregards the sovereignty of the flag, if any, that a pirate vessel is flying, and permits the seizure and confiscation of the vessel and trial of the crew by any state (while normally in international law so much emphasis is placed on the sovereignty and jurisdiction of each state within its own territory and over vessels carrying its own flag). The costs imposed on pirates and the wide scope for enforcement have acted as a severe deterrent to piracy on the high seas.

5. Politicised narratives of security issues

Participants in conflicts may have motives and adopt behaviours which are intended to alter public perceptions and should not be used as data for economic analysis. Western media is particularly vulnerable to this type of manipulation in which legitimacy can be easily fabricated and objective reporting lost in the process. Now, it is true that numerous conflicts have been initiated by the oppression of minority groups by political elites who have monopolised resources and restricted access to justice and to political representation; and that such conflicts have been resolved once these underlying causes have been removed. Given the widespread liberal sympathies within Western democracies toward the plight of such minority groups, and given terror groups’ skill in cultivating the media, the reader can be sure that both liberation groups with a high degree of popular support and legitimacy, and terror groups with neither support nor legitimacy amongst their ostensible constituencies, will lay claim to mass support, will have a media presence and moderate political wings which will attempt to contest elections similarly to conventional political parties, and will have links to civil rights movements advised by lawyers. The only difference between them is that the terror groups will use such marks of apparent legitimacy as human shields. The arguments made by the civil rights movements attached to such groups prove nothing about whether the underlying problems are those of resource allocation or political representation.

The following example illustrates the pitfalls of an oversimplified analysis of motives in conflict. Seldon noted that one of the causes cited for the “Troubles” in Northern Ireland was perceived injustice in a politically-controlled and sectarian process for allocating public housing, and suggested that this cause could be removed if the question of housing were depoliticised and dealt with by the market rather than by politicians. This justification for civil strife (though not Seldon’s proposed solution) was that given by the civil rights movement in Northern Ireland in the late 1960s. But it was not an analysis of the reasons why actors in that conflict behaved as they did. The terror group the IRA, which had lain almost dormant for many years until the late 1960s, faced a democratically-elected British government that believed that its responsibility, when faced with a mass opposition movement which at the extreme shaded off into terrorism, was to isolate the terrorists and to minimise support for them by making concessions to the moderate elements. Such concessions served, in fact, only to emphasize and enhance the power of the terrorists. The IRA’s support and encouragement for the civil rights movement relied primarily on the

predictability of the British response and had no necessary connection to the prima facie issue of public housing.

6. The security conundrum

Given the explanatory power of an economic approach to security questions, why does the technological approach retain its appeal? I believe this is a consequence of the explanatory power of the natural sciences allied to the prestige attaching to applied science and technology, which have created a sort of “common man’s logical positivism” whereby a scientific or technological explanation for any phenomenon, however implausible or irrelevant to the subject matter, is assumed to refute any other type of explanation.

7. Conclusion

Further research in this area should look at the following topics: the design of improvements to legal and institutional structures ensuring that incentives are defined so that security is optimised; the design and promotion of useful analytical techniques for costing security measures.

The naive technological view of security needs to be challenged in the public policy realm, in order that resources needed to counter genuine security threats are not squandered on expensive schemes which at best are wasteful and, at worst, severely damage security not to mention compromising civil rights and democratic accountability.

BIBLIOGRAPHY

Ross Anderson, “Why Information Security is Hard – An Economic Perspective”, in *Proceedings of the Seventeenth Computer Security Applications Conference*, IEEE Computer Society Press (2001), pp 358–365

Peter Earle, *The Pirate Wars*, London: Methuen 2003

Richard Posner, *Economic Analysis of Law*, Boston, MA: Little, Brown 1973

Arthur Seldon, *Capitalism*, Oxford: Blackwell 1991

Aaron Wildavsky*, But is it True?,* Cambridge, MA: Harvard University Press 1995

ABOUT THE AUTHOR

William Arthurs is a director of the Transatlantic Institute. He holds the Certified Information Systems Auditor designation and has worked in the fields of technology and security since the 1980s.

Mr Arthurs is a graduate of the University of Oxford, in Philosophy Politics and Economics.

Contact: williamarthurs {at} t-i.org.uk
Website: http://www.t-i.org.uk

- o -